Audits and Logs

Audit Configuration Archive and Software Management Changes (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 Audi**t from the left sidebar menu. 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

Audit Changes Made By Users (Change Audit)

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

- Generate a Change Audit Report
- Forward Changes as Change Audit Notifications

Generate a Change Audit Report

The Change Audit report lists the actions that Cisco EPN Manager users have performed using the Cisco 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
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 test remark test
Monitoring policies	Monitoring Template 'IPSLA (Threshold)' Created
Configuration templates	Configuration Template 'Add-Host-Name-IOS-Test' Created
Jobs	'Job_QoS_9_56_13_060_PM_1_26_2015' job of type QoS 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 Forward Changes as Change Audit Notifications).

Step 1 Choose **Reports > Report Launch Pad > Compliance > Change Audit Report** and click **New**.

Step 2 In the Settings area, enter the report criteria (time frame, when to start the report, and so forth).

Step 3 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 4 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.

Forward Changes as Change Audit Notifications

If desired, you can configure Cisco EPN Manager to forward these changes as change audit notifications to a Java Message Server (JMS) whenever the audit parameters you specified are changed. This feature is disabled by default.

Step 1 Select **Administration > Settings > System Settings > Change Audit Notification.**

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

Step 3 Enter the **IP Address** and **TCP Port Number** in the Syslog Receiver pane.

Step 4 Click **Save**.

LIMITED ORDERABILITY RELEASE

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 > 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 > Logging**:

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

LIMITED ORDERABILITY RELEASE

View and Manage General System Logs

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 > 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**.
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 > Logging**.

Step 2 In the General Log Settings area, select **Trace** from the Message Level drop-down list.

Step 3 Reproduce the problem on the system so the details can be captured in the logs.

Step 4 In the Download Log Files area, click **Download**. The download zip file will have the name:

NCS-*hostname***-logs-**y*y-mm-dd-hh-mm-ss*

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

Step 5 In the E-Mail Log File area, enter a comma-separated list of e-mail IDs.

Step 6 Repeat Step 2 but return the message level to the previous settings.

Forward System Audit Logs As Syslogs

Step 1 Choose **Administration > Logging > Syslog Logging Options**.

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

Step 3 In Syslog Host, 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 do the following:	From Administration > Logging:
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 box. 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	Adjust the SNMP Log File Settings. You will have to restart Cisco EPN Manager for the changes to take effect. **Note** Change these settings with caution to avoid impacting the system.