Audits and Logs

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** > **Device Management** > **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

The Change Audit report lists the actions that 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 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 11
Syslog	Forwards Cisco EPN Manager audit logs (as syslogs) to another recipient.	Forward System Audit Logs As Syslogs, on page 11

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 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 > Settings > Logging:
Change the size of logs and the number of logs saved	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 will be 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 will be 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 will be no changes to the files .log.3, .log.4, and .log.5.

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. When you restart Cisco EPN Manager , the log level resets to Error.
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** > **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 desired **Log Modules**.

Log Modules	Description
AAA	This log module enables the ncs-0-0.log, nms_sys_error.log, usermgmt.log, and XmpUserMgmtRbac.log files. The logs are printed when the user logs in. The AAA mode changes like local, tacacs, radius, and sso mode changes are performed.
Apic	This log module enables the ifm_apic.log file which captures the log that occurs when a PNP profile gets synced against APIC.
APICPIIntegration	This log module enables the apic_pi_integration.log file that captures the logs when the profiles are synced in APICEM as sites.
AppNav	This log module enables the appNav.log file to capture the logs when saving the ACL configuration in a template, deleting ACL from a template, creating and updating WAAS

Log Modules	Description
	interface, and when creating, updating, and deleting the service node group and controller group.
Assurance AppClassifier	This log module enables the assurance_appclassifier.log file that captures information related to NBAR classification on incoming AVC/Wireless Netflow data. This is for application classification/identification for flow record, as a part of the netflow processing in Cisco EPN Manager.
Assurance Netflow	This log module enables the assurance_netflow.log file that captures information pertaining to the processing of incoming Netflow data being sent from various Netflow devices to Cisco EPN Manager. It logs information related to netflow processing performed on flow exports received on UDP port 9991.
Assurance PfR	This log module enables the assurance_pfr.log file that captures information related to the PfRMonitoring process.
Assurance WirelessUser	This log module enables the assurance_wirelessuser.log file that captures the information when the WirelessUser job runs to read the user data and populate it in the memory caches that are added by the WIRELESS_ASSURANCE trigger.
Assurance WSA	This log module enables the wsa_collector.log, access_log , assurance_wsa.log, and error_log files that captures information while WLC processes data from device to Cisco EPN Manager. Logs are generated as a part of the Wireless Controller data collection.
AVC Utilities	This log module enables the aems_avc_utils.log file. The AVC configuration feature-specific utility flow logs are generated as a part of this component.
CIDS Device Logs	This log module captures information related to device pack operation of few devices that are not migrated to XDE.
Operations Center Logs	This log module enables the cluster.core.log file that captures information related to management Cisco EPN Manager servers.
Collection	This log module captures the information of the dashlet that is launched to check the readiness of a device.
Common Helper	This log module captures the XMP common related information.
Configuration	This log module enables the ifm_config.log file when the templates such as CLI, Composite, and MBC are deployed to the devices. The service business logic execution debug logs are captured.

Log Modules	Description
Configuration Archive	This log module enables the ifm_config_archive.log and ifm_config_archive_core.log files. The logs are captured based on the selected log level in GUI and logs are logged for all the Configuration Archive module supported operations like Configuration Archive Collection, Configuration Archive Overwrite, Configuration Archive Rollback, and Configuration Archive Deploy.
Configuration Archive Core	This log module enables the ifm_config_archive_core.log file which captures the information on the interaction between service layer and device pack while performing the operations like Configuration Archive Collection, Configuration Archive Overwrite, Configuration Archive Rollback, and Configuration Archive Deploy.
Configuration Templates	This log module enables the ifm_config.log and ifm_template.log files. These files are logged when a System template, Composite template, or Feature template is deployed to a device and the deploy job is created. The logs are captured based on the selected log level [INFO, ERROR, TRACE] in the GUI and are logged for all the Configuration templates that are deployed to the devices.
Container Management	This log module enables the logs for ifm_container.log file. This file is logged when the container management performs the life cycle operations (Install, Activate, Uninstall, and Deactivate) of the virtual appliances.
Credential Management	This log module enables the logs from NMS_SysOut.log file.
Credential Profile	This log module enables the ifm_credential_profile.log file that captures the profile creation, deletion, and profile update information.
DA	This log module enables the ifm_da.log and da_daemon.log files.This module captures the information such as SNMP polling, NAM polling and Packet Capture work flows.
Database	This log module enables the rman.log and db_migration.log files.
Datacenter	This log module enables the datacenterevent.log and ifm_datacenter.log files. These files contain debug information while adding, editing, and deleting devices (Discovery Sources, UCS, Nexus). Inventory module logs also contain the debug information about Datacenter devices.
Device Credential Verification	This log module enables the XDE.log file.

Log Modules	Description
Discovery	This log module enables the ifm_discovery.log and existenceDiscovery.log files that captures logs while creating, editing, and deleting discovery settings or discovery job, and running discovery job.
DSM	This log module captures the information related to Virtual Inventory Discovery Source Manager.
Fault Management	This log module enables the ifm_fault.log, xmp_correlation.log, and xmp_syslog.log files.
Faults	This log module enables the ifm_fault.log, xmp_correlation.log, and xmp_syslog.log files.
Firewall and AVC Configuration	This log module enables the aems_config.log file that captures the AVC, ZBFW, QoS, and NAT configuration details.
Firewall and AVC Inventory	This log module enables the aems_zbfw_ice_post_processors.log file that catures the device inventory time read on AVC, ZBFW, QoS, and NAT configuration.
Firewall and AVC REST API	This module enables the aems_config_access_layer.log file that captures the REST API call details for AVC, ZBFW, QoS, NAT, and PPM features.
Firewall and AVC Utilities	This log module enables the aems_utils.log file that captures the common utility calls in AVC/ZBFW/QoS, NAT and PPM features.
Firewall Utilities	This log module enables the aems_zbfw_utils.log file that captures the ZBFW utility calls.
Grouping	This log module enables the ifm_grouping.log, grouping-spring.log files. It captures data while adding, editing, and deleting groups, and adding and deleting members. It also captures the log while importing or exporting groups in CSV format and creating port groups, editing, and deleting port groups.
Inventory	This log module enables the inventory.log, ifm_inventory.log,existenceInventory.log, and xde.log files. It captures the data while adding, editing, and deleting devices and performing inventory collection.
Mobility	This log module captures the information related to the mobility anchor devices that are added to the server.
Monitor	This log module captures the information related to the APIs that appears while launching the monitor dashlets such as Top N Memory and Top N CPU.

Log Modules	Description
MSAP	This log module enables the ncs.log file. It captures the data related to MSE High Avaliabilty actions such as Proxy configuration and BBX configuration.
MSE	This log module enables the ncs.log file. It captures the data related to Mobility Service Engine actvities such as adding, editing, and deleting MSE and Controller and SiteMap synchronization with MSE.
nbifw	This log module allows you to change the logging level of the NBI API framework. You can view the information in the xmpNbiFw.log file.
ncs_nbi	This log module allows you to change the logging level of the Statistics NBI Services. You can view the information in the ncs_nbi.log file.
Network Topology	This log module enables the nms-topology.log and xmptopology.log files. This log module captures logs related to the **Maps > Network Topology** page. Information such as adding and deleting links between devices are captured.
nfvos	This log module is used for tracking esa dna integration process.
Nice	This log module captures the topology related information after adding a device.
Notifications	This log module captures information from the ncs-0-0.log, ncs_nb.log and alarm_notification_policy.log files.
PA	This log module enables the ifm_sam.log and sam_daemon.log files. The information such as application and service, dashboard and dashlet service API calls, NAM configuration, NAM polling, and Packet Capture feature work flow are captured.
Ping	This log module captures information related to network device polling interval job. Once the job is completed, each device in the system receives a ping.
Plug and Play	You can enable this module to capture the information related to PNP profile creation and provisioning, bootstrap initial configuration, APIC EM sync timeframe. The logs are captured in the ifm_pnp.log and ifm_apic.log files.
Protocol Pack Management	This module enables the aems_ppm_service.log , ifm_container.log , jobManager.log and ifm_jobscheduler.log files. This logs the information related to protocol pack import, distribution of protocol packs, and the jobs details.

Log Modules	Description
Reports	You can enable this module to view the report related queries, memory consumption, and time frame of report generation.
Smart Licensing	This log module enables the ifm_smartagent.log and smart_call_home.log files. The ifm_smartagent.log file contains licensing logs related to smart licensing and smart_call_home.log contains call home logs that captures information transmitted to CSSM (Cisco Smart Software Manager). These logs are captured in Periodic events and User action based events.
SWIM	You can enable this module to log the Software Image Management module logs in the ifm_swim.log file. The logs will be captured as per the selected log level in GUI. It logs the information related to the Software Image Management operations like Software Image Recommendation, Software Image Upgrade Analysis, Software Image Import, Software Image Distribution, Software Image Activation, and Software Image Commit.
System Monitoring	This log module enables the ifm_sysmon.log file. This logs information pertaining to the rule start time and end time as well as the operations performed in between.
ThreadManager	This log module enables the xmp _threadmanager.log file that captures the hybernate related information.
Threshold	You can enable this module to view the details of the events processed by the Threshold Monitor.
TrustSec	You can enable this module to capture the TrustSec readiness devices, devices capable for enforcement, device classification, and capable devices information. The list is displayed in Service-TrustSec-Readiness. You can view the logs in the ifm_trustsec.log file.
Wlan AVC Configuration	This log module enables the aems_config_wlan.log file to view the WLAN configuration work flow related information.
XMLMED	You can enable this module to capture the SOAP requests and responses. You can also view these logs in the ncs.log files.

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

Step 5 Click **Save**.

Step 6 Reproduce the problem on the system so the details can be captured in the logs.

Step 7 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.

The information captured in the ifm_da.log and ifm_sam.log files are now split-up into the accompanying classes:

- assurance_wirelessuser.log
- assurance_pfr.log
- assurance_netflow.log
- assurance_appclassifier.log

The ifm_da.log file logs the information related to the Netflow devices and their respective pcaps, post device inclusion on Cisco EPN Manager. The assurance_wirelessuser.log file logs the information that is captured when the WirelessUser job runs to read the user data and populate in the memory caches that are added by WIRELESS_ASSURANCE. The assurance_pfr.log file stores the PfR monitoring related information. The assurance_netflow.log file logs the processing of incoming Netflow data being sent from various Netflow devices to Cisco EPN Manager. The assurance_appclassifier.log file stores the logs for NBAR classification on incoming AVC/Wireless Netflow data.

Step 8 In the E-Mail Log File area, enter a comma-separated list of e-mail IDs.

Step 9 Revert to the original setting in the **Message Level** drop-down list.

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 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**.

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.

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 the global log level is set 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.

Once the device-level logging is enabled, DEBUG mode is enabled for the specified device(s). During sync, the generated log files are *xde.log.**, *inventory.log.** and *ifm_inventory.log.**. Cisco EPN Manager stores the inventory or XDE logs in DEBUG mode only for the specified device(s). For other devices, only INFO logs are stored. 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-level logging is enabled for a particular log, 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

Disable device-specific logging by running the following command. This disables device specific logging for the specified log, across all devices.

Note You cannot disable logging for specific devices.

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

logName - Enter xde or inventory as necessary.

Example

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

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.

Synchronize System Logs to an External Location

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 synchonize 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)

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

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.

- 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 injections	Input validation errors, irrespective of the source of the data. The logged data includes information about 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.