Audit logs

With audit logging, configuration changes to the Cisco Unified CCX system gets logged in separate log files for auditing.

Configuration Changes and Audit Logs

With audit logging, configuration changes to the Unified CCX system are logged in separate log files for auditing. The Cisco Audit Event Service, which is displayed under **Control Center - Network Services** in Cisco Unified Serviceability, monitors and logs any configuration change to the Cisco Unified CCX system that was made by a user or that resulted from a user action.

You access the Audit Log Configuration window in Cisco Unified Serviceability to configure the settings for the audit logs.

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.

The following Cisco Unified CCX components generate audit events:

- Cisco Unified Serviceability
- Cisco Unified Real-Time Monitoring Tool

Cisco Unified Serviceability

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.
- Review of any report in the Serviceability Reports Archive. This log gets viewed on the reporter node.

Cisco Unified Real-Time Monitoring Tool

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

- Alert configuration.
- Alert suspension.
- Email configuration.
- Set node alert status.
- Alert addition.
- Add alert action.
- Clear alert.
- Enable alert.
- Remove alert action.
- Remove alert.

Configure audit log

To configure the audit log, perform the following procedure:

Procedure

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

Step 2 Configure the settings in Table 1: Audit log configuration settings, on page 3.

Step 3 Click **Save**.

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

Audit log configuration settings

The table below 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 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 box.
Application Audit Log Settings	
Enable Audit Log	When you enable this check box, an audit log gets created for the application audit log, which supports configuration updates for Unified CCX graphical user interfaces (GUIs), such as Cisco Unified Real-Time Monitoring Tool and Cisco Unified Serviceability. This setting displays as enabled by default.
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**.
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 option is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. **Tip** When log rotation is disabled (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. The default setting specifies 250. The maximum number specifies 5000.
Maximum File Size	Enter the maximum file size for the audit log. The file size value must remain between 1 MB and 10 MB. You must specify a number between 1 and 10.
Database Audit Log Filter Settings	
Enable Audit Log	When you enable this check box, an audit log gets created for the database. 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 Only**—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 applicable Unified CCX system as mentioned in Configuration Changes and Audit Logs, on page 1 (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 Cisco Unified CCX system, plus all schema changes, administrative tasks changes, and database updates changes. **Tip** Choose the Database Reads level only when you want to get a quick look at the Cisco Unified CCX. This level uses significant amounts of system resources and only should be used 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 is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. When this setting 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.