Audit Logs

Audit Logs

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

Audit Logging (Standard)

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

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

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

Standard audit logging contains the following parts:

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

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

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

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

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

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

Cisco Unified Serviceability Standard Events Logging

Cisco Unified Serviceability logs the following events:

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

Cisco Unified Real-Time Monitoring Tool Standard Events Loggin

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

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

Unified Communications Manager Standard Events Logging

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

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

Cisco Unified CM Administration Standard Events Logging

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

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

Cisco Unified Communications Self Care Portal Standard Events Logging

User logging (user login and user logout) events are logged for Cisco Unified Communications Self Care Portal.

Command-Line Interface Standard Events Logging

All commands issued via the command-line interface are logged (for both Unified Communications Manager and Cisco Unity Connection).

Cisco Unity Connection Administration Standard Events Logging

Cisco Unity Connection Administration logs the following events:

- User logging (user logins and user logouts)

- All configuration changes, including but not limited to users, contacts, call management objects, networking, system settings, and telephony
- Task management (enabling or disabling a task)
- Bulk Administration Tool (bulk creates, bulk deletes)
- Custom Keypad Map (map updates)

Cisco Personal Communications Assistant (Cisco PCA) Standard Events Logging

The Cisco Personal Communications Assistant client logs the following events:

- User logging (user logins and user logouts)
- All configuration changes made via the Messaging Assistant

Cisco Unity Connection Serviceability Standard Events Logging

Cisco Unity Connection Serviceability logs the following events:

- User logging (user logins and user logouts).
- All configuration changes.
- Activating, deactivating, starting or stopping services.

Cisco Unity Connection Clients that Use the Representational State Transfer APIs Events Logging

Cisco Unity Connection clients that use the Representational State Transfer (REST) APIs log the following events:

- User logging (user API authentication).
- API calls that utilize Cisco Unity Connection Provisioning Interface.

Cisco Unified IM and Presence Serviceability Standard Events Logging

Cisco Unified IM and Presence Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service
- Changes in trace configurations and alarm configurations
- Changes in SNMP configurations
- Review of any report in the Serviceability Reports Archive (this log gets viewed on the reporter node)

Cisco Unified IM and Presence Real-Time Monitoring Tool Standard Events Logging

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

- Alert configuration
- Alert suspension

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

Cisco IM and Presence Administration Standard Events Logging

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

- Administrator logging (logins and logouts on IM and Presence interfaces such as Administration, OS Administration, Disaster Recovery System, and Reporting)
- User role membership updates (user added, user deleted, user role updated)
- Role updates (new roles added, deleted, or updated)
- Device updates (phones and gateways)
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, hostnames, Ethernet settings, and IM and Presence server additions or deletions)

IM and Presence Application Standard Events Logging

The following events get logged by the various components of the IM and Presence Application:

- End user logging on IM clients (user logins, user logouts, and failed login attempts)
- User entry to and exit from IM Chat Rooms
- Creation and destruction of IM Chat Rooms

Command Line Interface Standard Events Logging

All commands issued through the command line interface are logged.

Audit Logging (Detailed)

Detailed audit logging is an optional feature that logs additional configuration modifications that are not stored in standard (default) audit logs. In addition to all of the information that is stored in standard audit logs, detailed audit logging also includes configuration items that were added, updated, and deleted, including the modified values. Detailed audit logging is disabled by default, but you can enable it in the **Audit Log Configuration** window.

Audit Log Types

System Audit Logs

System audit logs track activities such as the creation, modification, or deletion of Linux OS users, log tampering, and any changes to file or directory permissions. This type of audit log is disabled by default due to the high volume of data gathered. To enable this function, you must manually enable utils auditd using the CLI. After you have enabled the system audit log feature, you can collect, view, download, or delete selected logs through Trace & Log Central from the Real-Time Monitoring Tool. System audit logs take on the format of `vos-audit.log`.

For information about how to enable this feature, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. For information about how to access collected logs from the Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* .

Application Audit Logs

The Application Audit logs monitor and record any configuration changes to the system that were made by a user or as a result of the user action.

Note The Application Audit Logs (Linux auditd) can be enabled or disabled only through the CLI. Other than the collection of vos-audit.log through the Real-Time Monitoring Tool, you can not change any settings for this type of audit log.

Database Audit Logs

Database Audit Logs track all activities associated with access to the Informix Database, such as logins.

Audit Log Configuration Task Flow

Complete the following tasks to configure audit logging.

Procedure

	Command or Action	Purpose
Step 1	Set up Audit Logging, on page 7	Set up your audit log configuration in the Audit Log Configuration window. You can configure whether you want to use remote audit logging and whether you want the Detailed Audit Logging option.
Step 2	Configure Remote Audit Log Transfer Protocol, on page 8	Optional. If you have remote audit logging configured, configure the transfer protocol. The system default in normal operating mode is UDP, but you can also configure TCP or TLS
Step 3	Configure Email Server for Alert Notifications, on page 8	Optional. In RTMT, set up the email server for email alerts.

	Command or Action	Purpose
Step 4	Enable Email Alerts, on page 8	Optional. Set up one of the following email alerts: • If you have remote audit logging configured with TCP, set up the email notification for the **TCPRemoteSyslogDeliveryFailed** alert. • If you have remote audit logging configured with TLS, set up the email notification for the **TLSRemoteSyslogDeliveryFailed** alert.
Step 5	Configure Remote Audit Logging for Platform Logs, on page 9	Set up remote audit logging for platform audit logs and remote server logs. For these types of audit logs, you must configure a FileBeat client and external logstash server.

Set up Audit Logging

Before you begin

For remote audit logging, you must have already set up your remote syslog server and configured IPSec between each cluster node and the remote syslog server, including connections to any gateways in between. For IPSec configuration, see the *Cisco IOS Security Configuration Guide*.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Audit Log Configuration**.

Step 2 From the **Server** drop-down menu, select any server in the cluster and click **Go**.

Step 3 To log all cluster nodes, check the **Apply to All Nodes** check box.

Step 4 In the **Server Name** field, enter the IP Address or fully qualified domain name of the remote syslog server.

Step 5 Optional. To log configuration updates, including items that were modified, and the modified values, check the **Detailed Audit Logging** check box.

Step 6 Complete the remaining fields in the **Audit Log Configuration** window. For help with the fields and their descriptions, see the online help.

Step 7 Click **Save**.

What to do next

Configure Remote Audit Log Transfer Protocol, on page 8

Configure Remote Audit Log Transfer Protocol

Use this procedure to change the transfer protocol for remote audit logs. The system default is UDP, but you can reconfigure to TCP or TLS.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils remotesyslog show protocol** command to confirm which protocol is configured.

Step 3 If you need to change the protocol on this node, do the following:

- To configure TCP, run the **utils remotesyslog set protocol tcp** command.
- To configure UDP, run the **utils remotesyslog set protocol udp** command.
- To configure TLS, run the **utils remotesyslog set protocol tls** command.

Note In Common Criteria Mode, strict host name verification is implemented. Hence, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

Step 4 If you changed the protocol, restart the node.

Step 5 Repeat this procedure for all Unified Communications Manager and IM and Presence Service cluster nodes.

What to do next

Configure Email Server for Alert Notifications, on page 8

Configure Email Server for Alert Notifications

Use this procedure to set up your email server for alert notifications.

Procedure

Step 1 In the Real-Time Monitoring Tool's System window, click **Alert Central**.

Step 2 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

Step 3 In the **Mail Server Configuration** popup, enter the details for the mail server.

Step 4 Click **OK**.

What to do next

Enable Email Alerts, on page 8

Enable Email Alerts

If you have remote audit logging with TCP or TLS configured, use this procedure to set up an email alert to notify you of transmission failures.

Procedure

Step 1 In the Real-Time Monitoring Tool **System** area, click **Alert Central**.

Step 2 In the **Alert Central** window,

- If you have remote audit logging with TCP, select **TCPRemoteSyslogDeliveryFailed**
- If you have remote audit logging with TLS, select **TLSRemoteSyslogDeliveryFailed**

Step 3 Choose **System** > **Tools** > **Alert** > **Config Alert Action**.

Step 4 In the **Alert Action** popup, select **Default** and click **Edit**.

Step 5 In the **Alert Action** popup, **Add** a recipient.

Step 6 In the popup window, enter the address where you want to send email alerts and click **OK**.

Step 7 In the **Alert Action** popup, make sure that the address appears under **Recipients** and that the **Enable** check box is checked.

Step 8 Click **OK**.

Configure Remote Audit Logging for Platform Logs

Complete these tasks to add remote audit logging support for platform audit logs, remote support logs, and Bulk Administration csv files. For these types of logs, the FileBeat client and logstash server get used.

Before you begin

Make sure that you have set up an external logstash server.

Procedure

	Command or Action	Purpose
Step 1	Configure Logstash Server Information, on page 9	Configure the FileBeat client with the external logstash server details, such as IP addresses, ports and file types.
Step 2	Configure the FileBeat Client, on page 10	Enable the FileBeat client for remote audit logging.

Configure Logstash Server Information

Use this procedure to configure the FileBeat client with the external logstash server information, such as IP address, port number, and downloadable file types.

Before you begin

Make sure that you have set up your external logstash server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat configure** command.

Step 3 Follow the prompts to configure the logstash server details.

Configure the FileBeat Client

Use this procedure to enable or disable the FileBeat client for uploads of platform audit logs, remote support logs, and Bulk Administration csv files.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat status** command to confirm whether the FileBeat client is enabled.

Step 3 Run one of the following commands:

- To enable the client, run the **utils FileBeat enable** command.
- To disable the client, run the **utils FileBeat disable** command.

Note TCP is the default transfer protocol.

Step 4 Optional. If you want to use TLS as the transfer protocol, do the following:

- To enable TLS as the transfer protocol, run the **utils FileBeat tls enable** command.
- To disable TLS as the transfer protocol, run the **utils FileBeat tls disable** command.

Note To use TLS, a security certificate has to be uploaded from logstash server to the tomcat trust store on Unified Communications Manager and IM and Presence service.

Step 5 Repeat this procedure on each node.

Do not run any of these commands on all nodes simultaneously.

Audit Log Configuration Settings

Before You Begin

Be aware that only a user with an audit role can change the audit log settings. By default, for Unified Communications Manager, the CCMAdministrator possesses the audit role after fresh installs and upgrades. The CCMAdministrator can assign any user that has auditing privileges to the Standard Audit Users group in the User Group Configuration window in Cisco Unified Communications Manager Administration. If you want to do so, you can then remove CCMAdministrator from the Standard Audit Users group.

For IM and Presence Service, the administrator possesses the audit role after fresh installs and upgrades, and can assign any user that has auditing privileges to the Standard Audit Users group.

For Cisco Unity Connection, the application administration account that was created during installation has the Audit Administrator role and can assign other administrative users to the role. You can also remove the Audit Administrator role from this account.

The Standard Audit Log Configuration role is to provide the ability to delete audit logs and to read/update access to Cisco Unified Real-Time Monitoring Tool, IM and Presence Real-Time Monitoring Tool, Trace Collection Tool, Real-Time Monitoring Tool (RTMT) Alert Configuration, Control Center - Network Services in the serviceability user interface, RTMT Profile Saving, Audit Configuration in the serviceability user interface, and a resource that is called Audit Traces.

The Standard Audit Log Configuration role is to provide the ability to delete audit logs and to read/update access to Cisco Unified RTMT, Trace Collection Tool, RTMT Alert Configuration, Control Center - Network Services in Cisco Unified Serviceability, RTMT Profile Saving, Audit Configuration in Cisco Unified Serviceability, and a resource that is called Audit Traces.

The Audit Administrator role in Cisco Unity Connection provides the ability to view, download and delete audit logs in Cisco Unified RTMT.

For information on roles, users, and user groups in Unified Communications Manager, refer to the *Administration Guide for Cisco Unified Communications Manager*.

For information on roles and users in Cisco Unity Connection, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

For information on roles, users, and user groups in IM and Presence, refer to *Configuration and Administration of IM and Presence Service on Unified Communications Manager*.

The following table describes the settings that you can configure in the Audit Log Configuration window in Cisco Unified Serviceability.

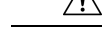
Table 1: Audit Log Configuration Settings

Field	Description
Select Server	
Server	Choose the server (node) where you want to configure audit logs; then, click **Go**.
Apply to All Nodes	If you want to apply the audit log configuration to all nodes in the cluster, check the **Apply to all Nodes** check box.
Application Audit Log Settings	

Field	Description
Enable Audit Log	When you check this check box, an audit log gets created for the application audit log. For Unified Communications Manager, the application audit log supports configuration updates for Unified Communications Manager user interfaces, such as Cisco Unified 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 user 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 user interfaces, including Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant, and clients that use the Connection REST APIs. This setting displays as enabled by default. **Note** The Network Service Audit Event Service must be running.
Enable Purging	The Log Partition Monitor (LPM) looks at the Enable Purging option to determine whether it needs to purge audit logs. When you check this check box, LPM purges all the audit log files in RTMT whenever the common partition disk usage goes above the high water mark; however, you can disable purging by unchecking the check box. If purging is disabled, the number of audit logs continues to increase until the disk is full. This action could cause a disruption of the system. A message that describes the risk of disabling the purge displays when you uncheck the Enable Purging check box. Be aware that this option is available for audit logs in an active partition. If the audit logs reside in an inactive partition, the audit logs get purged when the disk usage goes above the high water mark. You can access the audit logs by choosing **Trace and Log Central** > **Audit Logs** in RTMT. **Note** The Network Service Cisco Log Partitions Monitoring tool must be running.
Enable Log Rotation	The system reads this option to determine whether it needs to rotate the audit log files or it needs to continue to create new files. The maximum number of files cannot exceed 5000. When the Enable Rotation check box is checked, the system begins to overwrite the oldest audit log files after the maximum number of files is reached. **Tip** When log rotation is disabled (unchecked), audit log ignores the Maximum No. of Files setting.

Field	Description
Detailed Audit Logging	When this check box is checked, the system is enabled for detailed audit logs. Detailed audit logs provide the same items as regular audit logs, but also include configuration changes. For example, the audit log includes items that were added, updated, and deleted, including the modified values.
Server Name	Enter the name or IP address of the remote syslog server that you want to use to accept syslog messages. If server name is not specified, Cisco Unified IM and Presence Serviceability does not send the syslog messages. Do not specify a Unified Communications Manager node as the destination because the Unified Communications Manager node does not accept syslog messages from another server. This applies to IM and Presence Service only.
Remote Syslog Audit Event Level	Select the desired syslog messages severity for the remote syslog server. All the syslog messages with selected or higher severity level are sent to the remote syslog. This applies to IM and Presence Service only.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. The default setting specifies 250. The maximum number specifies 5000.
Maximum File Size	Enter the maximum file size for the audit log. The file size value must remain between 1MB and 10MB. You must specify a number between 1 and 10.
Warning Threshold for Approaching Log Rotation Overwrite (%)	The system can alert you when the audit logs are approaching the level where they will be overwritten. Use this field to set the threshold at which the system sends you an alert. For example, if you use the default settings of 250 files of 2 MB and a warning threshold of 80%, the system sends you an alarm when 200 files (80%) of audit logs have accumulated. If you want to keep the audit history, you can use RTMT to retrieve the logs before the system overwrites them. RTMT provides an option to delete the files after you collect them. Enter a value between 1 and 99%. The default is 80%. When you set this field, you must also check the **Enable Log Rotation** option. **Note** The total disk space allocated to audit logs is the Maximum No. of Files multiplied by the Maximum File Size. If the size of audit logs on the disk exceeds this percentage of total disk space allocated, the system raises an alarm in Alert Central.
Database Audit Log Filter Settings	
Enable Audit Log	When you check this check box, an audit log gets created for the Unified Communications Manager and Cisco Unity Connection databases. Use this setting in conjunction with the Debug Audit Level setting, which allows you create a log for certain aspects of the database.

Field	Description
Debug Audit Level	This setting allows you to choose which aspects of the database you want to audit in the log. From the drop-down list box, choose one of the following options. Be aware that each audit log filter level is cumulative. • **Schema** - Tracks changes to the setup of the audit log database (for example, the columns and rows in the database tables). • **Administrative Tasks** - Tracks all administrative changes to the Unified Communications Manager system (for example, any changes to maintain the system) plus all **Schema** changes. **Tip** Most administrators will leave the Administrative Tasks setting disabled. For users who want auditing, use the Database Updates level. • **Database Updates** - Tracks all changes to the database plus all **schema** changes and all **administrative tasks** changes. • **Database Reads** - Tracks every read to the system, plus all schema changes, administrative tasks changes, and database updates changes. **Tip** Choose the Database Reads level only when you want to get a quick look at the Unified Communications Manager, IM and Presence Service, or Cisco Unity Connection system. This level uses significant amounts of system resources and should be used only for a short time.
Enable Audit Log Rotation	The system reads this option to determine whether it needs to rotate the database audit log files or it needs to continue to create new files. When the Audit Enable Rotation option check box is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. When this setting check box is unchecked, audit log ignores the Maximum No. of Files setting.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. Ensure that the value that you enter for the Maximum No. of Files setting is greater than the value that you enter for the No. of Files Deleted on Log Rotation setting. You can enter a number from 4 (minimum) to 40 (maximum).
No. of Files Deleted on Log Rotation	Enter the maximum number of files that the system can delete when database audit log rotation occurs. The minimum that you can enter in this field is 1. The maximum value is 2 numbers less than the value that you enter for the Max No. of Files setting; for example, if you enter 40 in the Maximum No. of Files field, the highest number that you can enter in the No. of Files Deleted on Log Rotation field is 38.
Set to Default	The **Set to Default** button specifies the default values. It is recommended to set the audit logs to default mode unless it is required to be set to a different level for detailed troubleshooting. The **Set to Default** option minimizes the disk space utilized by log files.



Caution When enabled, database logging can generate large amounts of data in a short period, particularly if the debug audit level is set to **Database Updates** or **Database Reads**. This can result in a significant performance impact during heavy usage periods. In general, we recommend that you keep database logging disabled. If you do need to enable logging to track changes in the database, we recommend that you do so only for short periods of time, by using the **Database Updates** level. Similarly, administrative logging does impact on the overall performance of the web user interface, especially when polling database entries (for example, pulling up 250 devices from the database).