CHAPTER 14

Configuring the Audit Log

With audit logging, configuration changes to the Cisco Unified Communications Manager system gets logged in separate log files for auditing. This chapter contains the following topics:

Understanding Audit Logging

With audit logging, configuration changes to the Cisco Unified Communications Manager system gets logged in separate log files for auditing. The Cisco Audit Event Service, which displays under Control Center—Network Services in Cisco Unified Serviceability, monitors and logs any configuration change to the Cisco Unified Communications Manager system by a user or as a result of the user action. For a Cisco Unified Communications Manager Business Edition system, this service supports both Cisco Unified Communications Manager and Cisco Unity Connection.

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

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 Cisco Unified Communications Manager components provide their own logging.

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

  ```
  User ID: CCMAdministrator
  Client 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.

The following Cisco Unified Communications Manager components generate audit events:

- Cisco Unified Serviceability, page 14-2
- Cisco Unified Real-Time Monitoring Tool, page 14-2
- Cisco Unified Communications Manager CDR Analysis and Reporting, page 14-3
- Cisco Unified Communications Manager Administration, page 14-3

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.
- Changes in CDR management.
- 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.
- E-mail configuration.
- Set node alert status.
- Alert addition.
- Add alert action.
- Clear alert.
- Enable alert.
- Remove alert action.
- Remove alert.

Cisco Unified Communications Manager CDR Analysis and Reporting

Cisco Unified Communications Manager 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 Communications Manager Administration

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, host names, Ethernet settings, and Cisco Unified Communications Manager server additions or deletions).

Configuring the 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 14-1.

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.

Additional Information

See the "Related Topics" section on page 14-7.

Audit Log Configuration Settings

Table 14-1 describes the settings that you can configure in the Audit Log Configuration window in Cisco Unified Serviceability. For more information on audit logging, see the "Where to Find More Information" section on page 14-7.

Before You Begin

Be aware that only a user with an audit role can change the audit log settings. By default, 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.

The Standard Audit Log Configuration role provides the ability to delete audit logs and to read/update access to Cisco Unified Real-Time Monitoring Tool, 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.

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

Table 14-1 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 Cisco Unified Communications Manager graphical user interfaces (GUIs), such as Cisco Unified Communications Manager Administration, Cisco Unified Real-Time Monitoring Tool, Cisco Unified Communications Manager CDR Analysis and Reporting, and Cisco Unified Serviceability. This setting displays as enabled by default.

Table 14-1 Audit Log Configuration Settings (continued)

Field	Description
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.

Table 14-1 Audit Log Configuration Settings (continued)

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 Cisco Unified Communications Manager system (for example, any changes to maintain the system) plus all Schema changes. **Tip** Most administrators will leave the Administrative Tasks setting disabled. For users who want auditing, use the Database Updates level. • **Database Updates**—Tracks all changes to the database plus all schema changes and all administrative tasks changes. • **Database Reads**—Tracks every read to the Cisco Unified Communications Manager 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 Communications Manager system. 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.

Where to Find More Information

Related Topics

- Understanding Audit Logging, page 14-1
- Configuring the Audit Log, page 14-3
- Audit Log Configuration Settings, page 14-4
- Configuring Trace, page 7-1
- Configuring Troubleshooting Trace Settings, page 8-1
- Network Services, page 9-9

Additional Cisco Documentation

- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*
- *Cisco Unified Communications Manager Administration Guide*