



# Configuring Trace in Cisco Unified Serviceability

- [Trace Configuration and Collection Checklist, page 3-1](#)
- [About Trace Parameter Configuration, page 3-2](#)
- [Audit Log Configuration, page 3-10](#)
- [About Troubleshooting Trace Settings, page 3-17](#)

## Trace Configuration and Collection Checklist

[Table 3-1](#) provides an overview of the steps for configuring and collecting trace for feature and network services in Cisco Unified Serviceability.

**Table 3-1** *Trace Configuration and Collection Checklist*

Configuration Steps		Related Procedures and Topics
<b>Step 1</b>	If you want to enable trace compression, select <b>Zip Files</b> under Download File Options during Trace Collection setup.	<i>Real-Time Monitoring Tool Administration Guide for Cisco Unified Presence</i>
<b>Step 2</b>	Select <b>System &gt; Service Parameters</b> in Cisco Unified Presence Administration and configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service).	<i>Real-Time Monitoring Tool Administration Guide for Cisco Unified Presence</i>
<b>Step 3</b>	Configure the trace setting for the service for which you want to collect traces. You can configure trace for the service on one server or on all servers in the cluster.  To configure trace settings, select what information you want to include in the trace log by choosing the debug level and trace fields.  If you want to run predetermined traces on services, set troubleshooting trace for those services.	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Trace Parameters, page 3-6</a></li> <li>• <a href="#">About Troubleshooting Trace Settings, page 3-17</a></li> </ul>
<b>Step 4</b>	Install the Cisco Unified Communications Manager Real-Time Monitoring Tool on a local PC.	<i>Real-Time Monitoring Tool Administration Guide for Cisco Unified Presence</i>

Table 3-1 Trace Configuration and Collection Checklist (continued)

Configuration Steps		Related Procedures and Topics
<b>Step 5</b>	<p>If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert in RTMT.</p> <p>You can find the LogFileSearchStringFound alarm in the LpmTctCatalog. (In Cisco Unified Serviceability, select <b>Alarms &gt; Definitions</b>. In the Find alarms where list box, select the <b>System Alarm Catalog</b>; in the Equals list box, select <b>LpmTctCatalog</b>.)</p>	<ul style="list-style-type: none"> <li><i>Real-Time Monitoring Tool Administration Guide for Cisco Unified Presence</i></li> <li><a href="#">About Alarm Definitions and User-Defined Descriptions, page 2-4</a></li> </ul>
<b>Step 6</b>	If you want to automatically capture traces for alerts such as CriticalServiceDown, check <b>Enable Trace Download</b> in the Set Alert/Properties dialog box for the specific alert in RTMT; configure how often that you want the download to occur.	<i>Real-Time Monitoring Tool Administration Guide for Cisco Unified Presence</i>
<b>Step 7</b>	Collect the traces.	<i>Real-Time Monitoring Tool Administration Guide for Cisco Unified Presence</i>
<b>Step 8</b>	View the log file in the appropriate viewer.	<i>Real-Time Monitoring Tool Administration Guide for Cisco Unified Presence</i>
<b>Step 9</b>	<p>If you enabled troubleshooting trace, reset the trace settings services, so the original settings are restored.</p> <p><b>Note</b> Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.</p>	<a href="#">About Troubleshooting Trace Settings, page 3-17</a>

## About Trace Parameter Configuration

- [Service Groups in Trace Configuration, page 3-4](#)
- [Configuring Trace Parameters, page 3-6](#)

Cisco Unified Serviceability provides trace tools to assist you in troubleshooting issues with your Presence and Instant Messaging application. Cisco Unified Serviceability supports:

- SDI (System Diagnostic Interface) trace
- Log4J trace (for Java applications)

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the trace files.) You can configure trace for a single service or apply the trace settings for that service to all servers in the cluster.

In the Alarm Configuration window, you can direct alarms to various locations, including SDI trace log files. If you want to do so, you can configure trace for alerts in the Cisco Unified Presence Real-Time Monitoring Tool (RTMT).

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the Trace & Log Central option in the RTMT. You can configure trace parameters for any feature or network service that is available on any Cisco Unified Presence node in the cluster. Use the Trace Configuration window to specify the parameters that you want to trace for troubleshooting problems. If you want to use predetermined troubleshooting trace settings rather than choosing your own trace fields, you can use the Troubleshooting Trace Setting window.

**Note**

Enabling Trace decreases system performance; therefore, enable Trace only for troubleshooting purposes. For assistance in using Trace, contact Cisco TAC support.

## Service Groups in Trace Configuration

Table 3-2 lists the services and trace libraries that correspond to the options in the Service Group list box in the Trace Configuration window.

**Table 3-2** *Service Groups in Trace Configuration*

Service Group	Services and Trace Libraries	Notes
Database and Admin Services	<ul style="list-style-type: none"> <li>• Cisco Database Layer Monitor</li> <li>• CiscoCCMUserWebService</li> <li>• SOAP - Diagnostic Portal Database Service</li> <li>• Cisco UP User</li> <li>• Cisco Bulk Provisioning Service</li> <li>• Cisco AXL Web Service</li> <li>• Cisco UP Admin</li> <li>• Cisco TAPS Service</li> <li>• Cisco License Manager</li> <li>• Cisco GRT Communications Web Service</li> <li>• Cisco Unified ReportingWeb Service</li> <li>• Platform SOAP Service</li> </ul>	<p>For most services in the Database and Admin Services group, you enable all trace for the service/library, instead of enabling trace for specific components. For Cisco Database Layer Monitor, you can run trace for specific components.</p> <p><b>Note</b> You can control logging for services in the Cisco Unified Serviceability UI. To change the log level, select the "Database and Admin Services" group and "Cisco CCMUser Web Service" service.</p>
Performance and Monitoring Services	<ul style="list-style-type: none"> <li>• Cisco RIS Data Collector</li> <li>• Cisco Log Partition Monitoring Tool</li> <li>• Cisco Audit Event Service</li> <li>• Cisco RisBean Library</li> <li>• Cisco RTMT Web Service</li> <li>• Cisco AMC Service</li> <li>• Cisco CallManager SNMP Service</li> </ul>	<p>Selecting the Cisco RTMT Web Service option turns on trace for the RTMT servlets; running this trace creates the server-side log for RTMT client queries.</p>
Backup and Restore Services	<ul style="list-style-type: none"> <li>• Cisco DRF Local</li> <li>• Cisco DRF Master</li> </ul>	<p>You enable all trace for each service, instead of running trace for specific components.</p>
System Services	<ul style="list-style-type: none"> <li>• Cisco CCMService Web Service</li> <li>• Cisco Trace Collection Service</li> </ul>	

**Table 3-2**      ***Service Groups in Trace Configuration (continued)***

Service Group	Services and Trace Libraries	Notes
SOAP Services	<ul style="list-style-type: none"><li>• Cisco SOAP Web Service</li><li>• Cisco SOAPMessage Service</li></ul>	Selecting the Cisco SOAP Web Service option turns on the trace for the AXL Serviceability API.  You enable all trace for this service, instead of running trace for specific components.
Security Services	<ul style="list-style-type: none"><li>• Cisco Trust Verification Service</li><li>• Cisco Certificate Authority Proxy Function</li></ul>	Turns on trace for certificate management on Cisco Unified Presence.  You enable all trace for the service, instead of running trace for specific components.

**Table 3-2**      **Service Groups in Trace Configuration (continued)**

Service Group	Services and Trace Libraries	Notes
Cisco Unified Presence Services	<ul style="list-style-type: none"> <li>• Cisco UP ConfigAgent</li> <li>• Cisco UP Intercluster Sync Agent</li> <li>• Cisco UP OAM Agent</li> <li>• Cisco Client Profile Agent</li> <li>• Cisco UP Presence Engine</li> <li>• Cisco UP SIP Proxy</li> <li>• Cisco UP Sync Agent</li> <li>• Cisco UP XCP Text Conference Manager</li> <li>• Cisco UP XCP Web Connection Manager</li> <li>• Cisco UP XCP Connection Manager</li> <li>• Cisco UP XCP SIP Federation Connection Manager</li> <li>• Cisco UP XCP XMPP Federation Connection Manager</li> <li>• Cisco UP XCP Message Archiver</li> <li>• Cisco UP XCP Directory Service</li> <li>• Cisco UP XCP Authentication Service</li> <li>• Cisco UP Replication Watcher</li> <li>• Cisco UP XCP Config Manager</li> <li>• Cisco UP XCP Router</li> <li>• Cisco UP Server Recovery Manager</li> </ul>	<p>For a description of these services, see <a href="#">Chapter 4, “Understanding Feature and Network Services in Cisco Unified Serviceability.”</a></p> <ul style="list-style-type: none"> <li>• For these services, you should enable all trace for the service, instead of running trace for specific components.</li> <li>• For the Cisco UP Sync Agent you can enable trace for specific components.</li> </ul>
Platform Services	Cisco Unified OS Admin Web Service	

## Configuring Trace Parameters

### Before You Begin

Review the trace configuration and collection checklist.

## Procedure

**Step 1** Select **Trace > Configuration**.

**Step 2** Perform the following actions:

- a. Select the server that is running the service for which you want to configure trace from the Server list box.
- b. Select **Go**.
- c. Select the service group for the service that you want to configure trace from the Service Group list box. [Table 3-2](#) lists the services and trace libraries that correspond to the options that display in the Service Group list box.
- d. Select **Go**.
- e. Select the service for which you want to configure trace from the Service list box.
- f. Select **Go**.



**Note** The list box displays all services (active and inactive).

**Step 3** If you configured Troubleshooting Trace for this service, a message displays at the top of the window that indicates that Troubleshooting Traces have been set. The system disables all fields on the window except the Output Settings. To configure the Output Settings, go to [Step 9](#).

**Step 4** Check **Apply to All Nodes** if you want trace to apply to all Cisco Unified Presence servers in the cluster.

**Step 5** Check **Trace On**.

**Step 6** Select the level of information that you want traced from the Debug Trace Level list box. The Debug Trace Level options that display vary, depending on which service you are tracing.

Level	Description
Arbitrary	<p>Traces all Entry and Exit conditions plus low-level debugging information.</p> <p><b>Note</b> Do not use this trace level with the Cisco IP Voice Media Streaming Application service during normal operation.</p>
Debug	<p>Traces all State Transition conditions plus media layer events that occur during normal operation.</p> <p><b>Note</b> Do not use Debug logging with the Cisco UP Presence Engine service because this trace level degrades system performance. We strongly recommend that you use the Info trace level to debug issues during normal operation.</p>
Detailed	<p>Traces all Arbitrary conditions plus detailed debugging information.</p> <p><b>Note</b> Do not use Debug logging with the Cisco IP Voice Media Streaming Application service because this trace level degrades system performance. We strongly recommend that you use the Info trace level to debug issues during normal operation.</p>

Level	Description
Entry/Exit	Traces all significant conditions plus entry and exit points of routines. Not all services use this trace level (for example, Cisco Unified Presence does not).
Error	Traces alarm conditions and events. Used for all traces that are generated in abnormal path. Uses minimum number of CPU cycles.
Fatal	Traces very severe error events that may cause the application to cancel.
Info	Traces the majority of servlet problems and has a minimal effect on system performance.
Significant	Traces all State Transition conditions plus media layer events that occur during normal operation.
Special	Traces all Error conditions plus process and device initialization messages.
State Transition	Traces all Special conditions plus subsystem state transitions that occur during normal operation.
Warn	Traces potentially harmful situations.

**Step 7** Check the relevant trace check boxes for the service that you chose; for example, Cisco UP SIP Proxy Trace Fields check box.

**Step 8** Check the trace fields that you want to enable if the service that you chose has multiple trace fields, such as the Cisco UP SIP Proxy service. Check **Check All Traces** to enable all trace fields.

The table below describes the service trace filter settings for the Cisco Unified Presence SIP Proxy.

Parameter	Description
Enable CTI Gateway Trace	This parameter enables tracing for the CTI Gateway.
Enable Parser Trace	This parameter enables tracing of parser information related to the operation of the per-sipd child SIP parser.
Enable SIP TLS Trace	This parameter enables tracing for information related to the TLS transport of SIP messages by TCP services.
Enable Privacy Trace	This parameter enables tracing for information about processing of PAI, RPID, and Diversion headers in relation to privacy requests.
Enable Routing Trace	This parameter enables tracing for the Routing module.
Enable IPPM Trace	This parameter enables tracing for IP Phone Messenger.
Enable SIPUA Trace	This parameter enables tracing for the SIP UA application module.
Enable Number Expansion Trace	This parameter enables tracing for the Number Expansion module.
Enable Presence Web Service Trace	This parameter enables tracing for the Presence Web Service.
Enable SIP Message and State Machine Trace	This parameter enables tracing for information related to the operation of the per-sipd SIP state machine.



Parameter	Description
Enable SIP TCP Trace	This parameter enables tracing for information related to the TCP transport of SIP messages by TCP services.
Enable Authentication Trace	This parameter enables tracing for the Authentication module.
Enable Enum Trace	This parameter enables tracing for the Enum module.
Enable Registry Trace	This parameter enables tracing for the Registry module.
Enable Method/Event Routing Trace	This parameter enables tracing for the Method/Event routing module.
Enable CALENDAR Trace	This parameter enables tracing for the Calendar module.
Enable Server Trace	This parameter enables tracing for the Server.
Enable Access Log Trace	This parameter enables the proxy access log trace; the first line of each SIP message received by the proxy is logged.
Enable SIP XMPP IM Gateway Trace	This parameter enables trace for the SIP XMPP IM Gateway.

**Step 9** Specify the trace output setting to limit the number and size of the trace files, as described below.

Field	Description
Maximum No. of files	This field specifies the total number of trace files for a given service. Cisco Unified Presence automatically appends a sequence number to the file name to indicate which file it is; for example, esp000005. When the last file in the sequence is full, the trace data begins writing over the first file. The default varies by service.
Maximum File Size (MB)	This field specifies the maximum size of the trace file in megabytes. The default varies by service.

**Step 10** Perform one of the following actions:

- a. Select **Save** to save your trace parameters configuration.
- b. Select **Set Default** to set the default.

#### Troubleshooting Tips

- When you change either the Maximum number of files or Maximum file size (MB) parameter, the system deletes all the service log files except the current file if the service is running, or, if the service is not active, the system will delete the files when the service is initially turning on. If you want to keep a record of the log files, make sure that you download and save the service log files to another server before changing the Maximum No. of Files parameter or the Maximum File Size parameter.
- The changes to trace configuration take effect immediately for all services.
- The section in the Trace Filter Settings area that relates to devices is not relevant to Cisco Unified Presence.

- Depending on the service you select and the traces generated by that service, some trace fields may be disabled or selected by default on the Trace Configuration screen.

**Related Topics**

- [Trace Configuration and Collection Checklist, page 3-1](#)
- [About Troubleshooting Trace Settings, page 3-17](#)
- [Appendix A, “Trace Field Descriptions”](#)

## Audit Log Configuration

With audit logging, specific changes to the Cisco Unified Presence system get logged in separate log files for auditing. This section contains the following topics:

- [Understanding Audit Logging, page 3-10](#)
- [Configuring Audit Log Settings, page 3-13](#)

## Understanding Audit Logging

In Cisco Unified Presence Release 8.6(4), three different types of logs can be collected: System Audit Logs, Application Audit Logs, and Database Audit Logs. For a description of each type of audit log, see the following sections:

- [System Audit Logs, page 3-10](#)
- [Application Audit Logs, page 3-10](#)
- [Database Audit Logs, page 3-13](#)

### 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 Presence*. For information about how to access collected logs from the Real-Time Monitoring Tool, see the *Real-Time Monitoring Tool Administration Guide for Cisco Unified Presence*.

### Application Audit Logs

The Application Audit logs track configuration changes to the Cisco Unified Presence system and are stored in separate log files for auditing purposes. The Cisco Audit Event Service, which appears under **Control Center—Network Services** in Cisco Unified Serviceability, writes the Application Audit logs. The Application Audit logs monitor and record any configuration change to the Cisco Unified Presence system by a user or as a result of the user action.

You access the Audit Log Configuration window in Cisco Unified Serviceability to configure the settings for these audit logs: **Tools > Audit Log Configuration**

Here is an example of an Application Audit log:

```
User ID: CUPAdministrator
Client IP Address: 172.19.240.207
Severity: 5
EventType: GeneralConfigurationUpdate
ResourceAccessed: CUPSAdmin
EventStatus: Successful
Compulsory Event: No
AuditCategory: AdministrativeEvent
ComponentID: Cisco CUP Administration
AuditDetails: [Presence Settings]
Configuration Saved.
App ID: Cisco Tomcat
Cluster ID: Node
ID: cup-node-a
```

Common Application Audit Log fields are defined below:

- **UserID**—User ID of the user associated with the audit log. For example, the user logging into an Administration GUI or the user making a configuration change.
- **ClientAddress**—IP address of the client associated with the audit log. For example, the IP address of the browser where a configuration change on the Administration GUI was saved.
- **Severity**—Severity of the audit log.
- **EventType**—Type of the audit event.
- **ResourceAccessed**—The resource being accessed.
- **EventStatus**—Event status.
- **ComponentID**—Component associated with the audit log.
- **Audit Details**—Detailed message explaining the nature of the audit log.
- **NodeID**—Cisco Unified Presence node affected by the change being logged.

**Note**

Be aware that audit event logging is centralized, enabled by default, and the logs are configured to rotate. If, for some reason, the audit log alarm component cannot write the audit log, a critical error is generated and reported 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 Presence Real-Time Monitoring Tool.

The following components generate audit events:

- [Cisco Unified Serviceability, page 3-11](#)
- [Cisco Unified Presence Real-Time Monitoring Tool, page 3-12](#)
- [Cisco Unified Presence Administration, page 3-12](#)
- [Cisco Unified Presence Application, page 3-12](#)
- [Command-Line Interface, page 3-12](#)

**Cisco Unified Serviceability**

Cisco Unified 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
- Changes in CDR management
- Review of any report in the Serviceability Reports Archive. This log gets viewed on the reporter node

#### **Cisco Unified Presence Real-Time Monitoring Tool**

Cisco Unified 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 Unified Presence Administration**

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

- Administrator logging (logins and logouts on Cisco Unified 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)
- Server configuration updates (changes to alarm or trace configurations, service parameters, IP addresses, host names, and Ethernet settings)
- Topology configuration changes (adding, removing, modifying Cisco Unified Presence nodes and/or subclusters)

#### **Cisco Unified Presence Application**

The following events get logged by the various components of the Cisco Unified Presence Application:

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

#### **Command-Line Interface**

All commands issued via the command-line interface are logged.

## Database Audit Logs

Database Audit Logs track all activities related to the internal Cisco Unified Presence database. Database Audit Logs allow the auditing of the following activities:

- Schema—Tracks changes to the setup of the internal Cisco Unified Presence database (for example, the columns and rows in the database tables).
- Administrative tasks—Tracks all administrative changes to the Cisco Unified Presence system (for example, any changes to maintain the system) plus all Schema changes.
- Database updates—Tracks all changes to the database, schema changes, and administrative tasks.
- Database reads—Tracks every read to the internal Cisco Unified Presence database, schema changes, administrative tasks, and database updates.



### Tip

Most administrators leave the Administrative Tasks setting disabled. For users who want auditing, use the Database Updates level. Choose the Database Reads level only when you want to get a quick look at the Cisco Unified Presence system. This level uses a significant amount of system resources and should only be used for a short period of time.

## Configuring Audit Log Settings

To configure Application Audit Log or Database Audit Log settings, perform the following procedure:



### Note

The System Audit Logs (Linux auditd) can only be enabled or disabled 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.

### 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 3-2](#).
- 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

[Table 3-2](#) describes the settings that you can configure in the Audit Log Configuration window in Cisco Unified Serviceability. Settings can be configured for Application Audit Logs and Database Audit Logs but not System Audit Logs.

### Before You Begin

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

The Standard Audit Log Administration role in Cisco Unified Presence provides the ability to delete audit logs and to read or update access to Cisco Unified Presence 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 in Cisco Unified Presence, refer to the *Cisco Unified Presence Configuration and Maintenance Online Help*.

**Table 3-3**      **Audit Log Configuration Settings**

Field	Description
<b>Select Server</b>	
Server	Choose the server where you want to configure audit logs; then, click <b>Go</b> .
Apply to All Nodes	If you want to apply the audit log configuration to all nodes in the cluster, check the <b>Apply to All Nodes</b> box.
<b>Application Audit Log Settings</b>	
Enable Audit Log	<p>This setting configures the Application Audit logs. When you enable this setting and then restart the Cisco Audit Event Service, an audit log gets created for the Application Audit log.</p> <p>For a complete list of the events that are logged, see <a href="#">Application Audit Logs, page 3-10</a>.</p> <p><b>Note</b> The Network Service Audit Event Service must be running.</p>
Enable Purging	<p>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.</p> <p>If purging is disabled, the number of audit logs continues to increase until the disk is full. This action could disrupt 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.</p> <p>You can access the audit logs by choosing <b>Trace and Log Central &gt; Audit Logs</b> in RTMT.</p> <p><b>Note</b> The Network Service Cisco Log Partitions Monitoring tool must be running.</p>

**Table 3-3**      **Audit Log Configuration Settings (continued)**

Field	Description
Enable Log Rotation	<p>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.</p> <p><b>Tip</b>      When log rotation is disabled (unchecked), audit log ignores the Maximum No. of Files setting.</p>
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 Serviceability does not send the Syslog messages. Do not specify a Cisco Unified Communications Manager server as the destination because the Cisco Unified Communications Manager server does not accept Syslog messages from another server.
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.
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.
<b>Database Audit Log Filter Settings</b>	
Enable Audit Log	When you check this check box, DB audit log gets created for the Cisco Unified Presence 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 3-3**      **Audit Log Configuration Settings (continued)**

Field	Description
Debug Audit Level	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>Schema</b>—Tracks changes to the setup of the Cisco Unified Presence database (for example, the columns and rows in the database tables).</li> <li>• <b>Administrative Tasks</b>—Tracks all administrative changes to the Cisco Unified Presence system (for example, any changes to maintain the system) plus all Schema changes.</li> </ul> <p><b>Tip</b>      Most administrators leave the Administrative Tasks setting disabled. For users who want auditing, use the Database Updates level.</p> <ul style="list-style-type: none"> <li>• <b>Database Updates</b>—Tracks all changes to the database plus all schema changes and all administrative tasks changes.</li> <li>• <b>Database Reads</b>—Tracks every read to the Cisco Unified Presence system, plus all schema changes, administrative tasks changes, and database updates changes.</li> </ul> <p><b>Tip</b>      Choose the Database Reads level only when you want to get a quick look at the Cisco Unified Presence system. This level uses significant amounts of system resources and only should be used for a short time.</p>
Enable Audit Log Rotation	<p>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 Enable Audit Log Rotation option is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached.</p> <p>When this setting is unchecked, audit log ignores the Maximum No. of Files setting.</p>
Maximum No. of Files	<p>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.</p> <p>You can enter a number from 4 (minimum) to 40 (maximum).</p>
No. of Files Deleted on Log Rotation	<p>Enter the maximum number of files that the system can delete when database audit log rotation occurs.</p> <p>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.</p>

## How to Troubleshoot Trace Settings

- [About Troubleshooting Trace Settings, page 3-17](#)
- [Troubleshooting Trace Settings, page 3-17](#)



## About Troubleshooting Trace Settings

The Troubleshooting Trace Settings window allows you to select the services in Cisco Unified Serviceability for which you want to set predetermined troubleshooting trace settings. In this window, you can select the services on different Cisco Unified Presence nodes in the cluster. This populates the trace settings changes for all the services you choose. You can select specific active services for a single node, all active services for the node, specific active services for all nodes in the cluster, or all active services for all nodes in the cluster. In the window, N/A displays next to inactive services.

**Note**

The predetermined troubleshooting trace settings for a Cisco Unified Presence feature or network service include SDI, and Log4j trace settings. Before the troubleshooting trace settings are applied, the system backs up the original trace settings. When you reset the troubleshooting trace settings, the original trace settings get restored.

When you open the Troubleshooting Trace Settings window after you apply troubleshooting trace settings to a service, the service that you set for troubleshooting displays as checked. In the Troubleshooting Trace Settings window, you can reset the trace settings to the original settings.

After you apply Troubleshooting Trace Setting to a service, the Trace Configuration window displays a message that troubleshooting trace is set for the given service(s). From the Related Links list box, you can select the Troubleshooting Trace Settings option if you want to reset the settings for the service. For the given service, the Trace Configuration window displays all the settings as read-only, except for some parameters of trace output settings; for example, Maximum No. of Files.

## Troubleshooting Trace Settings

**Before You Begin**

Review the trace configuration and collection checklist.

**Procedure**



- 
- Step 1** Select **Trace > Troubleshooting Trace Settings**.
- Step 2** Select the server where you want to troubleshoot trace settings from the Server list box.
- Step 3** Select **Go**.

**Note**

A list of services display. The services that are not active on a Cisco Unified Presence node display as N/A.

---

**Step 4** Perform one of the following actions:

If you want to:	Action
Monitor specific services on the node that you selected from the Server list box	Check the service in the Services pane; for example, the Database and Admin Services, Performance and Monitoring Services, or the Backup and Restore Services pane (and so on).   <b>Note</b> This task affects only the node that you selected from the Server list box.
Monitor all services on the node that you selected from the Server list box	Check <b>Check All Services</b> .
Monitor specific services on all nodes in a cluster	Check <b>Check Selected Services on All Nodes</b> .   <b>Note</b> This setting applies for all nodes in the cluster where the service is active.
Monitor all services for all nodes in the cluster	Check <b>Check All Services on All Nodes</b> .

**Step 5** Select **Save**.

**Step 6** Select one of the following buttons to restore the original trace settings:

- **Reset Troubleshooting Traces**—Restores the original trace settings for the services on the node that you chose in the Server list box; also displays as an icon that you can select.
- **Reset Troubleshooting Traces On All Nodes**—Restores the original trace settings for the services on all nodes in the cluster.

#### Troubleshooting Tips

- Leaving Troubleshooting trace enabled for a long time increases the size of the trace files and may impact the performance of the services.
- The Reset Troubleshooting Traces button displays only if you have set troubleshooting trace for one or more services.
- After you select the Reset button, the window refreshes, and the service check boxes display as unchecked.

#### Related Topics

- [Trace Configuration and Collection Checklist, page 3-1](#)