Audits and Logs

- Audit Configuration Archive and Software Management Changes (Network Audit) , on page 1
- Audit Changes Made By Users (Change Audit), on page 1
- Audit Actions Executed from the GUI (System Audit), on page 3
- System Logs, on page 3

AuditConfigurationArchiveandSoftwareManagementChanges (Network Audit)

The **Network Audit** window displays changes made to devices using the Configuration Archive and Software Management features. To view these changes, choose **Inventory** > **Network Audit**. Cisco EPN Manager lists the most recent devices changes including the type of change (Configuration Archive, Software Image Management). For examples, see:

- Check the Network Audit for Configuration Archive Operations
- Check the Network Audit for Software Image Operations

You can also view the most recent changes for a device in the **Recent Changes** tab of its Device 360 view. See Get Basic Device Information: Device 360 View.

Audit Changes Made By Users (Change Audit)

Cisco EPN Manager supports managing change audit data in the following ways:

- Generate a Change Audit Report, on page 1
- Enable Change Audit Notifications and Configure Syslog Receivers, on page 2

Generate a Change Audit Report

The Change Audit report lists the actions that users have performed using theCisco EPN Manager features. The following table provides examples of what may appear in a Change Audit report.

Feature	Examples
Device management	Device '209.165.202.159' Added

Feature	Examples
User management	User ‘mmjones' added
Administration	Logout successful for user jlsmith from 209.165.202.129 Authentication Failed. Login failed for user fjclark from 209.165.202.125
Configuration changes	CLI Commands : ip access-list standard testremark test
Monitoring policies	Monitoring Template 'IF Outbound Errors (Threshold)' Created
Configuration templates	Configuration Template 'Add-Host-Name-IOS-Test' Created
Jobs	'Show-Users-On-Device-IOS_1' job of type Config Deploy - Deploy View scheduled.
Inventory	Logical File '/bootflash/tracelogs/inst_cleanup_R0-0.log.19999.20150126210302' deleted.

You can schedule a Change Audit report to run on a regular basis and, if desired, Cisco EPN Manager can e-mail the results to you. You can also forward this information in a Change Audit notification (see Enable Change Audit Notifications and Configure Syslog Receivers, on page 2).

Step 1 Choose **Reports** > **Report Launch Pad**, then choose **Compliance** > **Change Audit**.

Step 2 Click **New** to configure a new report.

Step 3 In the **Settings** area, enter the report criteria (time frame, when to start the report, and so forth).

Step 4 If you want to schedule the report to run at a later time, enter your settings in the **Schedule** area. You can also specify an e-mail address that the report should be sent to.

Step 5 If you want to run the report immediately, click **Run** at the bottom of the window.

The **Report Run Result** lists all users and the changes they made during the specified time period.

Enable Change Audit Notifications and Configure Syslog Receivers

If desired, you can configure Cisco EPN Manager to send a change audit notification when changes are made to the system. These changes include device inventory and configuration changes, configuration template and monitoring template operations, and user operations such as logins and logouts and user account changes.

You can configureCisco EPN Manager to:

- Forward changes as change audit notifications to a Java Message Server (JMS).
- Send these messages to specific syslog receivers.

If you configure syslog receivers but do not receive syslogs, you may need to change the anti-virus or firewall settings on the destination syslog receiver to permit reception of syslog messages.

Step 1 Select **Administration** > **Settings** > **System Settings**, then choose **Mail and Notification** > **Change Audit Notification**.

Step 2 Select the **Enable Change Audit Notification** check box to enable notifications.

Step 3 If you want to send the messages to specific syslog receivers:

a) Click the **Add** button (+) to specify a syslog receiver.

b) In the **Syslog Receivers** area, enter the IP address, protocol, and port number of the syslog receiver.

You can repeat these steps as needed to specify additional syslog receivers.

Step 4 Click **Save**.

Note It is recommended to restart the Cisco EPN Manager server for the records to be reflected in secure tls log.

Audit Actions Executed from the GUI (System Audit)

Note Cisco EPN Manager sends all change audit notifications in XML format to the topic **ChangeAudit.All**. You must be subscribed to **ChangeAudit.All** to receive the notifications.

The System Audit window lists all Cisco EPN Manager GUI pages that users have accessed. To view a System Audit, choose **Administration** > **Settings** > **System Audit**.

The following table shows some of the information you can find from the System Audit page using the quick filter. To enable the quick filter, choose **Quick Filter** from the **Show** drop-down list.

Find actions performed:	Do the following:
By a specific user	Enter the username in the **Username** quick filter field
By all users in a user group	Enter the group name in the **User Group** quick filter field
On devices in a specific virtual domain	Enter the virtual domain name in the **Active Virtual Domain** quick filter field
By the web GUI root user	Select **Root User Logs** from the **Show** drop-down list
On a specific device	Enter the IP address in the **IP Address** quick filter field
On a specific day	Enter the day in the **Audit Time** quick filter filed (in the format *yyyy–mmm–dd*)

System Logs

Cisco EPN Manager provides three classes of logs which are controlled by choosing **Administration** > **Settings** > **Logging**.

Logging Type	Description	See:
General	Captures information about actions in the system.	View and Manage General System Logs, on page 4
SNMP	Captures interactions with managed devices.	Enable SNMP Traces and Adjust SNMP Log Settings (Levels, Size), on page 5
Syslog	Forwards Cisco EPN Manager audit logs (as syslogs) to another recipient.	Forward System Audit Logs As Syslogs, on page 5

View and Manage General System Logs

You can view system logs after downloading them to your local server.

- View the Logs for a Specific Job, on page 4
- Adjust General Log File Settings and Default Sizes, on page 4
- Download and E-Mail Log Files for Troubleshooting Purposes, on page 5
- Forward System Audit Logs As Syslogs, on page 5

View the Logs for a Specific Job

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard** .

Step 2 Choose a job type from the Jobs pane, then select a job instance from the Jobs window.

Step 3 At the top left of the Job instance window, locate the **Logs** field, then click **Download**.

Step 4 Open or save the file as needed.

Adjust General Log File Settings and Default Sizes

By default, Cisco EPN Manager logs all error, informational, and trace messages generated by all managed devices. It also logs all SNMP messages and Syslogs that it receives. You can adjust these settings, changing logging levels for debugging purposes.

To do the following:	From Administration > System Settings > Logging:
Change the size of logs, number of logs saved, and log naming convention	Adjust the Log File Settings. **Note** Change these settings with caution to avoid impacting the system.
Change the logging level for specific modules	In the General Log Settings, select the files and the desired level, and click **Save**. You will have to restart Cisco EPN Manager for the changes to take effect.
Download log files for troubleshooting purposes	In the Download Log File area, click **Download**.

To do the following:	From Administration > System Settings > Logging:
E-mail log files (for example, to the Cisco Technical Center)	Enter a comma-separated list of e-mail IDs and click **Send**.

Download and E-Mail Log Files for Troubleshooting Purposes

Note This procedure sets and log message levels to Trace. Be sure to return the log message levels to their original setting so system performance is not impacted.

Step 1 Choose **Administration** > **Settings** > **Logging**, then choose **General Logging Options**.

Step 2 Note the setting in the **Message Level** drop-down list because you will need to reset it later.

Step 3 In the **Enable Log Modules** area, select the **Log Modules** check box to select all modules.

Step 4 Select **Trace** from the **Message Level** drop-down list.

Step 5 Reproduce the problem on the system so the details can be captured in the logs.

Step 6 In the **Download Log File** area, click **Download**. The download zip file will have the name:

NCS-*hostname*-logs-*yy-mm-dd-hh-mm-ss*.

The file includes an HTML file that lists all files included in the zip file.

Step 7 In the E-Mail Log File area, enter a comma-separated list of e-mail IDs.

Step 8 Revert to the original setting in the **Message Level** drop-down list.

Forward System Audit Logs As Syslogs

Step 1 Choose **Administration** > **Settings** > **Logging**, then choose **Syslog Logging Options**.

Step 2 Select the **Enable Syslog** check box to enable collecting and processing system logs.

Step 3 In the **Syslog Host** field, enter the IP address of the interface from which the message is to be transmitted.

Step 4 From the **Syslog Facility** drop-down list, choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.

Step 5 Click **Save**.

Enable SNMP Traces and Adjust SNMP Log Settings (Levels, Size)

Enable SNMP tracing to access more detailed information about the packets sent and received through SNMP. You may want to do this when troubleshooting, such as when a trap is dropped.

To make the following changes, choose **Administration** > **Settings** > **Logging**, then choose **SNMP Logging Options**.

If you want to:	Do the following:
Enable SNMP tracing on specific devices	In the **SNMP Log Settings** area: **1.** Select the **Enable SNMP Trace** check box and the **Display Values** check boxes. **2.** Enter the IP addresses of the devices you want to trace and click **Save**.
Change the size of logs and number of logs saved	In the **SNMP Log File Settings** area: **Note** Be careful when you change these settings so that you do not impact system performance (by saving too much data). **1.** Adjust the maximum number of files and file size. **2.** Restart Cisco EPN Manager for your changes to take effect. See Stop and Restart Cisco EPN Manager.