Cisco Unified Real-Time Monitoring Tool Administration Guide, Release 12.5(1)SU4

First Published: 2023-01-09

Last Modified: 2023-01-31

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

Full Cisco Trademarks with Software License

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

CONTENTS

Preface

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

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

About This Guide

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

Use this guide with the following documentation for your configuration:

Cisco Unified Communications Manager	*System Configuration Guide for Cisco Unified Communications Manager*, *Administration Guide for Cisco Unified Communications Manager*, *Cisco Unified Serviceability Administration Guide*, *CDR Analysis and Reporting Administration Guide*, and *Cisco Unified Communications Manager Call Detail Records Administration Guide*
Cisco Unified Communications Manager IM and Presence Service	*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* and *Cisco Unified Serviceability Administration Guide*
Cisco Unity Connection	*Cisco Unity Connection System Administration Guide* and *Cisco Unity Connection Serviceability Administration Guide*

These documents provide the following information:

- Instructions for administering Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, and Cisco Unity Connection.
- Descriptions of procedural tasks that you can perform by using the administration interface.

Audience

The *Cisco Unified Real-Time Monitoring Tool Administration Guide* provides information for network administrators who are responsible for managing and supporting Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, and Cisco Unity Connection. Network engineers, system administrators, or telecom engineers can use this guide to learn about, and administer, remote serviceability features. This guide requires knowledge of telephony and IP networking technology.

Related Documentation

For additional documentation about Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service, see the *Cisco Unified Communications Manager Documentation Guide*.

For additional documentation about Cisco Unity Connection, see the *Cisco Unity Connection Documentation Guide*.

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.

Convention	Description
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 Dkey.
<>	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.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Cisco Product Security

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`.

Organization

Administration overview

Overview of Unified RTMT, including browser support.

Getting started

Description of how to install, access, and use the Unified RTMT client.

System performance monitoring

Overview of system performance monitoring in RTMT, including how to manage predefined objects for your system, Cisco Unified Communications Manager, Cisco Intercompany Media Engine, Cisco Unified Communications Manager IM and Presence Service, and Cisco Unity Connection.

Cisco Unified Analysis Manager

Provides information about Cisco Unified Analysis Manager, including procedures to install and configure the Unified Analysis Manager; procedures to add nodes that the Unified Analysis Manager can diagnose; procedures for device management; and information about troubleshooting.

Profile and categories

Provides information about how to manage profiles and categories.

Performance counters

Provides procedures for working with performance monitors, including viewing performance counters and counter descriptions, and perfmon logs.

Alerts

Provides procedures for working with alerts.

Trace and Log Central

Provides information about configuring on-demand trace collection and crash dump files for system services and methods to view the trace files in the appropriate viewer.

(Appendix) Performance counters and alerts

Provides a complete list of performance objects and their associated counters for components of your system.

CHAPTER 1

Administration Overview

Cisco Unified Real-Time Monitoring Tool

The Cisco Unified Real-Time Monitoring Tool, which runs as a client-side application, monitors the real-time behavior of your system components. Unified RTMT uses Hypertext Transfer Protocol Secure (HTTPS) and Transmission Control Protocol (TCP) to monitor the following:

- System performance
- Device status
- Device discovery
- Computer Telephony Integration (CTI) applications

Unified RTMT can connect directly to devices through HTTPS to troubleshoot system problems.

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

Unified RTMT allows you to perform the following tasks:

- Monitor a set of predefined management objects that monitor the health of the system.
- Generate various alerts, in the form of email messages, for objects when values go above or below user-configured thresholds.
- Collect and view traces in various default viewers that exist in Unified RTMT.
- View syslog messages in SysLog Viewer.
- Work with performance-monitoring counters.
- Unified Communications Manager only: Translate Q931 messages.

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

- A Unified Communications Manager product on one server.
- Cisco Intercompany Media Engine (Cisco IME) product on one server.
- Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service) product on one server.
- A server on a cluster (to monitor the health of the cluster).

To monitor a product on a different server, you must use a new instance of Unified RTMT.

Operating System Support

You can install Unified RTMT on a computer that is running one of the following operating systems:

- Windows 8
- Windows 10
- Windows 2019
- Linux with KDE or GNOME client

Note For Windows 8 and later, ensure that you launch Unified RTMT in 'Run as administrator' mode. Otherwise, User Access Control (UAC) rights are disabled.

Consider the following information when you install Unified RTMT:

- Unified RTMT requires at least 128 MB in memory to run on a Windows OS platform.
- Unified RTMT requires at least 300 MB of disk space to run on a Windows and Linux OS platform.
- When you install Unified RTMT on a Windows 8 platform, you will see this User Account Control popup message: “An unidentified program wants to access your computer.” Click **Allow** to continue working with Unified RTMT.
- Unified RTMT runs on 32 bit and 64 bit Windows platforms.

CHAPTER 2

Getting Started

Install and Configure Unified RTMT

Install Unified RTMT

Before you begin

- Unified RTMT requires at least 128 MB in memory to run on a Windows OS platform; the tool requires at least 300 MB of disk space to run on a Windows/Linux OS platform.

Note The Linux Unified RTMT plugin CcmServRtmtPlugin.bin can be installed on RHEL 5, RHEL 6, or higher Linux machines. If you want to install it on a RHEL 4 machine, ensure that the glibc (OS library) version is 2.4.x or higher. If the glibc version is 2.3.x or earlier, the underlying JRE install fails.

- The current Unified RTMT download supports earlier releases of Unified Communications Manager or Cisco Unity Connection. Some releases of Unified Communications Manager may require different versions of Unified RTMT to be installed on your computer (one version per Unified Communications Manager release). Verify that the Unified RTMT version that you install is compatible with the product that you are monitoring. If the Unified RTMT version that you are using is not compatible with the server that you want to monitor, the system prompts you to download the compatible version.
- Your computer stores the user preferences, such as the IP address and Unified RTMT frame size, based on the last instance of Unified RTMT that you run.

Note Only the administrators with Standard Audit Users and Standard CCM Super Users privileges have access to Unified RTMT features. If an application user without these privileges logs into Unified RTMT, some of the features such as Call Control Discovery (CCD) and Service Advertisement Framework (SAF) will not work as expected.

Note On a Linux workstation, run RTMT with root access. Otherwise, when you initially install RTMT, the application will not start.

- The current Unified RTMT requires JRE to run. Verify that the system has JRE installed (Java 1.8).

Procedure

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

Interface	How to access
Unified Communications Manager	From Unified Communications Manager Administration, choose **Application** > **Plugins**.
Unified Communications Manager IM and Presence Service	From Unified Communications Manager IM and Presence Administration, choose **Application** > **Plugins**.
Cisco Unity Connection	From Cisco Unity Connection Administration, choose **System Settings** > **Plugins**.

Step 2 Click **Find**.

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

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

Tip When you install Unified RTMT on Windows 7 or later, ensure that you perform the installation as an administrator.

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

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

The extraction process begins.

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

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

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

Step 9 Choose the absolute path of Java Virtual Machine executable from your system (java.exe from the JRE installed directory, that is latest version 1.8) as prompted in the installation screen of Unified RTMT.

Step 10 Choose the location where you want to install Unified RTMT. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next**.

Step 11 To begin the installation, click **Next**.

The **Setup Status** window appears.

Step 12 To complete the installation, click **Finish**.

Upgrade RTMT

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

RTMT saves user preferences and downloaded module jar files locally on the client machine. The system saves user-created profiles in the database, so you can access these items in Unified RTMT after you upgrade the tool.

Before you begin

Before you upgrade to a newer version of RTMT, Cisco recommends that you uninstall the previous version.

Procedure

Step 1 From Unified Communications Manager Administration, choose **Application** > **Plugins**.

Step 2 Click **Find**.

Step 3 Perform one of the following actions:

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

Step 4 Download the installation file to your preferred location.

Step 5 Locate and run the installation file.
The extraction process begins.

Step 6 In the RTMT welcome window, click **Next**.

Step 7 Because you cannot change the installation location for upgrades, click **Next**.
The Setup Status window appears; do not click Cancel.

Step 8 In the **Maintenance Complete** window, click **Finish**.

Launch Unified RTMT

Before you begin

For single sign-on in Windows 8.1, run Unified RTMT as an administrator.

Note If your Root or Intermediate CA Certificate uses the RSASSA-PSS signature algorithm, do not sign the Tomcat certificate with this CA; otherwise, RTMT will not launch. This is because the TLS versions through 1.2 does not support the RSASSA-PSS Signature Algorithm and a bug is opened against Java to add this support in a future TLS version.

Note Ensure that all of the required hostnames for the Unified Communications Manager clusters are reachable from your local machine for the RTMT functionalities to work properly.

This requires adding the hostnames to the host file on the local machine. For example:

- For Unified RTMT running on Windows OS platform, use the following format to update the host file located at `C:\Windows\System32\drivers\etc\hosts`: **<ServerIP> <Hostname> <FQDN>**
- For Unified RTMT running on Linux OS platform, use the following format to update the host file located at

  `->/etc/hosts`: **<ServerIP> <Hostname> <FQDN>**

Download tzupdater.jar files to the JRE_HOME/bin directory used by Unified RTMT before launching Unified RTMT for the first time. It is required to update the time zone of your system's JRE used by Unified RTMT to that of the server that Unified RTMT tries to connect.

Procedure

Step 1 After you, install the plug-in, open Unified RTMT.

If you have a Windows 8.1, or Windows 10 client and you want to use the single sign-on feature, right click the Unified RTMT shortcut on your desktop or start menu and click **Run as Administrator**. Before launching RTMT on Windows 7 or Vista, ensure that the User Account Control (UAC) feature is disabled. For more information on UAC feature, go to this URL: https://docs.microsoft.com/en-us/windows/desktop/uxguide/winenv-uac.

Step 2 If you choose to synchronize the time zone, perform the following steps.

a) Open the command prompt and navigate to JRE_HOME/bin directory used by Unified RTMT.

b) Verify the existing time zone version using the TZUpdater tool with the following command, which is: **java -jar tzupdater.jar -V**

Important To update time zone data successfully, you should ensure that you have sufficient privileges to modify the JDK_HOME/jre/lib or JRE_HOME/lib directory used by Unified RTMT. If you do not have sufficient privileges to modify these directories, contact your system administrator.

Note The RTMT will not recognize the latest version if the JRE is upgraded automatically to a newer version, as the older JRE version is uninstalled from your machine.

For example, while RTMT installation, if you have selected the version JRE 1.8.0.131 which is installed in the following directory: C:\Program Files (x86)\Java\jre1.8.0_131. Then, when JRE is upgraded it deletes the older directory jre1.8.131 and new directory gets created which is not recognized by RTMT, that is C:\Program Files (x86)\Java\jre1.8.0_144.

When you try to launch RTMT from the desktop shortcut (Cisco Unified Real-Time Monitoring Tool 12.0.exe), it prompts the launch error message as `Windows error 2 occurred while loading the Java VM`. You can resolve this issue, by re-installing the RTMT or use the run.bat in the RTMT installed directory.

c) Download a copy of the desired tzdata.tar.gz bundle to a local directory from http://www.iana.org/time-zones/.

d) Enter the following command, which is: **Java -jar tzupdater.jar -l < location of tzdata.tar.gz bundle>**

Note -l supports URL protocols. For example, http://www.iana.org/time-zones/repository/tzdata-latest.tar.gz. The supported URL protocols are http://, https://, file://. If no URL link is provided, then the tool uses the latest IANA tzdata bundle at http://www.iana.org/time-zones/repository/tzdata-latest.tar.gz.

For more information on time zone updates, go to this URL:http://www.oracle.com/technetwork/java/javase/tzupdater-readme-136440.html.

e) Check the time zone version updated in your system by using the TZUpdater tool with the following command, which is: **java -jar tzupdater.jar -V**

f) Relaunch Unified RTMT.

Important Run the commands as an Administrator.

Step 3 In the **Host IP Address** field, enter either the IP address or hostname of the node or (if applicable) the node in a cluster.

Step 4 Click **OK**.

- If the single sign-on feature is enabled, Unified RTMT does not prompt for the username and password; proceed to step 9.
- If the single sign-on is not enabled, Unified RTMT displays another window prompting for the username and password. Enter the details as given in the following steps.

Step 5 In the **User Name** field, enter the Administrator username for the application.

Step 6 In the **Password** field, enter the Administrator user password that you established for the username.

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

Step 7 When prompted, add the certificate store by clicking **Yes**.

Unified RTMT starts.

Note If you sign in using the single sign-on feature, Unified RTMT prompts once for a username and password after you click any one of the following menus:

- **System** > **Performance** > **Performance log viewer**
- **System** > **Tools** > **Trace and Log Central**
- **System** > **Tools** > **Job status**
- **System** > **Tools** > **Syslog Viewer**
- **Voice/Video** > **CallProcess** > **Session Trace**
- **Voice/Video** > **CallProcess** > **Called Party Tracing**
- **Voice/Video** > **Report** > **Learned Pattern**
- **Voice/Video** > **Report** > **SAF forwarders**
- **Analysis Manager**

What to do next

You can create a user with a profile that is limited only to Unified RTMT usage. The user will have full access to Unified RTMT but will not have permission to administer a node.

You can create a Unified RTMT user by adding a new application user in the administration interface and adding the user to the predefined Standard RealtimeAndTraceCollection group.

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

Related Topics

Run a Program as an Administrator, on page 8

Run a Program as an Administrator

Follow this procedure to run a program as an administrator in Windows 7 and later.

Note To use SSO with Unified RTMT on Windows, run Unified RTMT as an administrator.

Before you begin

Be aware of the following behavior:

- If you're using single sign-on (SSO), allow time for Unified RTMT to load.
- For the time zone synchronization prompt, selecting **Yes** causes Unified RTMT to close itself. After this happens, you must manually restart the program as an administrator.

Procedure

Step 1 Locate the program shortcut.

Step 2 Right-click the shortcut.

Step 3 Perform one of the following actions:

- Right-click the shortcut and select **Run as administrator** (Windows 7 and 8.x).
- Right-click the shortcut and select **More** > **Run as administrator** (Windows 10).
- **a.** Right-click the shortcut.

  b. Select **Properties**.

  c. Under the shortcut tab, click **Advanced**.

  d. Check the **Run as administrator** check box.

Multiple installations of Unified RTMT

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

- A Unified Communications Manager product on one node
- An Intercompany Media Engine (IME) product on one node.
- An IM and Presence Service on one node.
- A node on a cluster to monitor the health of the cluster.

To monitor a product on a different node, you must use a new instance of Unified RTMT that is installed.

Multiple copies of Unified RTMT that are installed on your computer let you simultaneously monitor multiple IM and Presence Services that are installed on different nodes.

When you install multiple copies of Unified RTMT on a single computer, you must install Unified RTMT in different folders. Cisco recommends that you install no more than four copies of Unified RTMT on a computer.

Because installing another copy of Unified RTMT overwrites the shortcut icon, you should complete the following tasks:

1. Create another icon by creating a shortcut to `jrtmt.exe` in the folder with the previous installation.
2. Rename the icon accordingly.

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

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

Administration Tools

System Interface

The Unified RTMT interface consists of the following components:

- **Menu bar**: the menu bar includes some or all of the following options, depending on your configuration:

  File

  Allows you to save, restore, and delete existing RTMT profiles, monitor Java Heap Memory Usage, go to the Serviceability Report Archive window in Cisco Unified Serviceability, log off, or exit RTMT.

  > **Note**
  >
  > 1. The RTMT menu option **File** > **Cisco Unified Reporting** lets you access Cisco Unified Reporting from RTMT. You can use the Cisco Unified Reporting application to snapshot cluster data for inspection or troubleshooting. For more information, see the *Cisco Unified Reporting Administration Guide*.
  > 2. As part of creating the heap dump faster, a core(core.jvm.core) file is generated to make the heap dump creation process (generation) fast.

  System

  Allows you to monitor system summary, monitor server resources, work with performance counters, work with alerts, collect traces, and view syslog messages.

  Voice/Video

  Allows you to view Unified Communications Manager summary information on the server; monitor call-processing information; and view and search for devices, monitor services, and CTI.

  IM and Presence

  Allows you to view IM and Presence Service and Cisco Jabber summary information on the server.

  Cisco Unity Connection

  Allows you to view the Port Monitor tool.

  IME Service

  Allows you monitor server and network activity of the Cisco Intercompany Media Engine server.

  Edit

  Allows you to configure categories (for table format view), set the polling rate for devices and performance monitoring counters, hide the quick launch channel, and edit the trace setting for RTMT.

  Window

  Allows you to close a single RTMT window or all RTMT windows.

Application

Depending on your configuration, allows you to browse the applicable web pages for administration interfaces, Cisco Unified Serviceability, and Cisco Unity Connection Serviceability.

Help

Allows you to access RTMT online help documentation and to view the RTMT version.

- **Quick Launch channel**: Pane that displays information about the server or information about the applications. The tab contains groups of icons that you can click to monitor various objects.
- **Monitor pane**: Pane where monitoring results are displayed.

Performance Monitoring

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

You can monitor the performance of the components of the system and the components for the application on the system by choosing the counters for any object by using the Cisco Unified Real-Time Monitoring Tool. The counters for each object display when the folder expands.

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

RTMT integrates with existing software for performance monitoring:

- RTMT integrates with your administration and serviceability software.
- RTMT displays performance information for all system components.

RTMT provides alert notifications for troubleshooting performance. It also periodically polls performance counter to display data for that counter. You can choose to display perfmon counters in a chart or table format.

Performance monitoring allows you to perform the following tasks:

- Monitor performance counters from all Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection servers.
- Continuously monitor a set of preconfigured objects and receive notification in the form of an email message.
- Associate counter threshold settings to alert notification. An email or popup message provides notification to the administrator.
- Save and restore settings, such as counters that are being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.
- Display up to six perfmon counters in one chart for performance comparisons.
- Use performance queries to add a counter to monitor.

System summary status

The Real-Time Monitoring Tool provides a set of default monitoring objects that help you to monitor the health of the system. Default objects include performance counters or critical event status for the system and other supported services. The system summary in Unified RTMT allows you to monitor important common information in a single monitoring pane. In system summary, you can view information about the following predefined objects:

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

Server Status Monitoring

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

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

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

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

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

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

For a specific description of each state, see the following table.

Table 1: Status of Critical Services

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

Performance Counter Interface

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

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

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

Category Tabs

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

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

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

Sample Rate

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

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

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

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

Zoom In on Perfmon Counter

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

Procedure

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

- To zoom in predefined objects, such as System Summary, perform one of the following actions:
  - Drag the mouse over the plot area in the counter to frame the data and release the mouse button. The counter zooms in the chart.
  - Click the counter. The counter zooms in.
- To zoom counters in the Performance pane, perform one of the following actions (and resize the window, if necessary):

- Double-click the counter that you want to zoom. The box with the counter appears highlighted and the Zoom window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.
- Click the counter to select the counter to zoom. The box with the counter appears highlighted.
- Right-click the counter and select **Zoom Chart** or choose **System** > **Performance** > **Zoom Chart**. The **Zoom** window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.

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

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

Highlight Charts and Graphs

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

Procedure

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

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

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

Counter Properties

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

The Counter Property window contains the option to configure data samples for a counter. The performance counters that display in the Unified RTMT performance monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option to view the data that a perfmon counter collected.

Related Topics

Performance Counters and Alerts, on page 169

Alert Notification for Counters

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

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

Trace and Log Central

The Trace and Log Central feature in RTMT allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to a SFTP or FTP server on your network, or collect a crash dump file.

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

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

Note

- To use the Trace and Log Central feature, make sure that RTMT can directly access the node or all of the nodes in a cluster without Network Access Translation (NAT). If you have set up a NAT to access devices, configure the nodes with a hostname instead of an IP address, and make sure that the hostnames (Fully Qualified Domain Name of the host) and their routable IP address are in the DNS node or host file.
- For devices that support encryption, the SRTP keying material doesn't display in the trace file.

Related Topics

Cisco Unified Analysis Manager Setup, on page 68

Trace Files Collection, Throttling, and Compression

The Collect Files option in Trace and Log Central collects traces for services, applications, endpoints, and system logs on the server or on one or more servers in the cluster.

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

RTMT Trace and Log Central Disk I/O and CPU Throttling

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

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

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

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

Configuration Profiles

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

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

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

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

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

Related Topics

Add Configuration Profile, on page 89

Categories

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

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

Note Changes to the profile settings for the default profile on IM and Presence Service are not transferred to Unified Communications Manager. IM and Presence Service profiles are renamed with the prefix “Presence_”.

Related Topics

Add Category , on page 90

Alerts

The system generates alert messages to notify administrators when a predefined condition is met, such as when an activated service goes from up to down. Alerts can be sent out as email or epage.

Unified RTMT, which supports alert defining, setting, and viewing, contains preconfigured and user-defined alerts. Although you can perform configuration tasks for both types, you cannot delete preconfigured alerts (whereas you can add and delete user-defined alerts).

Alert options

The Alert menu (**System** > **Tools** > **Alert**) comprises the following menu options:

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

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

- Set Alert/Properties: This menu option allows you to set alerts and alert properties.
- Remove Alert: This menu category allows you to remove an alert.
- Enable Alert: With this menu category, you can enable alerts.
- Disable Alert: You can disable an alert with this category.
- Suspend cluster/Node Alerts: This menu category allows you to temporarily suspend alerts on a particular IM and Presence node or on the entire cluster.

- Clear Alerts: This menu category allows you to reset an alert (change the color of an alert item from red to black) to signal that an alert has been taken care of. After an alert has been raised, its color automatically changes to in Unified RTMT and stays that way until you manually clear the alert.
- Clear All Alerts: This menu category allows you to clear all alerts.
- Reset all Alerts to Default Config: This menu category allows you to reset all alerts to the default configuration.
- Alert Detail: This menu category provides detailed information on alert events.
- Config Email Server: In this category, you can configure your email server to enable alerts.
- Config Alert Action: This category allows you to set actions to take for specific alerts; you can configure the actions to send the alerts to desired email recipients.

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

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

Alert Fields

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

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

The following table provides a list of fields that you may use to configure each alert; users can configure preconfigured fields, unless otherwise noted.

Table 2: Alert Customization

Field	Description	Comment
Alert Name	High-level name of the monitoring item with which Unified RTMT associates an alert	Descriptive name. For precon you cannot change this field. related to Alert Central displ of preconfigured alerts.
Description	Description of the alert	You cannot edit this field for alerts. See topics related to A displays for a list of preconfi
Performance Counter(s)	Source of the performance counter	You cannot change this field associate only one instance o performance counter with an

Field	Description	Comment
Threshold	Condition to raise alert (value is...)	Specify up < - > down, less than greater than #, %, rate. This fiel applicable only for alerts based performance counters.
Value Calculated As	Method used to check the threshold condition	Specify value to be evaluated as delta (present - previous), or % field is applicable only for alerts performance counters.
Duration	Condition to raise alert (how long value threshold has to persist before raising alert)	Options include the system sendi immediately or after a specified the alert has persisted. This field applicable only for alerts based performance counters.
Number of Events Threshold	Raise alert only when a configurable number of events exceeds a configurable time interval (in minutes).	For ExcessiveVoiceQualityRepo default thresholds equal 10 to 60 For RouteListExhausted and MediaListExhausted, the defaul to 60 minutes. This field is appli for event based alerts.
Node IDs (Applies to Unified Communications Manager and the IM and Presence Service)	Cluster or list of servers to monitor	Unified Communications Manag CiscoTFTP server, or first server. is applicable only for non-cluste alerts. **Note** When you deactivat CiscoCallManager CiscoTFTP services server, the system c that server as remov the currently monito list. When you reacti CiscoCallManager CiscoTFTP services server is added bac settings are restored values.
Alert Action ID	ID of alert action to take (System always logs alerts no matter what the alert action.)	Alert action is defined first (see Customization topic). A blank fi indicates that e-mail is disabled.
Enable Alerts	Enable or disable alerts.	Options include enabled or disab
Clear Alert	Resets alert (change the color of an alert item from red to black) to signal that the alert is resolved	After an alert is raised, its color automatically changes to black a until you manually clear the alert. All to clear all alerts.

Field	Description	Comment
Alert Details (Applies to Unified Communications Manager and the IM and Presence Service)	Displays the detail of an alert (not configurable)	For ExcessiveVoiceQualityR RouteListExhausted, and MediaListExhausted, up to 30 details display in the current interval if an alert is raised in interval. Otherwise, the prev details in the previous interva DChannel OOS alert, the list o OOS devices at the time the a appears.
Alert Generation Rate	How often to generate alert when alert condition persists	Specify every X minutes. (Ra every X minutes if condition Specify every X minutes up (Raise alert Y times every X condition persists.)
User Provide Text	Administrator to append text on top of predefined alert text	—
Severity	For viewing purposes (for example, show only Sev. 1 alerts)	Specify defaults that are prov predefined (for example, Err Information) alerts.

Related Topics

Performance Counters and Alerts, on page 169

Alert Logs

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

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

The following filename format for the alert log applies: `AlertLog_MM_DD_YYYY_hh_mm.csv`.

The alert log includes the following attributes:

- Time Stamp: Time when RTMT logs the data
- Alert Name: Descriptive name of the alert
- Node: Server name for where RTMT raised the alert
- Alert Message: Detailed description about the alert
- Type: Type of the alert
- Description: Description of the monitored object

- Severity: Severity of the alert
- PollValue: Value of the monitored object where the alert condition occurred
- Action: Alert action taken
- Group ID: Identifies the source of the alert

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

Log Partition Monitoring Tool

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

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

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

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

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

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

To configure Log Partitioning Monitoring, set the alert properties for the LogPartitionLowWaterMarkExceeded and LogPartitionHighWaterMarkExceeded alerts in Alert Central.

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

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

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

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

Cisco Unified Analysis Manager

The Cisco Unified Analysis Manager, a tool included with the Cisco Unified Real-Time Monitoring Tool, is used to perform troubleshooting operations. When the Unified Analysis Manager is launched, it collects troubleshooting information from your system and provides an analysis of that information. You can use this information to perform your own troubleshooting operation or to send the information to Cisco Technical Assistance for analysis.

The Unified Analysis Manager application is installed as an option when you install the RTMT software. You can access the Unified Analysis Manager interface from the RTMT main menu and quick launch channel.

After it is installed, the application can identify the supported Unified Communications (UC) products and applications that you have in your system and troubleshoot call failures across these UC applications, collecting trace and log files.

The Unified Analysis Manager supports the following products:

- Unified Communications Manager
- Cisco Unified Contact Center Enterprise (Unified CCE)
- Cisco Unified Contact Center Express (Unified CCX)
- Cisco IOS Voice Gateways (37xx, 28xx, 38xx, 5350XM, 5400XM) IOS Release PI 11
- Cisco Unity Connection
- IM and Presence Service

The three primary components of the Unified Analysis Manager interface are as follows:

- Administration: The administration component lets you import device and group configuration from an external file and provide a status of jobs run by the Unified Analysis Manager.
- Inventory: The inventory component is used to identify all of the devices in your system that can be accessed and analyzed by the Unified Analysis Manager.
- Tools: The tools component contains all of the functions that Unified Analysis Manager supports. This includes configuring traces settings, collecting logs, and viewing configurations.

Related Topics

View Trace and Log Central Options, on page 126

Services, Servlets, and Service Parameters

To support the Unified RTMT client, there are a number of services that needs to be active and running on the server. Unified RTMT uses the following services and servlets:

- Cisco AMC service: This service starts up automatically after the installation and allows Unified RTMT to retrieve real-time information that exists on nodes in the cluster. The IM and Presence service automatically assigns the first node as the primary collector. For Unified RTMT to continue to retrieve information when the primary collector fails, you must configure a subsequent node as the failover collector in Service Parameters in the administration interface.

  The following list comprises some Cisco AMC service parameters that are associated with Unified RTMT. For the latest list of parameters, select **System** > **Service Parameters** in the administrative interface. Then, select the server and the Cisco AMC service.

  - Primary Collector
  - Failover Collector
  - Data Collection Enabled
  - Data Collection Polling Rate
  - Server Synchronization Period
  - RMI Registry Port Number
  - RMI Object Port Number
  - Logger Enabled
  - Unified Communications Manager: Alarm Enabled
  - Unified Communications Manager: AlertMgr Enabled
  - Cisco Unity Connection: PerfMon Log Deletion Age
  - Cisco Unity Connection: AlertMgr Enabled

  For information about these service parameters, select the **?** button that displays in the Service Parameter configuration window of the administrative interface.

The following list comprises some network services and servlets that are associated with Unified RTMT. In Cisco Unified Serviceability, select **Tools** > **Control Center - Network Services** to view these services.

- Cisco CallManager Serviceability RTMT: Supports the Unified RTMT; this service starts up automatically after the installation.
- Cisco RIS Data Collector: The Real-time Information Server (RIS) maintains real-time information such as performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as Real-Time Monitoring Tool, SOAP applications, and AlertMgrCollector (AMC) to retrieve the information that is stored on the server.
- Cisco Tomcat Stats Servlet: The Cisco Tomcat Stats Servlet allows you to monitor the Tomcat perfmon counters by using Unified 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 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 the Unified RTMT client. If you stop this service on a server, you cannot collect or view traces on that 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 Unified RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.
- Cisco Log Partition Monitoring Tool: This service which starts up automatically after the installation, monitors the disk usage of the log partition on a server.
- Cisco SOAP-Real-Time Service APIs: The Cisco SOAP-Real-Time Service APIs, which start automatically after the installation, allow Unified RTMT to collect real-time information for devices and CTI applications.
- Cisco SOAP-Performance Monitoring APIs: This service, which starts up automatically after the installation, allows Unified RTMT to use performance monitoring counters for various applications through SOAP APIs.
- Cisco RTMT Reporter servlet: This service, which starts up automatically after the installation, allows you to publish reports for Unified RTMT.

Nonconfigurable Components

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

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

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

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

You can display log files, except an alert log file, by using the Performance log viewer in Unified RTMT or by using the native Microsoft Performance viewer. You can view an alert log file by using any text editor.

To download log files to a local machine, you can use the collect files option in Trace and Log Central in Unified RTMT.

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

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

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

Tip The Unified RTMT reports appear in English only.

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

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

For more information about the Serviceability reports, see the “Serviceability Reports” chapter in the *Cisco Unified Serviceability Administration Guide*.

Java Requirements for SAML SSO Login to RTMT via Okta

If you have SAML SSO configured with Okta as the identity Provider, and you want to use SSO to log in to the Cisco Unified Real-Time Monitoring Tool, you must be running a minimum Java version of 8.221. This requirement applies to 12.5(x) releases of Cisco Unified Communications Manager and the IM and Presence Service.

Uninstall Unified RTMT

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

Note When you uninstall Unified RTMT on a Windows 8.1 machine, the following User Account Control popup message appears: "An unidentified program wants to access your computer." Click **Allow** to continue working with Unified RTMT.

Procedure

Step 1 Close any active sessions of Unified RTMT.

Step 2 To uninstall Unified RTMT, perform one of the following actions:

a) For a Windows client, choose **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**

b) For a Red Hat Linux installation with KDE or GNOME client, choose **Start** > **Accessories** > **Uninstall Real-time Monitoring tool** from the task bar.

Step 3 Finish uninstalling the plug-in.

CHAPTER 3

System Performance Monitoring

Predefined System Objects

Unified RTMT displays information about predefined system objects in the monitoring pane.

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

For information about service parameters, see the administration online help.

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

The following table provides information about the predefined objects that RTMT monitors.

Table 3: System Categories

Category	Description
System Summary	Displays information about Virtual Memory usage, CPU usage, Common Partition Usage, and the alert history log. To display information about predefined system objects, choose **System** > **System Summary**.

Category	Description
Server	• CPU and Memory: Displays information about CPU usage and Virtual memory usage for the server. To display information about CPU and Virtual memory usage, choose **System** > **Server** > **CPU and Memory**.To monitor CPU and memory usage for specific server, choose the server from the host drop-down list box. • Process: Displays information about the processes that are running on the server. To display information about processes running on the system, choose **System** > **Server** > **Process**. To monitor process usage for specific server, choose the server from the Host drop-down list box. • Disk Usage: Displays information about disk usage on the server. To display information about disk usage on the system, choose **System** > **Server** > **Disk Usage**. To monitor disk usage for specific server, choose the server from the host drop-down list box. • Critical Services: Displays the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services existed in a particular state for the server or for a particular server in a cluster (if applicable). To display information about critical services, choose **System** > **Server** > **Critical Services**, then click the applicable tab: • To display system critical services, click the **System** tab. • To display Unified Communications Manager critical services, click the **Voice/Video** tab. **Note** You can view the Voice/Video tab only if you select a Unified Communications Manager server from the host drop-down list box. • To display IM and Presence Service critical services, click the **IM and Presence** tab. **Note** You can view the IM and Presence tab only if you select an IM and Presence Service server from the host drop-down list box. • To display Cisco Unity Connection critical services, click the **Cisco Unity Connection** tab. • To monitor critical services for specific server on the tab, choose the server from the host drop-down list box and click the critical services tab in which you are interested. If the critical service status indicates that the administrator stopped the service, the administrator performed a task that intentionally stopped the service; for example, the service stopped because the administrator backed up or restored Unified Communications Manager; performed an upgrade; or stopped the service in Cisco Unified Serviceability or the CLI. **Note** If the critical service status displays as unknown state, the system cannot determine the state of the service.

Voice and Video Monitoring

Predefined Cisco Unified Communications Manager Objects

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

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

For more information about service parameters, see the *System Configuration Guide for Cisco Unified Communications Manager* or *Cisco Unity Connection System Administration Guide*.

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

The following table provides information about the predefined object that Unified RTMT monitors.

Table 4: Cisco Unified Communications Manager Categories

Category	Description
Voice and Video Summary	Displays registered phones, calls in progress, and active MGCP ports and channels. To display information about predefined Unified Communications Manager objects, choo **Voice/Video** > **Voice and Video Summary**.

Category	Description
Call Process	• Call Activity: Displays the call activity on Unified Communications Manager, including completed, calls attempted, calls in progress, and logical partition total failures. This incl all servers in the cluster, if applicable. To display information about call activities, choose **Voice/Video** > **Call Process** > **Call Activity**. • Gateway Activity: Displays gateway activity on Unified Communications Manager, inclu active ports, ports in service, and calls completed. This includes all servers in the cluster applicable. To display information about gateway activities, choose **Voice/Video** > **Call Process** > **Gateway Activity**. Select the type of gateway interface from the **Gateway Type** drop-d list. • Trunk Activity: Displays the trunk activity on Unified Communications Manager, incluc calls in progress and calls completed. This includes all servers in the cluster, if applicabl To display information about trunk activities, choose **Voice/Video** > **Call Process** > **Tru Activity**. Select the trunk type in the **Trunk Type** drop-down list. • SDL Queue: Displays SDL queue information, including number of signals in queue an number of processed signals. To display information about the SDL Queue, choose **Voice/Video** > **Call Process** > **SD Queue**. Select the type from the **SDL Queue Type** drop-down list. • SIP Activity: Displays SIP activity on Unified Communications Manager, including summ requests, summary responses, summary of failure responses in, summary of failure respo out, retry requests out, and retry responses out. This includes all servers in the cluster, if applicable. To display information about SIP activities, choose **Voice/Video** > **Call Process** > **SIP Acti**
Session Trace	Displays all SIP message activity: specifically, the incoming and outgoing calls and sessions pass through the Unified Communications Manager. Provides associated call flow diagram for SIP transaction. To display information about Session Trace, choose **Voice/Video** > **Call Process** > **Session Tr**
Device	Device Summary displays information about the Unified Communications Manager server, inclu the number of registered phone devices, registered gateway devices, registered other station dev and registered media resource devices. This includes all servers in the cluster, if applicable. Device Search displays cluster name and device types in a tree hierarchy and allows you to q for information about phones and devices. Phone Summary displays information about the Unified Communications Manager server, inclu the number of registered phones, registered SIP phones, registered SCCP phones, partially regist phones, and the number of failed registration attempts. This includes all servers in the cluster applicable. To display information about the number of registered phones, gateways, and media resource devices on Unified Communications Manager, choose **Voice/Video** > **Device** > **Device Summ** **Tip** To monitor other devices, you must perform additional configuration steps.

Category	Description
Service	• Cisco TFTP: Displays Cisco TFTP status on the Unified Communications Manager including total TFTP requests and total TFTP requests aborted. This includes all serv the cluster, if applicable. To display information about the Cisco TFTP service, choose **Voice/Video** > **Service** **TFTP**. • Heartbeat: Displays heartbeat information for the Unified Communications Manager TFTP service. To display the heartbeat status of Unified Communications Manager servers, Cisco T servers, choose **Voice/Video** > **Service** > **Heartbeat**. • Database Summary: Provides connection information for the server, such as the chan notification requests that are queued in the database, change notification requests tha queued in memory, the total number of active client connections, the number of replic have been created, and the status of the replication. To display information about the database, choose **Voice/Video** > **Service** > **Databa** **Summary**.
CTI	Displays information about the devices and applications that interfaces with the CTI Man To display information about CTI Applications, choose **Voice/Video** > **CTI** > **CTI Mana** To monitor specific CTI types, you must perform additional configuration steps. See topic to monitoring CTI applications, devices, and lines.
Intercompany Media Services	• Routing: Displays the total number of Cisco Intercompany Media Engine routes mai by Unified Communications Manager. To display information about call activities, choose **Voice/Video** > **Intercompany M** **Services** > **Routing**. • Call Activities: Displays the Cisco Intercompany Media Engine call activity, includi number of calls that were accepted, busy, no answer, and failed. To display information about call activities, choose **Voice/Video** > **Intercompany M** **Services** > **Call Activities**.

Cisco Unified Communications Manager Summary View

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

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

Call-Processing Activity Monitoring

The Call Process monitoring category monitors the following items:

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

The following table provides information about the call processing objects that RTMT monitors, the alert, thresholds, and defaults. For information about call activity daily reports, see the *Cisco Unified Serviceability Administration Guide*.

Table 5: Call Processing Category

Monitored Objects (displayed)	Alert/Threshold/Default
CallsAttempted, CallsCompleted, CallsInProgress, and Logical Partition Failures Total for each server and cluster (if applicable).	—
CallsAttempted, CallsCompleted, and CallsInProgress of each type of MGCP FXS/FXO/PRI/T1CAS/H.323 gateway, as well as SIP and H.323 Trunks for each server and cluster (if applicable).	—
Channel/Port Status of each MGCP FXS/FXO/PRI/T1CAS gateway.	—
SDL Queue activity on each server.	—

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

Call-Processing Logs

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

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

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

- trunkH323_CallsInProgress: Average of all the values collected in last 5 minutes
- trunkH323_CallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsAttempted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsInProgress: Average of all the values that were collected in last 5 minutes
- trunkSIP_CallsCompleted: Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXS_PortsInService: Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_PortsInService: Average of all the values that were collected in lasts 5 minutes
- gwMGCP_PRI_SpansInService: Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_SpansInService: Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_ActivePorts: Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_ActivePorts: Average of all the values that were collected in last 5 minutes
- gwMGCP_PRI_ActiveChannels: Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_ActiveChannels: Average of all the values that were collected in last 5 minutes

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

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

The first line of each log file comprises the header.

Perform Session Trace

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

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

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

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

You can also save the call logs on your local system. Based on the saved call logs, RTMT can search for the matching calls, list the matching records, and provide SIP Message Call Flow Diagrams.

Before you begin

Perform the following task:

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

Monitor Real-Time Data

Follow this procedure to monitor real-time data using RTMT.

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

Note In Calling Number/URI, Called Number/URI, you can use wildcard character "*" to match any number of characters. For example, a search for 123* fetches numbers like 123, 1234, or 123456.

If you want to search for numbers with a “*” in them, use “*”. For example, to search for a Called Number like 12*45, enter 12*45 in the search box.

Procedure

Step 1 To display information about Session Trace, from the RTMT menus, choose **Voice/Video** > **Call Process** > **Session Trace Log View** > **Real Time Data**.

The Real Time Data screen appears.

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

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

If matching calls are found, the Matching Call pane displays Start Time, Calling DN, Original Called DN, Final Called DN, Calling Device Name, Called Device Name, and Termination Cause Code.

Note The Called Party Trace feature adds the Calling Device Name and Called Device Name fields.

- Calling and Called device names will not be available for failed calls such as calls made to unreachable destinations.
- The Termination Cause Code helps to identify the failed calls, and provides the reason for the failure of the calls. The Termination Cause Code is displayed in parenthesis followed by description.
- If the call is in progress or if the call trace logging is turned off after the call, the Termination Cause Code column remains blank.

After the call records are displayed in the Matching Calls pane, you can trace calls.

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

Monitor Session Trace Data From Local Disk

Follow this procedure to monitor session trace data from the logs that are saved on your local disk:

Procedure

Step 1 From the RTMT menus, choose **Voice/Video** > **Call Process** > **Session Trace Log View** > **Open from Local Disk**.

The Open from Local Disk screen appears.

Step 2 In the **File Location** field, specify the directory where the call log files are saved on your local disk. You can click **Browse** to specify the directory path.

Step 3 Check the **Enable Time Based Search** check box to view call records for a specific duration. If you check this check box, you can specify the duration in **Duration** field. If you do not check this check box, you will not be able to specify the duration. In such cases, all the calls from the specified Start Time that are present in the saved log files will be displayed.

Step 4 Enter the search criteria and click **Run.**

Note In Calling Number/URI, Called Number/URI, you can use the wildcard character '*' to match any number of characters. For example, a search for 123* fetches numbers like 123, 1234, 123456.

If you want to search for numbers with a '*' in them, use '*'. For example, to search for a Called Number like 12*45, enter 12*45 in the search box.

If matching calls are found, the Matching Call pane displays Start Time, Calling DN, Original Called DN, Final Called DN, Calling Device Name, Called Device Name, and Termination Cause Code.

Note The Called Party Trace feature adds the Calling Device Name and Called Device Name fields.

a) Calling and Called device names will not be available for failed calls such as calls made to unreachable destinations.
b) The Termination Cause Code helps to identify the failed calls, and provides the reason for the failure of the calls. The Termination Cause Code is displayed in parentheses followed by description.
c) If the call is in progress or if the call trace logging is turned off after the call, the Termination Cause Code column remains blank.

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

Trace Calls

Follow this procedure to trace call records displayed as per the specified search criteria.

Note Use this procedure along with “Monitor real-time data” and “Monitor session trace data from local disk.”

Procedure

Step 1 Select a call (a row) to trace.

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

Step 2 To generate the SIP Message Call Flow Diagram, click **Trace Call**. If you want to stop the generation of the session information, click **Cancel** on the progress window.

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

Step 3 Click the tabs that you want to view. The following tabs are available:

a) Call Flow Diagram: Displays the corresponding SIP messages in the Call Flow Diagram.
b) Log File: Displays the entire log file.
c) SIP Message: Appears only when the **Include SIP Message** check box is checked. Displays the actual SIP message that is logged into the SDI log file.

Step 4 Move your mouse over the SIP messages in the Call Flow Diagram. The following table lists the details that are displayed:

Field	Description
Sender	Displays the IP address of the originating call.
GUID	Displays the SIP call ID.
Message Label	Displays the message type for the corresponding SIP message onto which you move your mouse; for example, 200 OK, or 180 Ringing.
Receiver	Displays the IP address of the destination call.
MAC_ADDRESS	Displays the name of the device.
Message Tag	Displays the sequence number to match the actual messages in the SDI Trace file.
MSG_TYPE	Displays the type of message.
Correlation ID	Displays the Correlation ID.
Timestamp	Displays the server time at which the call operation (call setup/split/join/release) happens.

Detailed SIP Message: Appears only when the Include SIP Message check box is checked. Displays the actual SIP message that is logged into the SDL log file.

Message in Log File: Displays the log file which contains the message.

To view the SIP messages that get logged into the SDL log file, perform the following actions:

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

- Set the trace level to any one of the following: State Transition, Significant, Arbitrary or Detailed.

Note If you are monitoring the session trace data from the logs stored on your local disk, the detailed SIP message will be available only if the SDL/SDI logs are present in the parent directory of the call logs.

Step 5 Click **Save**.

If you are monitoring real-time data, the Call Flow Diagram is saved as index.html in the specified folder along with the SDL files which contain the SIP messages. You can email the files to the Technical Assistance Center (TAC). For more information on monitoring real-time data, see “Monitor real-time data.” The SIP messages in the saved Call Flow Diagram appear as hyperlinks. When you click a SIP message, the detailed SIP message along with the following details is displayed in a new window.

Field	Description
Sender	Displays the IP address of the originating call.
GUID	Displays the SIP call ID.
Message Label	Displays the message type for the corresponding SIP message onto which you move your mouse; for example, 200 OK, or 180 Ringing.
Receiver	Displays the IP address of the destination call.
MAC_ADDRESS	Displays the name of the device.
Message Tag	Displays the sequence number to match the actual messages in the SDI Trace file.
MSG_TYPE	Displays the type of message.
Correlation ID	Displays the Correlation ID.
Timestamp	Displays the server time at which the call operation (call setup/split/join/release) happens.

If you open logs for Unified Communications Manager 8.5(1) or 8.6(1) using Open from Local Disk option and save the ladder diagram , the SIP messages, the SDI log files that contain the SIP messages and SDL Log files for a duration of from 5 minutes before the start of the call to 5 minutes after the start of the call will be saved. If you save logs from Unified Communications Manager 9.0(1) or later, the SDL log files that contain the call details are saved along with index.html and the SIP messages. For more information about monitoring the session trace data from the logs saved to your local disk, see “Monitor session trace data from local disk.”

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

You can perform the following actions:

a) To view the online help, click **Help**.
b) To exit the Analyze Call Diagram screen, click **Close**.

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

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

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

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

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

Detailed SIP messages are logged into SDI traces.

The Call Logs include the following message types:

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

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

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

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

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

- Search does not show incomplete calls.

  Example:

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

- The Call Flow Diagram does not show some SIP messages in the following scenarios:

  - Conference calls involving more than three parties.

  - A call leg is used to invoke a feature alone.

  Example:

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

  a. User A calls Phone B.

  b. User C lifts up the Phone C handset.

  c. User C presses the PickUp softkey to pickup the call.

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

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

Services Monitoring

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

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

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

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

For information about daily reports for CTI and Cisco TFTP usage statistics, see the *Cisco Unified Serviceability Administration Guide*.

The following table provides information about the service objects that RTMT monitors, the alert, thresholds, and defaults.

Table 6: Services Category

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

Service Logs

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

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

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

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

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

The first line of each log comprises the header.

Device Logs

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

The data is logged every five minutes for the following counters based on the following calculation:

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

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

The following filename format of the Device Log applies: `DeviceLog_MM_DD_YYYY_hh_mm.csv`.

The first line of each log file comprises the header.

Device Monitoring

Device Monitoring

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

For information about daily reports on registered devices, see the *Cisco Unified Serviceability Administration Guide*.

The following table provides information about the device objects that Unified RTMT monitors, the alert, thresholds, and defaults, and what kind of reports that Unified RTMT generates for those devices.

Table 7: Devices Category

Monitored Objects (Displayed)	Alert/Threshold/Default
Number of registered phones for each server or for all servers in a cluster (if applicable).	Total number of registered phones drops by X% in consecutive polls. Default specifies 10%.
Number of registered gateways on each server or for all servers in a cluster (if applicable).	For Unified Communications Manager: • (Warning) Clusterwide total number of registered gateways decreased in consecutive polls. • (Informational) Clusterwide total number of registered gateways increased in consecutive polls.
Number of registered media devices on each server or for all servers in a cluster (if applicable).	For Unified Communications Manager: • (Warning) Clusterwide total number of registered media devices decreased in consecutive polls. • (Informational) Clusterwide total number of registered media devices increased in consecutive polls. • Media List exhausted.

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

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

Note Currently, only 200 devices are displayed in the Device Search page for a single node in the cluster.

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

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

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

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

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

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

Find Specific Devices to Monitor

Follow this procedure to monitor data for the following device types:

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

Procedure

Step 1 Perform one of the following tasks:

a) On the Quick Launch Channel, perform the following steps:

   1. Click **Voice/Video**.
   2. In the tree hierarchy, double-click **Device**.
   3. Click the **Device Search** icon.

b) Choose **Voice/Video** > **Device** > **Device Search** > **Open Device Search** and select the device type; for example, Phone, Gateway, Hunt List, and so on. A device selection window displays where you enter the search criteria.

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

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

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

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

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

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

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

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

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

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

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

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

Step 9 Click **Next**.

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

Note If you enter the IPv6 address, the IP Subnet does not apply.

Step 11 Click **Next**.

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

Step 13 Click **Finish**.

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

View Phone Information

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

Procedure

Step 1 Find and display the phone in the RTMT device monitoring pane.

Step 2 Perform one of the following tasks:

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

The **Device Information** window appears.

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

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

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

Step 6 Click the **Any Model or Device Model** radio button.

If you click the **Device Model** radio button, choose a phone model that you want to display.

Step 7 Click **Next**.

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

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

Step 10 Click **Finish**.

The **Device Information** window appears. For more information about the device, choose any field that appears in the left pane of the window.

Generate PRT Information for Endpoints

Devices or endpoints generate alarms for each critical event for diagnostics and troubleshooting. Use the Generate PRT option to remotely trigger the log collection on the phone and upload it to the log server configured in the “Customer support upload URL” parameter.

Procedure

Step 1 Find and display the phone in the RTMT device monitoring pane.

Step 2 Right-click the phone for which you want information to display and choose **Generate PRT**.

The generated report is uploaded at the **Customer support upload URL**.

Note Check the **Customer support upload URL** parameter in either the Enterprise, Profile, or Device level configuration settings page. Else, PRT generation fails.

View Device Properties

You can view the properties of devices that appear in the RTMT device monitoring pane. Follow this procedure to view device properties.

Procedure

Step 1 Find and display the device in the RTMT device monitoring pane.

Step 2 Perform one of the following tasks:

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

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

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

Set Up Polling Rate for Devices and Perfmon Counters

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

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

Note The default value for devices is 10minutes.

Follow this procedure to update the polling rate:

Procedure

Step 1 Display the device or performance monitoring counter in the RTMT monitoring pane.

Step 2 Click the device and choose **Edit** > **Polling Rate**.

Step 3 In the Polling Interval pane, specify the time that you want to use.

Step 4 Click **OK**.

CTI Application, Device, and Line Monitoring

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

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

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

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

View CTI Manager Information

Follow this procedure to display a chart of open devices, lines, and CTI connections for each server or for each server in a cluster (if applicable).

Procedure

Step 1 Click **Voice/Video** in the quick launch channel.

Step 2 Double-click **CTI**.

Step 3 Click the **CTI Manager** icon.

Find CTI Applications to Monitor

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

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel, perform the following steps:
  a. Click **Voice/Video**.
  b. In the tree hierarchy, double-click **CTI**.
  c. Click the CTI Search icon.
- Choose **Voice/Video** > **CTI** > **CTI Search** > **CTI Applications**. The selection window appears where you can enter the search criteria.

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

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

Step 4 Click **Next**.

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

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

Note If you enter the IPv6 address, the IP Subnet does not apply.

Step 7 Click **Next**.

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

Step 9 Click **Finish**.

The applications monitoring pane displays the information that you choose.

Find CTI Devices To Monitor

Follow this procedure to find specific CTI devices to monitor.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel, perform the following steps:

  a. Click **Voice/Video**.

  b. In the tree hierarchy, double-click **CTI**.

  c. Click the CTI Search icon.

- Choose **Voice/Video** > **CTI** > **CTI Search** > **CTI Devices**. The selection window appears where you can enter the search criteria.

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

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

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

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

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

Step 5 Click **Next**.

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

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

Note If you enter the IPv6 address, the IP Subnet does not apply.

Step 8 Click **Next**.

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

Step 10 Click **Finish**.

The devices monitoring pane displays the information that you chose.

Find CTI Lines To Monitor

Follow this procedure to find specific CTI lines to monitor.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel, perform the following steps:
  - **a.** Click **Voice/Video**.
  - **b.** In the tree hierarchy, double-click **CTI**.
  - **c.** Click the CTI Search icon.
- Choose **Voice/Video** > **CTI** > **CTI Search** > **CTI Lines**. The selection window appears where you can enter the search criteria.

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

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

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

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

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

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

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

Step 6 Click **Next**.

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

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

Note If you enter the IPv6 address, the IP Subnet does not apply.

Step 9 Click **Next**.

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

Step 11 Click **Finish**.

The lines monitoring pane displays the information that you choose.

View Application Information

You can view the application information for selected devices such as the Cisco Unified IP Phone, CTI port, and CTI route point. Follow this procedure to view application information.

Procedure

Step 1 Find and display the devices in the RTMT monitoring pane.

Step 2 Perform one of the following tasks:

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

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

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

Access Learned Pattern and SAF Forwarder Reports for Call Control Discovery

Learned Pattern reports and Service Advertisement Framework (SAF) forwarder reports support the Call Control Discovery feature. When you configure the call control discovery feature, Unified Communications Manager advertises itself and its hosted DN patterns to other remote call-control entities that use the SAF network. Likewise, these remote call-control entities advertise their hosted DN patterns, which Unified Communications Manager can learn and insert in digit analysis. For more information about the call control discovery feature, see “Call Control Discovery” in the *Feature Configuration Guide for Cisco Unified Communications Manager* .

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

Learned Pattern reports include such information as learned pattern name, time stamp, and reachability status for the pattern. See the following table.

Table 8: Data From Learned Pattern Report

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

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

SAF Forwarder reports display information such as authentication status and registration status of SAF forwarders. See the following table.

Table 9: Data From SAF Forwarder Report

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

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

RTMT allows you to search based on different criteria; for example, if you specify a search for the remote call-control entity, all the learned patterns display for the remote call-control entity.

To access the Learned Patterns or SAF Forwarder reports in RTMT, perform the following procedure.

Procedure

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

a) For Learned Patterns: From the RTMT menus, choose **Voice/Video** > **Report** > **Learned Pattern**. Or, Click the **Voice/Video** tab; then, click **Learned Pattern**.
b) For SAF Forwarders: From the RTMT menus, choose **Voice/Video** > **Report** > **SAF Forwarders**. Or, click the **Voice/Video** tab; then, click **SAF Forwarders**.

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

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

Step 3 Review the data in the report.

See the Data from Learned Pattern Report table and the Data from SAF Forwarder Report table for descriptions of the items that were reported.

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

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

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

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

Access Called Party Trace Report

Called Party Trace 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.

The Called Party Trace feature provides information on the calling party number in addition to the called party number within a node. You can use the information from each node to trace a call back to the originator.

Note You must be an authorized administrator to access the directory number logs. To grant authorization to a specific role using MLA, the “Called Party Tracing” resource must have read permission enabled for the role.

To access the Called Party Trace report in the Real-Time Monitoring Tool, follow these steps:

Procedure

Step 1 From the RTMT menu, choose **Voice/Video** > **Callprocess** > **Called Party Trace**. Or, Click the **Voice/Video** tab; then, click **Called Party Trace**.

Step 2 Select the start time of the report using the drop-down box.

Note The start time cannot be older than five years from the current date.

Step 3 The report shows the following information:

- Start time
- Calling directory number
- Original called directory number
- Called directory number
- Calling device name
- Called device name

Note When 5 megabytes of trace file entries have been written to the log files being accessed by RTMT, the oldest log information is overwritten by new trace entries as they are recorded. The RTMT lists a maximum of 500 entries for any given search.

Intercompany Media Services

IME Service Monitoring

The IME Service category monitors the following items:

- Network Activity: Displays the activity on the Unified Communications Manager that relates to Cisco Intercompany Media Engine. The Network Activity object displays these charts:
    - IME Distributed Cache Health: Displays the health of the IME distributed cache based on the IMEDistributedCacheHealth counter for the IME Server performance object.
    - IME Distributed Node Count: Displays an approximation of the number of nodes in the IME distributed cache, based on the value of the IMEDistributedCacheNodeCount counter for the IME Server performance object. Because each physical Cisco Intercompany Media Engine server contains multiple nodes, the number that displays in the chart does not indicate the number of physical Cisco Intercompany Media Engine servers that participate in the IME distributed cache.
    - Internet BW Received: Displays the amount of bandwidth in Kbits/s that the Cisco IME service uses for incoming Internet traffic and represents the InternetBandwidthRecv counter for the IME Server performance object.
    - Internet BW Send: Displays the amount in Kbits/s that the Cisco IME service uses for outgoing Internet traffic and represents the InternetBandwidthSend counter for the IME Server performance object.
    - IME Distributed Cache Stored Data Records: Displays the number of IME Distributed Cache records that the Cisco Intercompany Media Engine server stores and represents the IMEDistributedCacheStoredData counter for the IME Server performance object.

      To display information about network activity, choose **Cisco IME Service** > **Network Activity**.

- Server Activity: Allows you to monitor the activity on the Cisco Intercompany Media Engine server. The Server Activity object displays these charts:
    - Number of Registered Clients: Displays the current number of clients that connect to the Cisco IME service and represents the value of the ClientsRegistered counter for the IME Server performance object.
    - IME Distributed Cache Quota: Indicates the number of individual DIDs that can be written into the IME Distributed Cache, by Unified Communications Manager servers attached to this IME server. This number is determined by the overall configuration of the IME Distributed Cache, and the IME license installed on the IME server.
    - IME Distributed Cache Quota Used: Indicates the total number of unique DID numbers that have been configured, to be published through enrolled patterns for Intercompany Media Services, by Unified Communications Manager sservers currently attached to this IME server.
    - Terminating VCRs: Indicates the total number of IME voice call records that are stored on the Cisco IME server for the terminating side of a call. These records can be used for validation of learned routes.

- Validations Pending: Displays the number of pending validations on the Cisco IME service as well as the threshold for validations. This chart represents the ValidationsPending counter for the Cisco IME Server performance object.

  To display information about server activity, choose **Cisco IME Service** > **Server Activity**.

IME System Performance Monitoring

The IME System Performance monitoring category provides the SDL Queue object that monitors the number of signals in the SDL queue and the number of signals that were processed for a particular signal distribution layer (SDL) queue type. The SDL queue types comprise high, normal, low, and lowest queue. You can monitor the SDL queue for a particular server or for an entire cluster (if applicable).

To display information about the SDL Queue, choose **Cisco IME Service** > **SDL Queue**. Select the type from the **SDL Queue Type** drop-down list box.

Monitor Intercompany Media Services

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

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

The Intercompany Media Services monitoring category monitors the following items:

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

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

    To display information about routing, choose **Voice/Video** > **Cisco IME Client** > **Routing**.

- Call Activities: Allows you to monitor the total number of Cisco Intercompany Media Engine calls. This total includes the following types of calls:
  - Calls that were attempted (including calls that were accepted, busy, no answer, and failed)
  - Calls that were received
  - Calls that were set up (that is, made by Unified Communications Manager and accepted by the remote party)
  - Calls that were accepted (that is, received by Unified Communications Manager and answered by the called party)
  - Calls that completed fallback to the PSTN
  - Calls that did not successfully fall back to the PSTN.

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

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

IM and Presence Monitoring

IM and Presence and Cisco Jabber summary monitoring

The Real-Time Monitoring Tool provides a set of important performance counters that assist you in monitoring the overall performance of the IM and Presence service and Cisco Jabber. The IM and Presence and Cisco Jabber summaries in RTMT allow you to monitor important common information in a single monitoring pane.

To display information on important performance counters that reflect the overall performance of IM and Presence and Cisco Jabber, select **IM and Presence** > **IM and Presence Summary** or **IM and Presence** > **Cisco Jabber Summary**.

Under IM and Presence Summary, review the following information:

- PE Active JSM Sessions
- XCP JSM IM Sessions
- Total IMs Handled
- Current XMPP Clients Connected
- Total Ad hoc Chat Rooms
- Total Persistant Chat Rooms

Under Cisco Jabber Summary, review the following information:

- Client Soap interface
- SIP Client Registered Users
- SIP Client Registered User Failures

- SIP Client IM Messages

Cisco XCP counters

Number of connected XMPP clients

Cisco XCP CM—CmConnectedSockets

View the current number of XMPP clients connected to the Cisco XCP Connection Manager on an individual IM and Presence server. This number should rise and fall based on the usage patterns of your deployment. Further investigation may be required if this number is higher than expected for your user base.

Number of connected CAXL clients

Cisco XCP Web CM—WebConnectedSockets

View the current number of CAXL web clients connected to the Cisco XCP Web Connection Manager on an individual IM and Presence server. This number should rise and fall based on the usage patterns of your deployment. Further investigation may be required if this number is higher than expected for your user base.

Number of active outbound SIP subscriptions

Cisco XCP SIP S2S—SIPS2SSubscriptionsOut

View the current number of active outgoing SIP Subscriptions being maintained by the Cisco XCP SIP Federation Connection Manager service on the IM and Presence server. Monitor this counter if IM and Presence server is configured for SIP Interdomain Federation or SIP Intradomain Federation.

Note The total combined count of SIPS2SSubscriptionsOut and SIPS2SSubscriptionsIn must not rise above 260,000 on any single IM and Presence server.

Number of active inbound SIP subscriptions

Cisco XCP SIP S2S—SIPS2SSubscriptionsIn

View the current number of active inbound SIP Subscriptions being maintained by the Cisco XCP SIP Federation Connection Manager service on the IM and Presence server. Monitor this counter if IM and Presence server is configured for SIP Interdomain Federation or SIP Intradomain Federation.

Note The total combined count of SIPS2SSubscriptionsOut and SIPS2SSubscriptionsIn must not rise above 260,000 on any single IM and Presence server.

Number of IM sessions

Cisco XCP JSM—JsmIMSessions

This counter gives the total number of IM sessions on the IM and Presence node across all users. The Presence Engine (PE), which provides presence composition services and rich, always-on, network presence, creates an IM session on behalf of all users at PE start-up time. This is necessary so that network presence events such as Unified Communications Manager Telephony Presence and Exchange Calendar notifications are reflected in a user's presence even if that user is not logged in to any IM clients.

Every licensed user on a IM and Presence node has one IM Session for Presence Engine rich presence composition in addition to one IM Session for any logged in clients.

Example

There are 100 licensed users on the IM and Presence node as follows:

- 50 users are not logged in
- 40 users are logged in on one IM client
- 10 users are logged in on two IM clients

This gives a total of 160 IM Sessions comprised of:

- 100 x 1 for rich Presence Engine sessions
- 40 x 1 for users logged in on a single client
- 10 x 2 for users logged in on two clients

Total IM Packets

Cisco XCP JSM—JsmTotalMessagePackets

This counter gives the total number of IM packets handled by the IM and Presence node across all users.

Note that if user Alice sends an IM to user Bob, and both users are assigned to the same IM and Presence node, then this IM packet will be counted twice. This is because the XCP Router and Jabber Session Manager treat the two users separately. For example, Alice's privacy rules will be applied to the IM packet before it is delivered to Bob, and then Bob's privacy rules will be applied to the IM packet before it is delivered to Bob's client. Whenever IM and Presence handles an IM packet it is counted once for the originator and once for the terminator.

If Alice and Bob are assigned to different IM and Presence nodes and Alice sends an IM packet to Bob, then the IM will be counted once on Alice's node and once on Bob's node.

IMs in last 60 seconds

Cisco XCP JSM—JsmMsgsInLastSlice

This counter gives the total number of IM packets handled by the IM and Presence node across all users in the past 60 seconds. This counter is reset to 0 every 60 seconds. The same rules for counting IM packets apply as for JsmTotalMessagePackets. Monitoring of this counter will help identify the busy IM hours in your organization.

Per user and per session counters

Cisco XCP JSM Session Counters

These per session counters only exist for the duration of an IM session or user login. One set of these counters exists for each Presence Engine network presence session, and one set of these counters exists for each client login session. In the example given above for the IMSessions counters, there are 160 different sets of Cisco XCP JSM Session Counters. When a user logs out, or when the Presence Engine is stopped, the associated Cisco XCP JSM Session Counters instance is deleted.

You can use the Cisco XCP JSM Session counters to get a snapshot of all users currently logged in. These counters can be accessed from the CLI using the following command:

```
admin: show perf list instances "Cisco XCP JSM Session Counters"
```

Every user assigned to an IM and Presence node that is logged into the system will have a set of JSM session counters for their current logged in client session and also their Presence Engine network session. On an IM and Presence node with 5000 users logged in this would result in a minimum of 10,000 sets of JSM Session counters. Updating these counters with new values as they change would place the system under stress. To combat this, JSM Session counter values are cached locally by the system and only updated to RTMT every 30 minutes.

IM packets sent per session

Cisco XCP JSM Session Counters—JsmSessionMessagesIn

This counts the total number of IM packets sent by the user from his IM client or session. Note that the terminology JsmSessionMessagesIn is used as from the perspective of the IM and Presence server, the IM packet sent by the client is an inbound IM packet to IM and Presence.

IM packets received per session

Cisco XCP JSM Session Counters—JsmSessionMessagesOut

This counts the total number of IM packets sent to the user on his IM client or session. Note that the terminology SessionMessagesOut is used as from the perspective of the IM and Presence server, the IM packet is sent to the client and is an outbound IM packet from IM and Presence.

Note JsmTotalMessagePackets, JsmMsgsInLastSlice, JsmSessionMessagesIn and JsmSessionMessagesOut each represent instant message packets being sent to IM and Presence and are not exact figures of Instant Messages on the system. The amount of IM packets sent to IM and Presence per IM can vary depending on the client in use.

Total text conferencing rooms

Cisco XCP TC—TcTotalRooms

This counter represents the total number of Text Conferencing rooms hosted on the node. This includes both ad hoc rooms and persistent chat rooms.

Total adhoc group chat rooms

Cisco XCP TC—TcAdHocRooms

This counter represents the total number of AdHoc chat rooms currently hosted on the node. Note that AdHoc chat rooms are automatically terminated when all users leave the room, so this counter should rise and fall in value regularly.

Total persistant chat rooms

Cisco XCP TC—TcPersistentRooms

This counter represents the total number of persistent chat rooms hosted on the node. Persistent chat rooms must be explicitly terminated by the room owner. You can monitor this counter to identify if the total number of persistent chat rooms is very large and also to help identify if some persistent chat rooms are not being used regularly anymore.

Per-chat room counters

Cisco XCP TC Room Counters

These pre-chat room counters exist only for the lifetime of a chat room. For ad hoc chat rooms, these counter instances are deleted when the Ad Hoc chat room is terminated. For persistent chat rooms, the counter instances are also deleted when the persistent chat room is terminated, however persistent chat rooms are long-lived, so they should rarely be terminated.

You can use these per-chat room counters to monitor the usage and participants in persistent (and ad hoc) chat rooms over their lifetime and can help identify persistent chat rooms that are no longer being used frequently.

You can use the Cisco XCP TC Room Counters to get a snapshot of all rooms that are currently hosted on the node. These counters can be accessed from the CLI using the following command:

```
admin:show perf list instances "Cisco XCP TC Room Counters"
```

IM packets received per room

Cisco XCP TC Room Counters—TCRoomMsgPacketsRecv

This counter represents the number of IM packets received per room.

Number of occupants per room

Cisco XCP TC Room Counters—TCRoomNumOccupants

This counter gives the current number of occupants of the chat room. Monitor this counter for Persistent Chat rooms to get an indication of the usage trend for the chat room.

It is possible to have a maximum of 16,500 Text Conferencing rooms on an IM and Presence node. Each of these rooms will have its own set of Per-Chat Room counters. Similar to JSM Session counters, updating these with new values as they change would place the system under stress. To combat this, Per-Chat Room counter values are cached locally by the system and only updated to RTMT every 30 minutes.

SIP proxy counters

Number of idle SIP proxy worker processes

SIP Proxy—NumIdleSipdWorkers

View the current number of idle, or free, SIP worker processes on the IM and Presence SIP Proxy. This counter gives a good indication of the load being applied to the SIP Proxy on each IM and Presence server. Monitor this counter if IM and Presence server is configured for SIP Interdomain Federation or SIP Intradomain Federation.

The number of idle processes can drop to zero on occasion and is not a cause for concern. However, if the number of idle processes are consistently below 5 processes, then it is an indication that the IM and Presence Server is being heavily loaded and requires further investigation

Cisco Unity Connection Monitoring

Port Monitor

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

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

Table 10: Fields and Descriptions in the Port Monitor

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

Field	Description
Port Ext	The extension of the port.
Connected To	For Unified Communications Manager SCCP integrations, the IP address and port of the Unified Communications Manager server to which the ports are registered.

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

Start Cisco Unity Connection Port Monitor Polling

Perform the following steps to use the Port Monitor.

Note Setting a low polling rate may impact system performance.

Procedure

Step 1 In the Real Time Monitoring Tool, access Unity Connection and click **Port Monitor**. The **Port Monitor** window appears.

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

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

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

CHAPTER 4

Cisco Unified Analysis Manager

Cisco Unified Analysis Manager Preferences

Use the Unified Analysis Manager dropdown menu to set preferences for:

FTP Server Setup

This function allows you to configure a FTP Server which you can then use to export information to. These servers can be Cisco TAC FTP servers. This information can include things such as logs, trace files, and system call trace information.

By default, the Cisco TAC FTP server will be pre-populated. You can modify this configuration for the default FTP server.

The FTP Server option allows you to manage the configured servers. You can perform the following operations:

- Add a new FTP server
- Edit an existing FTP server
- Delete FTP servers
- Test the connection of an FTP server

Cisco TAC has two FTP servers you can configure for exporting files:

- ftp-rtp.cisco.com
- ftp-sj.cisco.com

Note On both servers, files should be uploaded to the **/incoming** directory.

Access FTP Server Options

The following procedure explains how to access the FTP Server Options:

Procedure

Step 1 From the Unified Analysis Manager drop-down menu, select **AnalysisManager** > **Preferences**.

The **Preferences** window displays. Click **FTP Server**.

Step 2 The **FTP Servers** screen displays with a list of configured servers and buttons to **Add**, **Edit**, or **Delete** a server. The **Test Connection** button allows you to test connectivity to a server.

Step 3 Use the buttons to select the option you want.

Add or Edit FTP Server

Follow this procedure to add an FTP Server or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager drop-down menu, select **AnalysisManager** > **Preferences**. The Preferences window appears. Click **FTP Server**.

Step 2 The **FTP Servers** screen displays with a list of configured servers and buttons to **Add**, **Edit**, or **Delete** a server. The **Test Connection** button allows you to test connectivity to a server.

Step 3 Click the **Add** button to add a server or the **Edit** button to edit an existing configuration. The **Add FTP Server** screen appears.

Step 4 In the **Name/IP Address** field, enter the name or the IP address of the FTP server you are adding.

Step 5 In the **Protocol** field, select either the FTP or SFTP protocol, depending on the type of server you are connecting to. Use SFTP if you are connecting to a Cisco TAC server.

Step 6 In the **User Name** and **Password** fields, enter the username and password that gives you access to the server.

Step 7 In the **Port** field, enter the port number on the server that you will be using.

Step 8 In the **Destination Directory** field, enter the path for the directory to which you will be exporting files. If you are adding a Cisco TAC server, use the `/incoming` directory.

Step 9 Click the **OK** button to add the server. You can use the **Cancel** button to end the operation without adding the FTP server.

Set Up Mail Server

This option allows you to configure a mail server for the purpose of notifying a set of user configured recipients on the status of Unified Analysis Manager operations such as trace and log collections and file transfers.

You must configure at least one mail server in order to be able to send a notification.

Note

- You can configure a maximum of two mail servers.
- You can only use mail servers configured with this option for Unified Analysis Manager notifications. For RTMT notifications, you must configure a separate mail server.

Add or Edit Mail Server

The following procedure explains how to add a Mail Server or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager drop-down menu, select **AnalysisManager** > **Preferences**.

The **Preferences** window displays. Click **Mail Server**.

Step 2 The **Mail Servers** screen appears with a list of configured servers and buttons to **Add**, **Edit**, or **Delete** a server. The **Test Connectivity** button allows you to test connectivity to a server. The **Refresh** button allows you to reload the server.

Step 3 Click the **Add** button to add a server or the **Edit** button to edit an existing configuration. On clicking the **Add** button, the **Add Mail Server** screen appears.

Step 4 In the **Name/IP Address** field, enter the name or the IP address of the Mail server you are adding.

Step 5 In the **Port No.** field, enter the port number on the server that you will be using.

Step 6 Click **Save** button to save the settings or the **Cancel** button to end the operation without adding the Mail server. The **Test Connection** button allows you to test connectivity to a server.

Set Trace Collection Directory

Follow this procedure to use the Trace Collection option under Preferences to set a directory for trace logs:

Procedure

Step 1 From the Unified Analysis Manager drop-down menu, select **AnalysisManager** > **Preferences**.

The **Preferences** window appears. Click **Trace Collection**.

Step 2 The **Trace Collection** screen appears. Enter the directory you want to use for traces logs in the **Download Directory** box, or use the **Browse** button to locate the directory. Optionally, you can click the **Default** button to select the default dirctory.

Step 3 Click **Save**.

Cisco Unified Analysis Manager Limitations

Please consider the following limitations when you use the Unified Analysis Manager.

- The maximum number of call records that the CallSearch Report can display is 500.
- The maximum number of call records that the Call Track Report can display is 100.
- Since there is no globally unique callID to use, Unified Analysis Manager uses link-by-link approach to trace the call. If any record for a call is missing in one of the products in the call path, the link will be broken for the rest of the chain and the tracking will not be complete.
- Call records are not stored in the database orderly based on any particular column. When running Call Search Report, the number of returned records is limited to 500. The 500 records that are retrieved may not be the earliest (based on originating time, connection time, or disconnect time) in the specified time range. To make sure all of the call records within the specified time range are retrieved, you need to shorten the time range until the returned number of records is less than 500.
- The Unified Analysis Manager option is not displayed when the Unified RTMT is connected to a Cisco Unity Connection or IM and Presence node, because these products do not have a Call Record database.

  When you use the Unified RTMT to connect to a Unified Communications Manager node, you can add nodes to include Cisco Unity Connection and IM and Presence nodes in the Unified Analysis Manager.
- Call Tracking does not support tracking of SIP Unified Outbound Option calls from Unified CCE and Unified IME to Cisco IOS gateways.
- Call Tracking does not support direct call tracking of call paths using a GED-125 protocol from Unified CCE to Unified CVP.
- Unified Communications Manager needs to be in the call path for tracking calls from Unified Communications Manager.
- Call tracking only supports single branch tracking from Unified Communications Manager.
- No Call Detail Records (CDR) are generated for calls on the MGCP gateway, because the gateway does not implement call control and Q.931 is tunneled to the Unified Communications Manager for signaling. The CDR is available only on the Unified Communications Manager.
- With ACS servers, Unified Analysis Manager is used only for call tracing, and then used only if you want to include gateway records and information in the tracing data. If you do not have an ACS server or a supported hardware/software version of the ACS server, most of Unified Analysis Manager functions in your deployment will continue to work; however, your gateway information will not be included in your call traces.

Cisco Unified Analysis Manager Setup

The **Administration** option on the Unified Analysis Manager menu allows you to import device and group configurations from a .csv file to the Unified Analysis Manager tool.

Import Device and Group Settings

Follow this procedure to import device and group configuration from a .csv file into the Unified Analysis Manager.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Administration** > **Import**.

Step 2 Select the .csv configuration file that you want to import.

Step 3 Click the **Import** button.

The selected file appears.

Scheduled Trace and Log Collection Job Status Display

This function allows you to display status of scheduled trace setting and log collection jobs. Jobs can be scheduled using the Unified Analysis Manager Tools. Once a device is added to a group, you can schedule trace setting and log collections jobs on the device.

A scheduled job is linked to the machine it is configured on, and the job cannot be run on a different machine. If the machine on which a job was scheduled is not usable for any reason, the old job can be cloned and saved as a new job with new parameters to be run on the new machine.

Jobs running on a device can have one of the following states:

- Scheduled: A job is scheduled within Unified Analysis Manager; however it has not started
- Running: A job that is currently either setting traces or collecting logs
- Completed: A job that is done
- Pending: A job that has completed one run of collecting logs and is waiting to start the next run.
- Aborted: A job that has stopped abnormally due to an unexpected error
- Canceled: A job that has stopped due to a cancel operation by the user.

The Job Status screen gives a system view of all the jobs in Unified Analysis Manager. For jobs that have multiple runs, the status and time of the last run is also shown in this page.

The following operations can be performed on a job:

- View Details: Use this option to get more detailed view of the job.
- Cancel: Use this option to cancel a job. The Cancel operation can only be done on the machine that the job is running or scheduled on. This option cannot be used for jobs that are in the Completed/Aborted/Canceled state.
- Clone: Use this option to select any job and save it as a new job. The job being cloned from can be in any state. This option allows you to change any attribute of the job before saving. Cloning a job does not impact the attributes of the job being cloned.

Upload and Transfer Files to FTP Server

This option allows you to transfer files to a configured FTP server and send an email to interested parties. You can use this option to transfer some files to another machine so they can be viewed by others.

This screen allows you to specify the files and folders to be transferred as well as any annotations to accompany those files.

Follow this procedure to transfer files to an FTP server:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Administration** > **Upload Files**.

The Upload Files screen appears.

Step 2 In the **Case ID** field, enter the number that Cisco TAC has assigned to the case.

Step 3 Use the drop-down list box in the **Send to Server** field to select the FTP server you are sending the file to.

Step 4 Use the **Notes** box to provide any additional information about the file.

Step 5 Use the **Send Email Notifications** check box if you want to add the email addresses to send a notification that the file is uploaded. To add multiple email addresses, add the mail ids separated by comma. The mail addresses can be only the `<username>` or it can be of the format `username@domain.com`.

Step 6 In the bottom section of the screen, in the **Files to upload** box, select the files you want to transfer. Use the **Add** or **Remove** buttons to select or deselect files from the system. The files selected will be zipped by default and then uploaded. The name of the zipped file will be of the format `<case id>_uploadedfile.zip`.

Step 7 Click the **OK** button to transfer the file.

Cisco Unified Analysis Manager Tools

This chapter provides information about the Unified Analysis Manager, which provides a set of tools that allows you to perform management tasks for specific devices and groups of devices.

Analyze Call Path Tool

The Analyze Call Path tool allows you to trace a call between multiple Cisco Unified Communications products. In order to trace a call using the Analyze Call Path tool, a node must be defined in Unified Analysis Manager and the node must belong to a group.

Note All nodes that you define are assigned to the AllNodes group by default. Use the Node Groups function if you want to assign the node to a different group. See the topics related to the Analyze Call Path setup for more information on configuring a Call Record Repository before using the Analyze Call Path function.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools** > **Analyze Call Path**.

The **Analyze Call Path** Information window appears.

Step 2 Click the **Continue** button. The **Search Criteria** window appears.

Step 3 Enter the number where the call originated in the **Calling Number** field. The default is an asterisk (*) which is a wildcard that will trace all numbers for the node.

Step 4 Enter the number where the call terminated in the **Called Number** field. The default is an asterisk (*) which is a wildcard that will trace all numbers for the node.

Step 5 Use the **Termination Cause** drop-down list box to select the reason for the call termination; either Abandoned, Dropped, Failed or all three.

Step 6 Use the **Start Time** field to enter the start time for the trace.

Step 7 Use the **Duration** field to indicate the length of the time period you want to trace.

Step 8 Use the **Time Zone** drop-down list box to select the time zone where you are tracing calls.

Step 9 Use the **Filter Nodes by Group** drop-down list box to select the group of nodes that you want to trace.

Step 10 Use the **and Node Type** drop-down list box to select specific types of nodes that you want to trace.

When you have selected the Group and Node, information displays for each node. You can then use the check box for each node listed to select or deselect the node.

Note The limit for the number of nodes that you can select at a time is 20.

Step 11 Click the **Run** button to begin the trace. The trace results display on the bottom of the window. If you selected multiple nodes, a tab is displayed for each node. Click the tab to display information for that node.

Step 12 When the call record information appears, you can click the **View Full Path** button to see the complete call path. You can click the **View Record Details** button to see the information about the call. Use the **Save Results** button to save the reports.

Analyze Call Path Setup Considerations

⚠

Caution The Analyze Call Path Tool might not work correctly if your computer is set to a language other than English.

When using the Analyze Call Path tool, there are configuration considerations for each product that the Unified Analysis Manager manages.

The Analyze Call Path tool does not include information for Cisco Unity Connection and IM and Presence servers.

Cisco Unified Communications Manager

The following information applies when configuring the Analyze Call Path for Unified Communications Manager:

- Version Support—Unified Analysis Manager supports Release 8.0(1) and above for Unified Communications Manager.

- Call Record Repository—Use the first node (publisher) as the Call Record Repository with the HTTPS protocol and the default port 8443.
- User Group and Access Permissions— Users should belong to a user group whose role contains read and update permissions required to access Call Records for the following resources:
  - SOAP Call Record APIs
  - SOAP Control Center APIs
  - SOAP Diagnostic Portal Database Service
  - SOAP Log Collection API
  - SOAP Performance Informations APIs
  - SOAP Realtime Informations and Control Center APIs

Note New resources “SOAP Diagnostic Portal Database Service” and “SOAP Call Record APIs” added on an upgrade should not have the read and update permissions by default due to security reasons for existing users. Users need to create or copy the role to custom resources and update the required permissions for above mentioned resources as needed. See the *Administration Guide for Cisco Unified Communications Manager* for additional details.

- Configuring NTP—Each product installed in the solution should be configured to point to same set of external NTP clock sources. NTP is required to be configured on all nodes that involve calls for SCT features. For Unified Communications Manager, use the **utils ntp config** CLI command to configure NTP.
- Enable Call Record Logging—In Cisco Unified Communications Manager Administration, go to the Service Parameter Configuration window, and choose the **Cisco CallManager Service**. Enable the **CDR Enabled Flag** and the **CDR Log Calls with Zero Duration Flag** parameters. Restart the **Cisco CallManager** service for change-notification to take effect immediately. Repeat this procedure for all nodes in the Unified Communications Manager cluster.

Note You can verify that flags are set as desired at `https://<HOSTNAME:PORT>/ccmadmin/vendorConfigHelp.do`

- CDR CAR Loader—Ensure your CDR Analysis and Reporting (CAR) Loader is set to **Continuous Loading 24/7**. To verify this:
  - Go to the Cisco Unified Serviceability and select **Tools** > **CDR Analysis and Reporting (CAR)** page. The CAR page opens in a new browser.
  - Go to **System** > **Scheduler** > **CDR Load page**.
  - Verify if Loader is not disabled and that **Continuous Loading 24/7** is enabled. This allows CDR records that are generated from Unified Communications Manager nodes to be loaded into the CAR database as soon as they arrive to Unified Communications Manager first node (publisher).

If call records are not found on the Unified Communications Manager, it is possible that the CAR Loader failed or is having a delay loading the latest CDR records. If this occurs, go to the CAR **System** > **Database** > **Manual Purge** page and click the **Table Information** button. Check for the oldest and latest CDR records that are available in the CAR database. If records are not set to the latest date, go to **System** > **Log Screens** > **Event Log** and select **CDR Load** to check its recent run status to see if there were any Unsuccessful runs. If CDR Load failure is found, collect CAR Scheduler traces to provide to Cisco Support for troubleshooting.

- Raw Call Record Details—For information about Raw Call Record details help for Unified Communications Manager, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide*.

Cisco Unified Contact Center Express

The following information applies when configuring the Analyze Call Path for Unified CCX:

- Version Support—Unified Analysis Manager supports Unified CCX version 8.0(1) and later.
- Call Record Repository—The Call Record Repository used for Unified CCX is either (or both in the case of a High Availability system) of the Unified CCX nodes. The database is active on both nodes and the data is replicated. The JDBC user is **uccxsct** and the password is the encrypted version of the TFTP password. The password is typically set by the Unified CCX administrator.
- Default user for adding Unified CCX Call Record Repository—The Informix user for adding (and connecting to) Unified CCX Call Record Repository is: **uccxsct**. You can reset the default install time password for above user in the Unified CCX Application **Administration** > **Tools** > **Password Management** page. Typically, the Unified CCX administrator will reset to the desired password and pass it on to the Unified Analysis Manager administrator.
- User Group and Access Permissions—Unified CCX does not require any additional user group and access permission to access Call Records. The access permissions of the uccxsct user is set by Unified CCX install for read access to specific tables. No external settings are required.
- Configuring NTP—To configure NTP for Unified CCX, go to **OS Administration** > **Settings** > **NTP Server**.
- Enable Call Record Logging—Unified CCX always generates Call Records by default, so no configuration is required to enable logging of Call Records.

Cisco Unified Intelligent Contact Management Enterprise/Cisco Unified Contact Center Enterprise

The following information applies when configuring the Analyze Call Path for Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) and Unified CCE:

- Version Support—Unified Analysis Manager supports Release 8.0(1) and above for Unified ICME and Unified CCE.
- Call Record Repository—The Call Record Repository used for Unified ICME is either AW-HDS-DDS or HDS-DDS. The server used for Unified CCE is HDS/AW Database (port 1433).
- User Group and Access Permissions—For Release 8.0(1), the recommended user group and access permissions that are required to access Call records are the Windows only Authentication for SQL Server. This is done by using the **User List** tool from the Configuration Manager and creating a user with the right access privileges.

- Configuring NTP—Configuration for Time Synchronization of Unified CCE servers is based on Microsoft Windows Time Services. When setting up the Unified CCE router component, retain the default settings of the “Disable ICM Time Synchronization” box as checked. With the recommended default setting, the time synchronization for Unified CCE servers is provided by the Windows Time Service, which automatically synchronizes the computer's internal clock across the network. The time source for this synchronization varies, depending on whether the computer is in an Active Directory domain or a workgroup. For additional information on setting up Windows Time Service, refer to the Microsoft Windows Time Service Technical Reference documentation at: `http://technet.microsoft.com/en-us/library/cc773061(WS.10).aspx`.
- Enable Call Record Logging—To check that Call Record logging is enabled, first be sure that the Unified Analysis Manager service on Unified CCE is enabled. Using the web setup, you need to install the AW-HDS-DDS or HDS-DDS servers with Administration and Data Server roles. Once you install these roles using the web setup, the call records are available by default.
- Raw Call Record Details—To find help for the Raw Call Record details, refer to the Schema Help which you can access from the Unified CCE Administration Tool group on either the AW-HDS-DDS or HDS-DDS server. You can also refer to the United CCE Database Schema Handbook for a specific release at `http://www.cisco.com/en/US/products/sw/custcosw/ps1844/tsd_products_support_series_home.html`.

Note If you are using RTMT to monitor Cisco Unified Contact Center Enterprise, you must open the following file and change the value for ReadTimeout to 360: *<RTMT_INSTALLATION_FOLDER_PATH>/conf/rtmt.xml*. If you don't change the value, RTMT will not be able to collect OPC logs because RTMT's default timeout value is greater than the time it takes to collect OPC logs.

Cisco Unified Customer Voice Portal

The following information applies when configuring the Analyze Call Path for Unified CVP:

- Version Support—United Analysis Manager supports Unified CVP Release 8.0(1) and above.
- Call Record Repository—Unified CVP uses the Unified CVP Reporting Server for the Call Record Repository.
- User Group and Access Permissions—Unified CVP uses Unified CVP OAMP to set user group and access permissions required to access Call Records:
    - All users trying to access Unified CVP records from the Unified CVP database need to be created through Unified CVP OAMP.
    - Unified CVP Reporting users need to be granted the Unified CVP Reporting role in Unified CVP OAMP.
    - User passwords may expire if security hardening is installed on the Unified CVP Reporting Server. SNMP monitor displays alerts when this happens.
- Configuring NTP—Configuration for Time Synchronization of the Unified CVP servers is based on Microsoft Windows Time Services. For additional information on setting up Windows Time Service, refer to the Microsoft Windows Time Service Technical Reference documentation at `http://technet.microsoft.com/en-us/library/cc773061(WS.10).aspx`.

- Enable Call Record Logging—To ensure that Call Record logging is enabled, do the following:
    - Unified CVP Reporting Server is not installed nor configured by default. Customers and Partners will have to install a Unified CVP Reporting Server to use the Analyze Call Path tool with Unified CVP.
    - Unified CVP Database schema needs to be laid down by the Unified CVP_database_config.bat file. This file needs to be run by the user after Unified CVP Reporting Server installation is completed.
    - Once a Unified CVP Reporting Server is installed, it needs to be configured through Unified CVP OAMP and a Unified CVP Call Server needs to be associated with the Unified CVP Reporting Server.
    - Follow the Unified CVP CAG and RPT guidelines for configuring the Unified CVP Reporting Server, Unified CVP VXML Server, and Unified CVP Call Servers.
    - Unified CVP data retention is 30 days, by default. You can customize this value through Unified CVP OAMP. Unless you back up the database, data will be purged at the end of data retention day. Backed up Unified CVP data is not accessible unless it is imported back into the database.
    - Unified CVP VXML Server filters need to be configured on Unified CVP OAMP. Refer to the Unified CVP OAMP guide for configuring these filters.
- Raw Call Record Details—For information relating to Raw Call Record details, refer to the *Unified CVP Reporting Guide for version7.0(2)*.

Cisco Access Control Server and Cisco IOS Gateway

The following information applies when configuring the Analyze Call Path for Cisco Access Control (ACS) Servers and Cisco IOS Gateways:

- Version Support—Unified Analysis Manager supports ACS Release 5.1.
- Call Record Repository—To assign a Call Record Repository, one of the acs servers can be configured as a "collector" node.
- User Group and Access Permissions—To set user group and access permissions, after the ACS server is installed, in ssh/telnet access, enter **`acsadmin`** as the username and **`default`** as the password, You will be prompted to change the password.
- Configuring NTP—To configure an NTP server on an ACS server, use cli: **ntp server** *<NTP server IP/host>*.
- Enable Web View—Execute the CLI command acs **config-web-interface view enable** to enable web view. It is disabled by default.
- Cisco IOS gateways as ACS network devices or AAA clients—You need to configure ACS network device to have the correct Radius secret, which is the same secret as the one on the IOS gateway.
    - From acsadmin, access **Network Devices Group** > **Network Devices** and AAA clients to add the Cisco IOS gateway as the ACS network device or AAA client.
- For IOS configurations:
    - Use the CLI to configure NTP server: **ntp server** *<NTP server IP/host>*
    - Configure Cisco IOS gateway as a Radius client of the ACS server. Sample CLIs are below:

```
aaa new-model!
!
aaa group server radius acs
server 172.27.25.110 auth-port 1812 acct-port 1813
!
aaa authentication login h323 group acs
aaa authorization exec h323 group acs
aaa accounting connection h323 start-stop group acs
aaa session-id common
gw-accounting aaa
radius-server host 172.27.25.110 auth-port 1812 acct-port 1813
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

- Be sure you have local login access to your Cisco IOS gateways.
- Enable Call Record Logging—To check that Call Records logging is enabled:
    - aaa accounting connection h323 start-stop group acs
    - aaa session-id common
    - gw-accounting aaa
    - radius-server host 172.27.25.110 auth-port 1812 acct-port 1813
    - radius-server key cisco
    - radius-server vsa send accounting

Nodes

Node Management

Once configured, a supported node is added to the Unified Analysis Manager database and will appear on the supported Unified Analysis Manager node list. You can identify a Unified Analysis Manager node in one of three ways:

- Importing node and group configuration from a configuration file.
- Manually entering node and group information with the Unified Analysis Manager screens.
- Discovering Unified Analysis Manager nodes from a seed node. A seed node is one that can return information about all the nodes within a deployment. Once discovered, the nodes can then be added to the node inventory. This option saves you from manually entering details of these nodes.

For Unified Communications Manager, the first node (publisher) is the seed node. For Cisco Unified Customer Voice Portal (Unified CVP), the Cisco Unified CVP OAMP server is the seed node.

This option allows you to perform Add/Edit/Delete and Discover operations on nodes. All configured Unified Analysis Manager nodes (manually entered, imported from a file, or discovered) will be displayed in the list of nodes.

You can use the Nodes option to perform the following functions:

- Add—The Add button allows you to manually enter a new node.

- Edit—The Edit button allows you to edit a node that has already been configured.
- Delete—The Delete button allows you to delete one or more nodes.
- Discover—You can use the Discover option, which applies only to a seed node. Use the Discover button to send a query to the seed node, which then returns information about all the nodes within that deployment that the seed node is aware of. Once discovered, the nodes are automatically added to the node inventory.
- Test Connectivity—The Test Connectivity button allows you to test connectivity to the node using the configured access information.

Display Node Summary

The Node summary screen displays all of the nodes currently configured with the Unified Analysis Manager application. Use the following procedure to access the Node summary screen.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory** > **Nodes**.

Step 2 The **Node** summary screen displays with a list of configured nodes and buttons to **Add**, **Edit**, **Delete**, **Discover**. The **Test Connection** button allows you to test connectivity to a node. Nodes are listed by **Name** and **Product Type**.

Add or Edit a Node

The following procedure explains how to add a node or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory** > **Nodes**.

The **Nodes** window appears.

Step 2 Click the **Add** button to add a node or select a node from the list and click the **Edit** button to edit an existing configuration. The **Add** or **Edit Node** screen appears.

Note Fields on this screen that are marked with an asterisk (*) are required fields.

Step 3 Use the **Product Type** drop-down list box to select a product.

Step 4 In the **IP/Host Name** field, enter the hostname or the IP address of the node you are adding or editing.

Step 5 In the **Transport Protocol** field, select the protocol you want to use. Options for this field depend on the **Product Type** you selected.

Step 6 In the **Port Number** field, enter the port number on the node that you will be using.

Step 7 In the **User Name** and **Password** fields, enter the username and password that gives you access to the node. Reenter the password in the **Confirm Password** field.

Step 8 In the **Description** field, you can optionally provide a brief description of the node you are adding.

Step 9 In the **Associated Call Record Repositories** and **Associated Trace File Repositories** fields, use the drop down list to select the respective servers you want to use for the node.

Step 10 Use the **Associated Group** check boxes if you want to add the node to an existing group.

Step 11 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Node-Advanced** screen. Enter the appropriate information in the **Alternate IP/Hostname** and **Alternate Port** fields.

Step 12 Click the **Save** button to add the node. You can use the **Cancel** button to end the operation without adding the node.

Group Management

Within Unified Analysis Manager, you can create groups and add nodes to these groups. Once the nodes are added to a group, the user can perform a set of functions (for example, Trace Collection and Trace Setting) at a group level. A single node can belong to multiple groups. Nested groups will not be supported. Copying a group will not be supported.

Note The **AllNodes** group is added by default when a node is added in Unified Analysis Manager. Any nodes added to Unified Analysis Manager are part of the AllNodes group by default. The AllNodes group cannot be edited or deleted.

Note The number of groups you can have is limited to 20 and the number of nodes in a group (with the exception of the AllNodes group) is 20.

You can use the Group option to perform the following functions:

- Add—Use the Add button to create a group. Once a Group is created, you can add nodes to the group.
- Edit—Use the Edit button to select and edit group information. The Edit function also allows you add or delete the node members of the group. You can change which nodes belong to a group by adding or deleting nodes from that group.
- Delete—Use the Delete button to delete a Group. This function deletes that group from the Unified Analysis Manager. However, this function does not delete the individual nodes in the group from the Unified Analysis Manager. Nodes must be deleted individually using the Edit button.

Add or Edit Group

The following procedure explains how to add a group or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory** > **Node Groups**.

Step 2 The **Groups** window displays. Click the **Add** button to add a group or select a group from the list and click the **Edit** button to edit an existing configuration. The **Add** or **Edit Group** screen displays.

Step 3 Use the **Group Name** field to enter the name of the group.

Step 4 Use the **Group Description** field to enter a brief description of the group.

Step 5 The **Select Nodes** section contains a list of each configured node. To add a node to the group, highlight the node in the list and click the **Add** button.

Step 6 When you have finished selecting nodes for the group, click the **Add** button to add the group or the **Update** button if you are editing the group content. You can use the **Cancel** button to end the operation without adding or editing the group.

Trace File Repository Management

This option allows you to perform Add/Edit/Delete operations on trace file repositories for the Unified Analysis Manager. Managed nodes typically use the trace file repository to off load its trace and log files. The Unified Analysis Manager can then connect to the trace file repository to collect logs and traces.

You can use the Trace File Repository option to perform the following functions:

- Add—The Add button allows you to manually enter a new server.
- Edit —The Edit button allows you to edit a server that has already been configured.
- Delete—The Delete button allows you to delete one or more servers.
- Test Connectivity—The Test Connectivity button allows you to test connectivity to a server using the configured access information.

Add or Edit Trace File Repository

The following procedure explains how to add a Trace File Repository or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory** > **Trace File Repositories**.

Step 2 The **Trace File Repositories** window displays with a list of configured servers. Click the **Add** button to add a new server or highlight a server on the list and click the **Edit** button to edit an existing configuration.

Step 3 In the **IP/Host Name** field, enter the hostname or the IP address of the server you are adding.

Step 4 In the **Transport Protocol** field, use the drop-down list to select the protocol you want to use, either SFTP or FTP.

Step 5 In the **Port Number** field, enter the port number on the server that you will be using.

Step 6 In the **User Name** and **Password** fields, enter the username and password that gives you access to the server. Reenter the password in the **Confirm Password** field.

Step 7 In the **Description** field, you can optionally provide a brief description of the server you are adding.

Step 8 In the **Associated Nodes** field, use the check boxes to select the nodes that will have access to the server.

Step 9 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Trace File Repository-Advanced** screen. Enter the appropriate information in the **Alternate IP/Hostname** and **Alternate Port** fields.

Step 10 Click the **Add** button to add the server or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

Call Record Repository Management

This option allows you to perform Add/Edit/Delete operations on call record repositories for the Unified Analysis Manager. Managed nodes typically see the Call Record Repository to store the call data in a database. The Unified Analysis Manager can then connect to the Call Record Repository to obtain detailed call data.

You can use the Call Record Repository option to perform the following functions:

- Add: Allows you to manually enter a new server.
- Edit: Allows you to edit a server that has already been configured.
- Delete: Allows you to delete one or more servers.
- Test Connectivity: Allows you to test connectivity to a server using the configured access information.

Add or Edit Call Record Repository

Follow this procedure to add a call record repository or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory** > **Call Record Repositories**.

Step 2 The **Call Record Repositories** window appears with a list of configured servers. Click the **Add** button to add a new server or highlight a server on the list and click the **Edit** button to edit an existing configuration.

Step 3 Use the **Repository Type** drop down list to select the product type for the node that will be accessing the server.

Step 4 In the **Hostname** field, enter the name of the server you are adding.

Step 5 In the **JDBC Port** field, enter the port number on the server that you will be using.

Step 6 In the **JDBC User Name** and **JDBC Password** fields, enter the username and password that gives you access to the server. Re-enter the password in the **Confirm Password** field.

Step 7 In the **Description** field, you can optionally provide a brief description of the node you are adding.

Step 8 Use the **Nodes Available for Association** to select the nodes that will have access to the server.

Step 9 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Call Record Repository-Advanced** screen. Enter the appropriate information in the **Alternate Hostname** and **Alternate Port** fields.

Step 10 Click the **Add** button to add the server or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

Define Trace Templates

If you have large number of nodes in a group, the Unified Analysis Manager provides templates as a shortcut for selecting components to change trace levels. You can also use templates to establish the new trace levels for nodes. You can also use template for collecting logs and trace files.

You can use the Templates option to perform the following functions:

- Add—The Add button allows you to create a new template. When adding a template you should note that you are doing so for node types and not actual nodes. For a given node type, there is a known fixed set of components and services.

- Edit—The Edit button allows you to edit an existing template.
- Clone—The Clone button allows you to save an existing template as a new template without replacing the original one.
- Delete—The Delete button allows you to delete a template.
- Import—Use the Import button to import predefined templates from a flat file.
- Export—Use the Export button to export a template to a flat file.

Add or Edit Template

The following procedure explains how to add a template or edit an existing configuration:

Note Unified Analysis Manager has default templates which cannot be edited or deleted.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory** > **Templates**.

Step 2 The **Templates** window displays. Click the **Add** button to add a template or select a template from the list and click the **Edit** button to edit an existing configuration. The **Add** or **Edit Template** screen displays.

Step 3 Use the **Name** field to enter the name of the template.

Step 4 Use the **Description** field to enter a brief description of the group.

Step 5 The **Product Types** section contains a list of products supported by the Unified Analysis Manager. When you select a product from this list, the associated components display in the **Component Name** field.

Step 6 For each component displayed, you can apply a trace level by using the drop down list in the **Trace Level** field.

Note Not all components are available for setting trace levels with this screen.

Step 7 You can indicate if you want to collect trace logs for the component by checking the box in the **Collect** field.

Step 8 Click the **Add** button to add the template or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

Call Definitions

The following table defines the types of call termination.

Table 11: Call Definitions

Call Type	Call Termination Explanation
Failed call	The call is not connected for any reason other than user hang-up before the connection is completed.

Call Type	Call Termination Explanation
Abandoned call	The call is not connected because the user hangs up after initiating the call.
Dropped call	The call is disconnected after connection for any reason other than user hanging up.

The following table lists the products that support the failed, abandoned, and dropped calls.

Table 12: Product Support for Call Types

Call Type	Unified Communications Manager	Unified CCE	Unified CVP	Unified CCX
Failed Call	Supported	Supported	Supported	Supported
Abandoned call	Supported	Supported	Not Supported	Supported
Dropped Called	Supported	Supported	Not Supported	Supported

Trace Collection

Unified Analysis Manager allows you to collect log and trace files from services of supported devices. There are three ways you can collect logs and trace files:

- Collect Traces Now— Collect Traces Now option allows you to collect trace files based on a selection of services on a device or group of devices for any period of time that has occurred in the past.
- Schedule Trace Collection— Schedule Trace Collection option allows you to collect trace files based on a selection of services on a device or group of devices for any period of time in the future.
- Schedule Trace Settings and Collections—Schedule Trace Settings and Collection option allows you to collect trace files from the present into the future and also specify the trace levels to be used during the scheduled time.

Collect Traces Now

The Collect Traces Now option allows you to collect trace files based on a selection of services on a device or group of devices for any period of time that has occurred in the past.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools** > **Collect Traces Now**.

The **Collect Traces Now** window displays.

Step 2 Select either the Group to display a list of supported groups or the Node for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template** to dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to customize new trace levels for the group or device.

Step 4 Use the **Start Time** and **End Time** fields to select the collection time period.

Step 5 Use the **Referenced Time Zone** field to select the time zone for the collection time period.

Step 6 You can optionally click the **View Summary** button to view the Collection Summary window. This window contain a list of the components associated with the node.

Step 7 Click the **OK** button to start the trace. When the trace is completed, the window displays a Status Summary and Status Details for the trace. The Status Details provide the path to the directory to which the log was sent.

Schedule Trace Collection

Use the Schedule Trace Collection option if you want to collect trace files for any period of time from the present into the future.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools** > **Schedule Trace Collection**.

The **Schedule Trace Collection** window appears.

Step 2 Select either the Group to display a list of supported groups or the Node for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to collect traces for specific components.

Step 4 Use the **Start Time** and **End Time** fields to select the collection time period.

Step 5 Use the **Referenced Time Zone** field to select the time zone for the collection time period.

Step 6 Use the **Collect Traces Every** dropdown field to indicate the frequency of the collection.

Step 7 Optionally, you can choose to have an email notification sent regarding the trace collection. To do that, click the **Send Email Notification to** check box and enter the email address in the text box.

Step 8 You can optionally click the **View Summary** button to view the **Collection Summary** window. This window contains a list of the components associated with the node.

Step 9 Click the **OK** button to start the trace. When the trace is scheduled, the window displays a Status Summary and Status Details for the trace. When the trace is completed, a report is written to your log file and, if email information was provided, a system-generated email is sent.

Schedule Trace Settings and Collection

Use the Schedule Trace Settings and Collection option if you want to collect trace files for any period of time from the present into the future and, in addition, also specify the trace levels to be used during the scheduled time. If you change trace settings with this option, trace levels are restored to their default settings after the collection period is over.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools** > **Schedule Trace Collection**.

The **Schedule Trace Collection** window appears.

Step 2 Select either the Group to display a list of supported groups or Node, for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** drop-down list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to customize new trace levels for the group or device. This option also allows you to collect traces for specific components.

Step 4 Use the **Start Time** and **End Time** fields to select the collection time period.

Step 5 Use the **Referenced Time Zone** field to select the time zone for the collection time period.

Step 6 Use the **Collect Traces Every** drop-down field to indicate the frequency of the collection.

Step 7 Optionally, you can choose to have an email notification sent regarding the trace collection. To do that, click the **Send Email Notification to** check box and enter the email address in the text box.

Step 8 You can optionally click the **View Summary** button to view the **Collection Summary** window. This window contains a list of the components associated with the node.

Step 9 Click the **OK** button to start the trace. When the trace is scheduled, the window displays a Status Summary and Status Details for the trace. When the trace is completed, a report is written to your log file and, if email information was provided, a system-generated email is sent.

Set Trace Levels

Use the Set Trace Level option to assign trace levels for a group of devices or individual devices. You can assign trace levels using a template or you can customize trace levels. Trace levels can be set for the following Cisco Unified Communications components:

- Unified Communications Manager: Allows setting trace levels for Unified Communications Manager and Common Trace Components.
- IM and Presence: Allows setting trace levels for Unified Presence and Common Trace Components.
- Cisco Unity Connection: Allows setting trace level for Cisco Unity Connection and Common Trace Components.
- Cisco Unified Contact Center Express: Allows setting trace level only for Common Trace Components.

The following table describes the general trace level settings for the Cisco Unified Communications components that are managed by Unified Analysis Manager.

Table 13: Unified Analysis Manager Trace Level Settings

Trace Level	Guidelines	Expected Volume of Traces
Default	This level should include all traces generated in abnormal paths. This level is intended for coding error traces and error s traces that normally should not occur. **Note** Choose **Detailed** as **Default** trace level.	Minimum Traces expected

Trace Level	Guidelines	Expected Volume of Traces
Warning	This level should include traces for system-level operations. This should include all traces generated by “State Transitions” within components.	Medium Volume of Traces Expected when component is used
Informational	This should include traces that can be used in the lab for debugging difficult problems of the component.	High Volume of Traces Expected when component is used
Debug	This level should include detailed debug information or high volume of messages which are primarily used for debugging.	Very High Volume of Traces Expected when component is used

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools** > **Set Trace Level**.

The **Set Trace Level** window appears.

Step 2 Select either the Group to display a list of supported groups or the Node for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 From the **Select the template** drop-down list box, select the template containing the trace levels that you you want to use. Alternately, you can click the **Customize** button if you want to customize trace levels for the group or device. If you choose the **Customize** option, the Design Preview dialog displays with a list of supported devices. Choose the device you want and use the **Selected Components** fields to set the trace levels.

Step 4 Click **View Changes** to see any changes made to traces levels for the node. Click **OK** to set the level and exit the screen.

View Configuration

Use the View Configuration option to view configuration information related to a node. You can collect the version and configuration information and view it in a browser or save the results.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools** > **View Configuration**.

The **View Configuration** window appears and displays a list of nodes.

Step 2 Select a node and click the **Next** button to display the **Selected Components** screen. This screen lists the Version, Platform, License and other category configuration information for the product.

Step 3 Click **Finish** to collect the configuration information.

The summary window appears. Users can view the collected information in a browser or save the collected configuration information using the **Save As** button.

Cisco Unified Analysis Manager Troubleshooting

The following table provides a list of errors that you may see when testing Unified Analysis Manager connectivity to a node and the suggested action for correcting the errors.

Table 14: Test Connectivity Errors and Corrective Actions

No.	Error Code	Message	Corrective Action
1	NOT_AUTHORIZED_CODE	Username or password is not correct	Enter the correct username and password.
2	MISSING_SERVICE_CODE	Missing Service	The requested web service was not found. Check to see if the web service is down on the target application.
3	SERVER_BUSY_CODE	Server is busy	Check to see if there are any other ongoing jobs running on the server. If so, wait until the job is done. If not, wait a few minutes and try again.
4	INVALID_PORT_CODE	Invalid Port	The specified port may be syntactically incorrect or may be out of range.
5	CONNECTION_FAILED_CODE	Not connected to the specified node	Verify that you have entered the correct address for this node. If the address is correct, then verify that the node is up and that it is reachable.
6	NOT_SUPPORTED_CODE	Not supported	This version of the specified product is not supported for this release. Upgrade this product to a supported version.
7	CERTIFICATE_HANDLING_ERROR_CODE	SSL handshake failed. The client and server could not negotiate desired level of security	Verify that you have accepted the certificate that was sent to the client from the server.

No.	Error Code	Message	Corrective Action
8	GENERAL_CONNECTION_ERROR_CODE	An internal error has occurred	Save the recent Unified Analysis Manager log files and contact Unified Analysis Manager support for help.

CHAPTER 5

Profiles and Categories

Profiles

This section describes about how to add, restore, and delete the configuration profile.

Add Configuration Profile

With RTMT, you can customize your monitoring window by monitoring different performance counters and then create your own configuration profiles. You can restore these monitoring windows in a single step rather than opening each window again.

You can switch between different profiles during the same RTMT session or use the configuration profile in subsequent RTMT sessions.

Follow this procedure to create a profile.

Procedure

Step 1 Choose **File** > **Profile**.

The Preferences dialog box appears.

Step 2 Click **Save**.

The Save Current Configuration dialog box appears.

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

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

Note Profiles apply to all nodes within a cluster, but you cannot save and apply the profile to a different cluster.

The system creates the new configuration profile.

Restore Configuration Profile

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

Procedure

Step 1 Choose **File** > **Profile**.

The Preferences dialog box appears.

Step 2 Click the profile that you want to restore.

Step 3 Click **Restore**.

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

Delete Configuration Profile

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

Procedure

Step 1 Choose **File** > **Profile**.

The Preferences dialog box appears.

Step 2 Click the profile that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Close**.

Categories

Add Category

Follow this procedure to add a category.

Procedure

Step 1 Go to the applicable window for your configuration:

Unified Communications Manager	Choose **System** > **Performance** > **Open Performance Monitoring**.

Unified Communications Manager IM and Presence Service	Choose **System** > **Performance** > **Open Performance Monitoring**.
Cisco Unity Connection	Choose **System** > **Performance** > **Open Performance Monitoring**.

Step 2 Choose **Edit** > **Add New Category**.

Step 3 Enter the name of the category; click **OK**.

The category tab appears at the bottom of the window.

Rename Category

To rename a category, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

a) Right-click the category tab that you want to rename and choose **Rename Category**.
b) Click the category tab that you want to rename and choose **Edit** > **Rename Category**.

Step 2 Enter the new name and click **OK**.

The renamed category displays at the bottom of the window.

Delete Category

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

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

CHAPTER 6

Performance Counters

Counters

Add Counter Using Performance Queries

You can use queries to select and display perfmon counters. You can organize the perfmon counters to display a set of feature-based counters and save it in a category. After you save your Unified RTMT profile, you can quickly access the counters in which you are interested.

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

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

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

Procedure

Step 1 Choose **System** > **Performance** > **Open Performance Monitoring**.

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

The tree hierarchy expands and displays all the perfmon objects.

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

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

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

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

Step 7 Click **OK**.

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

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

- Double-click a single counter and select a single instance from the dialog box, and then click **Add**.
- Double-click a single counter and select multiple instances from the dialog box, and then, click **Add**.

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

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

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

A list of counters appears.

b) To display the counter information, either right-click the counter and click **Counter Monitoring**, double-click the counter, or drag and drop the counter into the Perfmon Monitoring pane.

The counter chart appears in the Perfmon Monitoring pane.

Remove Counter From Performance Monitoring Pane

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

You can remove counters from the RTMT Perfmon Monitoring pane when you no longer need them. Follow this procedure to remove a counter from the pane.

Procedure

Perform one of the following tasks:

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

Add Counter Instance

Follow this procedure to add a counter instance.

Procedure

Step 1 Find and display the performance monitoring counter.

Step 2 Click the performance monitoring counter in the performance monitoring tree hierarchy and choose **System** > **Performance** > **Counter Instances**.

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

The counter appears.

Set Up Counter Alert Notification

Follow this procedure to configure alert notification for a counter.

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

Procedure

Step 1 Find and display the performance counter.

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

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

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

Step 5 In the Description pane, enter a description of the alert and click **Next**.

Step 6 Configure the settings in the Threshold, Value Calculated As, Duration, Frequency, and Schedule panes. After you enter the settings in the window, click **Next** to proceed to the next panes.

Step 7 To configure the system to send an e-mail message for the alert, check the **Enable Email** check box.

Step 8 To trigger an alert action that is already configured, choose the alert action that you want from the **Trigger Alert Action** drop-down list box.

Step 9 To configure a new alert action for the alert, click **Configure**.

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

The **Alert Action** dialog box appears.

Step 10 To add a new alert action, click **Add**.

The Action Configuration dialog box appears.

Step 11 In the Name field, enter a name for the alert action.

Step 12 In the Description field, enter a description for the alert action.

Step 13 Click **Add** to add a new e-mail recipient for the alert action.

The Input dialog box appears.

Step 14 Enter either the e-mail or e-page address of the recipient that you want to receive the alert action notification and click **OK**

Step 15 In the User-defined email text box, enter the text that you want to display in the e-mail message and click **Activate**.

Display Counter Description

The following shows how to obtain a description of the counter:

Procedure

Step 1 Perform one of the following tasks:

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

Tip You can display the counter description and configure data-sampling parameters.

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

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

Local Perfmon Counter Data Logging

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

Start Perfmon Counter Logging

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

Procedure

Step 1 Find and display the performance monitoring counters.

Step 2 If you are displaying perfmon counters in the chart format, right-click the graph for which you want data sample information and choose **Start Counter(s) Logging**.

The **Counter Logging Configuration** dialog box appears.

Step 3 If you want to log all counters in a screen (both chart and table view format), you can right-click the category name tab at the bottom of the window and choose **Start Counter(s) Logging**.

The **Counter Logging Configuration** dialog box appears.

Step 4 Configure the maximum file size and maximum number of files parameter.

Step 5 In the **Logger File Name** field, enter a filename and click **OK**.

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

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

Note If you have already started logging perfmon counters and you want to change the maximum file size and maximum number of files, you must first stop the counters before you reconfigure the maximum file size and number of files parameters. After resetting the parameters, you can then restart logging perfmon counters.

Stop Perfmon Counter Logging

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

Procedure

Step 1 Find and display the performance monitoring counters.

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

Configure Data Sample

The **Counter Property** window contains the option to configure data samples for a counter. The perfmon counters that display in the RTMT Perfmon Monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option.

Follow this procedure to configure the number of data samples to collect for a counter.

Procedure

Step 1 Find and display the counter.

Step 2 Click the counter for which you want data sample information and choose **System** > **Performance** > **Monitoring Properties**.

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

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

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

The default specifies 100.

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

The default specifies 20.

Step 6 Click one of the following parameters:

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

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

View Counter Data

Follow this procedure to view the data that is collected for a performance counter.

Procedure

Step 1 In the RTMT Perfmon Monitoring pane, right-click the counter chart for the counter for which you want to view data samples.

Step 2 Choose **View All Data**.

The counter chart displays all data that has been sampled. The green dots display close together.

Step 3 Right-click the counter that currently appears.

Step 4 Choose **View Current**.

The counter chart displays the last configured data samples that were collected.

Log files on Perfmon Log Viewer and Microsoft Performance Tool

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

The following table describes the functions of different buttons that are available on the Performance Log Viewer.

Table 15: Performance Log Viewer

Button	Function
Select Counters	Allows you to add counters that you want to display in the p counter, uncheck the Display column next to the counter.
Reset View	Resets the performance log viewer to the initial default view
Save Downloaded File	Allows you to save the log file to your local computer.

View Log Files on Perfmon Log Viewer

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

Before you begin

The local perfmon logs consist of data from counters that you select and store locally on your computer.

Procedure

Step 1 Select **System** > **Performance** > **Open Performance Log Viewer**.

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

- For RisDC Perfmon Logs, perform the following steps:

  a. Select RisDC Perfmon Logs in the Select Perfmon Log Location section.

  b. Select a node from the list box.

  c. Select **Open**.

  d. Select the file and select **Open File**.

  e. Check the counters that you want to display.

  f. Select **OK**.

- For locally stored data, perform the following actions:
  a. Select **Local Perfmon Logs**.
  b. Select **Open**.
  c. Browse to the file directory.
  d. Select the file that you are interested in viewing or enter the filename in the filename field.
  e. Select **Open**.
  f. Check the counters that you want to display.
  g. Select **OK**.

Step 3 Select the counters that you want to display.

Step 4 Select **OK**.

Troubleshooting Tips

- The Real-Time Monitoring Tool saves the perfmon CSV log files in the log folder in the.jrtmt directory under the user home directory. In Windows, the path specifies D:\Documents and Settings\userA\.jrtmt\log, or in Linux, the path specifies /users/home/.jrtmt/log
- The RISDC perfmon logging is also known as Troubleshooting Perfmon Data logging. When you enable RISDC perfmon logging, the server collects data that are used to troubleshoot problems. Because the IM and Presence service collects a large amount of data in a short period of time, you should limit the time that RISDC perfmon data logging (troubleshooting perfmon data logging) is enabled.
- You can order each column by selecting on a column heading. The first time that you select on a column heading, the records display in ascending order. A small triangle pointing up indicates ascending order. If you select the column heading again, the records display in descending order. A small triangle pointing down indicates descending order. If you select the column heading one more time, the records displays in the unsorted state.

Zoom In and Out in Performance Log Viewer

The Performance Log viewer includes a zoom feature that allows you to zoom in on and out on an area in the chart.

Procedure

Step 1 Perform one of the following actions:

a) On the Quick Launch Channel:

- Select **System**.
- In the tree hierarchy, double-select **Performance to display the performance icons**.
- Select the **Performance** icon.

b) Select **System** > **Performance** > **Open Performance Monitoring**.

Step 2 Select the name of the server where the counter is located.

The tree hierarchy expands and displays all the perfmon objects for the node.

Step 3 Double-select the performance counter you want to monitor.

Step 4 Perform one of the following actions:

If you want to:	Action
Zoom in on an area in the chart	• Select and drag the left mouse button over the area of • Release the left mouse button when you have the sele
Reset the chart to the initial default view	Perform one of the following actions: • Select **Reset View**. • Right-mouse select the chart and select **Reset**.

View Perfmon Log Files with Microsoft Performance Tool

Note The method for accessing **Performance** may vary depending on the version of windows you install on your computer.

Procedure

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

Step 2 Perform the following actions in the application window:

a) Select the right mouse button.
b) Select **Properties**.

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

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

Step 5 Select **Apply**.

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

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

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

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

Step 10 Select **Add** to add the selected counters.

Step 11 Select **Close when you finish selecting counters**.

Troubleshooting

Perfmon Data Log Troubleshooting

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

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

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

- Enable and disable the trace filter for Troubleshooting perfmon data logging.
- Monitor a set of predefined System and performance objects and counters on each server.
- Log the monitored performance data in CSV file format on the server in the active log partition in the var/log/active/cm/log/ris/csv directory. The log file uses the following naming convention: PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv; for example, PerfMon_172.19.240.80_06_15_2005_11_25.csv. Specify the polling rate. This rate specifies the rate at which performance data is gathered and logged. You can configure the polling rate down to 5 seconds. Default polling rate equals 15 seconds.
- View the log file in graphical format by using the Microsoft Windows performance tool or by using the Performance Log viewer in the Real-Time Monitoring Tool.
- Specify the maximum number of log files that will be stored on disk. Log files exceeding this limit are purged automatically by removal of the oldest log file. The default specifies 50 files.
- Specify the rollover criteria of the log file based on the maximum size of the file in megabytes. The default value specifies 2 MB.
- Collect the Cisco RIS Data Collector PerfMonLog log file by using the Trace & Log Central feature of the Real-Time Monitoring Tool or Command Line Interface.

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

Note Cisco Unity Connection counters are not logged to the troubleshooting perfmon data log.

- Database Change Notification Server Object:
  - Clients

  - CNProcessed
  - QueueDelay
  - QueuedRequestsInDB
  - QueuedRequestsInMemory

- Database Local DSN Object:
  - CcmDbSpace_Used
  - CcmtempDbSpace_Used
  - CNDbSpace_Used
  - LocalDSN
  - RootDbSpace_Used
  - SharedMemory_Free
  - SharedMemory_Used

- Enterprise Replication DBSpace Monitors Object:
  - ERDbSpace_Used
  - ERSBDbSpace_Used

- IP Object:
  - In Receives
  - In HdrErrors
  - In UnknownProtos
  - In Discards
  - In Delivers
  - Out Requests
  - Out Discards
  - Reasm Reqds
  - Reasm Oks
  - Reasm Fails
  - Frag OKs
  - Frag Fails
  - Frag Creates
  - InOut Requests

- Memory Object:

  - % Page Usage
  - % VM Used
  - % Mem Used
  - Buffers Kbytes
  - Cached Kbytes
  - Free Kbytes
  - Free Swap Kbytes
  - HighFree
  - HighTotal
  - Low Total
  - Low Free
  - Page Faults Per Sec
  - Page Major Faults Per Sec
  - Pages
  - Pages Input
  - Pages Input Per Sec
  - Pages Output
  - Pages Output Per Sec
  - SlabCache
  - SwapCached
  - Shared Kbytes
  - Total Kbytes
  - Total Swap Kbytes
  - Total VM Kbytes
  - Used Kbytes
  - Used Swap Kbytes
  - Used VM Kbytes

- Network Interface Object:
  - Rx Bytes
  - Rx Packets
  - Rx Errors
  - Rx Dropped

  - Rx Multicast
  - Tx Bytes
  - Tx Packets
  - Tx Errors
  - Tx Dropped
  - Total Bytes
  - Total Packets
  - Tx QueueLen

- Number of Replicates Created and State of Replication Object:
  - Replicate_State

- Partition Object:
  - % CPU Time
  - %Used
  - Await Read Time
  - Await Time
  - Await Write Time
  - Queue Length
  - Read Bytes Per Sec
  - Total Mbytes
  - Used Mbytes
  - Write Bytes Per Sec

- Process Object:
  - % Memory Usage
  - Data Stack Size
  - Nice
  - PID
  - STime
  - % CPU Time
  - Page Fault Count
  - Process Status
  - Shared Memory Size

  - VmData
  - VmRSS
  - VmSize
  - Thread Count
  - Total CPU Time Used

- Processor Object:
  - Irq Percentage
  - Softirq Percentage
  - IOwait Percentage
  - User Percentage
  - Nice Percentage
  - System Percentage
  - Idle Percentage
  - %CPU Time

- System Object:
  - Allocated FDs
  - Freed FDs
  - Being Used FDs
  - Max FDs
  - Total Processes
  - Total Threads
  - Total CPU Time

- TCP Object:
  - Active Opens
  - Passive Opens
  - Attempt Fails
  - Estab Resets
  - Curr Estab
  - In Segs
  - Out Segs
  - Retrans Segs

  - InOut Segs

- Thread Object (Troubleshooting Perfmon Data Logger only logs Unified Communications Manager threads):
  - %CPU Time

- Cisco CallManager Object:
  - CallManagerHeartBeat
  - CallsActive
  - CallsAttempted
  - CallsCompleted
  - InitializationState
  - RegisteredHardwarePhones
  - RegisteredMGCPGateway
  - RegisteredOtherStationDevices

- Cisco SIP Stack Object:
  - CCBsAllocated
  - SCBsAllocated
  - SIPHandlerSDLQueueSignalsPresent

- Cisco CallManager System Performance Object:
  - AverageExpectedDelay
  - CallsRejectedDueToThrottling
  - CodeRedEntryExit
  - CodeYellowEntryExit
  - QueueSignalsPresent 1-High
  - QueueSignalsPresent 2-Normal
  - QueueSignalsPresent 3-Low
  - QueueSignalsPresent 4-Lowest
  - QueueSignalsProcessed 1-High
  - QueueSignalsProcessed 2-Normal
  - QueueSignalsProcessed 3-Low
  - QueueSignalsProcessed 4-Lowest
  - QueueSignalsProcessed Total

  - SkinnyDevicesThrottled
  - ThrottlingSampleActivity
  - TotalCodeYellowEntry

- Cisco TFTP Server Object:
  - BuildAbortCount
  - BuildCount
  - BuildDeviceCount
  - BuildDialruleCount
  - BuildDuration
  - BuildSignCount
  - BuildSoftkeyCount
  - BuildUnitCount
  - ChangeNotifications
  - DeviceChangeNotifications
  - DialruleChangeNotifications
  - EncryptCount
  - GKFoundCount
  - GKNotFoundCount
  - HeartBeat
  - HttpConnectRequests
  - HttpRequests
  - HttpRequestsAborted
  - HttpRequestsNotFound
  - HttpRequestsOverflow
  - HttpRequestsProcessed
  - HttpServedFromDisk
  - LDFoundCount
  - LDNotFoundCount
  - MaxServingCount
  - Requests
  - RequestsAborted
  - RequestsInProgress

- RequestsNotFound
- RequestsOverflow
- RequestsProcessed
- SegmentsAcknowledged
- SegmentsFromDisk
- SegmentsSent
- SEPFoundCount
- SEPNotFoundCount
- SIPFoundCount
- SIPNotFoundCount
- SoftkeyChangeNotifications
- UnitChangeNotifications

Troubleshoot Perfmon Data Logging

Follow this procedure to collect information from counters within the perfmon objects with the perfmon data-logging feature.

Before you begin

- Be aware that RISDC perfmon logging is also known as Troubleshooting Perfmon Data logging. When you enable RISDC perfmon logging, the server collects performance data that are used to troubleshoot problems.
- When you enable RIS Data Collector (RISDC) perfmon logs, Unified Communications Manager and the IM and Presence Service collect information for the system in logs that are written on the server.
- You can enable or disable RISDC perfmon logs in the administrative interface by selecting **System** > **Service Parameter** and selecting the Cisco RIS Data Collector Service from the Service list box. By default, RISDC perfmon logging is enabled.

Procedure

Step 1 Select **System** > **Service Parameters** the administration interface.

Step 2 Select the server from the Server list box.

Step 3 Select the Cisco RIS Data Collector from the Service drop-down list box.

Step 4 Enter the appropriate settings as described in the following table.

Table 16: Troubleshooting Perfmon Data-Logging Parameters

Field	Description
Enable Logging	From the drop-down list box, select **True** to enable or **Fals** The default value specifies False.

Field	Description
Polling Rate	Enter the polling rate interval (in seconds). You can enter a val default value specifies 15.
Maximum No. of Files	Enter the maximum number of Troubleshooting Perfmon Data You can enter a value from 1 (minimum) up to 100 (maximum Consider your storage capacity in configuring the Maximum N We recommend that you do not exceed a value of 100 MB whe value by the Maximum File Size value. When the number of files exceeds the maximum number of fil deletes log files with the oldest time stamp. **Caution** If you do not save the log files on another comput losing the log files.
Maximum File Size (MB)	Enter the maximum file size (in megabytes) that you want to st started. You can enter a value from 1 (minimum) to 500 (maxi Consider your storage capacity in configuring the Maximum N We recommend that you do not exceed a value of 100 MB whe value by the Maximum File Size value.

Step 5 Select **Save**.

Note You can collect the log files for Cisco RIS Data Collector service on the server by using RTMT to download the log files. If you want to download the log files by using the CLI, refer to *Administration Guide for Cisco Unified Communications Manager* . After you collect the log files, you can view the log file by using the Performance Log Viewer in RTMT or by using the Microsoft Windows performance tool.

CHAPTER 7

Alerts

Alert Central Displays

Unified RTMT displays both preconfigured alerts and custom alerts in Alert Central. Unified RTMT organizes the alerts under the applicable tabs: System, Voice/Video, IM and Presence Service, Cisco Unity Connection, and Custom.

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

System Alerts

The following list comprises the preconfigured system alerts:

- AuthenticationFailed
- CiscoDRFFailure
- CoreDumpFileFound
- CpuPegging
- CriticalServiceDown
- DBChangeNotifyFailure
- DBReplicationFailure
- DBReplicationTableOutofSync
- HardwareFailure
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded

- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown (Applies to Unified Communications Manager clusters)
- SparePartitionHighWaterMarkExceeded
- SparePartitionLowWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatched
- TotalProcessesAndThreadsExceededThreshold

Related Topics

System Alerts, on page 300

Automatic Trace Download Activation

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

- CriticalServiceDown: CriticalServiceDown alert is generated when any service is down. CriticalServiceDown alert monitors only those services that are listed in RTMT Critical Services.

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

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

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

Caution Trace Download may affect services on the node. A high number of downloads adversely impacts the quality of services on the node.

Voice and Video Alerts

The following list comprises the preconfigured Voice and Video alerts:

- BeginThrottlingCallListBLFSubscriptions
- CallAttemptBlockedByPolicy
- CallProcessingNodeCpuPegging
- CARIDSEngineCritical
- CARIDSEngineFailure
- CARSchedulerJobFailed
- CDRAgentSendFileFailed
- CDRFileDeliveryFailed
- CDRHighWaterMarkExceeded
- CDRMaximumDiskSpaceExceeded
- CodeYellow
- DDRBlockPrevention
- DDRDown
- EMCCFailedInLocalCluster
- EMCCFailedInRemoteCluster
- ExcessiveVoiceQualityReports
- ILSHubClusterUnreachable
- ILSPwdAuthenticationFailed
- ILSTLSAuthenticationFailed
- IMEDistributedCacheInactive
- IMEOverQuota
- IMEQualityAlert
- IMEServiceStatus
- InsufficientFallbackIdentifiers
- InvalidCredentials
- LocationOutOfResource
- MaliciousCallTrace
- MediaListExhausted
- MgcpDChannelOutOfService
- NumberOfRegisteredDevicesExceeded

- NumberOfRegisteredGatewaysDecreased
- NumberOfRegisteredGatewaysIncreased
- NumberOfRegisteredMediaDevicesDecreased
- NumberOfRegisteredMediaDevicesIncreased
- NumberOfRegisteredPhonesDropped
- RecordingCallSetupFail
- RecordingGatewayRegistrationRejected
- RecordingGatewayRegistrationTimeout
- RecordingGatewaySessionFailed
- RecordingResourcesNotAvailable
- RecordingSessionTerminatedUnexpectedly
- RouteListExhausted
- RTMTSessionExceedsThreshold
- SDLLinkOutOfService
- TCPSetupToIMEFailed
- TLSConnectionToIMEFailed
- UserInputFailure
- ProductInEval
- ProductEvalExpired
- ProductOutOfCompliance
- ProductRegistrationExpiringSoon
- ProductAuthorizationExpiringSoon
- ProductRegistrationExpired
- ProductAuthorizationExpired
- ProductCommunicationError

Related Topics

Voice and Video Alerts, on page 320

IM and Presence Service Alerts

The following list comprises the preconfigured IM and Presence Service alerts:

- CTIGWModuleNotEnabled
- CTIGWProviderDown

- CTIGWUserNotLicenced
- CTIGWUserNotAuthorized
- CTIGWProviderFailedToOpen
- CTIGWQBEFailedRequest
- CTIGWSystemError
- EspConfigAgentMemAllocError
- EspConfigAgentFileWriteError
- EspConfigAgentNetworkOutage
- EspConfigAgentNetworkRestored
- EspConfigAgentHighMemoryUtilization
- EspConfigAgentHighCPUUtilization
- EspConfigAgentLocalDBAccessError
- EspConfigAgentProxyDomainNotConfigured
- EspConfigAgentRemoteDBAccessError
- EspConfigAgentSharedMemoryStaticRouteError
- ESPConfigError
- ESPConfigNotFound
- ESPCreateLockFailed
- ESPLoginError
- ESPMallocFailure
- ESPNAPTRInvalidRecord
- ESPPassedParamInvalid
- ESPRegistryError
- ESPRoutingError
- ESPSharedMemCreateFailed
- ESPSharedMemSetPermFailed
- ESPSharedMemAllocFailed
- ESPSocketError
- ESPStopped
- ESPStatsLogFileOpenFailed
- ESPVirtualProxyError
- ESPWrongIPAddress

- ESPWrongHostName
- ICSACertificateCASignedTrustCertFound
- ICSACertificateFingerPrintMisMatch
- ICSACertificateValidationFailure
- InterclusterSyncAgentPeerDuplicate
- LegacyCUPCLogin
- NotInCucmServerListError
- PEAutoRecoveryFailed
- PEDatabaseError
- PEIDSQueryError
- PEIDSSubscribeError
- PEIDStoIMDBDatabaseSyncError
- PELoadHighWaterMark
- PEMemoryHighCondition
- PEPeerNodeFailure
- PESipSocketBindFailure
- PEStateDisabled
- PEStateLocked
- PEWebDAVInitializationFailure
- PWSSCBFindFailed
- PWSSCBInitFailed
- PWSAboveCPULimit
- PWSAboveSipSubscriptionLimit
- PWSRequestLimitReached
- SRMFailed
- SRMFailover
- SyncAgentAXLConnectionFailed
- UASCBFindFailed
- UASCBGetFailed
- XcpCmComponentConnectError
- XcpCmPauseSockets
- XcpCmStartupError

- XcpCmXmppdError
- XcpConfigMgrConfigurationFailure
- XcpConfigMgrHostNameResolutionFailed
- XcpConfigMgrJabberRestartRequired
- XcpConfigMgrR2RPasswordEncryptionFailed
- XcpConfigMgrR2RRequestTimedOut
- XcpDBConnectError
- XcpMdnsStartError
- XcpSIPFedCmComponentConnectError
- XcpSIPFedCmStartupError
- XcpSIPGWStackResourceError
- XcpThirdPartyComplianceConnectError
- XcpTxtConfComponentConfigError
- XcpTxtConfDBConnectError
- XcpTxtConfDBQueueSizeLimitError
- XcpTxtConfGearError
- XcpWebCmComponentConnectError
- XcpWebCmHttpdError
- XcpWebCmStartupError
- XcpXMPPFedCmComponentConnectError
- XcpXMPPFedCmStartupError

Related Topics

IM and Presence Service Alerts, on page 367

Cisco Unity Connection Alerts

The following list comprises the preconfigured Cisco Unity Connection alerts.

- NoConnectionToPeer
- AutoFailoverSucceeded
- AutoFailoverFailed
- AutoFailbackSucceeded
- AutoFailbackFailed
- SbrFailed (Split Brain Resolution Failed)

- DiskConsumptionCloseToCapacityThreshold
- DiskConsumptionExceedsCapacityThreshold
- LicenseExpirationWarning
- LicenseExpired

Note The first six alerts apply only to Cisco Unity Connection cluster configurations.

Related Topics

Cisco Unity Connection Alerts, on page 399

Alerts Updates

The following list comprises the alerts that are deleted in Release 12.5(1)SU4:

- CiscoGraceTimeLeft
- CiscoElmNotConnected
- CiscoNoProvisionTimeout
- CiscoSystemInOverage
- CiscoSystemSecurityMismatch
- CiscoSystemInDemo
- CiscoSystemEncryptionNotAllowed
- ICSACertificateSyncConnectionRefusedStart

The following list comprises the alerts that are added in Release 12.5(1)SU4:

- SmartLicenseInEval
- SmartLicenseNoProvision_EvalExpired
- SmartLicenseInOverage_AuthorizationExpired
- SmartLicenseNoProvision_AuthorizationExpired
- SmartLicenseRegistrationExpired
- SmartLicenseInOverage_OutOfCompliance
- SmartLicenseNoProvision_OutOfCompliance
- SmartLicenseCommunicationError
- SmartLicenseRegistrationExpiringSoon
- SmartLicenseAuthorizationExpiringSoon
- SmartLicenseRenewAuthFailed

- SmartLicenseRenewRegistrationFailed
- SmartLicenseExportControlNotAllowed
- SmartLicense_SLR_InEval
- SmartLicense_SLR_NoProvision_EvalExpired
- SmartLicense_SLR_InOverage_NotAuthorized
- SmartLicense_SLR_NoProvision_NotAuthorized
- SmartLicense_SLR_ExportControlNotAllowed
- CiscoHAProxyServiceDown
- XcpTxtConfTCMessagesMsgIdError
- JSMSessionsExceedsThreshold

Alert Action Setup

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

The following table provides a list of fields that you will use to configure alert actions. Users can configure all fields, unless otherwise marked.

Table 17: Alert Action Configuration

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

Access Alert Central and Set Up Alerts

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

Procedure

Step 1 Perform one of the following tasks:

a) On the Quick Launch Channel, do the following:

1. Click **System**.
2. In the tree hierarchy, double-click **Tools**.
3. Click the Alert Central icon.

b) Choose **System** > **Tools** > **Alert** > **Alert Central**.

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

Step 2 Perform one of the following tasks:

a) Set alert properties.
b) Suspend alerts.
c) Configure e-mails for alert notification.
d) Configure alert actions.
e) Sort alert information in the Alert Status pane. Click the up/down arrow that displays in the column heading.

For example, click the up/down arrow that displays in the Enabled or In Safe Range column.

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

f) To enable, disable, or remove an alert, perform one of the following tasks:

- From the Alert Status window, right-click the alert and choose **Disable/Enable Alert** (option toggles) or **Remove Alert**, depending on what you want to accomplish.
- Highlight the alert in the Alert Status window and choose **System** > **Tools** > **Alert** > **Disable/Enable (or Remove) Alert**.

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

g) To clear either individual or collective alerts after they get resolved, perform one of the following tasks:

- After the **Alert Status** window displays, right-click the alert and choose **Clear Alert** (or **Clear All Alerts**).
- Highlight the alert in the Alert Status window and choose **System** > **Tools** > **Alert** > **Clear Alert** (or **Clear All Alerts**).

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

h) To reset alerts to default configuration, perform one of the following tasks:

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

i) To view alert details, perform one of the following tasks:

- After the **Alert Status** window displays, right-click the alert and choose **Alert Details**.
- Highlight the alert in the **Alert Status** window and choose **System** > **Tools** > **Alert** > **Alert Details**.

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

Set Alert Properties

Using the alert notification feature, the application notifies you of system problems. The following configuration setup is required to activate alert notifications for a system performance counter.

From the RTMT Perfmon Monitoring pane, you select the system perfmon counter and perform the following actions:

- Set up an e-mail or a message popup window for alert notification.
- Determine the threshold for the alert.
- Determine the frequency of the alert notification (for example, the alert occurs once or every hour).
- Determine the schedule for when the alert activates (for example, on a daily basis or at certain times of the day).

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

Procedure

Step 1 Perform one of the following actions:

If you want to:	Action
Set alert properties for a performance counter	• Display the performance counter. • From the counter chart or table, right-select the counter for which y **Alert/Properties**. • Check the **Enable Alert** check box.
Set alert properties from Alert Central	• Access Alert Central. • Select the alert for which you want to set alert properties. Perform one of the following actions: • Right-select the alert and select **Set Alert/Properties**. • Select **System** > **Tools** > **Alert** > **Set Alert/Properties**. • Check the **Enable Alert** check box.

Step 2 Select the severity level at which you want to be notified in the Severity list check box.

Step 3 Enter a description of the alert in the Description pane.

Step 4 Select **Next**.

Step 5 Configure the settings in the Threshold, Value Calculated As, Duration, Frequency, and Schedule panes.

Table 18: Counter Alert Configuration Parameters

Setting	Description
Threshold Pane	
Trigger alert when following conditions met (Over, Under)	Check and enter the value that applies: • Over: Check to configure a maximum threshold that must be met befo value field, enter a value. For example, enter a value that equals the nu • Under: Check to configure a minimum threshold that must be met befo value field, enter a value. For example, enter a value that equals the nu **Tip** Use these check boxes in conjunction with the Frequency
Value Calculated As Pane	
Absolute, Delta, Delta Percentage	Select the radio button that applies: • Absolute: Because some counter values are accumulative, select Abso • Delta: Select Delta to display the difference between the current count • Delta Percentage: Select Delta Percentage to display the counter perfo
Duration Pane	
Trigger alert only when value constantly...; Trigger alert immediately	• Trigger alert only when value constantly...**:** If you want the alert notifi or over threshold for a desired number of seconds, select this radio but alert to be sent. • Trigger alert immediately: If you want the alert notification to be sent
Frequency Pane	
Trigger alert on every poll; trigger up to...	Select the radio button that applies: • Trigger alert on every poll: If you want the alert notification to activat this radio button. • Trigger up to...: If you want the alert notification to activate at certain number of alerts that you want sent and the number of minutes within
Schedule Pane	
24-hours daily; start/stop	Select the radio button that applies: • 24-hours daily: If you want the alert to be triggered 24 hours a day, se • Start/Stop: If you want the alert notification activated within a specifi start time and a stop time. If checked, enter the start and stop times of the counter to be checked every day from 9:00 a.m. to 5:00 p.m. or fro

Suspend Alerts

You may want to temporarily suspend some or all alerts; you can suspend alerts on a particular node or on an entire cluster. For example, if you are upgrading your system to a newer release, suspend alerts until the upgrade completes, so that you do not receive e-mails and e-pages during the upgrade.

Follow this procedure to suspend alerts in Alert Central.

Procedure

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

Note Per node suspend states do not apply to clusterwide alerts.

Step 2 Perform one of the following actions:

- To suspend all alerts in the cluster, click the **Cluster Wide** radio button and check the **Suspend all alerts** check box.
- To suspend alerts per server, click the **Per Server** radio button and check the **Suspend** check box of each server on which you want alerts to be suspended.

Step 3 Click **OK**.

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

Set up alerts for core dump and collect relevant logs

Core dumps can be difficult to reproduce so it is particularly important to collect the log files associated with them when they occur and before they are over written.

Set up an e-mail alert for core dumps, so that you are immediately notified when one occurs to assist in troubleshooting its cause.

Enable Email Alert

Important Enable TLS mode, Enable Authentication mode, Username, and Password fields are introduced from Release 14SU2 onwards.

Procedure

Step 1 Select **System** > **Tools** > **Alert** > **Alert Central**.

Step 2 Right-click **CoreDumpFileFound** alert and select **Set Alert Properties**.

Step 3 Follow the wizard prompts to set your preferred criteria:

a) In the **Alert Properties: Email Notification** popup, make sure that **Enable Email** is checked and click **Configure** to set the default alert action, which will be to email an administrator.

b) Follow the prompts and **Add** a Recipient email address. When this alert is triggered, the default action is to email this address.

c) Click **Save**.

Step 4 Set the default Email server:

a) Select **System** > **Tools** > **Alert** > **Config Email Server**.

b) Enter the e-mail server and port information to send email alerts.

c) Enter the **Send User Id**.

d) Click **OK**.

Collect logs

Follow this procedure to collect logs after you receive an e-mail alert.

Procedure

Step 1 Note which services initiated the alert, which are indicated by “Core” in the e-mail message.

Step 2 Select **Tools** > **Trace & Log Central** > **Collect Files** and select the relevant logs for all impacted services.

For example, if the service is Cisco Presence Engine, collect the Cisco Presence Engine, Cisco XCP router and Cisco XCP Connection Manager logs. Or, if the service is Cisco XCP Router, collect the Cisco XCP Router, and Cisco XCP Connection Manager and Cisco Presence Engine logs.

Step 3 Generate the stack trace by running the following commands from the CLI:

utils core active list

utils core active analyze core *filename*

Step 4 Select **Tools** > **Trace & Log Central** > **Collect Files** and select the **RIS Data Collector PerfMon Log**.

Step 5 Select **Tools** > **SysLog Viewer** to collect the system logs.

a) Select a node.

b) Click **System Logs** > **messages** to view and save the messages.

c) Click **Application Logs** > **CiscoSyslog** to view and save the log file.

Step 6 Attach the collected files to your Cisco technical support case.

CHAPTER 8

Traces and Logs

Trace and Log Central

Note For Trace and Log Central to work, you must resolve DNS lookup for all nodes in the cluster on the client machine.

Preparation

Import Certificates

Follow this procedure to import the node certificates.

You can import the server authentication certificate that the certificate authority provides for the node or for each node in the cluster.

We recommend that you import the certificates before using the trace and log central option. If you do not import the certificates, the Trace and Log Central option displays a security certificate for the nodes each time that you sign in to Unified RTMT and access the Trace and Log Central option. You cannot change any data that displays for the certificate.

Procedure

Step 1 To import the certificate, choose **Tools** > **Trace** > **Import Certificate**.

A messages appears that states that the system imported the node certificates.

Step 2 Click **OK**.

Types of trace support

This section describes the types of trace support.

Trace and Log Central disk IO and CPU throttling

Unified RTMT supports the throttling of critical Trace and Log Central operations and jobs, whether they are running on demand, scheduled, or automatic.

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

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

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

View Trace and Log Central Options

Follow this procedure to view Trace and Log Central options in Unified RTMT.

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

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

Before you begin

Before you begin, import the security certificates.

Procedure

Step 1 Perform one of the following actions to access Trace and Log Central:

a) Select **System** in the Quick Launch Channel**.**
b) Select **System** > **Tools** > **Trace** > **Trace & Log Central**.
c) Select the **Trace & Log Central** icon in the tree hierarchy.

Step 2 Perform one of the following tasks after you display the Trace and Log Central options in the Real-Time Monitoring Tool:

- Collect traces for services, applications, and system logs on one or more servers in the cluster.

- Collect and download trace files that contain search criteria that you specify as well as save trace collection criteria for later use.
- Collect a crash dump file for one or more servers on your network.
- View the trace files that you have collected.
- View all of the trace files on the server.
- View the current trace file being written on the server for each application. You can perform a specified action when a search string appears in the trace file.

Collect files

Collect Trace Files

Use the Collect Files option in Trace and Log Central to collect traces for services, applications, and system logs on one or more nodes in the cluster. You specify date and time range for which you want to collect traces, the directory in which to download the trace files and whether to delete the collected files from the node.

Follow this procedure to collect traces using the trace and log central feature.

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

Use the Query Wizard if you want to collect trace files that contain search criteria that you specify or you want to use trace collection criteria that you saved for later use.

Before you begin

Perform one or more of the following actions:

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

Procedure

Step 1 Open the Trace and Log Central options.

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

The Trace Collection wizard appears. The services that you have not activated also appear, so you can collect traces for those services.

Note Unified Communications Manager and Cisco Unity Connection clusters: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

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

Step 3 *Cisco Unity Connection* users go to Step 4. For Unified Communations Manager or Cisco Business Edition, perform one of the following actions in the **Select CCM Services/Application** tab:

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

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

b) To collect traces for all services and applications on a particular node (or for particular system logs on the node for *Cisco Unity Connection*), check the check box next to the node and click **Next**.
c) To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
d) To go to the next tab without collecting traces for services or applications, click **Next**.

   Go to Step 4 for Cisco Business Edition or go to Step 5 for Unified Communications Manager.

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

a) To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
b) To collect traces for particular system logs on the node, check the check boxes that apply and click **Next**.
c) To go to the next tab without collecting traces for system logs, click **Next**.

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

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

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

b) To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
c) To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
d) To continue the trace collection wizard without collecting traces for system logs, click **Next**.

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

Note During log collection for locales other than English, we recommend that you select the Server Time Zone instead of the Client or Laptop Time Zone in which the server is installed.

a) **Absolute Range**: Specify the node time zone and the time range (start and end date and time) for which you want to collect traces.

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

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

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

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

Note Unified RTMT returns logs of a different time stamp, than that configured through the wizard. This occurs specifically, when the specified time stamp is lesser than that of the existing log files.

Log files exist on the node for a specific service from 11/24/09, and you have given the time range from 11/23/09 5:50 to 11/23/09 7:50; Unified RTMT still returns the existing log files.

Step 7 In the **Download File** option group list, specify the options that you want for downloading traces. From the **Select Partition** drop-down list, choose the partition that contains the logs for which you want to collect traces.

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

This means that when you upgrade from one version of Unified Communications Manager, Cisco Business Edition 5000, or Cisco Unity Connection that is running on an appliance node to another version, and you restart the node with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log back in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Unified Communications Manager or Cisco Unity Connection versions that ran on the Windows platform.

Step 8 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies `<rtmt_users_directory>\<server name or server IP address>\<download time>`.

Step 9 To create a zip file of the trace files that you collect, choose the **Zip File** radio button. To download the trace files without zipping the files, choose the **Do Not Zip Files** radio button.

Step 10 To delete collected log files from the node, check the **Delete Collected Log Files from the server** check box.

Step 11 Click **Finish** or, to abort the settings, click **Cancel**.

If you clicked Finish, the window shows the progress of the trace collection.

When the trace collection process is complete, the message “Completed downloading for node <Server name or IP address>” appears at the bottom of the window.

Step 12 To view the trace files that you collected, you can use the Local Browse option of the trace collection feature.

Note You will see a message if the service parameter values are exceeded or if the system is in code yellow.

Query Wizard

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

Before You Begin

- Configure the information that you want to include in the trace files for the various services from the **Trace Configuration** window.
- If you want alarms to be sent to a trace file, select an SDI trace file as the alarm destination in the **Alarm Configuration** window.

Start a Query

Procedure

Step 1 Open Trace & Log Central.

Step 2 Double-select **Query Wizard** in the tree hierarchy.

Step 3 Perform one of the following actions:

If you want to:	Action	Result
Run a Saved Query	• Select **Saved Query**. • Select **Browse** to navigate to the query that you want to use. • Select the query and select **Open**.	• If you chose is connected run the quer those server • If you chose checkmark r you do not v • If you chose when you sa check or unc servers, you node
Create a query	Select **Create Query**.	
Run the query without any modification	• Select **Run Query**. • Complete the steps in “Execute a schedule.”	
Modify the query	Go to Step 4.	

Step 4 Select **Next**.

Step 5 Perform one of the following actions:

- If you selected **Saved Query** and chose a query, the criteria that you specified for query appear. If necessary, modify the list of services and applications for which you want to collect traces.
- If you selected **Create Query**, you must select all services and applications for which you want to collect traces.

Step 6 Select **Next**.

Step 7 Perform one of the following actions:

If you want to:	Action
Collect traces for system logs or all system logs for all servers in the cluster	• Check the traces that apply. • Check **Select All Services on All Servers**. • Select **Next**.
Collect traces for all services and applications for all servers in the cluster,	• Check **Select All Services on All Servers**. • Select **Next**.
Collect traces for all services and applications on a particular server,	• Check the name of the server. • Select **Next**.

Step 8 Perform one of the following actions to specify the time range for which you want to collect traces:

If you want to:	Action
Collect all the traces on the server for the services that you chose	Select **All Available Traces**.
Collect all the traces within an absolute date and time range	• Select **Absolute Range**. • Specify the server time zone and the time ra to collect traces.
Collect all the traces within a relative date and time range	• Select **Relative Range**. • Specify the time (in minutes, hours, days, w you want to collect traces.

Step 9 Enter the word or phrase in the Search String field to search by phrases or words that exist in the trace file. The tool searches for an exact match to the word or phrase that you enter.

What to do next

Execute a query.

Execute a Query

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

- You can install some listed services or applications only on a particular node in the cluster. To collect traces for those services or applications, make sure that you collect traces from the node on which you have activated the service or application.
- The services that you have not activated also display, so you can collect traces for those services.
- After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature.
- An error message displays if the service parameter values are exceeded or if the system is in code yellow.

Procedure

Step 1 Select **Run Query** to execute the query.

Step 2 Select **Save Query** to save the query and continue with the next step.

Step 3 Select **OK** when the dialog box displays that indicates that the query execution completed.

Step 4 Perform the following actions:

If you want to:	Action	Result
Create a query that you can run on nodes other than the one on which it was created	**a.** Select **Generic Query**. **b.** Select either the **Single Node Query** or **All Node Query**. **c.** Select **Finish**.	• You can only create a generi node. If you chose services c either save the query as a reg • If you select the Single Node node on which you created tl • If you select the All Node Q all of the servers in the clust
Run the query on that node or cluster on which you created the query	**a.** Select **Regular Query**. **b.** Select **Finish**.	

Step 5 Browse to the location to store the query, enter a name for the query in the File Name field.

Step 6 Select **Save**.

Step 7 Perform one of the following actions:

If you want to:	Action
Run the query that you have just saved	• Select **Run Query**.
Exit the query wizard without running the query that you created	Select **Cancel**.

Step 8 Perform one of the following actions after the query execution completes:

If you want to:	Action
View a file that you collected	Follow these steps to navigate the file: **a.** Double-select **Query Results**. **b.** Double-select the <node> folder, where <nod node that you specified in the wizard. **c.** Double-select the folder that contains the file **d.** After you have located the file, double-select
Download the trace files and the result file that contains a list of the trace files that your query collected	**a.** Select the files that you want to download. **b.** Select **Download**. **c.** Specify the criteria for the download. **d.** Select **Finish**.
Specify the directory in which you want to download the trace files and the results file	**a.** Select **Browse** next to the Download all files **b.** Navigate to the directory. **c.** Select **Open**.
Create a zip file of the trace files that you collected	Select **Zip File**.
Delete collected log files from the server	Check **Delete Collected Log Files from Server**.
Save the query	• Select **Save Query**.

Schedule Trace Collection in Cisco Unified Communications Manager

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

Note You can schedule up ten trace collection jobs, but only six trace collection can be concurrent. That is, only six jobs can be in a running state at the same time.

Before you begin

Note For large deployments, we recommend that you use a dedicated trace archive server and set up scheduled trace collections to this trace server.

Perform one or more of the following actions:

- Configure the information that you want to include in the trace files for the various services from the **Trace Configuration** window of Cisco Unified Serviceability. For more information, see the *Cisco Unified Serviceability Administration Guide*.
- If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the **Alarm Configuration** window. For more information, see the *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Open the Trace and Log Central options.

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

The Schedule Collection wizard appears.

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

Note If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

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

Step 3 Perform one of the following actions in the **Select CCM Services/Application** tab:

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

- To collect traces for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for services or applications, click **Next**.

Step 4 In the **Select System Services/Application** tab, perform one of the following actions:

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

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

Step 5 Specify the node time zone and the time range for which you want to collect traces.

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

Step 6 To specify the date and time that you want to start the trace collection, click the down arrow button next to the Schedule Start Date/Time field. In the **Date** tab, choose the appropriate date. In the **Time** tab, choose the appropriate time.

Step 7 To specify the date and time that you want to end the trace collection, click the down arrow button next to the Schedule End Date/Time field. In the **Date** tab, choose the appropriate date. In the **Time** tab, choose the appropriate time.

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

Step 8 From the **Scheduler Frequency** drop-down list, choose how often you want to run the configured trace collection.

Step 9 From the **Collect Files that are generated** in the last drop-down list, specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 10 To search by phrases or words that exist in the trace file, enter the word or phrase in the **Search String** field. The tool searches for a match to the word or phrase that you enter and collects those files that match the search criteria. If you want to search for an exact match to the word or phrase that you entered, check the **Case Sensitive** check box

Step 11 To create a zip file of the trace files that you collect, check the **Zip File** check box.

Step 12 To delete collected log files from the node, check the **Delete Collected Log Files from the Server** check box.

Step 13 Choose one or more of the following actions:

- Download Files and go to Step 14.
- Run Another Query and go to Step 15.
- Generate Syslog. If you chose Generate Syslog, go to Step 16.

Step 14 In the SFTP/FTP Server Parameters group box, enter the node credentials for the node where the trace and log central feature downloads the results and click **Test Connection**. Enter the fingerprint values, when asked. After the trace and log central feature verifies the successful connection to the SFTP or FTP server, click **OK**.

Note If the jobs were already scheduled before Cisco Prime Collaboration Deployment Migration, perform step 14 again for the jobs to be executed successfully. After this, click **Cancel** to avoid job creation in the Download Files window. If any of the nodes in a cluster is down, ensure that you perform step 14 and verify the SFTP connection after the node comes back up.

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

You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.

If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine. We recommend that you use SFTP server for scheduled trace collections.

Step 15 If you chose the Run Another Query Option, click the **Browse** button to locate the query that you want to run, and click **OK**.

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

Step 16 Click **Finish**.

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

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

Step 17 Click **OK**.

Step 18 To view a list of scheduled collections, click the **Job Status** icon in the Trace portion of the Quick Launch Channel.

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

Schedule Trace Collection in Cisco Unity Connection

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

Note You can schedule up ten trace collection jobs, but only six trace collection can be concurrent. That is, only six jobs can be in a running state at the same time.

Before you begin

Perform one or more of the following actions:

- Configure the information that you want to include in the trace files for the various services from the **Trace Configuration** window of Cisco Unified Serviceability. For more information, see the *Cisco Unified Serviceability Administration Guide*.
- If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the **Alarm Configuration** window. For more information, see the *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Open the Trace and Log Central options.

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

The Schedule Collection wizard appears.

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

Note Cisco Unity Connection: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note Cisco Unity Connection: You can install some listed services and applications on a particular node in the cluster. To collect traces for those services and applications, make sure that you collect traces from the node on which you have activated the service or application.

Step 3 In the **Select CUC Services/Application** tab, perform one of the following actions:

- To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To collect traces for particular system logs on the node, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

Step 4 In the **Select System Services/Application** tab, perform one of the following actions:

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

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

Step 5 Specify the node time zone and the time range for which you want to collect traces.

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

Step 6 To specify the date and time that you want to start the trace collection, click the down arrow button next to the Schedule Start Date/Time field. In the **Date** tab, choose the appropriate date. In the **Time** tab, choose the appropriate time.

Step 7 To specify the date and time that you want to end the trace collection, click the down arrow button next to the Schedule End Date/Time field. In the **Date** tab, choose the appropriate date. In the **Time** tab, choose the appropriate time.

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

Step 8 From the **Scheduler Frequency** drop-down list box, choose how often you want to run the configured trace collection.

Step 9 From the **Collect Files that are generated** in the last drop-down list boxes, specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 10 To search by phrases or words that exist in the trace file, enter the word or phrase in the **Search String** field. The tool searches for a match to the word or phrase that you enter and collects those files that match the search criteria. If you want to search for an exact match to the word or phrase that you entered, check the **Case Sensitive** check box

Step 11 To create a zip file of the trace files that you collect, check the **Zip File** check box.

Step 12 To delete collected log files from the node, check the **Delete Collected Log Files from the Server** check box.

Step 13 Choose one or more of the following actions:

- Download Files. If you chose Download Files or Run Another Query, continue with Step 15.
- Run Another Query.
- Generate Syslog. If you chose Generate Syslog, go to Step 17.

Step 14 In the SFTP/FTP Server Parameters group box, enter the node credentials for the node where the trace and log central feature downloads the results and click **Test Connection**. After the trace and log central feature verifies the connection to the SFTP or FTP server, click **OK**.

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

You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.

If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine. We recommend that you use SFTP server for scheduled trace collections.

Step 15 If you chose the Run Another Query Option, click the **Browse** button to locate the query that you want to run, and click **OK**.

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

Step 16 Click **Finish**.

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

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

Step 17 Click **OK**.

Step 18 To view a list of scheduled collections, click the **Job Status** icon in the Trace portion of the Quick Launch Channel.

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

Start a schedule

Before you begin

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window.
- If you want alarms to be sent to a trace file, select an SDI trace file as the alarm destination in the Alarm Configuration window.

Procedure

Step 1 Open Trace & Log Central.

Step 2 Double-select **Schedule Collection** in the tree hierarchy.

Step 3 Perform one of the following actions to collect trace on node logs:

If you want to:	Action
Collect traces for all services and applications for all nodes in the cluster	• Check **Select All Services on All Servers**. • Select **Next**.
Collect traces for all services and applications on a particular node	• Check the name of the node. • Select **Next**.
Collect traces for particular services or applications on particular nodes	• Check the traces that apply. • Select **Next**.
Continue the trace collection wizard without collecting traces for services or applications	Select **Next**.

Step 4 Perform one of the following actions to collect traces on system logs:

If you want to:	Action
Collect all system logs for all nodes in the cluster	• Check **Select All Services on All Servers**. • Select **Next**.
Collect traces for all system logs on a particular node	• Check the name of the node. • Select **Next**.
Collect traces for particular system logs on particular nodes	Check the traces that apply. For example, to collect CSA logs, check **Cisco Se** information about users that are signing in and ou
Continue the trace collection wizard without collecting traces for system logs	Select **Next**.

Step 5 Specify the node time zone and the time range for which you want to collect traces.

Step 6 Perform the following actions to specify the date and time that you want to start the trace collection:

a) Select the down arrow button next to the Schedule Start Date/Time field.

b) From the Date tab, select the appropriate date.
c) From the Time tab, select the appropriate time.

Step 7 To specify the date and time that you want to end the trace collection, perform the following actions:

a) Select the down arrow button next to the Schedule End Date/Time field.
b) From the Date tab, select the appropriate date.
c) From the Time tab, select the appropriate time.

Troubleshooting Tips

- The time zone of the client computer provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.
- Trace collection completes, even if the collection goes beyond the configured end time; however, the Trace and Log Central feature deletes this collection from the schedule.

What to do next

Execute a schedule, on page 140

Execute a schedule

Procedure

Step 1 Select how often you want to run the configured trace collection from the Scheduler Frequency list box.

Step 2 Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 3 Enter the word or phrase in the **Search String** field to search by phrases or words that exist in the trace file. The tool searches for an exact match to the word or phrase that you enter and only collects those files that match the search criteria.

Step 4 Check **Zip All Files** to create a zip file of the trace files that you collect.

Step 5 Check **Delete Collected Log Files from the Server** to delete collected log files from the server.

Step 6 Perform one or more of the following actions:

- To download files:
  - **a.** Select **Download Files**.
  - **b.** In the SFTP Server Parameters group box, enter the node credentials for the node where the trace and log central feature downloads the results.
  - **c.** Select **Test Connection**.
  - **d.** After the trace and log central feature verifies the connection to the SFTP server, select **OK**.
- To run another query:
  - **a.** Select **Run Another Query**.

b. Select **Browse** to locate the query that you want to run.

c. Select **OK**.

- To generate a Syslog, select **Generate Syslog**.

Step 7 Select **Finish**.

Troubleshooting Tips

- If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node does not appear in the Trace & Log Central windows.
- If Unified RTMT cannot access the SFTP server, a message appears. Verify that you entered the correct IP address, username, and password.
- You can install some of the listed services/applications only on a particular node in the cluster. To collect traces for those services/applications, make sure that you collect traces from the node on which you have activated the service/application.
- The services that you have not activated also appear, so you can collect traces for those services.
- The trace collection completes, even if the collection goes beyond the configured end time; however, the trace and log central feature deletes this collection from the schedule.
- The **Download Directory Path** field specifies the directory in which the trace and log central feature stores collected files. By default, the trace collection stores the files in the home directory of the user whose user ID you specify in the SFTP parameters fields: */home/<user>/Trace*.
- The trace and log central feature only executes the specified query if the first query generates results.

View Trace Collection Status

Follow this procedure to view the trace collection event status and to delete scheduled trace collections.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

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

The **Job Status** window appears.

Step 3 From the **Select a Node** drop-down list box, choose the server for which you want to view or delete trace collection events.

This list of scheduled trace collections appears.

Possible job types include the following:

- Scheduled Job
- OnDemand
- RealTimeFileMon

- RealTimeFileSearch

Possible statuses include the following:

- Pending
- Running
- Cancel
- Terminated

Step 4 To delete a scheduled collection, choose the event that you want to delete and click **Delete**.

Note You can cancel jobs with a status of "Pending" or "Running" and a job type of "Schedule Task" or job type of "RealTimeFileSearch."

Generate Problem Reporting Tool

The Problem Reporting Tool (PRT) on the Cisco IP Phone allows you to collect and send phone logs to your administrator. These logs are necessary for troubleshooting in case you run into issues with the phones.

Generate PRT for Endpoints

Use the Generate PRT option in Trace and Log Central to remotely trigger the log collection on the phone and upload it to the log server configured in the "Customer support upload URL" parameter.

Procedure

Step 1 Open the Trace and Log Central options.

Step 2 In the Trace & Log Central tree hierarchy, choose **Generate PRT**.
The Generate PRT wizard appears.

Step 3 Enter the Device name as configured in the Find and List Phones page in the Cisco Unified CM Administration user interface.

Step 4 Click **Generate PRT**.

The generated report is uploaded at the **Customer support upload URL**.

Note Configure the **Customer support upload URL** parameter in either the Enterprise, Profile, or Device level configuration page settings. Else, PRT generation fails.

Real-Time Trace

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

The real-time trace provides the option to view real-time data and monitor user events.

View Real-Time Data

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

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

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

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

Note Unified Communications Manager clusters and Cisco Unity Connection clusters only: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not display in the Trace and Log Central windows.

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

The View Real Time Data wizard appears.

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

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

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

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

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

Step 7 Perform one of the following actions:

- Check the **Show New Data** check box to keep the cursor at the end of the window to display new traces as they appear.
- Uncheck the **Show New Data** check box if you do not want the cursor to move to the bottom of the window as new traces display.

Step 8 Repeat this procedure to view data for additional services.

A message appears if you attempt to view data for too many services or too many services on a single node.

Step 9 After you finish with viewing the real-time data, click **Close** on the generic log viewer.

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

Monitor User Event

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

Before you begin

If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

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

Note Unified Communications Manager clusters and Cisco Unity Connection clusters only: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node does not display in the Trace and Log Central windows.

Step 3 Double-click **Monitor User Event**.

The Monitor User Event wizard appears.

Step 4 Perform one of the following actions:

If you want to:	Action
View the monitoring events that you have already set up	• Click **View Configured Events**. • Select a node from the drop-down list box. • Click **Finish**. **Note** To delete an event, choose the event and click **Delete**.
Configure new monitoring events	• Select **Create Events.** • Select **Next**. • Continue with Step 5.

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

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

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

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

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

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

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

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

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

If you want the system to:	Action
Generate an alarm when the system encounters the specified search string	Check **Alert**. **Note** For the system to generate the alarm, you must enable the enable the TraceCollectionToolEvent alert.
Log the errors in the application logs area in the SysLog Viewer	Check **Local Syslog**. **Note** The system provides a description of the alarm and a recommended action. You can access the SysLog Viewer from Unified RTMT.
Store the syslog messages on a syslog node	Check **Remote Syslog**. Enter the syslog node name in the **Server Name** field. **Note** By default, audit events are not sent to the remote syslog node, unless the severity is lowered to Warning, Notice, or Informational.
Download the trace files that contain the specified search string	Check **Download File**. Enter the node credentials for the node where you want to download the trace files in the SFTP Server Parameters group box. Select **Test Connection**. Select **OK** after the Trace and Log Central feature verifies the connection to the SFTP server. The Download Directory Path field specifies the directory in which the trace and log central feature stores collected files. By default, the trace collection

If you want the system to:	Action
	stores the files in the home directory of the user whose user ID you specify in the SFTP/FTP parameters fields: /home/<user>/Trace. You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers. If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command. **Note** FTP is not supported for Cisco Intercompany Media Engine. We recommend that you use SFTP server for scheduled trace collections.

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

The following message appears: `If trace compression is enabled, there might be a delay in catching the event after it occurs, due to buffering of data.`

Step 10 Click **Finish**.

Collect Crash Dump in Cisco Unified Communications Manager

Follow this procedure to collect a core dump of trace files.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

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

The Collect Crash Dump wizard appears.

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

Note If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

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

Step 3 Perform one of the following actions in the **Select CCM Services/Application** tab:

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

- To collect traces for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for services or applications, click **Next**.

Step 4 In the **Select System Services/Application** tab, perform one of the following actions:

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

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

Step 5 In the Collection Time group box, specify the time range for which you want to collect traces. Choose one of the following options:

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

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

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

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

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

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

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

When you upgrade from one version of your product that is running on the Linux platform to another version, and you restart the node with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection versions that ran on the Windows platform.

Step 7 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies `<rtmt_users_directory>\<server name or server IP address>\<download time>`.

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

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

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

Step 10 Click **Finish**.

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

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

Collect Crash Dump in Cisco Unity Connection

Follow this procedure to collect a core dump of trace files.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

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

The Collect Crash Dump wizard appears.

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

Note Cisco Unity Connection: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note Cisco Unity Connection: You can install some of the listed services or applications on a particular node in the cluster. To collect traces for those services or applications, make sure that you collect traces from the node on which you have activated the service or application.

Step 3 In the **Select CUC Services/Application** tab, perform one of the following actions:

- To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To collect traces for particular system logs on the nodes, check the check boxes that apply and click **Next**.

- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

Step 4 In the **Select System Services/Application** tab, perform one of the following actions:

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

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

Step 5 In the Collection Time group box, specify the time range for which you want to collect traces. Choose one of the following options:

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

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

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

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

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

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

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

When you upgrade from one version of your product that is running on the Linux platform to another version, and you restart the node with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection versions that ran on the Windows platform.

Step 7 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies

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

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

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

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

Step 10 Click **Finish**.

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

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

Collect Installation Logs

Follow this procedure to collect installation and upgrade logs.

Procedure

Step 1 Choose **Tools** > **Trace** > **Trace & Log Central**.

The **Trace & Log Central** window appears.

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

The Collect Install Logs wizard appears.

Step 3 In the Select Servers Options box, specify from which server you would like to collect the install logs.

- To collect the install logs for a particular server, check the check box next to the server.
- To collect the install logs for all servers, check the Select All Servers check box.

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

Step 5 Click **Finish**.

Collect audit logs

Browse Audit Logs

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Collect Audit Logs**.

The Collect Audit Logs Action Options wizard appears.

Step 3 Check the **Browse Audit Logs** check box.

Step 4 Click **Next**.

The Nodes Selection Options wizard appears.

Step 5 Perform one of the following actions in the **Action Options** window:

Note If you have a standalone server and check the **Select All Servers** check box, the system browses all audit logs for your standalone server.

a) To browse audit logs for all servers, check the **Select All Servers** check box.
b) To browse audit logs on a particular server, check the check box next to the server.

Step 6 Click **Finish**.

Step 7 The Remote Browse is Ready window appears. Click **Close**.

The Nodes pane appears.

Step 8 On the left side of the Nodes pane, double-click the **Nodes** folder. Navigate through the tree hierarchy until the Audit App folder appears.

Step 9 After the audit log file names display in the pane on the right side of the window, you can either right-click the mouse to select the type of program that you want to use to view each file or double-click the selected file to display the file in the default viewer.

Step 10 Select an audit log file and perform one of the following actions:

- To create a zip file of the audit log files that you collect, click the **Zip File** radio button.

  Note You cannot download a zipped audit log file that exceeds 2 gigabytes.

- To delete collected audit log files from the server, check the **Delete Files on Server** check box.
- To delete the selected audit log file, click **Delete**.
- To refresh the selected audit log file, click **Refresh**.
- To refresh all of the audit log files, click **Refresh All**.

Note Cisco Unified Serviceability does not retain audit logs from Unified Communications Manager or Unified Communications Manager IM and Presence Service versions that run on the Windows platform.

You have completed the steps for Browse Audit Logs.

Download Audit Logs

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Collect Audit Logs**.

The Collect Audit Logs Action Options wizard appears.

Step 3 Check the **Download Audit Logs** check box.

Step 4 Click **Next**.

The Nodes Selection Options wizard appears.

Step 5 Perform one of the following actions in the **Action Options** window:

Note If you have a standalone server and check the **Select All Servers** check box, the system downloads all audit logs for your standalone server.

a) To download audit logs for all servers, check the **Select All Servers** check box.

b) To download audit logs on a particular server, check the check box next to the server.

Step 6 Click **Finish**.

Step 7 To download audit logs, click **Next**.

The **Download Audit Logs** window appears.

Step 8 In the Nodes Selection Options pane, perform one of the following actions:

- Check the **Select All Servers** check box.
- Check a specific node check box.

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

- **Absolute Range**: Specify the server time zone and the time range (start and end date and time) for which you want to audit logs.

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

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

- **Relative Range**: Specify the length of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect audit logs based on the values from the following table:

Period of Time	Range
Minutes	5 - 60
Hours	2 - 24

Period of Time	Range
Days	1 - 31
Weeks	1 - 4
Months	1 -12

Step 10 In the Download File Options pane, select one of the following options:

a) To specify the directory in which you want to download the audit log file, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies `<\Program Files\Cisco\Unified RTMT\JRtmt>`.

b) To create a zip file of the audit log files that you collect, choose the **Zip File** radio button.

Note You cannot download a zipped audit log file that exceeds 2 gigabytes.

c) To delete collected audit log files from the server, check the **Delete Collected Log Files from Server** check box.

Step 11 Click **Finish**.

You have completed the steps for the download of audit logs.

Schedule Audit Log Download

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Collect Audit Logs**.

The Collect Audit Logs Action Options wizard appears.

Step 3 Check the **Schedule Download of Audit Logs** check box.

Step 4 Click **Next**.

The Nodes Selection Options wizard appears.

Step 5 Perform one of the following actions in the **Action Options** window:

Note If you have a standalone node and check the **Select All Servers** check box, the system browses, downloads, or schedules a download of all audit logs for your standalone node.

a) To schedule a download of audit logs for all nodes, check the **Select All Servers** check box.

b) To schedule a download of audit logs on a particular node, check the check box next to the node.

Step 6 Click **Finish**.

The **Schedule Download of Audit Logs** window appears.

Step 7 In the Nodes Selection Options pane, perform one of the following actions:

- Check the **Select All Servers** check box.

- Check a specific node check box.

Step 8 In the Schedule Time pane, perform the following actions:

a) Highlight the **Select Reference Server Time Zone**.
b) Use the calendar and highlight a **Start Date/Time**.
c) Use the calendar and highlight an **End Date/Time**.
d) Select the Scheduler Frequency. You may choose Hourly, Daily, Weekly, or Monthly.
e) Check the **Zip All Files** check box to zip the audit log files.
f) Check the **Delete Collected Log Files From Server** check box to delete the collected audit log files from the node.

Step 9 In the Action Options pane, check the **Download Files** check box.
The **Trace Download Configuration Dialog** window appears.

Step 10 Enter the following information:

- Protocol: Select FTP (default) or SFTP.
- Host IP Address: Enter the IP address of the host node.
- User Name: Enter your username.
- Password: Enter your password.
- Port: Enter the FTP or SFTP port information.
- Download Directory Path: Enter the complete directory path where the files get downloaded.
- Click **Test Connection**. When the connection has been tested, the files are downloaded.

Note You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.

If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine. We recommend that you use SFTP server for scheduled trace collections.

You have completed the steps to schedule the download of audit logs.

Display Downloaded Trace Files Using Local Browse

After you collect trace files and download them to your PC, you can view them with a text editor that can handle UNIX variant line terminators such as WordPad on your PC, or you can view them by using the viewers within Unified RTMT.

Tip Do not use NotePad to view collected trace files.

Follow this procedure to display the log files that you collected with the Trace and Log Central feature. If you zipped the trace files when you downloaded them to your PC, you need to unzip the files to view them by using the viewers within Unified RTMT.

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

Before you begin

Collect the required traces files. See topics related to collecting trace files, downloading trace files using Query Wizard, and scheduling trace collection for instructions.

Procedure

Step 1 Open Trace and Log Central.

Step 2 Double-click **Local Browse**.

Step 3 Browse to the directory where you stored the log file and choose the file that you want to view.

Step 4 To display the results, double-click the file.

If the file type has a viewer that is already associated with it, the file opens in that viewer. Otherwise, the Open With dialog box appears.

Step 5 Click the program that want to use to view the file. If your preferred program is not on the list, choose another program by clicking **Other**.

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

Unified RTMT displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, Unified RTMT opens files in the Generic Log Viewer.

Display and Download Trace Files in Cisco Unified Communications Manager

After the system generates trace files, you can view them on the node by using the viewers within Unified RTMT. You can also use the remote browse feature to download the traces to your PC.

Follow this procedure to display and download the log files on the node with the Trace and Log Central feature.

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

Before you begin

Collect the required traces files. See topics related to collecting trace files, downloading trace files using Query Wizard, and scheduling trace collection.

Procedure

Step 1 Open the Trace and Log Central options.

Step 2 Double-click **Remote Browse**.

Step 3 Choose the appropriate radio button, and click **Next**.

- If you choose Trace Files, go to Step 4.
- If you choose Crash Dump, go to Step 7.

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

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

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

Step 4 Perform one of the following actions in the Select CCM Services/Application tab:

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

- To collect traces for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for services or applications, click **Next**.

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

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

a) To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
b) To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
c) To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
d) To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.
e) Go to Step 10.

Step 6 Perform one of the following actions in the **Select CCM Services/Application** tab:

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone node.

a) To choose crash dump files for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
b) To choose crash dump files for all services and applications on a particular node, check the check box next to the node and click **Next**.
c) To choose crash dump files for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
d) To continue the Remote Browse wizard without collecting crash dump files, click **Next**.

Go to Step 8 for Cisco Business Edition or go to Step 9 for Unified Communications Manager.

Step 7 In the **Select System Services/Application** tab, perform one of the following tasks:

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone node.

a) To choose crash dump files for all nodes, check the **Select All Services on all Servers** check box.
b) To choose crash dump files for all system logs on a particular node, check the check box next to the node.
c) To choose crash dump files for particular system logs on particular nodes, check the check boxes that apply.
d) To continue the Remote Browse wizard without collecting crash dump files, go to the next step.

Step 8 Click **Finish**.

Step 9 After the traces become available, a message appears. Click **Close**.

Step 10 Perform one of the following actions:

- To display the results, navigate to the file through the tree hierarchy. After the log filename appears in the pane on the right side of the window, you can either right-click the mouse to select the type of program that you would like to use to view the file or double-click the file to display the file in the default viewer.

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

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

- To download the trace files, choose the files that you want to download, click **Download**, specify the criteria for the download, and click **Finish**.
  - To specify the directory in which you want to download the trace files, click **Browse** next to the Download all files field, navigate to the directory, and click **Open**. The default specifies `<rtmt_users_directory>\<server name or server IP address>\<download time>`.
  - To create a zip file of the trace files that you collect, check the **Zip File** check box.
  - To delete collected log files from the node, check the **Delete Files on server** check box.
- To delete trace files from the node, click the file that appears in the pane on the right side of the window; then, click **Delete**.
- To refresh a specific service or a specific node in a cluster, click the service or node name; then, click **Refresh**. After a message states that the remote browse is ready, click **Close**.

- To refresh all services or all nodes in a cluster that appear in the tree hierarchy, click **Refresh All**. After a message states that the remote browse is ready, click **Close**.

  Tip After you download the trace files, you can view them in Local Browse.

Display And Download Trace Files in Cisco Unity Connection

After the system generates trace files, you can view them on the node by using the viewers within Unified RTMT. You can also use the remote browse feature to download the traces to your PC.

Follow this procedure to display and download the log files on the node with the Trace and Log Central feature.

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

Before you begin

Collect the required traces files. See topics related to collecting trace files, downloading trace files using Query Wizard, and scheduling trace collection.

Procedure

Step 1 Open the Trace and Log Central options.

Step 2 Double-click **Remote Browse**.

Step 3 Choose the appropriate radio button, and click **Next**.

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

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

Note Cisco Unity Connection clusters: You can install some of the listed services on applications on a particular node in the cluster. To choose traces for those services or applications, make sure that you choose traces from the node on which you have activated the service or application.

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

- To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To collect traces for particular system logs on the node, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.

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

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

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.

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

- To choose crash dump files for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To choose crash dump files for particular system logs on the node, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting crash dump files, click **Next**.

Step 7 In the **Select System Services/Application** tab, perform one of the following tasks:

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone node.

- To choose crash dump files for all nodes, check the **Select All Services on all Servers** check box.
- To choose crash dump files for all system logs on a particular node, check the check box next to the node.
- To choose crash dump files for particular system logs on particular nodes, check the check boxes that apply.
- To continue the Remote Browse wizard without collecting crash dump files, go to the next step.

Step 8 Click **Finish**.

Step 9 After the traces become available, a message appears. Click **Close**.

Step 10 Perform one of the following actions:

- To display the results, navigate to the file through the tree hierarchy. After the log filename appears in the pane on the right side of the window, you can either right-click the mouse to select the type of program that you would like to use to view the file or double-click the file to display the file in the default viewer.

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

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

- To download the trace files, choose the files that you want to download, click **Download**, specify the criteria for the download, and click **Finish**.
  - To specify the directory in which you want to download the trace files, click **Browse** next to the Download all files field, navigate to the directory, and click **Open**. The default specifies `<rtmt_user_directory>\<server name or server IP address>\<download time>` where `<rtmt_user_directory>` specifies the directory where Unified RTMT is installed.

- To create a zip file of the trace files that you collect, check the **Zip File** check box.
- To delete collected log files from the node, check the **Delete Files on server** check box.

- To delete trace files from the node, click the file that appears in the pane on the right side of the window; then, click **Delete**.
- To refresh a specific service or a specific node in a cluster, click the service or node name; then, click **Refresh**. After a message states that the remote browse is ready, click **Close**.
- To refresh all services or all nodes in a cluster that appear in the tree hierarchy, click **Refresh All**. After a message states that the remote browse is ready, click **Close**.

Tip After you download the trace files, you can view them in Local Browse.

Set Trace Collection Attributes

Before you begin

Collect traces files.

Procedure

Step 1 Open Trace & Log Central.

Step 2 Double-select **Remote Browse**.

Step 3 Select the appropriate radio button, Trace Files or Crash Dump.

Step 4 Select **Next**.

Step 5 Perform one of the following actions:

a) If you select Trace Files, go to step 6.
b) If you select Crash Dump, go to step 8.

Step 6 Perform one of the following actions in the Voice/Video or IM and Presence Applications/Services tab:

If you want to:	Action
Collect traces for all services and applications for all servers in the cluster	• Select **All Services on All Servers** • Select **Next**.
Collect traces for all services and applications on a particular server	• Check the name of the server. • Select **Next**.
Collect traces for particular services or applications on particular servers	• Check the traces that apply. • Select **Next**.
Continue the trace collection wizard without collecting traces for services or applications	Select **Next**.

Step 7 Perform one of the following actions in the Select System Services/Application tab:

If you want to:	Action
Collect all system logs for all servers in the cluster	• Check **Select All Services on all Servers**. • Select **Next**
Collect traces for all system logs on a particular server	• Check the name of the server. • Select **Next**.
Collect traces for particular system logs on particular servers	• Check the traces that apply. **Note** For example, to collect CSA logs, che information about users that are signi • Select **Next**.
Continue the remote browse wizard without collecting traces for system logs	Go to Select finish.

Step 8 Perform one of the following actions in the Voice/Video or IM and Presence Applications/Services tab:.

If you want to:	Action
Collect crash dump files for all services and applications for all servers in the cluster	• Check **Select All Services on All Servers**. • Select **Next**.
Collect crash dump files for all services and applications on a particular server	• Check the name of the server. • Select **Next**.
Collect crash dump files for particular services or applications on particular servers	• Check the traces that apply. • Select **Next.**

Step 9 Perform one of the following actions in the Select System Services/Application tab:.

If you want to:	Action
Collect crash dump files for all services and applications for all servers in the cluster	• Check **Select All Services on All Servers**. • Select **Next**.
Collect crash dump files for all services and applications on a particular server	• Check the name of the server. • Select **Next**.
Collect crash dump files for particular services or applications on particular servers.	• Check the traces that apply. • Select **Next.**
Continue the collect crash dump wizard without collecting crash dump files	Go to Step 10.

Step 10 Select **Finish**.

What to do next

View trace results.

View Trace Results

- You can install some listed services/applications only on a particular node in the cluster. To select traces for those services/applications, make sure that you select traces from the server on which you have activated the service/application.
- The services that you have not activated also display, so you can select traces for those services.
- After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature.
- To sort the files that displays in the pane, select a column header; for example, to sort the files by name, select the Name column header.
- The Real-Time Monitoring Tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the Real-Time Monitoring Tool opens files in the Generic Log Viewer.
- The IM and Presence service does not support the Q931 Translator. IM and Presence does not support QRT report information.

Before you begin

Set your trace collection attributes.

Procedure

Step 1 Select **Close** when a message states that the trace results are available.

Step 2 Perform one of the following actions:

If you want to:	Action
To display the results	Perform one of the following actions to navigate Right-select the mouse to select the type of progr file.Double-select the file to display the file in the
Download the trace files and the result file that contains a list of the trace files that your query collected	• Select the files that you want to download. • Select **Download**. • Specify the criteria for the download. • Select **Finish**.
Specify the directory in which you want to download the trace files and the results file	• Select **Browse** next to the Download all files • Navigate to the directory. • Select **Open**. The default specifies C:\Progra address>\<download time>
Create a zip file of the trace files that you collected	Check **Zip File**.
Delete collected log files from the server	Check **Delete Collected Log Files from Server**.
Delete trace files from the node	• Select the file that displays in the pane on th • Select **Delete**.

If you want to:	Action
Refresh a specific service or node	• Select the server name or service. • Select **Refresh**. • Select **Close** when a message states that
Refresh all services and nodes that display in the tree hierarchy	• Select **Refresh All**. • Select **Close** when a message states that

Display Report Information

You can view the QRT log files by either viewing the files on the server or by downloading the files onto your computer.

Note This section applies only to Unified Communications Manager.

You can view the IP phone problem reports that the Quality Report Tool generates by using the QRT viewer. QRT serves as a voice-quality and general problem-reporting tool for Cisco Unified IP Phones. After you collect the QRT log files, you can use the following procedure to list and view Unified Communications Manager IP Phone problem reports by using the QRT viewer. The QRT viewer allows you to filter, format, and view phone problem reports that are generated. For more information about how to configure and use QRT, see the *System Configuration Guide for Cisco Unified Communications Manager* .

Before you begin

Collect or view the Quality Report Tool (QRT) log files. See topics related to collecting trace files, scheduling trace collection, and downloading trace files using either Query Wizard or the Remote Browser.

Procedure

Step 1 Display the log file entries by using the Query Wizard, the Remote Browse, or the Local Browse option in Trace and Log Central.

The QRT Viewer window appears.

Note Only log files from the Cisco Extended Functions service contain QRT information. The following format for the log filename that contains QRT data applies: qrtXXX.xml.

Note The QRT viewer allows only the .xml files with a specific structure (having phone details), not the default one. If you open generic log files, you may see the following error message:

```
Fail to Open Cisco QRT Viewer, No Records Available!
```

Step 2 From the **Extension** drop-down list box, choose the extension or extensions that you want the report to include.

Step 3 From the **Device** drop-down list box, choose the device or devices that you want the report to include.

Step 4 From the **Category** drop-down list box, choose the problem category that you want the report to include.

Step 5 From the **Select Fields** drop-down list box, choose the fields that you want the report to include.

Note The order in which you choose the fields determines the order in which they appear in the QRT Report Result pane.

Step 6 To view the report in the QRT Report Result pane, click **Display Records**.

Log Compression

In Unified Communications Manager 8.0 onward, the log compression feature only compresses the following log files:

- `cm/trace/cti/sdl`
- `cm/trace/cti/sdi`
- `cm/trace/ccm/sdl`
- `cm/trace/ccm/sdi`

The other log files are not compressed and are written directly to the hard disk.

The compressed files have a .gz extension. The file that is being actively written to the disk will have a .gzo extension.

All the CLI commands used to view and tail the files will work on the compressed files and will automatically uncompress them for viewing or tailing. The only difference is in specifying file names with the .gz and .gzo extension.

The following option is available with the file tail command:

file tail activelog cm/trace/cti/sdl recent

The recent option, when used with a compressed directory, continually tails the most recent log file. You do not need to switch to a newer log file when the currently written-to log file is closed, so it is an infinite and ongoing tail. This option is only available with the compressed log files.

The log files are compressed in the gzip format. For uncompressing the log files, the open source program 7-Zip is available at `http://www.7-zip.org`, and works on all Windows platforms. You can use 7-Zip on any computer, including a computer in a commercial organization. You do not need to register or pay for 7-Zip. On a Linux platform, you can use the gzip or gunzip commands.

Edit Trace Settings

Follow this procedure to edit trace settings for Unified RTMT.

Note The Error radio button is the default setting.

Procedure

Step 1 Choose **Edit** > **Trace Setting**

Step 2 Click the radio button that applies.

The system stores the rtmt.log file in the Documents and Settings directory for the user; for example, on a Windows machine, the log is stored in `C:\Documents and Settings\<userid>\.jrtmt\log`.

Log Viewers

Messages in AuditLog Viewer

You can display the following messages in AuditLog Viewer:

- AuditApp Logs: These logs are related to Unified Communications Manager application audit logs.
- Vos Logs: These logs are related to platform (terminal, port or network address of the system) activities.

The following table describes the AuditLog Viewer buttons.

Table 19: AuditLog Viewer Buttons

Button	Function
Refresh	Updates the contents of the current log on the Auditlog Viewer. **Tip** You can enable the Auditlog Viewer to automatically update the current log file every 5 seconds by checking the **Auto Refresh** check box.
Clear	Clears the display of the current log.
Filter	For auditapp logs, limits the logs displayed based on the UserID you select. For vos logs, limits the logs displayed based on the set of options (Address, Terminal, and Type) that you select. **Tip** You can display logs other than the set of options you selected by checking the **Filter Inverse** check box.
Clear Filter	Removes the filter that limits the type of logs that appear.
Find	Allows you to search for a particular string in the current log.
Save	Saves the currently selected log on your PC.

To make a column larger or smaller when viewing an auditlog message, drag the arrow that displays when your mouse hovers between two column headings.

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

Display AuditApp Logs

Procedure

Step 1 Choose **System** > **Tools** > **AuditLog Viewer**.

Step 2 From the Select a Node drop-down list, choose the server on which the logs that you want to view are stored.

Step 3 Double-click the **AuditApp Logs** folder.

Step 4 Click the **.log** file located outside the Archive folder to view the current logs. The AuditApp Logs for the selected node are displayed in a tabular form.

Note If you want see the old logs, double-click the **Archive** folder and click the corresponding file.

Step 5 Double-click the entry that you want to view. The auditlog message for that particular entry appears in a new window.

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

Display Cisco Unified OS Logs

Procedure

Step 1 Choose **System** > **Tools** > **AuditLog Viewer**

Step 2 From the **Select a Node** drop-down list, choose the node where the logs that you want to view are stored.

Step 3 Double-click the **Cisco Unified OS Logs** folder.

Step 4 Click the **vos-audit.log** file located outside the Archive folder to view the current logs. The Cisco Unified OS Logs for the selected node appear in a tabular form.

Note If you want see the old logs, double-click the **Archive** folder and click the corresponding file.

Step 5 Double-click the entry that you want to view. The Cisco Unified OS log message for that particular entry is displayed in a new window.

Tip You can filter the Cisco Unified OS log message display results by choosing the set of options in a pop up window that appears after you click **Filter**. To remove the filter, click **Clear Filter**. All logs appear after you clear the filter.

Display Messages in SysLog Viewer

You can display messages in SysLog Viewer.

Tip CiscoSyslog messages also display the syslog definition, which includes recommended actions, in an adjacent pane when you double-click the syslog message. You do not have to access the Alarm Definitions in Cisco Unified Serviceability for this information.

The following table describes the SysLog Viewer buttons.

Table 20: Syslog Viewer Buttons

Button	Function
Refresh	Updates the contents of the current log on the syslog viewer. **Tip** You can enable the syslog viewer to automatically update the syslog messages every 5 seconds by checking the Auto Refresh check box.
Clear	Clears the display of the current log.
Filter	Limits the messages that appear based on the set of options that you select.
Clear Filter	Removes the filter that limits the type of messages that appear.
Find	Allows you to search for a particular string in the current log.
Save	Saves the currently selected log on your PC.

When you view the syslog message, drag the arrow that appears when your mouse hovers between two column headings to make the column larger or smaller.

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

Procedure

Step 1 Choose **System** > **Tools** > **SysLog Viewer** > **Open SysLog Viewer**.

Step 2 From the **Select a Node** drop-down list box, choose the server where the logs that you want to view are stored.

Step 3 Click the tab for the logs that you want to view.

Step 4 After the log appears, double-click the log icon to list the filenames in the same window.

Tip If some syslog messages do not appear in the window, scrolling the mouse pointer over the missing syslog messages refreshes the display.

Step 5 To view the contents of the file at the bottom of the window, click the filename.

Step 6 Click the entry that you want to view.

To view the complete syslog message, double-click the syslog message. You can also use the buttons described in the SysLog Viewer Buttons table to view the syslog messages.

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

Plugins

Download and Install Application Plug-Ins

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

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

Procedure

Step 1 Choose **Application** > **CCO Voice Tools Download**.

The Login Prompt appears.

Step 2 Enter your Cisco.com username and password and click **OK**.

Step 3 Download the file to your PC.

Step 4 To begin the installation, double-click the download file.

Step 5 Follow the installation instructions.

Launch Application Plug-Ins

After downloading and installing the plug-in, you can access the application in the RTMT viewer.

Procedure

Under **System** > **Tools** > **Plugin**, choose the plug-in that you want to launch.

The application appears in the plugin window. See the application document for usage information.

APPENDIX A

Performance Counters and Alerts

System Counters

Cisco HAProxy

The HAProxy object offers proxy capabilities for HTTP-based applications. This object frontend all the incoming web traffic into Unified Communication Manager and IM and Presence Service.

HAProxy handles all the HTTP/HTTPS requests and provides improved Tomcat stability through offloading of crypto functionality.

The following table contains information about the HAProxy counters.

Table 21: Cisco HAProxy

Counters	Counter Description
TotalDeniedRequests	The total number of denied requests since the process started.
TotalDeniedResponse	The total number of denied responses since the process started.
Econ	The total number of failed connections to the server since the process st
TimeInQueue	The average time measured in milliseconds spent by the requests in the counter measure is averaged upto the last 1024 requests on the backend

Counters	Counter Description
TotalRequestAndResponseTime	The total time spent for processing the agent requests and response time. It the request time, no. of connections in the queue, their response, and the total p time. This counter measure is averaged upto the last 1024 requests on the b server.

Cisco Tomcat Connector

The Tomcat Hypertext Transport Protocol (HTTP) and HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors.

A Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when application web pages are accessed. The Secure Socket Layer (SSL) status of web application URLs provides the basis for the instance name for each Tomcat HTTP Connector. For example, `https://<IP Address>:8443` for SSL or `http://<IP Address>:8080` for non-SSL.

The following table contains information about the Tomcat HTTP connector counters.

Table 22: Cisco Tomcat Connector

Counters	Counter Description
Errors	The total number of HTTP errors (for example, `401 Unauthorized`) that the encountered.
MBytesReceived	The amount of data that the connector received.
MBytesSent	The amount of data that the connector sent.
Requests	The total number of request that the connector handled.
ThreadsTotal	The current total number of request processing threads, including available threads, for the connector.
ThreadsMax	The maximum number of request processing threads for the connector. Each incoming request on a web application window requires a thread for th of that request. If more simultaneous requests are received than the currently request processing threads can handle, additional threads are created up to the maximum shown in this counter. If still more simultaneous requests are rece accumulate within the server socket that the connector created, up to an int specified maximum number. Any further simultaneous requests receive co refused messages until resources are available to process them.
ThreadsBusy	This counter represents the current number of busy/in-use request processi for the connector.

Cisco Tomcat JVM

The Cisco Tomcat Java Virtual Machine (JVM) object provides information about the pool of common resource memory used by web applications such as Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unity Connection Administration. The dynamic memory block stores all objects that Tomcat and its web applications create.

The following table contains information about the Tomcat JVM counters.

Table 23: Tomcat JVM

Counters	Counter Description
KBytesMemoryFree	The amount of free dynamic memory block (heap memory) in the Tomca Machine. When the amount of free dynamic memory is low, more memory is aut allocated, and total memory size (represented by the KbytesMemoryTo increases but only up to the maximum (represented by the KbytesMemory You can determine the amount of memory in use by subtracting KBytes from KbytesMemoryTotal.
KBytesMemoryMax	The amount of free dynamic memory block (heap memory) in the Tomca Machine.
KBytesMemoryTotal	The current total dynamic memory block size, including free and in-use Tomcat Java Virtual Machine.

Cisco Tomcat Web Application

The Cisco Tomcat Web Application object provides information about how to run web applications.

The URLs for the web application provide the basis for the instance name for each Tomcat Web Application, as explained in the following examples:

- Cisco Unified Communications Manager Administration (`https://<IP Address>:8443/ccmadmin`) is identified by `ccmadmin`.
- Cisco Unified Serviceability (`https://<IP Address>:8443/ccmservice`) is identified by `ccmservice`.
- Cisco Unified Communications Manager User Options (`https://<IP Address>:8443/ccmuser`) is identified by `ccmuser`.
- Cisco Unity Connection Administration (`https://<IP Address>:8443/cuadmin`) is identified by `cuadmin`.
- URLs that do not have an extension, such as `https://<IP Address>:8443` or `http://<IP Address>:8080`), are identified by _root.

The following table contains information on the Tomcat Web Application counters.

Table 24: Tomcat Web Application

Counters	Counter Description
Errors	The total number of HTTP errors (for example, 401 Unauthorized) that a U Communications Manager-related or Cisco Unity Connection-related web a encounters.
Requests	The total number of requests that the web application handles. Each time th application is accessed, its Requests counter increments accordingly.
SessionsActive	The number of active or in use sessions in the web application.

Cisco UDS Tomcat Connector

The UDS Tomcat Hypertext Transport Protocol (HTTP) and HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors.

A UDS Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when application web pages are accessed. The Secure Socket Layer (SSL) status of web application URLs provides the basis for the instance name for each UDS Tomcat HTTP Connector. For example, `https://<IP Address>:8443` for SSL or `http://<IP Address>:8080` for non-SSL.

The following table contains information about the UDS Tomcat HTTP connector counters.

Table 25: Cisco UDS Tomcat Connector

Counters	Counter Description
Errors	The total number of HTTP errors (for example, `401 Unauthorized`) that the encountered.
MBytesReceived	The amount of data that the connector received.
MBytesSent	The amount of data that the connector sent.
Requests	The total number of request that the connector handled.
ThreadsBusy	This counter represents the current number of busy/in-use request processi for the connector.
ThreadsTotal	The current total number of request processing threads, including available threads, for the connector.

Counters	Counter Description
ThreadsMax	The maximum number of request processing threads for the connector. Each incoming request on a web application window requires a thread fo of that request. If more simultaneous requests are received than the curre request processing threads can handle, additional threads are created up to t maximum shown in this counter. If still more simultaneous requests are r accumulate within the server socket that the connector created, up to an specified maximum number. Any further simultaneous requests receive refused messages until resources are available to process them.

Cisco UDS Tomcat JVM

The Cisco UDS Tomcat Java Virtual Machine (JVM) object provides information about the UDS Tomcat JVM, which represents, among common things, a pool of common resource memory used by Cisco Unified Communications Manager-related web applications such as UDS, tomcatstats, and more.

The following table contains information about the UDS Tomcat JVM counters.

Table 26: Cisco UDS Tomcat JVM

Counters	Counter Description
KBytesMemoryFree	The amount of free dynamic memory block (heap memory) in the UDS Virtual Machine. When the amount of free dynamic memory is low, more memory is aut allocated, and total memory size (represented by the KbytesMemoryTo increases but only up to the maximum (represented by the KbytesMemory You can determine the amount of memory in use by subtracting KBytes from KbytesMemoryTotal.
KBytesMemoryMax	The amount of free dynamic memory block (heap memory) in the UDS Virtual Machine.
KBytesMemoryTotal	The current total dynamic memory block size, including free and in-use UDS Tomcat Java Virtual Machine.

Cisco UDS Tomcat Web Application

The Cisco UDS Tomcat Web Application object provides information about how to run Unified Communications Manager web applications.

The URLs for the web application provide the basis for the instance name for each Tomcat Web Application, as explained in the following examples:

- Cisco Unified Communications Manager Administration (`https://<IP Address>:8443/ccmadmin`) is identified by `ccmadmin`.
- Cisco Unified Serviceability (`https://<IP Address>:8443/ccmservice`) is identified by `ccmservice`.

- Cisco Unified Communications Manager User Options (`https://<IP Address>:8443/ccmuser`) is identified by `ccmuser`.
- Cisco Unity Connection Administration (`https://<IP Address>:8443/cuadmin`) is identified by `cuadmin`.
- URLs that do not have an extension, such as `https://<IP Address>:8443` or `http://<IP Address>:8080`), are identified by _root.

The following table contains information on the UDS Tomcat Web Application counters.

Table 27: Cisco UDS Tomcat Web Application

Counters	Counter Description
Errors	The total number of HTTP errors (for example, 401 Unauthorized) that a U Communications Manager-related or Cisco Unity Connection-related web a encounters.
Requests	The total number of requests that the web application handles. Each time th application is accessed, its Requests counter increments accordingly.
SessionsActive	The number of active or in use sessions in the web application.

Database Change Notification Client

The Database Change Notification Client object provides information about change notification clients. The following table contains information about the Database Change Notification Client counters.

Table 28: Database Change Notification Client

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

Counters	Counter Descriptions
TablesSubscribed	The number of tables in which this client has subscribed.

Database Change Notification Server

The Database Change Notification Server object provides information about different change-notification-related statistics. The following table contains information about the Database Change Notification Server counters.

Table 29: Database Change Notification Server

Counter	Counter Descriptions
Clients	The number of change notification clients (services and servlets) that ha for change notification.
CNProcessed	The total number of change notification messages processed by the serve
Queue Delay	The number of seconds that the change notification process has messag but is not processing them. This condition is true if: • either Change Notification Requests Queued in Database (QueuedR and Change Notification Requests Queued in Memory (QueuedRequestsInMemory) are non-zero, or • the Latest Change Notification Messages Processed count is not ch This condition is checked every 15 seconds.
QueuedRequestsInDB	The number of change notification records that are in the DBCNQueue Change Notification Queue) table through direct TCP/IP connection (no shared memory). This counter refreshes every 15 seconds.
QueuedRequestsInMemory	The number of change notification requests that are queued in shared m

Database Change Notification Subscription

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

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

Database Local DSN

The Database Local Data Source Name (DSN) object and LocalDSN counter provide the DSN information for the local machine. The following table contains information on the Database local DSN.

Table 30: Database Local Data Source Name

Counters	Counter Descriptions
CcmDbSpace_Used	The amount of Ccm DbSpace that is consumed
CcmtempDbSpace_Used	The amount of Ccmtemp DbSpace that is consumed.
CNDbSpace_Used	The percentage of CN DbSpace that is consumed.
LocalDSN	The DSN that is being referenced from the local machine.
SharedMemory_Free	The total shared memory that is free.
SharedMemory_Used	The total shared memory that is used.
RootDbSpace_Used	The amount of RootDbSpace that is consumed.

DB User Host Information Counters

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

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

Enterprise Replication DBSpace Monitors

The enterprise replication DBSpace monitors object displays the usage of various ER DbSpaces. The following table contains information about the enterprise replication DB monitors.

Table 31: Enterprise Replication DBSpace Monitors

Counters	Counter Descriptions
ERDbSpace_Used	The amount of enterprise replication DbSpace that was consumed.
ERSBDbSpace_Used	The amount of ERDbSpace that was consumed.

Enterprise Replication Perfmon Counters

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

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

IP

The IP object provides information on the IPv4-related statistics on your system. The following table contains information about the IP counters.

Note These counters are also part of the IP6 object, which supports Unified Communications Manager and provides information about the IPv6-related statistics on your system.

Table 32: IP Counters

Counters	Counter Descriptions
Frag Creates	The number of IP datagrams fragments that are generated at this entity.
Frag Fails	The number of IP datagrams that are discarded at this entity because th cannot be fragmented, such as datagrams where the Do not Fragment fl
Frag OKs	The number of IP datagrams that are successfully fragmented at this en
In Delivers	The number of input datagrams that are delivered to IP user protocols. T includes Internet Control Message Protocol (ICMP).
In Discards	The number of input IP datagrams where no issues are encountered, bu discarded. One possible reason is a lack of buffer space. This counter do any datagrams that are discarded while awaiting reassembly.
In HdrErrors	The number of input datagrams that are discarded with header errors. T includes bad checksums, version number mismatch, other format errors exceeded, and other errors that are discovered in processing their IP opt
In Receives	The number of input datagrams that are received from all network inter counter includes datagrams that were received with errors
In UnknownProtos	The number of locally addressed datagrams that are received successfully because of an unknown or unsupported protocol.
InOut Requests	The number of incoming IP datagrams that are received and the numbe IP datagrams that are sent.
Out Discards	The number of output IP datagrams that are not transmitted and are disc possible reason is a lack of buffer space.
Out Requests	This counter represents the total number of IP datagrams that local IP u (including ICMP) supply to IP in requests transmission. This counter do any datagrams that were counted in ForwDatagrams.
Reasm Fails	The number of IP reassembly failures that the IP reassembly algorithm including time outs and errors. This counter does not represent the discarded IP fragments because som such as the algorithm in RFC 815, can lose track of the number of fragn these algorithms combine fragments as they are received.
Reasm OKs	The number of IP datagrams that are successfully reassembled.

Counters	Counter Descriptions
Reasm Reqds	The number of IP fragments that are received that require reassembly at thi

Memory

The memory object provides information about the usage of physical memory and swap memory on the server. The following table contains information about memory counters.

Table 33: Memory

Counters	Counter Descriptions
% Mem Used	Displays the system physical memory utilization as a percentage. The valu counter is calculated as follows: `Total KBytes - Free KBytes - Buffers KBytes - Cached + Shared KBytes) / Total KBytes` This value also corresponds to the Used KBytes/Total KBytes
% Page Usage	The percentage of active pages.
% VM Used	Displays the system virtual memory utilization as a percentage. The value counter is calculated as follows: `Total KBytes - Free KBytes - Buffers KBytes - Cached + Shared KBytes + Used Swap KBytes) / (Total KBytes Swap KBytes)` This value also corresponds to Used VM KBytes/Total VM KBytes.
Buffers KBytes	The capacity of buffers in your system in kilobytes.
Cached KBytes	The amount of cached memory in kilobytes.
Free KBytes	The total amount of memory that is available in your system in kilobytes.
Free Swap KBytes	The amount of free swap space that is available in your system in kilobytes
HighFree	The amount of free memory in the high region. The Linux kernel splits the virtual memory address space into memory regi high memory is memory above a certain physical address, and its amount d the total memory and the type of kernel on the system. For the Unified Communications Manager system with 4 GB memory, the hig is roughly in the address of 896M to 4096M.

Counters	Counter Descriptions
HighTotal	The total amount of memory in the high region. The Linux kernel splits the virtual memory address space into memory high memory is memory above a certain physical address, and its amou the total memory and the type of kernel on the system. For the Unified Communications Manager system with 4 GB memory, the is roughly in the address of 896M to 4096M.
Page Faults Per Sec	The number of page faults (both major and minor) that the system mak (post 2.5 kernels only). This reading does not necessarily represent a co faults that generate input and output (I/O) because some page faults ca without I/O.
Low Total	The total low (non-paged) memory for kernel.
Low Free	The total free low (non-paged) memory for kernel.
Page Major Faults Per Sec	The number of major faults that the system makes per second that requ page from the disk (post 2.5 kernels only).
Pages	The number of pages that the system pages in from the disk, plus the nu that the system pages out to the disk.
Pages Input	The number of pages that the system pages in from the disk.
Pages Input Per Sec	The total number of kilobytes that the system pages in from the disk pe
Pages Output	The number of pages that the system pages out to the disk.
Pages Output Per Sec	The total number of kilobytes that the system pages out to the disk per
Shared KBytes	The amount of shared memory in your system in kilobytes.
SlabCache	The memory used by created slabcaches by various kernel components macroscopic counter representing the sum of all the individual entries i slabinfo.
SwapCached	The amount of Swap used as cache memory. Memory that once was sw swapped back in, but is still in the swapfile.
Total KBytes	The total amount of memory in your system in kilobytes.
Total Swap KBytes	The total amount of swap space in your system in kilobytes.
Total VM KBytes	The total amount of system physical and memory and swap space (Tota Total Swap Kbytes) that is in use in your system in kilobytes.

Counters	Counter Descriptions
Used KBytes	The amount of in-use physical memory. The value of the Used KBytes cou calculated as follows: `Total KBytes - Free KBytes - Buffers KBytes - Cached + Shared KBytes.` The Used KBytes value differs from the Linux term that displays in the top command output. The Used value that displays in the top or free command equals the difference in Total KBytes - Free KBytes and also includes the s Buffers KBytes and Cached KBytes.
Used Swap KBytes	This counter represents the amount of swap space that is in use on your sys kilobytes.
Used VM KBytes	This counter represents the system physical memory and the amount of swa that is in use on your system in kilobytes. The value is calculated as follow `Total KBytes - Free KBytes - Buffers KBytes - Cached + Shared KBytes + Used Swap KBytes` This value corresponds to Used Mem KBytes + Used Swap KBytes.

Network Interface

The network interface object provides information about the network interfaces on the system. The following table contains information about network interface counters.

Table 34: Network Interface

Counters	Counter Descriptions
Rx Bytes	The number of bytes, including framing characters, that are received on this
Rx Dropped	The number of inbound packets that are chosen to be discarded even though have been detected. This action prevents the packet from being delivered to higher-layer protocol. Discarding packets also frees up buffer space.
Rx Errors	The number of inbound packets (packet-oriented interfaces) and the number o transmission units (character-oriented or fixed-length interfaces) that conta that prevented them from being delivered to a higher-layer protocol.
Rx Multicast	The number of multicast packets that are received on this interface.
Rx Packets	The number of packets that this sublayer delivered to a higher sublayer. Thi does not include the packets that are addressed to a multicast or broadcast a this sublayer.
Total Bytes	The total number of received (Rx) bytes and transmitted (Tx) bytes.
Total Packets	The total number of Rx packets and Tx packets.

Counters	Counter Descriptions
Tx Bytes	The total number of octets, including framing characters, that are transm the interface.
Tx Dropped	The number of outbound packets that are chosen to be discarded even tho are detected. This action prevents the packet from being delivered to a h protocol. Discarding a packet also frees up buffer space.
Tx Errors	The number of outbound packets (packet-oriented interfaces) and the nu outbound transmission units (character-oriented or fixed-length interfac transmitted because of errors.
Tx Packets	The total number of packets that the higher-level protocols requested for including those that are discarded or not sent. This situation does not in that are addressed to a multicast or broadcast address at this sublayer.
Tx QueueLen	The length of the output packet queue (in packets).

Number of Replicates Created and State of Replication

The Number of Replicates Created and State of Replication object provides real-time replication information for the system. The following table contains information about replication counters.

Table 35: Number of Replicates Created and State of Replication

Counters	Counter Descriptions
Number of Replicates Created	The number of replicates that are created by Informix for the DB tables displays information during Replication Setup.
Replicate_State	The state of replication. The following list provides possible values: **0** Initializing. The counter equals 0 when the server is not defined or w is defined but realizes the template has not completed. **1** Replication setup script fired from this node. Cisco recommends tha **dbreplication status** on the CLI to determine the location and caus **2** Good Replication. **3** Bad Replication. A counter value of 3 indicates replication in the c It does not mean that replication failed on a particular server in the recommends that you run **utils dbreplication status** on the CLI the location and cause of the failure. **4** Replication setup did not succeed.

Partition

The partition object provides information about the file system and its usage in the system. The following table contains information about partition counters. These counters are also available for the spare partition, if present.

Table 36: Partition

Counters	Counter Descriptions
% CPU Time	The percentage of CPU time that is dedicated to handling IO requests that w to the disk.
% Used	The percentage of disk space that is in use on this file system.
% Wait in Read	Not Used. The Await Read Time counter replaces this counter. This counte longer valid with the counter value -1.
% Wait in Write	Not Used. The Await Write Time counter replaces this counter. This counte longer valid with the counter value -1.
Await Read Time	The average time measured in milliseconds for read requests that are issued device to be served.
Await Time	The average time measured in milliseconds for input and output (I/O) reques issued to the device to be served. This reading includes the time spent by th in queue and the time spent servicing them.
Await Write Time	The average time measured in milliseconds for write requests that are issue device to be served.
Queue Length	The average queue length for the requests that are issued to the disk.
Read Bytes Per Sec	The amount of data in bytes per second that is read from the disk.
Total Mbytes	The amount of total disk space in megabytes that is on this file system.
Used Mbytes	The amount of disk space in megabytes that is in use on this file system.
Write Bytes Per Sec	The amount of data that is written to the disk in bytes per second.

Process

The process object provides information about the processes that are running on the system. The following table contains information about process counters.

Table 37: Process

Counters	Counter Descriptions
% CPU Time	This counter, which is expressed as a percentage of total central processing u time, represents the tasks share of the elapsed CPU time since the last upda

Counters	Counter Descriptions
% MemoryUsage	This counter represents the percentage of physical memory that a task i using.
Data Stack Size	This counter represents the stack size for task memory status.
Nice	This counter represents the nice value of the task. • A negative nice value indicates that the process has a higher priori • A positive nice value indicates that the process has a lower priority **Note** If the nice value equals zero, do not adjust the priority whe determining the dispatchability of a task.
Page Fault Count	This counter represents the number of major page faults that a task enc requires the data to be loaded into memory.
PID	This counter displays the task-unique process ID. The ID periodically v value never equals zero.
Process Status	This counter displays the process status: **0** Running **1** Sleeping **2** Uninterruptible disk sleep **3** Zombie **4** Stopped **5** Paging **6** Unknown
Shared Memory Size	This counter displays the amount of shared memory in kilobytes (KB) t using. Other processes could potentially share the same memory.
STime	This counter displays the system time (STime), measured in jiffies, that has scheduled in kernel mode. A jiffy corresponds to a unit of CPU tim as a base of measurement. One second comprises 100 jiffies.

Counters	Counter Descriptions
Thread Count	This counter displays the number of threads that are currently grouped wit negative value (-1) indicates that this counter is currently not available. Thi happens when thread statistics (which include all performance counters in t object as well as the Thread Count counter in the Process object) are turned o the system total processes and threads exceed the default threshold value.
Total CPU Time Used	This counter displays the total CPU time in jiffies that the task used in user kernel mode since the task started.
UTime	This counter displays the time, measured in jiffies, that a task has schedule mode.
VmData	This counter displays the virtual memory usage of the heap for the task in
VmRSS	This counter displays the virtual memory (Vm) resident set size (RSS) that i in physical memory in KB. This reading includes the code, data, and stack.
VmSize	This counter displays the total virtual memory usage for a task in KB. This includes all code, data, shared libraries, and pages that have been swapped Virtual Image = swapped size + resident size
Wchan	This counter displays the channel (system call) in which the process is wai

Processor

The processor object provides information about different processor time usage in percentages. The following table contains information about processor counters.

Table 38: Processor

Counters	Counter Descriptions
% CPU Time	This counter displays the processors share of the elapsed central processing time, excluding idle time, since the last update. This share is expressed as a of total CPU time.
Idle Percentage	This counter displays the percentage of time that the processor is in the idl does not have an outstanding disk input and output (I/O) request.
IOwait Percentage	This counter represents the percentage of time that the processor is in the i while the system had an outstanding disk I/O request.
Irq Percentage	This counter represents the percentage of time that the processor spends ex interrupt request that is assigned to devices, including the time that the proces sending a signal to the computer.
Nice Percentage	This counter displays the percentage of time that the processor spends execu user level with nice priority.

Counters	Counter Descriptions
Softirq Percentage	This counter represents the percentage of time that the processor spends soft IRQ and deferring task switching to get better CPU performance.
System Percentage	This counter displays the percentage of time that the processor is execut at the system (kernel) level.
User Percentage	This counter displays the percentage of time that the processor is execu processes at the user (application) level.

System

The System object provides information about file descriptors on your system.

The following table contains information about system counters.

Table 39: System

Counters	Counter Descriptions
Allocated FDs	The number of allocated file descriptors.
Being Used FDs	The number of file descriptors that are currently in use in the system.
Freed FDs	The number of allocated file descriptors on the system that are freed.
IOPerSecond	The number of input and output (I/O) operations on all disk partitions p this server. If you experience a system performance issue, use the infor counter to measure the impact of the aggregate I/O operations on this se
IOReadReqMergedPerSecond	The number of read requests merged per second that are queued to all d server.
IOWriteReqMergedPerSecond	The number of write requests merged per second that are queued to all d server.
IOReadReqPerSecond	The number of read requests per second that are issued to all devices or
IOWriteReqPerSecond	The number of write requests per second that are issued to all devices o
IOSectorsReadPerSecond	The number of sectors read per second from all devices on this server.
IOSectorsWrittenPerSecond	The number of sectors written per second to all devices on this server.
IOKBytesReadPerSecond	The number of KBytes read per second from all devices on this server.
IOKBytesWrittenPerSecond	The number of KBytes written per second to all devices on this server.
IOSectorsReqSizeAvg	The average size in sectors of the requests that are issued to all devices
IOReqQueueSizeAvg	The average queue length of the requests that are issued to all devices o

Counters	Counter Descriptions
IOAwait	The average time in milliseconds for I/O requests that are issued to all devi served. This reading includes the time spent by the requests in queue and th spent servicing the requests.
IOServiceTime	The average service time in milliseconds for I/O requests that are issued to a on this server.
IOCpuUtil	The percentage of CPU time during which I/O requests are issued to the de (bandwidth utilization for the device) on this server.
Max FDs	The maximum number of file descriptors that are allowed on the system.
Total CPU Time	The total time in jiffies that the system has been up and running.
Total Processes	The number of processes on the system.
Total Threads	The number of threads on the system.

TCP

The TCP object provides information on the TCP statistics on your system.

The following table contains information about the TCP counters.

Table 40: TCP

Counters	Counter Description
Active Opens	This counter displays the number of times that the TCP connections make a transition to the SYN-SENT state from the CLOSED state.
Attempt Fails	This counter displays the number of times that the TCP connections make a transition to the CLOSED state from either the SYN-RCVD state or the SY state. The counter also displays the number of times TCP connections mak transition to the LISTEN state from the SYS-RCVD state.
Curr Estab	This counter displays the number of TCP connections with a current state o ESTABLISHED or CLOSE- WAIT.
Estab Resets	This counter displays the number of times that the TCP connections make a transition to the CLOSED state from the ESTABLISHED state or the CLO state.
In Segs	This counter displays the total number of segments that are received, incluc that are received in error. This count only includes segments that are receiv currently established connections.
InOut Segs	This counter displays the total number of segments that are sent and the tot of segments that are received.

Counters	Counter Description
Out Segs	This counter displays the total number of segments that are sent. This c includes segments that are sent on currently established connections, bu retransmitted octets.
Passive Opens	This counter displays the number of times that TCP connections make a di to the SYN-RCVD state from the LISTEN state.
RetransSegs	This counter displays the total number of segments that are retransmitte segment contains one or more previously transmitted octets.

Thread

The Thread object provides a list of running threads on your system.

The following table contains information about the Thread counters.

Table 41: Thread

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

AXL Web Service

The AXL Web Service object provides information about the AXL Web Service running on your system. The following table contains information about the AXL Web Service counters.

Table 42: AXL Web Service

Counters	Counter Description
ThrottleCount	This counter represents the number of times Administrati restart of the Cisco AXL Web Service. Throttling occurs to process.
ThrottleState	This counter represents whether Administrative XML La value of 1 in this counter indicates that throttling is curre a write request to Unified Communications Manager thro continue to be allowed and processed while AXL throttlin at this time and all read and write requests will be proces

Ramfs

The Ramfs object provides information about the ram file system. The following table contains information on the Ramfs counters.

Table 43: Ramfs

Counters	Counter Description
FilesTotal	This counter represents the total number of files in the ram-based file syste
SpaceFree	This counter represents the amount of free data blocks in the ram-based file data storage for a filesystem. The block size specifies the size that the file s Communications Manager system, the block size is 4096 bytes.
SpaceUsed	This counter represents the amount of used data blocks in the ram-based fil data storage for a file system. The block size specifies the size that the file Communications Manager system, the block size is 4096 bytes.

Voice and Video Counters

Cisco Analog Access

The Cisco Analog Access object provides information about registered Cisco Analog Access gateways. The following table contains information about CiscoAnalog Access counters.

Table 44: Cisco Analog Access

Counters	Counter Description
OutboundBusyAttempts	This counter represents the total number of times that Unified Communication attempts a call through the analog access gateway when all ports were busy
PortsActive	This counter represents the number of ports that are currently in use (active appears active when a call is in progress on that port.
PortsOutOfService	This counter represents the number of ports that are currently out of service applies only to loop-start and ground-start trunks.

Cisco Annunciator Device

The Cisco Annunciator Device object provides information about registered Cisco annunciator devices. The following table contains information about CiscoAnnunciator counters.

Table 45: Cisco Annunciator Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that Unified Communication attempted to allocate an annunciator resource from an annunciator device a for example, because all resources were already in use.
ResourceActive	This counter represents the total number of annunciator resources that are c active (in use) for an annunciator device.

Counters	Counter Description
ResourceAvailable	This counter represents the total number of resources that are not active available to be used at the current time for the annunciator device.
ResourceTotal	This counter represents the total number of annunciator resources that a for an annunciator device.

Cisco Call Restriction

The Cisco Call Restriction object provides information about the number of failures that result due to logical partitioning policy restrictions. The following table contains information about Cisco Call Restriction counters.

Table 46: Cisco Call Restriction

Counters	Counter Description
AdHocConferenceFailures	This counter represents the number of attempts that failed to add a parti Ad Hoc Conference because the call path between the geolocation of th already in conference and the device being invited to the conference wa due to a logical partition policy.
BasicCallFailures	This counter represents the number of basic calls that have failed becau partition policy restrictions between the geolocations of the called and c A basic call is any call that does not utilize supplementary services such forward, and so on.
ForwardingFailures	This counter represents the number of attempts to forward an incoming failed because of a logical partition policy restriction between the geolo two parties involved.
LogicalPartitionFailuresTotal	This counter represents the total number of call attempts that have failed restriction of calls between geolocations of the calling and called parties. the number of failures for Transfer, AdHoc Conference, Meet-Me Confer Call Park, Shared Lines and Basic Calls.
MeetMeConferenceFailures	This counter represents the number of attempts that failed to add a parti Meet-Me conference because the call path between the geolocation of t already in conference and the device attempting to join the conference due to a logical partition policy.
MidCallFailures	This counter represents the number of calls that have failed because of a between the geolocations of the called or connected parties after the ini check.
ParkRetrievalFailures	This counter represents the number of attempts to perform a Call Park c failed because the device that was attempting to retrieve the call had a lo policy restriction with the geolocation of the parked party.
PickUpFailures	This counter represents the number of attempts to perform a PickUp op failed because the device on which the pickup was being attempted had partition policy restriction with the geolocation of the calling device.

Counters	Counter Description
SharedLineFailures	This counter represents the number of attempts to use a shared line which faile the caller or callee has a logical partition policy restriction with the geoloca devices having the shared lines.
TransferFailures	This counter represents the number of call transfer attempts that failed due to of calls between the geolocation of the transferred party and the transferred d

Cisco CallManager

The CiscoCallManager object provides information about calls, applications, and devices that are registered with the Unified Communications Manager. The following table contains information about CiscoCallManager counters.

Table 47: CiscoCallManager

Counters	Counter Description
AnnunciatorOutOfResources	This counter represents the total number of times that Unified Communica Manager attempted to allocate an annunciator resource from those that are to a Unified Communications Manager when none were available.
AnnunciatorResourceActive	This counter represents the total number of annunciator resources that are in use on all annunciator devices that are registered with a Unified Commu Manager.
AnnunciatorResourceAvailable	This counter represents the total number of annunciator resources that are and are currently available.
AnnunciatorResourceTotal	This counter represents the total number of annunciator resources that are by all annunciator devices that are currently registered with Unified Comm Manager.
AuthenticatedCallsActive	This counter represents the number of authenticated calls that are currently use) on Unified Communications Manager. An authenticated call designat which all the endpoints that are participating in the call are authenticated. authenticated phone uses the Transport Layer Security (TLS) authenticate protocol signaling with Unified Communications Manager.
AuthenticatedCallsCompleted	This counter represents the number of authenticated calls that connected a subsequently disconnected through Unified Communications Manager. An authenticated call designates one in which all the endpoints that are partici the call are authenticated. An authenticated phone uses the TLS authentica protocol signaling with Unified Communications Manager.
AuthenticatedPartiallyRegisteredPhone	This counter represents the number of partially registered, authenticated S
AuthenticatedRegisteredPhones	This counter represents the total number of authenticated phones that are r to Unified Communications Manager. An authenticated phone uses the TL authenticated Skinny protocol signaling with Unified Communications Ma

Counters	Counter Description
BRIChannelsActive	This counter represents the number of BRI voice channels that are curr active call on this Unified Communications Manager.
BRISpansInService	This counter represents the number of BRI spans that are currently ava
CallManagerHeartBeat	This counter represents the heartbeat of Unified Communications Man incremental count indicates that Unified Communications Manager is up If the count does not increment, that indicates that Unified Communicat is down.
CallsActive	This counter represents the number of voice or video streaming connec currently in use (active); in other words, the number of calls that actuall path that is connected on Unified Communications Manager.
CallsAttempted	This counter represents the total number of attempted calls. An attempt anytime that a phone goes off hook and back on hook, regardless of whe were dialed, or whether it connected to a destination. The system consi attempts during feature operations (such as transfer and conference) to calls.
CallsCompleted	This counter represents the number of calls that were actually connecte or video stream was established) through Unified Communications Ma number increases when the call terminates.
CallsInProgress	This counter represents the number of voice or video calls that are curren on Unified Communications Manager, including all active calls. When a phone that is registered with Skinny Client Control Protocol (S hook, the CallsInProgress progress counter increments. until it goes ba For Cisco Unified IP Phones 7940, and 7960 that register with SIP, the C counter increments when the dial softkey is pressed. For all other phones that are running SIP, the CallsInProgress counter i when the first digit is pressed. When all voice or video calls that are in progress are connected, the nu CallsInProgress represents the number of CallsActive. The counter dec when a phone goes back on hook.
CM_MediaTermPointsRequestsThrottled	This counter represents the total number of media termination point (M requests that have been denied due to throttling (a resource from this M allocated because, as specified by the Cisco CallManager service para and Transcoder Resource Throttling Percentage, the MTP was being ut the configured throttle percentage). This counter increments each time an MTP on this Unified Communications Manager node is requested a to MTP throttling and reflects a running total since the start of the Cisco Service.

Counters	Counter Description
CM_TranscoderRequestsThrottled	This counter represents the total number of transcoder resource requests th been denied due to throttling (a resource from this transcoder was not allocate as specified by the Cisco CallManager service parameter MTP and Transc Resource Throttling Percentage, the transcoder was being utilized beyond configured throttle percentage). This counter increments each time a reque transcoder on this Unified Communications Manager node is requested an due to transcoder throttling and reflects a running total since the start of th CallManager Service.
EncryptedCallsActive	This counter represents the number of encrypted calls that are currently acti on this Unified Communications Manager. An encrypted call represents on all the endpoints that are participating in the call are encrypted.
EncryptedCallsCompleted	This counter represents the number of encrypted calls that were connected subsequently disconnected through this Unified Communications Manage encrypted call represents one in which all the endpoints that are participati call are encrypted.
EncryptedPartiallyRegisteredPhones	This counter represents the number of partially registered, encrypted SIP p
EncryptedRegisteredPhones	This counter represents the total number of encrypted phones that are regis this Unified Communications Manager.
FXOPortsActive	This counter represents the number of FXO ports that are currently in use (a Unified Communications Manager.
FXOPortsInService	This counter represents the number of FXO ports that are currently availab in the system.
FXSPortsActive	This counter represents the number of FXS ports that are currently in use (a Unified Communications Manager.
FXSPortsInService	This counter represents the number of FXS ports that are currently availab in the system.
HuntListsInService	This counter represents the number of hunt lists that are currently in service Communications Manager.
HWConferenceActive	This counter represents the total number of hardware conference resources provided by all hardware conference bridge devices that are currently regis Unified Communications Manager.
HWConferenceCompleted	This counter represents the total number of conferences that used a hardware bridge (hardware-based conference devices such as Cisco Catalyst 6000, Cisc 4000, Cisco VG200, Cisco series 26xx and 36xx) that is allocated from U Communications Manager and that have completed, which means that the c bridge has been allocated and released. A conference activates when the fi connects to the bridge. The conference completes when the last call discon the bridge.

Counters	Counter Description
HWConferenceOutOfResources	This counter represents the total number of times that Unified Commu Manager attempted to allocate a hardware conference resource from th registered to a Unified Communications Manager when none was avai
HWConferenceResourceActive	This counter represents the total number of conference resources that ar hardware conference devices (such as Cisco Catalyst 6000, Catalyst 40 VG200, Cisco series 26xx and 36xx) that are registered with Unified Co Manager. System considers conference to be active when one or more connected to a bridge.
HWConferenceResourceAvailable	This counter represents the number of hardware conference resources t use and that are available to be allocated on all hardware conference de Cisco Catalyst 6000, Cisco Catalyst 4000, Cisco VG200, Cisco series 2 that are allocated from Unified Communications Manager and that hav completed, which means that the conference bridge has been allocated A conference activates when the first call connects to the bridge. The c completes when the last call disconnects from the bridge.
HWConferenceResourceTotal	This counter represents the number of active conferences on all hardwa devices that are registered with Unified Communications Manager.
InitializationState	This counter represents the current initialization state of Unified Comm Manager. Unified Communications Manager includes the following initi values: 1-Database, 2-Regions, 3-Locations, 4-QoS Policy, 5-Time Of Day, 6- Neighborhoods, 7-Digit Analysis, 8-Route Plan, 9-Call Control, 10-RS Manager, 11-Supplementary Services, 12-Directory, 13-SDL Link, 14- 100-Initialization Complete. Not all states display when this counter is used. This display does not i error occurred; this display simply indicates that the states initialized a within the refresh period of the performance monitor.
IVRResourceActive	This represents the total number of IVR resources that are currently in devices registered with Unified Communications Manager.
IVROutOfResources	This represents the total number of times Unified Communications Mana to allocate an IVR resource from those that are registered to Unified Co Manager when none were available.
IVRResourceAvailable	This represents the total number of IVR resources provided by all IVR are currently registered with Unified Communications Manager.
IVRResourceTotal	This represents the total number of IVR resources provided by all IVR are currently registered with Unified Communications Manager.
LocationOutOfResources	This counter represents the total number of times that a call through Lo due to the lack of bandwidth.

Counters	Counter Description
MCUConferencesActive	This counter represents the total number of active conferences on all Cisc TelePresence MCU conference bridge devices that are registered with Uni Communications Manager.
MCUConferencesCompleted	This counter represents the total number of conferences that used a Cisco Tel MCU conference bridge allocated from Unified Communications Manage completed, implying that the conference bridge was allocated and released conference is activated when the first call is connected to the bridge. The c is completed when the last call is disconnected from the bridge.
MCUHttpConnectionErrors	This counter represents the total number of times Unified Communications attempted to create HTTP connections to Cisco TelePresence MCU confere device, and failed due to connection errors on the Cisco TelePresence MCU c bridge side.
MCUHttpNon200OKResponse	This counter represents the total number of times Unified Communications received a non 200 OK HTTP Response from Cisco TelePresence MCU co bridge, for any HTTP query sent.
MCUOutOfResources	This counter represents the total number of times Unified Communications attempted to allocate a conference resource from Cisco TelePresence MCU c bridge device and failed. For example, the attempt to allocate a conference fails, if all the resources are already in use.
MOHMulticastResourceActive	This counter represents the total number of multicast Music On Hold (MOH) that are currently in use (active) on all MOH servers that are registered with Communications Manager.
MOHMulticastResourceAvailable	This counter represents the total number of active multicast MOH connect are not being used on all MOH servers that are registered with a Unified Communications Manager.
MOHOutOfResources	This counter represents the total number of times that the Media Resource attempted to allocate an MOH resource when all available resources on all servers that are registered with a Unified Communications Manager were a active.
MOHTotalMulticastResources	This counter represents the total number of multicast MOH resources or co that are provided by all MOH servers that are currently registered with a U Communications Manager.
MOHTotalUnicastResources	This counter represents the total number of unicast MOH resources or stre are provided by all MOH servers that are currently registered with Unified Communications Manager. Each MOH unicast resource uses one stream.
MOHUnicastResourceActive	This counter represents the total number of unicast MOH resources that are in use (active) on all MOH servers that are registered with Unified Commu Manager. Each MOH unicast resource uses one stream.

Counters	Counter Description
MOHUnicastResourceAvailable	This counter represents the total number of unicast MOH resources tha available on all MOH servers that are registered with Unified Commun Manager. Each MOH unicast resource uses one stream.
MTPOutOfResources	This counter represents the total number of times that Unified Commu Manager attempted but failed to allocate a media termination point (M from one MTP device that is registered with Unified Communications also means that no transcoders were available to act as MTPs.
MTPResourceActive	This counter represents the total number of MTP resources that are cu (active) on all MTP devices that are registered with a Unified Commun Manager. Each MTP resource uses two streams. An MTP in use repres resource that has been allocated for use in a call.
MTPResourceAvailable	This counter represents the total number of MTP resources that are not available to be allocated on all MTP devices that are registered with U Communications Manager. Each MTP resource uses two streams. An represents one MTP resource that has been allocated for use in a call.
MTPResourceTotal	This counter represents the total number of MTP resources that are pro MTP devices that are currently registered with Unified Communicatio
MTP_RequestsThrottled	This counter represents the total number of MTP resource requests tha denied due to throttling (a resource from this MTP was not allocated b specified by the Cisco CallManager service parameter MTP and Transc Throttling Percentage, the MTP was being utilized beyond the configu percentage). This counter increments each time a resource is requested and is denied due to throttling. This counter reflects a running total sin device registered with the Cisco CallManager Service.
PartiallyRegisteredPhone	This counter represents the number of partially registered phones that ar
PRIChannelsActive	This counter represents the number of PRI voice channels that are in an a Unified Communications Manager.
PRISpansInService	This counter represents the number of PRI spans that are currently ava
RegisteredAnalogAccess	This counter represents the number of registered Cisco analog access g are registered with system. The count does not include the number of access ports.
RegisteredHardwarePhones	This counter represents the number of Cisco hardware IP phones (for e Unified IP Phones 7960, 7940, and so on.) that are currently registered
RegisteredMGCPGateway	This counter represents the number of MGCP gateways that are curren in the system.
RegisteredOtherStationDevices	This counter represents the number of station devices other than Cisco phones that are currently registered in the system (for example, Cisco CTI port, CTI route point, Cisco voicemail port).

Counters	Counter Description
SIPLineServerAuthorizationChallenges	This counter represents the number of authentication challenges for incom requests that the Unified Communications Manager server issued to phone running SIP. An authentication challenge occurs when a phone that is runn with Digest Authentication enabled sends a SIP line request to Unified Comm Manager.
SIPLineServerAuthorizationFailures	This counter represents the number of authentication challenge failures for SIP requests from SIP phones to the Unified Communications Manager se authentication failure occurs when a SIP phone with Digest Authenticatior sends a SIP line request with bad credentials to Unified Communications I
SIPTrunkAuthorization	This counter represents the number of application-level authorization chec incoming SIP requests that Unified Communications Manager has issued to S An application-level authorization check occurs when Unified Communica Manager compares an incoming SIP request to the application-level settin SIP Trunk Security Profile Configuration window in Cisco Unified Comm Manager Administration.
SIPTrunkAuthorizationFailures	This counter represents the number of application-level authorization failu incoming SIP requests that have occurred on Unified Communications Ma trunks. An application-level authorization failure occurs when Unified Comm Manager compares an incoming SIP request to the application-level autho settings on the SIP Trunk Security Profile Configuration window in Cisco Communications Manager Administration and finds that authorization for o of the SIP features on that window is not allowed.
SIPTrunkServerAuthenticationChallenges	This counter represents the number of authentication challenges for incom requests that Unified Communications Manager issued to SIP trunks. An auth challenge occurs when a SIP trunk with Digest Authentication enabled ser request to Unified Communications Manager.
SIPTrunkServerAuthenticationFailures	This counter represents the number of authentication challenge failures tha for incoming SIP requests from SIP trunks to Unified Communications Ma authentication failure occurs when a SIP trunk with Digest Authentication sends a SIP request with bad credentials to Unified Communications Man
SWConferenceActive	This counter represents the number of active conferences on all software c devices that are registered with Unified Communications Manager.
SWConferenceCompleted	This counter represents the total number of conferences that used a software c bridge that was allocated from a Unified Communications Manager and th been completed, which means that the conference bridge has been allocate released. A conference activates when the first call connects to the bridge. conference completes when the last call disconnects from the bridge.
SWConferenceOutOfResources	This counter represents the total number of times that Unified Communica Manager attempted to allocate a software conference resource from those registered to Unified Communications Manager when none were available includes failed attempts to add a new participant to an existing conference

Counters	Counter Description
SWConferenceResourceActive	This counter represents the total number of conference resources that ar software conference devices that are registered with Unified Communicat The system considers a conference to be active when one or more calls bridge. One resource equals one stream.
SWConferenceResourceAvailable	This counter represents the number of new software-based conferences started at the same time, for Unified Communications Manager. You m minimum of three streams available for each new conference. One reso one stream.
SWConferenceResourceTotal	This counter represents the total number of software conference resour provided by all software conference bridge devices that are currently r Unified Communications Manager.
SystemCallsAttempted	This counter represents the total number of server-originated calls and a to the Unity message waiting indicator (MWI).
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are call on a Unified Communications Manager.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently use.
TLSConnectedSIPTrunks	This counter represents the number of SIP trunks that are configured a through Transport Layer Security (TLS).
TLSConnectedWSM	This counter represents the number of WSM Connectors that is configu connected to Motorola WSM through Transport Layer Security (TLS).
TranscoderOutOfResources	This counter represents the total number of times that Unified Commu Manager attempted to allocate a transcoder resource from a transcoder registered to a Unified Communications Manager when none was avai
TranscoderResourceActive	This counter represents the total number of transcoders that are in use on devices that are registered with Unified Communications Manager. A t use represents one transcoder resource that has been allocated for use i transcoder resource uses two streams.
TranscoderResourceAvailable	This counter represents the total number of transcoders that are not in u available to be allocated on all transcoder devices that are registered w Communications Manager. Each transcoder resource uses two streams
TranscoderResourceTotal	This counter represents the total number of transcoder resources that ar all transcoder devices that are currently registered with Unified Comm Manager.
VCBConferenceActive	This counter represents the total number of active video conferences o conference bridge devices that are registered with Unified Communicat
VCBConferenceAvailable	This counter represents the total number of new video conferences on a conference bridge devices that are registered with Unified Communicat

Counters	Counter Description
VCBConferenceCompleted	This counter represents the total number of video conferences that used a v conference bridge that is allocated from Unified Communications Manage have been completed, which means that the conference bridge has been allo released. A conference activates when the first call connects to the bridge. conference completes when the last call disconnects from the bridge.
VCBConferenceTotal	This counter represents the total number of video conferences that are sup all video conference bridge devices that are registered with Unified Comm Manager.
VCBOutOfConferences	This counter represents the total number of times that Unified Communica Manager attempted to allocate a video conference resource from those tha registered to Unified Communications Manager when none was available.
VCBOutOfResources	This counter represents the total number of failed new video conference re conference request can fail because, for example, the configured number of c is already in use.
VCBResourceActive	This counter represents the total number of video conference resources that ar in use on all video conference devices that are registered with Unified Comm Manager.
VCBResourceAvailable	This counter represents the total number of video conference resources tha active and are currently available.
VCBResourceTotal	This counter represents the total number of video conference resources that ar by all video conference bridge devices that are currently registered with U Communications Manager.
VideoCallsActive	This counter represents the number of active video calls with active video connections on all video conference bridge devices that are registered with Communications Manager.
VideoCallsCompleted	This counter represents the number of video calls that were actually conne video streams and then released.
VideoOutOfResources	This counter represents the total number of times that Unified Communica Manager attempted to allocate a video-streaming resource from one of the conference bridge devices that is registered to Unified Communications M when none was available.
XCODE_RequestsThrottled	This counter represents the total number of transcoder resource requests th been denied due to throttling (a resource from this transcoder was not allocate as specified by the Cisco CallManager service parameter MTP and Transc Resource Throttling Percentage, the transcoder was being utilized beyond configured throttle percentage). This counter increments each time a resou requested from this transcoder and is denied due to throttling. This counte running total since the transcoder device registered with the Cisco CallManag

Cisco CallManager System Performance

The CiscoCallManager System Performance object provides system performance information about Unified Communications Manager. The following table contains information about CiscoCallManager system performance counters.

Table 48: CiscoCallManager System Performance

Counters	Counter Description
AverageExpectedDelay	This counter represents the current average expected delay before any inco gets handled.
CallsRejectedDueToICTThrottling	This counter represents the total number of calls that were rejected sinc CiscoCallManager service due to Intercluster Trunk (ICT) call throttlin threshold limit of 140 calls per 5 seconds is met, the ICT will start throttli new calls. One cause for ICT call throttling occurs when calls across an route loop condition.
CallThrottlingGenericCounter3	This counter represents a generic counter that is used for call-throttling
CodeRedEntryExit	This counter indicates whether Unified Communications Manager has ent a Code state (call-throttling mode). Valid values include 0 (Exit) and 1 (
CodeYellowEntryExit	This counter indicates whether Unified Communications Manager has ent a Code Yellow state (call-throttling mode). Valid values include 0 (Exit)
EngineeringCounter1	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter2	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter3	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter4	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter5	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter6	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter7	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.
EngineeringCounter8	Do not use this counter unless directed by a Cisco Engineering Special uses information in this counter for diagnostic purposes.

Counters	Counter Description
QueueSignalsPresent 1-High	This counter indicates the number of high-priority signals in the Unified Communications Manager queue. High-priority signals include timeout even Unified Communications Manager keepalives, certain gatekeeper events, ar process creation, among other events. A large number of high-priority even cause degraded performance on Unified Communications Manager and resu call connection or loss of dial tone. Use this counter in conjunction with th QueueSignalsProcessed 1-High counter to determine the processing delay o Communications Manager.
QueueSignalsPresent 2-Normal	This counter indicates the number of normal-priority signals in the Unified Communications Manager queue. Normal-priority signals include call-proc functions, key presses, on-hook and off-hook notifications, among other ev large number of normal-priority events will cause degraded performance o Communications Manager, sometimes resulting in delayed dial tone, slow c connection, or loss of dial tone. Use this counter in conjunction with the QueueSignalsProcessed 2-Normal counter to determine the call-processing Unified Communications Manager. Remember that high-priority signals mus before normal-priority signals begin to process, so check the high-priority c well to get an accurate picture of the potential delay.
QueueSignalsPresent 3-Low	This counter indicates the number of low-priority signals in the Unified Comm Manager queue. Low-priority signals include station device registration (ex initial station registration request message), among other events. A large nu signals in this queue could result in delayed device registration, among oth
QueueSignalsPresent 4-Lowest	This counter indicates the number of lowest priority signals in the Unified Communications Manager queue. Lowest priority signals include the initia registration request message during device registration, among other event number of signals in this queue could result in delayed device registration, other events.
QueueSignalsProcessed 1-High	This counter indicates the number of high-priority signals that Unified Comm Manager processes for each 1-second interval. Use this counter in conjunct the QueueSignalsPresent 1-High counter to determine the processing delay queue.
QueueSignalsProcessed 2-Normal	This counter indicates the number of normal-priority signals that Unified Communications Manager processes for each 1-second interval. Use this co conjunction with the QueueSignalsPresent 2-Normal counter to determine the p delay on this queue. Remember that high-priority signals get processed bef normal-priority signals.
QueueSignalsProcessed 3-Low	This counter indicates the number of low-priority signals that Unified Comm Manager processes for each 1-second interval. Use this counter in conjunct the QueueSignalsPresent 3-Low counter to determine the processing delay queue. The number of signals processed gives an indication of how much d registration activity is being processed in this time interval.

Counters	Counter Description
QueueSignalsProcessed 4-Lowest	This counter indicates the number of lowest priority signals that Unifie Communications Manager processes for each 1-second interval. Use th conjunction with the QueueSignalsPresent 4-Lowest counter to determine delay on this queue. The number of signals that are processed gives an how many devices began the Unified Communications Manager registr in this time interval.
QueueSignalsProcessed Total	This counter provides a sum total of all queue signals that Unified Com Manager processes for each 1-second period for all queue levels: high, and lowest.
SkinnyDevicesThrottled	This counter represents the total number of Skinny devices that are bein Skinny device gets throttled (asked to shut down and reregister) when the of events that the Skinny device generated exceeds the configured maxim value (default value specifies 2000 events) within a 5-second interval.
ThrottlingSampleActivity	This counter indicates how many samples, out of the configured sample non-zero averageExpectedDelay values. This counter resets when any s averageExpectedDelay value of zero. This process repeats for each batc A batch represents the configured sample size.
TotalCodeYellowEntry	This counter indicates the number of times that Unified Communicatio call processing enters the code yellow state. This counter remains cumul start of the Unified Communications Manager process.

Cisco CTIManager

The Cisco CTI Manager object provides information about Cisco CTI Manager. The following table contains information about CiscoCTIManager counters.

Table 49: Cisco CTI Manager

Counters	Counter Description
CcmLinkActive	This counter represents the total number of active Unified Communicat links. CTI Manager maintains links to all active servers in a cluster, if a
CTIConnectionActive	This counter represents the total number of CTI clients that are currently the CTIManager. This counter increases by one when new connection i and decreases by one when a connection is released. The CTIManager serv MaxCTIConnections determines the maximum number of active conne
DevicesOpen	This counter represents the total number of devices that are configured Communications Manager that CTI applications control and/or monitor include hardware IP phones, CTI ports, CTI route points, and so on.
LinesOpen	This counter represents the total number of lines that are configured in Communications Manager that control and/or monitor CTI applications

Counters	Counter Description
QbeVersion	This counter represents the version number of the Quick Buffer Encoding (interface that the CTIManager uses.

Cisco Dual-Mode Mobility

The Cisco Dual-Mode Mobility object provides information about the dual-mode mobility application on Unified Communications Manager. The following table contains information about CiscoDual-Mode Mobility counters.

Table 50: Cisco Dual-Mode Mobility

Counters	Counter Description
CallsAnchored	This counter represents the number of calls that are placed or received on d phones that are anchored in Unified Communications Manager. The counter i when a call is received from or placed to a dual-mode phone. The counter i twice if a dual-mode phone calls another dual-mode phone.
DMMSRegistered	This counter represents the number of Dual-mode Mobile Station (DMMS) s that are registered in the wireless LAN (WLAN).
FollowMeAborted	This counter represents the number of failed follow-me operations.
FollowMeAttempted	This counter represents the number of follow-me operations that Unified Communications Manager attempted. The counter increments when a SIP 30 Temporarily message is received from the Wireless Service Manager (WSM Unified Communications Manager redirects the call to the DMMS in WLA
FollowMeCompleted	This counter represents the number of follow-me operations that were succ completed. The counter increments when the DMMS in WLAN answers th the media (voice path) is successfully established with the calling device.
FollowMeInProgress	This counter represents the number of follow-me operations that are curren progress. The counter increments when a follow-me is attempted, and it de when the follow-me operation is aborted or completed.
H1HandOutAttempted	This counter represents the number of H1 hand-out operations that dual-mo attempt. The counter increments when Unified Communications Manager p a call to the H1 number from a DMMS.
H1HandOutCompleted	This counter represents the number of successfully completed H1 hand-out The counter increments when the DMMS in WLAN successfully reestablish (voice path).
H2HandOutCompleted	This counter represents the number of successfully completed H2 hand-out The counter increments when the DMMS in WLAN successfully reestablish (voice path).

Counters	Counter Description
H2HandOutsAttempted	This counter represents the number of H2 hand-out operations that dual- attempt. The counter increments when Unified Communications Manag call to the H2 number from a DMMS.
HandInAborted	This counter represents the number of hand-in operations that failed.
HandInAttempted	This counter represents the number of hand-in operations that dual-moc attempt.
HandInCompleted	This counter represents the number of successfully completed hand-in op counter increments when the DMMS in WLAN successfully reestablish (voice path).
HandInInProgress	This counter represents the number of hand-in operations that are currentl The counter increments when a hand-in is attempted, and the counter dec the hand-in is aborted or completed.
HandOutAborted	This counter represents the number of hand-out operations that failed.
HandOutInProgress	This counter represents the number of H1 and H2 hand-out operations tha in progress. The counter increments when a H1 or H2 hand-out is attem decrements when the hand-out is aborted or completed.

Cisco Extension Mobility

The Cisco Extension Mobility object provides information about the extension mobility application. The following table contains information about Cisco Extension Mobility counters.

Table 51: Cisco Extension Mobility Application

Counters	Counter Description
RequestsHandled	This counter represents the total number of HTTP requests that the exter application handled since the last restart of the CiscoCallManager servi login would constitute two HTTP requests: one to query the initial login device and another to log in the user on a device. Similarly, a typical logo in two HTTP requests.
RequestsInProgress	This counter represents the number of HTTP requests that the extension application currently is handling. A typical login would constitute two H one to query the initial login state of the device and another to log in th device. Similarly, a typical logout also results in two HTTP requests.
RequestsThrottled	This counter represents the total number of Login/Logout Requests that throttling.
LoginsSuccessful	This counter represents the total number of successful login requests tha completed through EM Service.
LogoutsSuccessful	This counter represents the total number of successful logout requests t completed through EM Service

Counters	Counter Description
Total Login/LogoutRequestsAttempted	This counter represents the total number of Login and Logout requests that attempted through this EM Service. This number includes both successful a unsuccessful attempts.

Cisco Gatekeeper

The Cisco Gatekeeper object provides information about registered Cisco gatekeeper devices. The following table contains information about Ciscogatekeeper device counters.

Table 52: Cisco Gatekeeper

Counters	Counter Description
ACFsReceived	This counter represents the total number of RAS Admission Confirm mess are received from the configured gatekeeper and its alternate gatekeepers.
ARQsAttempted	This counter represents the total number of RAS Admission Request messa are attempted by using the configured gatekeeper and its alternate gatekeep
RasRetries	This counter represents the number of retries due to loss or delay of all RA acknowledgement messages on the configured gatekeeper and its alternate ga
VideoOutOfResources	This counter represents the total number of video-stream requests to the co gatekeeper or its alternate gatekeepers that failed, most likely due to lack of b

Cisco H.323

The Cisco H.323 object provides information about registered Cisco H.323 devices. The following table contains information about Cisco H.323 device counters.

Table 53: Cisco H.323

Counters	Counter Description
CallsActive	This counter represents the number of streaming connections that are curre (in use) on the configured H.323 device; in other words, the number of call actually have a voice path that is connected.
CallsAttempted	This counter represents the total number of calls that have been attempted o including both successful and unsuccessful call attempts.
CallsCompleted	This counter represents the total number of successful calls that were made device.
CallsInProgress	This counter represents the number of calls that are currently in progress o

Counters	Counter Description
CallsRejectedDueToICTCallThrottling	This counter represents the total number of calls rejected due to Interclu (ICT) call throttling since the start of the CiscoCallManager service. Wh reaches a threshold limit of 140 calls per 5 seconds, ICT will start throttli new calls. One cause for ICT call throttling occurs when calls across an route loop condition.
VideoCallsActive	This counter represents the number of video calls with video streaming that are currently active (in use) on all H.323 trunks that are registered v Communications Manager; in other words, the number of calls that actu video-streaming connections on a Unified Communications Manager.
VideoCallsCompleted	This counter represents the number of video calls that were actually con video streams for all H.323 trunks that were registered with a Unified Co Manager. This number increases when the call terminates.

Cisco Hunt Lists

The Cisco Hunt Lists object provides information about the hunt lists that are defined in Cisco Unified Communications Manager Administration. The following table contains information about Cisco hunt list counters.

Table 54: Cisco Hunt Lists

Counters	Counter Description
CallsAbandoned	This counter represents the number of abandoned calls that occurred thr list. An abandoned call represents one in which a caller hangs up before answered.
CallsActive	This counter represents the number of calls that are currently active (in occurred through a hunt list. An active call represents one that gets distr answered, and to which a voice path connects.
CallsBusyAttempts	This counter represents the number of times that calls through a hunt list w when all members of the line and/or route groups were busy.
CallsInProgress	This counter represents the number of calls that are currently in progres hunt list. A call in progress represents one that the call distributor is atte extend to a member of a line or route group and that has not yet been an Examples of a hunt list member include a line, a station device, a trunk port/channel of a trunk device.
CallsRingNoAnswer	This counter represents the total number of calls through a hunt list that called parties did not answer.

Counters	Counter Description
HuntListInService	This counter specifies whether the particular hunt list is currently in service of 0 indicates that the hunt list is out of service; a value of 1 indicates that th is in service. Reasons that a hunt list could be out of service include the hun running on a primary Unified Communications Manager based on its Unifi Communications Manager Group or the hunt list has been disabled in Cisc Communications Manager Administration.
MembersAvailable	This counter represents the total number of available or idle members of line groups that belong to an in-service hunt list. An available member currentl a call and will accept a new call. An idle member does not handle any call accept a new call. A hunt list member can comprise a route group, line grou combination. A member of a line group represents a directory number of a IP phone or a voice-mail port. A member of a route group represents a statio a trunk gateway, or port/channel of a trunk gateway.

Cisco HW Conference Bridge Device

The Cisco HW Conference Bridge Device object provides information about registered Cisco hardware conference bridge devices. The following table contains information about Cisco hardware conference bridge device counters.

Table 55: Cisco HW Conference Bridge Device

Counters	Counter Description
HWConferenceActive	This counter represents the number of conferences that are currently active (a HW conference bridge device. One resource represents one stream.
HWConferenceCompleted	This counter represents the total number of conferences that have been allo released on a HW conference device. A conference starts when the first cal to the bridge. The conference completes when the last call disconnects from t
OutOfResources	This counter represents the total number of times that an attempt was made a conference resource from a HW conference device and failed, for exampl all resources were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (a this HW conference device. One resource represents one stream.
ResourceAvailable	This counter represents the total number of resources that are not active an available to be used now for a HW conference device. One resource repres stream.
ResourceTotal	This counter represents the total number of resources for a HW conference device. This counter equals the sum of the counters ResourceAvailable and ResourceActive. One resource represents one stream.

Cisco IP Manager Assistant

The Cisco IP Manager Assistant (IPMA) Service object provides information about the Cisco Unified Communications Manager Assistant application. The following table contains information on Cisco IPMA counters.

Table 56: Cisco IP Manager Assistant Service

Counters	Counter Description
AssistantsActive	This counter represents the number of assistant consoles that are curren active assistant console exists when an assistant is logged in from the ass desktop application.
LinesOpen	This counter represents the number of phone lines that the Cisco Unifie Communications Manager Assistant application opened. An open phon when the application assumes line control from CTI.
ManagersActive	This counter represents the current number of managers that the Cisco I servicing.
SessionsCurrent	This counter represents the total number of managers assistants that are c the Cisco Unified Communications Manager Assistant application. Each each assistant constitute an active session; so, for one manager/assistan counter would reflect two sessions.

Cisco LBM service

The Cisco LBM service object provides information about LBM service that is defined in Unified Communications Manager. The following table contains information on Cisco LBM service counters.

Table 57: Cisco LBM service

Counters	Counter Description
Is Hub[1] or Spoke[0]	This counter represents the state of Location Bandwidth Manager is represented by 0 and hub state with a value of 1.
LocalHubNodesConnected	This counter represents the number of local hub nodes connected
LocalSpokesNodesConnected	This counter represents the number of local spoke nodes connecte
RemoteHubNodesConnectedInsecure	This counter represents the number of insecure remote hub nodes
RemoteHubNodesConnectedSecure	This counter represents the number of secure remote hub nodes c

Cisco Lines

The Cisco Lines object represents the number of Cisco lines (directory numbers) that can dial and connect to a device. Lines represent all directory numbers that terminate on an endpoint. The directory number that is assigned to it identifies the line. The Cisco Lines object does not include directory numbers that include wildcards such as a pattern for a Digital or Analog Access gateway.

The Active counter represents the state of the line, either active or not active. A zero indicates that the line is not in use. When the number is greater than zero, this indicates that the line is active, and the number represents the number of calls that are currently in progress on that line. If more than one call is active, this indicates that the call is on hold either because of being placed on hold specifically (user hold) or because of a network hold operation (for example, a transfer is in progress, and it is on transfer hold). This applies to all directory numbers that are assigned to any device.

Cisco Locations LBM

The Cisco Location LBM object provides information about locations that are defined in Unified Communications Manager clusters. The following table contains information on Cisco location counters.

Table 58: Cisco Locations LBM

Counters	Counter Description
BandwidthAvailable	This counter represents the current audio bandwidth in a l a link between two locations. A value of 0 indicates that n bandwidth is available.
BandwidthMaximum	This counter represents the maximum audio bandwidth that i in a location or a link between two locations. A value of 0 that no audio bandwidth is available.
BandwidthOversubscription	This represents the current oversubscribed audio bandwidt location or link between two locations. A value of zero ind bandwidth oversubscription.
CallsInProgress	This counter represents the number of calls that are curren progress on a particular Cisco Location Bandwidth Manag
ImmersiveOutOfResources	This represents the total number of failed immersive video bandwidth reservations associated with a location or a link two locations due to lack of immersive video bandwidth.
ImmersiveVideoBandwidthAvailable	This counter represents the maximum bandwidth that is av video in a location or a link between two locations. A valu indicates that no bandwidth is allocated for video.
ImmersiveVideoBandwidthMaximum	This counter represents the bandwidth that is currently ava video in a location or a link between two locations. A valu indicates that no bandwidth is available.
ImmersiveVideoBandwidthOversubscription	This represents the current immersive video oversubscribed in a location or link between two locations. A value of zero no bandwidth oversubscription.
OutOfResources	This counter represents the total number of failed audio call reservations associated with a given location or a link betw locations due to lack of audio bandwidth.

Counters	Counter Description
VideoBandwidthAvailable	This counter represents the bandwidth that is currently video in a location or a link between two locations. A indicates that no bandwidth is available.
VideoBandwidthMaximum	This counter represents the maximum bandwidth that is video in a location and a link between two locations. A indicates that no bandwidth is allocated for video.
VideoOversubscription	This represents the current video oversubscribed band in a location and a link between two locations. A value indicates no bandwidth oversubscription.
VideoOutOfResources	This counter represents the total number of failed video reservations associated with a given location or a link locations due to lack of video bandwidth.

Cisco Locations RSVP

The Cisco Location RSVP object provides information about RSVP that is defined in Unified Communications Manager. The following table contains information on Cisco location RSVP counters.

Table 59: Cisco Locations RSVP

Counters	Counter Description
RSVP AudioReservationErrorCounts	This counter represents the number of RSVP reservation errors in the a
RSVP MandatoryConnectionsInProgress	This counter represents the number of connections with mandatory RS progress.
RSVP OptionalConnectionsInProgress	This counter represents the number of connections with optional RSVP progress.
RSVP TotalCallsFailed	This counter represents the number of total calls that failed due to a RS failure.
RSVP VideoCallsFailed	This counter represents the number of video calls that failed due to a RS failure.
RSVP VideoReservationErrorCounts	This counter represents the number of RSVP reservation errors in the v

Cisco Media Streaming Application

The Cisco IP Voice Media Streaming Application object provides information about the registered MTPs, MOH servers, conference bridge servers, and annunciators. The following table contains information on Cisco IP Voice Media Streaming Application counters.

Note One object exists for each Unified Communications Manager in the Unified Communications Manager group that is associated with the device pool that the annunciator device is configured to use.

Table 60: Cisco Media Streaming Application

Counter	Counter Description
ANNConnectionsLost	This counter represents the total number of times since the last restart of th Voice Media Streaming Application that a Unified Communications Mana connection was lost.
ANNConnectionState	For each Unified Communications Manager that is associated with an annu this counter represents the current registration state to Unified Communica Manager; 0 indicates no registration to Unified Communications Manager; registration to the primary Unified Communications Manager; 2 indicates c to the secondary Unified Communications Manager (connected to Unified Communications Manager but not registered until the primary Unified Comm Manager connection fails).
ANNConnectionsTotal	This counter represents the total number of annunciator instances that have b since the Cisco IP Voice Media Streaming Application service started.
ANNInstancesActive	This counter represents the number of actively playing (currently in use) announcements.
ANNStreamsActive	This counter represents the total number of currently active simplex (one d streams for all connections. Each stream direction counts as one stream. O stream provides the audio input and another output stream to the endpoint
ANNStreamsAvailable	This counter represents the remaining number of streams that are allocated annunciator device that are available for use. This counter starts as 2 multip number of configured connections (defined in the Cisco IP Voice Media St App service parameter for the Annunciator, Call Count) and is reduced by o active stream that started.
ANNStreamsTotal	This counter represents the total number of simplex (one direction) stream connected to the annunciator device since the Cisco IP Voice Media Strea Application service started.
CFBConferencesActive	This counter represents the number of active (currently in use) conference
CFBConferencesTotal	This counter represents the total number of conferences that started since th Voice Media Streaming Application service started.
CFBConnectionsLost	This counter represents the total number of times since the last restart of th Voice Media Streaming Application that a Unified Communications Mana connection was lost.

Counter	Counter Description
CFBConnectionState	For each Unified Communications Manager that is associated with a SV Bridge, this counter represents the current registration state to Unified Co Manager; 0 indicates no registration to Unified Communications Manag registration to the primary Unified Communications Manager; 2 indicat to the secondary Unified Communications Manager (connected to Unif Communications Manager but not registered until the primary Unified Co Manager connection fails).
CFBStreamsActive	This counter represents the total number of currently active simplex (or streams for all conferences. Each stream direction counts as one stream. I conference, the number of active streams equals 6.
CFBStreamsAvailable	This counter represents the remaining number of streams that are alloca conference bridge that are available for use. This counter starts as 2 mu number of configured connections (defined in the Cisco IP Voice Medi App service parameter for Conference Bridge, Call Count) and is reduc each active stream started.
CFBStreamsTotal	This counter represents the total number of simplex (one direction) stre connected to the conference bridge since the Cisco IP Voice Media Stre Application service started.
MOHAudioSourcesActive	This counter represents the number of active (currently in use) audio so MOH server. Some of these audio sources may not be actively streamin if no devices are listening. The exception exists for multicast audio sou will always be streaming audio. When an audio source is in use, even after the listener has disconnected will always have one input stream for each configured MOH codec. For u the stream may exist in a suspended state where no audio data is received connects to listen to the stream. Each MOH multicast resource uses one each audio source and codec combination. For example, if the default a configured for multicast, G.711 mu-law and wideband codecs, then two used (default audio source + G.711 mu-law and default audio source +
MOHConnectionsLost	This counter represents the total number of times since the last restart o Voice Media Streaming Application that a Unified Communications M connection was lost.
MOHConnectionState	For each Unified Communications Manager that is associated with an M counter represents the current registration state to Unified Communicati 0 indicates no registration to Unified Communications Manager; 1 indicat to the primary Unified Communications Manager; 2 indicates connectio secondary Unified Communications Manager (connected to Unified Co Manager but not registered until the primary Unified Communications connection fails).

Counter	Counter Description
MOHStreamsActive	This counter represents the total number of active (currently in use) simple direction) streams for all connections. One output stream exists for each dev listening to a unicast audio source, and one input stream exists for each act source, multiplied by the number of MOH codecs. When an audio source has been used once, it will always have one input str each configured MOH codec. For unicast streams, the stream may exist in a state where no audio data is received until a device connects to listen to the Each MOH multicast resource uses one stream for each audio source and c combination. For example, if the default audio source is configured for mu G.711 mu-law and wideband codecs, then two streams get used (default au + G.711 mu-law and default audio source + wideband).
MOHStreamsAvailable	This counter represents the remaining number of streams that are allocated MOH device that are available for use. This counter starts as 408 plus the n configured half-duplex unicast connections and is reduced by 1 for each act that started. The counter gets reduced by 2 for each multicast audio source, by the number of MOH codecs that are configured. The counter gets reduce each unicast audio source, multiplied by the number of MOH codecs confi
MOHStreamsTotal	This counter represents the total number of simplex (one direction) streams connected to the MOH server since the Cisco IP Voice Media Streaming A service started.
MTPConnectionsLost	This counter represents the total number of times since the last restart of th Voice Streaming Application that a Unified Communications Manager con was lost.
MTPConnectionState	For each Unified Communications Manager that is associated with an MTP, th represents the current registration state to Unified Communications Manager; no registration to Unified Communications Manager; 1 indicates registratio primary Unified Communications Manager; 2 indicates connection to the s Unified Communications Manager (connected to Unified Communications but not registered until the primary Unified Communications Manager con fails).
MTPConnectionsTotal	This counter represents the total number of MTP instances that have been sta the Cisco IP Voice Media Streaming Application service started.
MTPInstancesActive	This counter represents the number of active (currently in use) instances of
MTPStreamsActive	This counter represents the total number of currently active simplex (one d streams for all connections. Each stream direction counts as one stream.
MTPStreamsAvailable	This counter represents the remaining number of streams that are allocated MTP device that are available for use. This counter starts as 2 multiplied by th of configured connections (defined in the Cisco IP Voice Media Streaming A parameter for MTP, Call Count) and is reduced by one for each active strea
MTPStreamsTotal	This counter represents the total number of simplex (one direction) streams connected to the MTP device since the Cisco IP Voice Media Streaming Ap service started.

Counter	Counter Description
IVRInstancesActive	This represents the number of current active interactive voice responses
IVRStreamsActive	This represents the total number of current active simplex (one directio all connections. Each stream direction counts as one stream. There is or stream providing the audio input and another output stream to the endp
IVRStreamsAvailable	This represents the remaining number of streams allocated for the IVR d available for use. This counter starts as 3 multiplied by the number of c connections (defined in the Cisco IP Voice Media Streaming App servic for the IVR, Call Count) and is reduced by one for each active stream s
IVRConnectionsTotal	This represents the total number of IVR instances that have been started s IP Voice Media Streaming Application service started.
IVRStreamsTotal	This represents the total number of simplex (one direction) streams that connected to the IVR device since the Cisco IP Voice Media Streaming service started.
IVRConnectionsLost	This represents the total number of times the Unified Communications connection was lost, since the last restart of the Cisco IP Voice Media S Application.
IVRErrors	This represents the total number of times the IVR failed to play, since t of the Cisco IP Voice Media Streaming Application.

Cisco Messaging Interface

The Cisco Messaging Interface object provides information about the Cisco Messaging Interface (CMI) service. The following table contains information on Cisco Messaging Interface (CMI) counters.

Table 61: Cisco Messaging Interface

Counters	Counter Description
HeartBeat	This counter represents the heartbeat of the CMI service. This incremer indicates that the CMI service is up and running. If the count does not i (increment), the CMI service is down.
SMDIMessageCountInbound	This counter represents the running count of inbound SMDI messages s restart of the CMI service.
SMDIMessageCountInbound24Hour	This counter represents the rolling count of inbound SMDI messages in hours.
SMDIMessageCountOutbound	This counter represents the running count of outbound SMDI messages restart of the CMI service.
SMDIMessageCountOutbound24Hour	This counter represents the rolling count of outbound SMDI messages i hours.

Counters	Counter Description
StartTime	This counter represents the time in milliseconds when the CMI service star real-time clock in the computer, which simply acts as a reference point that the current time and the time that has elapsed, in milliseconds, since the servi provides the basis for this time. The reference point specifies midnight, Jan 1970.

Cisco MGCP BRI Device

The Cisco Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) Device object provides information about registered Cisco MGCP BRI devices. The following table contains information on CiscoMGCP BRI device counters.

Table 62: Cisco MGCP BRI Device

Counters	Counter Description
CallsCompleted	This counter represents the total number of successful calls that were made MGCP Basic Rate Interface (BRI) device
Channel 1 Status	This counter represents the status of the indicated B-Channel that is associa the MGCP BRI device. Possible values: 0 (Unknown) indicates the status of th could not be determined; 1 (Out of service) indicates that this channel is no for use; 2 (Idle) indicates that this channel has no active call and is ready fo (Busy) indicates an active call on this channel; 4 (Reserved) indicates that th has been reserved for use as a D-channel or for use as a Synch-Channel for
Channel 2 Status	This counter represents the status of the indicated B-Channel that is associa the MGCP BRI device. Possible values: 0 (Unknown) indicates the status of th could not be determined; 1 (Out of service) indicates that this channel is no for use; 2 (Idle) indicates that this channel has no active call and is ready fo (Busy) indicates an active call on this channel; 4 (Reserved) indicates that th has been reserved for use as a D-channel or for use as a Synch-Channel for
DatalinkInService	This counter represents the state of the Data Link (D-Channel) on the corre digital access gateway. This value will get set to 1 (one) if the Data Link is service) or 0 (zero) if the Data Link is down (out of service).
OutboundBusyAttempts	This counter represents the total number of times that a call through this M device was attempted when no voice channels are available.

Cisco MGCP FXO Device

The Cisco Media Gateway Control Protocol (MGCP) Foreign Exchange Office (FXO) Device object provides information about registered Cisco MGCP FXO devices. The following table contains information on CiscoMGCP FXO device counters.

Table 63: Cisco MGCP FXO Device

Counters	Counter Description
CallsCompleted	This counter represents the total number of successful calls that were m port on an MGCP FXO device.
OutboundBusyAttempts	This counter represents the total number of times that a call through the MGCP FXO device was attempted when no voice channels were availa
PortStatus	This counter represents the status of the FXO port associated with this device.

Cisco MGCP FXS Device

The Cisco MGCP Foreign Exchange Station (FXS) Device object provides information about registered Cisco MGCP FXS devices. One instance of this object gets created for each port on a Cisco Catalyst 6000 24 port FXS Analog Interface Module gateway. For example, a fully configured Catalyst 6000 Analog Interface Module would represent 24 separate instances of this object. The following table contains information on CiscoMGCP FXS device counters.

Table 64: Cisco MGCP FXS Device

Counters	Counter Description
CallsCompleted	This counter represents the total number of successful calls that were m port on the MGCP FXS device.
OutboundBusyAttempts	This counter represents the total number of times that a call through thi MGCP FXS device was attempted when no voice channels were availab
PortStatus	This counter represents the status of the FXS port that is associated with device.

Cisco MGCP Gateways

The Cisco MGCP Gateways object provides information about registered MGCP gateways. The following table contains information on CiscoMGCP gateway counters.

Table 65: Cisco MGCP Gateways

Counters	Counter Description
BRIChannelsActive	This counter represents the number of BRI voice channels that are curre a call in the gateway
BRISpansInService	This counter represents the number of BRI spans that are currently avai in the gateway.
FXOPortsActive	This counter represents the number of FXO ports that are currently acti the gateway.

Counters	Counter Description
FXOPortsInService	This counter represents the number of FXO ports that are currently availab in the gateway.
FXSPortsActive	This counter represents the number of FXS ports that are currently active i the gateway.
FXSPortsInService	This counter represents the number of FXS ports that are currently availabl in the gateway.
PRIChannelsActive	This counter represents the number of PRI voice channels that are currently a call in the gateway.
PRISpansInService	This counter represents the number of PRI spans that are currently availabl in the gateway.
T1ChannelsActive	This counter represents the number of T1 CAS voice channels that are curren in a call in the gateway.
T1SpansInService	This counter represents the number of T1 CAS spans that are currently ava use in the gateway.

Cisco MGCP PRI Device

The Cisco MGCP Primary Rate Interface (PRI) Device object provides information about registered Cisco MGCP PRI devices. The following table contains information on CiscoMGCP PRI device counters.

Table 66: Cisco MGCP PRI Device

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use MGCP PRI device.
CallsCompleted	This counter represents the total number of successful calls that were made MGCP PRI device.
Channel 1 Status through Channel 15 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associa MGCP PRI device. Possible values: 0 (Unknown) indicates that the status of t could not be determined; 1 (Out of service) indicates that this channel is no for use; 2 (Idle) indicates that this channel has no active call and is ready fo (Busy) indicates that an active call exists on this channel; 4 (Reserved) indi this channel has been reserved for use as a D-Channel or for use as a Synch for E-1.
Channel 16 Status	This counter represents the status of the indicated B-Channel that is associa MGCP PRI Device. Possible values: 0-Unknown, 1-Out of service, 2-Idle, 4-Reserved, for an E1 PRI Interface, this channel is reserved for use as a D
Channel 17 Status through Channel 31 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is associa the MGCP PRI Device. 0-Unknown, 1-Out of service, 2-Idle, 3-Busy, 4-Re

Counters	Counter Description
DatalinkInService	This counter represents the state of the Data Link (D-Channel) on the c digital access gateway. This value will be set to 1 (one) if the Data Link service) or 0 (zero) if the Data Link is down (out of service).
OutboundBusyAttempts	This counter represents the total number of times that a call through an device was attempted when no voice channels were available.

Cisco MGCP T1 CAS Device

The Cisco MGCP T1 Channel Associated Signaling (CAS) Device object provides information about registered Cisco MGCP T1 CAS devices. The following table contains information on CiscoMGCP TI CAS device counters.

Table 67: Cisco MGCP T1 CAS Device

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in MGCP T1 CAS device.
CallsCompleted	This counter represents the total number of successful calls that were m MGCP T1 CAS device.
Channel 1 Status through Channel 24 Status (consecutively numbered)	This counter represents the status of the indicated B-Channel that is ass an MGCP T1 CAS device. Possible values: 0 (Unknown) indicates the channel could not be determined; 1 (Out of service) indicates that this c available for use; 2 (Idle) indicates that this channel has no active call ar use; 3 (Busy) indicates that an active call exists on this channel; 4 (Reser that this channel has been reserved for use as a D-Channel or for use as a S for E-1.
OutboundBusyAttempts	This counter represents the total number of times that a call through the CAS device was attempted when no voice channels were available.

Cisco Mobility Manager

The Cisco Mobility Manager object provides information on registered Cisco Unified Mobility Manager devices. The following table contains information on Cisco Unified Mobility Manager device counters.

Table 68: Cisco Mobility Manager

Counters	Counter Description
MobileCallsAnchored	This counter represents the total number of are associated with single-mode/dual-mode that is currently anchored on a Unified Comm Manager. Call anchoring occurs when a call enterprise gateway and connects to a mobili application that then uses redirection to send back out an enterprise gateway. For exampl counter increments twice for a dual-mode phone-to-dual-mode phone call: once for the call and once for the terminating call. When terminates, this counter decrements accordi
MobilityHandinsAborted	This counter represents the total number of handins.
MobileHandinsCompleted	This counter represents the total number of that were completed by dual-mode phones. A handin occurs when the call successfully co the enterprise network and the phone moves f to WLAN.
MobilityHandinsFailed	This counter represents the total number of (calls on mobile devices that move from cell wireless network) that failed.
MobilityHandoutsAborted	This counter represents the total number of handouts.
MobileHandoutsCompleted	This counter represents the total number of (calls on mobile devices that move from the WLAN network to the cellular network) tha completed. A completed handout occurs wh successfully connects.
MobileHandoutsFailed	This counter represents the total number of (calls on mobile devices that move from cell wireless network) that failed.
MobilityFollowMeCallsAttempted	This counter represents the total number of calls that were attempted.
MobilityFollowMeCallsIgnoredDueToAnswerTooSoon	This counter represents the total number of calls that were ignored before the AnswerTo timer went off.
MobilityIVRCallsAttempted	This counter represents the total number of IVR calls.
MobilityIVRCallsFailed	This counter represents the total number of calls.

Counters	Counter Description
MobilityIVRCallsSucceeded	This counter represents the total number IVR calls.
MobilitySCCPDualModeRegistered	This counter represents the total number SCCP devices that are registered.
MobilitySIPDualModeRegistered	This counter represents the total number SIP devices that are registered.

Cisco Music On Hold (MOH) Device

The Cisco Music On Hold (MOH) Device object provides information about registered Cisco MOH devices. The following table contains information on CiscoMOH device counters.

Table 69: Cisco MOH Device

Counters	Counter Description
MOHHighestActiveResources	This counter represents the largest number of simultaneously active MOI for an MOH server. This number includes both multicast and unicast co
MOHMulticastResourceActive	This counter represents the number of currently active multicast connectio addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source ar combination. For example, if the default audio source is configured for G.711 mu-law and wideband codecs, two streams get used (default aud G.711 mu-law and default audio source + wideband).
MOHMulticastResourceAvailable	This counter represents the number of multicast MOH connections to m addresses that are served by an MOH server that are not active and are to be used now for the MOH server. Each MOH multicast resource uses one stream for each audio source ar combination. For example, if the default audio source is configured for G.711 mu-law and wideband codecs, two streams get used (default aud G.711 mu-law and default audio source + wideband).
MOHOutOfResources	This counter represents the total number of times that the Media Resou attempted to allocate an MOH resource when all available resources on servers that are registered with a Unified Communications Manager we active.
MOHTotalMulticastResources	This counter represents the total number of multicast MOH connections th to multicast addresses that are served by an MOH server. Each MOH multicast resource uses one stream for each audio source ar combination. For example, if the default audio source is configured for G.711 mu-law and wideband codecs, two streams get used (default aud G.711 mu-law and default audio source + wideband).

Counters	Counter Description
MOHTotalUnicastResources	This counter represents the total number of unicast MOH connections that ar by an MOH server. Each MOH unicast resource uses one stream.
MOHUnicastResourceActive	This counter represents the number of active unicast MOH connections to a server. Each MOH unicast resource uses one stream.
MOHUnicastResourceAvailable	This counter represents the number of unicast MOH connections that are no and are still available to be used now for an MOH server. Each MOH unicast resource uses one stream.

Cisco MTP Device

The Cisco Media Termination Point (MTP) Device object provides information about registered Cisco MTP devices. The following table contains information on CiscoMTP device counters.

Table 70: Cisco MTP Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was made t an MTP resource from an MTP device and failed; for example, because all were already in use.
ResourceActive	This counter represents the number of MTP resources that are currently in us for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP that has been allocated for use in a call.
ResourceAvailable	This counter represents the total number of MTP resources that are not acti still available to be used now for an MTP device. Each MTP resource uses two streams. An MTP in use represents one MTP that has been allocated for use in a call.
ResourceTotal	This counter represents the total number of MTP resources that an MTP device This counter equals the sum of the counters ResourceAvailable and Resour

Cisco Phones

The Cisco Phones object provides information about the number of registered Cisco Unified IP Phones, including both hardware-based and other station devices.

The CallsAttempted counter represents the number of calls that have been attempted from this phone. This number increases each time that the phone goes off hook and on hook.

Cisco Presence Feature

The Cisco Presence object provides information about presence subscriptions, such as statistics that are related to the speed dial or call list Busy Lamp Field (BLF) subscriptions. The following table contains information on CiscoPresence feature.

Table 71: Cisco Presence

Counters	Counter Description
ActiveCallListAndTrunkSubscriptions	This counter represents the active presence subscriptions for the call lis well as presence subscriptions through SIP trunk.
ActiveSubscriptions	This counter represents all active incoming and outgoing presence subs
CallListAndTrunkSubscriptionsThrottled	This counter represents the cumulative number of rejected call list and presence subscriptions due to throttling for the call list feature.
IncomingLineSideSubscriptions	This counter represents the cumulative number of presence subscriptio received on the line side.
IncomingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptio received on the trunk side.
OutgoingTrunkSideSubscriptions	This counter represents the cumulative number of presence subscriptio sent on the trunk side.

Cisco QSIG Feature

The Cisco QSIG Feature object provides information about the operation of various QSIG features, such as call diversion and path replacement. The following table contains information about the Cisco QSIG feature counters.

Table 72: Cisco QSIG Feature

Counters	Counter Description
CallForwardByRerouteCompleted	This counter represents the number of successful calls that has been for rerouting. Call forward by rerouting enables the path for a forwarded ca optimized (minimizes the number of B-Channels in use) from the originato This counter resets when the CiscoCallManager service parameter Call Reroute Enabled is enabled or disabled, or when the Cisco CallManager Se
PathReplacementCompleted	This counter represents the number of successful path replacements that h Path replacement in a QSIG network optimizes the path between two ec (PBXs) that are involved in a call. This counter resets when the CiscoC service parameter Path Replacement Enabled is enabled or disabled, or w CallManager Service restarts.

Cisco Signaling Performance

The Cisco Signaling Performance object provides call-signaling data on transport communications on Unified Communications Manager. The following table contains information about the Cisco Signaling Performance counter.

Table 73: Cisco Signaling Performance

Counters	Counter Description
UDPPacketsThrottled	This counter represents the total number of incoming UDP packets that wer (dropped) because they exceeded the threshold for the number of incoming per second that is allowed from a single IP address. Configure the threshol SIP Station UDP Port Throttle Threshold and SIP Trunk UDP Port Throttle service parameters in Cisco Unified Communications Manager Administra counter increments for every throttled UDP packet that was received since restart of the Cisco CallManager Service.

Cisco SIP

The Cisco Session Initiation Protocol (SIP) object provides information about configured SIP devices. The following table contains information on the CiscoSIP counters.

Table 74: Cisco SIP

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in use SIP device.
CallsAttempted	This counter represents the number of calls that have been attempted on this S including the successful and unsuccessful call attempts.
CallsCompleted	This counter represents the number of calls that were actually connected (a was established) from a SIP device. This number increments when the call is t
CallsInProgress	This counter represents the number of calls that are currently in progress o device, including all active calls. When all calls that are in progress are con number of CallsInProgress equals the number of CallsActive.
VideoCallsActive	This counter represents the number of video calls with streaming video co that are currently active (in use) on this SIP device.
VideoCallsCompleted	This counter represents the number of video calls that were actually conne video streams for this SIP device. This number increments when the call is t

Cisco SIP Line Normalization

The Cisco SIP line normalization performance object contains counters that allow you to monitor aspects of the normalization script for SIP lines, including initialization errors, runtime errors, and script status. For SIP lines, each script has only one set of performance counters. This is true even if two endpoints share the same script. The following table contains information about the Cisco SIP line normalization counters.

Display Names	Description
DeviceResetAutomatically	This counter indicates the number of times that Unified Communications Manager automatically resets the device (SIP phone). Automatic resets occur only if the value specified in Script Execution Error Recovery Action or System Resource Error Recovery Action field is set to Reset Device. This counter increments each time Unified Communications Manager automatically resets a device (SIP phone) due to an error. The count is restarted when the script is reset following a change to the script configuration.
ErrorExecution	This counter indicates the number of execution errors that occur while the script executes. Execution errors can occur while a message handler executes. Execution errors can be caused by problems such as resource errors or an argument mismatch in a function call. When an execution error occurs, Unified Communications Manager performs the following actions: • Automatically restores the message to the original content before applying additional error-handling actions. • Increments the value of the counter. • Takes appropriate action based on the configuration of the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in Cisco Unified Communications Manager Administration. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script as needed, and reset the script by clicking the Reset button at the top of the script configuration page. The counter increments for each execution error since the last time the script was reset following a change to the script configuration. Both a script configuration change and a script reset must occur to restart the counter. If the counter continues to increment after you fix the script problem, examine the script again.

Display Names	Description
ErrorInit	This counter indicates the number of times a script error occurred after the script was successfully loaded into memory but failed to initialize in Unified Communications Manager. A script can fail to initialize due to resource errors, an argument mismatch in a function call, and so on. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script if needed, and reset the script by clicking the Reset button at the top of the script configuration page. The counter for the script instance increments every time an initialization error occurs. This counter provides a count from the most recent script reset that was accompanied by a change to the script configuration. Both a script configuration change and a script reset must occur to restart the counter. If the counter continues to increment after you fix the script problem, examine the script again. When the error occurs during initialization, Unified Communications Manager automatically disables the script.
ErrorInternal	This counter indicates the number of internal errors that have occurred while the script executed. Internal errors are extremely rare. If the value in this counter is higher than zero, there is a defect in the system not related to the script content or execution. Collect SDI traces and contact the Technical Assistance Center (TAC).
ErrorLoad	This counter indicates the number of times that a script error occurred while the script loaded into memory in Unified Communications Manager. A script can fail to load due to memory issues or syntax errors; check the SIPNormalizationScriptError alarm for details such as the script line number where the syntax error exists, check the script for syntax errors, upload a corrected script if needed and reset the script by clicking the Reset button at the top of the script configuration page. The counter for the script instance increments for each load error since the last time the script was reset following a change to the script configuration. Both a script configuration change and a script reset must have occurred to restart the counter. If the counter continues to increment after you believe you have fixed the script problem, examine the script again.

Display Names	Description
ErrorResource	This counter indicates whether or not the script encountered a resource error. There are two kinds of resource errors: exceeding the value configured in the Memory Threshold field or exceeding the value configured in the Lua Instruction Threshold field. Both fields display in the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration. If either condition occurs, Unified Communications Manager immediately closes the script and issues the SIPNormalizationScriptError alarm. If a resource error occurs while the script loads or initializes, the script is disabled. If a resource error occurs during execution, the configured system resource error recovery action is taken as configured in the System Resource Error Recovery Action field on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration.
MemoryUsage	This counter indicates the amount of memory, in bytes, that the script consumes based on the accumulation for all SIP phones using this script. This counter increases and decreases to match the amount of memory being utilized by the script. The count gets cleared when the script is closed (because a closed script consumes no memory) and restarts when the script is opened (enabled). A high number in this counter could indicate a resource problem. Check the MemoryUsagePercentage counter and check for a SIPNormalizationResourceWarning alarm, which occurs when the resource consumption exceeds an internally set threshold.
MemoryUsagePercentage	This counter indicates the percentage of the total amount of memory the script consumes based on the accumulation for all SIP phones using this script. The value in this counter is derived by dividing the value in the MemoryUsage counter by the value in the Memory Threshold field (in the SIP Normalization Script Configuration window) and multiplying that result by 100 to arrive at a percentage value. This counter increases and decreases in accordance with the MemoryUsage counter. This count is cleared when the script is closed (because closed scripts consume no memory) and restarts when the script is opened (enabled). When this counter reaches the internally controlled resource threshold, the SIPNormalizationResourceWarning alarm is issued.
MessageRollback	This counter indicates the number of times a message was not modified by the script due to an error while the script executes. This can occur only if the value in the Script Execution Error Recovery Action field is set to Message Rollback Only. When an execution error occurs, Unified Communications Manager automatically restores the message to the original contents prior to applying additional error-handling actions. If error handling specifies Rollback Only, no further action is taken beyond rolling back to the original message prior to the normalization attempt. For the other possible Script Execution Error Recovery Action settings, the action specified occurs after the message restores to the original contents.

Display Names	Description
msgAddContentBody	This counter indicates the number of times that the script adds a content body to the message. Assuming your message variable name is “msg”, if you are using the msg:addContentBody API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgAddHeader	This counter indicates the number of times that the script adds a SIP header to the message. Assuming your message variable name is “msg”, if you are using the msg:addHeader API in the script, this counter increases each time this API executes successfully. If the counter behavior is unexpected, examine the script logic for errors.
msgAddHeaderUriParameter	This counter indicates the number of times that the script adds a SIP header URI parameter to a SIP header in the message. Assuming your message variable name is “msg”, if you are using the msg:addHeaderUriParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgAddHeaderValueParameter	This counter indicates the number of times that the script adds a SIP header value parameter to a SIP header in the message. Assuming your message variable name is “msg”, if you are using the msg:addHeaderValueParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgApplyNumberMask	This counter indicates the number of times that the script applies a number mask to a SIP header in the message. Assuming your message variable name is “msg”, if you are using the msg:applyNumberMask API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgBlock	This counter indicates the number of times that the script blocks a message. Assuming your message variable name is “msg”, if you are using the msg:block API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgConvertDiversiontoHl	This counter indicates the number of times that the script converts Diversion headers into History-Info headers in the message. Assuming your message variable name is “msg”, if you are using the msg:convertDiversionToHI API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgConvertHlToDiverion	This counter indicates the number of times that the script converts History-Info headers into Diversion headers in the message. Assuming your message variable name is “msg”, if you are using the msg:convertHIToDiversion API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.

Display Names	Description
msgModifyHeader	This counter indicates the number of times that the script modifies a SIP header in the message. Assuming your message variable name is “msg”, if you are using the msg:modifyHeader API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgRemoveContentBody	This counter indicates the number of times that the script removes a content body from the message. Assuming your message variable name is “msg”, if you are using the msg:removeContentBody API in the script, this counter increases each time this API successfully executed. If the counter behavior is unexpected, examine the script logic for errors.
msgRemoveHeader	This counter indicates the number of times that the script removes a SIP header from the message. Assuming your message variable name is “msg”, if you are using the msg:removeHeader API in the script, this counter increases each time this API is successfully executed. If the counter behavior is unexpected, examine the script logic for errors.
msgRemoveHeaderValue	This counter indicates the number of times that the script removes a SIP header value from the message. Assuming your message variable name is “msg”, if you are using the msg:removeHeaderValue API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgRemoveUnreliableSdp	This counter indicates the number of times that the script removes SDP body from an unreliable 18x SIP message. Assuming your message variable name is “msg”, if you are using the msg:removeUnreliableSDP API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgSetRequestUri	This counter indicates the number of times that the script modifies the request URI in the message. Assuming your message variable name is “msg”, if you are using the msg:setRequestUri API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgSetResponseCode	This counter indicates the number of times that the script modifies the response code or response phrase in the message. Assuming your message variable name is “msg”, if you are using the msg:setResponseCode API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
msgSetSdp	This counter indicates the number of times that the script sets the SDP in the message. Assuming your message variable name is “msg”, if you are using the msg:setSdp API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.

Display Names	Description
ptAddContentBody	This counter indicates the number of times that the script adds a content body to the PassThrough object. Assuming your PassThrough object name is “pt”, if you are using the pt:addContentBody API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ptAddHeader	This counter indicates the number of times that the script adds a SIP header to the PassThrough object. Assuming your PassThrough object name is “pt”, if you are using the pt:addHeader API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ptAddHeaderUriParameter	This counter indicates the number of times that the script adds a SIP header URI parameter to the PassThrough object. Assuming your PassThrough object name is “pt”, if you are using the pt:addHeaderUriParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ptAddHeaderValueParameter	This counter indicates the number of times that the script adds a SIP header value parameter to the PassThrough object. Assuming your PassThrough object name is “pt”, if you are using the pt:addHeaderValueParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ptAddRequestUriParameter	This counter indicates the number of times that the script adds a request URI parameter to the PassThrough object. Assuming your PassThrough object name is “pt”, if you are using the pt:addRequestUriParameter API in the script, this counter increases each time this API successfully executes. If the counter behavior is unexpected, examine the script logic for errors.
ScriptActive	This counter indicates whether the script is currently active (running on SIP phones). A value of 0 indicates that the script is closed (disabled). A value of 1 indicates that the script is open and operational. To open the script that should be running, check for any alarms that might indicate why the script is not open, correct any errors, upload a new script if necessary, and reset the script.
ScriptClosed	This counter indicates the number of times that Unified Communications Manager closes the script. When the script closes on one SIP phone, it can still be enabled on other SIP phones. Unified Communications Manager closes the script because the last SIP phone using this script was either reset manually, reset automatically (due to an error), or deleted. This count restarts when the script resets following a change to the script configuration and when Cisco CallManager restarts.

Display Names	Description
ScriptDisabledAutomatically	This counter indicates the number of times that the system automatically disables the script. The values that are specified in the Execution Error Recovery Action or System Resource Error Recovery Action field in the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration determine whether the script is disabled. Automatic script disable occurs if either of these fields are set to Disable Script. The script also gets disabled as a result of script error conditions that are encountered during loading and initialization. This counter provides a count from the most recent manual device reset that involves a script configuration change (a device reset alone does not restart the count; the script must also have changed before the reset occurs). The counter increments each time Unified Communications Manager automatically disables a script due because of script errors. If the number in this counter is higher than expected, perform the following steps: • Check for a SIPNormalizationScriptError alarm and SIPNormalizationAutoResetDisabled alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.
ScriptOpened	This counter indicates the number of times that Unified Communications Manager attempts to open the script. For the script to open, it must load into memory in Unified Communications Manager, initialize, and be operational. A number greater than 1 in this counter means that Unified Communications Manager has made more than one attempt to open this script either for an expected reason or due to an error during loading or initialization. The error can occur due to execution errors or resource errors or invalid syntax in the script. Expect this counter to be greater than 1 if the ScriptResetAutomatically counter increments. If the number in this counter is higher than expected, perform the following steps: • Check for alarms such as the SIPNormalizationScriptClosed, SIPNormalizationScriptError, or SIPNormalizationResourceWarning. • Check resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files. This count restarts when the script resets after a script configuration change and when Unified Communications Manager restarts.

Display Names	Description
ScriptResetAutomatically	This counter indicates the number of times that the system automatically resets the script. The script resets based on the values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration. Automatic resets can occur if the value in either of these fields is Reset Script. This counter specifies the number of times that the system automatically resets the script following the last time the script is reset after a change to the script configuration. The counter increments each time Unified Communications Manager automatically resets a script because of script errors. If the number in this counter is higher than expected, perform the following steps: • Check for a SIPNormalizationScriptError alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.
ScriptResetManually	This counter indicates the number of times that the script manually resets in Cisco Unified Communications Manager Administration or by other methods, such as AXL, or a reset on the last SIP phone that used the script. This counter increments when a script is reset due to configuration changes. This counter restarts when the script is deleted, or when Cisco CallManager restarts.

Cisco SIP Normalization

The Cisco SIP Normalization performance object contains counters that allow you to monitor aspects of the normalization script, including initialization errors, runtime errors, and script status. Each device that has an associated script causes a new instance of these counters to be created. The following table contains Unified Communications Manager the CiscoSIP Normalization counters.

Table 75: Cisco SIP Normalization

Display Name	Description
DeviceResetAutomatically	This counter indicates the number of times that Unified Communications Manag automatically resets the device (SIP trunk). The device reset is based on the value are specified in the Script Execution Error Recovery Action and System Resource Recovery Action fields on the SIP Normalization Script Configuration window in Unified Communications Manager Administration. When the device (SIP trunk) i due to script errors, the counter value increments. This count restarts when the dev reset manually.

Display Name	Description
DeviceResetManually	This counter indicates the number of times that the device (SIP trunk) is reset in Cisco Unified Communications Manager Administration or by other metho as AXL. When the device associated with a script is reset due to configuration the counter value increments. The counter restarts in the following situations: • The SIP trunk is deleted. • The script on the trunk gets changed or deleted. • Unified Communications Manager restarts.
ErrorExecution	This counter represents the number of execution errors that occurred while th executed. Execution errors can occur while a message handler executes. Execut can be caused by resource errors, an argument mismatch in a function call, an When an execution error occurs, Unified Communications Manager performs following actions: • Automatically restores the message to the original content before applying error handling actions. • Increments the value of the counter. • Takes appropriate action based on the configuration of the Script Execut Recovery Action and System Resource Error Recovery Action fields in Unified Communications Manager Administration. Check the SIPNormalizationScriptError alarm for details, including the line n the script that failed. Correct the script problem, upload the corrected script as and reset the trunk. This counter increments every time an execution error occ counter provides a count from the most recent trunk reset that involved a scrip configuration change. (A device reset alone does not restart the count; the scr configuration must also change before the reset occurs.) If the counter continues to increment after you fix the script problem, examine again.
ErrorInit	This counter represents the number of times a script error occurred after the s successfully loaded into memory, but failed to initialize in Unified Communic Manager. A script can fail to initialize due to resource errors, an argument mis a function call, the expected table was not returned, and so on. Check the SIPNormalizationScriptError alarm for details, including the line n the script that failed. Correct the script problem, upload the corrected script as and reset the trunk. This counter increments every time an initialization error This counter provides a count from the most recent trunk reset that was accomp a script configuration change. (A device reset alone does not restart the count; configuration must also change before the reset occurs.) If the counter continu increment after you fix the script problem, examine the script again. When th occurs during initialization, Unified Communications Manager automatically the script.

Display Name	Description
ErrorInternal	This counter indicates the number of internal errors that occurred while the script executed. Internal errors are very rare. If the value in this counter is higher than z defect exists in the system that is not related to the script content or execution. Co SDI traces and contact the Technical Assistance Center (TAC).
ErrorLoad	This counter represents the number of times a script error occurred when the script l into memory in Unified Communications Manager. A script can fail to load due t memory issues or syntax errors. Check the SIPNormalizationScriptError alarm for details. Check the script syntax errors, upload the corrected script as needed, and reset the trunk. This counter incre every time a load error occurs. This counter provides a count from the most recent reset that was accompanied by a script configuration change. (A device reset alon not restart the count; the script configuration must also change before the reset oc If the counter continues to increment even after you fix the script problem, exami script again.
ErrorResource	This counter indicates whether the script encountered a resource error. Two kinds of resource errors exist: exceeding the value in the Memory Threshold and exceeding the value in the Lua Instruction Threshold field. (Both fields displa the SIP Normalization Script Configuration window in Cisco Unified Communic Manager Administration.) If either condition occurs, Unified Communications Ma immediately closes the script and issues the SIPNormalizationScriptError alarm. If a resource error occurs while the script loads or initializes, the script is disabled resource error occurs during execution, the configured system resource error reco action is taken. (The setting of the System Resource Error Recovery Action field SIP Normalization Script Configuration window in Cisco Unified Communicatio Manager Administration defines this action.)
MemoryUsage	This counter specifies the amount of memory, in bytes, that the script consumes. counter increases and decreases to match the amount of memory that the script us This count gets cleared when the script closes (because a closed script does not co memory) and restarts when the script opens (gets enabled). A high number in this c indicates a resource problem. Check the MemoryUsagePercentage counter and th SIPNormalizationResourceWarning alarm, which occur when the resource consum exceeds an internally set threshold.
MemoryUsagePercentage	This counter specifies the percentage of the total amount of memory that the scrip consumes. The value in this counter is derived by dividing the value in the MemoryUsage co by the value in the Memory Threshold field (in the SIP Normalization Script Configuration window) and multiplying the result by 100 to arrive at a percentag This counter increases and decreases in accordance with the MemoryUsage coun This count gets cleared when the script closes (because closed scripts do not cons memory) and restarts when the script opens (gets enabled). When this counter rea the internally controlled resource threshold, the SIPNormalizationResourceWarni alarm is issued.

Display Name	Description
MessageRollback	This counter indicates the number of times that the system automatically rolle message. The system rolls back the message by using the error handling that is in the Script Execution Error Recovery Action field in the SIP Normalization Configuration window in Cisco Unified Communications Manager Administr When an execution error occurs, Unified Communications Manager automaticall the message to the original content before applying additional error handling a error handling specifies Rollback only, no further action is taken beyond rollin the original message before the normalization attempt. For the other possible Execution Error Recovery Actions, message rollback always occurs first, foll the specified action, such as disabling the script, resetting the script automatic resetting the trunk automatically.
msgAddContentBody	This counter represents the number of times that the script added a content bo message. If you are using the msg:addContentBody API in the script, this cou increases each time that the msg:addContentBody API executes successfully. counter behavior is not as expected, examine the script logic for errors.
msgAddHeader	This counter represents the number of times that the script added a SIP heade message. If you are using the msg:addHeader API in the script, this counter in each time that the msg:addHeader API executes successfully. If the counter b not as expected, examine the script logic for errors.
msgAddHeaderUriParameter	This counter represents the number of times that the script added a SIP heade parameter to a SIP header in the message. If you are using the msg:addHeaderUriParameter API in the script, this counter increases each tim msg:addHeaderUriParameter API executes successfully. If the counter behavi as expected, examine the script logic for errors.
msgAddHeaderValueParameter	This counter represents the number of times that the script added a SIP heade parameter to a SIP header in the message. If you are using the msg:addHeaderValueParameter API in the script, this counter increases each t the msg:addHeaderValueParameter API executes successfully. If the counter b is not as expected, examine the script logic for errors.
msgApplyNumberMask	This counter represents the number of times that the script applied a number m SIP header in the message. If you are using the msg:applyNumberMask API in t this counter increases each time that the msg:applyNumberMask API execute successfully. If the counter behavior is not as expected, examine the script log errors.
msgBlock	This counter represents the number of times that the script blocked a message are using the msg:block API in the script, this counter increases each time tha msg:block API executes successfully. If the counter behavior is not as expected the script logic for errors.
msgConvertDiversionToHI	This counter represents the number of times that the script converted Diversio into History-Info headers in the message. If you are using the msg:convertDiver API in the script, this counter increases each time that the msg:convertDiversi API executes successfully. If the counter behavior is not as expected, examine logic for errors.

Display Name	Description
msgConvertHIToDiversion	This counter represents the number of times that the script converted Diversion he into History-Info headers in the message. If you are using the msg:convertDiversion API in the script, this counter increases each time that the msg:convertDiversionT API executes successfully. If the counter behavior is not as expected, examine the logic for errors.
msgModifyHeader	This counter represents the number of times that the script modified a SIP header message. If you are using the msg:modifyHeader API in the script, this counter inc each time that the msg:modifyHeader API executes successfully. If the counter bel is not as expected, examine the script logic for errors.
msgRemoveContentBody	This counter represents the number of times that the script removed a content body the message. If you are using the msg:removeContentBody API in the script, this co increases each time that the msg:removeContentBody API executes successfully. counter behavior is not as expected, examine the script logic for errors.
msgRemoveHeader	This counter represents the number of times that the script removed a SIP header the message. If you are using the msg:removeHeader API in the script, this count increases each time that the msg:removeHeader API executes successfully. If the co behavior is not as expected, examine the script logic for errors.
msgRemoveHeaderValue	This counter represents the number of times that the script removed a SIP header from the message. If you are using the msg:removeHeaderValue API in the script counter increases each time that the msg:removeHeaderValue API executes succes If the counter behavior is not as expected, examine the script logic for errors.
msgSetRequestUri	This counter represents the number of times that the script modified the request U the message. If you are using the msg:setRequestUri API in the script, this count increases each time that the msg:setRequestUri API executes successfully. If the co behavior is not as expected, examine the script logic for errors.
msgSetResponseCode	This counter represents the number of times that the script modified the response and/or response phrase in the message. If you are using the msg:setResponseCod in the script, this counter increases each time that the msg:setResponseCode API ex successfully. If the counter behavior is not as expected, examine the script logic f errors.
msgSetSdp	This counter represents the number of times that the script set the SDP in the mes If you are using the msg:setSdp API in the script, this counter increases each time the msg:setSdp API executes successfully. If the counter behavior is not as expec examine the script logic for errors.
ptAddContentBody	This counter represents the number of times that the script added a content body PassThrough (pt) object. If you are using the pt:addContentBody API in the scrip counter increases each time that the pt:addContentBody API executes successfull the counter behavior is not as expected, examine the script logic for errors.
ptAddHeader	This counter represents the number of times that the script added a SIP header to PassThrough (pt) object. If you are using the pt:addHeader API in the script, this co increases each time that the pt:addHeader API executes successfully. If the count behavior is not as expected, examine the script logic for errors.

Display Name	Description
ptAddHeaderUriParameter	This counter represents the number of times that the script added a SIP heade parameter to the PassThrough (pt) object. If you are using the pt:addHeaderUriI API in the script, this counter increases each time that the pt:addHeaderUriPa API executes successfully. If the counter behavior is not as expected, examine logic for errors.
ptAddHeaderValueParameter	This counter represents the number of times that the script added a SIP heade parameter to the PassThrough (pt) object. If you are using the pt:addHeaderValueParameter API in the script, this counter increases each tim pt:addHeaderValueParameter API executes successfully. If the counter behavi as expected, examine the script logic for errors.
ptAddRequestUriParameter	This counter represents the number of times that the script added a request URI to the PassThrough (pt) object. If you are using the pt:addRequestUriParamet the script, this counter increases each time that the pt:addRequestUriParamete executes successfully. If the counter behavior is not as expected, examine the sc for errors.
ScriptActive	This counter indicates whether the script is currently active (running on the tr following values display for the counter: • 0—Indicates that the script is closed (disabled). • 1—Indicates that the script is open and operational. To open the script that should be running on this trunk, perform the following **1.** Check for any alarms that might indicate why the script is not open. **2.** Correct any errors. **3.** Upload a new script if necessary. **4.** Reset the trunk.
ScriptClosed	This counter indicates the number of times that Unified Communications Ma closed the script. When the script is closed, it is not enabled on this device. Unified Communications Manager closes the script under one of the following c • The device was reset manually. • The device was reset automatically (due to an error). • The device was deleted. This count restarts when the SIP trunk is reset after a change to the script con and when Unified Communications Manager restarts.

Display Name	Description
ScriptDisabledAutomatically	This counter indicates the number of times that the system automatically disabled script. The values that are specified in the Script Execution Error Recovery Actio System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administratio determine whether the script is disabled. The script also gets disabled as a result of error conditions that are encountered during loading and initialization. This count provides a count from the most recent manual device reset that involved a script configuration change (a device reset alone does not restart the count; the script mus have changed before the reset occurs). This counter increments every time Unifie Communications Manager automatically disables a script due to script errors. If the number in this counter is higher than expected, perform the following actio • Check for SIPNormalizationScriptError alarm and SIPNormalizationAutoResetDisabled alarm. • Check for any resource-related alarms and counters in RTMT to determine wl a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.
ScriptOpened	This counter indicates the number of times that the Unified Communications Mar attempted to open the script. For the a script to open, it must load into memory in U Communications Manager, initialize, and be operational. A number greater than c this counter means that Unified Communications Manager has made more than o attempt to open the script on this SIP trunk, either for an expected reason or due t error during loading or initialization. The error can occur due to execution errors resource errors or invalid syntax in the script. Expect this counter to be greater tha if any of these counters increment: DeviceResetManually, DeviceResetAutomatic or ScriptResetAutomatically. The DeviceResetManually counter increments wher expected event, such as a maintenance window on the SIP trunk, causes the scrip close. If the number in this counter is high for an unexpected reason, perform the follow actions: • Check for alarms, such as the SIPNormalizationScriptClosed, SIPNormalizationScriptError, or SIPNormalizationResourceWarning. • Check resource-related alarms and counters in RTMT to determine whether resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files. This count restarts when the SIP trunk resets after a script configuration change a when Unified Communications Manager restarts.

Display Name	Description
ScriptResetAutomatically	This counter indicates the number of times that the system automatically reset t The script resets based on the values that are specified in the Script Execution Recovery Action and System Resource Error Recovery Action fields in the SI Normalization Script Configuration window in Cisco Unified Communications Administration. This counter specifies a count of the number of automatic scr after the last manual device reset; this counter increments every time the Unif Communications Manager automatically resets a script due to script errors. If the number in this counter is higher than expected, perform the following a • Check for a SIPNormalizationScriptError alarm. • Check for any resource-related alarms and counters in RTMT to determin a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace file

Cisco SIP Stack

The Cisco SIP Stack object provides information about Session Initiation Protocol (SIP) stack statistics that are generated or used by SIP devices such as SIP Proxy, SIP Redirect Server, SIP Registrar, and SIP User Agent. The following table contains information on Cisco SIP Stack counters.

Table 76: Cisco SIP Stack

Counters	Counter Description
AckIns	This counter represents the total number of ACK requests that the SIP de
AckOuts	This counter represents the total number of ACK requests that the SIP c
ByeIns	This counter represents the total number of BYE requests that the SIP de This number includes retransmission.
ByeOuts	This counter represents the total number of BYE requests that the SIP d This number includes retransmission.
CancelIns	This counter represents the total number of CANCEL requests that the received. This number includes retransmission.
CancelOuts	This counter represents the total number of CANCEL requests that the SI This number includes retransmission.
CCBsAllocated	This counter represents the number of Call Control Blocks (CCB) that a in use by the SIP stack. Each active SIP dialog uses one CCB.
GlobalFailedClassIns	This counter represents the total number of 6xx class SIP responses that t has received. This number includes retransmission. This class of respon that a SIP device, that is providing a client function, received a failure resp Generally, the responses indicate that a server had definitive information called party and not just the particular instance in the Request-URI.

Counters	Counter Description
GlobalFailedClassOuts	This counter represents the total number of 6xx class SIP responses that the S sent. This number includes retransmission. This class of responses indicates device, that is providing a server function, received a failure response mess Generally, the responses indicate that a server had definitive information on a called party and not just the particular instance in the Request-URI.
InfoClassIns	This counter represents the total number of 1xx class SIP responses that the S received. This includes retransmission. This class of responses provides inf on the progress of a SIP request.
InfoClassOuts	This counter represents the total number of 1xx class SIP responses that the S sent. This includes retransmission. This class of responses provides inform the progress of processing a SIP request.
InfoIns	This counter represents the total number of INFO requests that the SIP dev received. This number includes retransmission.
InfoOuts	This counter represents the total number of INFO requests that the SIP devic This number includes retransmission.
InviteIns	This counter represents the total number of INVITE requests that the SIP d received. This number includes retransmission.
InviteOuts	This counter represents the total number of INVITE requests that the SIP d sent. This number includes retransmission.
NotifyIns	This counter represents the total number of NOTIFY requests that the SIP received. This number includes retransmission.
NotifyOuts	This counter represents the total number of NOTIFY requests that the SIP sent. This number includes retransmission.
OptionsIns	This counter represents the total number of OPTIONS requests that the SIP received. This number includes retransmission.
OptionsOuts	This counter represents the total number of OPTIONS requests that the SIP sent. This number includes retransmission.
PRAckIns	This counter represents the total number of PRACK requests that the SIP d received. This number includes retransmission.
PRAckOuts	This counter represents the total number of PRACK requests that the SIP d sent. This number includes retransmission.
PublishIns	This counter represents the total number of PUBLISH requests that the SIP received. This number includes retransmissions.
PublishOuts	This counter represents the total number of PUBLISH requests that the SIP sent. This number includes retransmission

Counters	Counter Description
RedirClassIns	This counter represents the total number of 3xx class SIP responses that t has received. This number includes retransmission. This class of respon information about redirections to addresses where the callee may be rea
RedirClassOuts	This counter represents the total number of 3xx class SIP responses that t has sent. This number includes retransmission. This class of responses information about redirections to addresses where the callee may be rea
ReferIns	This counter represents the total number of REFER requests that the SI received. This number includes retransmission.
ReferOuts	This counter represents the total number of REFER requests that the SI sent. This number includes retransmission.
RegisterIns	This counter represents the total number of REGISTER requests that th has received. This number includes retransmission.
RegisterOuts	This counter represents the total number of REGISTER requests that th has sent. This number includes retransmission.
RequestsFailedClassIns	This counter represents the total number of 4xx class SIP responses that t has received. This number includes retransmission. This class of respon a request failure by a SIP device that is providing a client function.
RequestsFailedClassOuts	This counter represents the total number of 4xx class SIP responses that t has sent. This number includes retransmission. This class of responses i request failure by a SIP device that is providing a server function.
RetryByes	This counter represents the total number of BYE retries that the SIP de To determine the number of first BYE attempts, subtract the value of this the value of the sipStatsByeOuts counter.
RetryCancels	This counter represents the total number of CANCEL retries that the SI sent. To determine the number of first CANCEL attempts, subtract the counter from the value of the sipStatsCancelOuts counter.
RetryInfo	This counter represents the total number of INFO retries that the SIP de To determine the number of first INFO attempts, subtract the value of th from the value of the sipStatsInfoOuts counter.
RetryInvites	This counter represents the total number of INVITE retries that the SIP sent. To determine the number of first INVITE attempts, subtract the va counter from the value of the sipStatsInviteOuts counter.
RetryNotify	This counter represents the total number of NOTIFY retries that the SIF sent. To determine the number of first NOTIFY attempts, subtract the v counter from the value of the sipStatsNotifyOuts counter.
RetryPRAck	This counter represents the total number of PRACK retries that the SIP sent. To determine the number of first PRACK attempts, subtract the va counter from the value of the sipStatsPRAckOuts counter.

Counters	Counter Description
RetryPublish	This counter represents the total number of PUBLISH retries that the SIP d been sent. To determine the number of first PUBLISHs attempts, subtract t of this counter from the value of the sipStatsPublishOuts counter.
RetryRefer	This counter represents the total number of REFER retries that the SIP devic To determine the number of first REFER attempts, subtract the value of thi from the value of the sipStatsReferOuts counter.
RetryRegisters	This counter represents the total number of REGISTER retries that the SIP sent. To determine the number of first REGISTER attempts, subtract the va counter from the value of the sipStatsRegisterOuts counter.
RetryRel1xx	This counter represents the total number of Reliable 1xx retries that the SIP sent.
RetryRequestsOut	This counter represents the total number of Request retries that the SIP devic
RetryResponsesFinal	This counter represents the total number of Final Response retries that the S has sent.
RetryResponsesNonFinal	This counter represents the total number of non-Final Response retries that device has sent.
RetrySubscribe	This counter represents the total number of SUBSCRIBE retries that the SI has sent. To determine the number of first SUBSCRIBE attempts, subtract of this counter from the value of the sipStatsSubscribeOuts counter.
RetryUpdate	This counter represents the total number of UPDATE retries that the SIP de sent. To determine the number of first UPDATE attempts, subtract the valu counter from the value of the sipStatsUpdateOuts counter.
SCBsAllocated	This counter represents the number of Subscription Control Blocks (SCB) currently in use by the SIP stack. Each subscription uses one SCB.
ServerFailedClassIns	This counter represents the total number of 5xx class SIP responses that the S has received. This number includes retransmission. This class of responses that failure responses were received by a SIP device that is providing a clien
ServerFailedClassOuts	This counter represents the total number of 5xx class SIP responses that the S has sent. This number includes retransmission. This class of responses indi failure responses were received by a SIP device that is providing a server f
SIPGenericCounter1	Do not use this counter unless directed to do so by a Cisco Engineering Spe Cisco uses information in this counter for diagnostic purposes.
SIPGenericCounter2	Do not use this counter unless directed to do so by a Cisco Engineering Spe Cisco uses information in this counter for diagnostic purposes.
SIPGenericCounter3	Do not use this counter unless directed to do so by a Cisco Engineering Spe Cisco uses information in this counter for diagnostic purposes.

Counters	Counter Description
SIPGenericCounter4	Do not use this counter unless directed to do so by a Cisco Engineering Cisco uses information in this counter for diagnostic purposes.
SIPHandlerSDLQueueSignalsPresent	This counter represents the number of SDL signals that are currently on priority queues of the SIPHandler component. The SIPHandler compon the SIP stack.
StatusCode1xxIns	This counter represents the total number of 1xx response messages, incl retransmission, that the SIP device has received. This count includes th 1xx responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress
StatusCode1xxOuts	This counter represents the total number of 1xx response messages, incl retransmission, that the SIP device has sent. This count includes the fol responses: • 100 Trying • 180 Ringing • 181 Call is being forwarded • 182 Queued • 183 Session Progress
StatusCode2xxIns	This counter represents the total number of 2xx response messages, incl retransmission, that the SIP device has received. This count includes th 2xx responses: • 200 OK • 202 Success Accepted
StatusCode2xxOuts	This counter represents the total number of 2xx response messages, inc retransmission, that the SIP device has sent. This count includes the fol responses: • 200 OK • 202 Success Accepted
StatusCode3xxins	This counter represents the total number of 3xx response messages, incl retransmission, that the SIP device has received. This count includes th 3xx responses: • 300 Multiple Choices • 301 Moved Permanently • 302 Moved Temporarily • 303 Incompatible Bandwidth Units • 305 Use Proxy • 380 Alternative Service

Counters	Counter Description
StatusCode302Outs	This counter represents the total number of 302 Moved Temporarily response including retransmission, that the SIP device has sent.
StatusCode4xxIns	This counter represents the total number of 4xx response messages, includi retransmission, that the SIP device has received. This count includes the fo 4xx responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending

Counters	Counter Description
StatusCode4xxOuts	This counter represents the total number of 4xx response messages, inc retransmission, that the SIP device has sent. This count includes the fol responses: • 400 Bad Request • 401 Unauthorized • 402 Payment Required • 403 Forbidden • 404 Not Found • 405 Method Not Allowed • 406 Not Acceptable • 407 Proxy Authentication Required • 408 Request Timeout • 409 Conflict • 410 Gone • 413 Request Entity Too Large • 414 Request-URI Too Long • 415 Unsupported Media Type • 416 Unsupported URI Scheme • 417 Unknown Resource Priority • 420 Bad Extension • 422 Session Expires Value Too Small • 423 Interval Too Brief • 480 Temporarily Unavailable • 481 Call/Transaction Does Not Exist • 482 Loop Detected • 483 Too Many Hops • 484 Address Incomplete • 485 Ambiguous • 486 Busy Here • 487 Request Terminated • 488 Not Acceptable Here • 489 Bad Subscription Event • 491 Request Pending
StatusCode5xxIns	This counter represents the total number of 5xx response messages, incl retransmission, that the SIP device has received. This count includes the 5xx responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed

Counters	Counter Description
StatusCode5xxOuts	This counter represents the total number of 5xx response messages, includi retransmission, that the SIP device has sent. This count includes the follow responses: • 500 Server Internal Error • 501 Not Implemented • 502 Bad Gateway • 503 Service Unavailable • 504 Server Timeout • 505 Version Not Supported • 580 Precondition Failed
StatusCode6xxIns	This counter represents the total number of 6xx response messages, includi retransmission, that the SIP device has received. This count includes the fo 6xx responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
StatusCode6xxOuts	This counter represents the total number of 6xx response messages, includi retransmission, that the SIP device has sent. This count includes the follow responses: • 600 Busy Everywhere • 603 Decline • 604 Does Not Exist Anywhere • 606 Not Acceptable
SubscribeIns	This counter represents the total number of SUBSCRIBE requests that the S has received. This number includes retransmission.
SubscribeOuts	This counter represents the total number of SUBSCRIBE requests that the S has sent. This number includes retransmission.
SuccessClassIns	This counter represents the total number of 2xx class SIP responses that the S has received. This includes retransmission. This class of responses provides in on the successful completion of a SIP request.
SuccessClassOuts	This counter represents the total number of 2xx class SIP responses that the S has sent. This includes retransmission. This class of responses provides inf on the successful completion of a SIP request.
SummaryRequestsIn	This counter represents the total number of SIP request messages that have received by the SIP device. This number includes retransmissions.

Counters	Counter Description
SummaryRequestsOut	This counter represents the total number of SIP request messages that th This number includes messages that originate on the device and messag being relayed by the device. When a particular message gets sent more th transmission gets counted separately; for example, a message that is re- retransmission or as a result of forking.
SummaryResponsesIn	This counter represents the total number of SIP response messages that t received. This number includes retransmission.
SummaryResponsesOut	This counter represents the total number of SIP response messages that t sent (originated and relayed). This number includes retransmission.
UpdateIns	This counter represents the total number of UPDATE requests that the S received. This number includes retransmission.
UpdateOuts	This counter represents the total number of UPDATE requests that the S sent. This number includes retransmission.

Cisco SIP Station

The Cisco SIP Station object provides information about SIP line-side devices. The following table contains information about the Cisco SIP Station counters.

Table 77: Cisco SIP Station

Counters	Counter Description
ConfigMismatchesPersistent	This counter represents the number of times that a phone that is running persistently unable to register due to a configuration version mismatch TFTP server and Unified Communications Manager since the last restart Communications Manager. This counter increments each time that Uni Communications Manager cannot resolve the mismatch and manual int required (such as a configuration update or device reset).
ConfigMismatchesTemporary	This counter represents the number of times that a phone that is running temporarily unable to register due to a configuration version mismatch TFTP server and Unified Communications Manager since the last resta CallManager Service. This counter increments each time Unified Com Manager is able to resolve the mismatch automatically.
DBTimeouts	This counter represents the number of new registrations that failed beca occurred while the system was attempting to retrieve the device config the database.
NewRegAccepted	This counter represents the total number of new REGISTRATION requ been removed from the NewRegistration queue and processed since the the Cisco CallManager Service.

Counters	Counter Description
NewRegQueueSize	This counter represents the number of REGISTRATION requests that are c on the NewRegistration queue. The system places REGISTRATION reques received from devices that are not currently registered on this queue before processed.
NewRegRejected	This counter represents the total number of new REGISTRATION requests rejected with a 486 Busy Here response and not placed on the NewRegistrat since the last restart of the Cisco CallManager Service. The system rejects REGISTRATION requests if the NewRegistration queue exceeds a program
TokensAccepted	This counter represents the total number of token requests that have been gra the last Unified Communications Manager restart. Unified Communications grants tokens as long as the number of outstanding tokens remains below th that is specified in the Cisco CallManager service parameter Maximum Phon Queue Depth.
TokensOutstanding	This counter represents the number of devices that have been granted a toke not yet registered. The system requires that devices that are reconnecting to priority Unified Communications Manager server be granted a token before r Tokens protect Unified Communications Manager from being overloaded w registration requests when it comes back online after a failover situation.
TokensRejected	This counter represents the total number of token requests that have been reje the last Unified Communications Manager restart. Unified Communications will reject token request if the number of outstanding tokens is greater than th that is specified in the Cisco CallManager service parameter Maximum Phon Queue Depth.

Cisco SW Conf Bridge Device

The Cisco SW Conference Bridge Device object provides information about registered Cisco software conference bridge devices. The following table contains information on the Cisco software conference bridge device counters.

Table 78: Cisco SW Conf Bridge Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was made t a conference resource from a SW conference device and failed because all were already in use.
ResourceActive	This counter represents the number of resources that are currently in use (a a SW conference device. One resource represents one stream.
ResourceAvailable	This counter represents the total number of resources that are not active and available to be used now for a SW conference device. One resource represe stream.

Counters	Counter Description
ResourceTotal	This counter represents the total number of conference resources that a S device provides. One resource represents one stream.This counter equal the ResourceAvailable and ResourceActive counters.
SWConferenceActive	This counter represents the number of software-based conferences that active (in use) on a SW conference device.
SWConferenceCompleted	This counter represents the total number of conferences that have been released on a SW conference device. A conference starts when the first to the bridge. The conference completes when the last call disconnects fro

Cisco Telepresence MCU Conference Bridge Device

The Cisco Telepresence MCU Conference Bridge Device provides information about registered MCU conference bridge devices. The following table contains information about the Cisco Telepresence MCU Conference Bridge Device counters.

Table 79: Cisco Telepresence MCU Conference Bridge Device

Counters	Counter Description
ConferencesActive	This counter represents the total number of active conferences on all Cisco MCU conference bridge devices that are registered with Unified Comm Manager.
ConferencesCompleted	This counter represents the total number of conferences that used a Cisco MCU conference bridge allocated from Unified Communications Mana completed, implying that the conference bridge was allocated and released. is activated when the first call is connected to the bridge. The conference when the last call is disconnected from the bridge.
HttpConnectionErrors	This counter represents the total number of times Unified Communicati attempted to create HTTP connections to Cisco Telepresence MCU conf device, and failed due to connection errors on the Cisco Telepresence MC bridge side.
HttpNon200OKResponse	This counter represents the total number of times Unified Communicati received a non 200 OK HTTP Response from Cisco Telepresence MCU bridge, for any HTTP query sent.
OutOfResources	This counter represents the total number of times Unified Communicati attempted to allocate a conference resource from Cisco Telepresence MC bridge device and failed. For example, the attempt to allocate a confere fails, if all the resources are already in use.

Cisco TFTP Server

The Cisco Trivial File Transfer Protocol (TFTP) Server object provides information about the CiscoTFTP server. The following table contains information about Cisco TFTP server counters.

Table 80: Cisco TFTP Server

Counters	Counter Description
BuildAbortCount	This counter represents the number of times that the build process aborted v received a Build all request. This counter increases when building of device/unit/softkey/dial rules gets aborted as a result of group level change not
BuildCount	This counter represents the number of times since the TFTP service started TFTP server has built all the configuration files in response to a database c notification that affects all devices. This counter increases by one every time server performs a new build of all the configuration files.
BuildDeviceCount	This counter represents the number of devices that were processed in the la all the configuration files. This counter also updates while processing devic notifications. The counter increases when a new device is added and decrea an existing device is deleted. **Note** For 11.5 and above, you can built the configuration files and serv of caching. When a build happens, BuildDeviceCount increments. When t request from the phone, counter increases and never decreases stable monitoring is not required.
BuildDialruleCount	This counter represents the number of dial rules that were processed in the of the configuration files. This counter also updates while processing dial ru notifications. The counter increases when a new dial rule is added and decre an existing dial rule is deleted.
BuildDuration	This counter represents the time in seconds that it took to build the last con files.
BuildSignCount	This counter represents the number of security-enabled phone devices for v configuration file was digitally signed with the Unified Communications M server key in the last build of all the configuration files. This counter also u while processing security-enabled phone device change notifications.
BuildSoftKeyCount	This counter represents the number of softkeys that were processed in the l of the configuration files. This counter increments when a new softkey is a decrements when an existing softkey is deleted.
BuildUnitCount	This counter represents the number of gateways that were processed in the of all the configuration files. This counter also updates while processing un notifications. The counter increases when a new gateway is added and decre an existing gateway is deleted.
ChangeNotifications	This counter represents the total number of all the Unified Communications database change notifications that the TFTP server received. Each time tha configuration is updated in Unified Communications Manager, the TFTP s sent a database change notification to rebuild the XML file for the updated
DeviceChangeNotifications	This counter represents the number of times that the TFTP server received change notification to create, update, or delete configuration files for devic

Counters	Counter Description
DialruleChangeNotifications	This counter represents the number of times that the TFTP server recei change notification to create, update, or delete configuration files for di
EncryptCount	This counter represents the number of configuration files that were enc counter gets updated each time a configuration file is successfully encr
GKFoundCount	This counter represents the number of GK files that were found in the c counter gets updated each time a GK file is found in the cache
GKNotFoundCount	This counter represents the number of GK files that were not found in t counter gets updated each time a request to get a GK file results in the cac it
HeartBeat	This counter represents the heartbeat of the TFTP server. This incremen indicates that the TFTP server is up and running. If the count does not i means that the TFTP server is down.
HttpConnectRequests	This counter represents the number of clients that are currently requesti GET file request.
HttpRequests	This counter represents the total number of file requests (such as reques configuration files, phone firmware files, audio files, and so on.) that the handled. This counter represents the sum total of the following counter HTTP service started: RequestsProcessed, RequestsNotFound, Request RequestsAborted, and RequestsInProgress.
HttpRequestsAborted	This counter represents the total number of HTTP requests that the HT canceled (aborted) unexpectedly. Requests could get aborted if the requ cannot be reached (for instance, the device lost power) or if the file tran interrupted due to network connectivity problems.
HttpRequestsNotFound	This counter represents the total number of HTTP requests where the r was not found. When the HTTP server does not find the requested file, a sent to the requesting device.
HttpRequestsOverflow	This counter represents the total number of HTTP requests that were re the maximum number of allowable client connections was reached. The have arrived while the TFTP server was building the configuration files some other resource limitation. The Cisco TFTP advanced service parame Serving Count, sets the maximum number of allowable connections.
HttpRequestsProcessed	This counter represents the total number of HTTP requests that the HT successfully processed.
HttpServedFromDisk	This counters represents the number of requests that the HTTP server c the files that are on disk and not cached in memory.
LDFoundCount	This counter represents the number of LD files that were found in the c counter gets updated each time a LD file is found in cache memory.

Counters	Counter Description
LDNotFoundCount	This counter represents the number of LD files that were not found in cache This counter gets updated each time a request to get an LD file results in the finding it.
MaxServingCount	This counter represents the maximum number of client connections that the serve simultaneously. The Cisco TFTP advanced service parameter, Maximu Count, sets this value.
Requests	This counter represents the total number of file requests (such as requests f configuration files, phone firmware files, audio files, and so on.) that the TF handles. This counter represents the sum total of the following counters since service started: RequestsProcessed, RequestsNotFound, RequestsOverflow RequestsAborted, and RequestsInProgress.
RequestsAborted	This counter represents the total number of TFTP requests that the TFTP serve (aborted) unexpectedly. Requests could be aborted if the requesting device reached (for instance, the device lost power) or if the file transfer was inter to network connectivity problems.
RequestsInProgress	This counter represents the number of file requests that the TFTP server cu processing. This counter increases for each new file request and decreases file request that is completed. This counter indicates the current load of the server.
RequestsNotFound	This counter represents the total number of TFTP requests for which the req was not found. When the TFTP server does not find the requested file, a me sent to the requesting device. If this counter increments in a cluster that is c as secure, this event usually indicates an error condition. If, however, the cl configured as non-secure, it is normal for the CTL file to be absent (not fou results in a message being sent to the requesting device and a corresponding in this counter. For non-secure clusters, then, this normal occurrence does no an error condition.
RequestsOverflow	This counter represents the total number of TFTP requests that were rejecte the maximum number of allowable client connections was exceeded, becaus arrived while the TFTP server was building the configuration files, or becau other resource limitation. The Cisco TFTP advanced service parameter, Ma Serving Count, sets the maximum number of allowable connections.
RequestsProcessed	This counter represents the total number of TFTP requests that the TFTP se successfully processed.
SegmentsAcknowledged	This counter represents the total number of data segments that the client de acknowledged. Files get sent to the requesting device in data segments of 5 and for each 512-byte segment, the device sends the TFTP server an acknow message. Each additional data segment gets sent upon receipt of the acknow for the previous data segment until the complete file successfully gets trans the requesting device.
SegmentsFromDisk	This counter represents the number of data segments that the TFTP server r the files on disk, while serving files.

Counters	Counter Description
SegmentSent	This counter represents the total number of data segments that the TFTI Files get sent to the requesting device in data segments of 512 bytes.
SEPFoundCount	This counter represents the number of SEP files that were successfully cache. This counter gets updated each time that a SEP file is found in th
SEPNotFoundCount	This counter represents the number of SEP files that were not found in th counter gets updated each time that a request to get a SEP file produces in cache memory result.
SIPFoundCount	This counter represents the number of SIP files that were successfully f cache. This counter gets updated each time that a SIP file is found in th
SIPNotFoundCount	This counter represents the number of SIP files that were not found in th counter gets updated each time that a request to get a SIP file produces cache memory result.
SoftkeyChangeNotifications	This counter represents the number of times that the TFTP server recei change notification to create, update, or delete configuration files for so
UnitChangeNotifications	This counter represents the number of times that the TFTP server recei change notification to create, update, or delete gateway-related configu

Cisco Transcode Device

The Cisco Transcode Device object provides information about registered Cisco transcoding devices. The following table contains information on Cisco transcoder device counters.

Table 81: Cisco Transcode Device

Counters	Counter Description
OutOfResources	This counter represents the total number of times that an attempt was ma a transcoder resource from a transcoder device and failed; for example, resources were already in use.
ResourceActive	This counter represents the number of transcoder resources that are curr (active) for a transcoder device. Each transcoder resource uses two streams.
ResourceAvailable	This counter represents the total number of resources that are not active available to be used now for a transcoder device. Each transcoder resource uses two streams.
ResourceTotal	This counter represents the total number of transcoder resources that a t device provided. This counter equals the sum of the counters Resource ResourceAvailable.

Cisco Video Conference Bridge

The Cisco Video Conference Bridge object provides information about registered Cisco video conference bridge devices. The following table contains information on Cisco video conference bridge device counters.

Table 82: Cisco Video Conference Bridge

Counters	Counter Description
ConferencesActive	This counter represents the total number of video conferences that are curren (in use) on a video conference bridge device. The system specifies a confer active when the first call connects to the bridge.
ConferencesAvailable	This counter represents the number of video conferences that are not active still available on a video conference device.
ConferencesCompleted	This counter represents the total number of video conferences that have been and released on a video conference device. A conference starts when the fi connects to the bridge. The conference completes when the last call discon the bridge.
ConferencesTotal	This counter represents the total number of video conferences that are conf a video conference device.
OutOfConferences	This counter represents the total number of times that an attempt was made a video conference from a video conference device and failed because the already had the maximum number of active conferences that is allowed (as by the TotalConferences counter).
OutOfResources	This counter represents the total number of times that an attempt was made a conference resource from a video conference device and failed, for exampl all resources were already in use.
ResourceActive	This counter represents the total number of resources that are currently activ on a video conference bridge device. One resource gets used per participan
ResourceAvailable	This counter represents the total number of resources that are not active an available on a device to handle additional participants for a video conferen device.
ResourceTotal	This counter represents the total number of resources that are configured o conference bridge device. One resource gets used per participant.

Cisco Web Dialer

The Cisco WebDialer object provides information about the Cisco Web Dialer application and the Redirector servlet. The following table contains information on the CiscoWebDialer counters.

Table 83: Cisco Web Dialer

Counters	Counter Description
CallsCompleted	This counter represents the number of Make Call and End Call requests Web Dialer application successfully completed.
CallsFailed	This counter represents the number of Make Call and End Call requests unsuccessful.
RedirectorSessionsHandled	This counter represents the total number of HTTP sessions that the Red handled since the last service startup.
RedirectorSessionsInProgress	This counter represents the number of HTTP sessions that are currently b by the Redirector servlet.
RequestsCompleted	This counter represents the number of Make Call and End Call requests WebDialer servlet has successfully completed.
RequestsFailed	This counter represents the number of Make Call and End Call requests
SessionsHandled	This counter represents the total number of CTI sessions that the Cisco servlet handled since the last service startup.
SessionsInProgress	This counter represents the number of CTI sessions that the Cisco Web is currently servicing.

Cisco WSM Connector

The WSM object provides information on WSMConnectors that are configured on Unified Communications Manager. Each WSMConnector represents a physical Motorola WSM device. The following table contains information on the CiscoWSM Connector counters.

Table 84: Cisco WSM Connector

Counters	Counter Description
CallsActive	This counter represents the number of calls that are currently active (in WSMConnector device.
CallsAttempted	This counter represents the number of calls that have been attempted or WSMConnector device, including both successful and unsuccessful cal
CallsCompleted	This counter represents the number of calls that are connected (a voice established) through the WSMConnector device. The counter incremen call terminates.
CallsInProgress	This counter represents the number of calls that are currently in progres WSMConnector device. This includes all active calls. When the numbe CallsInProgress equals the number of CallsActive, this indicates that al connected.

Counters	Counter Description
DMMSRegistered	This counter represents the number of DMMS subscribers that are registere WSM.

IME Client

The IME Client object provides information about the Cisco IME client on the Unified Communications Manager server. The following table contains information on the Cisco IME client counters.

Table 85: Cisco IME Client

Counters	Counter Description
CallsAccepted	This counter indicates the number of Cisco IME calls that the Unified Comm Manager received successfully and that the called party answered, resulting call.
CallsAttempted	This counter indicates the number of calls that the Unified Communications received through Cisco IME. This number includes accepted calls, failed ca busy, no-answer calls. The counter increments each time that Unified Comm Manager receives a call through Cisco IME.
CallsReceived	This counter indicates the number of calls that Unified Communications M receives through Cisco IME. This number includes accepted calls, failed ca busy, no-answer calls. The counter increments on call initiation.
CallsSetup	This counter indicates the number of Cisco IME calls that Unified Commu Manager placed successfully and that the remote party answered, resulting call.
DomainsUnique	This counter indicates the number of unique domain names of peer enterpris Cisco IME client discovered. The counter serves as an indicator of overall usage.
FallbackCallsFailed	This counter indicates the total number of failed fallback attempts.
FallbackCallsSuccessful	This counter indicates the total number of Cisco IME calls that have fallen b PSTN mid-call due to a quality problem. The counter includes calls initiated received by this Unified Communications Manager.
IMESetupsFailed	This counter indicates the total number of call attempts for which a Cisco I was available but that were set up through the PSTN due to a failure to con target over the IP network.
RoutesLearned	This counter indicates the total number of distinct phone numbers that the C has learned and that are present as routes in the Unified Communications M routing tables. If this number grows too large, the server may exceed the pe limit, and you may need to add additional servers to your cluster.

Counters	Counter Description
RoutesPublished	This counter indicates the total number of DIDs that were published suc the IME distributed cache across all Cisco IME client instances. The cou a dynamic measurement that gives you an indication of your own provi and a sense of how successful the system has been in storing the DIDs ir
RoutesRejected	This counter indicates the number of learned routes that were rejected be administrator restricted the particular number or domain. This counter p indication of the number of cases where a VoIP call cannot happen in the f of the blocked validation.
VCRUploadRequests	This counter indicates the number of voice call record (VCR) upload rec Unified Communications Manager has sent to the Cisco IME server to the IME distributed cache.

IME Client Instance

The IME Client Instance object provides information about the Cisco IME client instance on the Unified Communications Manager server. The following table contains information on the Cisco IME client instance counters.

Table 86: IME Client

Counters	Counter Description
IMEServiceStatus	This counter indicates the overall health of the connection to the Cisco for a particular Cisco IME client instance (Unified Communications Ma following values may display for the counter: • 0—Indicates an unknown state (which may mean that the Cisco IM not active). If the value specifies 0, an alert gets generated once per hour while t remains in the unknown state. • 1—Indicates a healthy state; that is, the Cisco IME service is activ Unified Communications Manager has successfully established a c its primary and backup servers for the Cisco IME client instance, i • 2—Indicates an unhealthy state; that is, the Cisco IME service is a Unified Communications Manager has not successfully established to its primary and backup servers for the Cisco IME client instance,

SAML Single Sign-On

The following table contains information about SAML Single Sign-On counters.

Table 87: SAML Single Sign-On Counters

Counter	Counter description
SAML_REQUESTS	This counter represents the total number of SAML requests sent to the configured Identity Provider.
SAML_RESPONSES	This counter represents the total number of SAML responses received from the configured Identity Provider.

Additionally, the following SAML SSO counters are also displayed in the Unified RTMT but they are not functional in Unified Communications Manager 10.0(1):

- OAUTH_TOKENS_ISSUED
- OAUTH_TOKENS_ACTIVE
- OAUTH_TOKENS_VALIDATED
- OAUTH_TOKENS_EXPIRED
- OAUTH_TOKENS_REVOKED

Cisco IVR Device

This object provides information about registered Cisco Interactive Voice Response (IVR) devices.

Counters	Counter Description
ResourceTotal	This represents the total number of IVR resources configured for this IVR device.
ResourceActive	This represents the total number of IVR resources that are currently active for this IVR device.
ResourceAvailable	This represents the total number of resources that are not active and are still available to be used at the current time for the IVR device.
OutOfResources	This represents the total number of times an attempt was made to allocate an IVR resource from this IVR device and failed, because all the resources were in use.

IM and Presence Service Counters

Cisco Client Profile Agent

This object provides information about the Cisco Client Profile (SOAP) interface.

The following table contains information about client profile agent counters.

Table 88: Cisco Client Profile Agent counters

Counters	Counter Descriptions
SoapCrossClusterRedirect	This counter represents the number of login requests recei in a peer cluster.
SoapLoginFailures	This counter represents the number of failed login reques
SoapNodeRedirect	This counter represents the number of login requests recei node.

Cisco Presence Engine

The Cisco Presence Engine object provides information about the SIP messages that the Presence Engine receives and sends.

The following table contains information about Cisco Presence Engine performance counters.

Table 89: Cisco Presence Engine counters

Counters	Counter Description
Subscribe	
SubscribesReceived	This counter represents the number of SUBSCRIBE messages re refreshes, fetches & unsubscribes.
SubscribesSent	This counter represents the total number of SUBSCRIBE mess
SubscribesReceivedPresence	This counter represents the number of SUBSCRIBE messages presence.
SubscribesReceivedProfileConfig	This counter represents the number of SUBSCRIBE messages profileconfig.
SubscribesInitial	This counter represents the number of initial non-calendar SU
SubscribesRefresh	This counter represents the number of non-calendar refresh SU
SubscribesFetch	This counter represents the number of non-calendar fetch SUB
SubscribesRemove	This counter represents the number of non-calendar remove SU

Counters	Counter Description
ActiveSubscriptions	This counter represents the number of non-calendar subscriptions
SubscribesRedirect3xx	This counter represents the number of SUBSCRIBE messages red
SubscribesRejected4xx	This counter represents the number of SUBSCRIBE messages rej
SubscibesRejected5xx	This counter represents the number of SUBSCRIBE messages rej
SubscibesRejected6xx	This counter represents the number of SUBSCRIBE messages rej
SubcribesRejectedWith503	This counter represents the number of SUBSCRIBE messages rej
SubscriptionActiveSentForeign	This counter represents the number of active subscriptions sent by
SubscriptionActiveReceivedFrom Foreign	This counter represents the number of active subscriptions receive
WatcherInfoPresenceSubscriptions	This counter represents the number of watcher-info presence subs
Calendar	
ActiveCalendarSubscriptions	This counter represents the n.umber of calendar subscriptions that
SubscribesSentCalendarInitial	This counter represents the number of initial SUBSCRIBE messag
SubscribesSentCalendarRefresh	This counter represents the number of refresh SUBSCRIBE messa
SubscribesSentCalendarRetry	This counter represents the number of retry SUBSCRIBE messag
SubscribesReceivedCalendar	This counter represents the number of SUBSCRIBE messages rec calendar.
NotifiesReceivedCalendar	This counter represents the number of NOTIFY messages by the
NotifiesSentCalendar	This counter represents the number of NOTIFY messages sent fro
MeetingsStarted	This counter represents the number of meetings that were started
MeetingsEnded	This counter represents the number of meetings that were ended t
Publish	
PublicationsProcessed	This counter represents the number of successful publications pro
PublishInitial	This counter represents the number of initial PUBLISH messages
PublishRefresh	This counter represents the number of refresh PUBLISH message
PublishModify	This counter represents the number of modify PUBLISH message
PublishRemove	This counter represents the number of remove PUBLISH message
Notify	
NotificationsInQueue	This counter represents the number of the existing number of outgo

Counters	Counter Description
NotifiesSent	This counter represents the number of successful NOTIFY me
NotifiesReceived	This counter represents the number of NOTIFY messages rece
NotifiesSentPresence	This counter represents the number of NOTIFY messages sent
NotifiesSentProfileConfig	This counter represents the number of NOTIFY messages sent fr
NotifiesRetried	This counter represents the number of NOTIFY messages sent
NotifiesTimedouts	This counter represents the number of NOTIFY messages that
NotifiesRejected3xx	This counter represents the number of NOTIFY messages reje
NotifiesRejected4xx	This counter represents the number of NOTIFY messages reje
NotiffiesRejected5xx	This counter represents the number of NOTIFY messages reje
NotifiesRejected503	This counter represents the number of NOTIFY messages reje
NotifiesRejected6xx	This counter represents the number of NOTIFY messages reje
WatcherInfoPresenceNotifications	This counter represents the number of watcher-info presence n
WatcherInfoPresenceSubscriptions	This counter represents the number of watcher-info presence s
HighWaterMark	
HighWaterMark	This counter represents the number of times the load high wat
Active Views	
ActiveViews	This counter represents the number of Active Views in the Pre
Active Resources	
ActiveResources	This counter represents the number of active resources in the P
JSM	
ActiveJsmSessions	This counter represents the number of client emulation session
XMPP	
XMPPPresenceReceived	This counter represents the number of XMPP presence packets
XMPPPresenceFiltered	This counter represents the number of XMPP presence packets
XMPPPresenceNotificationsSent	This counter represents the number of composed presence upd
XMPPIMReceived	This counter represents the number of XMPP Instant Message
XMPPIMSent	This counter represents the number of XMPP Instant Message
XMPPIMTcInviteErrors	This counter represents the number of XMPP TC Invites rejec

Counters	Counter Description
XMPPIMResourceNotFoundErrors	This counter represents the number of XMPP Instant Message pac
XMPPIMIgnored	This counter represents the number of XMPP Instant Message pac
XMPPIMGoneGenerated	This counter represents the number of gone messages sent to the F
RFIErrors	This counter represents the number of errors when sending XMPP
RFIMessageQueueSize	This counter represents the current number of XMPP Messages th
SIP	
SIPIMReceived	This counter represents the number of SIP Instant Message packet
SIPIMSent	This counter represents the number of SIP Instant Message packet
SIPIMGoneGenerated	This counter represents the number of gone messages sent to the F
SIPIMRetry	This counter represents the number of SIP Instant Message resent
SIPIMTimeout	This counter represents the number of SIP Instant Message packet
SIPIMReject3xx	This counter represents the number of 3xx errors when attempting
SIPIMReject4xx	This counter represents the number of 4xx errors when attempting
SIPIMReject5xx	This counter represents the number of 5xx errors when attempting
SIPIMReject6xx	This counter represents the number of 6xx errors when attempting
ActiveIMSessions	This counter represents the number of Active Instant Message ses
Roster Sync	
RosterSyncAddBuddySuccess	This counter represents the number of successful add buddy reque
RosterSyncAddBuddyFailure	This counter represents the number of failed add buddy requests p
RosterSyncUpdateBuddySuccess	This counter represents the number of successful update buddy rec
RosterSyncUpdateBuddyFailure	This counter represents the number of failed update buddy request
RosterSyncDeleteBuddySuccess	This counter represents the number of successful delete buddy req
RosterSyncDeleteBuddyFailure	This counter represents the number of failed delete buddy requests
RosterSyncSubscribeSuccess	This counter represents the number of successful subscribe reques
RosterSyncSubscribeFailure	This counter represents the number of failed subscribe requests pr
RosterSyncUnSubscribeSuccess	This counter represents the number of successful unsubscribe requ
RosterSyncUnSubscribeFailure	This counter represents the number of failed unsubscribe requests
PolicyUpdateSent	This counter represents the number of privacy policy update sent t

Counters	Counter Description
PolicyUpdateReceived	This counter represents the number of privacy policy update re
RosterSyncUnSubscribedSuccess	This counter represents the number of successful unsubscribed
RosterSyncUnSubscribedFailure	This counter represents the number of failed unsubscribed requ

Cisco Server Recovery Manager

This object provides information about the Cisco Server Recovery Manager (SRM) state. The following table contains information about SRM counters.

Table 90: Cisco Server Recovery Manager Counters

Counters	Counter Descriptions
SRMState	This counter represents the state of the SRM. • 0 = Unknown • 1 = Initializing • 2 = Idle • 3 = Active Normal • 4 = Backup Activated • 5 = Taking Over • 6 = Taking Back • 7 = Failing Over • 8 = Failed Over • 9 = Failed Over Affected Service • 10 = Falling Back • 11 = Failed • 12 = Down State

Cisco SIP Proxy

The following table contains information about Cisco SIP Proxy counters.

Table 91: Proxy counters

Counters	Counter Descriptions
CTIGWConferenceReq	This counter represents the number of conference call reques

Counters	Counter Descriptions
CTIGWInboundCalls	This counter represents the number of inbound calls received by
CTIGWLineOpenRequest	This counter represents the number of LineOpen requests receiv
CTIGWMakeCallRequest	This counter represents the number of MakeCall requests receive
CTIGWRefreshCount	This counter represents the number of INVITE Refreshes receiv MOC client.
CTIGWRetrieveReq	This counter represents the number of retrieve call requests recei
CTIGWSip4XXRes	This counter represents the number of SIP 4XX response sent by
CTIGWSip5XXRes	This counter represents the number of SIP 5XX response sent by
CTIGWSSXrefReq	This counter represents the number of single step transfer call re
CTIGWUsersAuthorized	This counter represents the number of users authorized by CTIG
CTIGWUsersCurrentlyAuthorized	This counter represents the number of users currently logged int
CTIGWXrefReq	This counter represents the number of transfer call requests recei
HttpRequests	This counter represents the number of HTTP requests processed.
IMCTRLActiveSessions	This counter represents the current number of active federated I
IMGWActiveSessions	This counter represents the current number of active SIP XMPP
IMGWClientMessageSent	This counter represents the current number of SIP Messages sen
IMGWPeMessageReceived	This counter represents the current number of SIP Messages rece
IMGWPeMessageSent	This counter represents the current number of SIP Messages sen
Ipc_Requests	This counter represents the number of IPC requests from the TC
NumIdleSipdWorkers	This counter represents the number of idle sipd worker processe
NumSipdWorker	This counter represents the number of sipd worker processes at a
Proxy_Due_Timer_Events	This counter represents the number of past-due timer events that
Proxy_Timer_Events	This counter represents the number of expired timer events.
PWSAppUserLoginRequest	This counter represents the number of Application User login re
PWSAppUserLogoutRequest	This counter represents the number of Application User logout r
PWSEndpointExpired	This counter represents the number of subscriptions that expire b
PWSEndpointRefreshRequest	This counter represents the number of Endpoint refresh requests
PWSEndUserLoginRequest	This counter represents the number of End User login requests r

Counters	Counter Descriptions
PWSEndUserLogoutRequest	This counter represents the number of End User logout reque
PWSGetPolledPresenceRequest	This counter represents the number of GetPolledPresence req
PWSGetSubscribedPresenceRequest	This counter represents the number of GetSubscribedPresenc
PWSPresenceNotifies	This counter represents the number of Presence Notifications
PWSRegisterEndpointRequest	This counter represents the number of Register Endpoint requ
PWSSetPresenceRequest	This counter represents the number of SetPresence requests r
PWSSipNotifies	This counter represents the number of SIP Notifies received
PWSSipPublishRequests	This counter represents the number of SIP Publish requests s
PWSSipSubscribeRequests	This counter represents the number of SIP Subscribe requests
PWSSipUnpublishRequests	This counter represents the number of SIP Unpublish request
PWSSipUnsubscribeRequests	This counter represents the number of SIP Unsubscribe reque
PWSSubscribeExpired	This counter represents the number of endpoint registrations
PWSSubscribeRefreshRequest	This counter represents the number of Subscribe refresh requ
PWSSubscribeRequest	This counter represents the number of Subscribe requests rec
PWSUnregisterEndpointRequest	This counter represents the number of Unregister Endpoint re
PWSUnsubscribeRequest	This counter represents the number of Unsubscribe requests
ServerLoadStatus	This counter represents the Server load status on scale of 0 (i
SIPClientImMessage	This counter represents the number of SIP Client Instant Mes
SIPClientRegistered	This counter represents the number of SIP Client REGISTER
SIPClientRegisterFailed	This counter represents the number of failed SIP Client REG
Sip_Tcp_Requests	This counter represents the number of sip requests received c
Sip_Udp_Requests	This counter represents the number of sip requests received c
SIPInviteRequestIn	This counter represents the number of INVITE requests recei
SIPInviteRequestInForeign	This counter represents the current number of INVITE reque
SIPInviteRequestOut	This counter represents the number of INVITE requests sent
SIPInviteRequestOutForeign	This counter represents the current number of INVITE reque
SIPMessageRequestIn	This counter represents the number of MESSAGE requests re
SIPMessageRequestInForeign	This counter represents the current number of MESSAGE req

Counters	Counter Descriptions
SIPMessageRequestOutForeign	This counter represents the current number of MESSAGE reques
SIPNotifyRequestIn	This counter represents the number of NOTIFY requests receive
SIPNotifyRequestInForeign	This counter represents the current number of NOTIFY requests
SIPNotifyRequestOutForeign	This counter represents the current number of NOTIFY requests
SIPRegisterRequestIn	This counter represents the number of REGISTER requests recei
SIPRequestInForeign	This counter represents the current number of requests received
SIPRequestOutForeign	This counter represents the current number of requests sent direc
SIPRetransmits	This counter represents the number of retransmits executed by th
SIPSubscribeRequestIn	This counter represents the number of SUBSCRIBE requests rec
SIPSubscribeRequestInForeign	This counter represents the current number of SUBSCRIBE reque
SIPSubscribeRequestOutForeign	This counter represents the current number of SUBSCRIBE requ

Cisco Sync Agent

This object provides information about the number of errors that occur during synchronization. The following table contains information about the Cisco Sync Agent counter.

Table 92: Cisco Sync Agent Counter

Counter	Counter Description
NumberOfSyncErrors	This counter displays the number of errors that occur during synchronization. The counter resets to 0 when the Cisco sync agent is restarted. This counter is always 0 on the subscriber node.

Cisco XCP Auth Component

The following table contains information about Cisco XCP Authentication performance counters.

Table 93: Cisco XCP Auth Component Counters

Counter	Counter description
SASLPlainSuccess	This counter represents the total number of successful SASL plain authentication attempts.
SASLPlainFailed	This counter represents the total number of failed SASL plain authentication attempts.

Counter	Counter description
VtgTokenSuccess	This counter represents the number of successful vtg-token authentication attempts.
VtgTokenFailed	This counter represents the number of failed vtg-token authentication attempts.
FailedLicense	This counter represents the total number of failed authentication attempts due to no license.
FailedSASLCredentials	This counter represents the total failed SASL plain authentication attempts due to invalid username and password.
FailedTokenCredentials	This counter represents the total failed vtg-token authentication attempts due to invalid username and password.

Cisco XCP CM

The following table contains information about Cisco XCP Connection Manager (CM) performance counters.

Table 94: Cisco XCP CM Counters

Counter	Counter Description
CmConnectedSockets	This counter represents the number of connected sockets in the Web Connection Manager component.
CmFailedRequests	This counter represents the total number of failed connection requests.

Cisco XCP Component Stanza Traffic

The following table provides information about Cisco XCP Component Stanza Traffic performance counters.

Table 95: Cisco XCP Component Stanza Traffic Counters

Counter	Counter description
CompStanzaBytesSent	This counter represents the number of bytes sent on a per-component basis.
CompStanzaBytesRecv	This counter represents the number of bytes received on a per-component basis.
CompStanzaErrorsRecv	This counter represents the number of errors sent on a per-component basis.

Counter	Counter description
CompStanzaErrorsSent	This counter represents the number of errors received on a per-component basis.
CompStanzaPacketsDropped	This counter represents the number of packets dropped on a per-component basis.
CompStanzaStanzasSent	This counter represents the number of stanzas sent on a per-component basis.
CompStanzaStanzasRecv	This counter represents the number of stanzas received on a per-component basis.
CompStanzaMessagePacketsSent	This counter represents the number of message packets sent on a per-component basis.
CompStanzaMessagePacketsRecv	This counter represents the number of message packets received on a per-component basis.
CompStanzaPresencePacketsSent	This counter represents the number of presence packets sent on a per-component basis.
CompStanzaPresencePacketsRecv	This counter represents the number of presence packets received on a per-component basis.
CompStanzaIQPacketsRecv	This counter represents the number of IQ packets received on a per-component basis.
CompStanzaIQPacketsSent	This counter represents the number of IQ packets sent on a per-component basis.

Cisco XCP JDS

The following table contains information about the Cisco XCP JDS performance counters.

Table 96: Cisco XCP JDS Counters

Counter	Counter description
JdsLDAPSuccess	This counter represents the total number of successful LDAP searches.
JdsLDAPFailed	This counter represents the total number of failed LDAP searches.
JdsInvalidRequests	This counter represents the number of invalid LDAP search requests rejected by Cisco XCP JDS and not sent to LDAP.

Cisco XCP JSM

The following table contains information about the XCP JSM performance counters.

Table 97: Cisco XCP JSM Counters

Counter	Counter description
JsmMessagesIn	This counter represents the number of message stanzas received by the JSM component.
JsmMessagesOut	This counter represents the number of message stanzas sent by the JSM component.
JsmPresenceIn	This component represents the number of presence stanzas received by the JSM component.
JsmPresenceOut	This component represents the number of presence stanzas sent by the JSM component.
JsmIMSessions	This counter represents the total number of active JSM sessions on the IM and Presence service. On IM and Presence, the Presence Engine creates a JSM client emulation session for every licensed user at startup time. Additional JSM sessions are also created while users are signed in on their clients. Users may be signed in on multiple clients simultaneously resulting in multiple additional JSM sessions per user.
JsmOnlineUsers	This counter represents the number of users with one or more JSM sessions. On IM and Presence, the Presence Engine creates a JSM client emulation session for every licensed user. The value of this counter should therefore match the value of the Presence Engine ActiveJsmSessions counter.
JsmLoginRate	This counter represents the current login rate being tracked by the JSM component.
JsmSuccessfulLogins	This counter represents the total number of successful logins.
JsmFailedLogins	This counter is always 0 on IM and Presence. For details on failed login attempts, see the Cisco XCP Auth Component counters.
JsmTotalMessagePackets	This counter represents the total message packets processed by the JSM component.
JsmTotalPresencePackets	This counter represents the total presence packets processed by the JSM component.
JsmTotalIQPackets	This counter represents the total number of IQ packets processed by the JSM.

Counter	Counter description
JsmMsgsInLastSlice	This counter represents the total messages processed by the JSM component in last time slice.
JsmAverageMessageSize	This counter represents the average message size processed by the JSM component.
JsmTotalStateChangePackets	This counter is always set to 0 on IM and Presence and is reserved for future use.
JsmStateChangePacketsInSlice	This counter is always set to 0 on IM and Presence and is reserved for future use.
JsmAverageStateChangeSize	This counter is always set to 0 on IM and Presence and is reserved for future use.

Cisco XCP JSM IQ Namespaces

The following table contains information about the Cisco XCP JSM IQ Namespaces performance counters.

Table 98: Cisco XCP JSM IQ Namespaces

Counter	Counter description
JSM IQ Namespace	This counter represents the number of IQ packets handles on a per-namespace basis.

Cisco XCP JSM Session

The following table contains information about the Cisco XCP JSM Session performance counters.

Table 99: Cisco XCP JSM Session Counters

Counter	Counter description
JsmSessionIQIn	This counter represents IQ packets received by JSM on a per-session basis.
JsmSessionIQOut	This counter represents IQ packets sent by JSM on a per-session basis.
JsmSessionMessagesIn	This counter represents message packets received by JSM on a per-session basis.
JsmSessionMessagesOut	This counter represents message packets sent by JSM on a per-session basis.
JsmSessionPresenceIn	This counter represents presence packets received by JSM on a per-session basis.

Counter	Counter description
JsmSessionPresenceOut	This counter represents presence packets sent by JSM on a per-session basis.
JsmSessionRosterSize	This counter represents the size of the user's roster on a per-session basis.

Cisco XCP MA Basic

The following table contains information about the Cisco XCP Message Archiver Basic performance counters.

Table 100: Cisco XCP MA Basic Counters

Counter	Counter description
ReceivedPackets	This counter represents the total number of packets received by IM and Presence and archived by the Message Archiver component.
SentPackets	This counter represents the total number of packets sent from IM and Presence and archived by the Message Archiver component.
SuccessfulDBWriters	This counter represents the confirmed IMs records written to the Database.
FailedDBWriters	This counter represents the failed attempts to write to the Database.
PacketsDropped	This counter represents the number of packets Message Archiver receives but are not written to the Database, for example, isTyping packets.
DBQueueSize	This counter represents the number of packets that Message Archiver has queued pending write to Database.

Cisco XCP Managed File Transfer

The following table contains information about the Cisco XCP Managed File Transfer performance counters.

Table 101: Managed File Transfer Counters

Counter	Counter description
MFTBytesDownloadedLastTimeslice	This counter represents the number of bytes downloaded during the last reporting interval (typically 60 seconds).
MFTBytesUpoadedLastTimeslice	This counter represents the number of bytes uploaded during the last reporting interval (typically 60 seconds).

Counter	Counter description
MFTFilesDownloaded	This counter represents the total number of files downloaded.
MFTFilesDownloadedLastTimeslice	This counter represents the number of files downloaded during the last reporting interval (typically 60 seconds).
MFTFilesUploaded	This counter represents the total number of files uploaded.
MFTFilesUploadedLastTimeslice	This counter represents the number of files uploaded during the last reporting interval (typically 60 seconds).

Cisco XCP Router

The following table contains information about the Cisco XCP Router performance counters.

Table 102: Cisco XCP Router Counters

Counter	Counter description
RouterNormalPackets	This counter represents the total number of normal packets handled by the Cisco XCP router.
RouterXdbPackets	This counter represents the total number of xdb packets handled by the Cisco XCP router.
RouterRoutePackets	This counter represents the total number of route packets handled by the Cisco XCP router.
RouterLogPackets	This counter represents the total number of log packets handled by the Cisco XCP router.

Cisco XCP SIP S2S

The following table contains information about Cisco XCP SIP Server-to-Server (S2S) performance counters.

Table 103: Cisco SIP S2S counters

Counter	Counter description
SIPS2SIncomingDomains	This counter represents the total foreign domains with incoming subscriptions.
SIPS2SOutgoingDomains	This counter represents the total foreign domains with outgoing subscriptions.
SIPS2SSubscriptionsOut	This counter represents the total active SIP outgoing subscriptions.
SIPS2SSubscriptionsIn	This counter represents the total active SIP incoming subscriptions.

Counter	Counter description
SIPS2SSubscriptionsPending	This counter represents the total pending SIP outgoing subscriptions.
SIPS2SNotifyIn	This counter represents the total SIP NOTIFY messages received.
SIPS2SNotifyOut	This counter represents the total SIP NOTIFY messages sent.
SIPS2SMessageIn	This counter represents the total SIP MESSAGE messages received.
SIPS2SMessageOut	This counter represents the total SIP MESSAGE messages sent.
SIPS2SByeIn	This counter represents the SIP BYE messages received.
SIPS2SInviteIn	This counter represents the SIP INVITE messages received.
SIPS2SInviteOut	This counter represents the SIP INVITE messages sent.

Cisco XCP S2S

The following table contains information about Cisco XCP Server-to-Server (S2S) performance counters.

Table 104: Cisco XCP S2S Counters

Counters	Counter description
S2SIncomingDomains	This counter represents the total foreign domains with incoming subscriptions.
S2SOutgoingDomains	This counter represents the total foreign domains with outgoing subscriptions.
S2SFailedDialbackIn	This counter represents the total failed incoming dialback attempts.
S2SFailedDialbackOut	This counter represents the total failed outgoing dialback attempts.

Cisco XCP TC

The following table contains information about Cisco XCP Text Conferencing (TC) performance counters.

Table 105: Cisco XCP TC Counters

Counter	Counter description
TcTotalRooms	This counter represents the total number of all types of text chat rooms.
TcAdhocRooms	This counter represents the total number of ad hoc text chat rooms.
TcPersistentRooms	This counter represents the total number of permanent text chat rooms.
TcCreatedRooms	This counter represents the total number of created text chat rooms.
TcDeletedRooms	This counter represents the total number of deleted text chat rooms.
TcMessagesIn	This counter represents the total number of group chat messages received.
TcMessagesOut	This counter represents the total number of group chat messages sent.
TcDirectedMessagesIn	This counter represents the total number of private and invite messages received.
TcMessagesPersisted	This counter represents the total number of messages archived to the external database.
TcMessagesIgnored	This counter represents the total number of messages not archived to the external database.

Cisco XCP TC Room

The following table contains information about the Cisco XCP TC Room performance counters.

Table 106: Cisco XCP TC Room Counters

Counter	Counter description
TCRoomNumOccupants	This counter represents the number of occupants on a per-chat room basis.
TCRoomBytesSent	This counter represents the number of bytes sent on a per-chat room basis.

Counter	Counter description
TCRoomBytesRecv	This counter represents the number of bytes received on a per-chat room basis.
TCRoomStanzasSent	This counter represents the number of stanzas sent on a per-chat room basis
TCRoomStanzasRecv	This counter represents the number of stanzas received on a per-chat room basis.
TCRoomMsgPacketSent	This counter represents the number of messages sent on a per-chat room basis.
TCRoomMsgPacketsRecv	This counter represents the number of messages received on a per-chat room basis.
TCRoomPresencePacketsSent	This counter represents the number of presence packets sent on a per-chat room basis.
TCRoomPresencePacketsRecv	This counter represents the number of presence packets received on a per-chat room basis.
TCRoomIQPacketsSent	This counter represents the number of IQ packets sent on a per-chat room basis.
TCRoomIQPacketsRecv	This counter represents the number of iq packets received on a per-chat room basis.

Cisco XCP WebCM

The following table contains information about the Cisco XCP Web Connection Manager performance counters.

Table 107: Cisco XCP WebCM Counters

Counter	Counter description
WebCMConnectedSockets	This counter represents the cumulative total number of connected XMPP client sessions.
WebCMFailedRequests	This counter represents the total number of failed connection requests.

Cisco Unity Connection Counters

CUC Data Store

The CUC Data Store object provides information about registered database usage by Cisco Unity Connection. The following table contains information about CUC Data Store counters.

Table 108: CUC Data Store

Counters	Counter Descriptions
Allocated Memory [kb]	Amount of database server virtual-address space [in kilobytes].
Database Connections	Total number of connections to the database server.
Disk Reads	Total number of disk read operations for all data chunks (rows) in the last 30 seconds.
Disk Reads/second	Number of read operations from the disk per second.
Disk Writes	Number of write operations to the disk in the last 30 seconds.
Disk Writes/second	Number of write operations to the disk per second.
Shared Memory [kb]	Amount of database server shared memory used [in kilobytes].

CUC Data Store: Databases

The CUC Data: Databases object provides information about the databases that Cisco Unity Connection uses.

Table 109: CUC Data Store: Databases

Counters	Counter Descriptions
Disk Reads/chunk	Number of read operations for the selected data chunk
Disk Writes/chunk	Number of write operations for the selected data

CUC Digital Notifications

The CUC Digital Notifications object provides information about the total number of SMS and SMTP notifications. The following table contains information about CUC Digital Notification counters.

Table 110: CUC Digital Notifications

Counters	Counter Descriptions
SMS Notifications Failed	The total number of SMS notifications failing to connect.
SMS Notifications Total	The total number of SMS notifications sent to subscribers by Cisco Unit
SMTP Notifications Total	The total number of SMTP notifications that Cisco Unity Connection sent
HTML Notifications with Summary of voice messages	The counter to maintain count of summary notifications.
HTML Notifications with Summary of voice messages in Last One Minute	The counter to maintain count of summary notifications sent in last one
Scheduled Notifications Total	The counter to maintain count of scheduled summary notifications sent
Scheduled Notifications in Last One Minute	The counter to maintain count of scheduled summary notifications sent i
Scheduled Notifications dropped due to Parent Schedule off	The counter to maintain count of scheduled summary notifications drop because the parent schedule was turned off.
Scheduled Notifications dropped due to Parent Schedule off in Last One Minute	The counter to maintain count of scheduled summary notifications drop in last one minute because the parent schedule was turned off.
Missed Call Notifications Total	The total number of missed call notifications sent fromCisco Unity Con

CUC Directory Services

The CUC Directory Services object provides information about the performance of the directory services that Cisco Unity Connection uses.

The Directory Search Duration Average [s] counter represents the average time [in seconds] to complete a directory search request for the Cisco Unity Connection server.

CUC Feeder

The CUC Feeder object keeps a count of total requests processed by the Feeder. The following table contains information about CUC Feeder counters.

Counters	Counter Descriptions
Total objects requests processed	The total number of HTTP[S]/CCI objects requests processed by Feeder.
Objects requests processed in last 15 minutes	The total number of HTTP[S]/CCI objects requests processed by Feeder in last 15 minutes.
Total object requests processed	The total number of HTTP[S]/CCI object requests processed by Feeder.

Counters	Counter Descriptions
Object requests processed in last 15 minutes	The total number of HTTP[S]/CCI object requests processed by Feeder in last 15 minutes.

CUC Mailbox Sync

The Mailbox Sync service synchronizes messages between Unity Connection and Exchange.

The following table contains information about Mailbox Sync counters.

Counters	Counter Description
Active thread count	Cisco Unity Connection maintains threads for synchronization of voicemail from Cisco Unity Connection to Exchange server and vice-versa. At any moment, this counter specifies the number of threads that are actively in use for voicemail synchronization.
Background queue size	Mailbox sync has three types of priority queues: Background, Normal, and Time-Sensitive. Background queue is the lowest priority queue. This queue has items that are scheduled because of background re-synchronization of each mailbox hourly.
Normal queue size	Normal queue has moderate priority. This queue has items that are scheduled because of messaging operation (such as message CREATE, READ, UNREAD, DELETE) performed by user or any configuration update by administrator on Unified Messaging page on Cisco Unity Connection Administration.
Time sensitive queue size	Time sensitive queue has highest priority. This queue has such items that are scheduled because of keep-alive message sent by Cisco Unity Connection to Exchange server to keep subscription alive. This is applicable for 2003 Exchange server only.
Total connection errors	It specifies the number of times the CuMbxSync process fails to retrieve or update some data from database.
Total Mailbox Adds	It specifies the number of times a user mailbox has been setup for subscription. Any communication error between Unity Connection and Exchange, results in user mailbox remove and re-add.

Counters	Counter Description
Total Mailbox Removes	It specifies the number of times a user mailbox has been setup for un-subscription. Any communication error between Unity Connection and Exchange, results in user mailbox remove and re-add.
Total Resyncs	It specifies the total number of times user mailbox is resynchronized with Exchange server. Cisco Unity Connection does background resynchronization for all the user mailboxes hourly.
Total Retries	Whenever there is a communication failure between Cisco Unity connection and Exchange server, Unity Connection does mailbox synchronization retry for particular user mailbox. This counter specifies the count of such occurrences.
Total Work Items	It specifies number of times any messaging operation, such as CREATE, READ, UNREAD, and DELETE, has been performed on any user mailbox.

CUC Mailbox Sync on Gmail Server

Google Workspace service synchronizes messages between Unity Connection and mailbox on Gmail server. The following table contains information about its counters.

Counters	Counter Description
Active Thread Count From Gmail To Connection	This counter will record the count of currently active threads performing synchronization from Gmail server to Unity Connection
Active Thread Count From Connection to Gmail	This counter will record the count of currently active threads performing synchronization from Unity Connection to Gmail server.
Outstanding Request of Gmail to Connection	This counter will record the count of queue size for messages which are going to be synchronized from Gmail server to Unity Connection at specific point of time.
Outstanding Request of Connection to Gmail	This counter will record the count of queue size for messages which are going to be synchronized from Unity Connection to Gmail server at specific point of time.
Total Database Connection Errors	This counter will record all the operations which failed in performing database functionality while synchronizing the message.

Counters	Counter Description
Total HTTPs Requests	This counter will record all the HTTP requests sent to Gmail server.
Total HTTPs Failure	This counter will record all the errors occurred in HTTP requests.
Total Mailbox Adds	This counter will record the total count of Unified Messaging Accounts (UMA) added on the system. (Removing a UMA will not decrease its value)
Total Mailbox Removes	This counter will record the total count of Unified Messaging Accounts(UMA) removed from system. (Adding a UMA will not decrease its value)
Total Resyncs	This counter will record the total count of resynchs done on the system.
Total Retries	This counter will record the total count of retries done for the message to be synchronized.
Read Message on Connection	This counter will record the count for messages marked read on Unity Connection in response to synchronization from Gmail server.
Unread Message on Connection	This counter will record the count for messages marked unread on Unity Connection in response to synchronization from Gmail server.
Delete Message on Connection	This counter will record the count for messages marked delete on Unity Connection in response to synchronization from Gmail server.
Create Message on Connection	This counter will record the count for messages created on Unity Connection in response to synchronization from Gmail server.
Read Message on Gmail	This counter will record the count for messages marked read on Gmail server in response to synchronization from Unity Connection.
Unread Message on Gmail	This counter will record the count for messages marked unread on Gmail server in response to synchronization from Unity Connection.
Delete Message on Gmail	This counter will record the count for messages marked delete on Gmail server in response to synchronization from Unity Connection.
Create Message on Gmail (Inbox Folder)	This counter will record the count for messages created on mailbox on Gmail server in response to synchronization from Unity Connection.

Counters	Counter Description
Create Message on Gmail (Sent Folder)	This counter will record the count for messages created on mailbox on Gmail server(Sent) in response to synchronization from Unity Connection.

CUC Message Store

The CUC Message Store object provides information about the performance of the Cisco Unity Connection message store. The following table contains information about CUC Message Store counters.

Table 111: CUC Message Store

Counters	Counter Descriptions
Bad Mail Total	Total number of messages sent to the Bad Mail folder since the last resta server.
Delivery Receipts Total	Total number of delivery receipts since the last restart of the MTA serve
Incoming Recalls	Number of incoming requests to recall local copies of messages initiate senders on other network locations.
Intersite Messages Delivered Per Minute	Number of intersite messages delivered in the last minute.
Intersite Messages Delivered Total	Total number of intersite messages delivered since the last restart of the
Intersite Messages Received Per Minute	Number of intersite messages received in the last minute.
Intersite Messages Received Total	Total number of intersite messages received since the last restart of the
Intersite Messages Total	Total number of intersite messages that have been delivered and receive last restart of the MTA server.
Local Recalls	Number of message recalls initiated by local senders on this server.
Message Size Average [kb]	The average size of the MTA at each sample in kilobytes.
Messages Delivered Total	Total number of messages delivered since the last restart of the MTA se
Messages Received Per Minute	Total number of messages received Per Minute by MTA.
Messages Received Total	Total number of messages received since the last restart of the MTA ser
Non-delivery Receipts Total	Total number of non-delivery receipts since the last restart of the MTA
Number of Items Recalled	Total number of message recalls. This number includes each individual message that was sent to multiple recipients, so this number could be mu the Total Recalls, Local and Remote performance counter.
Queued Messages Current	The number of messages currently queued in the MTA.
Read Receipts Total	Total number of read receipts since the last restart of the MTA server.

Counters	Counter Descriptions
Retries Total	Total number of retries since the last restart of the MTA server.
Total dispatch message folder items delivered	Total number of dispatch messages that have been delivered to individual u mailboxes since the MTA started. This number includes a count of each inc copy of a message sent to multiple recipients.
Total dispatch messages accepted	Total number of dispatch messages that have been accepted since the last res MTA server
Total dispatch messages delivered	Total number of dispatch messages that have been delivered since the MTA This number includes each message just once, regardless of the number of r
Total dispatch message items rejected	Total number of individual copies of dispatch messages that have been decl the last restart of the MTA server.
Total dispatch messages removed due to acceptance	Total number of dispatch messages that have been removed from user mail to the message being accepted by another user since the last restart of the M
Total recalls, local and remote	Total number of message recalls initiated by local and remote senders. This should be equal to the total of Incoming Recalls and Local Recalls perform counters.
VPIM Message Decode Duration Average [s]	The average time [in seconds] to decode voice messages in MIME format to th format.
VPIM Message Encode Duration Average [s]	The average time [in seconds] to encode voice messages to MIME format.
VPIM Messages Delivered Per Minute	The number of VPIM messages that the Cisco Unity Connection Messages delivered within a minute.
VPIM Messages Delivered Total	The total number of VPIM messages that the Cisco Unity Connection Mess delivered.
VPIM Messages Received Per Minute	The number of VPIM messages that the Cisco Unity Connection Messages received per minute.
VPIM Messages Received Total	The total number of VPIM messages that the Cisco Unity Connection Mess received.
VPIM Messages Total	The total number of VPIM messages that the Cisco Unity Connection Mess processed.
Messages Undelivered Mailbox Quota Full Notification Total	The total number of missed call notification sent when mailbox quota is ful
Video Messages Delivered Total	The total number of video messages delivered since the last restart of the M
Video Messages Delivered Per Minute	The total number of video messages delivered per minute since the last rest MTA server.
Video Messages Processed by MTA Total	The total number of video messages processed (both successful and unsucc the MTA server since the last restart of the server.

Counters	Counter Descriptions
Video Messages Processed by MTA Per Minute	The total number of video messages processed (both successful and uns the MTA server per minute since the last restart of the server.

CUC Message Store: Databases

The CUC Message Store: Databases object provides information about the message store database that Cisco Unity Connection uses.

The Messages Delivered Per Message Store counter represents the total number of messages that were delivered per message store since the last restart of the MTA server.

CUC Personal Call Transfer Rules

The CUC Personal Call Transfer Rules object provides information about the numbers and usage of the personal call transfer rules (PCTR). The following table contains information about CUC Personal Call Transfer Rules counters.

Table 112: CUC Personal Call Transfer Rules

Counters	Counter Descriptions
Applicable Rule Found	Personal call transfer rule (PCTR) call resulted in rule processing, and a transfer rule is found.
Destinations Tried	Number of destinations tried while transfer rules were applied.
PCTR Calls	Calls that are subject to personal call transfer rule (PCTR) processing: u COS is enabled for PCTR, user is a Unified Communications Manager not disabled PCTR.
Rules Evaluated	Number of rules that are evaluated during rule processing in a personal rule (PCTR) call.
Subscriber Reached	Number of times that a subscriber was reached while transfer rules were
Transfer Failed	Number of times that Cisco Unity Connection fails to transfer a call to a while personal call transfer rules were applied. Transfer failures include except when the called destination is connected, busy, or RNA or times hanging up during a transfer gets considered a transfer failure.
Voicemail Reached	Number of times that voice mail was reached while transfer rules were

CUC Phone System

The CUC Phone System object provides information about the performance of the phone system integration. The following table contains information about CUC Phone System counters.

Table 113: CUC Phone System

Counters	Counter Descriptions
Call Count Current	The current number of incoming and outgoing calls to the Cisco Unity Con server.
Call Count Total	The total number of incoming and outgoing calls to the Cisco Unity Connect
Call Duration Average [s]	The average duration [in seconds] of incoming and outgoing calls from the C Connection server.
Call Duration Total [s]	The total duration [in seconds] of incoming and outgoing calls from the Cis Connection server.
Calls Unanswered Total	The total number of unanswered calls on the Cisco Unity Connection serve
Incoming Calls CFB Current	The current number of incoming calls that were received as Call Forward B
Incoming Calls CFB Total	The total number of incoming calls that were received as Call Forward Bus
Incoming Calls CFNA Current	The current number of incoming calls that were received as Call Forward N
Incoming Calls CFNA Total	The total number of incoming calls that were received as Call Forward No
Incoming Calls Current	The current number of incoming calls.
Incoming Calls Direct Current	The current number of incoming calls that were received as direct calls.
Incoming Calls Direct Total	The total number of incoming calls that were received as direct calls.
Incoming Calls Duration Average [s]	The average duration [in seconds] of all incoming calls to the Cisco Unity C server.
Incoming Calls Duration Total [s]	The total duration [in seconds] of all incoming calls to the Cisco Unity Con server.
Incoming Calls No Info Total	The total number of incoming calls without integration information.
Incoming Calls Total	The total number of incoming calls.
Message Notification Duration Average [s]	The average time [in seconds] to complete all message notifications from t Unity Connection server.
Message Notification Duration Total [s]	The total time [in seconds] to complete all message notifications from the C Connection server.
Message Notifications Failed	The total number of message notifications that failed to connect to a destinatio
Message Notifications Total	The total number of message notifications that Cisco Unity Connection sen subscribers.
MWI Request Duration Average [ms]	The average duration [in milliseconds] of all MWI requests from the Cisco Connection server.

Counters	Counter Descriptions
MWI Request Duration Total [ms]	The total duration [in milliseconds] of all MWI requests from the Cisco Connection server.
MWI Requests Failed Total	The total number of MWI requests that failed to connect to a destination complete MWI operation.
MWI Requests Total	The total number of MWI requests that Cisco Unity Connection sent.
Outgoing Calls Duration Average [s]	The average duration [in seconds] of all outgoing calls from the Cisco Uni server.
Outgoing Calls Duration Total [s]	The total duration [in seconds] of all outgoing calls from the Cisco Unit server.
Outgoing Calls Release Transfers Completed	The number of completed release transfers from the Cisco Unity Conne
Outgoing Calls Release Transfers Failed	The number of release transfers from the Cisco Unity Connection server connect to a destination number.
Outgoing Calls Release Transfers Total	The total number of release transfers that were attempted from the Cisc Connection server.
Outgoing Calls Supervised Transfers Completed	The number of completed supervised transfers from the Cisco Unity Conn
Outgoing Calls Supervised Transfers Dropped	The number of supervised transfers from the Cisco Unity Connection se dropped while in progress.
Outgoing Calls Supervised Transfers Failed	The number of supervised transfers from the Cisco Unity Connection ser to connect to a destination number.
Outgoing Calls Supervised Transfers Total	The total number of supervised transfers from the Cisco Unity Connect
Outgoing Calls Transfers Total	The total number of release and supervised transfers that Cisco Unity C attempted.
Pager Notifications Duration Average [s]	The average time [in seconds] to complete all pager notifications from th Connection server.
Pager Notifications Duration Total [s]	The total time [in seconds] to complete all pager notifications from the Connection server.
Pager Notifications Failed	The total number of pager notifications that failed to connect to a destin
Pager Notifications Total	The total number of pager notifications that Cisco Unity Connection sent t
Port Idle Duration [s]	The total time [in seconds] that any port remains idle between incoming Cisco Unity Connection server.
Port Idle Duration Average [s]	The average time [in seconds] that any port remains idle between incon the Cisco Unity Connection server.

Counters	Counter Descriptions
Ports Idle Current	The current number of integration ports that are not in use by the Cisco Un Connection server.
Ports In Use Current	The current number of integration ports that are in use by the Cisco Unity C server.
Ports Locked	The current count of the ports that no longer respond or are otherwise unus Cisco Unity Connection.
Missed Call Total	The total number of missed call notifications triggered by theCisco Unity C server.

CUC Phone System: Ports

The CUC Phone System: Ports object provides information about the voice messaging ports on Cisco Unity Connection. The following table contains information about CUC Phone System: Ports counters.

Table 114: CUC Phone System: Ports

Counters	Counter Descriptions
Port Calls	The total number of calls that were received on this port since the Cisco Ur Connection server was last restarted. This includes all types of calls: Incom MWI dialouts, Notification dialouts, TRAP dialouts, and VPIM dialouts.
Port Idle Percent	The distribution percentage of idle ports on the Cisco Unity Connection ser
Port Usage Duration Average [s]	The average time [in seconds] that a port has been actively processing calls
Port Usage Duration Total [s]	The total time [in seconds] that a port has been actively processing calls.
Port Usage Percent	The distribution percentage of calls into ports on the Cisco Unity Connecti

CUC Replication

The CUC Replication object provides information about the replication for Cisco Unity Connection redundancy. The following table contains information about CUC Replication counters.

Table 115: CUC Replication

Counters	Counter Descriptions
File Replication Latency [s]	How long file exists before replication starts.
File Replication Latency Max [s]	Maximum file replication latency since the service started.
File Transfer Rate [kbytes/s]	Transfer rate for each replicated file.
Files Replicated Total	Number of files replicated since the service started.

Counters	Counter Descriptions
Transfer Rate [bytes/s]	Number of bytes transferred each second.

CUC Replicator: Remote Connection Locations

The CUC Replicator: Remote Connection Locations object provides information about replication with remote Connection locations. The following table contains information about CUC Replicator: Remote Connection Locations counters.

Table 116: CUC Replicator: Remote Connection Locations

Counters	Counter Descriptions
Dependencies Requests Received	The number of replication dependencies requested received from the Co location.
Dependencies Requests Sent	The number of replication dependencies requests sent to the Connectio
Message Receive Failures	The number of replication messages from this Connection location that received because of failures.
Message Send Failures	The number of replication messages to the Connection location that we because of failures.
Messages Received	The number of replication messages received from the Connection loca
Messages Sent	The number of replication messages sent to the Connection location.
NDR Messages Received	The number of replication NDR messages received from the Connectio
USN Requests Received	The number of USN request received from the Connection location. Th indicates that a USN timeout occurred on the remote node.

Connection REST Tomcat Connector

The Tomcat Hypertext Transport Protocol (HTTP) and HTTP Secure (HTTPS) Connector object provides information about Tomcat connectors.

Connection Rest Tomcat HTTP connector represents an endpoint that receives requests and sends responses. The connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when VMREST requests of application are accessed. The Secure Socket Layer (SSL) status of VMREST request URL's provide the basis for instance name for each Rest Tomcat Connector. For example, https://<IP Address>:8443 for SSL or http://<IP Address>:8080 for non-SSL.

The following table contains information about the Connection Rest Tomcat connector counters.

Counter	Counter Description
Errors	The total number of HTTP errors (for example, `401 Unauthorized`) that the connector encountered.

Counter	Counter Description
MBytesReceived	The amount of data that the connector received.
MBytesSent	The amount of data that the connector sent.
Requests	The total number of request that the connector handled.
ThreadsTotal	The current total number of request processing threads, including available and in-use threads, for the connector.
ThreadsMax	The maximum number of request processing threads for the connector. Each incoming VMREST request requires a thread for the duration of that request. If more simultaneous requests are received than the currently available request processing threads can handle, additional threads are created up to the configured maximum shown in this counter. If still more simultaneous requests are received, they accumulate within the server socket that the connector created, up to an internally specified maximum number. Any further simultaneous requests receive connection refused messages until resources are available to process them.
ThreadsBusy	This counter represents the current number of busy/in-use request processing threads for the connector.

Connection REST Tomcat JVM

The Cisco Tomcat Java Virtual Machine (JVM) object provides information about the pool of common resource memory used by VMREST requests URL’s. The dynamic memory block stores all objects that Tomcat and its VMREST requests create.

The following table contains information about the Connection REST Tomcat JVM counters.

Counters	Counter Description
KBytesMemoryFree	The amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. When the amount of free dynamic memory is low, more memory is automatically allocated, and total memory size (represented by the KbytesMemoryTotal counter) increases but only up to the maximum (represented by the KbytesMemoryMax counter). You can determine the amount of memory in use by subtracting KBytesMemoryFree from KbytesMemoryTotal.

Counters	Counter Description
KBytesMemoryMax	The amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine.
KBytesMemoryTotal	The current total dynamic memory block size, including free and in-use memory, of Tomcat Java Virtual Machine.

Connection REST Tomcat Web Application

Cisco Rest Tomcat Web Application object provides information about how to run VMREST request URL's.

VMREST request URL's provide the basis for instance name for each Rest Tomcat Web Application, as explained in the following examples:

- Cisco Unified Communications Manager Administration (https://<IP Address>:8443/ccmadmin) is identified by ccmadmin.
- Cisco Unified Serviceability (https://<IP Address>:8443/ccmservice) is identified by ccmservice.
- Cisco Unified Communications Manager User Options (https://<IP Address>:8443/ccmuser) is identified by ccmuser.
- Cisco Unity Connection Administration (https://<IP Address>:8443/cuadmin) is identified by cuadmin.
- URLs that do not have an extension, such as https://<IP Address>:8443 or http://<IP Address>:8080), are identified by _root.

The following table contains information on the Connection Rest Tomcat Web Application counters.

Counters	Counter Description
Errors	The total number of HTTP errors (for example, 401 Unauthorized) that a Unified Communications Manager-related or Cisco Unity Connection-related web application encounters.
Requests	The total number of VMREST requests that the web application handles. Each time that a web application is accessed, its Requests counter increments accordingly.
SessionsActive	The number of active or in use sessions in the web application.

CUC Sessions: Authz Server

Table 117: CUC Sessions: Authz Server

Counters	Counter Description
CUC Authz Total Validation Requests	Total Number of Authz validation requests.
CUC Authz Successful Validation Requests	Total Number of successful Authz validations.

Counters	Counter Description
CUC Authz Failed Validation Requests	Total Number of failed Authz validations.
CUC Authz Total Validation Requests in Last minute	Total Number of Authz validations in Last minute.
CUC Authz Successful Validation Requests in Last minute	Total Number of successful Authz validations in last minute.
CUC Authz Failed Validation Requests in Last minute	Total Number of failed Authz validations in last minute.

CUC Sessions: Calendar Access

The CUC Sessions: Calendar Access object provides information about the Cisco Unity Connection calendar integration. The following contains information about CUC Sessions: Calendar Access counters.

Table 118: CUC Sessions: Calendar Access

Counters	Counter Descriptions
Connections To Exchange Failure - Total	Total number of Exchange connection failures.
Connections To MP Failure - Total	Total number of MeetingPlace connection failures.
Exchange Requests - Total	Total number of Exchange calendar requests.
Exchange Response Time [ms] - Current	Current Exchange Response Time in milliseconds.
Meeting Join Request - Total	Total number of requests to join the meeting.
MP Request - Total	Total number of MeetingPlace calendar requests.
MP Response Time [ms] - Current	Current MeetingPlace Response Time in milliseconds.

CUC Sessions: E-Mail Access

The CUC Sessions: E-mail Access object provides information about e-mail voice sessions. The following table contains information about CUC Sessions: E-mail Access counters.

Table 119: CUC Sessions: E-Mail Access

Counters	Counter Descriptions
Messages Read - Total	The total number of e-mail messages that were read since the last restart of C Connection.
Session Duration Average [ms]	The average duration [in milliseconds] of all e-mail sessions as measured on basis.
Session Duration Total [ms]	The total duration [in milliseconds] of all e-mail sessions as measured on a basis.

Counters	Counter Descriptions
Sessions - Current	The number of active e-mail voice sessions.
Sessions - Total	The total number of e-mail voice sessions since the last restart of Cisco Connection.

CUC Sessions: IMAP Server

The CUC Sessions: IMAP Server object provides information about the IMAP server. The following table contains information about CUC Sessions: IMAP Server counters.

Table 120: CUC Sessions: IMAP Server

Counters	Counter Descriptions
Commands per minute	The number of IMAP commands per minute.
Connection Length Average [s]	The average duration [in seconds] of the connections to the IMAP server i minute.
Current IDLE Sessions	The number of idle sessions on the IMAP server.
Errors Total	The total number of IMAP errors that the IMAP server returned since t of the IMAP server.
EXAMINE Requests Total	The total number of EXAMINE requests to the IMAP server since the l the IMAP server.
Failed Login Requests Total	The total number of failed LOGIN requests to the IMAP server since th of the IMAP server.
FETCH Requests Total	The total number of FETCH requests to the IMAP server since the last IMAP server.
Login Requests Total	The total number of LOGIN requests to the IMAP server since the last IMAP server.
Logout Requests Total	The total number of LOGOUT requests to the IMAP server since the las IMAP server.
Messages Read Total	The total number of IMAP FETCH commands that have returned the b message since the IMAP was last restarted.
Messages Read/hour	The number of IMAP FETCH commands in the previous hour that retu of a message.
Messages/fetch Average	Average number of messages that the IMAP FETCH command returne
NOOP Requests Total	The total number of NOOP requests to the IMAP server since the last r IMAP server.
Response Time [ms]	The response time [in milliseconds] for IMAP commands.

Counters	Counter Descriptions
SEARCH Requests Total	The total number of SEARCH requests to the IMAP server since the last res IMAP server.
Socket Connections Current	The number of active socket connections to the IMAP server.
Socket Connections Total	The total number of socket connections that have been made to the IMAP se it was last restarted.
STARTTLS Requests Total	The total number of STARTTLS requests to the IMAP server since the last the IMAP server. This counter also increments when clients connect to the I port directly.
STATUS Requests Total	The total number of STATUS requests to the IMAP server since the last res IMAP server.
TLS Connections Current	The number of active Transport Layer Security connections to the IMAP se
TLS Errors Total	The total number of failed TLS connections to the IMAP server since the la of the IMAP server.
Unsolicited Notify Response Time Average [ms]	Average Unsolicited Notify Response Time [in milliseconds] for the IMAP
Unsolicited Notify Responses Total	Total number of Unsolicited Notify Responses that the IMAP server made si last restarted.

CUC Sessions: RSS

The CUC Sessions: RSS object provides information about RSS sessions. The following table contains information about CUC Sessions: RSS counters.

Table 121: CUC Sessions: RSS

Counters	Counter Descriptions
RSS Messages Offered Total	The total number of RSS messages that were offered for streaming.
RSS Messages Streamed Total	The total number of RSS messages that the Cisco Unity Connection server
RSS Sessions Current	The current number of RSS sessions.
RSS Sessions Total	The total number of RSS sessions.

CUC Sessions: SMTP Server

The CUC Sessions: SMTP Server object provides information about SMTP server sessions. The following table contains information about CUC Sessions: SMTP Server counters.

Table 122: CUC Sessions: SMTP Server

Counters	Counter Descriptions
Total Delivered Messages	The number of SMTP messages that were delivered since the start of th
Total Messages	The number of SMTP messages delivered or received since the start of
Total Received Messages	The number of SMTP messages that were received since the start of the

CUC Sessions: SpeechView Processor

The CUC Sessions: SpeechView Processor object provides information about the SpeechView Processor service. The following table contains information about CUC Sessions: SpeechView Processor counters.

Table 123: CUC Sessions: SpeechView Processor

Counters	Counter Descriptions
Average wait time	The average time it takes to receive successful transcriptions from the ex
Total failures	The total number of failed transcriptions since the last restart of the Spe Processor service.
Total timeouts	The total number transcriptions that timed out since the last restart of the Processor service.
Transcribed messages	The total number successful transcriptions since the last restart of the S Processor service.

CUC Sessions: TRaP

The CUC Sessions: TRaP object provides information about telephone record and playback (TRaP) sessions. The following table contains information about CUC Sessions: TRaP counters.

Table 124: CUC Sessions: TRaP

Counters	Counter Descriptions
Reverse TRaP Session Duration Average [s]	The average duration [in seconds] of all reverse TRaP sessions.
Reverse TRaP Session Duration Total [s]	The total duration [in seconds] of all reverse TRaP sessions.
Reverse TRaP Sessions Current	The current number of active reverse TRaP sessions.
Reverse TRaP Sessions Total	The total number of reverse TRaP sessions since the last start of Cisco Connection.
TRaP Session Duration Average [s]	The average duration [in seconds] of all TRaP sessions.
TRaP Session Duration Total [s]	The total duration [in seconds] of all TRaP sessions.

Counters	Counter Descriptions
TRaP Sessions Current	The current number of active TRaP sessions.
TRaP Sessions Total	The total number of TRaP sessions since the last start of Cisco Unity Conn

CUC Sessions: TTS

The CUC Sessions: TTS object provides information about text-to-speech (TTS) sessions. The following table contains information about CUC Sessions: TTS counters.

Table 125: CUC Sessions: TTS

Counters	Counter Descriptions
Session Duration Average [s]	The average duration [in seconds] of all TTS sessions.
Session Duration Total [s]	The total duration [in seconds] of all TTS sessions.
Sessions Current	The current number of active TTS voice sessions.
Sessions Total	The total number of TTS voice sessions since the last start of Cisco Unity Co

CUC Sessions: Unified Client

The CUC Sessions: Unified Client object provides information about the Unified Client for Cisco Unity Connection.

The Connections Total counter represents the total number of Unified Client IMAP requests.

CUC Sessions: Video

CUC Sessions Video: Video session object provides information about video sessions with video server. The following table contains information about CUC Sessions: Video

Table 126: CUC Sessions: Video

Counters	Counter Descriptions
Audio calls Negotiated Total	The total number of Audio calls negotiated despite video offer.
Audio Calls Negotiated In Last One Minute	The total number of audio calls negotiated despite video offer in last one minute.
Outgoing Video calls Release Transfer	The total number of outgoing video calls transferred as Release to Switch.
Supervise Transfer Calls Total	The total number of Supervise transfers initiated from video calls since the last restart of Cisco Unity Connection.

Counters	Counter Descriptions
Video calls downgraded to Audio Total	The total number of video calls downgraded to audio since the last restart of Unity Connection.
Video calls downgraded to Audio In Last One Minute	The total number of video calls downgraded to audio in last one minute.
Video calls downgraded with prompt total	Total number of video calls downgraded with prompt "Video services are not available using audio only for duration of this call".
Video calls downgraded with prompt in Last One Minute	Total number of video calls downgraded with prompt "Video services are not available using audio only for duration of this call" in last minute.
Video Sessions Total	The total number of video session requests sent from Unity Connection to Video Server.
Video Sessions Current	The total number of current video session requests sent from Unity Connection to Video Server.
Video Session Playbacks Total	The total number of video session playbacks since the last restart of Cisco Unity Connection.
Video Session Playbacks Current	The total number of current video session playbacks.
Video Media File Playbacks Total	The total number of image playbacks from video server since the last restart of Unity Connection.
Video Media File Playbacks Current	The current number of Video Media File playbacks from video server.
Video Recordings Total	The total number of Video Recordings saved at video server since the last restart of Unity Connection.
Video Recordings Current	The current number of Video Recordings saved at video server.
Video Playback Completed Events from MS Total	The total number of Video Playback completed events from video server since the last restart of Unity Connection.
Video Playback Completed Events from MS In Last One Minute	The total number of Video Playback completed events from video server since last one minute.
Video Keep Alive Total	The total number of Keep Alive sent by Unity Connection to video server since the last restart of Unity Connection.
Video Keep Alive In Last One Minute	The total number of Keep Alive sent by Unity Connection to video server since last one minute.

Counters	Counter Descriptions
Video Get Media Capabilities Total	The total number of GetMediaCapabilities sent by Unity Connection to video server since the last restart of Unity Connection.
Video Get Media Capabilities In Last One Minute	The total number of GetMediaCapabilities sent by Unity Connection to video server since last one minute.
Video SignIn Total	The total number of SignIn request sent by Unity Connection to video server since the last restart of Unity Connection.
Video SignIn Total In Last One Minute	The total number of SignIn sent by Unity Connection to video server since last one minute.
KeyFrame Request sent Total	The total number of KeyFrame requests sent during video recording to EndPoint since the last restart of Cisco Unity Connection.
KeyFrame Request sent In Last One Minute	The total number of KeyFrame requests sent during video recording to EndPoint since the last restart of Cisco Unity Connection.
Video Record Successful Total	The total number of successful Video Recordings since the last restart of Cisco Unity Connection.
Video Sessions Failed Total	The total number of video sessions failed since the last restart of Cisco Unity Connection.
Video Session Failed In Last One Minute	The total number of video sessions failed in last one minute.
Media Sense Timeout Total	The total number of connection timeout errors while connecting to MediaSense server since the last restart of Cisco Unity Connection. This counter is applicable for the following events: • During a video call • At the time of sign in • During exchange of media capabilities with the MediaSense server.
Video Play Failed Total	The total number of video messages that are played as audio messages since the last restart of Cisco Unity Connection.

CUC Sessions: Voice

The CUC Sessions: Voice object provides information about voice sessions. The following table contains information on CUC Sessions: Voice counters.

Table 127: CUC Sessions: Voice

Counters	Counter Descriptions
Delay - Directory Search [ms]	The delay [in milliseconds] that a caller experienced when the caller att search through the directory. This counter measures the time between th search criteria and the return results.
Delay - Opening Greeting [ms]	The delay [in milliseconds] that a caller experienced before any audio v This counter measures the time between the system receiving a call and t begins streaming to the caller.
Delay - Subscriber Delete Message [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber ex when the subscriber attempted to delete a message. This counter measu between the last delete message prompt and the confirmation of the del
Delay - Subscriber Logon [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber ex to authentication.
Delay - Subscriber Message Count [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber ex during message counting in the subscriber message box.
Delay - Subscriber Message Header [ms]	The delay [in milliseconds] that a caller experienced while Cisco Unity gathering message header information.
Failsafes Total	The total number of times that the failsafe conversation has been playec
G.711a Sessions Current	The current number of active G.711 (a-law) voice sessions.
G.711a Sessions Total	The total number of active G.711 (a-law) voice sessions since the last re Unity Connection.
G.711u Sessions Current	The current number of active G.711 (u-law) voice sessions.
G.711u Sessions Total	The total number of active G.711 (u-law) voice sessions since the last re Unity Connection.
G.722 Sessions Current	The current number of active G.722 voice sessions.
G.722 Sessions Total	The total number of active G.722 voice sessions since the last restart of Connection.
G.729 Sessions Current	The current number of active G.729 voice sessions.
G.729 Sessions Total	The total number of active G.729 voice sessions since the last restart of Connection.
iLBC Sessions Current	The current number of active iLBC voice sessions.
iLBC Sessions Total	The total number of active iLBC voice sessions since the last restart of Connection.
Meeting search delay delay [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber ex to looking up meetings.

Counters	Counter Descriptions
Messages Deleted	The total number of voice messages that were deleted through the TUI fror Cisco Unity Connection was last restarted.
Messages Forwarded	The total number of voice messages that were forwarded through the TUI f time Cisco Unity Connection was last restarted.
Messages Read	The total number of voice messages that were read through the TUI from tl Cisco Unity Connection was last restarted.
Messages Replied	The total number of voice messages that received replies through the TUI f time Cisco Unity Connection was last restarted.
Messages Sent	The total number of voice messages that were sent through the TUI from th Cisco Unity Connection was last restarted.
MRCP Define Grammar Delay [ms]	The delay [in milliseconds] between an MRCP define-grammar request and its
MRCP Define Grammar Delay Average [ms]	The average delay [in milliseconds] between an MRCP define-grammar rec its response.
MRCP Define Grammar Delay Max [ms]	The maximum delay [in milliseconds] between an MRCP define-grammar re its response.
MRCP Delay [ms]	The delay [in milliseconds] between an MRCP request and its response.
MRCP Delay Average [ms]	The average delay [in milliseconds] between an MRCP request and its resp
MRCP Delay Max [ms]	The maximum delay [in milliseconds] between an MRCP request and its re
OPUS Sessions Current	This displays the current number of active OPUS voice sessions.
OPUS Sessions Total	This displays the total number of OPUS voice sessions since the last restart Unity Connection.
Sessions Current	The current number of all active voice sessions for any codec.
Sessions Total	The total number of voice sessions for any codec - G.711 mu-law and G.72 the last restart of Cisco Unity Connection.
Subscriber Lookup Delay [ms]	The delay [in milliseconds] that a Cisco Unity Connection subscriber experi to finding and loading a subscriber by DTMF ID.

CUC Sessions: VUI

The CUC Sessions: VUI object provides information about the voice user interface (VUI). The following table contains information on CUC Sessions: VUI counters.

Table 128: CUC Sessions: VUI

Counter	Counter Descriptions
Delay - Subscriber Message Access [ms]	The delay [in milliseconds] that a user when experienced when the user access a message. This counter measures the time between the voice co intending to listen to a message and the actual playback of the message
Matches Total	The total number of matches in the VUI conversation.
Messages Read	The total number of messages that were read through the VUI from the ti Unity Connection was last restarted.
No-matches Total	The total number of no-matches in the VUI conversation.
Session Duration Average/call [s]	The average duration [in seconds] of a VUI session as measured on a p
Session Duration Total [s]	The duration [in seconds] of all VUI sessions.
Sessions Current	The current number of active VUI sessions for any codec.
Sessions Total	The total number of VUI and voice sessions for any codec.

CUC Sessions: Web

The CUC Sessions: Web object provides information about the Cisco Personal Communications Assistant (Cisco PCA) and Cisco Unity Connection Administration sessions. The following table contains information on CUC Sessions: Web counters.

Table 129: CUC Sessions: Web

Counters	Counter Descriptions
CPCA Authentication Delay Max [s]	The maximum delay [in seconds] in authentication to a user Inbox or A
CPCA Failed Authentications Total	The number of failed authentications.
CPCA Pages Served Total	The total number of CPCA pages that the Cisco Unity Connection serv
CPCA Requests In Queue Current	The number of requests in CPCA queue waiting to be processed.
CPCA Server Busy Pages Total	The total number of server busy pages that the Cisco Unity Connection se
CPCA Sessions Current	The current number of CPCA sessions.
CPCA Sessions Total	The total number of CPCA sessions.
CUCA Authentication Delay Max [s]	The maximum delay [in seconds] in authentication to the System Adminis
CUCA Response Time Max [ms]	The maximum time [in milliseconds] for the Tomcat server to respond t request.

CUC Sessions: Web E-Mail Access

The CUC Sessions: Web E-mail Access object provides information about web e-mail access sessions (IMAP). The following table contains information about CUC Sessions: Web E-mail Access counters.

Table 130: CUC Sessions: Web E-Mail Access

Counters	Counter Descriptions
Messages Read - Total	The total number of e-mail messages that were read since the last restart of C Connection.
Session Duration Average [ms]	The average duration [in milliseconds] of all e-mail sessions as measured on basis.
Session Duration Total [ms]	The total duration [in milliseconds] of all e-mail sessions as measured on a basis.
Sessions - Current	The number of active e-mail voice sessions.
Sessions - Total	The total number of e-mail voice sessions since the last restart of Cisco Un Connection.

CUC System Agent

The CUC System Agent object records the information about the periodic system tasks. The following table contains information about CUC System Agent counters.

Counters	Counter Descriptions
Message Related Files Shredded Total	The total number of messaging related files that have been shredded.
Message Related Files Shredded Failed	The total number of messaging related files that have failed to shred.
Total Number of Requests sent by HTTP[S]/CCI Link	The cumulative number of HTTP(S) requests sent by the Reader.
Total Number of successful response of HTTP[S]/CCI Requests	The cumulative number of HTTP(S) requests that were successfully processed by the Feeder.
Total Number of failure response of HTTP[S]/CCI Requests	The cumulative number of HTTP(S) requests that were not successfully processed by the Feeder.
Total Number of Directory Objects Successfully Processed	The cumulative number of Directory Objects that were successfully processed.
Directory Objects Processed Successfully In Last One Minute	Directory objects successfully processed per minute.

Counters	Counter Descriptions
Delete Request sent to Media Sense Total	The total number of delete requests sent to MediaSense server since the last restart of Unity Connection.
Media Sense Timeout While Delete Total	The total number of connection timeouts in response to the delete requests sent to MediaSense server since the last restart of Unity Connection.

CUC VMREST

The CUC VMREST object provides information about internal VMREST requests.

The following table contains information about VMREST counters.

Counters	Counter Description
Total VMREST active threads	To maintain Total Number of active VMREST threads.
Total VMREST Throttled Requests	To maintain Total Number of Throttled VMREST requests by Throttle Semaphore.
Total VMREST Throttled Requests in last hour	To maintain Total Number of Throttled VMREST requests by Throttle Semaphore in last hour.

CUC VMREST Container

The CUC VMREST Container object provides information about REST container operations for handling VMREST requests from external clients.

The following table contains information about VMREST Container counters.

Counters	Counter Description
Total VMREST CONTAINER active threads	To maintain Total Number of active VMREST threads for REST container.
Total VMREST CONTAINER throttled Requests	To maintain Total Number of Throttled VMREST requests by Throttle Semaphore for REST container.
Total VMREST CONTAINER throttled Requests in last hour	To maintain Total Number of Throttled VMREST requests by Throttle Semaphore in last hour for REST container.

System Alerts

AuditLogOverFlowDueToLogRotation

This alarm indicates that the audit log overflow occurred. An existing audit log file is overwritten resulting in overflow and eventual loss of audit data.

Default Configuration

Table 131: Default Configuration for the AuditLogOverFlowDueToLogRotation RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: AuditLogOverFlowDueToLogRotation event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AuditLogOverflowDueToLPMPurge

This alarm indicates that overflow occurred due to purge by LPM clean-up logic. When the total disk space usage of log partition crosses the high water mark configured, the LPM tools clean-up logic deletes the oldest files from the log partition so that the new logs can be written.

Default Configuration

Table 132: Default Configuration for the AuditLogOverflowDueToLPMPurge RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Value	Default Configuration
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: AuditLogOverflowDueToLPMPurge event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AuditLogsExceedsConfiguredThreshold

This alarm indicates the percentage of disk space configured for application audit logging exceeds the configured threshold. Audit logs files are overwritten sooner or later depends on the frequency of audit logging by the Unified Communications Manager applications.

Default Configuration

Table 133: Default Configuration for the AuditLogsExceedsConfiguredThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: AuditLogsExceedsConfiguredThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AuthenticationFailed

Authentication validates the user ID and password that are submitted during log in. An alarm gets raised when an invalid user ID and/or the password gets used.

Default Configuration

Table 134: Default Configuration for the AuthenticationFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Number of AuthenticationFailed events exceeds: 1 time in the last 1 minute
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CCMEncryptionErrorDetected

This alert occurs when the CCMEncryptionErrorDetected event is generated.

Default Configuration

Table 135: Default Configuration for the CCMEncryptionErrorDetected RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CCMEncryptionErrorDetected event generated

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CiscoDRFFailure

This alert occurs when the DRF backup or restore process encounters errors.

Default Configuration

Table 136: Default Configuration for the CiscoDRFFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CiscoDRFFailure event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CiscoHAProxyServiceDown

The HAProxy Service Down alarm indicates when the incoming web traffic into Unified Communications Manager and IM and Presence Service is down.

The following table contains information about the CiscoHAProxyServiceDown counter.

Table 137: CiscoHAProxyServiceDown

Counters	Counter Description
Enable Alert	Selected
Severity	Warning
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: when HAProxy service down generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CoreDumpFileFound

This alert occurs when the CoreDumpFileFound event gets generated. This indicates that a core dump file exists in the system.

Default Configuration

Table 138: Default Configuration for the CoreDumpFileFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CoreDumpFileFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
Trace download Parameters	Not Selected
Enable Email	Selected
Trigger Alert Action	Default

CpuPegging

CPU usage gets monitored based on configured thresholds. If the usage goes above the configured threshold, this alert gets generated.

Default Configuration

Table 139: Default Configuration for the CpuPegging RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: 99%
Duration	Trigger alert only when value constantly below or over threshold for 60 seconds
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CriticalServiceDown

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

Default Configuration

Table 140: Default Configuration for the CriticalServiceDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Service status is DOWN
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace download Parameters	Enable Trace Download not selected
Enable Email	Selected
Trigger Alert Action	Default

DBChangeNotifyFailure

This alert occurs when the Cisco Database Notification Service experiences problems and might stop. This condition indicates change notification requests that are queued in the database got stuck and changes made to the system will not take effect. Ensure that the Cisco Database Layer Monitor is running on the node where the alert exists. If it is, restart the service. If that does not return this alert to safe range, collect the output of **show tech notify** and **show tech dbstateinfo** and contact TAC for information about how to proceed.

Default Configuration

Table 141: Default Configuration for the DBChangeNotifyFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: DBChangeNotify queue delay over 2 minutes
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DBReplicationFailure

This alarm indicates a failure in IDS replication and requires database administrator intervention.

Note Be aware that DBReplicationFailure is based on the replication status perfmon counter (instead of DBReplicationFailure alarm as was previously the case). This alert gets triggered whenever the corresponding replication status perfmon counter specifies a value of **3** (Bad Replication) or **4** (Replication Setup Not Successful).

Default Configuration

Table 142: Default Configuration for the DBReplicationFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: DBReplicationFailure occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DBReplicationTableOutOfSync

Default Configuration

Table 143: Default Configuration for the DBReplicationTableOutOfSync RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IDSReplicationFailure event with alarm number 888 generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

HardwareFailure

This alert occurs when a hardware failure event (disk drive failure, power supply failure, and others) has occurred.

Default Configuration

Table 144: Default Configuration for the HardwareFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: HardwareFailure event generated

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogFileSearchStringFound

This alert occurs when the LogFileSearchStringFound event gets generated. This indicates that the search string was found in the log file.

Default Configuration

Table 145: Default Configuration for the LogFileSearchStringFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: LogFileSearchStringFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionHighWaterMarkExceeded

This alert occurs when the percentage of used disk space in the log partition exceeds the configured high water mark. When this alert gets generated, LPM deletes files in the log partition (down to low water mark) to avoid running out of disk space.

Note LPM may delete files that you want to keep. You should act immediately when you receive the LogPartitionLowWaterMarkExceeded alert.

Note In the case, when **logpartitionhighwatermarkexceeded** is set to a lower percentage and deletes the cdr/cmr files from the temporary folder then use **RTMT** to ensure that the alert parameter is set back to the default value of 95%.

Default Configuration

Table 146: Default Configuration for the LogPartitionHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LogPartitionLowWaterMarkExceeded

This alert occurs when the LogPartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the log partition has exceeded the configured low water mark.

Note Be aware that this alert is an early warning. The administrator should start freeing up disk space. Using RTMT/TLC, you can collect trace/log files and delete them from the server. The administrator should adjust the number of trace files that are kept to avoid hitting the low water mark again.

Default Configuration

Table 147: Default Configuration for the LogPartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds Low Water Mark (90%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowActivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space on the active partition is lower than the configured value.

Default Configuration

Table 148: Default Configuration for the LowActivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: Active Partition available disk space below (4%) **Note** In customer environments, virtual machines configured with 80 GB disk space and where 91% or more space has been reserved for disk space/active partition, a 6% increase in utilization results in automatic trigger of the LowActivePartitionAvailableDiskSpace alert after the Unified Communications Manager upgrade. Here, the alert is triggered when the Active Partition available disk space is below (2%). You must log in to RTMT to fix this issue manually.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowAvailableVirtualMemory

RTMT monitors virtual memory usage. When memory runs low, a LowAvailableVirtualMemory alert is generated.

Default Configuration

Table 149: Default Configuration for the LowAvailableVirtualMemory RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Available virtual memory below (15%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected

Value	Default Configuration
Trigger Alert Action	Default

LowInactivePartitionAvailableDiskSpace

This alert occurs when the percentage of available disk space of the inactive partition equals less than the configured value.

Default Configuration

Table 150: Default Configuration for the LowInactivePartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Inactive Partition available disk space below (4%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowSwapPartitionAvailableDiskSpace

This alert indicates that the available disk space on the swap partition is low.

Note The swap partition is part of virtual memory, so low available swap partition disk space means low virtual memory as well.

Default Configuration

Table 151: Default Configuration for the LowSwapPartitionAvailableDiskSpace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Swap Partition available disk space below (10%)
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ServerDown

This alert occurs when a remote node cannot be reached.

Note Unified Communications Manager and IM and Presence Service: The ServerDown alert is generated when the currently active AMC (primary AMC or the backup AMC, if the primary is not available) cannot reach another server in a cluster. This alert identifies network connectivity issues in addition to a server down condition.

Default Configuration

Table 152: Default Configuration for the ServerDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: ServerDown occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SparePartitionHighWaterMarkExceeded

This alert occurs when the SparePartitionHighWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition exceeds the configured high water mark.

Default Configuration

Table 153: Default Configuration for the SparePartitionHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Spare Partition Used Disk Space Exceeds High Water Mark (95%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SparePartitionLowWaterMarkExceeded

This alert occurs when the SparePartitionLowWaterMarkExceeded event gets generated. This indicates that the percentage of used disk space in the spare partition has exceeded the low water mark threshold.

Default Configuration

Table 154: Default Configuration for the SparePartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Spare Partition Used Disk Space Exceeds Low Water Mark (90%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SyslogSeverityMatchFound

This alert occurs when the SyslogSeverityMatchFound event gets generated. This indicates that a syslog message with the matching severity level exists.

Default Configuration

Table 155: Default Configuration for the SyslogSeverityMatchFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SyslogSeverityMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Value	Default Configuration
Schedule	24 hours daily
Syslog Severity Parameters	Critical
Enable Email	Selected
Trigger Alert Action	Default

SyslogStringMatchFound

This alert occurs when the SyslogStringMatchFound event gets generated. The alert indicates that a syslog message with the matching search string exists.

Default Configuration

Table 156: Default Configuration for the SyslogStringMatchFound RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SyslogStringMatchFound event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Syslog Alert Parameters	(Text box for search string)
Enable Email	Selected
Trigger Alert Action	Default

SystemVersionMismatched

This alert occurs when a mismatch in system version exists.

Default Configuration

Table 157: Default Configuration for the SystemVersionMismatched RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SystemVersionMismatched occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TCPRemoteSyslogDeliveryFailed

This alert occurs when delivery of alarms, audits, or syslog generate events to the configured remote syslog servers fails. The reason could be that the configured syslog server is down, or TCP is not configured on port 601, or there is a network failure.

Default Configuration

Table 158: Default Configuration for the TCPRemoteSyslogDeliveryFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TCPRemoteSyslogDeliveryFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TLSRemoteSyslogDeliveryFailed

This alert occurs when delivery of alarms, audits, or syslog generate events to the configured remote syslog servers fails. The reason could be that the configured syslog server is down, or TLS over TCP is not configured on port 6514, or there is a network failure, or certificate of the remote syslog server is not uploaded to Unified Communications Manager Tomcat trust.

Default Configuration

Table 159: Default Configuration for the TLSRemoteSyslogDeliveryFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TLSRemoteSyslogDeliveryFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TotalProcessesAndThreadsExceededThreshold

This alert occurs when the TotalProcessesAndThreadsExceededThreshold event gets generated. The alert indicates that the current total number of processes and threads exceeds the maximum number of tasks that are configured for the Cisco RIS Data Collector Service Parameter. This situation could indicate that a process is leaking or that a process has thread leaking.

Default Configuration

Table 160: Default Configuration for the TotalProcessesAndThreadsExceededThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TotalProcessesAndThreadsExceededThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

Voice and Video Alerts

BeginThrottlingCallListBLFSubscriptions

This alert occurs when the BeginThrottlingCallListBLFSubscriptions event gets generated. This indicates that the Unified Communications Manager initiated a throttling of the CallList BLF Subscriptions to prevent a system overload.

Default Configuration

Table 161: Default Configuration for the BeginThrottlingCallListBLFSubscriptions RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: BeginThrottlingCallListBLFSubscriptions event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CallAttemptBlockedByPolicy

Default Configuration

Table 162: Default Configuration for the CallAttemptBlockedByPolicy RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CallAttemptBlockedByPolicy event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CallProcessingNodeCpuPegging

This alert occurs when the percentage of CPU load on a call processing server exceeds the configured percentage for the configured time.

If the administrator takes no action, high CPU pegging can lead to a Unified Communications Manager crash, especially in CallManager service. The CallProcessingNodeCpuPegging alert gives you time to work proactively to avoid a crash.

During CPU usage spikes, other alarms that may be issued in addition to the CallProcessingNodeCpuPegging alert include: CoreDumpFound, CriticalServiceDown, SDLLinkOutOfService, and NumberOfRegisteredPhonesDropped alarms.

Note Unified Communications Manager VMware installations can experience high CPU usage spikes while performing tasks such as DRF backups and Bulk Administration Tool exports. The processes that are commonly responsible for CPU usage spikes are gzip and DRFLocal.

If your system is generating CallProcessingNodeCpuPegging alarms, add an additional vCPU for the support of 7500 Unified Communications Manager users following the Open Virtualization Archives (OVA) template specifications for your system.

Default Configuration

Table 163: Default Configuration for the CallProcessingNodeCpuPegging RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Processor load over (90%)
Duration	Trigger alert only when value constantly below or over threshold for 60 seconds
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CARIDSEngineCritical

Default Configuration

Table 164: Default Configuration for the CARIDSEngineCritical RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CARIDSEngineCritical event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CARIDSEngineFailure

Default Configuration

Table 165: Default Configuration for the CARIDSEngineFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CARIDSEngineFailure event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CARSchedulerJobFailed

Default Configuration

Table 166: Default Configuration for the CARSchedulerJobFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CARSchedulerJobFailed event generated.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRAgentSendFileFailed

This alert gets raised when the CDR Agent cannot send CDR files from a Unified Communications Manager node to a CDR repository node within the Unified Communications Manager cluster.

Default Configuration

Table 167: Default Configuration for the CDRAgentSendFileFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRAgentSendFileFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRFileDeliveryFailed

This alert gets raised when FTP delivery of CDR files to the outside billing server fails.

Default Configuration

Table 168: Default Configuration for the CDRFileDeliveryFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRFileDeliveryFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRFileDeliveryFailureContinues

This alert occurs when the CDRFileDeliveryFailureContinues event is generated. This indicates that FTP delivery of CDR files to the outside remote server failed after 3 or more attempts.

Default Configuration

Table 169: Default Configuration for the CDRFileDeliveryFailureContinues RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRFileDeliveryFailureContinues event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRHighWaterMarkExceeded

This alert gets raised when the high water mark for CDR files gets exceeded. It also indicates that some successfully delivered CDR files got deleted.

Default Configuration

Table 170: Default Configuration for the CDRHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: CDRHighWaterMarkExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRMaximumDiskSpaceExceeded

This alarm gets raised when the CDR files disk usage exceeds the maximum disk allocation. It also indicates that some undelivered files got deleted.

Default Configuration

Table 171: Default Configuration for the CDRMaximumDiskSpaceExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRMaximumDiskSpaceExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CiscoWLCSyncServiceDown

This alert occurs when the exceeded maximum number of devices(50000) in the Switches and Access points.

Default Configuration

Table 172: Default Configuration for the CiscoWLCSyncServiceDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CiscoWLCSyncServiceDown event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CodeYellow

The AverageExpectedDelay counter represents the current average expected delay to handle any incoming message. If the value exceeds the value that is specified in Code Yellow Entry Latency service parameter, the CodeYellow alarm gets generated. You can configure the CodeYellow alert to download trace files for troubleshooting purposes.

Default Configuration

Table 173: Default Configuration for the CodeYellow RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco CallManager CodeYellowEntry event generated
Duration	Trigger alert immediately

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace Download Parameters	Enable Trace Download not selected
Enable Email	Selected
Trigger Alert Action	Default

DDRBlockPrevention

This alert gets triggered when the IDSReplicationFailure alarm with alarm number 31 occurs, which invokes a proactive procedure to avoid denial of service. This procedure does not impact call processing; you can ignore replication alarms during this process.

The procedure takes up to 60 minutes to finish. Check that RTMT replication status equals 2 on each node to make sure that the procedure is complete. Do not perform a system reboot during this process.

Default Configuration

Table 174: Default Configuration for the DDRBlockPrevention RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IDSReplicationFailure alarm with alarm number 31 generated
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DDRDown

This alert gets triggered when the IDSReplicationFailure alarm with alarm number 32 occurs. An auto recover procedure runs in the background and no action is needed.

The procedure takes about 15 minutes to finish. Check that RTMT replication status equals 2 on each node to make sure the procedure is complete.

Default Configuration

Table 175: Default Configuration for the DDRDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IDSReplicationFailure alarm with alarm number 32 generated
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

EMCCFailedInLocalCluster

Default Configuration

Table 176: Default Configuration for the EMCCFailedInLocalCluster RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: EMCCFailedInLocalCluster event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

EMCCFailedInRemoteCluster

Default Configuration

Table 177: Default Configuration for the EMCCFailedInRemoteCluster RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: EMCCFailedInRemoteCluster event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ExcessiveVoiceQualityReports

This alert gets generated when the number of QRT problems that are reported during the configured time interval exceed the configured value. The default threshold specifies 0 within 60 minutes.

Default Configuration

Table 178: Default Configuration for the ExcessiveVoiceQualityReports RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of quality reports exceeds 0 times within the last 60 minutes
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSDuplicateURI

This alert occurs when the Unified Communications Manager identifies that it has learned duplicate URI entries through ILS during a call to the URI. Whenever there are duplicate entries for a URI(such as the URI user@example.com existing on two clusters), the call is routed to the cluster from which the URI that was first learned. Calls will not be routed to the other duplicate entries.

Default Configuration

Table 179: Default Configuration for the ILSDuplicateURI RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: ILSDuplicateURI event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSHubClusterUnreachable

Default Configuration

Table 180: Default Configuration for the ILSHubClusterUnreachable RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: A connection to the remote ILS server could not be established.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSPeerLimitApproachingWarning

This alert occurs when the current peer count has reached 90% or more of the ILS network capacity.

Default Configuration

Table 181: Default Configuration for the ILSPeerLimitApproachingWarning RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Value	Default Configuration
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: ILSPeerLimitApproachingWarning event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSPeerLimitExceeded

This alert occurs when the number of peers for this cluster in the ILS network is more than the limit set for ILSP_MSG_PEER_MAX. The system is allowed to add spokes, hubs, and imported catalogs continuously. However, only maximum number of peers are advertised to the ILS network.

Default Configuration

Table 182: Default Configuration for the ILSPeerLimitExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: The number of peers have exceeded the limit set for ILSP_MSG_PEER_MAX
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSPwdAuthenticationFailed

Default Configuration

Table 183: Default Configuration for the ILSPwdAuthenticationFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Password Authentication Failure with ILS at remote cluster.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ILSTLSAuthenticationFailed

Default Configuration

Table 184: Default Configuration for the ILSTLSAuthenticationFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TLS Failure to ILS at remote cluster.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheInactive

This alarm gets generated when a Unified Communications Manager attempts to connect to the Cisco IME server, but the IME distributed cache is not currently active.

Ensure that the certificate for the Cisco IME server is provisioned and that the IME distributed cache has been activated through the CLI.

Default Configuration

Table 185: Default Configuration for the IMEDistributedCacheInactive Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Inactive IME Distributed Cache
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEOverQuota

This alert indicates that the Unified Communications Manager servers that use this Cisco IME service have exceed the quota for published direct inward dialing numbers (DIDs) to the IME distributed cache. The alert includes the name of the Cisco IME server as well as the current and target quota values.

Ensure that you have correctly provisioned the DID prefixes on all of the Unified Communications Manager servers that use this Cisco IME service.

If you have provisioned the prefixes correctly, you have exceeded the capacity of your Cisco IME service, and you need to configure another service and divide the DID prefixes across the Cisco IME client instances (Unified Communications Managers) on different Cisco IME services.

Default Configuration

Table 186: Default Configuration for the IMEOverQuota Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: VAP over quota
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEQualityAlert

This alert gets generated when Unified Communications Manager determines that a substantial number of Cisco IME calls fail back to PSTN or fail to be set up due to IP network quality problems. Two types of events trigger this alert:

- A large number of the currently active Cisco IME calls have all requested fallback or have fallen back to the PSTN.
- A large number of the recent call attempts have gone to the PSTN and not been made over IP.

When you receive this alert, check your IP connectivity. If no problems exist with the IP connectivity, you may need to review the CDRs, CMRs, and logs from the firewalls to determine why calls have fallen back to the PSTN or have not been made over IP.

Default Configuration

Table 187: Default Configuration for the IMEQualityAlert Alert

Value	Default Configuration
Enable Alert	Selected

Value	Default Configuration
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME link quality problem
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEServiceStatus

This alert indicates the overall health of the connection to the Cisco IME services for a particular Cisco IME client instance (Unified Communications Manager). The alert indicates the following states:

- 0—Unknown. Likely indicates that the Cisco IME service has not been activated.
- 1—Healthy. Indicates that the Unified Communications Manager has successfully established a connection to its primary and backup servers for the Cisco IME client instance, if configured.
- 2—Unhealthy. Indicates that the Cisco IME has been activated but has not successfully completed handshake procedures with the Cisco IME server. Note that this counter reflects the handshake status of both the primary and the secondary IME servers.

Default Configuration

Table 188: Default Configuration for the IMEServiceStatus Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: VAP Connection Problem

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert every 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InsufficientFallbackIdentifiers

This alert gets generated when too many Cisco IME calls that are currently in progress use the same fallback DID and no more DTMF digit sequences exist to allocate to a new Cisco IME call that Unified Communications Manager is processing. The new call continues, but the call cannot fallback to the PSTN if voice-quality deteriorates.

If this alert gets generated, note the fallback profile that associates with this call. Check that profile in Cisco Unified Communications Manager Administration, and examine the current setting for the "Fallback Number of Correlation DTMF Digits" field. Increase the value of that field by one, and check whether the new value eliminates these alerts. In general, this parameter should be large enough so that the number of simultaneous Cisco IME calls that are made to enrolled numbers that associate with that profile is always substantially less than 10 raised to the power of this number. For example, if you always have fewer than 10,000 simultaneous Cisco IME calls for the patterns that associate with this fallback profile, setting this value to 5 (10 to the power of 5 equals 100,000) should keep Unified Communications Manager from generating this alert.

However, increasing this value results in a small increase in the amount of time it takes to perform the fallback. As such, you should set the "Fallback Number of Correlation DTMF Digits" field to a value just large enough to prevent this alert from getting generated.

Instead of increasing the value of the DTMF digits field, you can add another fallback profile with a different fallback DID and associate that fallback profile with a smaller number of enrolled patterns. If you use this method, you can use a smaller number of digits.

Default Configuration

Table 189: Default Configuration for the InsufficientFallbackIdentifiers Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cannot allocate fallback identifier

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within one minute
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCredentials

The alert indicates that the Unified Communications Manager cannot connect to the Cisco IME server because the username and/or password configured on Unified Communications Manager do not match those configured on the Cisco IME server.

The alert includes the username and password that were used to connect to the Cisco IME server as well as the IP address and name of the target Cisco IME server. To resolve this alert, log into the Cisco IME server and check that the configured username and password match the username and password that are configured in Unified Communications Manager.

Default Configuration

Table 190: Default Configuration for the InvalidCredentials Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Credential Failure to Cisco IME server
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LocationOutOfResource

This alert occurs when the number of LocationOutOfResource events exceeds the configure threshold during the configured time interval. This indicates that one or all of audio or video or immersive bandwidth for a location or link is used up.

Default Configuration

Table 191: Default Configuration for the LocationOutOfResource Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: LocationOutOfResource event generated 5 times within 60 seconds
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MaliciousCallTrace

This indicates that a malicious call exists in Unified Communications Manager. The malicious call identification (MCID) feature gets invoked.

Default Configuration

Table 192: Default Configuration for the MaliciousCallTrace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: Malicious call trace generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MediaListExhausted

This alert occurs when the number of MediaListExhausted events exceeds the configured threshold during the configured time interval. This indicates that all available media resources that are defined in the media list are busy. The default specifies 0 within 60 minutes.

Default Configuration

Table 193: Default Configuration for the MediaListExhausted RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of MediaListExhausted events exceeds 0 times within the last 60 minutes
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MgcpDChannelOutOfService

This alert gets triggered when the BRI D-Channel remains out of service.

Default Configuration

Table 194: Default Configuration for the MgcpDChannelOutOfService RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: MGCP DChannel is out-of-service
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredDevicesExceeded

This alert occurs when the NumberOfRegisteredDevicesExceeded event gets generated.

Default Configuration

Table 195: Default Configuration for the NumberOfRegisteredDevicesExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: NumberOfRegisteredDevicesExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredGatewaysDecreased

This alert occurs when the number of registered gateways in a cluster decreases between consecutive polls.

Default Configuration

Table 196: Default Configuration for the NumberOfRegisteredGatewaysDecreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of registered gateway decreased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredGatewaysIncreased

This alert occurs when the number of registered gateways in the cluster increased between consecutive polls.

Default Configuration

Table 197: Default Configuration for the NumberOfRegisteredGatewaysIncreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Value	Default Configuration
Threshold	Trigger alert when following condition met: Number of registered gateways increased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredMediaDevicesDecreased

This alert occurs when the number of registered media devices in a cluster decreases between consecutive polls.

Default Configuration

Table 198: Default Configuration for the NumberOfRegisteredMediaDevicesDecreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered media devices decreased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredMediaDevicesIncreased

This alert occurs when the number of registered media devices in a cluster increases between consecutive polls.

Default Configuration

Table 199: Default Configuration for the NumberOfRegisteredMediaDevicesIncreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered media devices increased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredPhonesDropped

This alert occurs when the number of registered phones in a cluster drops more than the configured percentage between consecutive polls.

Default Configuration

Table 200: Default Configuration for the NumberOfRegisteredPhonesDropped RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered phones in the cluster drops (10%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingCallSetupFail

Default Configuration

Table 201: Default Configuration for the RecordingCallSetupFail RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: RecordingCallSetupFail event(s) generated
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingGatewayRegistrationRejected

Default Configuration

Table 202: Default Configuration for the RecordingGatewayRegistrationRejected RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: RecordingGatewayRegistrationRejected event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingGatewayRegistrationTimeout

Default Configuration

Table 203: Default Configuration for the RecordingGatewayRegistratioNTimeout RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: RecordingGatewayRegistrationTimeout event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingGatewaySessionFailed

Default Configuration

Table 204: Default Configuration for the RecordingGatewaySessionFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: RecordingGatewaySessionFailed event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingResourcesNotAvailable

Default Configuration

Table 205: Default Configuration for the RecordingResourcesNotAvailable RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: RecordingGatewayRegistrationTimeout event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RecordingSessionTerminatedUnexpectedly

Default Configuration

Table 206: Default Configuration for the RecordingSessionTerminatedUnexpectedly RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: RecordingCallSetupFail event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RouteListExhausted

This alert occurs when the number of RouteListExhausted events exceeds the configured threshold during the configured time interval. This indicates that all available channels that are defined in the route list are busy. The default specifies 0 within 60 minutes.

Default Configuration

Table 207: Default Configuration for the RouteListExhausted RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of RouteListExhausted exceeds 0 times within the last 60 minutes

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RTMTSessionsExceedsThreshold

Default Configuration

Table 208: Default Configuration for the RTMTSessionsExceedsThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: When number of ast session is more than 250.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SDLLinkOutOfService

This alert occurs when the SDLLinkOutOfService event gets generated. This event indicates that the local Unified Communications Manager cannot communicate with the remote Unified Communications Manager. This event usually indicates network errors or a non-running remote Unified Communications Manager.

Default Configuration

Table 209: Default Configuration for the SDLLinkOutOfService RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SDLLinkOutOfService event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseAuthorizationExpiringSoon

This alert occurs when the Unified Communications Manager authorization with Cisco Smart Software Manager or Cisco Smart Software Manager satellite is going to expire soon.

Default Configuration

Table 210: Default Configuration for the SmartLicenseAuthorizationExpiringSoon RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseAuthorizationExpiringSoon event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseCommunicationError

This alert occurs when Unified Communications Manager is unable to communicate successfully with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Default Configuration

Table 211: Default Configuration for the SmartLicenseCommunicationError RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseCommunicationError event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseExportControlNotAllowed

This alert occurs when Unified Communications Manager is not registered with the Registration Token received from the Smart account or Virtual account that has Allow export-controlled functionality checked and is not licensed to operate in mixed-mode

Default Configuration

Table 212: Default Configuration for the SmartLicenseExportControlNotAllowed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseExportControlNotAllowed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseInEval

This alert occurs when Unified Communications Manager is not registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite and is operating in Evaluation Mode that is soon going to expire.

Default Configuration

Table 213: Default Configuration for the SmartLicenseInEval RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseInEval event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseInOverageAuthorizationExpired

This alert occurs when you do not renew the license authorization for Unified Communications Manager before the authorization expiry date and the license authorization has expired. It runs on the overage period that is soon going to expire.

Default Configuration

Table 214: Default Configuration for the SmartLicenseInOverage_AuthorizationExpired RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseInOverage_AuthorizationExpired event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseInOverageOutOfCompliance

This alert occurs when Cisco Unified Communication Manager operates with insufficient number of licenses and the status is out of compliance. It runs on the overage period that is soon going to expire.

Default Configuration

Table 215: Default Configuration for the SmartLicenseInOverage_OutOfCompliance RTMT Alert

Value	Default Configuration
Enable Alert	Selected

Value	Default Configuration
Severity	Alert
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseInOverage_OutOfCompliance event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseNoProvisionAuthorizationExpired

This alert occurs when the license authorization for Unified Communications Manager is not successful and the overage period has expired. You are not allowed to add, update, or delete any users or devices.

Default Configuration

Table 216: Default Configuration for the SmartLicenseNoProvision_AuthorizationExpired RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseNoProvision_AuthorizationExpired event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseNoProvisionEvalExpired

This alert occurs when the Cisco Smart Licensing evaluation period is expired for Unified Communications Manager. You are not allowed to add, update, or delete any users or devices.

Default Configuration

Table 217: Default Configuration for the SmartLicenseNoProvision_EvalExpired RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseNoProvision_EvalExpired event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseNoProvisionOutOfCompliance

This alert occurs when Cisco Unified Communication Manager operates with insufficient number of licenses and the overage period has expired. You are not allowed to add, update, or delete any users or devices.

Default Configuration

Table 218: Default Configuration for the SmartLicenseNoProvision_OutOfCompliance RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseNoProvision_OutOfCompliance event generated

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseRegistrationExpired

This alert occurs when you do not renew the license registration for Unified Communications Manager before the registration expiry date and the license registration has expired. You are not allowed to add, update, or delete any users or devices.

Default Configuration

Table 219: Default Configuration for the SmartLicenseRegistrationExpired RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseRegistrationExpired event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseRegistrationExpiringSoon

This alert occurs when the Unified Communications Manager registration with Cisco Smart Software Manager or Cisco Smart Software Manager satellite is going to expire soon.

Default Configuration

Table 220: Default Configuration for the SmartLicenseRegistrationExpiringSoon RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseRegistrationExpiringSoon event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseRenewAuthFailed

This alert occurs when the Unified Communications Manager license authorization renewal fails.

Default Configuration

Table 221: Default Configuration for the SmartLicenseRenewAuthFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseRenewAuthFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

SmartLicenseRenewRegistrationFailed

This alert occurs when the Unified Communications Manager license registration renewal fails.

Default Configuration

Table 222: Default Configuration for the SmartLicenseRenewRegistrationFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when the following condition is met: SmartLicenseRenewRegistrationFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicense_SLR_InEval

This alert occurs when Cisco Unified Communications Manager running in the Evaluation period is enabled for Specified License Reservation and pending installation of reserved authorization code.

Default Configuration

Table 223: Default Configuration for the SmartLicense_SLR_InEval RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning

Value	Default Configuration
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: **SmartLicense_SLR_InEval** event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicense_SLR_NoProvision_EvalExpired

This alert occurs when the Unified Communications Manager license Evaluation period is expired and pending installation of Specified license reservation authorization code.

Default Configuration

Table 224: Default Configuration for the SmartLicense_SLR_NoProvision_EvalExpired RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: **SmartLicense_SLR_NoProvision_EvalExpired** event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicense_SLR_InOverage_NotAuthorized

This alert occurs when the Unified Communications Manager is running in Specified License Reservation mode and with insufficient number of licenses and the overage period is active.

Default Configuration

Table 225: Default Configuration for the SmartLicense_SLR_InOverage_NotAuthorized RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: **SmartLicense_SLR_InOverage_NotAuthorized** event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicense_SLR_NoProvision_NotAuthorized

This alert occurs when the Unified Communications Manager is running in Specified License Reservation mode and with insufficient number of licenses and the overage period has expired thereby moving into no provision state.

Default Configuration

Table 226: Default Configuration for the SmartLicense_SLR_NoProvision_NotAuthorized RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: **SmartLicense_SLR_NoProvision_NotAuthorized** event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SmartLicense_SLR_ExportControlNotAllowed

This alert occurs when Unified Communication Manager has mixed-mode and Specific License Reservation is enabled, and also when Unified Communication Manager in Evaluation mode, Evaluation period expired, and Registered-Specific License Reservation states.

Default Configuration

Table 227: Default Configuration for the SmartLicense_SLR_ExportControlNotAllowed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: **SmartLicense_SLR_ExportControlNotAllowed** event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SwitchesAndAccessPointReached75PercentCapacity

This alert occurs when the current record count for switches and access points has reached 75% of maximum capacity of 50000 records.

Default Configuration

Table 228: Default Configuration for the SwitchesAndAccessPointReached75PercentCapacity RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SwitchesAndAccessPointReached75PercentCapacity
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SwitchesAndAccessPointReached90PercentCapacity

This alert occurs when the current record count for switches and access points has reached 90% of maximum capacity of 50000 records.

Default Configuration

Table 229: Default Configuration for the SwitchesAndAccessPointReached90PercentCapacity RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SwitchesAndAccessPointReached90PercentCapacity
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

SwitchesAndAccessPointReached95PercentCapacity

This alert occurs when the current record count for switches and access points has reached 95% of maximum capacity of 50000 records.

Default Configuration

Table 230: Default Configuration for the SwitchesAndAccessPointReached95PercentCapacity RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SwitchesAndAccessPointReached95PercentCapacity
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TCPSetupToIMEFailed

This alert occurs when Unified Communications Manager cannot establish a TCP connection to a Cisco IME server. This alert typically occurs when the IP address and port of the Cisco IME server are misconfigured in Unified Communications Manager or when an Intranet connectivity problem exists and prevents the connection from being set up.

Ensure that the IP address and port of the Cisco IME server in the alert are valid. If the problem persists, test the connectivity between the Unified Communications Manager servers and the Cisco IME server.

Default Configuration

Table 231: Default Configuration for the TCPSetupToIMEFailed Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Connection Failure to Cisco IME server
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TLSConnectionToIMEFailed

This alert occurs when a TLS connection to the Cisco IME service could not be established because the certificate presented by the Cisco IME service has expired or is not in the Unified Communications Manager CTL.

Ensure that the Cisco IME service certificate has been configured into the Unified Communications Manager.

Default Configuration

Table 232: Default Configuration for the TLSConnectionToIMEFailed Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TLS Failure to Cisco IME service
Duration	Trigger alert immediately

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

UserInputFailure

Default Configuration

Table 233: Default Configuration for the UserInputFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: UserInputFailure event(s) generated.
Duration	Trigger alert immediately
Frequency	Trigger up to 3 alerts every 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IM and Presence Service Alerts

CTIGWModuleNotEnabled

Alert Description

This alert indicates that the Cisco CTI Gateway application is either not fully configured or enabled.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Configure and enable the Cisco CTI Gateway application using the Unified Communications Manager IM and Presence CTI Gateway Settings page.

CTIGWProviderDown

Alert Description

This alert indicates that the CTI provider is down.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the connection to the configured Unified Communications Manager nodes and verify that the Cisco CTI Gateway application is enabled on the Cisco Unified CM IM and Presence Administration GUI CTI Settings page.

CTIGWProviderFailedtoOpen

Type

IM and Presence Service

Alert Description

This alert indicates that the CTI Provider failed to open due to a configuration error.

Unified RTMT Default Threshold

Not Applicable.

Recommended Actions

Verify the Unified Communications Manager addresses and application user credentials on the Administration GUI CTI Settings page.

CTIGWQBEFailedRequest

Alert Description

This alert indicates that the Cisco CTI Gateway application received a failed response to a request.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

CTIGWSystemError

Alert Description

This alert indicates Cisco CTI Gateway application system errors.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

CTIGWUserNotAuthorized

Alert Description

This alert indicates that the user failed to authorized due to wrong device or line DN.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Verify user device configuration and MOC settings.

CTIGWUserNotLicenced

Alert Description

This alert indicates that the user failed to authorize due to no license available.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the Cisco CTI Gateway application license and user configuration.

DuplicateDirectoryURI

Alert Description

This alert indicates that there are multiple users within the intercluster deployment that are assigned the same directory URI value when the Directory URI IM Address scheme is configured.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Take immediate action to correct the issue. Each user must be assigned a unique directory URI. Affected users may be homed on an intercluster peer.

DuplicateUserid

Alert Description

This alert indicates that there are duplicate user IDs assigned to one or more users on different clusters within the intercluster deployment.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Take immediate action to correct the issue. Each user must be assigned a unique user ID. The affected users may be homed on an intercluster peer.

EspConfigAgentFileWriteError

Alert Description

This alert indicates that the Cisco Config Agent service cannot write to the file system.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Using Unified RTMT, verify whether the disk space is low or exhausted. This alarm may indicate that the system is overloaded, which may require reassigning users to other nodes in the IM and Presence

Service cluster. You can reassign users to other nodes using the Topology page on the IM and Presence Service Administration GUI.

EspConfigAgentHighCPUUtilization

Alert Description

This alert indicates that CPU utilization has exceeded the configured threshold.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Unified RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

EspConfigAgentHighMemoryUtilization

Alert Description

This alert indicates that the virtual memory utilization has exceeded the configured threshold.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Unified RTMT to monitor memory utilization and reduce system load to improve performance if necessary.

EspConfigAgentLocalDBAccessError

Alert Description

This alert indicates that the Cisco Config Agent service failed to read or write to the local IM and Presence Service database.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Verify the system health using Cisco RTMT. Verify that the service A Cisco DB is running.

EspConfigAgentMemAllocError

Alert Description

This alert indicates that the Cisco Config Agent service cannot allocate memory.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Using Unified RTMT, verify if the system memory is low or exhausted. This alarm may indicate that the system is overloaded which may require reassigning users to other nodes in the IM and Presence Service cluster. You can reassign users to other nodes using the Topology page on the IM and Presence Service Administration GUI.

EspConfigAgentNetworkOutage

Alert Description

This alert indicates Cisco Config Agent network outage.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Verify system health and network connectivity using Cisco RTMT.

EspConfigAgentNetworkRestored

Alert Description

This alert indicates that Cisco Config Agent network is restored.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Verify system health and network connectivity using Cisco RTMT.

EspConfigAgentProxyDomainNotConfigured

Alert Description

This alert indicates that the Cisco Config Agent service is not configured. Cisco Config Agent service uses the proxy domain to properly generate ACLs. If not configured it could lead to routing failures.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Go to the Service Parameters drop-down menu on the IM and Presence Service publisher. Select the Cisco SIP Proxy service. Enter the IM and Presence Service domain into the Proxy Domain service parameter and save.

EspConfigAgentRemoteDBAccessError

Alert Description

This alert indicates that the Cisco Config Agent service cannot access a remote IM and Presence Service database.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Verify that the service A Cisco DB is running on the node specified in the alert. Sometimes these errors can be transient. In some cases the Config Agent may be accessing remote nodes that are not available for some reason. If that is the case, then this error is expected. This result would happen in a user reassignment to a node that is not installed or available.

EspConfigAgentSharedMemoryStaticRouteError

Alert Description

This alert indicates that the Cisco Config Agent service failed to access static routes in shared memory. This may indicate that the system is out of memory.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Using Cisco RTMT, verify if the system shared memory is low or exhausted. This alarm may indicate the system is overloaded which may require reassigning users to other nodes in the IM and Presence

Service cluster. You can reassign users to other nodes using the Topology page on the Administration GUI.

ESPConfigError

Alert Description

This alert indicates Cisco SIP Proxy service configuration file error.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Verify that the Cisco Config Agent service is running. This service is responsible for writing the proxy configuration file.

ESPConfigNotFound

Alert Description

This alert indicates that Cisco SIP Proxy service configuration file is not found.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Verify that the configuration files `/usr/local/sip/conf/sipd.conf` and `/usr/local/sip/conf/dynamic.sipd.conf` exist on the IM and Presence server.

ESPCreateLockFailed

Alert Description

This alert indicates that lock file has not been created.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPLoginError

Alert Description

This alert indicates that an error occurred while communicating with the login datastore.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPMallocFailure

Alert Description

This alert indicates that memory allocation has failed. This may indicate a low or no memory issue with the server.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Unified RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPNAPTRInvalidRecord

Alert Description

This alert indicates that NAPTR record format error.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPPassedParamInvalid

Alert Description

This alert indicates that invalid parameters were specified. This could be because the parameters were NULL.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Unified RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPRegistryError

Alert Description

This alert indicates that it is not possible to add registration to the SIP Registry because a resource limit was exceeded.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPRoutingError

Alert Description

This alert indicates SIP Route Interface resource limit exceeded error.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPSharedMemAllocFailed

Alert Description

This alert indicates that the Cisco SIP Proxy service failed to allocate shared memory segments while trying to initialize tables.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Use Unified RTMT to check system shared memory, check the Cisco SIP Proxy service trace log file for any detailed error messages and contact Cisco TAC for assistance.

ESPSharedMemCreateFailed

Alert Description

This alert indicates that the Cisco SIP Proxy service failed to create shared memory segments while trying to initialize tables.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Use Unified RTMT to check system shared memory, check the Cisco SIP Proxy service trace log file for any detailed error messages, and contact Cisco TAC for assistance.

ESPSharedMemSetPermFailed

Alert Description

This alert indicates that the Cisco SIP Proxy service failed to set permissions on shared memory segments while trying to initialize tables.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Use Unified RTMT to check system shared memory, check the Cisco SIP Proxy service trace log file for any detailed error messages, and contact Cisco TAC for assistance.

ESPSocketError

Alert Description

This alert indicates network socket errors that could be caused by binding errors such as get socket address failures.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPStatsLogFileOpenFailed

Alert Description

This alert indicates that the Cisco SIP Proxy service stats log file has failed to open.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPStopped

Alert Description

This alert indicates that the Cisco SIP Proxy service child process has stopped.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

If the administrator has not manually stopped the Proxy service, this may indicate a problem. Use Unified RTMT to check for any related alarms and contact Cisco TAC for assistance.

ESPVirtualProxyError

Alert Description

This alert indicates Virtual_Proxy_Domain related error.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPWrongHostName

Alert Description

This alert indicates an invalid IP address or an unresolvable hostname.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ESPWrongIPAddress

Alert Description

This alert indicates that an invalid IP address has been provided.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

ICSACertificateCAConflict

Alert Description

This alert indicates that the Cisco Intercluster Sync Agent service detected a CA certificate conflict.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

A conflicting CA certificate was detected on Unified Communications Manager when auditing certificates. Stop the Cisco Intercluster Sync Agent on all IM and Presence nodes in the cluster. Delete the conflicting certificate on all IM and Presence and Unified Communications Manager nodes and re-upload the valid certificate to each node. Start the Cisco Intercluster Sync Agent.

ICSACertificateCASignedTrustCertFound

Alert Description

This alert indicates that the Cisco Intercluster Sync Agent service has detected a signed CA trust certificate.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Allow only unsigned CA trust certificates.

ICSACertificateFingerPrintMisMatch

Alert Description

This alert indicates that the Cisco Intercluster Sync Agent service detected a fingerprint mismatch on the certificate being processed.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Use the IM and Presence Service OS Administration GUI to compare the certificates that are loaded on this server with the certificates on the source server. You might need to delete the problem certificates and reload them.

ICSACertificateValidationFailure

Alert Description

This alert indicates that the Cisco Intercluster Sync Agent service detected a validation error on the certificate being processed.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Use the IM and Presence OS Administration GUI to compare the certificates that are loaded on this server with the certificates on the source server. You might need to delete the problem certificates and reload them.

InterclusterSyncAgentAXLConnectionFailed

Alert Description

This alert indicates that the Cisco Intercluster Sync Agent service failed authentication to the remote IM and Presence Service cluster and therefore cannot connect.

Unified RTMT Default Threshold

Not Applicable.

Recommended Actions

Verify that the AXL credentials are correct and whether the Cisco AXL Web service is running on the remote IM and Presence Service cluster.

InterclusterSyncAgentPeerDuplicate

Alert Description

This alert indicates that the Cisco Intercluster Sync Agent service failed to sync user location data from a remote peer. The remote peer is from an IM and Presence Service cluster that already has a peer in the local cluster.

Unified RTMT Default Threshold

Not Applicable.

Recommended Actions

Verify that the hostname of the remote peer is not a secondary node from the identified existing peer. If the new peer is a secondary node, then remove this peer from the IM and Presence Service Administration GUI Inter-cluster details page. You can also run the System Troubleshooter for more details.

InvalidDirectoryURI

Alert Description

This alert indicates that one or more users within the deployment are assigned an empty or invalid directory URI value when the Directory URI IM Address scheme is configured.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Take immediate action to correct the issue. Affected users may be homed on an intercluster peer.

JSMSessionsExceedsThreshold

This alert indicates when the client registrations get out of hand and exceeds the number of sessions created on the node.

The following table contains information about the JSMSessionsExceedsThreshold counter.

Table 234: JSMSessionsExceedsThreshold

Counters	Counter Description
Enable Alert	Selected
Severity	Critical
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: when JsmTotalSessionsThre exceeds the threshold
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected

Counters	Counter Description
Trigger Alert Action	Default

LegacyCUPCLogin

Alert Description
This alert indicates that a legacy Cisco Unified Personal Communicator client has attempted to login to the Cisco Client Profile Agent service.

Unified RTMT Default Threshold
Not applicable.

Recommended Actions
Upgrade the legacy Cisco Unified Personal Communicator client as it is currently not supported.

NotInCucmServerListError

Alert Description
This alert indicates that the Cisco Sync Agent failed to start because the IM and Presence node is not in the server list on the Unified Communications Manager publisher.

Unified RTMT Default Threshold
Not applicable.

Recommended Actions
Add the IM and Presence node to the server list on the Unified Communications Manager server and start the Cisco Sync Agent service.

PEAutoRecoveryFailed

Alert Description
This alert indicates that an error occurred during the startup sequence of the Cisco Presence Engine service.

Unified RTMT Default Threshold
Not applicable.

Recommended Actions
This error may indicate a possible configuration issue. Correct the problem identified in the failure message.

PEDatabaseError

Alert Description
This alert indicates that the Cisco Presence Engine service encountered an error while retrieving information from the database. This may indicate a problem with the Cisco DB service.

Unified RTMT Default Threshold
Not Applicable

Recommended Actions
Verify that the Cisco DB service is running. Use Unified RTMT to check the Cisco Presence Engine service logs for errors. Consult Cisco TAC for guidance.

PEIDSQueryError

Alert Description

This alert indicates that the Cisco Presence Engine service has detected an error while querying the IM and Presence Service database.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Restart the Cisco Presence Engine service when convenient. See the associated error message and log files and consult Cisco TAC if the problem persists.

PEIDSSubscribeError

Alert Description

This alert indicates that the Cisco Presence Engine service was unable to subscribe for IM and Presence Service database change notifications.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Restart the Cisco Presence Engine service when convenient. See the associated error message and log files and consult Cisco TAC if the problem persists.

PEIDStoIMDBDatabaseSyncError

Alert Description

This alert indicates that synchronization between the IM and Presence database and the Cisco Presence Engine and a database service has failed (Cisco Login Datastore, Cisco Route Datastore, Cisco Presence Datastore, and Cisco SIP Registration Datastore).

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Restart the Cisco Presence Engine service when convenient. See associated error message and log files and consult Cisco TAC if the problem persists.

PELoadHighWaterMark

Alert Description

This alert indicates that the Cisco Presence Engine service has exceeded CPU utilization threshold.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Inspect the number of active subscription counters using Cisco RTMT: ActiveSubscriptions, ActiveViews, SubscriptionActiveReceivedFromForeign, and SubscriptionActiveSentForeign. If this condition persists, you may consider moving users to a different IM and Presence Service node in the cluster.

PEMemoryHighCondition

Alert Description

This alert indicates that the Cisco Presence Engine service has hit a high memory threshold.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the number of active subscription counters: ActiveSubscriptions, ActiveViews, SubscriptionActiveReceivedFromForeign, and SubscriptionActiveSentForeign using Unified RTMT. If this condition persists, offload some users to a different IM and Presence node in the cluster.

PEPeerNodeFailure

Alert Description

This alert indicates that Cisco Presence Engine service on the peer node of a subcluster has failed.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Use Cisco Unified Serviceability to verify that the Cisco Presence Engine service is running. Consult Cisco TAC for further assistance.

PESipSocketBindFailure

Alert Description

This alert indicates that the Cisco Presence Engine service cannot connect to the indicated configured interface. No SIP traffic can be processed on this interface.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Verify that the Cisco Presence Engine service listen interface is configured correctly on the IM and Presence Service Administration GUI Application Listener page. Verify that no other process is listening on the same port using netstat.

PEStateDisabled

Alert Description

This alert indicates that the Cisco Presence Engine service is inoperable and cannot process traffic.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the log files and monitor the Cisco Presence Engine service with Unified RTMT.

PEStateLocked

Alert Description

This alert indicates that the Cisco Presence Engine service is administratively prohibited from processing traffic.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

This alert is only for notification purpose. No action is required.

PEWebDAVInitializationFailure

Alert Description

This alert indicates that the Cisco Presence Engine service has failed to initialize the WebDAV library.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Restart the Cisco Presence Engine service.

PWSAboveCPULimit

Alert Description

This alert indicates that the Presence Web Service module running in the Cisco SIP Proxy service has detected that the CPU utilization has exceeded the configured threshold. During this time, new requests are blocked until the CPU utilization drops below the configured threshold.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Using Unified RTMT, inspect the Cisco SIP Proxy service logs for more details.

PWSAboveSipSubscriptionLimit

Alert Description

This alert indicates that the Presence Web Service running in the Cisco SIP Proxy service has detected that the subscription count has exceeded the configured limit. During this time the Presence Web Service will block new incoming SIP subscriptions until the subscription count drops below the configured limit.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Using Cisco RTMT, inspect the Cisco SIP Proxy service logs for more details.

PWSRequestLimitReached

Alert Description

This alert indicates that the Cisco SIP Proxy service request per second limit has been reached.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

You may need to throttle back the incoming request rate.

PWSSCBFindFailed

Alert Description

This alert indicates that a call to find_scb() returned NULL which indicates the SCB lookup failed.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

PWSSCBInitFailed

Alert Description

This alert indicates that SCB init has failed.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Restart the Cisco SIP Proxy service.

ReplicationDefaultIMDomainChangeFailure

Alert Description

This alert occurs when a local default IM domain change fails.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Rerun the local default IM domain change procedure from the Advanced Presence Setting page.

ReplicationIMAddressSchemeChangeFailure

Alert Description

This alert occurs when an IM Address Scheme change fails.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Rerun the IM Address Scheme change procedure from the Advanced Presence Settings page.

SRMFailover

Type

IM and Presence Service

Alert Description

This alert indicates that the Server Recovery Manager is performing an automatic failover.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Verify that the failed node is up and that critical services are running.

SRMFailed

Alert Description

This alert indicates that the Server Recovery Manager is in the Failed state.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

When it is convenient restart the Server Recovery Manager.

SyncAgentAXLConnectionFailed

Alert Description

This alert occurs when the Cisco Sync Agent service failed authentication.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please verify that the AXL credentials are correct and whether the Cisco AXL Web service is activated and running on the remote Unified Communications Manager publisher.

UASCBFindFailed

Alert Description

This alert indicates that a call to find_scb() returned NULL which indicates the SCB lookup failed.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

UASCBGetFailed

Alert Description

This alert indicates that a call to tcbtable_acquire_tcb() returned NULL which indicates a SCB get/create failure.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Use Cisco RTMT to check the Cisco SIP Proxy service trace log file for any detailed error messages.

XcpCmComponentConnectError

Alert Description

This alert indicates that the Cisco XCP Connection Manager is shutting down because it failed to connect to the Cisco XCP Router.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the Cisco XCP Connection Manager log file for more details.

XcpCmPauseSockets

Alert Description

This alert indicates that the outstanding XCP internal packet or database requests have reached configured limit. Client connections will be paused until pending requests have dropped back below threshold. Users will experience lag until issue is resolved. Users may be disconnected if configured timeout is reached before resolution.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the XCP Router log file for more details. Monitor client disconnecting due to timeout from the XCP Connection Managers.

XcpCmStartupError

Alert Description

This alert indicates that the XCP Connection Manager service failed to startup.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the CM log file for more details.

XcpCmXmppdError

Alert Description

This alert indicates that the XCP Connection Manager (CM) service has errors in the XMPP interface.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the CM log file for more details.

XCPConfigMgrConfigurationFailure

Alert Description

This alert indicates that the Cisco XCP Config Manager failed to successfully update XCP configuration.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

See the Cisco XCP Config Manager logs for the root cause. Contact Cisco TAC for assistance.

XCPConfigMgrHostNameResolutionFailed

Alert Description

This alert indicates that the Cisco XCP Config Manager could not resolve a DNS name to allow Cisco XCP Routers to connect to that node.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Verify DNS resolvability of all hostnames and FQDNs in both local and remote clusters. Restart the Cisco XCP Config Manager and then restart the Cisco XCP Router after DNS is resolvable.

XCPConfigMgrJabberRestartRequired

Alert Description

This alert indicates that the Cisco XCP Config Manager has regenerated XCP XML files after system halt due to buffer size. The Cisco XCP Router must now be restarted to apply changes.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

When it is convenient to do so, restart the Cisco XCP Router.

XCPConfigMgrR2RPasswordEncryptionFailed

Alert Description

This alert indicates that the Cisco XCP Config Manager was unable to encrypt the password that is associated with an Inter-cluster Router-to-Router configuration.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

When it is convenient to do so, restart the Cisco XCP Config Manager and then restart the Cisco XCP Router.

XCPConfigMgrR2RRequestTimedOut

Alert Description

This alert indicates that Cisco XCP Config Manager sent an R2R configuration request to the XCP Router, but the XCP Router did not acknowledge the request in the time allowed.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Restart the Cisco XCP Config Manager and then restart the XCP Router.

XcpDBConnectError

Alert Description

Cisco XCP data access layer was unable to connect to the DB. This may indicate that the local or external database is down or the network connectivity to the external database is lost.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the System Troubleshooter for more information. Also check that the external database is running healthy and if there is any problem with the network connectivity to the external database server.

XcpMdnsStartError

Alert Description

This alert indicates that the XCP Router failed to startup the Multicast Domain Name Service (MDNS). This can cause connectivity failures to other routers in the cluster.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the XCP Router log file for more details.

XcpMessArchDBConnectError

Alert Description

This alert occurs when the Cisco XCP data access layer was unable to connect to the dB.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please check the System Troubleshooter for more information. Also check that the external database is running healthy and if there is any problem with the network connectivity to the external database server.

XcpMessArchDBFullError

Alert Description

This alert occurs when the Cisco XCP data access layer was unable to insert data into the dB due to insufficient disk space or tablespace.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please free up the disk space or tablespace on the external dB.

XcpMFTDBConnectError

Alert Description

This alert indicates that the Cisco XCP data access layer was unable to connect to the external database.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Check the System Troubleshooter for more information. Also check that the external database is running healthy and if there is a problem with the network connectivity to the external database server.

XcpMFTDBFullError

Alert Description

This alert occurs when the Cisco XCP data access layer was unable to insert data into the dB due to insufficient disk space or tablespace.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please free up the disk space or tablespace on the dB.

XcpMFTExtFsFreeSpaceWarn

Alert Description

This alert indicates that the Cisco XCP File Transfer Manager has detected that the available disk space on the external file server is low.

Unified RTMT Default Threshold

Less than 10% of the file server disk space remains.

Recommended Actions

The alert is cleared by increasing disk space to greater than 15%. Free up space on the external file server by deleting unwanted files from the partition used for file transfers.

XcpMFTExtFsMountError

Alert Description

This alert indicates that the Cisco XCP File Transfer Manager has lost its connection to the external file server.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Check the External File Server Troubleshooter for more information. Also check that the external file server is running correctly or if there is a problem with the network connectivity to the external file server.

XcpSIPFedCmComponentConnectError

Alert Description

This alert indicates that the Cisco XCP SIP Federation Connection Manager is shutting down as it failed to connect to the Cisco XCP Router.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the Cisco XCP SIP Federation Connection Manager log file for more details.

XcpSIPFedCmPauseSockets

Alert Description

This alert occurs when the XCP Router has directed the XCP SIP Federation Connection Manager (CM) to pause listening on its socket due to load on the system.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please check the XCP Router log file for more details. Watch for the client disconnecting due to timeout from the XCP Connection Managers.

XcpSIPFedCmStartupError

Alert Description

This alert indicates that the Cisco XCP SIP Federation Connection Manager service has failed to start.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the Cisco XCP SIP Federation Connection Manager log file for more details.

XcpSIPGWStackResourceError

Alert Description

This alert indicates that the maximum supported concurrent SIP Federation subscriptions or SIP Federation IM sessions has been reached, and the Cisco XCP SIP Federation Connection Manager does not have the resources that are required to handle any addition subscriptions or IM sessions.

Unified RTMT Default Threshold

Not Applicable

Recommended Actions

Increase the Pre-allocated SIP stack memory Service Parameter for the Cisco XCP SIP Federation Connection Manager. Note: If you are changing this setting, make sure that you have the memory available. If you do not have enough memory, you may have reached the limit of your hardware capability.

XcpThirdPartyComplianceConnectError

Alert Description

This alert indicates that Cisco XCP Router is unable to connect to the Third Party Compliance Server. This may be because of a network problem or a Third Party Compliance Server configuration or licensing problem.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

This is a serious error that breaks IM on the IM and Presence Service. Check network connection to and configuration(including licensing) on Third Party Compliance Server. To restore IM services set the Compliance Settings option in the Administration GUI to Not Configured until the connection failure cause is identified.

XcpTxtConfComponentConfigError

Alert Description

This alert occurs when the XCP component detected a bad configuration.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please check the component log file for more details.

XcpTxtConfDBConnectError

Alert Description

This alert indicates that the Cisco XCP Text Conferencing data access layer was unable to connect to the external database.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the system troubleshooter for more information. Also check if the external database is running properly and if there is any problem with the network connectivity to the external database server.

XcpTxtConfDBFullError

Alert Description

This alert occurs when the Cisco XCP data access layer was unable to insert data into the dB due to insufficient disk space or tablespace.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please free up the disk space or tablespace on the dB.

XcpTxtConfDbQueueSizeLimitError

Alert Description

This alert occurs when the number of dBrequests has reached the maximum limit specified by the configuration.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the state of the external database server and check that it is accessible over the network. Then restart the Cisco XCP Text Conference Manager on CUP.

XcpTxtConfGearError

Alert Description

This alert indicates that the XCP Text Conference Manager (TC) Service has failed to load a configured component. This can prevent the service to start or behave as expected.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the XCP Text Conference log file for more details.

XcpTxtConfTCMessagesMsgIdError

This alert occurs when the XCP component detected an error message.

The following table contains information about the XcpTxtConfTCMessagesMsgIdError counter.

Table 235: XcpTxtConfTCMessagesMsgIdError

Counters	Counter Description
Enable Alert	Selected
Severity	Error
Enable or Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: when Invalid state of table tc_ in the external database event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

XcpWebCmComponentConnectError

Alert Description

This alert indicates that the Cisco XCP Web Connection Manager is shutting down as it failed to connect to the Cisco XCP Router.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the Cisco XCP Web Connection Manager log file for more details.

XcpWebCmHttpdError

Alert Description

This alert indicates that the Cisco XCP Web Connection Manager service has errors in the HTTP interface.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the Cisco XCP Web Connection Manager log file for more details.

XcpWebCmPauseSockets

Alert Description

This alert occurs when the XCP Router has directed the XCP Web Connection Manager (CM) to pause listening on its socket due to load on the system.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please check the XCP Router log file for more details. Watch for the client disconnecting due to timeout from the XCP Connection Managers.

XcpWebCmStartupError

Alert Description

This alert indicates that the Cisco XCP Web Connection Manager service has failed to start.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the Cisco XCP Web Connection Manager log file for more details.

XcpXMPPFedCmComponentConnectError

Alert Description

This alert indicates that the Cisco XCP XMPP Federation Connection Manager is shutting down because it failed to connect to the Cisco XCP Router.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Check the Cisco XCP XMPP Federation Connection Manager log file for more details.

XcpXMPPFedCmPauseSockets

Alert Description

This alert occurs when the XCP Router has directed the XCP XMPP Federation Connection Manager (CM) to pause listening on its socket due to load on the system.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please check the XCP Router log file for more details. Watch for the client disconnecting due to timeout from the XCP Connection Managers.

XcpXMPPFedCmStartupError

Alert Description

This alert occurs when the XCP XMPP Federation Connection Manager service failed to startup.

Unified RTMT Default Threshold

Not applicable.

Recommended Actions

Please check the CM log file for more details.

Intercompany Media Engine Alerts

BannedFromNetwork

This alert indicates that network administrators have banned this Cisco IME server from the network (IME distributed cache ring), making this Cisco IME service fully or partly inoperative. Network administrators rarely ban servers but do so if they detect that the server is being used to launch malicious attacks into the network. If you receive this alert in error, contact TAC immediately.

Default Configuration

Table 236: Default Configuration for the BannedFromNetwork Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME service banned from network
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheCertificateExpiring

This alert indicates the number of days that remain until the certificate that is used for the IME distributed cache expires. You must replace the certificate prior to expiration.

Default Configuration

Table 237: Default Configuration for the IMEDistributedCacheCertificateExpiring Alert

Value	Default Configuration
Enable Alert	Selected

Value	Default Configuration
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME distributed cache certificate about to expire. 14 days.
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 1440 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheFailure

This alert indicates the health of the IME distributed cache. A value of zero (red) means that the IME distributed cache is suffering from a significant problem such as one of the following conditions:

- The Cisco IME cannot resolve issues after the network was partitioned. In this case, validation attempts may fail.
- The Cisco IME service is not connected to the network at all and is unable to reach the bootstrap servers.

A value of one (yellow) indicates that the Cisco IME network is experiencing minor issues, such as connectivity between bootstrap servers or other Cisco IME network issues. Check for any alarms that may indicate why this counter is 1. A value of two indicates that IME distributed cache is functioning normally and the system is considered healthy.

Default Configuration

Table 238: Default Configuration for the IMEDistributedCacheFailure Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers

Value	Default Configuration
Threshold	Trigger alert when following condition met: IME distributed cache failure in states 1: network experience minor issues 0: network in trouble
Duration	Trigger alert immediately
Frequency	Trigger 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMESdlLinkOutOfService

This alert indicates that the Cisco IME service has lost communication with Cisco IME Config Manager services, such as the Cisco AMC Service or the Cisco CallManager Service.

This alert usually indicates that one of these services has gone down (either intentionally, for maintenance; or unintentionally, due to a service failure or connectivity failure).

Default Configuration

Table 239: Default Configuration for the IMESdlLinkOutOfService Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SDLLinkOOS event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCertificate

This alert indicates that the administrator enabled the IME distributed cache on the Cisco IME server but omitted the configuration of a valid certificate or configured an incorrect certificate.

Default Configuration

Table 240: Default Configuration for the InvalidCertificate Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Invalid certificate configured
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCredentials

The alert indicates that the Unified Communications Manager cannot connect to the Cisco IME server, because the username and password that are configured on Unified Communications Manager do not match those configured on the Cisco IME server.

The alert includes the username and password that were used to connect to the Cisco IME server as well as the IP address and name of the target Cisco IME server. To resolve this alert, log into the Cisco IME server and check that the username and password that are configured match those configured in Unified Communications Manager.

Default Configuration

Table 241: Default Configuration for the InvalidCredentials Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Invalid or mismatched credentials.
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MessageOfTheDay

The Cisco IME service generates this alert when the administrators of the Cisco IME network have a message for you.

Default Configuration

Table 242: Default Configuration for the MessageOfTheDay Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Notice
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Message from network administrators
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 1440 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SWUpdateRequired

The Cisco IME server generates this alert when a new version of the Cisco IME server software is required. This alert repeats until you perform the upgrade. To obtain more information about the software update, go to the Cisco website. You should install critical updates within days of receiving this alert.

These upgrades address security vulnerabilities or key functional outages. In some cases, if you do not apply a critical upgrade immediately, the Cisco IME server may become unable to connect to the network.

Default Configuration

Table 243: Default Configuration for the SWUpdateRequired Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Software update required
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TicketPasswordChanged

The Cisco IME server generates this alert when the administrator changes the password that is used to generate the validation tickets.

Verify that an authorized administrator changed the password. Unauthorized changes may indicate compromise to the administrative interfaces on the Cisco IME service. If you determine that unauthorized changes have been made, change the administrative passwords on the Cisco IME server immediately to prevent further unauthorized access. To change the administrative password, type **set password admin** in the Cisco IME server CLI.

Default Configuration

Table 244: Default Configuration for the TicketPasswordChanged Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Notice
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Ticket password changed
Duration	Trigger alert immediately
Frequency	Trigger on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ValidationsPendingExceeded

This alert indicates the number of pending validations on the Cisco IME server. This number provides an indicator of the backlog of work on the Cisco IME server.

Default Configuration

Table 245: Default Configuration for the ValidationsPendingExceeded Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME pending validations exceeded 100
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within 60 minutes

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

Cisco Unity Connection Alerts

NoConnectionToPeer

(Cisco Unity Connection cluster configuration) This alert is generated when the servers of a Cisco Unity Connection cluster cannot communicate with each other (for example, when the network connection is lost).

Default Configuration

Table 246: Default Configuration for the NoConnectionToPeer RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: NoConnectionToPeer event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailoverSucceeded

(Cisco Unity Connection cluster configuration) This alert is generated in the following conditions:

- When the server with the Secondary status automatically changes its status to Primary (for example, when a critical failure occurs on the server with the Primary status) and assumes responsibility for handling the voice messaging functions and database for the cluster. This alert signals that the following events occurred:

  - The server that originally had the Primary status experienced a serious failure.
  - The server that originally had the Secondary status now has the Primary status and is handling all calls successfully.

- When the server that stopped functioning (described above) is brought back online and the server status automatically changes so that both servers resume sharing responsibility for handling the voice messaging functions and replication.

Default Configuration

Table 247: Default Configuration for the AutoFailoverSucceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailoverSucceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailoverFailed

(Cisco Unity Connection cluster configuration) This alert is generated in the following conditions:

- When the server with the Secondary status attempts to automatically change its status to Primary (for example, when a critical failure occurs on the server with the Primary status), but the automatic server status change fails so that the server with the Secondary status keeps the Secondary status.
- When a server that has stopped functioning (for example, a critical failure occurred) is not brought back online. Only one server in the cluster is functioning.

Default Configuration

Table 248: Default Configuration for the AutoFailoverFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailoverFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailbackSucceeded

(Cisco Unity Connection cluster configuration) This alert is generated when the problem that caused the server with the Primary status to stop functioning (causing the server with the Secondary status to change its status to Primary) is resolved and both servers are again online. Then, the servers automatically change status so that the server that had stopped functioning has the Primary status and the other server has the Secondary status.

Default Configuration

Table 249: Default Configuration for the AutoFailbackSucceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailbackSucceeded event generated

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

AutoFailbackFailed

(Cisco Unity Connection cluster configuration): This alert occurs when the publisher node is not online and the server with the Primary status fails to automatically change status.

Default Configuration

Table 250: Default Configuration for the AutoFailbackFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: AutoFailbackFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SbrFailed (Split Brain Resolution Failed)

When a Cisco Unity Connection cluster is configured, if two servers cannot communicate with each other, they will both have the Primary status at the same time (a “split brain” condition), handle voice messaging functions, save messages to their own message stores, but not perform any replication. Users can retrieve their messages, but only one server knows that these messages have been retrieved.

When both servers are able to communicate with each other, they resolve this split brain condition by determining the correct contents and state of each user mailbox:

- Whether new messages that have been received.
- Whether MWIs for new messages have already been sent.
- Which messages have been listened to.
- Which messages have been deleted.

If the resolution of the split brain condition fails, this alert occurs.

Default Configuration

Table 251: Default Configuration for the SbrFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational
Threshold	Trigger alert when following condition met: SbrFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DiskConsumptionCloseToCapacityThreshold

This alert is generated when the hard disk usage on the Cisco Unity Connection server reaches ten percent below the percentage limit that the **System Settings** > **Advanced** > **Disk Capacity** window in Cisco Unity Connection Administration specifies. For example, with a capacity threshold limit of 95 percent, the alert gets triggered when usage reaches at least 85 percent.

Default Configuration

Table 252: Default Configuration for the DiskConsumptionCloseToCapacityThreshold RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error

Value	Default Configuration
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: DiskConsumptionCloseToCapacityThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DiskConsumptionExceedsCapacityThreshold

This alert is generated when the hard disk usage on the Cisco Unity Connection server meets or exceeds the percentage limit that the **System Settings** > **Advanced** > **Disk Capacity** window in Cisco Unity Connection Administration specifies.

Default Configuration

Table 253: Default Configuration for the DiskConsumptionExceedsCapacityThresholdRTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: DiskConsumptionExceedsCapacityThreshold event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LicenseExpirationWarning

Cisco Unity Connection licenses several features, including users and ports. The system enforces these licenses. If a customer uses a time-limited license to sample a feature, this license includes an expiration date. Before the license expiration date is reached, the system sends a message, and this alert occurs. The log indicates how many days remain until the license expires.

Default Configuration

Table 254: Default Configuration for the LicenseExpirationWarning RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: LicenseExpirationWarning event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LicenseExpired

Cisco Unity Connection licenses several features, including users and ports. The system enforces these licenses. If a customer uses a time-limited license to sample a feature, this license includes an expiration date. When the license expiration date is reached, the license becomes invalid, and this alert occurs.

Default Configuration

Table 255: Default Configuration for the LicenseExpired RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Informational

Value	Default Configuration
Enable/Disable this alert on following server(s)	Enabled
Threshold	Trigger alert when following condition met: LicenseExpired event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

System Error Messages

System Error Messages

For a complete list of system error messages, see the *System Error Messages for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-system-message-guides-list.html.