Audits and Logs

This section contains the following topics:

AuditConfigurationArchiveandSoftwareManagementChanges ()

The window displays changes made to devices using the Configuration Archive and Software Management features. To view these changes, choose . lists the most recent devices changes including the type of change (Configuration Archive, Software Image Management).

You can also view the most recent changes for a device in the **Recent Changes** tab of its Device 360 view.

Audit Changes Made By Users (Change Audit)

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 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

Feature	Examples
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, 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 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 configure 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 server for the records to be reflected in secure tls log.

View Change Audit Details

Step 1 Log in to as an administrator

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

The **Change Audit Dashboard** displays the network audit logs and change audit data of device management, user management, configuration template management, device community and credential changes, and inventory changes of devices. The **Change Audit report** and **Change Audit** dashboard display the details irrespective of the virtual domain you are logged in.

Audit Actions Executed from the GUI (System Audit)

Note 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 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

Find actions performed:	Do the following:
On a specific day	Enter the day in the **Audit Time** quick filter filed (in the format *yyyy–mmm–dd*)

System Logs

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 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, 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 11

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, 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.
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. You will have to restart 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** > **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 Prime Infrastructure profiles are synced in APICEM as sites.

Log Modules	Description
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 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 Prime Infrastructure.
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 Prime Infrastructure. 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 Prime Infrastructure. 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 Prime Infrastructure 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.

Log Modules	Description
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.
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, Custome CLI template, Composite Template, or Feature Template is deployed to a device and the deploy job is created. The logs are captured in based on the selected log level [INFO, DEBUG, TRACE] in GUI and are logged for all the Configuration templates that is 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

Log Modules	Description
	(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.
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.

Log Modules	Description
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.
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.

Log Modules	Description
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.
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 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.

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 . 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 . The assurance_appclassifier.log file stores the logs for NBAR classification on incoming AVC/Wireless Netflow data.

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

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 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 for your changes to take effect. See Stop and Restart.