Audits and Logs

Audit Changes Made By Users (Change Audit)

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

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.

View Change Audit Details

Step 1 Log in to Cisco EPN Manager as an administrator.

Step 2 Choose **Monitor** > **Tools** > **Change Audit Dashboard**.

The **Change Audit Dashboard** displays:

- Change audit data from:
  - Device management
  - User management
  - Configuration template management
  - Device community and credential changes
  - Inventory changes of devices

The **Change Audit report** and **Change Audit** dashboard display the details irrespective of the virtual domain you are logged in.

The **Change Audit Dashboard** screen also displays the Device Name apart from other details such as IP Address, Audit Description, User Name, Audit Name, and Client IP Address. Click the *i* icon next to the IP Address field to view the Device 360 details.

Note If you have logged in as a root user, then you can view all the Audit changes. If you have logged in as a non-root user, then you can only view the Audit changes performed by you.

Cisco EPN Manager logs all the details in **Change Audit Dashboard** at `/opt/CSCOlumos/logs/audit.log`, see Audit Log, on page 7 for more information.

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*)

Forward OS Logs to Remote System

To enable EPNM to forward OS CLI system logs to a remote system or to configure the log level, use the following logging command in configuration mode.

Note You can configure only one remote system to forward the logs to.

```
logging {ip-address | hostname} {loglevel level}
```

Where,

Syntax	Description
`ip-address`	IP address of remote system to which you forward the logs to. Up to 32 alphanumeric characters.
`hostname`	Hostname of remote system to which you forward the logs to. Up to 32 alphanumeric characters.
`loglevel`	The command to configure the log level for the logging command.
`level`	Number of the desired priority level at which you set the log messages. Priority levels are (enter the number for the keyword): • 0 - emerg—Emergencies: System unusable • 1 - alert—Alerts: Immediate action needed • 2 - crit—Critical: Critical conditions

Syntax	Description
	• 3 - err—Error: Error conditions • 4 - warn—Warning: Warning conditions • 5 - notif—Notifications: Normal but significant conditions • 6 - inform—(Default) Informational messages • 7 - debug—Debugging messages

To disable this function, use the no form of this command.

This command requires an **IP address** or **hostname** or the **loglevel** keyword. An error occurs if you enter two or more of these arguments.

Example 1:

```
ncs/admin(config)# logging 209.165.200.225
ncs/admin(config)#
```

Example 2:

```
ncs/admin(config)# logging loglevel 0
ncs/admin(config)#
```

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 6
Syslog	Forwards Cisco EPN Manager audit logs (as syslogs) to another recipient.	Forward System Audit Logs As Syslogs, on page 6

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

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

Step 2 Choose a job type from the Jobs pane, then click on a job instance link from the Jobs window.

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

Note You can download the logs only for Configuration Archive Software, Configuration Rollback, Configuration Overwrite, and Configuration Deploy job types.

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 > Settings > Logging:
Change the size of logs, number of logs saved, and the file compression options	Adjust the Log File Settings. **Note** Change these settings with caution to avoid impacting the system. As per log4j MaxBackupIndex, there will be one main file accompanied by the set number of backup files. For example, if the number of log files is set to 3, there is one main file (.log) and 3 backup files (.log.1, .log.2, and .log.3). If the **Number of files** is modified to a value lower than the one previously set, the log file settings are applied only to the newly generated files. For example, if the preset value was 5 and now you modify it to 2, the settings will only be applied to files .log, .log.1 and .log.2. There is no changes to the files .log.3, .log.4, and .log.5. If you select the **Compression (Zip)** option, log files are compressed and archived in the folder of the process. Retention of the compressed log files is subject to the criteria: • Storage (MB): Maximum size of the folder in MB • Number of Days: Maximum age of the log files The purge is triggered when either of the criteria is met. Optionally, if **Backup to external location** is enabled, log files marked for cleanup are copied to the specified external repository prior to deletion.

To do the following:	From Administration > Settings > Logging:
Change the logging level for specific modules	In the General Log Settings, select the files and the desired level, and click **Save**. For example, from the **Message Level** drop-down list, choose one of the following as current logging level: • Error—Captures error logs on the system. • Information—Captures informational logs on the system. • Trace—Reproduces problems of managed devices on the system so the details can be captured in the logs. • Debug—Captures debugging logs on the system. When you restart Cisco EPN Manager , the log level resets to Error.

Forward System Audit Logs As Syslogs

Before you begin

To work with Forward System Audit Logs as Syslogs, the user must configure Enable Change Audit Notifications and Configure Syslog Receivers.

Step 1 Choose **Administration** > **Settings** > **Logging**, then choose **Syslog** tab to view **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 destination server to 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**.

Note If you enable system logs forwarding to remote server through an admin CLI, logs will not be registered to ade.log file.

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 select the **SNMP Log** tab.

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 and/or DNS addresses of the devices you want to trace and click **Save**.

If you want to:	Do the following:
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.

Audit Log

Cisco EPN Manager logs the information displayed under **Monitor** > **Tools** > **Change Audit Dashboard** in the `audit.log`. Logging is enabled by default. This information is logged irrespective of message level or log module changes.

To view the `audit.log`, navigate to `/opt/CSCOlumos/logs/audit.log` in admin CLI (see Establish an SSH Session With the Cisco EPN Manager Server).

Device-Specific Logging

Cisco EPN Manager enables you to store the XDE and Inventory logs in DEBUG mode for specific devices. You can enable or disable the logging from SSH CLI. (See Establish an SSH Session With the Cisco EPN Manager Server).

Enable device-specific logging

Important Before you enable device-specific logging for XDE or inventory logs, ensure that you have set the global log level to INFO by running the following command:

`/opt/CSCOlumos/bin/setLogLevel.sh` *`logName`* `INFO`

logName - Enter xde or inventory as necessary.

To enable device-specific logging, run the following command:

`/opt/CSCOlumos/bin/setDeviceLevelDebug.sh` *`logName`* `DEBUG` *`deviceIP`*

Where:

- *logName* - Enter xde or inventory as necessary. Enabling device-specific logging for inventory logs enables logging for ifm_inventory logs as well.
- *deviceIP* - Specify the IP address of the device for which you want to enable the logging. You may specify multiple IP addresses in the same command separated by a comma.

The inventory or XDE logs in DEBUG mode are stored only for the specified device(s). For other devices, only INFO logs are stored. The log files generated during sync are *xde.log.**, *inventory.log.** and *ifm_inventory.log.**.

Cisco EPN Manager overrides previously specified IP address with the IP address that you specify each time you run this command.

Example

For Inventory logs:

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh inventory DEBUG 1.2.3.4,5.6.7.8
```

For XDE logs:

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh xde DEBUG 1.2.3.4,5.6.7.8
```

View list of devices for which device-specific logging is enabled

To view the list of devices for which device-specifc logging is enabled, run the following command:

```
/opt/CSCOlumos/bin/listDeviceLevelDebug.sh logName
```

logName - Enter xde or inventory as necessary.

Example

```
/opt/CSCOlumos/bin/listDeviceLevelDebug.sh inventory
```

Disable device-specific logging

To disable device-specific logging for the specified log, set the log level to INFO. This disables device-specific logging for all devices

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh logName INFO
```

logName - Enter xde or inventory as necessary.

Note You cannot disable logging for specific devices.

Example

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh inventory INFO
```

Inventory Discovery Process Logs

The logs for inventory-discovery-process are available at:
`/opt/CSCOlumos/logs/inventory-discovery-process`

To change log level for inventory-discovery-process, enter the following commands in the admin CLI (see Establish an SSH Session With the Cisco EPN Manager Server):

- To change the log level to INFO:

```
/opt/CSCOlumos/bin/setLogLevel.sh logName INFO inventory-discovery-process
```

- To change the log level to DEBUG:

```
/opt/CSCOlumos/bin/setLogLevel.sh logName DEBUG inventory-discovery-process
```

logName- Enter XDE or Inventory as necessary.

Synchronize System Logs to an External Location

You can configure to synchronize the *ncs* (Cisco EPN Manger logs) and *os* logs to a local or NFS based repository.

To synchronize the logs to a repository:

Before you begin

Create a local or NFS based repository to which you want to synchronize the logs. For more information on how to do this, see Set Up and Manage Repositories.

Step 1 Open a CLI session with the Cisco EPN Manager server. See Connect via CLI.

Step 2 Enter the following commands in the configuration mode to synchronize the system logs.

- To synchronize the *ncs* logs:

```
logging sync-logs ncs repository repository-name
```

- To synchronize the *os* logs:

```
logging sync-logs os repository repository-name
```

Where *repository-name* refers to the repository you configured.

Note To disable the synchronization, enter these commands instead in the configure terminal mode.

- To disable synchronizing the *ncs* logs:

```
no logging sync-logs ncs repository repository-name
```

- To disable synchronizing the *os* logs:

```
no logging sync-logs os repository repository-name
```

Step 3 Exit configuration mode:

```
exit
```

Example

Example 1

```
(config)# logging sync-logs ncs repository myrepository
(config)# logging sync-logs os repository myrepository
```

```
config# exit
```

Example 2

```
(config)# no logging sync-logs ncs repository myrepository
(config)# no logging sync-logs os repository myrepository
config# exit
```

Security Log

Cisco EPN Manager maintains a log of security-related actions performed by a root user and members of the admin and super-user user group in active and past web GUI or CLI sessions.

The logged information includes a description of the event, the IP address of the client from which the user performed the task, and the time at which the task was performed. The following events are logged:

- User login
- User logout
- User creation
- User added
- User deleted
- Lock user
- Unlock user
- Linux shell entering
- User modifications (mail, password)

To view details of this log, enter the following command. You must be logged in as an admin CLI user to use this command. For more information, see Establish an SSH Session With the Cisco EPN Manager Server.

```
show logging security
```

Cisco EPN Manager always maintains a log of security-related actions locally.

Event entries from the CLI have the prefix “SYSTEM-CLI:” and entries from the web interface have the prefix “SYSTEM-WEB:” The structure of each event entry is based on a JSON format and is JSON valid.

Events CLI	• SYSTEM-CLI:SSH:LOGIN:FAILED:WRONG_PASSWORD • SYSTEM-CLI:SSH:LOGIN:FAILED:MAXIMUM_ATTEMPTS_REACHED • SYSTEM-CLI:SSH:LOGIN:SUCCESSFUL • SYSTEM-CLI:SSH:LOGOUT:SUCCESSFUL • SYSTEM-CLI:CONSOLE:LOGIN:WRONG_PASSWORD • SYSTEM-CLI:CONSOLE:LOGIN:SUCCESSFUL • SYSTEM-CLI:CONSOLE:LOGOUT:SUCCESSFUL

	• SYSTEM-CLI:USER:ADD • SYSTEM-CLI:USER:DELETE • SYSTEM-CLI:USER:GROUP • SYSTEM-CLI:USER:PASSWORD • SYSTEM-CLI:USER:PASSWORD:POLICY • SYSTEM-CLI:USER:ROLE • SYSTEM-CLI:USER:STATE:LOCK • SYSTEM-CLI:USER:STATE:UNLOCK • SYSTEM-CLI:USER:MAIL • SYSTEM-CLI:USER:OS:SHELL:ENTERED • SYSTEM-CLI:OS:SHELL:ENABLED • SYSTEM-CLI:OS:SHELL:DISABLED
Events UI	• SYSTEM-WEB:UI:NCS:BODGE:LOGIN:SUCCESSFUL • SYSTEM-WEB:UI:LOGOUT • SYSTEM-WEB:UI:LOGIN:SUCCESSFUL • SYSTEM-WEB:UI:LOGIN:AUTHENTICATION_FAILED • SYSTEM-WEB:UI:USER:DELETE • SYSTEM-WEB:UI:USER:ADD • SYSTEM-WEB:UI:USER:STATE:UNLOCK • SYSTEM-WEB:UI:USER:STATE:LOCK • SYSTEM-WEB:UI:USER:UPDATE • SYSTEM-WEB:HM:LOGIN:AUTHENTICATION_FAILED

Send Security Log to an External location

Remote logging is supported and you can configure to forward security-related events to a remote syslog server.

Step 1 Open a CLI session with the Cisco EPN Manager server, making sure you enter configure terminal mode. See Connect via CLI.

Step 2 Enter the following command:

```
logging security hostname[:port]
```

Where *hostname* is the name or IP address of the remote logging host server.

Note This command sends the log to UDP port 514 by default, if the port is not specified.

Step 3 Exit the configuration mode:

```
exit
```

Example

```
/admin(config)# logging security a.b.c.d
/admin(config)# exit
```

Security Events Log

Cisco EPN Manager maintains a log of the following events in the security_events.log files.

- Sessions created or destroyed over cryptographics protocols
- Probable security attacks

Events related to security attacks are logged by default. You must enable logging of cryptographic sessions-related information by setting the log level to **Info**. To do this, run the following command in admin CLI at /opt/CSCOlumos/bin in the server path.

```
./setLogLevel.sh SecurityEvents.crypto INFO
```

Event type	Events	Information Logged
Events related to security attacks	SQL and LDAP injections	Input validation errors, irrespective of the source of the data. The logged data includes the reason why the data is invalid.
Information related to cryptographic sessions	Sessions created and destroyed over the following protocols: • raw • SSH2, Telnet • NETCONF • TL1	• Notification type • Target device • Connection port • Username • Connection type • Session details

You can view the content of the log by entering the following commands in the admin CLI. See Establish an SSH Session With the Cisco EPN Manager Server for more information.

```
less /opt/CSCOlumos/logs/security_events.log
less /opt/CSCOlumos/logs/security_events.log.x
```

Where:

- *x* is a number greater than or equal to 1 since this is a rolling event log file.