CHAPTER 9

System Audit Reports

This chapter explains:

- Viewing System Audit Log Report
- Performance Audit Reports
- Generating a Inventory and Config Audit Trail Report
- Device Administration Reports and IPSLA Audit Report

You can perform the following activities from the generated reports window:

- Sort the report using any column in the ascending or descending order.
- View the report in a printer-friendly format.
- Export the report to a file of CSV or PDF format.
- Set the number of records to be displayed per report page, as desired. You can set the number as 20, 50, 100, or 500.

Viewing System Audit Log Report

Audit log report provides information on:

- User login and logout from Cisco Prime
- Local Authentication user addition
- Local Authentication user modification
- Local Authentication user deletion

Audit Logs are stored as comma-separated value lists (CSVs) on a local server.

To view the Audit Log Report:

Step 1 Select **Reports > Audit > System.**

The Report Generator page appears.

Step 2 Click **Generate Report**.

The Audit Log Data Viewer contains a list of audit logs.

The Audit Logs are listed in reverse chronological order, with the most recent logs appearing at the bottom of the list. The logs are named and listed by the date on which they were created. For example: `Audit-Log-2004-10-27.csv`.

Step 3 Click an Audit Log file link to view the audit log details.

The Audit Log report contains:

Item	Description
Date	Date on which the activity was carried out.
Time	Time at which the activity was carried out.
User	User who performed the activity. If you reset the Cisco Prime user password using resetpasswd utility, User is shown as `CLI Utility`
Acct-Flags	Status of the activity. For example: start
Service	Functionality that the user accessed. The values displayed are : • cwhp and classic for Common Services • ipm for IPSLA Monitoring • dfm and triveni for Fault Management • rme for Configuration, Inventory and Software Image Management. • cm and cmapps for Topology and Layer 2 Services • cwlms for Getting Started, Reports and Troubleshooting. • CVng for CiscoView • cwportal for Portal • pmcgroups for Port and Module Configuration • vnm for VRF-Lite • upm for Device Performance Management
Cmd	Activity that was performed. Examples: 1. Logout 2. Mode
Reason	Description of the activity. Example: User admin logged out of cwhp

Performance Audit Reports

Cisco Prime LMS 4.2 logs all the changes made to the individual Device Performance Management modules as Audit Trail messages. These Audit Trail messages are logged and stored in the Cisco Prime LMS 4.2 database.

You can use the Audit Trail Logging option to view the Audit Trail Logging report for all modules, categories and users.

This section contains Understanding Performance Audit Report

To generate the Performance Audit report:

Step 1 Select **Reports > Audit > Performance Audit.**

The Performance Audit Report dialog box appears.

Table 9-1 describes the fields in the Performance Audit Report dialog box.

Table 9-1 Performance Audit Report Fields

Field	Description
Date Range	
24 Hours	Check the 24 Hours check box to generate Performance Audit report for last 24 hours.
From	Specify the start date and time of your Performance Audit report. Select the date by clicking the calendar icon and time from the drop-down list. The From date must be earlier than the current date. This field is disabled if you have selected the 24 Hours check box.
To	Specify the end date and time of your Performance Audit report. Select the date by clicking the calendar icon and time from the drop-down list. The To date must be later than the From date and earlier than the current date. This field is disabled if you have selected the 24 Hours check box.
Options	
Module	Select one of the following modules from the drop-down list to generate the Performance Audit report: • All • Poller Managemen • Template Managemen • Polling Engine • Threshold Manage • Job Manager • Summarization • Purge • Admin • Trendwatch Management • Group Evaluation The drop-down list displays All, by default.

Table 9-1 Performance Audit Report Fields (continued)

Field	Description
Category	View the Performance Audit report for each Module category. See Table 9-2 for the list of categories. This field is disabled if you have selected **All** in the Module option.
User	Select one of the following users from the drop-down list to generate the Performance Audit report: • All—The report is generated for changes done by All users. • Admin—The report is generated for changes done by the Admin user. • System—The report is generated for changes done by the System user. The drop-down list displays all users, by default.

Step 2 Update the necessary fields in the following panes:

- Date Range
- Options

See Table 9-1 for the description of fields that appear in the Performance Audit report dialog box.

Step 3 Click **OK** to launch the Performance Audit report or **Cancel** to cancel report generation.

The Performance Audit report page appears, displaying the report details. For more information, see Understanding Performance Audit Report.

Table 9-2 lists the categories available in each module

Table 9-2 Modules and Categories

Module	Category	Description
Poller Management	• All • Poller Creation • Poller Modification • Poller Deletion • Poller State Change • Delete Devices From Poller • Delete Failures from Poller • Clear Missed Cycles • Suspended devices from Poller • Managed devices added to Poller	The report is generated for the category selected in the Poller Management module. If you have selected **All**, the report generated for all the categories in the Poller Management module.
Template Management	• Template Creation • Template Modification • Template Deletion • Template Import • Template Export	The report is generated for the category selected in the Template Management module. If you have selected **All**, the report generated for all the categories in the Template Management module.
Polling Engine	• Polling Cycle Missed • Change Index Updated	The report is generated for the category selected in the Polling Engine module. If you have selected **All**, the report generated for all the categories in the Polling Engine module.
Threshold Manager	• Threshold Creation • Threshold Modification • Threshold Deletion	The report is generated for the category selected in the Threshold Manager module. If you have selected **All**, the report generated for all the categories in the Threshold Manager module.
Job Manager	• Job Creation • Job Updation • Job Deletion • Job Suspended • Job Resumed	The report is generated for the category selected in the Job Manager module. If you have selected **All**, the report generated for all the categories in the Job Manager module.

Table 9-2 Modules and Categories (continued)

Module	Category	Description
Summarization	• Summarization Start • Summarization End • Summarization Ended with Failure	The report is generated for the category selected in the Summarization module. If you have selected **All**, the report generated for all the categories in the Summarization module.
Purge	• Purge Start • Purge End • Purge Ended with Failure	The report is generated for the category selected in the Purge module. If you have selected **All**, the report generated for all the categories in the Purge module.

Table 9-2 Modules and Categories (continued)

Module	Category	Description
Admin	• Report Location Modification • Report Location Creation • Data Purge Policy Modification • Quick Report Time Modified • Poll Settings Updated • Job Purge Job updated • Job Purge Job Created • Data Purge Job Updated • Data Purge Job Created • Failure Tracker Job Updated • New MIB Loaded • Log Level Modified • Trap Group Creation • Trap Group Deletion • Trap Group Modification • Syslog Group Creation • Syslog Group Deletion • Syslog Group Modification	The report is generated for the category selected in the Admin module. If you have selected **All**, the report generated for all the categories in the Admin module.

Understanding Performance Audit Report

This section describes the fields available in the Performance Audit report. The Performance Audit report provides information on the changes that occurred in each module.

Table 9-3 describes the fields in the Audit Trail Log report.

Table 9-3 Audit Trail Log Report Fields

Field	Description
Module	Name of the module. For example, Job Manager
Category	Name of the module category. For example, Job Creation
Time Stamp	Displays the date and time at which the change was made to the module. For example, Mon, Apr 21 2008, 12:44:08
User	User who made the change in the module. For example, admin or system
Description	Change that occurred in the module. For example, Poller XYZ Created at Mon, Apr 21 2008, 12:44:08

Device Administration Reports and IPSLA Audit Report

Audit reports track all the configuration changes on the server performed by the LMS users.

You can also track the changes performed by the server . As the server updates the device space whenever a device gets added/edited/deleted in DCR if the Automatically Manage Devices from Credential Repository option is selected on the Application Settings page (**Admin > Application Settings**).

This section contains:

- Generating Device Administration Reports
- Generating IPSLA Audit Reports
- Tasks With Audit Reports
- Purging Audit Reports

You can perform the following tasks on the audit reports:

- Generating Device Administration Reports

  You can view the complete device list in the DCR.
- Generating IPSLA Audit Reports

  You can track the changes that are performed on the server.

  To view the list of tasks that trigger an Audit report, see Generating Device Administration Reports
- Purging Audit Reports

You can purge the IPSLA Audit Report.

Generating Device Administration Reports

The DCR Audit Report displays the complete device list in DCR within a specified period of time.

To generate DCR Audit reports:

Step 1 Select **Reports > Audit > Device Administration**.

The Reports page appears.

Step 2 Select a date range to generate the device list for a specific period of time.

Use the calendar icon displayed to enter a From Date and a To Date. The To Date should be later than the From Date.

The calendar displays the date from the client system.

Step 3 Click **Generate Reports** to view the selected report.

The Report window appears with the following details:

Table 9-4 Audit Trail Log Report Fields

Item	Description
Device	Device name of devices.
Changed Information	Description of the device information modified. For example, when a device is added to DCR, this field displays Device Added. When a device is removed from DCR, this field displays Device Deleted.
Date & Time	Date and time when the device information is changed. The date and time is displayed in *yyyy-mm-dd hh:mm:ss* format.
User	Login name of the user who has modified the device information in DCR.

Generating IPSLA Audit Reports

You can generate audit reports on all Audit changes that occurred in the network during a specified time period.

Note View Permission Report (**Reports > System > Users > Permission Report**) to check whether you have the privileges required to perform this task.

Step 1 Select **Reports > Audit > IPSLA**.

The IPSLA Audit Report page appears.

Step 2 Specify the required details in the Selection Criteria and Report Period sections. See Table 9-5 for more information.

Table 9-5 Audit Report Table

Field	Description
Selection Criteria	
User Name	Select the user name from the drop-down list. This report will be filtered on user names.
Module	Select the module name. This report will be filtered on module names.
Report period	
From	Click the calendar icon and select the start date of the report.
To	Click the calendar icon and select the end date of the report.

Audit reports contain all change information provided based on your filter criteria.

Step 3 Click **Generate**.

The Audit Reports window appears. See Table 9-6 for more information.

Table 9-6 Audit Reports

Field	Description
User Name	Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which the module is running or the name under which the Telnet connection is established.
Module	Name of the module involved in the network change. For example, Collector Management, Device Management, etc.
Description	Brief summary of the change that occurred on the server.
Time Stamp	Date and time at which the changes were performed.

Tasks With Audit Reports

An Audit report is triggered and logged when you perform the following tasks See Table 9-7:

Table 9-7 Audit Reports Page

Module Name	Tasks	Navigation
Device Management	Enabling IPSLA responder	**Inventory > Device Administration > IPSLA Devices > Enable IPSLA Responder**
	Delete	**Inventory > Device Administration > IPSLA Devices > Delete**
	Add Adhoc Target	**Inventory > Device Administration > IPSLA Devices > Add Adhoc Target**
	Edit Device Attributes	**Inventory > Device Administration > IPSLA Devices > Edit Device Attributes**
	Update IPSLA Config	**Inventory > Device Administration > IPSLA Devices > Update IPSLA Config**
Collector Management	Creating collectors	**Monitor > Performance Management > IPSLA > Collectors > Create**
	Editing a collector	**Monitor > Performance Management > IPSLA > Collectors > Edit**
	Deleting collectors	**Monitor > Performance Management > IPSLA > Collectors > Delete**
	Starting Collectors	**Monitor > Performance Management > IPSLA > Collectors > Start**
	Stopping Collectors	**Monitor > Performance Management > IPSLA > Collectors > Stop**
Operation Management	Creating a operation	**Monitor > Performance Management > IPSLA > Operations > Create**
	Editing an operation	**Monitor > Performance Management > IPSLA > Operations > Edit**
	Deleting an operation	**Monitor > Performance Management > IPSLA > Operations > Delete**
Admin	NVRAM Settings	**Admin > Network > Performance Collection Settings > IPSLA application settings**
	Log Level Settings	**Admin > System Administration > Debug Settings > IPSLA Debugging Settings**
	IPSLA Syslog Configuration	**Admin > Network Administration > Notification and Action Settings > IPSLA Syslog Configuration**
	Purge Settings	**Admin > Network Administration > Purge Settings > IPSLA data purge settings**

Table 9-7 Audit Reports Page (continued)

Module Name	Tasks	Navigation
Job Management	Creating a Job	**Reports > Performance > IPSLA Detailed > Availability**
		Reports > Performance > IPSLA Detailed > Ethernet Jitter
		Reports > Performance > IPSLA Detailed > HTTP
		Reports > Performance > IPSLA Detailed > ICMP
		Reports > Performance > IPSLA Detailed > Latency
		Reports > Performance > IPSLA Detailed > Path Echo
		Reports > Performance > IPSLA Detailed > RTP
		Reports > Performance > IPSLA Detailed > UDPJitter
		Reports > Fault and Event > Threshold Violation > IPSLA
		Reports > Performance > IPSLA Summary > Availability
		Reports > Performance > IPSLA Summary > Latency
		Reports > Performance > IPSLA Summary > Jitter
Report Management	Immediate reports and successfully scheduled IPSLA reports	**Reports > Fault and Event > Threshold Violation > IPSLA**
		Reports > Performance > IPSLA Detailed > Availability
		Reports > Performance > IPSLA Detailed > Ethernet Jitter
		Reports > Performance > IPSLA Detailed > HTTP
		Reports > Performance > IPSLA Detailed > ICMP
		Reports > Performance > IPSLA Detailes > Latency
		Reports > Performance > IPSLA Detailed > PATHECHO
		Reports > Performance > IPSLA Detailed > RTP
		Reports > Performance > IPSLA Detailed > UDPJitter
		Reports > Performance > IPSLA Summary > Availability
		Reports > Performance > IPSLA Summary > Latency
		Reports > Performance > IPSLA Summary > Jitter

Purging Audit Reports

You can set the purge period for audit reports on the Purge Settings page. After you set the purge period, the audit reports that are greater than the set purge period are purged. This frees disk space and maintains your audit reports at a manageable size.

Note View Permission Report (**Reports > System > Users > Permission**) to check whether you have the privileges required to perform this task.

To purge the Audit reports:

Step 1 Select **Administration > Network Administration > Purge settings**.

The Purge Settings page appears.

Step 2 Enter the purge period in the Audit Report Purge Period text box.

The audit reports older than the number of days you specify will be purged. The default purge period is 180 days.

Step 3 Click **Apply**.

Generating a Inventory and Config Audit Trail Report

This option lets you compile a report on all Audit Trail changes that occurred in the network during a specific time period.

This section contains:

- Understanding the Inventory and Config Report
- Audit Trail Record

Note View Permission Report (**Reports > Systrm Reports > Permission Reports**) to check if you have the privileges required to perform this task.

To generate the Inventory and Config Audit Report:

Step 1 Select **Reports > Audit > Inventory and Config**.

The Audit Trail Standard Report dialog box appears.

Step 2 Enter the information required to generate the required report.

Field	Description
Date Range	
24 Hours	Select this option, only if you want to generate a 24-Hour Report. This report will contain all the Audit Trail data gathered during the last 24 hours.

Field	Description
Last *X*	Select this option, if you want to generate a report for the last *X* days or weeks or months or years. Where *X* represents the number of days or weeks or months or years. For example, if you want to generate a Standard Audit Trail report for the last 6 days, you can enter **6** in the textbox and select **days** from the listbox. The generated report will consist of Audit Trail data gathered for the last 6 days. This option applies only to Standard Audit Trail Reports.
From	Click on the calendar icon and select the start date. The From field is enabled only if you have deselected the 24 Hours check box.
To	Click on the calendar icon and select the end date. The To field is enabled only if you have deselected the 24 Hours check box.
Selection Criteria	
User Name	Select the user name. This report will be filtered on user name selected.
Application	Select the name of the application. This report will be filtered on application name selected.

Step 3 Click **Finish**.

The Audit Trail Standard report appears in a separate browser window.

If you want to revert to the default values in the Report Generator dialog box, click **Reset**.

Understanding the Inventory and Config Report

The Inventory and Config Audit Report contains all change information provided by LMS 4.2 based on your filter criteria. It contains the following fields, See Table 9-8.

Table 9-8 Audit Trail Report

Field	Description
User Name	Name of the person who performed the change. This is the name entered when the person logged in. It can be the name under which LMS 4.2 is running, or the name under which the Telnet connection is established.
Application Name	Name of the application involved in the network change. For example, ChangeAudit, Device Management, ICServer, NetConfig, NetShow etc.
Server Name	Host name of the server.
Creation Time	Date and time at which the changes were performed on the server.
Description	Brief summary of the change that occurred on the server.

The following buttons are available on the Audit Trail Standard report:

Button	Description
Export to File (Icon)	You can export this report in either PDF or CSV format.
Print (Icon)	You can generate a format that can be printed.

Audit Trail Record

The following tasks trigger an Audit Trail record:

Application Name	Tasks	Navigation
Install/Migration	The following Audit records are logged at the time of migration: • Device information is migrated • Syslog message filters are migrated • Syslog automated actions are migrated • Enabling the shadow directory	Not applicable
Change Audit	Setting the Purge Policy. An Audit Trail record is logged any time you make a change in the Purge Policy dialog box.	**Admin > Network Administration > Purge Settings > Change Audit Purge Policy**
Change Audit	Performing a Forced Purge. An Audit Trail record is logged when a Force Purge job is scheduled.	**Admin > Network Administration > Purge Settings > Change Audit force purge**
Change Audit	An Audit Trail record is logged when you: • Add an automated action. • Enable or disable the automated actions. • Edit an automated action. • Import the automated actions. • Delete the automated actions.	**Admin > Network Administration > Notification and Action Settings > Syslog Automated Actions**.

Application Name	Tasks	Navigation
Change Audit	An Audit Trail record is logged when you: • Add an Exception Profile • Delete the Exception Profiles • Enable or disable the Exception Profiles	**Admin > Network Administration > Change Audit Settings > Exception Periods**
Configuration Management—Archive Management	An Audit Trail record is logged when you: • Change the Archive location • Enable or disable the Shadow directory option	**Admin > Network Administration > Collection Settings > Config Archive settings**
Configuration Management—Archive Management	An Audit Trail record is logged when you: • Enable or disable the Periodic Polling option • Change the Periodic Polling schedule • Enable or disable the Periodic Collection option • Change the Periodic Collection schedule	**Admin > Network Administration > Collection Settings > Config Collection settings**
Configuration Management—Archive Management	Setting up the Archive Purge Policy An Audit Trail record is logged any time you make a change in the Archive Purge Setup dialog box.	**Admin > Network Administration > Purge Settings > Config Archive purge settings**
Configuration Management	Setting up the Transport Protocol Order An Audit Trail record is logged any time you make a change in the Config Transport Settings dialog box.	**Admin > Network Administration > Collection Settings > Config transport settings** (Archive Mgmt, Config Editor, NetShow, and NetConfig)
Configuration Management	Setting up the Job Policy An Audit Trail record is logged any time you make a change in the Job Policy dialog box.	**Admin > Network Administration > Configuration Settings > Config Job Policies** (Archive Mgmt, Config Editor, NetShow, and NetConfig)
Device Management	Managing devices in LMS 4.2	**Inventory > Device Administration > Add / Import / Manage Devices**
Device Management	Deleting devices in LMS 4.2. Also, when a device gets deleted as a result of alias resolution.	**Inventory > Device Administration > Add / Import / Manage Devices**

Application Name	Tasks	Navigation
Device Management	Enabling and disabling these settings in the Device Management Settings window: • Automatically Manage Devices from Credential Repository • Verify Device Credentials While Adding Devices	**Inventory > Device Administration > Auto Update Server Management**
Inventory	An Audit Trail record is logged when you: • Create a job for Inventory polling and Inventory collection. • Edit a scheduled job of Inventory polling and Inventory collection. • Cancel the scheduled jobs of Inventory polling and Inventory collection. • Stop the running jobs of Inventory polling and Inventory collection. • Delete the jobs of Inventory polling and Inventory collection.	**Inventory > Job Browsers > Inventory Collection** **or** **Admin > Network Administration > Collection Settings > Inventory Jobs**
Inventory	Scheduling a Inventory Polling and Collection Job.	**Admin > Network Administration > Collection Settings > Inventory system job schedule**
Inventory	Setting the Inventory Change Filter.	**Admin > Network Administration > Change Audit Settings > Inventory Change Filter**
Reports	Purging Reports Jobs and Archived Reports	**Reports > Settings and Administration > UT Report Settings**
Software Management	Viewing and editing preferences. An Audit Trail record is logged any time you make a change in the View/Edit Preferences dialog box.	**Admin > Network Administration > Software Image Management Settings > View/Edit Preferences**
Syslog Analysis	Setting up Backup Policy An Audit Trail record is logged any time you make a change in the Backup Policy dialog box	**Admin > Network Administration > Purge Settings > Syslog backup settings**
Syslog Analysis	Setting the Purge Policy. An Audit Trail record is logged any time you make a change in the Purge Policy dialog box.	**Admin > Network Administration > Purge Settings > Syslog purge settings**
Syslog Analysis	Performing a Forced Purge An Audit Trail record is logged when a Force Purge job is scheduled.	**Admin > Network Administration > Purge Settings > Syslog force purge**

Application Name	Tasks	Navigation
Syslog Analysis	An Audit Trail record is logged when you: • Add an automated action. • Enable or disable the automated actions. • Edit an automated action. • Import the automated actions. • Delete the automated actions.	**Admin > Network Administration > Notification and Action Settings > Syslog Automated Actions**
Syslog Analysis	An Audit Trail record is logged when you: • Create a message filter • Edit a message filter • Enable or disable the filters • Import a filter • Delete a filter • Change message filters type from **drop** to **keep** and vice versa.	**Admin > Network Administration > Notification and Action Settings > Syslog Message Filters**
Syslog Analysis	An Audit Trail record is logged when you subscribe/unsubscribe to a remote syslog collector.	**Admin > Network Administration > Collection Settings > Syslog Collector Status**
System Preferences	Viewing and editing System Preferences.	**Admin > System Administration > Server Administration > System Preferences**
Loglevel Settings	Setting the Loglevels.	**Admin > System Administration > Debug Settings > Config and Image Management debugging settings**
Editing Device Attributes	Editing the device attributes	**Inventory > Device Administration > Add / Import / Manage Devices**