CHAPTER 11

Administering Change Audit and Software Management

Change Audit tracks and reports changes made in the network. Change Audit allows other LMS to log change information to a central repository. Device Configuration, Inventory, and Software Management changes can be logged and viewed using Change Audit.

LMS writes change records to Change Audit. Change Audit stores these records in the log tables (summary and details) for later use with reports.

For example, Software Management records a change for each completed device upgrade. If a job has ten devices, then Software Management writes ten entries to the Change Audit log, but the Change Audit report shows only one job with ten devices. You can then access individual device information.

Each application writes its own change records to Change Audit. For example, in Inventory you can set inventory change filters to filter out all kinds of information for different device types. Change Audit record maintenance is controlled by the Change Audit Delete Change History option.

You can convert change records into SNMP V1 traps and forward them to a destination of your choice. This allows system administrators to forward critical network change data to their own NMS.

You can define automated actions (e-mail and automated scripts) on creation of change audit record. The automated action gets triggered on creation of the change audit record.

This section contains:

Setting Up Preferences

You can use this feature to set up your editing preferences. Config Editor remembers your preferred mode, even across different invocations of the application.

You can change the mode using the Device and Version, Pattern Search, Baseline or External Configuration option but the changes do not affect the default settings.

To set up preferences:

Step 1 Select **Configuration > Tools > Config Editor > Edit Mode Preference**.

The User Preferences dialog box appears.

Step 2 Set the default edit mode:

- Select **Processed** to display the file in the Processed mode.

  The configuration file appears at the configlet level (a set of related configuration commands). The default is Processed.

- Select **Raw** to display the file in the Raw mode.

  The entire file appears as shown in the device.

Step 3 Click **Apply** to apply the set preferences.

Performing Change Audit Tasks

Change Audit allows you to:

- Determine changes being made in the network during critical operations time

  System administrators can define the start and end times during the day when network changes should not be made. Based on this selection you can quickly see, for a given day, whether changes were made when they should not be.

  See Defining Exception Periods for defining the exception periods.

- Define automated actions on creation of change audit record

  Automated action gets triggered on creation of the change audit record. You can define any number of automated actions. The supported automated actions are, E-mail, Traps, and Automated scripts

  See Defining Change Audit Automated Actions for defining the Change Audit automated actions.

- Monitor your software image distribution and download history for software changes made using the Software Management application.

  Software Management automatically sends network change data to the Change Audit summary and details tables.

- Track any configuration file changes

  Device Configuration automatically sends data on configuration file changes to the Change Audit log.

  See Generating 24 Hours and Standard Change Audit Reports for generating the Change Audit reports.

- Monitor inventory additions, deletions, or changes

  Inventory tracks specific messages or monitors any and all changes in your network inventory. To set inventory filters, use the Inventory Change Filter option.

  See Generating 24 Hours and Standard Change Audit Reports for generating the Change Audit reports.

- View all the latest changes that occurred in the network over the last 24 hours

  24-Hour Reports provides a quick way to access the latest changes in the Change Audit log.

  See Generating 24 Hours and Standard Change Audit Reports for generating the Change Audit reports.

- Purging the Change Audit records

  Frees disk space and maintains your Change Audit records at a manageable size. You can either schedule for periodic purge or perform a forced purge of Change Audit data.

  See Performing Maintenance Tasks for scheduling a periodic purge.

- Generating change audit data in XML format

  `cwcli export changeaudit` is a command line tool that also provides servlet access to change audit data. This tool uses the existing Change Audit log data and generates the Change Audit log data in XML format.

- Set the debug mode for Change Audit application

  You can set the debug mode for Change Audit application in the Log Level Settings dialog box (Select **Admin > System > Debug Settings > Config and Image Management Debugging settings**; select Change Audit from the Application drop-down list.).

Generating 24 Hours and Standard Change Audit Reports

To generate 24 Hours and Standard Change Audit Reports:

Step 1 Select **Reports > Audit**.

Step 2 Select **Change Audit** from the first drop-down list box.

Step 3 Select **Standard f**rom the second drop-down list box.

Performing Maintenance Tasks

You can either schedule for periodic purge or perform a forced purge of Change Audit data. This frees disk space and maintains your Change Audit data at a manageable size.

You can perform these tasks:

- Setting the Purge Policy
- Performing a Forced Purge
- Config Change Filter

Setting the Purge Policy

You can specify a default policy for the periodic purging of Change Audit data.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To set the Change Audit Purge Policy:

Step 1 Select **Admin > Network > Purge Settings > ChangeAudit Purge Policy**.

The Purge Policy dialog box appears in the Periodic Purge Settings pane.

Step 2 Enter the following information:

Field	Description
Purge change audit records older than	Enter the number of days. Only Change Audit records older than the number of days that you specify here, will be purged. The default is 180 days.
Purge audit trail records older than	Enter the number of days. Only Audit Trail records older than the number of days that you specify here, will be purged. The default is 180 days.
Scheduling	
Run Type	You can specify when you want to run the Purge job for Change Audit and Audit Trail records. To do this select one of the following options from the drop-down menu: • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete. For example: If you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed. If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, then the next job will start only at 10:00 a.m. on November 3.
Date	You can select the date and time (hours and minutes) to schedule.
at	Enter the start time, in the hh:mm:ss format (23:00:00).

Field	Description
Job Info	
Job Description	The system default job description, *ChangeAudit Records - default purge job* is displayed. You cannot change this description.
E-mail	Enter e-mail addresses to which the job sends messages at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). We recommend that you configure the E-mail ID in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). When the job starts or completes, an e-mail is sent with the E-mail ID as the sender's address.

Caution You might delete data by changing these values. If you change the number of days to values lower than the current values, messages over the new limits will be deleted.

Step 3 Click either **Save** to save the Purge policy that you have specified, or click **Reset** to reset the changes made to a Purge policy.

Performing a Forced Purge

You can perform a Forced Purge of Change Audit, as required.

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To perform a Change Audit Forced Purge:

Step 1 Select **Admin > Network > Purge Settings > ChangeAudit Force Purge**.

The Purge Policy dialog box appears.

Step 2 Enter the information required to perform a Forced Purge:

Field	Description
Purge change audit records older than	Enter the number of days. Only Change Audit records older than the number of days that you specify here, will be purged.
Purge audit trail records older than	Enter the number of days. Only Audit Trail records older than the number of days that you specify here, will be purged.

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Force Purged job for Change Audit and Audit Trail records. To do this select one of the following options from the drop-down menu: • Immediate—Runs this task immediately. • Once—Runs this task once at the specified date and time.
Date	Enter the start date in the dd-mmm-yyyy format, for example, 02-Dec-2003, or click on the Calendar icon and select the date. The Date field is enabled only if you have selected Once as the Run Type.
at	Enter the start time, in the hh:mm:ss format (23:00:00). The At field is enabled only if you have selected Once as the Run Type
Job Info	
Job Description	Enter a description for the job. This is mandatory.
E-mail	Enter e-mail addresses to which the job sends messages at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). We recommend that you configure the E-mail ID in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). When the job starts or completes, an e-mail is sent with the E-mail ID as the sender's address.

Step 3 Click **Submit** for the Forced Purge to become effective.

Config Change Filter

You can use this option to enable or disable VLAN Change audit filtering. When there is a change to the device configuration, a change record is created. By default, the VLAN change audit record is created for those devices that have a VLAN configuration.

To enable or disable the VLAN Change Audit Filter option:

Step 1 Select **Admin > Network > Change Audit Settings > Config Change Filter.**

The Config Change Filter dialog box appears.

Step 2 Check or uncheck the Enable VLAN Change Audit Filter option.

- Check **Enable VLAN Change Audit Filter**, if you do not want the change audit record to be created for devices that have a VLAN configuration.
- Uncheck **Enable VLAN Change Audit Filter**, if you want the change audit record to be created for devices that have VLAN configuration. By default, this option is unchecked.

Step 3 Click either **Apply** to apply the option or click **Cancel** to discard the changes.

Defining Exception Periods

An Exception period is a time you specify when no network changes should occur. This period does not prevent you from making any changes in your network. The set of Exception periods is known as an Exception profile.

You can have only one Exception period for a day.

You perform the following tasks for Exception profiles:

Tasks	Description
Creating an Exception Period	Creating an exception profile.
Enabling and Disabling an Exception Period	Enabling and disabling a set of exception profiles.
Editing an Exception Period	Editing an exception profile.
Deleting an Exception Period	Deleting a set of exception profiles.

Creating an Exception Period

To create an Exception profile:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Admin > Network > Change Audit Settings > Exception Periods**.

The Define Exception Period dialog box appears.

Step 2 Select:

- Days of the week from the Day drop-down list box
- Start and end times from the Start Time and the End Time drop-down list box.

Step 3 Click **Add**.

The defined exception profile appears in the List of Defined Exception Periods pane.

To enable the exception period, see Enabling and Disabling an Exception Period.

Enabling and Disabling an Exception Period

To enable and disable a set of exceptions periods:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Admin > Network > Change Audit Settings > Exception Periods**.

The Define Exception Period dialog box appears.

Step 2 Select one or more exception profiles in the List of Defined Exception Periods pane.

Step 3 Click **Enable/Disable**.

- If you have selected Enabled, then the exception period report is generated for that specified time frame.
- If you have selected Disabled, then the exception period report is not generated for that whole day.

  For example: If you have disabled exception period for Monday from 10:00 am to 12:30 pm, then there will not be any exception period report generated for Monday.

Editing an Exception Period

To edit an exception profile:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Admin > Network > Change Audit Settings > Exception Periods**.

The Define Exception Period dialog box appears.

Step 2 Select a day from the Day drop-down list box for which you want to change the exception period.

Step 3 Change the start and end times in the Start Time and the End Time drop-down list box.

If required you can also enable or disable the status for the exception period.

Step 4 Click **Add**.

The edited exception profile appears in the List of Defined Exception Period dialog box. This will overwrite the existing exception profile for that day.

Deleting an Exception Period

To delete a set of Exceptions Periods:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Admin > Network > Change Audit Settings > Exception Periods**.

The Define Exception Period dialog box appears.

Step 2 Select one or more exception profiles in the List of defined Exception Periods pane.

Step 3 Click **Delete**.

Defining Change Audit Automated Actions

You can define automated actions on creation of change audit record. This automated action gets triggered on creation of the change audit record. You can define any number of automated actions. The supported automated actions are:

- E-mail
- Traps
- Automated scripts

This section contains:

Understanding the Automated Action Window

This window contains the following entries:

Field	Description
Name	Name of the automated action.
Status	Status of the automated action—Enabled, or disabled.
Type	Type of automated action—Email, Script or Trap.

You perform the following tasks from this window:

Tasks	Description
Creating an Automated Action	Creating an automated action.
Enabling and Disabling an Automated Action	Enabling and disabling a set of automated actions. This button gets activated only after selecting an automated action.
Editing an Automated Action	Editing an automated action. This button gets activated only after selecting an automated action.
Exporting and Importing an Automated Action	Exporting and importing a set of automated actions.
Deleting an Automated Action	Deleting a set of automated actions. This button gets activated only after selecting an automated action.

Creating an Automated Action

To create an automated action:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Admin > Network > Notification and Action Settings > ChangeAudit Automated Actions**.

The Automated Action dialog box appears.

Step 2 Click **Create**.

The Define Automated Action dialog box appears.

Step 3 Enter the following:

Field	Description
Name	Name for the automated action.
Status	Select either Enabled or Disabled For the automated action to trigger.
Application	Select the name of the application on which the automated action has to be triggered.
Category	Select the types of the changes, for example, configuration, inventory, or software on which the automated action has to be triggered.
Mode	Select the connection mode on connection modes on which the automated action has to be triggered.
User	Select the user name on which the automated action has to be triggered.

Step 4 Click **Next**.

The Automated Action Type dialog box appears.

Step 5 Select either **E-mail** or **Trap** or **Script**. Based on your selection, enter the following data:

Field	Description
If you have selected E-mail, enter:	
Send To	Enter the E-mail ID for which the trigger has to be notified. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). We recommend that you configure the E-mail ID in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). You will receive the e-mail with the E-mail ID as the sender's address.
Subject	Enter the subject of the e-mail.
Content	Enter the content of the e-mail.

Field	Description
If you have selected Trap, perform:	
Enables configuration of a single or dual destination port numbers and hostnames for the traps generated by Change Audit. Ensure that you have copied these files: • CISCO-ENCASE-MIB.my • CISCO-ENCASE-APP-NAME-MIB.my into the destination system to receive the traps. These files are available in the following directories on LMS server: On UNIX: /opt/CSCOpx/objects/share/mibs On Windows: *NMSROOT*\objects\share\mibs. Where *NMSROOT* is the root directory of the LMS Server. **a.** Enter the Server and Port details in the Define Trap field. **b.** Click **Add**. The server and port information appears in the List of Destinations text box. If you want delete, the server and port information, select the server and port information from the List of Destinations text box and click **Delete**.	
If you have selected Script, enter...	
You can run only shell scripts (*.sh) on Unix and batch files (*.bat) on Windows. The shell script or batch file should have only write/execute permissions for casuser:casusers in Solaris/Soft Appliance and casuser/Administrator in Windows. The other users should have only read permission. You must ensure that the scripts contained in the file has permissions to execute from within the *casuser* account. The following are the parameters for change audit automated action that will appear in the script: – Application Name – Category – User Name – Description – Connection Mode – Host Name The script files must be available at this location: On UNIX: /var/adm/CSCOpx/files/scripts/changeaudit On Windows: *NMSROOT*/files/scripts/changeaudit To select the script file: **a.** Click **Browse**. The Server Side File Browser dialog box appears with the predefined location. **b.** Select the script file (*.sh on Unix and *.bat on Windows) **c.** Click **OK**.	

Step 6 Click **Finish**.

The Automated Action window appears with the defined automated action.

Editing an Automated Action

To edit an automated action:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Admin > Network > Notification and Action Settings > Change Audit Automated Actions**.

The Automated Action dialog box appears.

Step 2 Select an Automated Action.

Step 3 Click **Edit**. (See step 3 to step 5 in Creating an Automated Action.).

Step 4 Click **Finish**.

The Automated Action window appears with the updated data.

Enabling and Disabling an Automated Action

To enable or disable a set of automated actions:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Admin > Network > Notification and Action Settings > Change Audit Automated Actions**.

The Automated Action dialog box appears.

Step 2 Select one or more Automated actions.

Step 3 Click **Enable/Disable**.

The Automated Action window appears with the updated data.

Exporting and Importing an Automated Action

To export or import an automated action:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Admin > Network > Notification and Action Settings > Change Audit Automated Actions**.

The Automated Action dialog box appears.

Step 2 If you want to export an Automated action, then select the automated actions else go to next step.

Step 3 Click **Export/Import**.

The Export/Import dialog box appears.

Step 4 Select the task to be performed—**Export** or **Import**.

Step 5 Either:

- Enter the filename along with the absolute path.

Or

- Click **Browse**,

  The Server Side File Browser dialog box appears.

a. Select a folder.

b. Click **OK**.

c. Enter the filename.

Step 6 Click **OK**.

Deleting an Automated Action

To delete a set of automated actions:

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

Step 1 Select **Admin > Network > Notification and Action Settings > Change Audit Automated Actions**.

The Automated Action dialog box appears.

Step 2 Select a or a set of Automated actions.

Step 3 Click **Delete**.

The Automated Action window appears with the updated data.

Software Management Administration Tasks

You can set your preference to download images. To do this, select **Admin > Network > Software Image Management**.

The following section explains how to set the Software Management preferences:

- Viewing/Editing Preferences

Viewing/Editing Preferences

Edit Preferences helps you to set or change your Software Management preferences.

The options you specify here are applicable to Software Management tasks such as image distribution, image import, etc.

This section contains:

- Selecting and Ordering Protocol Order
- How Recommendation Filters Work for an IOS Image

Note View Permission Report (**Reports > System > Users > Permission**) to check if you have the required privileges to perform this task.

To view and edit the preferences:

Step 1 Select **Admin > Network > Software Image Management > View/Edit Preferences**.

The View/Edit Preferences dialog box appears.

Step 2 Enter the following:

Field	Description	Usage Notes
Repository Management		
Image Location	New directory to store software images. By default the software images are stored at this location: On Solaris/Soft Appliance: /var/adm/CSCOpx/files/rme/repository/ On Windows: *NMSROOT*/files/rme/repository Where *NMSROOT* is the Cisco Prime installed directory.	If you enter a new name, all existing files are moved to this directory. If the directory does not have enough space, the files are not moved and an error message appears. If the specified directory does not exist, Software Management creates a new directory before moving the files to the new directory. The new directory should be empty. The new directory specified by you should have the permission for *casuser*:*casusers* in Solaris/Soft Appliance and *casuser* should have Full Control in Windows.

Field	Description	Usage Notes
Distribution		
Script Location	You can specify only shell scripts (*.sh) on UNIX and batch files (*.bat) on Windows. The script files *must* be available at this location: On UNIX: /var/adm/CSCOpx/files/scripts/swim On Windows: *NMSROOT*/files/scripts/swim To select the script file: a. Click **Browse**. The Server Side File Browser dialog box appears with the predefined location. b. Select the script file (*.sh on Unix and *.bat on Windows) c. Click **OK**. You can use **Clear** to clear your selections for Script Location. This clears all previous values.	On UNIX, the scripts should have read, write, and execute permissions for the owner (casuser) and read and execute permissions for group casusers. That is, the script should have 750 permission. On Windows, the script should have read, write, and execute permissions for casuser/Administrator. The other users should have only read permission. You must ensure that the scripts contained in the file have permissions to execute from within the *casuser* account. This script is run before and after completing each device software upgrade for all scheduled jobs.
Script Timeout (seconds)	Number of seconds the user's script can run (default = 90).	Software Management waits for the time specified before concluding that the script has failed.
Protocol Order	Specify an order of preferred protocol for image import/distribution. The supported protocols are: • RCP • TFTP • SCP • HTTP See Selecting and Ordering Protocol Order for further details.	This preferred protocol order is followed only for those devices that permit more than one protocol for image transfer. In devices, where multiple protocol option is not available for image transfers, Software Management uses its own knowledge and selects the relevant protocol to upgrade the device. For fetching configuration from device, the protocol settings of Configuration Management is used. Software Management uses the same protocol for fetch and download of configurations. You can set the Configuration Management protocol order using **Admin > Collection Settings > Config > Config Transport Settings**.

Field	Description	Usage Notes
Use SSH for software image upgrade and software image import through CLI (with fallback to TELNET).	Uses this protocol to connect to the devices. By default, Telnet is used to connect to the devices. If SSH fails, then Telnet is used to connect to the devices.	The device must support SSH for Software Management to use this protocol. Software Management uses command line interface to upgrade software images and to import software images. When you select the SSH protocol for the Software Management, the underlying transport mechanism checks whether the device is running SSHv2. If so, it tries to connect to the device using SSHv2. If the device does not run SSHv2 and runs only SSHv1 then it connects to the device through SSHv1. If the device runs both SSHv2 and SSHv1, then it connects to the device using SSHv2. If a problem occurs while connecting to the device using SSHv2, then it does not fall back to SSHv1 for the device that is being accessed and Telnet is used to connect to the device. See the Software Management Functional Supported Device tables on Cisco.com for SSH and CLI device support information. http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html
Recommendation Filters (See How Recommendation Filters Work for an IOS Image.)		
Include Cisco.com images for image recommendation	During image distribution, recommend Cisco.com images for Cisco devices.	
Include General deployment images	Includes only GD images.	For Cisco IOS devices only.
Include latest maintenance release (of each major release).	Includes the latest major releases of IOS images. For example, if Release 12.2(5) was latest maintenance version in the 12.2 major release, the recommended image is IOS 12.2(5).	For Cisco IOS devices only.
Include images higher than running image.	Includes the images that are newer than the images running on your device. For example, if the device is running Release 11.2(3), the recommended images are 11.2(4) and later.	For Cisco IOS devices only.

Field	Description	Usage Notes
Include same image feature subset as running image.	Include only images that have the same feature subset as the current image. For example, if you want IOS images with the ENTERPRISE IPSEC feature, the recommended images contain the latest version. This version contains feature subset that fits the Flash.	For Cisco IOS devices only.
Password Policy		
Enable Job Based Password	Enter a username and password for running a specific Software Management job. If you enter a username and password, Software Management application uses this username and password to connect to the device, instead of taking these credentials from the Device and Credential Repository.	• If you have enabled User Configurable option, you can disable this option while scheduling the distribution jobs. • If you have disabled User Configurable option, you must enter the username and password while scheduling the distribution jobs. These passwords are used only to connect to devices for which Software Management uses CLI, Telnet, and SSH.for software upgrades. See the Software Management Functional Supported Device tables on Cisco.com for CLI, Telnet and SSH device support information. http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Step 3 Either:

- Click **Apply** to save your changes.
- Click **Defaults** to display the default configuration.
- Click **Cancel** to discard the values entered and revert to previously saved values.

Selecting and Ordering Protocol Order

In the View/Edit Preferences dialog box (**Admin > Network > Software Image Management > View/Edit Preferences**) you can define the protocol order that Software Management has to use for software image download.

Software Management tries to download the software images based on the specified protocol order.

While downloading the images, Software Management uses the first protocol in the list. If the first protocol in the list fails, these jobs use the second protocol and so on, until Software Management finds a transport protocol for downloading the images.

To Enable the Protocols:

Step 1 Select a protocol from the Available Protocols pane.

Step 2 Click **Add** or double click the mouse.

To Disable the Protocols:

Step 1 Select a protocol from the Selected Protocol Order pane.

Step 2 Click **Remove** or double click the mouse.

To Reorder the Protocols

Step 1 Select the protocols from the Selected Protocol Order pane.

Step 2 Click **Remove**.

You can either select the protocols individually or use the mouse to select all of them and click **Remove**.

Step 3 Select a protocol from the Available Protocols pane.

Step 4 Click **Add** or double click the mouse.

How Recommendation Filters Work for an IOS Image

This section describes how the recommendation filters that you select in the View/Edit Preferences dialog box (**Admin > Network > Software Image Management > View/Edit Preferences**) work for a Cisco IOS image.

If you have selected the option, Include Cisco.com Images for image recommendation, Software Management checks for the images that are available on Cisco.com and the Software repository.

If the same image is available in the Software repository and Cisco.com, the image is recommended from the Software repository.

If you have not selected the option, Include Cisco.com Images for image recommendation, the Software Management checks and recommends images only from Software repository.

Table 11-1 Recommending Images for an Cisco IOS Image

Option Number	Include General Deploy-ment Images	Include Latest Mainten ance Release (of Each Major Release)	Include Images Higher Than Running Image	Include Same Image Feature Subset as Running Image	Recommendation
1	Not selected	Not selected	Not selected	Not selected	The recommendation image list includes: • All available images. • In case of, – Multiple images with the same version as that of the running image version are present, the image with a higher compatible feature than the running image is recommended. – Similar images in Cisco.com and Software Management repository, the image from the repository is recommended. • The image feature can be the same or a superset of the running image. If a higher version is not available, then no recommendation is made.
2	Not selected	Not selected	Not selected	Selected	The recommended list contains images that have the same feature set as that of the running image. The images with the highest version among the recommended image list are recommended.
3	Not selected	Not selected	Selected	Not selected	The recommend list contains all types of releases (deployment status). The images with the highest version among recommended image list are recommended. The feature set of the recommended image may be superior than the running image.
4	Not selected	Selected	Not selected	Not selected	The latest maintenance version in each release is available in the recommend image list. The latest image version is recommended.

Table 11-1 Recommending Images for an Cisco IOS Image (continued)

Option Number	Include General Deploy-ment Images	Include Latest Mainten ance Release (of Each Major Release)	Include Images Higher Than Running Image	Include Same Image Feature Subset as Running Image	Recommendation
5	Selected	Not selected	Not selected	Not selected	The images with deployment status identified as GD are available in the recommended image list and other recommendation flow remains the same as the option 1.
6	Selected	Not selected	Not selected	Selected	Same as option5. However, the recommended list contains images that have the same feature set as that of running image.
7	Selected	Not selected	Selected	Not selected	Same as option 5. However, the image with the highest version in the recommended image list is recommended. The feature set of the recommended image may be superior than the running image.
8	Selected	Not selected	Selected	Selected	Same as option 6. However, the image with the highest version in the recommended image list is recommended. All recommend images will have the same feature subset as the running image.
9	Selected	Selected	Not selected	Not selected	The images with the highest version among recommended image list are recommended. The images of GD types of releases are available in the recommended image list.
10	Selected	Selected	Not selected	Selected	The images with the same feature as that of running image is available in the recommended list and the latest maintenance version of all release is available in the recommended list. Only an image with higher version than running image is recommended. The recommended images can have only GD status.
11	Selected	Selected	Selected	Not selected	Same as option 9. In addition to this, an image with the higher version than running image is also recommended.

Setting Change Report Filters

Using the Inventory Change Filter dialog box, you can select the attributes that you do not wish to log using Change Audit. The history of inventory changes are logged by and viewed through Change Audit.

The attributes that you select in the Inventory Change Filter dialog box, are monitored for Inventory changes like other variables. However, they are not logged using Change Audit. Consequently, these changes are not displayed in your inventory change reports.

For example, for Stack devices, if you do not want to log the operational status for changes in Change Audit, select the Operational Status option in the Inventory Change Filter dialog box.

The Inventory Change Filter dialog box, displays each attribute group and the corresponding filters for the attribute group, for your selection.

- To view all inventory change reports, select **Reports > Inventory**. In the Report Generator dialog box, first select the application, Change Audit, and then select the Exception Period Report from the respective drop-down lists.
- To view inventory changes from the last 24 hours, select **Reports > Inventory**. In the Report Generator dialog box, first select the application, Inventory, and then select report 24 Hour Inventory Change report from the respective drop-down lists.

Note View the Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

To set Inventory change filters:

Step 1 Select **Admin > Network > Change Audit Settings > Inventory Change Filter**.

The Inventory Change Filter dialog box appears.

Step 2 Select a group from the Select a Group drop-down list. See Table 11-2.

The dialog box refreshes to display the filters available for the attribute group that you selected.

Step 3 Select the attributes that you do not want to monitor for changes.

Step 4 Click **Save**.

A confirmation dialog box appears.

Step 5 Click **OK** to save the details.

You can use **Reset All** to reset your selections for *all* groups. This resets all previous values to blanks.

Table 11-2 Inventory Change Filters

Report Inventory Group	Custom Report Group/Attribute	Description
Asset	Orderable Part Number	Orderable part number of asset.
	Tag	Asset tag.
	CLE Identifier	Represents CLIE (Common Language Equipment Identifier) code for the physical entity.
	Mfg Assembly Revision	Manufacturing assembly revision of asset.
	Mfg Assembly Number	Manufacturing assembly number of asset.
	Physical Index	Physical index of asset
Back Plane	Operational Status	Operational status of backplane.
	Parent Relative Position	Indicates the relative position of this child component among all its sibling components.
	Manufacturer Name	Name of manufacturer.
	Physical Entity Name	Name of physical entity.
	Slot Configuration	Configuration of backplane slots
	Model Name	Name of model.
	Vendor Type	Type of vendor.
	Serial Number	Serial number of backplane.
	Description	Description of backplane.
	Component Type	Type of component.
	Index	Index of backplane.
	Field Replaceable Unit	FRU of backplane. Field-replaceable unit is a hardware component that can be removed and replaced on site.
	Alias Name	Alias name of backplane.
Bridge	Bridge Type	Type of bridge.
	Number of Ports	Number of ports in the bridge.
	Base Bridge Address	Base address of bridge.

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Chassis	Chassis Model Name	Name of the chassis model.
	Chassis Serial Number	Serial number of the chassis.
	Chassis Vendor Type	Type of vendor.
	Chassis Version	Version number of the chassis.
	Report Published	Indicates whether Report is published or not. Displays the value as True or False.
	Description	Description of chassis.
	Field Replaceable Unit	FRU of chassis.
	Component Type	Type of component.
	Alias Name	Alias name of chassis.
	Index	Physical index of chassis.
	Parent Relative Position	Indicates the relative position of this child component among all its sibling components.
	Physical Entity Name	Name of physical entity.
	Free Slots	Free slots in chassis.
	Slot Capacity	Slot capacity of chassis.
	Power Available (Watts)	Power available at chassis level
	Power Consumption (Watts)	Power consumption at chassis level
	Power Consumption (%)	Percentage of power consumption at chassis level.
	Power Remaining (Watts)	Power remaining at chassis level.
	Operational Status	Operational status of chassis.
	Manufacturer Name	Name of manufacturer.
	Slot Configuration	Slot configuration of chassis.
Component	Index	Physical index of component.
	Field Replaceable Unit	FRU of component.
	Alias Name	Alias name of component.
	Parent Relative Position	Indicates the relative position of this child component among all its sibling components.
	Operational Status	Operational status of component.
	Manufacturer Name	Name of manufacturer.
	Name	Name of component.
	Slots Configured	Slot configuration of component.
	Model Name	Name of model.
	Vendor Type	Vendor type of component.
	Serial Number	Component serial number.
	Description	Description of component.
	Component Type	Type of component.

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Container	Alias Name	Alias name of container.
	Operational Status	Operational status of container.
	Manufacturer Name	Name of manufacturer of container.
	Slot Configuration	Slot configuration of container.
	Container Model Name	Model name of container.
	Container Vendor Type	Vendor type of container.
	Parent Relative Position	Parent Relative Position of container.
	Container Serial Number	Serial number of container.
	Physical Entity Name	Physical entity name of container.
	Description	Description of container.
	Component Type	Type of container component.
	Index	Index of container.
	Field Replaceable Unit	FRU of container.
Fan	Fan Model Name	Name of model of fan.
	Fan Vendor Type	Vendor type of fan.
	Parent Relative Position	Parent Relative Position of fan.
	Fan Serial Number	Serial number of fan.
	Description	Description of fan.
	Physical Entity Name	Physical entity name of fan.
	Component Type	Component type of fan.
	Index	Index of fan.
	Field Replaceable Unit	FRU of fan.
	Alias Name	Alias name of fan.
	Operational Status	Operational status of fan.
	Manufacturer Name	Name of manufacturer of fan.
	Slot Configuration	Slot configuration of fan.
Flash	Module Index	Module index of flash.

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Flash Device	Removable	Indicates whether the flash device removable.
	Jumper	Jumper of the flash device.
	Controller	Flash device controller.
	Chip Count	Flash device chip count.
	Size (MB)	Total flash device size in MB.
	Partition Count	Partition count of flash device.
	Maximum Partitions	Maximum partitions in flash device.
	Minimum Partition Size (MB)	Minimum partition size of flash device.
	Name	Name of the flash device.
	Index	Index of flash device.
	Description	Description of flash device.
Flash File	Index	Flash file index.
	Status	Flash file status.
	Checksum	Checksum of flash file.
	Size (MB)	Size of flash file.
	Name	Name of flash file.
Flash Partition	Algorithm	Algorithm of the flash partition
	Filename Length	Flash filename length.
	Erase Needed	Whether an erase is needed.
	Upgrade Method	Method of upgrade of flash partition.
	Status	Status of flash partition.
	Free (MB)	Free space in MB.
	Size (MB)	Flash partition size in MB.
	Name	Name of flash partition.
	Index	Flash partition index.

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
IP Address	IP Address	IP Address of the device.
	Index	IP Address index.
	Address State	IP Address state.
	Address Type	Type of IP Address.
	Protocol of Address	Protocol of IP Address.
	Max Re-assemble Size	Maximum re-assemble size.
	Broadcast Address	Broadcast address.
	Network Mask	Network mask of IP Address.
Image	ROM Sys Version	ROM system software version.
	ROM Version	Version of ROM.
	System Boot Variable	System Boot Variable
	System Image File	System image file.
	Minimum Boot Flash (MB)	Minimum Boot Flash in MB.
	Minimum NVRAM (MB)	Minimum NVRAM in MB.
	Minimum DRAM (MB)	Minimum DRAM in MB.
	Media	Media of image.
	Feature	Image feature
	Module	Image module.
	Image	Software image present on the device.
	Build Time	Build time of image.
	Family	Image family.
	System Description	Image system description.
	Version	Version of the software image on the device.
	Description	Description of image.
	Processor Index	Processor index of image.
Interface	MTU	Maximum transmission unit. Maximum packet size, in bytes, that this interface can handle.
	Alias	Interface alias.
	Last Changed	Time of last change.
	Operational Status	Operational status of interface.
	Admin Status	Administrative status of interface.
	Speed (Mbps)	Speed of interface in Mbps.
	Type	Type of interface.
	Description	Description of interface.
	Name	Name of interface
	Physical Address	Physical address of interface.

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
	Index	Index of interface.
	Identifier	Identifier of interface.
	FlexLink Enabled	FlexLink status of the interface.
	SPAN Enabled	Whether the interface is Span enabled
Memory	Processor Index	Processor index.
	Total Memory (MB)	Total memory in MB.
Memory Pool	Lowest Free Block (MB)	Lowest free block of memory in MB.
	Largest Free Block (MB)	Largest free block of memory in MB.
	Free (MB)	Free memory in MB
	Used (MB)	Used memory in MB.
	Validity	Validity of memory pool.
	Alternate Pool	Alternate memory pool.
	Name	Name of the memory pool.
	Type	Memory pool type.

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Module	Parent Relative Position	Parent Relative Position of module.
	Field Replaceable Unit	FRU of module.
	Alias Name	Alias name of module.
	Reset Reason	Module reset reason.
	Admin Status	Administrative status of module
	Additional Status	Additional status of module
	Module IP Address	IP Address of module
	Hardware Encryption	Hardware encryption of module
	Slot Number	Slot number of module
	Inline Power Capable	Inline power capability of module
	Parent Type	Module parent type.
	Multiservice	Is this a multiservice module
	Parent Index	Parent index of module
	Number of Slots	Number of slots in module
	FW Version	Firmware version of module
	SW Version	Software version of module
	HW Version	Module hardware version.
	Operational Status	Operational status of module
	Manufacturer Name	Name of manufacturer of module
	Physical Entity Name	Physical entity name of module
	Slot Configuration	Slot configuration of module
	Model Name	Name of module.
	Vendor Type	Vendor type of the module.
	Serial Number	Serial number of module.
	Description	Description of module
	Component Type	Component type of module
	Index	Index of module

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Port	Manufacturer Name	Port manufacturer name.
	Slot Configuration	Slot configuration of port.
	Port Model Name	Model name of port.
	Port Vendor Type	Port vendor type.
	Port Serial Number	Serial number of port.
	Parent Relative Position	Parent Relative Position of port.
	Description	Description of port.
	Component Type	Port component type.
	Physical Entity Name	Physical Entity Name of port.
	Port Index	Port index.
	Field Replaceable Unit	FRU of port.
	Alias Name	Alias name of port.
	Status	Status of port
	Operational Status	Operational Status of port
	POE Admin Status	The POE Port Admin Status.
	POE Power Allocated	The amount of power allocated from the Power Sourcing Equipment (PSE) for the Powered device. This is a POE device specific attribute.
	POE Maximum Power	The maximum amount of power that the PSE makes available to the Powered device connected to the Port interface. This is a POE device specific attribute.
	Power Consumption (%)	Power consumption percentage of the port.
	Power Consumption	Power consumption of the port.
	Power Available	Power available for a powered device connected to the port.
	Power Remaining	Power remaining for a powered device connected to the port.
Port Interface	Number	Port interface number.

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Power Supply	Parent Relative Position	Parent Relative Position of power supply.
	Physical Entity Name	Physical Entity Name of power supply.
	Admin Status	Administrative status of power supply.
	Operational Status	Operational status of power supply.
	Manufacturer Name	Manufacturer Name of power supply.
	Field Replaceable Unit	FRU of power supply.
	Slot Configuration	Slot configuration of power supply.
	Alias Name	Alias name of power supply.
	Power Supply Model Name	Model name of power supply.
	Power Supply Vendor Type	Vendor type of power supply.
	Power Supply Serial Number	Serial number of power supply.
	Description	Description of power supply.
	Component Type	Component type of power supply.
	Index	Index of power supply.

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Processor	Field Replaceable Unit	Processor FRU.
	Alias Name	Alias name of processor.
	Slot Number	Slot number of processor.
	Parent Type	Parent type of processor.
	Parent Index	Parent index of processor.
	Reboot Config Register Value	Reboot configuration register value.
	Config Register Value	Configuration register value
	Physical Entity Name	Name of physical entity.
	NVRAM Used (KB)	Size of the processor NVRAM that has been utilized, in KB.
	NVRAM Size (KB)	Size of the processor NVRAM in KB.
	RAM Size (MB)	Size of processor RAM in MB.
	Operational Status	Operational status of processor.
	Manufacturer Name	Manufacturer name of processor.
	Slot Configuration	Slot configuration of processor.
	Model Name	Name of the processor model.
	Reset Reason	Processor reset reason.
	Vendor Type	Processor vendor type.
	Admin Status	Administrative status of processor.
	Serial Number	Serial number of processor.
	Additional Status	Additional status of processor.
	Description	Description of processor.
	Module IP Address	Module IP Address of processor.
	Component Type	Component type of processor.
	Hardware Encryption	Hardware encryption.
	Index	Index of processor.
	Inline Power Capable	Inline power capability of processor.
	Multiservice	Multiservice.
	Number of Slots	Number of slots in processor.
	FW Version	Firmware version of processor.
	SW Version	Software version of processor.
	HW Version	Hardware version of processor.
	Parent Relative Position	Parent Relative Position of processor.

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
Sensor	Parent Relative Position	Parent Relative Position of sensor.
	Physical Entity Name	Name of physical entity of sensor.
	Operational Status	Operational status of sensor
	Manufacturer Name	Manufacturer name of sensor
	Field Replaceable Unit	FRU of sensor
	Alias Name	Alias name of sensor
	Slot Configuration	Slot configuration of sensor
	Sensor Model Name	Model name of sensor
	Sensor Vendor Type	Vendor type of sensor
	Sensor Serial Number	Serial number of sensor
	Description	Description of sensor
	Component Type	Component type of sensor
	Index	Index of sensor
Slot	Serial Number	Serial number of slot.
	Description	Description of slot.
	Component Type	Component type of slot.
	Index	Index of slot.
	Parent Relative Position	Parent Relative Position of slot.
	Physical Entity Name	Physical Entity Name of slot.
	Operational Status	Operational Status of slot.
	Manufacturer Name	Name of manufacturer of slot.
	Field Replaceable Unit	FRU of slot.
	Slot Configuration	Configuration of slot.
	Alias Name	Alias name of slot.
	Model Name	Model name of slot.
	Vendor Type	Vendor type of slot.
Stack	Field Replaceable Unit	FRU of stack.
	Operational Status	Operational status of stack.
	Alias Name	Alias name of stack
	Manufacturer Name	Manufacturer name of stack
	Slot Configuration	Slot configuration of stack
	Stack Model Name	Model name of stack
	Stack Vendor Type	Vendor type of stack
	Stack Serial Number	Serial number of stack
	Description	Description of stack
	Parent Relative Position	Parent Relative Position of stack

Table 11-2 Inventory Change Filters (continued)

Report Inventory Group	Custom Report Group/Attribute	Description
	Component Type	Stack component type.
	Index	Index of stack.
	Physical Entity Name	Physical Entity Name of stack.
Sys Application	Index	Index of system application
	Software Serial Number	Software serial number of system application.
	Software Version	Software version of system application
	Software Product Name	Name of software product.
	Software Manufacturer	Software manufacturer of system application
System	SysUpTime	System Up Time.
	Host Name	Host name of the system
	Management Type	Management type of system.
	Modular	Modularity of system.
	OSI Layer Services	OSI layer services of system.
	System Name	System name.
	System Object ID	System Object ID of the device.
	Last Updated At	Date and time of last system update.
	Location	System location.
	Contact	System contact.
	Domain Name	Domain name of the system.
	Description	Description of the system.