

Configure Real Time Monitoring Tool to Audit Admin Activity in Cisco Unified Communications Manager

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure the Real Time Monitoring Tool (RTMT) to view and audit real time activity in Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CUCM Administration
- CUCM Trace Configuration
- RTMT Navigation

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Unified Communications Manager
- Real Time Monitoring Tool

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, Ensure that you understand the potential impact of any command.

Background Information

For CUCM the application audit log supports configuration updates for CUCM interfaces such as

Communications Manager Administration, Cisco Unified RTMT, Cisco Unified Communications Manager CDR Analysis and Reporting and Cisco Unified Serviceability.

For IM and Presence Service the application audit log supports configuration updates for IM and Presence interfaces such as Cisco Unified Communications Manager IM and Presence Administration, Cisco Unified IM and Presence Real-Time Monitoring Tool and Cisco Unified IM and Presence Serviceability.

For Cisco Unity Connection the application audit log supports configuration updates for Cisco Unity Connection interfaces, Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant and clients that use the Connection REST Application Programming Interfaces (APIs).

Configure

Follow these steps in order to configure audit log capability and view audit trail from RTMT.

Step 1. Enable Audit Log. Navigate to **Cisco Unified Serviceability > Tools > Audit Log Configuration** and enable these parameters

- Enable Audit Log
- Enable Purging
- Enable Log Rotation
- Detailed Audit Logging (Detailed audit logs provide the same items as regular audit logs, but also include configuration changes. For example, the audit log includes items that were added, updated, and deleted, including the modified values.)

Note: You must enable these services, **Network Service Audit Event Service** and **Network Service Cisco Log Partitions Monitoring**

Tip: When log rotation is disabled (unchecked), audit log ignores the Maximum No. of Files setting.

Audit Log Configuration



Save



Set to Default

Status:

Ready

Select Server

Server*

Apply to All Nodes

Application Audit Log Settings

Filter Settings

- Enable Audit Log
- Enable Purging
- Enable Log Rotation
- Detailed Audit Logging

Remote Syslog

Server Name¹

Remote Syslog Audit Event Level

Output Settings

Maximum No. of Files*

Maximum File Size (MB)*

Notification Settings

Warning Threshold for Approaching Log Rotation Overwrite (%)*

Database Audit Log Filter Settings

Enable Audit Log

Debug Audit Level

Output Settings

Enable Audit Log Rotation

Maximum No. of Files*

No. of Files Deleted on Log Rotation*

Step 2. Now you can use RTMT to view Audit Logs. Open and log in to Cisco RTMT. Navigate to **System > Tools > AuditLog Viewer** and select the node from which you would like to monitor activity.

Step 3. Select **AuditApp Logs** and from the selection list and choose the desired .log file. You are presented with a view of events for the selected log file.

File System Voice/Video AnalysisManager IM and Presence Edit Window Application Help

Real Time Monitoring Tool For Cisco Unified Communications Solutions

System
AuditLog Viewer cucm1151pub.ad.erleite.com Auto Refresh

System Summary

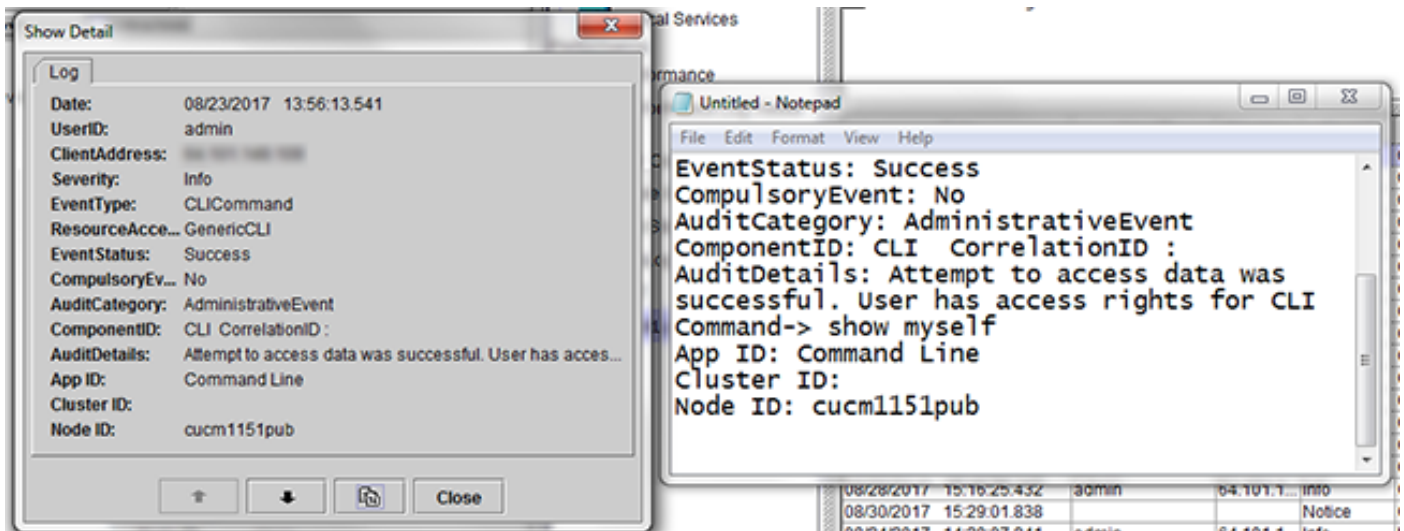
- System Summary
- Server
 - CPU and Memory
 - Process
 - Disk Usage
 - Critical Services
- Performance
 - Performance
 - Performance Log Viewer
- Tools
 - Alert Central
 - Trace & Log Central
 - Job Status
 - SysLog Viewer
 - VLT
 - AuditLog Viewer**

Logs

- AuditApp Logs
 - Archive
 - Audit00000012.log**
- Cisco Unified OS Logs

Date	UserID	ClientAd...	Severity ▾	EventType	Re
08/24/2017 16:37:04.752	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/24/2017 16:37:06.257	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/24/2017 16:37:17.131	admin	64.101.1...	Error	UserLogging	Cisco SOAP Serve
08/24/2017 16:40:31.716	admin	64.101.1...	Error	UserLogging	Cisco Trace Collec
08/25/2017 15:18:37.030	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/25/2017 15:18:38.314	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/25/2017 15:18:48.385	admin	64.101.1...	Error	UserLogging	Cisco SOAP Serve
08/25/2017 15:20:04.751	admin	64.101.1...	Error	UserLogging	Cisco Trace Collec
08/28/2017 15:09:15.698		64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:15.751		64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:28.996	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:29.053	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:48.575	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:09:48.720	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:11:32.090	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:11:32.142	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:14:27.341	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:14:28.661	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 15:14:38.874	admin	64.101.1...	Error	UserLogging	Cisco SOAP Serve
08/28/2017 16:33:50.695	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 16:33:51.944	admin	64.101.1...	Error	UserLogging	Cisco CallManage
08/28/2017 16:34:01.460	admin	64.101.1...	Error	UserLogging	Cisco SOAP Serve
08/29/2017 13:25:12.187	admin	10.201.2...	Error	UserLogging	Apache-Axis2
08/29/2017 13:50:16.272	admin	10.201.2...	Error	UserLogging	Apache-Axis2

Step 4. Select the desired entry twice to view further event details. In this example we have a CLI command audit trail that indicates the command **show myself** was performed on node, **cucm1151pub**. Select the icon with double page image to copy the alert details which can be pasted elsewhere.



Tip: Select the checkbox for **Auto Refresh** to enable dynamic updates to log entries within the AuditLog Viewer.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Audit Log Configuration Settings](#)