



Device Configurations and Software Images

Cisco Prime Network Change and Configuration Management (CCM) provides tools for managing the software images and device configuration files used by the devices in your network.

CCM is also the launch point for the following Prime Network features:

- Transaction Manager, which is used to manage and execute activations on groups of devices. Information appears in the Transaction Manager tab only if transactions have been created outside of Prime Network and then added to Prime Network, as described in the [Cisco Prime Network 4.0 Customization Guide](#).
- Command Manager, which provides a repository of all commands available in the system. It can be used to create new commands and command sequences, which can then be applied to groups of devices. Command Manager is described in the [Cisco Prime Network 4.0 Customization Guide](#).

These topics provide an overview of the features that CCM provides, some initial setup tasks you must perform, and how to work with the GUI:

- [What is Change and Configuration Management?](#), page 4-1
- [Set Up Change and Configuration Management](#), page 4-3
- [Use the CCM Dashboard](#), page 4-10
- [Device Configurations](#), page 4-12
- [Software Images](#), page 4-26
- [Configuration Audit](#), page 4-45
- [Compliance Audit](#), page 4-51
- [Global Settings and Administration](#), page 4-61

For information on the devices supported by CCM, see [Cisco Prime Network 4.0 Supported Cisco VNEs](#).

What is Change and Configuration Management?

Cisco Prime Network Change and Configuration Management provides tools that allow you to manage the software and device configuration changes that are made to devices in your network. Device configuration management tools are provided by the Configuration Management (CM) function, and software image management tools are provided by the Image Management function. Operations can be performed on user-created groups of devices. For more information on user-defined device groups, see [Device Groups Setup Tasks](#), page 4-9.

Configuration Management

Configuration Management enables you to control and track changes that are made to a device configuration. It uses a change management feature to detect ongoing changes to devices in two ways:

- When doing periodic archiving of device configurations. If CM detects a change in a configuration file, it will get the new version of the file from the device and copy it to the archive.
- When a configuration change notification is received from a device. This is called event-triggered archiving. You can configure CM to copy a new version of a configuration file to the archive whenever a change is detected, or to queue the changes and then copy the files to the archive according to a schedule.

By default, neither of these methods are enabled. You can configure them from the Configuration Management Settings page (see [Configuration Management Setup Tasks, page 4-5](#)).

Change Logs provide information on the changes made to devices in the network, sorted by their time stamp. The Configuration Management Settings page controls how long these logs are saved. CM saves messages that can be used for debugging in `PRIME_NETWORK_HOME/XMP_Platform/logs/ConfigArchive.log`.



Note

All configuration management operations are performed only on devices with Communication State as Reachable and Investigation State as Operational, Partially Discovered, or Currently Unsynchronized. For a Cisco IOS device with SNMPv3 configuration, configuration management operations can be performed only if the device is configured with write permission for CISCO-CONFIG-COPY-MIB MIB group.

Compliance Audit (and Configuration Audit)

Compliance Audit ensures that existing device configurations comply to your deployment's policies. Using Compliance Audit, you can create policies that can contain multiple rules, and policies can be grouped together to create a policy profile which can be run on a set of devices, called audit of devices. There is no limit on the number of policies, profiles, rules, and conditions that you can create using Compliance Audit. It can scale up to 35,000 devices.

When a device is detected to be not confirming to a determined policy, Compliance Manager calls it a violation. Subsequently, if available, it also recommends a fix, as configured by the administrator. The violation details are saved in DB Schema for your reference later.

Compliance Audit replaces Configuration Audit (although Configuration Audit is still available.)

Image Management

Image Management provides tools for performing rapid, reliable software upgrades and automate the steps associated with upgrade planning and monitoring. This topic provides an overview of both features and an introduction to the Change and Configuration Management dashboard. Cisco IOS and Cisco IOS XR software images are stored in the Prime Network image repository, to which you can add new images by importing them from Cisco.com, from existing devices, from a local file system, or from an external image repository. Software images in the repository are stored in binary format. Before an image is distributed, NEIM performs an upgrade analysis to ensure that the network element is compatible with the image; after an image is distributed, the images are applied immediately. For Cisco IOS XR devices, you can add individual packages, deactivate packages, test changes before committing them, commit changes, and roll packages back to stored rollback points. The image repository is located in the Cisco Prime database. NEIM saves messages that can be used for debugging in `PRIME_NETWORK_HOME/XMP_Platform/logs/NEIM.log`.

**Note**

All image management operations are performed only on completely managed devices. (This means the Communication State of the device must be Reachable and Investigation State of the device must be Operational.)

**Note**

We recommend that you verify that an image operation is correct on a single device, preferably in a lab, prior to distributing and activating a change in image on multiple devices in a production network.

Set Up Change and Configuration Management

The following topics explain the setup tasks required for Change and Configuration Management:

- [Prime Network Setup Tasks, page 4-3](#)
- [Device Setup Tasks, page 4-4](#)
- [Configuration Management Setup Tasks, page 4-5](#)
- [NEIM Setup Tasks, page 4-7](#)
- [Device Groups Setup Tasks, page 4-9](#)

Prime Network Setup Tasks

Verify the following:

- You can control user access in two ways:
 - By requiring users to enter device credentials before they can execute a CCM operation
 - By allowing users to run CCM jobs only if they have been granted those privileges (controlled in their user account)

For information on enabling these features, see the information on global user settings in the [Cisco Prime Network 4.0 Administration Guide](#).

- Verify that CCM is installed. The installation process is described in the [Cisco Prime Network 4.0 Installation Guide](#). CCM can be installed using the `network-conf` command. The guide includes information about supported browsers, ports that must be available, and so forth.

To check if CCM is installed, log into the Prime Network gateway and enter the following command:

```
# cd $PRIME_NETWORK_HOME/Main
# dmctl status
```

If you see the following in the output, CCM is installed and running.

```
- Checking Prime Network Web Server Status [UP]
```

- Verify the port to be used. 8043 is the secure HTTP port enabled by default for Change and Configuration Management web client. However, you can still use port 8080 to launch the Change and Configuration Management GUI. To do so, you must manually enable it using this command:

```
# cd $NCCM_HOME/scripts/
# ./nccmHTTP.csh enable
# dmctl stop
# dmctl start
```

To disable port 8080, perform the same operation but use the disable argument.

- The SCP port being used by a device must match the SCP port configured in the device VNE (the VNE is Prime Network's model of the device). If a device is not using the default SCP port, be sure that the VNE is also configured with the correct port. You can change the VNE's SCP port from the Administration GUI client by editing the VNE properties (the Telnet/SSH tab). See the description of VNE properties in the [Cisco Prime Network 4.0 Administration Guide](#).
- If a gateway is behind a firewall, you must open special ports. You do not have to open special ports if units are located behind firewalls (and with NAT). This approach prevents issues when the unit is behind NAT, as the unit does not require a publicly available IP address for the gateway to contact it.
- SNMP read-write community in Cisco Prime Network Administration must match that on the devices. Make sure that pop-up windows are enabled on the Firefox and Internet Explorer browsers.
- For IPv6, CM and NEIM functions run smoothly on a combination of network and devices with IPv6 addresses. Either the device or the unit must be configured with an IPv6 address to work. For Cisco IOS devices with IPv6 address, the CM and NEIM operations will work only in FTP mode.
- For NEIM, verify that the gateway has sufficient space for the storing and staging directories (see [Change Image Management Global Settings, page 4-66](#)).
- For config and image transfers using TFTP, verify that the TFTP directory is set up and available in the Prime Network gateway and/or unit. To modify and verify the TFTP directory, run the following commands:

- To change the TFTP directory, go to the Prime Network directory and run the following commands in the Prime Network gateway:

```
./runRegTool.sh -gs 127.0.0.1 set <GW/Unit IP> avm83/services/tftp/read-dir tftp
dir name
```

```
./runRegTool.sh -gs 127.0.0.1 set <GW/Unit IP> avm83/services/tftp/write-dir tftp
dir name
```

- To check the TFTP directory, run the following commands:

```
./runRegTool.sh -gs 127.0.0.1 get <GW/Unit IP> avm83/services/tftp/read-dir
```

```
./runRegTool.sh -gs 127.0.0.1 get <GW/Unit IP> avm83/services/tftp/write-dir
```

- Restart AVM 83 in the gateway or the unit, by using the following command:

```
anactl -avm 83 restart
```

Device Setup Tasks

- Verify that the device is supported. See [Cisco Prime Network 4.0 Supported Cisco VNEs](#).
- For CM, verify that devices are configured to forward configuration change notifications to Prime Network. This is documented as a prerequisite to adding VNEs, in the [Cisco Prime Network 4.0 Administrator Guide](#). (Specifically, if you will be using event-triggered archiving, make sure the logging gateway-IP command is configured on all devices. This command should have been configured as a prerequisite to adding VNEs to Prime Network.)
- Simple Network Management Protocol (SNMP) read-write community must be configured on devices. For more information on configuring SNMP community strings for devices, see the [Cisco Prime Network 4.0 Administrator Guide](#). SNMP read-write community in Cisco Prime Network Administration must match that on the devices.

- Ensure reachability from Prime Network units to devices and vice versa.
- Make sure you have performed all of the device configuration prerequisites for adding VNEs. These commands are described in the [Cisco Prime Network 4.0 Administrator Guide](#).
- Change and Configuration Management supports FTP for all config and image transfers. Although you can configure a username and password using the **ip ftp** command, adding the unit's FTP credentials to the device may not be safe if the network is not secure. Before using FTP for Change and Configuration Management, we recommend that you:
 - Configure the network device to add the *Prime Network Unit User* credentials of the unit that manages the device. You need not add the super user credentials of the *Prime Network Unit Server* to the device configuration.
 - For Cisco Carrier Packet Transport (CPT) devices, add the *Prime Network Unit User* credentials to the registry. This is required because Prime Network initiates the FTP operation using a TL1 interface, and the TL1 commands require the username and password as input parameters. After you add this information to the registry, the credentials are automatically read when needed.


```
# $ANAHOME/Mail/runRegTool.sh -gs 127.0.0.1 setEncrypted 127.0.0.1
nccm-settings/ftpsettings/username ftp-username

# $ANAHOME/Mail/runRegTool.sh -gs 127.0.0.1 setEncrypted 127.0.0.1
nccm-settings/ftpsettings/password ftp-passwd
```
 - Restrict the FTP configuration such that the *Prime Network Unit User* has read-write access only to the \$PRIME_NETWORK_HOME/tftp directory and hence does not have access to unwanted files outside the home directory.



Note FTP support is not available for Cisco IOS XR devices and Cisco Nexus 5000 and Cisco Nexus 7000 series devices.

- For IPv6, CM and NEIM functions run smoothly on a combination of network and devices with IPv6 addresses. Either the device or the unit must be configured with an IPv6 address to work. For Cisco IOS devices with IPv6 address, the CM and NEIM operations will work only in FTP mode.

Configuration Management Setup Tasks



Note

In the Configuration Management and Image Management Settings pages, Change and Configuration Management does not support the following special characters:

- For Password fields—>, <, ', /, \, !, :, ;, and "
- For all other fields—`, ~, @, #, \$, %, ^, &, *, (,), +, =, |, {, }, [,], ', ?, >, <, /, \, !, :, ;, and "

The CM features are disabled by default so that you do not encounter unexpected processing loads on your server. The following steps explain what you must do to set up CM. All of these items are configured from the Configuration Management Settings page (**Configurations > Settings**). Many of these settings can be overridden when you create specific jobs.

1. Configure the transport protocol that Prime Network will use between the device and the gateway. these are controlled from the **Transport Protocol** area. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. To use FTP as the transfer protocol, you must install FTP on the gateway and the unit servers that manage the VNEs. Note the following:

**Caution**

FTP is not a secure mode of transfer. Use SCP/SFTP instead, for secure config and image transfers.

- The TFTP source interface on the devices must be able to reach the unit. Otherwise, the configuration management jobs that require TFTP may fail.
- To use SFTP/SCP for config transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS XR devices, you need to configure the device with K9 security (k9sec) enabled images such that the SSH server is up and running on the device.
- To use SCP as the protocol to retrieve configuration and image files, you must execute the following command on the device:

```
# ip scp server enable
```

2. Enable CM to perform an initial synchronization of the CM archive files with the configurations that are running on the network devices. Whenever the Prime Network gateway is restarted, CM will perform this synchronization. By default, synchronization is disabled. To enable it, activate **Enable Initial Config Syncup**.
3. Configure the policies that control how often CM retrieves information from devices and copies configuration files to the archive. By default, all of these settings are disabled. You must answer the following basic questions:

- a. How much disk space is available? Smaller space may require more frequent purging.
- b. Should new configuration files be copied (backed up) to the archive on a periodic basis or on an event-driven basis?

If configurations are changing frequently and the changes are not important to you, you should use periodic backups by selecting **Enable Period Config Backup**. This will minimize server workload.



Note The periodic setting is recommended.

If every change is considered significant, use event-driven backups (**Enable Event-Triggered Config Archive**).

- c. For event-driven archiving, should information be copied to the archive immediately upon receiving a change (**Sync archive on each configuration change**)? Or should changes be queued and then copied at a certain interval (**Sync archives with changed configurations every ___ hours and ___ minutes**)? If information needs to be copied to the archive immediately, you must sync the archive on each configuration change. Otherwise, you can sync the archive with changed configurations at a certain interval (every 1-24 hours).
4. Enable CM to perform periodic synchronization of out-of-sync devices by selecting **Enable Periodic Sync for Out of Sync Devices (24Hours)**.
5. Enable CM to export archived configuration to an export server on a periodic basis by selecting **Enable Periodic Config Export** and **Export Settings**. This allows you to free up disk space while keeping a permanent record of historical archives.
6. Configure when configuration files should be purged from the archive using the **Archive Purge Settings**. You should consider:
 - How big are the configuration files?

- How often are changes made to devices?
7. Specify the default mode of restoring configuration files to the devices using **Restore Mode**.
 8. Configure the SMTP server and e-mail IDs to send notifications on the status of configuration management jobs to users. (You can also specify e-mail settings when you create a job.)
 9. Specify the commands that you want CM to exclude when comparing files (for example, clock rates). A set of common exclude commands is provided by default (for example, ntp-clock-period). these are controlled in the **Exclude Commands** area (see [Notes on Exclude Commands, page 4-65](#)).

**Note**

Configuring exclude commands is especially important if you are using event-driven archiving. Doing so avoids unnecessary file backups to the archive.

NEIM Setup Tasks

**Note**

In the Configuration Management and Image Management Settings pages, Change and Configuration Management does not support the following special characters:

- For Password fields—>, <, ', /, \, !, :, ;, and "
- For all other fields—`, ~, @, #, \$, %, ^, &, *, (,), +, =, |, {, }, [,], ', ?, >, <, /, \, !, :, ;, and "

**Caution**

FTP is not a secure mode of transfer. Use SCP/SFTP instead, for secure config and image transfers.

The following are the NEIM prerequisites, all of which are controlled by the Image Management Settings page (**Images > Settings**). Many of these settings can be overridden when you create specific jobs.

1. Configure the transport protocol that Prime Network will use between the device and the gateway; these are controlled from the **Transport Protocol** area. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. To use FTP as the transfer protocol, you must install FTP on the gateway and the unit servers that manage the VNEs. Note the following:
 - The TFTP source interface on the devices must be able to reach the unit. Otherwise, the image management jobs that require TFTP may fail.
 - To use SFTP/SCP for image transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS XR devices, you need to configure the device with K9 security (k9sec) enabled images such that the SSH server is up and running on the device.
2. Configure the gateway staging directory to use when transferring images from Prime Network out to devices in the **File Locations** area. The default is `PRIME_NETWORK_HOME/NCCMComponents/NEIM/staging/`. `PRIME_NETWORK_HOME` is the Cisco Prime Network installation directory (by default, `/export/home/network-user`; where `network-user` is the operating system user for the Prime Network application and an example of `network-user` is `network39`).
3. In case of insufficient memory, use the **Clear Flash** option (under **Flash Properties**). This deletes any one file (other than the running image) and recovers the disk space occupied by the file. This procedure is repeated until adequate space is available in the selected flash.

4. Enable the warm upgrade facility to reduce the downtime of a device during planned Cisco IOS software upgrades or downgrades (in the **Warm Upgrade** area).
5. Configure the gateway storing directory to use when transferring images from an outside source into the image repository (from Cisco.com or from another file system). This is controlled from the **File Locations** area. The default is *PRIME_NETWORK_HOME/NCCMComponents/NEIM/images/*. *PRIME_NETWORK_HOME* is the Prime Network installation directory (by default, */export/home/network-user*; where *network-user* is the operating system user for the Prime Network application and an example of *network-user* is *network39*).
6. Configure the SMTP server and e-mail IDs to send notifications on the status of image management jobs to users. (You can also specify e-mail settings when you create a job.) This is controlled in the **E-mail Settings** area.
7. If you plan to download files from Cisco.com, configure the necessary vendor credentials to connect to Cisco.com. These are set in the **Vendor Credentials** area. If you do not have login privileges, follow the procedure in [Obtaining Cisco.com Login Privileges for Image Management](#), page 4-8.
8. Configure the proxy server details to use while importing images to the archive from Cisco.com (in the **Proxy Settings** field).
9. If you plan to download images from an external repository, set up the details of the external server to import images to the Prime Network image repository (in the **External Server Details** area).

Obtaining Cisco.com Login Privileges for Image Management

Login privileges are required for all Images operations that access Cisco.com. To get access, you must have a Cisco.com account. If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco website.

You can register by going to the following URL:

<http://tools.cisco.com/RPF/register/register.do>

To download cryptographic images from Cisco.com, you must have a Cisco.com account with cryptographic access.

To obtain the eligibility for downloading strong encryption software images:

-
- Step 1** Go to the following URL:
http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y&return_url=http://www.cisco.com
 - Step 2** Enter your Cisco.com username and password, and click **Log In**.
 - Step 3** Follow the instructions provided on the page and update the user details.
 - Step 4** Click **Accept** to submit the form.
 - Step 5** To verify whether you have obtained the eligibility to download encrypted software:
 - a. Go to the following URL:
http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y&return_url=http://www.cisco.com
 - b. Enter your username and password, and click **Log In**.
The following confirmation message is displayed:
You have been registered for download of Encrypted Software.
-

Device Groups Setup Tasks

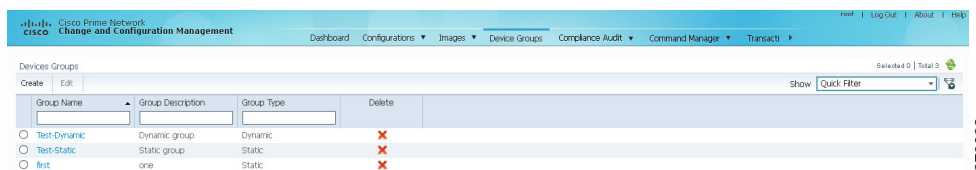
You can create user-defined device groups for ease of performing operations. A static group contains a specific set of devices; new devices must be added manually. A dynamic group is populated according to membership rules; if newly-added devices match the rules, they are automatically added to the group.

If you are backing up the configuration archive or importing software images from devices into the repository, and a device group changes during the operation, Prime Network updates the job accordingly such that all the devices available in the group at the time of execution of the job are considered for the backup or import operation. All other job types are not updated; you must delete and recreate the job.

To view the existing and create new user-defined device groups:

- Step 1** Click the **Device Groups** tab. The Device Groups page appears as shown in [Figure 4-1](#).

Figure 4-1 Device Groups Page



The Device Groups page displays the name, description, and whether the membership is static or dynamic. To delete a group, click the red X next to the group name.

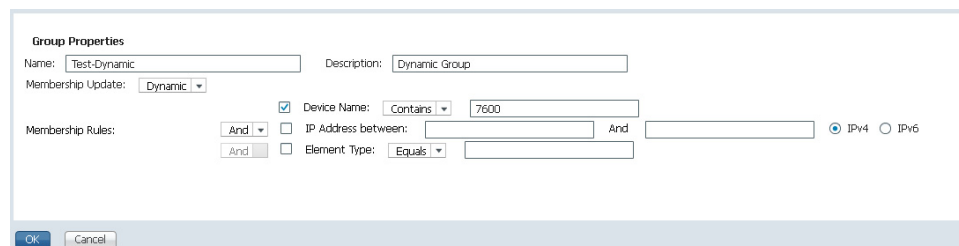
To view the devices in a group, click the hyperlinked group name to view the devices mapped to the group in the Group Members page. The device status, IP address and element type is listed. To display more properties, click the Device Name hyperlink. The status icons are illustrated in the following.

Symbol	Description
	Device is in operational state.
	Device is not in operational state. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device.

- Step 2** To create a new group, click **Create** and enter the required information. Names must be unique; do not use the reserved names **adminGroup** and **ROOT-DOMAIN**.

- Step 3** In the Membership Update drop-down list box, choose Static or Dynamic.

- For dynamic groups, set up a membership rule to indicate which devices must be added to the group. The following figure provides an example of the Create Device Group page for a dynamic group.



You can set up membership rules with parameters such as device name, range of device IP addresses, and the device element type. For example:

```
Device Name equals 1800
IP Address between 10.77.214.107 And 10.77.214.171 IPv4
Element Type equals Cisco 1801
```


Note

You can choose to include any one or a combination of these parameters in the rule by using the And/Or operator. Also, you can provide multiple values for the Device Name and Element Type parameters as a comma-separated list, if required.

- For static device groups, in the Group Members section, under the Available Devices list, Prime Network lists all the devices that are available in the database. The following figure provides an example of the Create Device Group page for a static group.

Group Properties

Name: Description:

Membership Update:

Membership Rules:

☐ Device Name:

☐ IP Address between: And ☐ IPv4 ☐ IPv6

☐ Element Type:

Group Members

Available Devices Selected 0 / Total 3

Status	Device Name	IP Address	Element Type
<input type="checkbox"/>	ASR500	10.77.214.70	Cisco ASR 5000 M...
<input type="checkbox"/>	GSRXR	10.76.92.188	Cisco 12406
<input checked="" type="checkbox"/>	Nexus7K	10.77.214.142	Cisco Nexus 7010...

Selected Devices Selected 0 / Total 1

Status	Device Name	IP Address	Element Type
<input checked="" type="checkbox"/>	ASR5500	10.96.66.35	Cisco ASR 5500

OK Cancel

Step 4 Click **OK** to save the group.

Use the CCM Dashboard

To launch the GUI from a web browser, enter the following URL in the address bar:

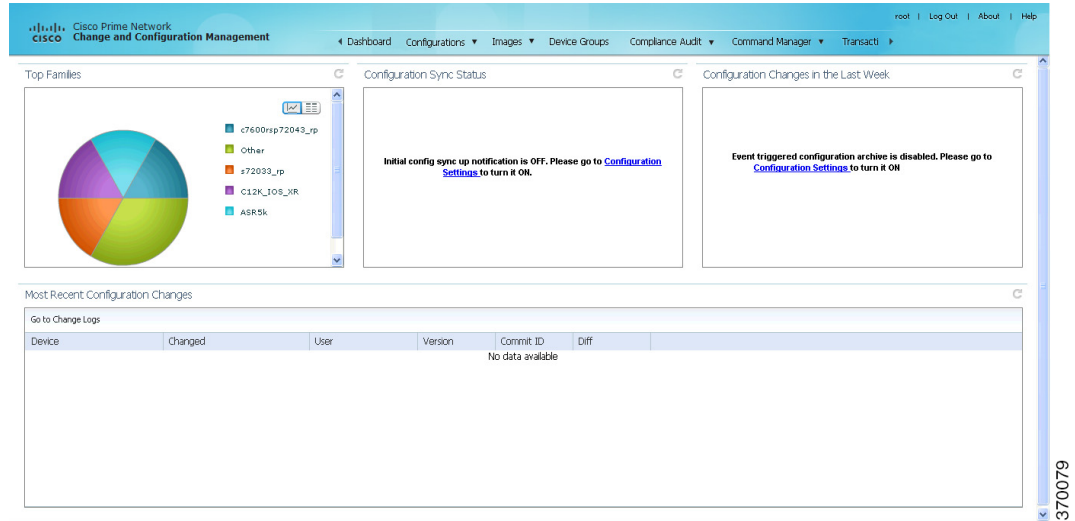
<https://gateway-IP:8043/ccmweb/ccm/login.htm>


Note

Change and Configuration Management does not support special characters for any of the editable fields in the GUI, including filters.



Figure 4-2 shows the CCM Dashboard, which contains four dashlets or subdivisions to display real-time information about the most frequently used software images, devices with startup and running configurations that are not in sync, and recent configuration changes.

Figure 4-2 CCM Dashboard



Dashlet	Provides information about:
Top Families	<p>Four device families with the highest number of devices in the network. Smaller groups can be viewed by toggling to the tabular form. From here, you can distribute and activate software images to a selected family.</p> <p>Note You may face resizing issues when you hover the cursor over this dashlet, if you have enabled the Right to Left (Hebrew) settings in your browser.</p>
Configuration Sync Status	<p>(Cisco IOS) Devices for which the startup and running device configurations are in sync or not in sync. Whenever a Cisco IOS configuration file is retrieved from a device and copied to the archive, Prime Network compares the latest version of the startup configuration with the latest version of the running configuration file. If there is a mismatch, Prime Network adds the device to the list of out-of-sync devices. The information is refreshed whenever you click the Dashboard.</p> <p>A “100% Unavailable” message is displayed when there are no Cisco IOS device images or if the initial configuration sync up setting is not enabled (controlled by the “Enable/Disable Initial config sync up on restart” setting on the Configuration Management Settings page).</p>
Configuration Changes in the Last Week	<p>Number of device configuration changes detected for each day of the previous week. This dashlet is empty when configuration change notification is not enabled (controlled by the “Enable/Disable Event-Triggered Config Archive” setting on the Configuration Management Settings page).</p>
Most Recent Configuration Changes	<p>Last five device configuration changes that were made to devices in the network. This dashlet is empty if configuration change notification is not enabled. It is controlled by the “Enable/Disable Event Triggered Config Archive” setting on the Configuration Management Settings page (see Change Configuration Management Global Settings, page 4-61).</p> <p>The Commit ID and Diff columns apply only to Cisco IOS XR devices. Other device types will display N/A in those columns.</p>

Use the following icons to toggle between different views in the Top Families, Configuration Sync Status, and Configuration Changes in the Last Week dashlets.

Icon	Description
	Displays the details in the form of a pie or bar chart. If you hover your mouse cursor over a section in the pie chart, a tooltip displays the information associated with that section.
	Displays the details in a tabular form.

Device Configurations

The following topics explain how to work with device configurations:

- [What is In the Archive?, page 4-12](#)
- [Protect Configurations in the Archive, page 4-13](#)
- [Find Out What is Different Between Configurations, page 4-14](#)
- [Copy a Configuration File to a Central Server, page 4-16](#)
- [Are Running and Startup Configs Mismatched? \(Cisco IOS and Cisco Nexus\), page 4-17](#)
- [Copy the Device Files to the Archive \(Backups\), page 4-18](#)
- [Fix a Live Device Configuration \(Restore\), page 4-22](#)
- [Clean Up the Archive, page 4-25](#)
- [Find Out What Changed on Live Devices, page 4-25](#)

What is In the Archive?

Choose **Tools > Change and Config Mgmnt** to open Change and Configuration Management.

Choose **Configurations > Archives** to view the contents of the archive. The CM archive maintains copies of device configuration files, storing them in the Prime Network database. Configuration files are stored in readable format, as received from the device. You can edit existing archive files and save for deployment at a later time. The edited archive files are available in the Edited Archive tab. The total number of archives available in the Prime Network database is also displayed in the header. The configuration, after deployment, can also be restored to the original state. Users can only see devices that are in their device scope. For enhanced security, you might be prompted to enter your device access credentials when you try viewing device details or when you try performing configuration changes on devices. This option is enabled if, from the **Prime Network Administration > Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**.

The Archived Configurations page displays the following information about each configuration file.

Protect Configurations in the Archive

Table 4-1 Configuration Information Displayed on Archived Configurations Page

Field	Description
Device Name	<p>Name of device. Click the icon next to the device name to open a popup that displays device properties. Additional information is listed depending on the device type:</p> <ul style="list-style-type: none"> Current active packages on the device—For Cisco IOS XR devices Active kickstart images—For Cisco Nexus series devices Priority list—For Cisco ASR 5000 series devices. The priority list displays various combinations of a configuration file and an image file in priority order for the device.
Version	<p>An internally-used number. A version will not have an associated configuration file under the following circumstances:</p> <ul style="list-style-type: none"> The associated configuration file was deleted from the archive. The associated configuration file has not yet been copied to the archive. (Prime Network supports queuing change notifications and copying the configuration files to the archive at a later time. See Change Image Management Global Settings, page 4-66.) <p>Click a version number hyperlink to launch the Device Configuration Viewer, from which you can view the contents of a configuration file.</p>
Type	<p>Type of configuration:</p> <ul style="list-style-type: none"> Cisco IOS and Cisco Nexus series devices—Running or Startup Cisco IOS XR devices—Running or Admin Cisco ASR 5000 series devices—Running or Boot. For boot configuration, the version is always displayed as 1. Cisco CPT devices—Startup
Vendor	Specifies the device vendor: Cisco or non-Cisco device.
Date Changed	<p>Date and time of last change, displayed accordingly to the local time zone settings of the client.</p> <p>For Cisco CPT and Cisco ASR 5000 series devices, this field displays N/A.</p>
Label	User-assigned archive labels.
Running Image	The software image currently running on the device.
Context / Module / Priority	<p>For Cisco Nexus series devices, this field displays the virtual device context (VDC) name.</p> <p>For Cisco 7600 series devices, this field displays the module name.</p> <p>For Cisco ASR 5000 series devices, this field displays the boot configuration files with their priorities.</p> <p>For other devices, this field displays N/A.</p>
Comments	User-assigned free text.
Commit Id	(Cisco IOS XR only) ID that identifies the last configuration change on the device (maximum number saved is 100).

Assigning labels to configuration files is a clear, simple way to identify important configurations and convey critical information. You can manage labels by choosing **Labels > Manage**.

- Adding a label adds it to the catalog where it is made available to all users. Add labels by clicking **Add Row**.
- Deleting a label unassigns the label from configurations that are using it. Likewise, if you edit a label, the change is applied to all configurations using the label.
- Unassigning a label does not delete the label from the catalog.
- Labels with the “do not purge” property will not be purged from the archive (the delete action is disabled). When calculating the total number of archives to see if the maximum has been reached and archives should be purged, CM does not include configurations with this label in the total (see [Change Configuration Management Global Settings, page 4-61](#)).

Editing an Archive Configuration

You can edit an existing device archive file and save the edited file. This edited archived file is stored in the Prime Network database, and the edited file can be deployed at any time. This can be viewed from the **Edited Archive** tab, in the Archive page. Every time you edit and save an existing file, a new version is added in the database, and is also listed in the Edited Archive page.

**Note**

The option to edit existing device archive file and save the edited file is not available for non-Cisco devices.

Edit archive files following the procedure below:

Step 1 From the **Archive** page, choose a configuration file, and click **Edit**.

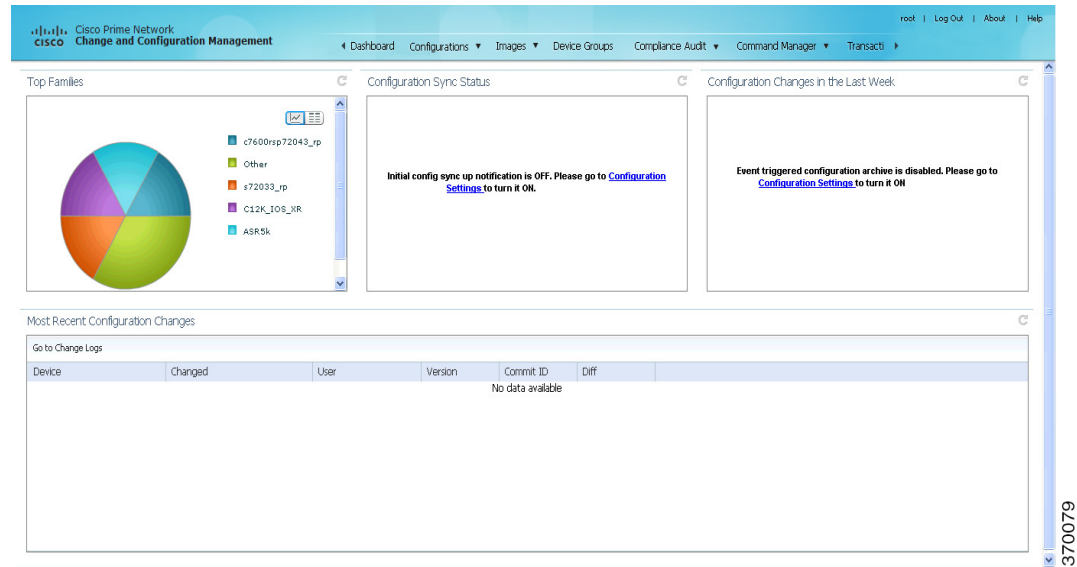
Step 2 Edit and save the configuration file.

An edited archive version is created. This edited version will belong to the same configuration type as that of the original archive file.

The edited archive files can be restored to the devices.

Find Out What is Different Between Configurations

Prime Network allows you to compare two configuration files that are saved in the archive and display them side by side, highlighting configuration differences and allowing you to move between them. Prime Network excludes a small set of commands by default, such as the NTP clock rate (which constantly changes on a managed network element but is not considered a configuration change). You can change the excluded commands list as described in [Change Configuration Management Global Settings, page 4-61](#). Additions, deletions, and excluded values are color-coded as shown in the following example.

Figure 4-3 Compare Configurations Dialog Box

You can compare any types of configurations as long as they run on the same operating system. However, you cannot compare a Cisco IOS configuration with Cisco IOS XR configuration.

The following are typical scenarios for using the compare function:

- Compare the latest and next-to-latest configuration to see the most recent change.
- Compare Cisco IOS running and startup configurations to see how they are out of sync.
- Compare the configurations on two different devices to find out how they are different.
- Compare the configurations after eliminating excluded lines from comparison.

**Note**

When you are trying to compare an archive with an active startup, running, or admin configuration, if there is a change in the device configuration, Prime Network initiates a backup job and creates a latest version of the device configuration file. You can view the latest version of the configuration file in the Archived Configurations page.

To compare configurations:

- Step 1** Choose **Configurations > Archives**.
- Step 2** Locate the archives you want to compare. You can click the Version hyperlink next to a device to open the Device Configuration Viewer and quickly view the contents of the configuration file.

Step 3 You can choose to do the following:

Device Type or OS	Supported Function
For Cisco IOS XR devices	Compare > To Active Running or Compare > To Active Admin
Cisco IOS device	Compare > To Active Startup or Compare > To Active Running
Cisco ASR 5000 series device	Compare > To Active Boot or Compare > To Active Running
All	Compare > Selected Archives

Copy a Configuration File to a Central Server

You can export configurations to an FTP or SFTP server that is specified on the Configuration Management Settings page. They are exported as a .cfg (configuration) file.

Configuration files are saved using the following format:

deviceName-configurationType-version-configChangeTimestamp.cfg

For example, the following file would contain the 18th version of a running configuration for the device named 7200-5, saved on March 27, 2010 at 2:40:30 P.M.:

7200-5-RUNNING_CONFIG-18-2010327144030.cfg



Note

Export of configuration files of IPv6 devices to servers running Windows OS is not supported.

Before You Begin

Make sure of the following:

- Export location and required credentials, and (for emails) SMTP host and port are configured on the Configuration Management Settings page.
- Specified FTP or SFTP server must have sufficient free space to accommodate the exported configurations. Also, the destination subdirectory on the FTP or SFTP server must have the required permissions.

To export configuration files:

Step 1 Choose **Configurations > Archives** and locate the archives you want to export. You can click the Version hyperlink next to a device to open the Device Configuration Viewer and quickly view the contents of the configuration file.

Step 2 Click **Export** and set the desired schedule and enter the e-mail ID(s) to which to send a notification after the scheduled export job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Configuration Management Settings page.



Note

The time you specify here to schedule the export job is the server time.

- Step 3** Click **Export**. The export job is created and you are redirected to the Job Manager page, where you can monitor the status of the job.
-

Are Running and Startup Configs Mismatched? (Cisco IOS and Cisco Nexus)

Cisco IOS and Cisco Nexus series devices contain a startup and running configuration file. The startup configuration is loaded when a device is restarted. Ongoing changes to the device are applied to the running configuration. As a result, unless the running configuration is saved as the startup configuration, upon a device restart, any changes would be lost. It is therefore important to ensure that the device startup and running configurations are in sync. When Prime Network synchronizes a file, it overwrites the startup configuration on the device with the configuration that is currently running on the device.

Whenever a configuration file is retrieved from a device and copied to the archive (that is, backed up), Prime Network compares the latest version of the startup configuration with the latest version of the running configuration file. If there is a mismatch, Prime Network adds the device to the list of out-of-sync devices.

For Cisco Nexus series devices, CM backs up the startup and running configurations for all VDCs configured in the device. If there is a mismatch between the startup and running configurations of a VDC, CM creates an out-of-sync entry for that VDC.



Note

The synchronize operation affects only the configurations running on the device. It does not affect any configuration files that are saved in the archive. Configuration sync is not applicable for Cisco CPT and Cisco ASR 5000 series devices.

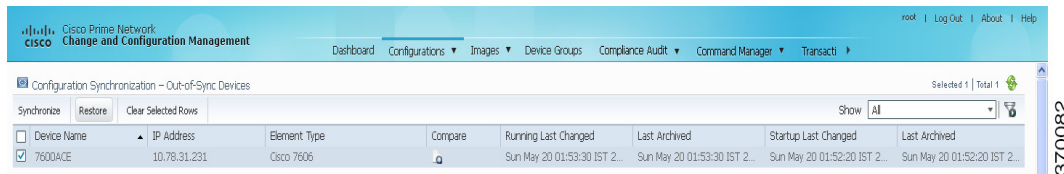
The Dashboard maintains a Configuration Sync Status pie chart that shows how many devices have out-of-sync startup and running configuration files. When you click the pie chart (or choose **Configurations > Synchronize**), you are directed to the Out of Sync Devices page, where Prime Network lists all of the out-of-sync devices in tabular format. The information is refreshed whenever you choose **Configurations > Synchronize**.

Before You Begin

Make sure the specified FTP or SFTP server must have sufficient free space to accommodate the exported configurations. Also, the destination subdirectory on the FTP or SFTP server must have the required permissions.

To view differences and synchronize configurations:

- Step 1** Choose **Configurations > Synchronize**. Prime Network lists all out-of-sync devices, the date and time when the device configurations were last changed, and when the files were last archived. [Figure 4-4](#) provides an example. The date and time are displayed according to the local time zone settings of the client.

Figure 4-4 Configuration Synchronization - Out of Sync Devices Page

- Step 2** Click the **Compare** icon to launch the Compare Configuration window, which provides a side-by-side view of the two configurations and highlights the differences.
- Step 3** Choose the network elements you want to synchronize. This directs Prime Network to overwrite the startup configuration on the device with the configuration that is currently running.
- Step 4** Click **Synchronize**. The Schedule Synchronization page opens.
- Step 5** Set the desired schedule and enter the e-mail ID(s) to which to send a notification after the scheduled synchronization job is complete. For two or more users, enter a comma-separated list of e-mail IDs. The time you specify here to schedule the synchronization job is the server time.

**Note**

You might be prompted to enter your device access credentials. This option is enabled if, from the **Prime Network Administration > Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure restrict access to devices.

- Step 6** Click **Synchronize**. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

Copy the Device Files to the Archive (Backups)

These topics describe how to automatically and manually back up configuration files to the archive:

- [Automatic Backups and Manual Backups](#)
- [Manually Backing Up Configuration Files](#)

Backing up a device configuration entails getting a copy of the configuration file from the device, and copying that file to the configuration archive. As part of the backup procedures, it is compared with the latest archived version of the same type (e.g. running with running, startup with startup). A new version of the file is archived only if the two files are different. If the number of archived versions exceeds the maximum, the oldest archive is purged (according to the values on the Configuration Management Settings page). Configurations marked with a “do not purge” label are not removed from the archive by the auto-purging procedures.

The backup procedure is also when Prime Network identifies out-of-sync devices.

The backup operation includes:

- Cisco IOS XR devices: Includes active packages. CCM does not back up running configurations for Cisco IOS XR devices that are managed with non-system user credentials; because copy command is not available in the command-line interface (CLI) for non-system users.

- Cisco Nexus series devices: Startup and running configurations for all VDCs configured in the device.
- Cisco 7600 series devices with an ACE card: Startup and running configurations of the ACE card.
- Cisco ASR 5000 series devices: Boot configuration file (Prime Network always overwrites the existing boot configuration in the archive)

Automatic Backups and Manual Backups

Table 4-2 describes the methods you can use to back up configuration files to the archive. None of these methods are enabled by default. Choose the method that is appropriate to your network and how often changes are made to it. For more information, see [Configuration Management Setup Tasks, page 4-5](#).



Note

While scheduling automatic backup operations, you might be prompted to enter your device access credentials. The device credentials are taken from the Configuration Settings. This option is enabled if, from the **Prime Network Administration > Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure restrict access to devices.

Table 4-2 **Methods for Archiving Configuration Files**

Method	Description
Initial Sync	Activates CM to perform an initial synchronization of the CM archive files with the configurations that are running on the network devices. If this setting is enabled, whenever the Prime Network gateway is restarted, CM performs this synchronization. This behavior is controlled by the Enable Initial Config sync up setting on the Configuration Management Settings page. See Change Image Management Global Settings, page 4-66 .
Manual	<p>A user-driven backup that is controlled from the Configurations > Backup page. Performing a backup from the Backup page overrides all other archive settings. You can schedule the file backup to occur immediately or according to a schedule.</p> <p>Note Any backups scheduled using this method are completely independent of any schedules for ongoing archiving. However, users can only back up devices that are within their scope, and if they have a sufficient device scope-based role.</p> <p>See Manually Backing Up Configuration Files, page 4-20.</p>



Table 4-2 Methods for Archiving Configuration Files (continued)

Method	Description
Ongoing	<ul style="list-style-type: none"> Event-Driven—Backs up device files when Prime Network receives a configuration change notification. Use this method if you consider every configuration file change to be significant. This is controlled by the Enable Event-triggered Config Archive setting on the Configuration Management Settings page. <p>For this form of backup, you can choose one of the following methods for performing the archiving:</p> <ul style="list-style-type: none"> Back up the files to the archive immediately when a change is detected. Queue the changes and back up the files to the archive according to a schedule. <p>Both of these settings are controlled from the Configuration Management Settings page.</p> <p>If you are using event-driven archiving, you should also make sure that exclude commands are properly configured. Exclude commands are commands that Prime Network ignores when comparing configurations, and they are controlled from the Settings page. Using this mechanism eliminates unnecessary file backups to the archive.</p> <ul style="list-style-type: none"> Periodic—Archives device files every 72 hours and this is configurable. A new archive is created only if the newly-collected device configuration is different from the last version in the archive. Use this method if configurations change frequently and the changes are not important to you. This setting is controlled by the Enable Periodic Config Backup setting on the Configuration Management Settings page. <p>Note This CM collection is independent of the Prime Network inventory collection.</p> <p>See Change Configuration Management Global Settings, page 4-61.</p>

Manually Backing Up Configuration Files

Files are automatically backed up to the archive according to the values on the Configuration Management Settings page. To perform an on-demand backup of configuration files to the archive:

- Step 1** Choose **Configurations > Backup**. Prime Network lists all devices with the following status symbols as shown in [Figure 4-5](#).

Symbol	Description
	Device is available for backup.
	Device is not available for backup. The device is most likely in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device.

- Step 2** Choose the devices with files you want to back up.

Figure 4-5 Configuration Backup Page

Status	Device Name	IP Address	Vendor Name	Element Type
<input checked="" type="checkbox"/>	10.66.163.166	10.66.163.166	Cisco	Cisco Catalyst 6500 VSS
<input checked="" type="checkbox"/>	3750	10.77.210.183	Cisco	Cisco Catalyst 3750
<input checked="" type="checkbox"/>	9003	10.104.120.178	Cisco	Cisco ASR 9003
<input checked="" type="checkbox"/>	ASR9000	10.56.59.142	Cisco	Cisco ASR 9006
<input checked="" type="checkbox"/>	ASR9K	10.104.120.198	Cisco	Cisco ASR 9006
<input checked="" type="checkbox"/>	CRS	10.104.120.80	Cisco	CISCO CRS980
<input checked="" type="checkbox"/>	Juniper	10.77.240.131	Juniper Networks	Juniper M10
<input checked="" type="checkbox"/>	asr5k	10.77.214.10	Cisco	Cisco ASR 5000 Mobile-Gate...
<input checked="" type="checkbox"/>	cat6500	10.76.92.129	Cisco	Cisco Catalyst 6509
<input checked="" type="checkbox"/>	gms	10.104.120.189	Cisco	Cisco 12406
<input checked="" type="checkbox"/>	gms	10.104.120.198	Cisco	Cisco 12406
<input checked="" type="checkbox"/>	n7	172.25.125.109	Cisco	Cisco Nexus 7009 Switch
<input checked="" type="checkbox"/>	smt	10.104.120.62	Cisco	Cisco ASR 901

- Step 3** To choose devices from a specific device group, click **Select Groups**. Click the hyperlinked device group name to view the list of devices that belong to the group.
- Step 4** Select the required device group in the Device Groups page and click **OK**. The devices that belong to the selected device group are highlighted in the Configuration Backup page. You can also schedule a backup simultaneously for all the devices existing in a group:
- Select a device group and click **Backup Groups**.
 - Enter the scheduling information as explained after [Step 5](#) and click **Backup Groups**.
- Step 5** In the Configuration Backup page, click **Backup** to configure the backup schedule. By default, the backup is performed as soon as possible. Other schedule choices (once, periodically, weekly, and so forth) are activated when you deselect Start as Soon as Possible. The time you specify here to schedule the synchronization job is the server time.

**Note**

You might be prompted to enter your device access credentials. This option is enabled if, from the **Prime Network Administration > Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure restrict access to devices.

- Step 6** Enter the e-mail ID(s) to which to send a notification after the schedule backup job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Configuration Management Settings page.
- Step 7** Click **Backup**. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

**Note**

If a backup is scheduled for an entire device group and if there is a change in the group by addition or deletion of devices after job creation, Prime Network updates the job accordingly such that all the devices available in the group at the time of execution of the job are considered for backup.

Fix a Live Device Configuration (Restore)

CCM performs the configuration restore operation in either *overwrite* or *merge* mode, as described in the following. As part of restore operation, the configuration files are backed up again after the restore procedure is complete.

- **Overwrite mode**—CCM overwrites the existing configuration on the device with a configuration file from the archive. After the restore operation is performed, the device configuration is identical to the configuration that was chosen from the archive.

The following devices support overwrite mode:

- Cisco Catalyst 3550 Series Switches
- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3750 Series Switches
- Cisco Catalyst 6500 Series Switches (IOS)
- Cisco 800 Series Routers
- Cisco 1800 Series Routers
- Cisco 1700 Series Routers
- Cisco 2600 Series Multiservice Platform Routers
- Cisco 2800 Series Integrated Services Routers
- Cisco 3700 Series Multiservice Access Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco 7200 Series Routers
- Cisco 7600 Series Routers
- Cisco 10000 Series Routers
- Cisco 12000 Series Routers (IOS)
- Cisco ASR 901 Series Routers
- Cisco ASR 903 Series Routers
- Cisco MWR 2941 Router

For Cisco IOS XR devices, the restore operation rolls back the configuration file to a commit ID associated with the selected archived configuration. If no commit ID is associated with the selected archived version, the restore will fail.

For all other devices supported by CCM, restore operations in overwrite mode is *not* supported.

- **Merge mode**—CCM merges the selected configuration file from the archive with the configuration on the device. New commands in the archived version—that is, commands that are *not* in the device's current configuration—are pushed to the device. After the restore operation, the device configuration file retains its original commands, but it also contains new commands from the archived version.

**Note**

The restore operation is not applicable to boot configuration files on Cisco ASR 5000 series devices.

By default, Prime Network uses the restore mode setting (overwrite or merge) that is specified in the Configuration Management Settings page (see [Change Configuration Management Global Settings, page 4-61](#)). However, you can modify the default mode while scheduling the restore operation. If you have selected the overwrite mode, you can use the **Use Merge on Failure** option to restore the files in merge mode, if overwrite mode fails.

If you select the devices by checking the check box next to Devices (in the table headline), only the first 100 devices in the first page are selected. Click Next to move to the next 100 devices. If you filter the devices based on a parameter, only the filtered details are displayed, and by default, no row is selected.

If you selected all the entries in a page, and then deselected one or few options from the selection, and then move to the subsequent pages to select all the devices from the Devices (in the table headline), the selection in the previous page disappears.

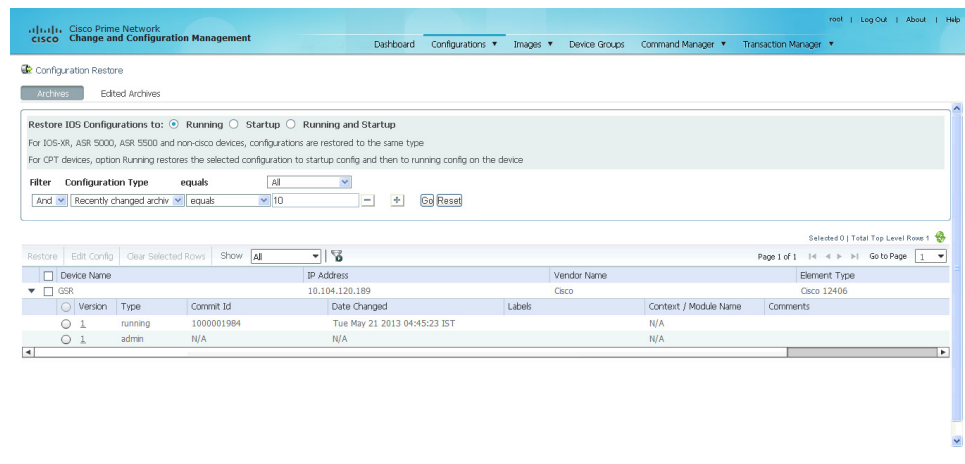
Before You Begin

- Make sure you have installed Flash Player version 10 or higher to view the Configuration Restore page.
- Make sure you have the permissions to perform the restore operation. You will not be allowed to schedule a restore job, if you do not have permissions.

To restore a configuration:

- Step 1** Choose **Configurations > Restore**. Prime Network lists all configuration files in the archive. [Figure 4-6](#) shows an example of a filtered page.

Figure 4-6 Configuration Restore Page



- Step 2** (Cisco IOS only) Specify the type of configuration files you want to restore: Running, Startup, or both. If you choose to restore to startup configuration, Prime Network will first copy the file to running configuration and then to startup configuration.



Note Cisco IOS XR, Cisco ASR 5000 series, and non-Cisco device configuration files are always restored to the same type. For Cisco CPT devices, the Running option restores the selected configuration to startup config and then to running config on the device.

- Step 3** Choose the configuration files you want to restore. You can click the arrow mark next to the device name to view the different versions of the configuration file of the device. You can also click the Version hyperlink to view the contents of a file. If the file is a binary file, clicking the version hyperlink does not open the various versions of the configuration file.

If you prefer to restore an edited archive file, open the Edited Archive tab. Select the files and click **Next**. The list of devices that belong to the same device family with respect to the selected edited configuration is displayed. Select the required devices. Skip to [Step 5](#).

**Note**

Edited files are restored only in merge mode. If you are restoring to startup mode on the devices ASR 901, ASR 903, and MWR2941, the restore procedure is performed on overwrite mode.

- Step 4** If you want to edit a file before restoring it, click **Edit Config** (edited files are restored only in merge mode). You can view the details of the selected configuration file in the Configuration Editor page as shown in [Figure 4-7](#).

**Note**

If you selected non-Cisco devices, the **Edit Config** button is disabled.

Figure 4-7 Configuration Edit



Edit the configuration lines, as required. Note the following:

- To remove a command, add **no** in front of the command.
- To update a command, add **no** in front of the command and then add the new command.

- Step 5** Click **Restore**. The Config Restore Schedule dialog box opens.
- Step 6** (Optional) Override the default transport protocol and default restore mode.
- Step 7** Enter a comma-separated list of e-mail ID(s) to which to send a notification after the scheduled restore job is complete.

**Note**

You might be prompted to enter your device access credentials. This option is enabled if, from the **Prime Network Administration > Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure to restrict access to devices.

- Step 8** Click **Restore**. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

Clean Up the Archive

Deleting a file removes it from the archive. You cannot delete an archived file if:

- It is marked “do not purge.”
- Deleting it would bring the number of versions below the minimum number of versions that must be retained (as specified on the Configuration Management Settings page).

When a device is removed from Prime Network, its configuration files are also removed from the archive.

To delete a configuration file from the archive:

- Step 1** Choose **Configurations > Archives**.
- Step 2** Choose the configuration file you want to delete. You can click the Version hyperlink to verify the contents of the configuration file.
- Step 3** To delete a single configuration file, click the delete icon (red **X**) at the end of the row. If the delete icon is disabled, this means the archive is assigned a label that is marked “do not purge.” To delete this type of configuration, you must first unassign the label from the configuration.
- Step 4** To delete multiple configuration files, select the required files and then click the **Delete** button in the table header.
- Step 5** Confirm your choice. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.

Find Out What Changed on Live Devices

The Change Logs page displays a list of the latest device configuration changes detected by Prime Network. How Prime Network responds to these changes depends on the values on the Configuration Management Settings page. By default, Prime Network does not get new information from the device and copy it to the archive when a change occurs, but you can set it to do so. See [Change Configuration Management Global Settings](#), page 4-61.

All users can view the change logs, regardless of the user access role or assigned device scopes. To view the latest changes, choose **Configurations > Change Logs**. [Figure 4-8](#) provides an example.

Figure 4-8 Configuration Change Logs

Device Name	Changed	User	Version	Commit ID	Diff	Compare
3400-5	Fri Mar 16 11:47:25 IST 2012	console	5	N/A	N/A	Compare
3400-5	Fri Mar 16 11:47:32 IST 2012	console	5	N/A	N/A	Compare
3400-5	Fri Mar 16 14:44:04 IST 2012	console	5	N/A	N/A	Compare
3400-5	Fri Mar 16 14:44:07 IST 2012	console	5	N/A	N/A	Compare
GSRXR	Fri Mar 30 00:57:24 IST 2012	cisco	2	1000001146	II IOS XR Configuration 4.2	Compare
3400-5	Fri Mar 30 13:44:35 IST 2012	vti1	5	N/A	N/A	Compare
3400-5	Fri Mar 9 13:32:47 IST 2012	vti1	4	N/A	N/A	Compare
GSRXR	Mon Apr 2 00:27:16 IST 2012	cisco	3	1000001147	II IOS XR Configuration 4.2	Compare
GSRXR	Mon Apr 2 00:29:54 IST 2012	cisco	3	1000001148	II IOS XR Configuration 4.2	Compare
GSRXR	Mon Apr 2 00:35:49 IST 2012	cisco	3	1000001149	II IOS XR Configuration 4.2	Compare
3400-5	Mon Apr 2 14:08:14 IST 2012	console	5	N/A	N/A	Compare
3400-5	Mon Apr 2 14:08:19 IST 2012	console	5	N/A	N/A	Compare
3400-5	Mon Apr 2 14:16:29 IST 2012	console	5	N/A	N/A	Compare
3400-5	Mon Apr 2 14:16:29 IST 2012	console	5	N/A	N/A	Compare
3750me-6	Mon Apr 9 12:19:15 IST 2012	prime	3	N/A	N/A	Compare
3750me-6	Mon Apr 9 12:19:24 IST 2012	prime	3	N/A	N/A	Compare
GSRXR	Mon Mar 26 01:02:05 IST 2012	cisco	2	1000001144	II IOS XR Configuration 4.2	Compare
GSRXR	Mon Mar 26 01:02:46 IST 2012	cisco	2	1000001145	II IOS XR Configuration 4.2	Compare
GSRXR	Sun Mar 25 20:30:32 IST 2012	cisco	2	1000001142	II IOS XR Configuration 4.2	Compare
GSRXR	Sun Mar 25 20:30:47 IST 2012	cisco	2	1000001143	II IOS XR Configuration 4.2	Compare
3400-5	Thu Mar 15 14:16:17 IST 2012	console	5	N/A	N/A	Compare

The Configuration Change Logs page displays change information, sorted according to the latest time stamp. (For a description of common fields, see [Device Configurations, page 4-12](#).) The date and time stamps are displayed according to the local time zone settings of the client. These fields are specific to the Configuration Change Logs page:

Field	Description
Diff	(Cisco IOS XR only) Displays only the commands that were changed. For long text, hover the cursor over the hyperlink to display the entire contents.
Compare	<p>Launches the Compare Configuration window, which displays the entire original and changed files side by side. This data is generated only if file versions are available.</p> <p>Additions and deletions are color-coded. From here, you can:</p> <ul style="list-style-type: none"> Click Show All Lines or Only Differences to display the entire file contents or just the differences between the two files. Click Previous Diff or Next Diff to jump forward or backward to the previous or next difference between the two files. Click the arrow buttons or enter the page number to jump forward or backward to view the file contents that are running across pages. Click Differences Without Excluded Lines to eliminate excluded lines from comparison.

Software Images

The following topics explain how to work with software images and packages:

- [Add New Images to the Repository, page 4-27](#)
- [New Devices: Create an Image Baseline, page 4-28](#)
- [Distribute Images and Make Sure They Will Work, page 4-29](#)
- [Activate Cisco IOS Software Images, page 4-34](#)
- [Perform Cisco IOS XR Software Package Operations, page 4-37](#)

- [Clean Up the Repository, page 4-44](#)

Add New Images to the Repository

Images are copied to the storing directory specified on the Image Management Settings page. Prime Network verifies whether the file contents are different from the previous version in the repository. If there are no differences, the image is not added to the repository. By default, the storing directory is `PRIME_NETWORK_HOME/NCCMComponents/NEIM/images/`, where `PRIME_NETWORK_HOME` is the Prime Network installation directory (by default, `/export/home/network-user`; where *network-user* is the operating system user for the Prime Network application and an example of *network-user* is `network310`). From there, they are imported into the repository.



Note

Before importing images, make sure internet connectivity is available to the server; otherwise, the imported images will not be populated with RAM, boot ROM, and feature set.

When you download an image from Cisco.com, Prime Network creates a job for the download. The job information is saved, along with other job information, in the database.

To import images into the Prime Network image repository:

Step 1 Choose **Images > Repository**.

Step 2 Choose the appropriate method:

To import from:	Choose:	Notes
Cisco.com web site	From Cisco.com	Make sure the Cisco.com credentials are set on the Image Management Settings page. You must enter a device type, software version, and feature set.
Another IPv4 or IPv6 gateway server	From External Repository	The GUI will display available images, their size, and whether they already exist in the repository.
A file system on the local gateway server	From File System	Change and Configuration Management displays all images or packages (bin, pie, smu, and so on) from the directory specified in the Image Management Settings page, and also from its sub directory in order to support tar files.

Step 3 Select the images and import them. Change and Configuration Management redirects you to the Jobs page, where you can monitor the status of the import job.

Step 4 Choose **Images > Repository** again to refresh the list of images.

Step 5 If a field displays NA, the image attributes were not available from the image header. (If pre-existing filters are still in use, you may need to click **Clear Filter**.) We recommend that you manually enter the information to ensure the accuracy of the upgrade analysis.

Step 6 Delete files from the storing directory (if applicable) to free space for future imports.

After the import, you can also add informational text to the Comments field. Normally at this point you will distribute the images; see [Distribute Images and Make Sure They Will Work, page 4-29](#).

New Devices: Create an Image Baseline

Use this method to create an image baseline—that is, import software images directly from existing devices to the Prime Network image repository. This is useful when you add devices from a new device series or family. This information is imported:

- Cisco IOS devices: Currently-running images. For Cisco 7600 series devices with ACE cards: ACE card images in the Cisco 7600 supervisor module filesystem (FTP, TFTP, and SCP are all supported).
- Cisco IOS XR devices: .pie and .vm files corresponding to active packages.



Note

Image baseline is not applicable for Cisco CPT devices.

To import images from devices into the Prime Network image repository:

Step 1 Choose **Images > Repository**.

Step 2 From the Import drop-down list, choose **From Devices**. The Devices dialog box displays information about the device. For long texts in the **Element Type**, **Software Version**, and **Running Image** fields, hover the cursor over the hyperlink to display the entire contents.

Step 3 To import images from devices of a specific group, click **Select Groups**. Click the hyperlinked device group name to view the list of devices that belong to the group. See [Device Groups Setup Tasks, page 4-9](#) for more information on user-defined device grouping.

Step 4 Select the required device group in the Device Groups page and click **OK**.

The devices that belong to the selected device group are highlighted in the Devices page. You can also import all the devices existing in a group. To do so:

- Select a device group and click **Import from Group**.
- Enter the scheduling information as explained after [Step 5](#) and click **Import from Group**.

Step 5 In the Devices page, click **Import**. A scheduler popup window appears.



Note

You might be prompted to enter your device access credentials. This option is enabled if, from the **Prime Network Administration > Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure to restrict access to devices.

Step 6 Enter the scheduling information. By default, jobs are scheduled to run as soon as possible.



Note

The time you specify here to schedule the import job is the server time.

Step 7 If you do not want to use the default transfer protocol, select a different protocol:

- TFTP (unsecured; Cisco ASR 5000 series devices use this protocol for importing images)
- SFTP/SCP (secured; Cisco IOS XR devices and Cisco Nexus 5000 and 7000 series devices use SFTP, and Cisco IOS devices use SCP)
- FTP (unsecured)

- Step 8** If you have selected two or more devices, click one of the following to specify the operation mode:
- **Parallel Order**—Imports images from all devices at the same time.
 - **Sequential Order**—Allows you to specify the order of the devices to import the images from. You can do so by moving the devices up and down in the Device Order box.



Note The Device Order box will not be available, if the number of devices is more than 300. Prime Network sequences the devices based on the default order (that you used while selecting the devices.)

- Step 9** Enter the e-mail ID(s) to which to send a notification after the import job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.



Note Before you enter the e-mail ID(s), ensure that you have set up the SMTP host and SMTP port in the Image Management Settings page (see [Change Image Management Global Settings, page 4-66](#)). The e-mail ID(s) configured in the Image Management Settings page, if any, will be displayed by default. You can modify the e-mail ID(s) if required.

- Step 10** Click **Import**. Prime Network redirects you to the Jobs page, where you can monitor the status of the import job.



Note If you chose to import all devices from a group and if there is a change in the group by addition or deletion of devices after job creation, Prime Network updates the job accordingly such that all the devices available in the group at the time of execution of the job are considered.

- Step 11** Choose **Images > Repository** again to refresh the list of images. If any of the image information could not be retrieved, the field will display NA. (If pre-existing filters are still in use, you may need to click **Clear Filter**.)

- Step 12** If a field displays NA, the image attributes were not available from the image header. (If pre-existing filters are still in use, you may need to click **Clear Filter**.) We recommend that you manually enter the information to ensure the accuracy of the upgrade analysis.

- Step 13** Delete files from the storing directory (if applicable) to free space for future imports.

After the import, you can also add informational text to the Comments field. Normally at this point you will distribute the images; see [Distribute Images and Make Sure They Will Work, page 4-29](#).

Distribute Images and Make Sure They Will Work

Prime Network copies an image to a network element without activating it. This lets you perform these tasks before activating the image:

- Find out if there is insufficient memory, clear the disk space for distributing the image or package
- Do an upgrade analysis to check the suitability of the device for the chosen image

If appropriate, the images can be activated as part of the distribution job, and these tasks can also be performed:

- Commit Cisco IOS XR (so that changes are saved across device reloads).
- Perform a warm upgrade, where one Cisco IOS image can read in and decompress another Cisco IOS image and transfer control to this new image (thus reducing the downtime of a device during planned software upgrades and downgrades).



Note You can perform a warm upgrade only on Cisco IOS devices 12.3(2)T or later, such as 12.4T, 15.0, 15.1T, and for ISR 800/1800/2800/3800 series and 1900/2900/3900 series.

- Perform an in-service software upgrade (ISSU) for Cisco ASR 903 devices to update the router software with minimal service interruption. CCM performs a *single command upgrade* that installs a complete set of sub-packages using one command. The device must be configured in SSO redundancy mode. Before you perform an ISSU, you must verify if sufficient memory is available in standby boot flash.



Note Cisco ASR 903 devices must be booted in sub-package mode only through boot flash and not through any sub-directories of boot flash *before* using CCM to perform an ISSU. For more information, see the [Cisco ASR 903 Series Router Chassis Configuration Guide](#).

- Perform an in-service software upgrade (ISSU) for Cisco 9000 series devices and CRS devices to update the router software with minimal service interruption. The option to perform ISSU is supported only for SMU packages.
- Activate Cisco ASR 5000 boot configuration files

Prime Network uses the image staging location and transport protocol (TFTP, by default) specified on the Image Management Settings page. Prime Network displays the available upgradable modules and the storage partitions (if any) on the network element for the image distribution, from which you can choose the storage location you want to use.

The final step is to schedule the distribution job to occur either as soon as possible or at a future date (the default is as soon as possible).

What is Upgrade Analysis?

An upgrade analysis checks the attributes of the selected image, checks certain device features, and generates a separate report for each device. It is required before any image can be distributed. However, even if the upgrade analysis reports errors, Prime Network will allow you to proceed with the distribution (because an error can be a simple matter of an unpopulated field). Prime Network gathers this information from two sources:

- The Prime Network image repository, which contains information about minimum RAM, minimum Flash, and so on, in the image header.
- The Prime Network inventory, which contains information about the active images on the device, as well as Flash memory, modules, and processor details.






Note For Cisco Nexus 5000 or Cisco Nexus 7000 series devices, Prime Network displays the upgrade analysis results for both the system and kickstart images selected for the device.

An upgrade analysis verifies that the device contains sufficient RAM or storage, the image is compatible with the device family, and the software version is compatible with the image version running on the device.

Table 4-3 denotes the symbols used on the Distribution page.

Table 4-3 Status Icons

Symbol	Description	
	In Device Status Column	In Distribution Upgrade Analysis Column or Activation Analysis Results
	Device is available for upgrade analysis and distribution.	Device passed without warnings.
	Device is not available for upgrade analysis or distribution. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device.	Device passed with warnings. Click the icon to get more information.
	n/a	Device did not pass analysis. Click the icon to get more information.

Distribute Images to Devices

The following procedure explains how to perform an image distribution. You can also use this procedure to perform an upgrade analysis and then exit the procedure before performing the distribution.

Before You Begin

- If you are doing a Cisco IOS XR version upgrade (which upgrades the core package), see [Software Images, page 4-26](#) for information about other packages that you should upgrade at the same time.
- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the [Cisco Prime Network 4.0 Administrator Guide](#).)
- Make sure you have the permissions to perform the distribute operation. You will not be allowed to schedule a distribution job, if you do not have permissions.



Note

For all devices, you can distribute images to a standby or alias file system, but you cannot activate the images.

To distribute images and use upgrade analysis:

Step 1 Choose **Images > Distribute**.

Step 2 Choose the device type (**IOS** or **IOS XR**) and selection method (by image or package, or by device). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.



Note Prime Network does not support TAR file operations on devices. If you have TAR files to import, you must extract the TAR file and then import the image from the device. TAR file operations are supported only Cisco Catalyst devices.

- a. To choose devices of a specific device group, click **Select Groups** in the table header. Click the hyperlinked device group name to view the list of devices that belong to the group.
- b. Select the required device group in the Device Groups page and click **OK**.
- c. Choose one or more devices and click **Next**.

Step 3 Prime Network displays all images or packages which are valid for the selected devices from the internal image repository (for example, kickstart images for Cisco Nexus 5000 or Cisco Nexus 7000, and boot configs for Cisco ASR 5000). You can also choose **From External Repository** from the drop-down list (in the table header) to display the images or packages from the external image repository. Choose an image and click **Next**.



Note CCM allows image distribution from external repository only through FTP. Make sure you have configured the required credentials for accessing the external image repository in the Image Management Settings page.

Step 4 In the Select Storage page, choose a storage location by device or for all devices. This specifies where on the network element the image or package will be copied when it is distributed. This operation is not applicable for Cisco CPT devices.

Step 5 Perform an upgrade analysis to check whether the network element has sufficient space for the image or package by clicking **Upgrade Analysis**. After a few moments, Prime Network displays the results of the analysis in the Upgrade Analysis column. Click the symbol next to the icon to see the Upgrade Analysis report.

Symbol	Description	
	In Device Status Column	In Distribution Upgrade Analysis Column or Activation Analysis Results
	Device is available for upgrade analysis and distribution.	Device passed without warnings.
	Device is not available for upgrade analysis or distribution. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device.	Device passed with warnings. Click the icon to get more information.
	n/a	Device did not pass analysis. Click the icon to get more information.

If an error is reported, you will see a prompt asking you to confirm whether or not to proceed with the operation.

**Note**


Check the report to verify whether the storage location has sufficient space for the image or package. If the space is insufficient, the distribution will fail. If there is insufficient memory, you can choose to clear the disk space while scheduling the distribution in the Schedule Distribution page.

- Step 6** If you do not want to distribute any images or packages (for example, if you only wanted to perform a manual upgrade analysis), click **Cancel**. Otherwise, proceed to [Step 7](#).
- Step 7** Click **Next** to open the Schedule Distribution page in the wizard, and complete the schedule information.

**Note**

You can proceed with scheduling the distribution only if upgrade analysis is completed for all the devices (spanning across multiple pages) in the Select Storage page.

Field	Description
Schedule Distribution	When the distribution job should run. Note The time you specify here to schedule the distribution job is the server time.
File Transport Protocol	Overrides the default transfer protocol (as configured on the Image Management Settings page).
Clear Flash	(Optional) In case of insufficient memory, use the Clear Flash option (under Flash Properties). This deletes any one file (other than the running image) and recovers the disk space occupied by the file. This procedure is repeated until adequate space is available in the selected flash.
E-mail Id(s)	E-mail ID(s) to which to send a notification after the scheduled distribution job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.
Install Add Package(s)	(Optional) Adds packages during distribution for Cisco IOS XR devices
Schedule Activation	(Optional) Starts an activation job once the images or packages are distributed (immediately or at future time). For multiple devices, we recommend that you perform the activation separately from the distribution.
Process	For multi-device jobs, controls the job processes for both distribution and activation. If you chose Sequentially, you can also do the following: <ul style="list-style-type: none"> Specify the order in which the operations should be processed, by moving the items up and down in the Reorderable Rows box. Stop the job if an error is encountered by checking the Stop if an error occurs check box. Note If the job includes a reload, choose Sequentially . Otherwise, routers in the connectivity path of other routers may reload and cause problems.
Commit	Commits the packages after distribution for Cisco IOS XR devices.

Field	Description
Warm Upgrade	<p>(For Cisco IOS only) Activates the Warm Upgrade feature to reduce the device downtime during the distribution process.</p> <hr/> <p> Note You can perform a warm upgrade only on Cisco IOS devices 12.3(2)T or later, such as 12.4T, 15.0, 15.1T, and for ISR 800/1800/2800/3800 series and 1900/2900/3900 series.</p>
ISSU	<p>(For Cisco ASR 9000 series devices, Cisco ASR 903, and Carrier Routing System [CRS] devices only) Activates in-service software upgrade (ISSU) to update the router software with minimal service interruption. For CRS and ASR 9000 series routers, ISSU support is available only for software maintenance upgrade (SMU) package.</p>

Step 8 Click **Finished**. You are redirected to the Jobs page, where you can check the status of the distribution job.



Note Distribution fails if a timeout occurs after 30 minutes. You can view the job results for information on why the distribution failed. Remember to delete older images and packages from the staging directory.

Activate Cisco IOS Software Images

These topics describe the tasks you can perform from the Activate page:

- [Activate Cisco IOS Software Images](#)
- [Activate After Performing Boot Priority Modification for Cisco ASR 5000 Series Devices](#)

When a new Cisco IOS image is activated on a device, it becomes the running image on the disk. Deactivated images remain on the disk to be removed by a user. Older images are automatically deactivated.



Note For all devices, you can distribute images to a standby or alias file system, but you cannot activate the images.




Before You Begin

- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the [Cisco Prime Network 4.0 Administrator Guide](#).)
- Make sure you have the permissions to perform the activate operation. You will not be allowed to schedule an activation job, if you do not have permissions.

Activate Cisco IOS Software Images

To activate a Cisco IOS image on a network element:

- Step 1** Choose **Images > Activate**.
- Step 2** From the Cisco Devices tab, choose **IOS** by activation method (**IOS by Images** or **IOS by Devices**). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.
- Step 3** Prime Network displays all managed devices. It also displays the images that are currently running on the devices. You can filter by device name, IP address, element type, running image, or software version.
- To choose devices of a specific device group, click **Select Groups** in the table header. Click the hyperlinked device group name to view the list of devices that belong to the group.
 - Select the required device group in the Device Groups page and click **OK**.
 - Choose one or more devices and click **Next**. Prime Network displays all images or packages which are valid for the selected devices from the internal image repository (for example, kickstart images for Cisco Nexus 5000 or Cisco Nexus 7000, and boot configs for Cisco ASR 5000). You can also choose **From External Repository** from the drop-down list (in the table header) to display the images or packages from the external image repository.
- Step 4** Prime Network displays all images or packages which are valid for the selected devices from the internal image repository.
- Prime Network displays only root level bin files for selection. For a Cisco Nexus 5000 or Cisco Nexus 7000 series device, Prime Network displays the kickstart images available on the device in the Kickstart Images field. The field displays N/A if there are no kickstart images for the device.
- Step 5** Choose the image that you want to activate on the devices, and click **Next**.
- Step 6** For Cisco ASR 5000 series device, the Enter Boot Config page appears. You can activate a boot configuration file on the device in addition to an image. Select a boot configuration file from the available list and click **Save** and then **Next**.
- Step 7** Prime Network performs an image analysis. Check the Image Analysis page to see if analysis was successful. Click the icon in the Analysis column to get information about why the operation can or cannot proceed.

Symbol	Description	
	In Device Status Column	In Distribution Upgrade Analysis Column or Activation Analysis Results
	Device is available for upgrade analysis and distribution.	Device passed without warnings.
	Device is not available for upgrade analysis or distribution. Most likely the device is in the Maintenance investigation state or the Unreachable communication state. Click the device hyperlink and open the device properties popup to see details about the device.	Device passed with warnings. Click the icon to get more information.
	n/a	Device did not pass analysis. Click the icon to get more information.

If it cannot proceed, you will not be permitted to continue. Otherwise, click **Next**.

- Step 8** Enter the scheduling information in the **Schedule Activation** page. By default, jobs are scheduled to run as soon as possible.



Note The time you specify here to schedule the activation job is the server time.

- Step 9** Enter the e-mail ID(s) to which to send a notification after the scheduled activation job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.
- Step 10** (For Cisco IOS only) Activate the **Warm Upgrade** option, which allows a Cisco IOS image to read in and decompress another Cisco IOS image and transfer control to this new image (thus reducing the downtime of a device during planned software upgrades and downgrades).
- Step 11** (For Cisco ASR 903 devices only) Check the **ISSU** option, to update the router software with minimal service interruption.
- Step 12** Click one of the following to specify the operation mode, if you have selected two or more devices in the Select Devices page.
- **In Parallel**—Activates all packages for the devices at the same time.
 - **Sequentially**—Allows you to define the order of the devices to activate the packages for.
- Step 13** Click **Finished to schedule the activation**.

Activate After Performing Boot Priority Modification for Cisco ASR 5000 Series Devices

To modify boot priorities for Cisco ASR 5000 series devices and then perform activation:

- Step 1** Choose **Images > Activate > IOS** and the activation method (by **Devices**).
- Step 2** Choose the Cisco ASR 5000 device family from the table header.
- Prime Network displays all managed Cisco ASR 5000 series devices. It also displays the images that are currently running on the devices. You can filter by device name, IP address, element type, running image, or software version.
- Step 3** Select a Cisco ASR5000 series device, choose the **Perform Edit Boot Priorities** option from the drop-down menu in the table header, and then click **Next**. The Select Boot Config page appears.
- Step 4** Click the **Edit Boot Priorities** hyperlink. The Current Boot Priorities table lists the existing boot configuration files with their priorities.
- Step 5** Provide the following inputs to set up and fetch the desired boot priorities:
- Number of boot priority entries to be maintained. Value should be in the range of 1-10.
 - Boot priority number to start with. Value should be in the range of 1-100. Boot priority starting value should be greater than or equal to the number of boot priorities to be maintained.
- Step 6** Click **Go** to generate boot priorities based on the inputs provided. The modified boot priorities are listed in the table below.

- Step 7** You can choose to perform one of the following for each row in the table:
- **Edit**—Modify the boot priority value, the image name, and the configuration file, if required. The modified boot priority value should be unique.
 - **Delete**—Delete the boot configuration priority.
 - **Add Row**—Add boot priorities to the existing list. CCM generates boot priority values based on the inputs provided. Note that only the top ten boot priorities are considered for the device.
- Step 8** Click **Save**. A dialog box appears listing the existing and the modified boot priorities for your confirmation.
- Step 9** Click **Save** to confirm and apply the boot priority changes.
- Step 10** You can then schedule the activation as explained in steps 7 through 13 in the [Activate Cisco IOS Software Images](#) topic.
-

Perform Cisco IOS XR Software Package Operations



Note We recommend that you do *not* commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

These topics explain how to perform package operations:

- [Notes on Cisco IOS XR Packages, page 4-37](#)
- [Add Cisco IOS XR Packages, page 4-38](#)
- [Activate, Deactivate, and Delete Cisco IOS XR Packages, page 4-39](#)
- [Synchronize and Upgrade Satellites for Cisco ASR 9000 Devices, page 4-40](#)
- [Commit Cisco IOS XR Packages Across Device Reloads, page 4-41](#)
- [Roll Back Cisco IOS XR Packages, page 4-42](#)

Notes on Cisco IOS XR Packages

Package management includes the add, activate, deactivate, commit, and rollback operations on Cisco IOS XR devices. Before you perform any of these operations, read the following:

- When doing a version upgrade (which upgrades the core package and involves a router reload) on a Cisco IOS XR device, all of the packages on the router should be upgraded at the same time, as part of the same job. For example, if the c12k-mini, c12k-mgbl, c12k-mpls, c12k-k9sec, and c12k-mcast packages are on the router at version 3.4.1, when upgrading to version 3.5.0, all of the packages must be upgraded at the same time to version 3.5.0.



Note An upgrade pie is required only when you upgrade Cisco IOS XR devices from version 3.x to 4.x. You must deactivate and remove the upgrade pie, if you wish to perform any install operations, including the install commit operation on the devices upgraded from 3.x to 4.x.

- When upgrading the core router package (such as c12k-mini or comp-hfr-mini), the manageability package (such as c12k-mgbl or hfr-mgbl-p) must be upgraded at the same time to ensure that the router remains manageable after the reload.
- Cisco IOS XR routers support the **clear install rollback oldest x** command, that allows you to manage the number of rollback points maintained on the router. Executing this CLI command periodically on the router allows you to limit the number of rollback points. When executing this command, you must ensure that at least one valid rollback point is always maintained to enable Prime Network to show the package status correctly. We recommend that you maintain about 20 rollback points on the router.
- NEIM does not support upgrading a router running Cisco IOS software to Cisco IOS XR software.

For more information, refer to the [System Management Configuration Guide](#) for the Cisco IOS XR release and device of interest.

Add Cisco IOS XR Packages

Image Management supports package addition as a separate operation for Cisco IOS XR devices. To complete the package management life cycle, Image Management supports adding a package from a pie file, which is already present in the Cisco IOS XR device storage.

Before you begin:

Make sure you have the permissions to perform package addition. You will not be allowed to schedule a package addition job, if you do not have permissions.

To add packages for Cisco IOS XR devices:

-
- Step 1** Choose **Images > Package Add**. The Package Add wizard displays all the Cisco IOS XR devices in the Select Device(s) page.
 - Step 2** Select a device and click **Next** to open the Select Package(s) page. Prime Network displays all the packages available for the selected device.
 - Step 3** Choose the package(s) that you want to add for the selected device and click **Next** to open the Schedule Package Addition page in the wizard.
 - Step 4** Enter the scheduling information. By default, jobs are scheduled to run as soon as possible.



Note The time you specify here to schedule the package addition job is the server time.

- Step 5** If you have selected two or more devices in the Select Devices page, click one of the following to specify the operation mode:
 - In Parallel Order—Add packages for all devices at the same time.
 - In Sequential Order—Allows you to specify the order of the devices to import the packages for.
 - Step 6** Enter the e-mail ID(s) to which to send a notification after the scheduled package addition job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.
 - Step 7** Click **Finished**. Prime Network schedules the job and redirects you to the Jobs page, where you can monitor the status of the job.
-

Activate, Deactivate, and Delete Cisco IOS XR Packages



Note

For Cisco IOS XR devices, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

Before You Begin

- If you are doing a Cisco IOS XR version upgrade (which upgrades the core package), see [Software Images, page 4-26](#) for information about other packages that you should upgrade at the same time.
- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the [Cisco Prime Network 4.0 Administrator Guide](#).)

To activate or deactivate a Cisco IOS XR package, or delete a Cisco IOS XR package from a device:

- Step 1** Choose **Images > Activate > IOS-XR** and the activation method (by **Packages** or **Devices**). It is often easier to start with devices due to the sometimes cryptic nature of software image names. In this example we start with devices.
- Step 2** Prime Network displays all managed devices. (It also displays the packages that are currently running on the devices.) From this page you can also view the running package of the Cisco IOS XR device.
 - a. To choose devices of a specific device group, click **Select Groups**. In the Device Groups page, you can view the user-defined device groups. Click the hyperlinked device group name to view the list of devices that belong to the group. See [Device Groups Setup Tasks, page 4-9](#) for more information on user-defined device grouping.
 - b. Select the required device group in the Device Groups page and click **OK**.
 - c. Choose one or more devices and click **Next**. Prime Network displays all packages which are valid for the selected devices. You can filter your results by package name and version.
 - d. Choose the packages that you want to activate on the devices, and click **Next**.
- Step 3** Specify the operations you want to perform. You can perform different operations on different devices or the same operation on all devices (by selecting the desired operation from the **Use the following Operation for all Packages** drop-down list in the table header). When you select a device, Prime Network will display all of the packages that are installed on the device.
 - a. Choose a package operation for each package. Cisco IOS XR packages can be removed from a device only if they have been deactivated. If you want to apply the same operation to all packages, choose the operation from the **Use the following Operation for all Packages** drop-down list in the table header, and click **Apply**.
 - b. (Optional) Check **Test Only** to run a test of the activation (or deactivation) procedure on the device. This will not change the real device configuration. (This is similar to using the Compatibility Check option in the rollback process.)
 - c. Click **Next**. The Package Analysis page is displayed. Check the Package Analysis page to see if analysis was successful. Click the icon in the Analysis column to get information about why the operation can or cannot proceed (it will be one of the icons listed in [Table 4-3 on page 4-31](#)). If it cannot proceed, you will not be permitted to continue. Otherwise, click **Next**.

Step 4 Enter the scheduling information. By default, jobs are scheduled to run as soon as possible.



Note The time you specify here to schedule the activation job is the server time.

Step 5 Enter the e-mail ID(s) to which to send a notification after the scheduled activation job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

Step 6 (For Cisco ASR 9000 series routers and Cisco Carrier Routing System (CRS) devices only) Check the **ISSU** option, to update the router software with minimal service interruption.

Step 7 Check the **Commit** check box to commit the packages after activation.



Note We recommend that you do *not* commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

Step 8 Click one of the following to specify the operation mode, if you have selected two or more devices in the Select Devices page.

- **In Parallel**—Activates packages for all devices at the same time.
- **Sequentially**—Allows you to define the order of the devices to activate the packages for.

Step 9 Click **Finished to schedule the activation**.

Step 10 After the job completes:

- For Test Only jobs, repeat this procedure to activate the packages.
- If you activated or deactivated a Cisco IOS XR package, remember to commit your changes. However, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads. See [Commit Cisco IOS XR Packages Across Device Reloads, page 4-41](#).

Synchronize and Upgrade Satellites for Cisco ASR 9000 Devices


CCM provides satellite support for Cisco ASR 9000 devices. Satellites are used to enhance performance bandwidth of Cisco ASR 9000 devices. Each satellite is a Cisco IOS device connected to the Cisco ASR 9000 device. Multiple satellites can be connected to a single Cisco ASR 9000 device and all communications to the satellites happen only through the Cisco ASR 9000 device. Each satellite has its own configuration and software image.

CCM provides the following support for Cisco ASR 9000 device with satellites:

- Synchronization of all satellites together.
- Activation of the satellite pie image on Cisco ASR 9000 device with and without synchronization of satellites. You must run a CLI/XML command to check for compatibility and then push the image to the remote satellite.

Synchronize All Satellites Without Performing an Activation


To synchronize all satellites together without activation:

-
- Step 1** Choose **Images > Activate > IOS-XR** and the activation method (by **Devices**).
- Step 2** Choose the Cisco ASR 9000 device family and the **Sync Satellites** option from the **Select Operations** drop-down menu in the table header.
- Prime Network displays all managed Cisco ASR 9000 series devices having satellites. (It also displays the packages that are currently running on the devices.)
- Step 3** Click **Next** to schedule the synchronization for all the satellites together. You cannot select a particular satellite for synchronization. The Select Operation function is not applicable for the Sync Satellites option.
- Step 4** In the Schedule Activation page, provide the scheduling information for synchronization of all satellites.
- 

Note The time you specify here to schedule the synchronization job is the server time.
-
- Step 5** Check the **Sync Satellite(s)** check box and click **Finished**. The Sync Satellite(s) check box is available only for Cisco ASR 9000 devices having satellites.
-

Activate satellite image on Cisco ASR 9000 device with/without synchronization

To activate a satellite image on the Cisco ASR 9000 device with/without satellite synchronization:

-
- Step 1** Choose **Images > Activate > IOS-XR** and the activation method (by **Devices**).
- Step 2** Choose the Cisco ASR 9000 device family and the **Activate and/or Sync Satellites** option from the **Select Operations** drop-down menu in the table header.
- Step 3** Perform steps 3 through 7 in the [Activate, Deactivate, and Delete Cisco IOS XR Packages, page 4-39](#) topic.
- Step 4** Check the **Sync Satellite(s)** check box, if you wish to upgrade and synchronize the satellites. The Sync Satellite(s) check box is available only for Cisco ASR 9000 devices having satellites.
- 

Note Synchronization of satellites is done, only if the operation selected is activation or deactivation. Otherwise, synchronization will not happen even if this check box is selected.
-
- Step 5** Click **Finished to schedule the activation and/or synchronization**.
-

Commit Cisco IOS XR Packages Across Device Reloads

Committing a Cisco IOS XR package makes the device package configurations persist across device reloads. The commit operation also creates a rollback point on the device. See [Roll Back Cisco IOS XR Packages, page 4-42](#), for more information on rollback points.

**Note**

We recommend that you do not commit package changes until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads.

Before You Begin

- Verify that the package to be committed is operating properly (for example, by doing a **show status** command).
- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the [Cisco Prime Network 4.0 Administrator Guide](#).)
- Make sure you have the permissions to perform the commit operation. You will not be allowed to schedule a commit job, if you do not have permissions.

To commit a package after it has been activated, deactivated, or rolled back:

Step 1 Choose **Images > Commit**.

Step 2 Choose the network elements with the packages you want to commit.

Step 3 Click one of the following (in the table header) to specify the commit mode:

- **Commit in Parallel**—Commits all changes at the same time.
- **Commit Sequentially**—Allows you to define the order in which the changes are committed.

Step 4 Enter the scheduling information.



Note The time you specify here to schedule the commit job is the server time.

Step 5 Enter the e-mail ID(s) to which to send a notification e-mail after the scheduled commit job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.

Step 6 Click **Commit**. By default, jobs are scheduled to run as soon as possible.

Roll Back Cisco IOS XR Packages

Rolling back a Cisco IOS XR package reverts the device packages to a previous installation state—specifically, to a package installation rollback point. If a package has been removed from a device, all rollback points associated with the package are also removed and it is no longer possible to roll back to that point.

Before You Begin

- Read [Software Images, page 4-26](#), for information about managing rollback points on Cisco IOS XR devices.
- The device VNE (the device model in Prime Network) must be in a managed state when you run the command. (This means the VNE Communication State must be Reachable, and the Investigation State must be Normal or Incomplete. For more information on VNE states, see the [Cisco Prime Network 4.0 Administrator Guide](#).)

- Make sure you have the permissions to perform the rollback operation. You will not be allowed to schedule a rollback job, if you do not have permissions.

To roll back a Cisco IOS XR package:

- Step 1** Choose **Images > Rollback**. Prime Network displays all Cisco IOS XR devices. You can filter the results by using the **Quick Filter** option.
- Step 2** Choose the network elements. Prime Network populates the rollback points for the selected device package.
- Step 3** Choose a rollback ID from the Rollback ID drop-down list. The Rollback Point Details field lists the packages that were active when that ID was created.
- Step 4** To view all of the packages associated with the rollback point, place the mouse cursor on the Rollback Point Details field; see [Figure 4-9](#) for an example. To view the time stamp associated with the selected rollback, see the value displayed in the Time Stamp field.



Note The date and time stamps are displayed according to the local time zone settings of the client.

Figure 4-9 Packages Rollback Page with Rollback Point Details

Rollback	Rollback and Commit	Compatibility Check	Clear Selected Rows	Status	Device Name	IP Address	Element Type	Rollback Point	Rollback Point Details	Time Stamp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	GSRXR	10.76.92.188	Cisco 12406			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	GSR-189	10.76.92.189	Cisco 12406	103	dsd0:c12k-mcast-3.9.0, dsd0:c12k-kc-3.9.0, dsd0:c12k-es-mb-3.9.0, dsd0:c12k-mpb-3.9.0, dsd0:c12k-rout-3.9.0, dsd0:c12k-fwdp-3.9.0, dsd0:c12k-mpb-3.9.0, dsd0:c12k-admin-3.9.0, dsd0:c12k-base-3.9.0	05:16:59 UTC Tue Apr...

- Step 5** Click **OK** to close the popup window.



Note If a package has been deleted from the repository, the rollback points of the package are still displayed in the GUI. If you choose a rollback point for a deleted package, the rollback will fail. The job results popup provides information explaining why it failed.

- Step 6** (Optional) Click **Compatibility Check in the table header** to run a test of the rollback procedure on the device. This will not change the real device configuration. (This is similar to using the Test Only option in the activation process.)

- Step 7** Click **Rollback or Rollback and Commit**.



Note We recommend that you do not commit package changes until the device runs with its configuration for a period of time, until you are sure the change is appropriate. In that way, the change is not yet persisted across device reloads. See [Commit Cisco IOS XR Packages Across Device Reloads](#), page 4-41.

Step 8 Enter the scheduling information.



Note The time you specify here to schedule the rollback job is the server time.

Step 9 Enter the e-mail ID(s) to which to send a notification after the scheduled rollback job is complete. For two or more users, enter a comma-separated list of e-mail IDs. A notification e-mail is sent based on the e-mail option specified in the Image Management Settings page.



Note Before you enter the e-mail ID(s), ensure that you have set up the SMTP host and SMTP port in the Image Management Settings page (see [Change Image Management Global Settings, page 4-66](#)). The e-mail ID(s) configured in the Image Management Settings page, if any, will be displayed by default. You can modify the e-mail ID(s) if required.

Step 10 Click **Rollback**.

Clean Up the Repository

The repository is purged according to the settings described in [NEIM Setup Tasks, page 4-7](#). When files are removed from the repository, this does not affect files that are installed on the device. However, deleting a package could cause a rollback point to become unexecutable. If a package or version of a package that is associated with a specific rollback point is removed, it will no longer be possible to roll back to that point. See [Roll Back Cisco IOS XR Packages, page 4-42](#).

To delete images from the Prime Network image repository:

Step 1 Choose **Images > Repository**.

Step 2 Select the image you want to delete and click the Delete button (with red **X**) in the table header.

Step 3 To collectively delete all images in the repository, click the **Delete All** button in the table header. You will see a prompt asking you to confirm whether or not to proceed with the operation.

Step 4 Click **OK** to confirm and image(s) available in the repository will be deleted.

These topics provide administrative information on CCM:

- [Global Settings and Administration, page 4-61](#)—How to use the Configuration Management Settings page to specify when configurations should be collected, when they should be purged, commands to exclude from comparisons, and other global settings.
- [Change Image Management Global Settings, page 4-66](#)—How to use the Image Management Settings page to specify the default transfer protocol, staging and storing locations, and credentials for accessing a vendor web site.
- [Check the Processes, page 4-68](#)—How CCM ensures communication security, authenticates and authorizes users, where log files for debugging purposes are located, and so forth.

You should also make sure you have properly set up CCM by reading [Configuration Management Setup Tasks, page 4-5](#).

**Note**

In the Configuration Management and Image Management Settings pages, CCM does not support the following special characters:

- For Password fields—>, <, ', /, \, !, :, ;, and "
- For all other fields—`, ~, @, #, \$, %, ^, &, *, (,), +, =, |, {, }, [,], ', ? , >, <, /, \, !, :, ;, and "

Configuration Audit

**Note**

Starting Prime Network 4.0, Configuration Audit is being replaced by Compliance Audit. However, if you enabled the option to retain Configuration Audit during an upgrade procedure from Prime Network 3.11 (or earlier), the feature will still be available from CCM. For more information on Compliance Audit, see [Compliance Audit, page 4-51](#).

CCM facilitates a configuration compliance mechanism, which enables auditing configurations on a device against a specified configuration policy file (also called as a baseline or expected configuration). Prime Network facilitates administering multiple configuration policy files through a Configuration Audit Policy Manager. Each configuration policy is a set of CLI commands that define a desired baseline or expected configuration. Configuration policies can also be configured using valid, Java-based regular expressions. [Table 4-4](#) provides examples of configuration policy CLIs.

Table 4-4 Configuration Policy CLI Examples

Policy Name	Policy Description	Policy CLI
SamplePolicy1	Sample policy for global configuration auditing	spanning-tree mode rapid-pvst
SamplePolicy2	Sample policy for global regex and first sub level cli matching audit	interface GigabitEthernet(.*) port-type nni
SamplePolicy3	Sample policy for global regex, first sub level cli matching, and second sub level regex matching	router (.*) address-family ipv4 unicast network (.*)
SamplePolicy4	Sample policy for fixed cli matching	interface GigabitEthernet3/4 address-family ipv4 unicast

Sample Configuration Policy

The following example shows a policy that performs audit for BGP configuration for a Cisco IOS router:

```
#BGP Configuration Audit
router bgp (.)
  neighbor (.) remote-as (.)
  address-family ipv4
```

If you want an audit check for specific BGP AS or neighbor IP address, the above CLI can be changed accordingly. For example:

```
router bgp 65000
  neighbor (.) remote-as 65001
  address-family ipv4
```

You can combine multiple different configurations into one policy. For example:

```
#BGP Configuration Audit
router bgp (.*
    neighbor (.* remote-as (.*
    address-family ipv4
# Interface MEP check
interface GigabitEthernet(.*
    ethernet (.*
    mep domain UP (.*
```

Configuration audit can be scheduled against multiple configuration files to obtain an audit report that indicates the existence of configuration sequences stated in the baseline policy and any deviations from the baseline.

You can define a configuration policy, select the devices that need to be audited against the policy, and schedule the audit job to run immediately or at a later point in time. The audit job compares the CLI commands (as part of the configuration policy) against the actual running configuration on the device to identify the discrepancies.

You can view the status of all the scheduled configuration audit jobs in the Job Manager page. The configuration audit results are in the form of a report indicating the discrepancies (missing configuration commands on the device) in red and the matching commands in green.

Manage Configuration Policies

CCM allows you to create, modify, view, and delete configuration policies. Choose **Configuration Audit > Configuration Policies**. The Configuration Policies page provides the list of existing policies. You can search the configuration policies by CLI strings.

Create Configuration Policy

To create a configuration policy:

-
- Step 1** In the Configuration Policies page, click **Create**.
 - Step 2** Provide the policy name and description.
 - Step 3** Enter the CLI commands to set up a baseline configuration for that policy. This can also be a valid, Java-based regular expression. See [Table 4-4](#) for sample configuration CLIs.
 - Step 4** Make sure you follow the guidelines while entering the CLI commands. Click **Guidelines** to view these guidelines as shown in [Figure 4-10](#).

Figure 4-10 Create Configuration Policy-Showing Guidelines

Create Configuration Policy

Policy Name:

Description:

CLI Commands:

Guidelines:

Following rules should be followed, while entering CLI command:

1. Global command should not start with a space character.
2. First level sub-command should starts with 3 leading space characters.
3. Second level sub-command should starts with 6 leading space characters.
4. First level sub-command must have a global command.
5. Second level sub-command must have a first level sub-command.
6. Comment will starts with hash (#) character.
7. Third level sub-commands are not supported.

OK Cancel

320079

Edit, View, or Delete Configuration Policy

In the Configuration Policies page, you can also do the following:

- Select a policy and click **Edit** to modify the policy description and CLI commands. You cannot modify the policy name. Keep in mind the policy guidelines while modifying the CLI commands.
- Select a policy and click **View** to view the policy name, description, and CLI commands.
- Select a policy or multiple policies and click **Delete** to delete the configuration policies. You cannot delete a policy if it is part of a scheduled audit job.

Schedule Configuration Audit

You can schedule configuration audit jobs to run immediately or at a later point in time.



Note

Only a maximum of 10 policies and 500 devices can be used for scheduling an audit job.

To schedule a configuration audit job:

- Step 1** Choose **Configuration Audit > Basic Audit**. The Select Configuration Policies page lists the available configuration policies. You can search the configuration policies by using CLI strings.
- Step 2** Select the desired configuration policy from the available list and click **Next**.
- Step 3** In the Select Devices page, select the devices that must be audited against the selected configuration policy, and then click **Next**.

- Step 4** In the Schedule Audit page, provide a job name and the scheduling information for the configuration audit job. You can choose to run the audit job immediately or at a later point in time. A popup with the server time is available to assist you in setting up the time for scheduling the audit job.
- Step 5** Click **Audit**. You will be redirected to the Configuration Audit Jobs page.



Note Once scheduled, you cannot edit the policies or devices that are part of the scheduled job.

View Configuration Audit Jobs and Audit Results

The Configuration Audit Jobs page (**Configuration Audit > Configuration Audit Jobs**) provides the following details:

- **Jobs**—This table lists all configuration audit jobs submitted by the login user. The ‘root’ user can view jobs submitted by other users, by selecting the username from the table header.
- **History**—For a selected job in the Jobs table, this table lists all the instances. You can select only one job at a time to view the history details.

You can select a job and click **View** to view the associated devices and policies, and the schedule for the selected audit job.

You can also use this page to suspend, resume, cancel, delete, or reschedule a job.

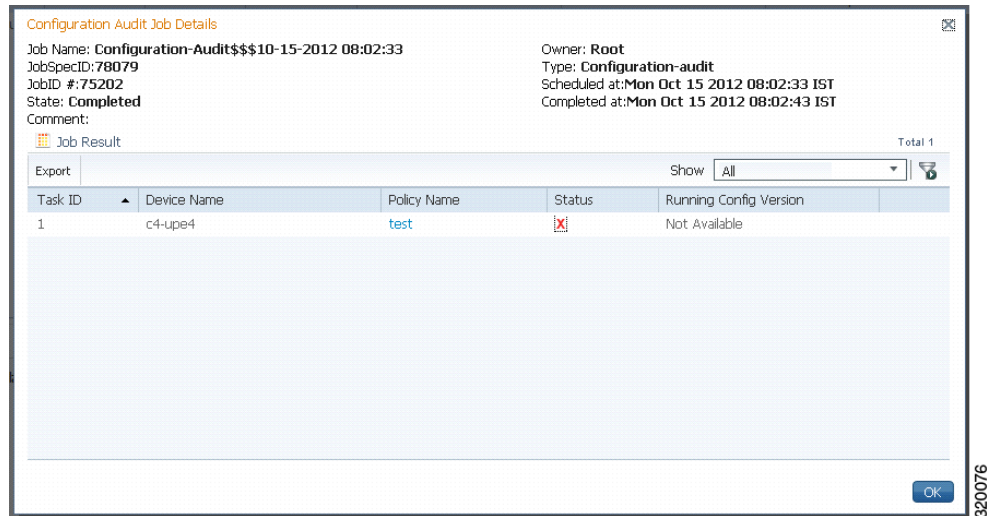
To view the configuration audit job details and the audit result:

- Step 1** Click on the hyperlinked **LastRun Result** (Success/Partial Success/Failure) against a particular job in the Jobs table.

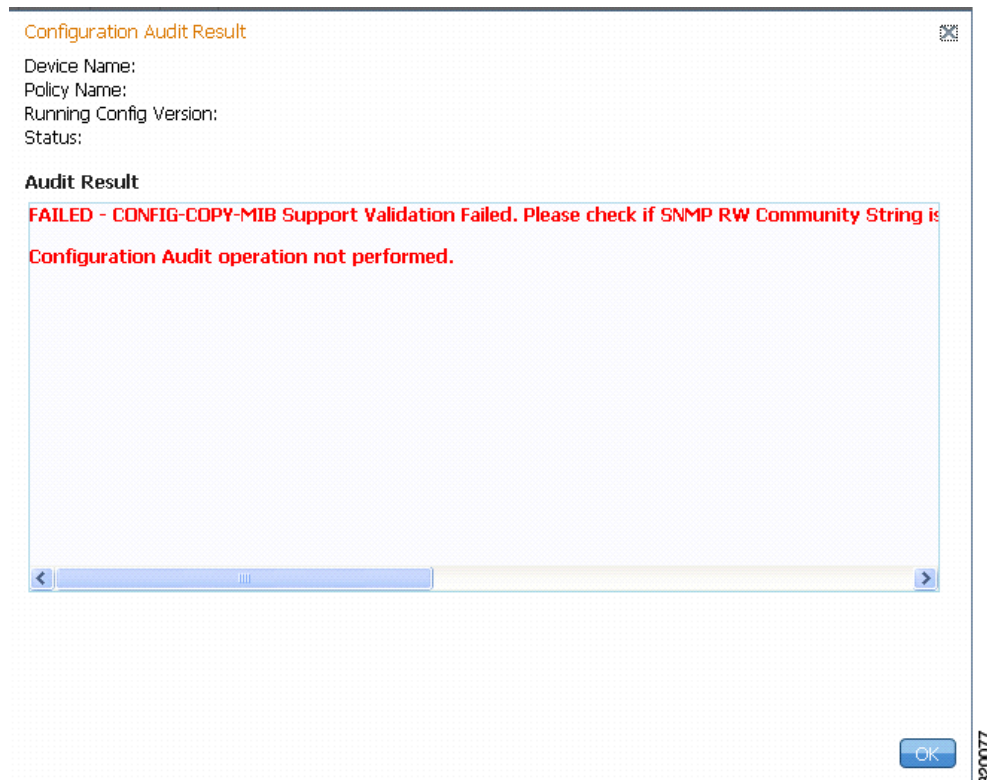
The Configuration Audit Job Details dialog box displays the job details and the audit results for a device and policy combination, as shown in [Figure 4-11](#). The Job Results table includes the device audited, policy against which the device was audited, audit status, and the running configuration version used for the audit. A blue tick mark in the Status column indicates ‘Audit Pass’, and a red X indicates ‘Audit Fail’. Click the hyperlinked policy name to view the configuration policy details, with updates if the policy has been modified.



Note For Cisco Nexus devices, the VDC name is also displayed in the Device Name column.

Figure 4-11 Configuration Audit Job Details

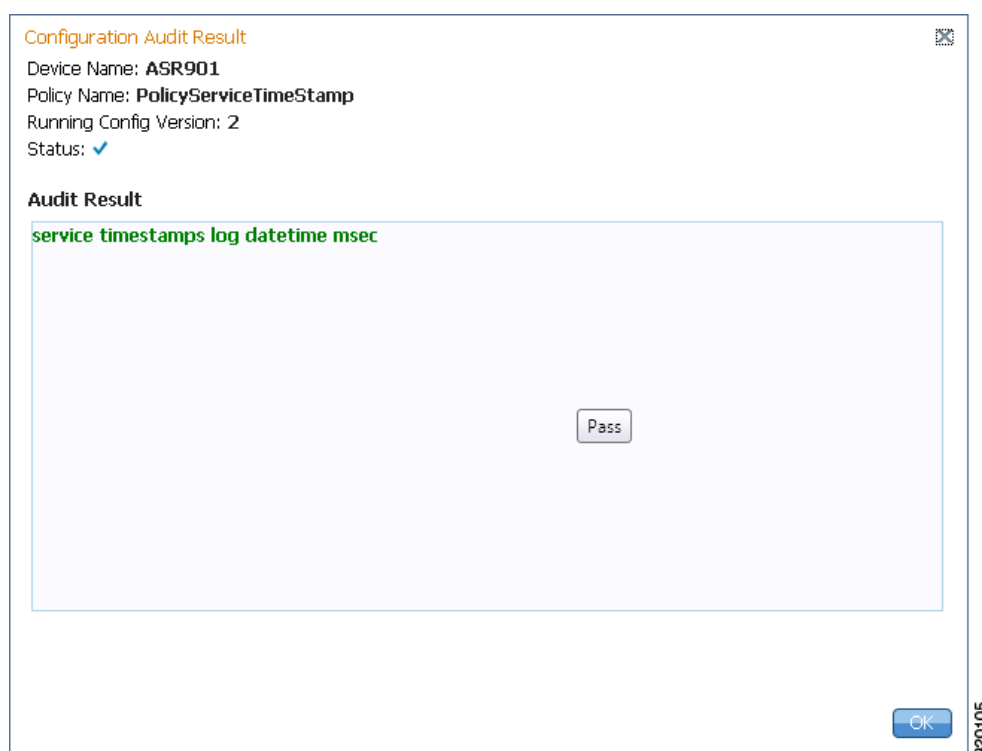
- Step 2** Click on the hyperlinked **Status** (Pass/Fail icon) in the Job Results table. Or, click the hyperlinked Success or Failure hyperlink in the **Result** field of the History table. The Configuration Audit Result dialog box displays the audit result with matching commands (for 'Audit Pass') and discrepancies or missing commands (for 'Audit Fail') between the policy and the running configuration on the device. See [Figure 4-12](#) for an example of the Configuration Audit Result dialog box for an 'Audit Fail' scenario.

Figure 4-12 Configuration Audit Result - Audit Fail

The matching commands are displayed in green (see [Figure 4-13](#)), while the discrepancies are displayed in red (see [Figure 4-12](#)). For a failed job, the Audit Result section also displays the reason why the audit was not successful as shown in [Figure 4-12](#). Some reasons for audit failure are:

- Failed to back up running configuration of the device
- Device not reachable
- Unable to download running configuration
- Device not under the scope of the user
- Policy is not available
- Invalid regular expression in the CLI

Figure 4-13 Configuration Audit Result - Audit Pass



Step 3 Click **Export** in the Job Results table to export the audit job results to a .csv file. You can view the job details and audit results in the exported file.

Compliance Audit

The Compliance Audit feature (**Cisco Change and Configuration Management > Compliance Audit**) ensures that existing device configurations comply to your deployment's policies. It replaces the Configuration Audit features that was provided in previous releases of Prime Network. This feature is enabled by default.

Using Compliance Audit, you can create policies that can contain multiple rules, and policies can be grouped together to create a policy profile which can be run on a set of devices, called audit of devices. There is no limit on the number of policies, profiles, rules, and conditions that you can create using Compliance Audit. It can scale up to 35,000 devices.

When a device is detected to be not confirming to a determined policy, Compliance Manager calls it a violation. Subsequently, if available, it also recommends a fix, as configured by the administrator. The violation details are saved in DB Schema for your reference later.

In some scenarios, the fix is readily available as configured by the administrator and can be directly applied, while in some others, it has to be carefully scrutinized by the administrator before it is run. Automatic application of some of the fixes can be disabled since it may conflict with other policies and configurations that may be specific to the device and the setup.

This section contains the following topics:

- [User Authentication and Authorization, page 4-52](#)
- [Creating Policies and Profiles, and Running a Compliance Audit Job, page 4-53](#)

User Authentication and Authorization

Compliance Audit uses the security methods employed by Prime Network. These are described in the [Cisco Prime Network 4.0 Administrator Guide](#).



Note

If authentication fails, check the status of AVM 77 (XMP runtime DM) and Prime Network using Cisco Prime Network Administration. Cisco Prime Network Administration displays AVM 77 only when Ciis installed. For information on how to use Cisco Prime Network Administration, see the [Cisco Prime Network 4.0 Administrator Guide](#).

The GUI-based functions and required roles are listed in [Table 4-5](#). The scope of your operation depends on your role and scope.



Note

If your role is Viewer, you cannot see Compliance Audit listed in CCM despite enabling it in the Registry Controller.

The following table lists the permissions:

Table 4-5 **Default Permission/Security Level Required to Use Compliance Audit**

Task	Administrator	Configurator	OperatorPlus	Operator	Viewer
Creating policies	X	X	—	—	—
Creating policy profiles	X	X	X	X	—
Executing audit job	X	X	X	X	—
Viewing audit job results	X (For all users' jobs)	X (For jobs that the specific user has created)	X (For Operator Plus jobs only)	X (For Operator jobs only)	—

Table 4-5 Default Permission/Security Level Required to Use Compliance Audit (continued)

Task	Administrator	Configurator	OperatorPlus	Operator	Viewer
Executing a Fix job Note To execute a fix job, the device-level role of the user must be Configurator or Administrator. The role of the user for a device overrides the role of a user on Prime Network.	X	X	—	—	—
Viewing the fix job results	X (For all users' jobs)	X (For jobs that the specific user has created).	—	—	—

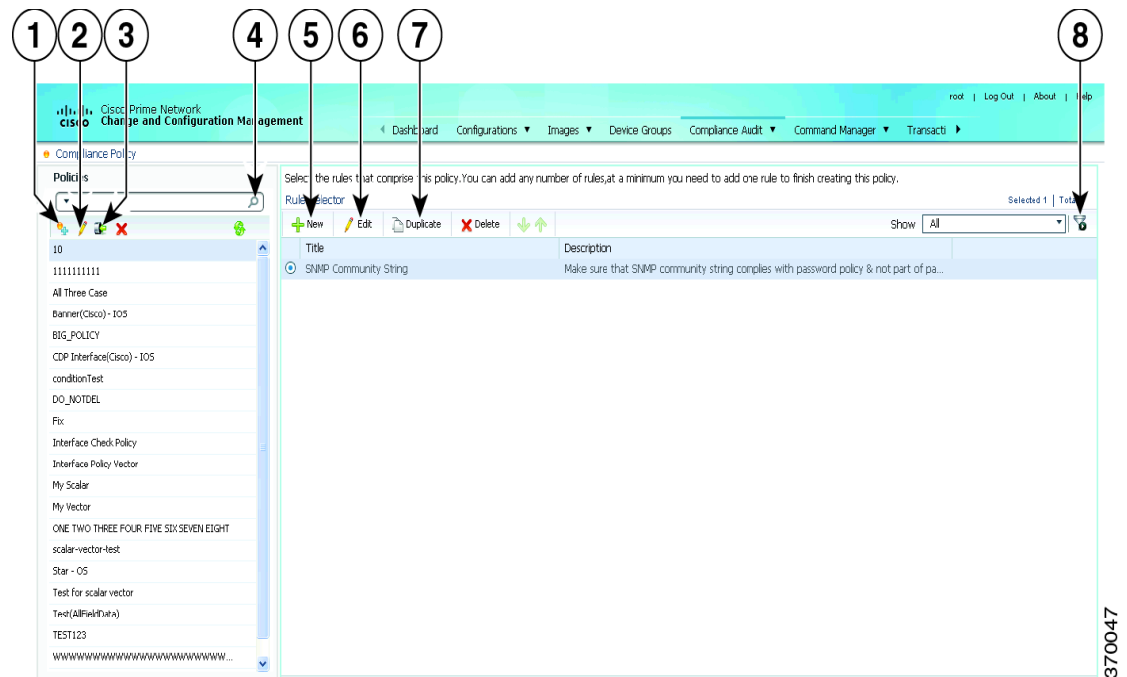
Creating Policies and Profiles, and Running a Compliance Audit Job

Running an audit job the first time requires you to follow a specific workflow:

	Description	See:
Step 1	Create a policy containing multiple rules	Creating a Policy, page 4-53
Step 2	Group policies into policy profiles so you can apply them	Creating a Policy Profile, page 4-58
Step 3	Run the policy against your specified devices	Auditing Devices, page 4-58
Step 4	View the results and fix any violations	Viewing the Results of an Audit Job and Running Fixes for Violations, page 4-59

Creating a Policy

The first step in auditing devices is to create a policy (**Compliance Audit > Compliance Policy**). The Compliance Policy page ([Figure 4-14](#)) appears.

Figure 4-14 Compliance Policy Page

1	Create Compliance Policy icon	5	New Rule icon
2	Edit Policy Description icon	6	Edit Rule icon
3	Import Policy as XML icon	7	Duplicate Rule icon.
4	Search field	8	Filter icon

The following steps explain the procedure:

You can either create a new policy or you can import an existing policy by clicking the **Import** icon. You can export existing policies as XML files to your local drive.

- Step 1** Click **Create Compliance Policy** icon and enter the policy details. The policy is listed in the left pane. After you add a new policy, you must associate one or more rules to the policy.
- Step 2** From the Rule Selector pane, click **New Rule** icon. For more information on creating a new rule, see [Creating a Rule](#).

Creating a Rule

For a policy to run against devices and generate violations, you must specify rules within the policy and define the conditions and the relevant fixes for violations. Rules are platform-specific. Each policy must contain at least one rule; however, there is no limitation on the number of rules you can define for a policy. You can also duplicate an existing rule and add to a policy. Click the **Duplicate** button to clone a rule. Follow the procedure below to create a rule and add the rule to a specific policy:

- Step 1** From the left navigation pane, select the policy to which you want to add rules.
- Step 2** From the work area pane, click the **Create Rule** icon.
- Step 3** Enter the following details. For sample rules, see [Creating Rules—Samples, page 4-56](#).


Table 4-6 New Rule - Fields

Field	Description
Rule Information	
All information entered in this section is for your consumption. This information does not impact the conditions and the subsequent violations.	
Name	Enter a name for the rule.
Description	Enter a brief description
Impact	Enter a brief note on the impact of the violation that the rule will generate.
Suggested Fix	Enter a brief description of the fix that will help you decide to choose or to not choose the rule against a specific policy. This description appears when you check the rule in the Rule Selector pane.
Platform Selection	
Available Platforms	Check the platforms on which the condition must be run. If you select Cisco Devices, all of Cisco platforms specified in the list are included. The platforms checked in this section impacts the ignore count of an audit job. For example, if you run a rule on all the devices within your scope, including devices not selected in the Available Platforms pane, such devices are not audited and are marked against Ignore count.
Rule Inputs	
New Input	<p>Click the New icon to add inputs for the new rule. This field is optional. The input you create in this pane reflects in the Policy Profile page. You must provide rule inputs for the rule you have selected. For example, you can create an input to be IP Address. Any user who wants to run this rule can enter an IP address specific to the rule and add it to a specific profile. Enter the following details:</p> <ul style="list-style-type: none"> • Title • Identifier—Click the Generate button to generate an identifier based on the title. The identifier is used in Block Start Expression, Conditions Match Criteria (value field), Action Details Tab - Violation Message, Fix CLI (if action is Raise a Violation, and Violation Message Type is Define Custom Violation Message for the Condition). • Data Type—Choose a data type. The type of data you enter in the Parameter Substitution field depends on your selection here. • Input Required—Check the option, as required.

Table 4-6 **New Rule - Fields (continued)**

Field	Description
Conditions and Actions—Conditions Details tab	
Condition Scope Details	<ul style="list-style-type: none"> Condition Scope—Choose the scope of the conditions from one of the below: <ul style="list-style-type: none"> Configuration—Checks the complete running configuration Previously Matched Blocks—Runs the conditions against blocks that have been defined in previous conditions. To run the condition with this option, you must have checked Parse as Block option in one of the previous conditions. You cannot select this option for the first condition of a rule. Device Properties—This checks against the device properties and not the running configuration. Device Property—This option is enabled only if you selected Device Properties option in the Condition Scope option.
Block Options	
Parse as Blocks	Checking this option enables you to run conditions on specific blocks (as defined in this section) in running configuration files. This option is enabled only if you selected Configuration in the Condition Scope option.
Block Start Expression	This field is mandatory if Parse as Blocks option is enabled. This must be a regular expression. Rule Inputs can be used here.
Block End Expression	This field is optional. By default, blocks end when the top-level or a sub-level command begins. If you prefer to break the block earlier, enter the value as a regular expression.
Rule Pass Criteria	<p>Check the option, as required. If you select:</p> <ul style="list-style-type: none"> All Sub Blocks—The rule is marked a success only if all the blocks fulfill the specified condition. Any Sub Block—The rule is marked a success even if one of the sub blocks fulfill the condition. Raise One Violation for Each Failing Instance—If you check this option, the violation count specified in the Job view increases by as many number of violations as the condition encounters in each block.
Condition Match Criteria	
Operator	Choose an option based on the value you will enter in the subsequent field.
Value	The value must be a regular expression. This variable can be grepped for use in the subsequent conditions. It follows the convention of condition <number.value number> such as, <2.1> <2.2>... This numerical identifier can be used from the next condition as input parameter for Operator selected in the previous field.
Rule Pass Criteria	<p>Check the option, as required. If you select:</p> <ul style="list-style-type: none"> All Sub Blocks—The rule is marked a success only if all the blocks fulfill the specified condition. Any Sub Block—The rule is marked a success even if one of the sub blocks fulfill the condition. Raise One Violation for Each Failing Instance—If you check this option, the violation count specified in the Job view increases by as many number of violations as the condition encounters in each block.

Table 4-6 New Rule - Fields (continued)

Field	Description
New Conditions and Actions—Action Details tab (applicable for both Match Action and Does Not Match Action)	
Select Action	<p>Select one of the following actions that Compliance Audit must perform upon detecting a violation:</p> <ul style="list-style-type: none"> Continue—If the condition is met or not met, the rule continues to run based on the condition number specified in the field. If a condition number is not specified, the rule skips to the next immediate condition. Raise a Violation—Raises a violation and stops further execution of rule. Do Not Raise a Violation—Does not raise a violation; stops further execution of rule.
Condition Number	Specify the condition number to which the rule must continue with in case the condition is met or is not met. You cannot specify a condition number that is lesser than or equal to the current condition number. This field is enabled only if you selected the option Continue from the Select Action field.
Violation Severity	Specify a severity that Compliance Audit must flag if a violation is detected. This field is enabled only if you selected one of the options, Raise a Violation from the Select Action field.
Violation Message Type	Select a message type. If you determine a violation as not fixable (or requiring manual intervention), select the Generate Default Violation Message During Audit option. To enter a fix for a violation, select the option Define Custom Violation Message for the Condition.
Violation Message	Enter a violation message that is displayed in the Job View window. select the option Define Custom Violation Message for the Condition.
Fix CLI	<p>Enter a relevant CLI fix if the device does not meet the condition specified. select the option Define Custom Violation Message for the Condition.</p> <p>Do not enter <code>config t</code> and its <code>exit</code> commands.</p> <p> Note <code>exit</code> command is allowed at main and sub-level commands.</p>

After you complete adding rules to the policy, a profile must be created. For more information, see [Creating a Policy Profile](#).

Creating Rules—Samples

This section explains three scenarios in which rules can be created.

Problem This policy checks if at least one of the pre-defined DNS servers are configured on device.

The following condition checks if either **IP name-server 1.2.3.4** or **IP name-server 2.3.4.5** is configured on the device, and raises a violation if neither of them are configured.

Solution The following settings have to be made in the appropriate sections.

Field	Value
Configuration Scope	Configuration
Operator	Matches the expression
Value	<code>ip name-server (1.2.3.4 2.3.4.5)\$</code>
Match Action	Do not raise a violation and exit this rule

Field	Value
Does Not Match Action	Raise a violation and exit this rule
Violation Text	DNS Server must be configured as either 1.2.3.4 or 2.3.4.5.

Problem This policy checks if at least two NTP servers are configured on the device for NTP server redundancy.

The following condition checks if the command `ntp server` appears at least twice.

Solution The following settings have to be made in the appropriate sections.

Field	Value
Configuration Scope	Configuration
Operator	Matches the expression
Value	<code>(ntp server.*\n){2,}</code>
Match Action	Continue
Does Not Match Action	Raise a violation and exit this rule
Violation Text	At least two NTP servers must be configured.

Problem This policy checks if the device is not configured with any prohibited community strings or community strings that must be avoided for SNMP.

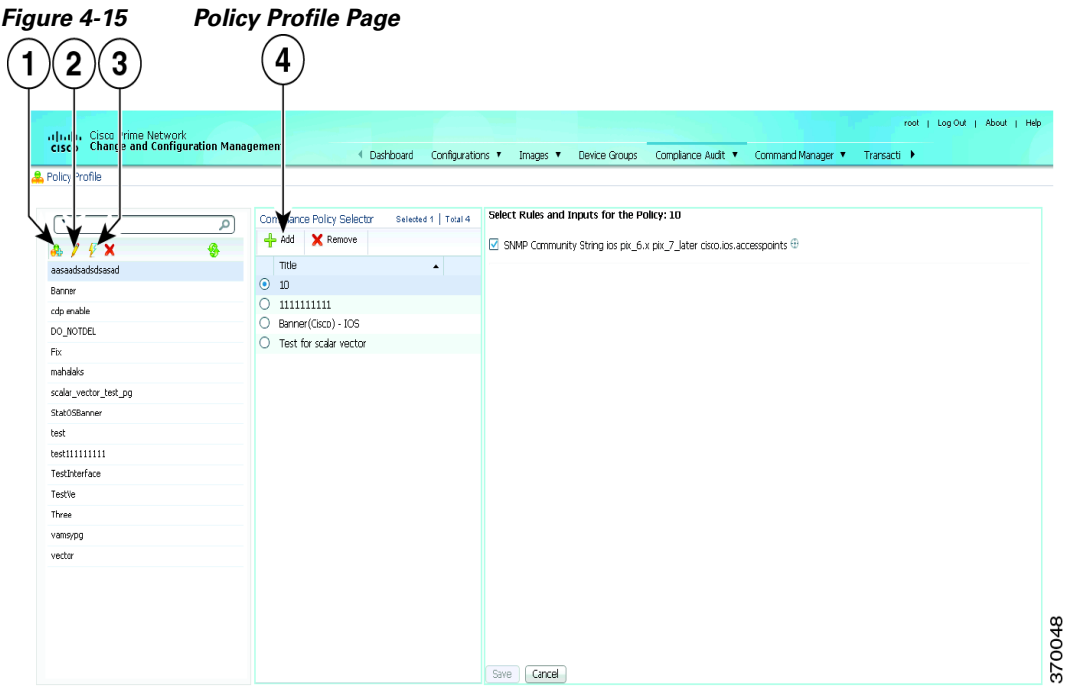
This condition checks if either `snmp-server community public` or `snmp-server community private` is configured on the device. If configured, Compliance Audit raises a violation. Note that `</>` in the violation text is replaced with the actual community string configured on the device, at the runtime. In this example, `</>` indicates first captured group in the current condition.

Solution The following settings have to be made in the appropriate sections.

Field	Value
Configuration Scope	Configuration
Operator	Matches the expression
Value	<code>snmp-server community (public private)</code>
Match Action	Raise a violation and exit this rule.
Does Not Match Action	Continue
Violation Text	Community string <code></></code> configured.

Creating a Policy Profile

After you have created policies, create a policy profile that will contain a set of policies. Go to **Compliance Audit > Policy Profile**. The Policy Profile page ([Figure 4-15](#)) appears.



1	Create Policy Profile icon	3	Run Compliance Audit icon
2	Edit Policy Profile Description icon	4	Add Compliance Policy icon

Follow the procedure below to create a new policy profile:

- Step 1

From the left navigation pane, click the **Create New Policy Profile** icon. Enter name and description of the policy profile.
- Step 2

Choose a policy profile from the left navigation pane. From the Compliance Policy Selector pane, click the **Add Compliance Policy** icon. The list of policies appear. Choose the required policies.
- Step 3

After you choose the policies, select the rules within the selected which you want to audit against. Later, if applicable, enter values for rule inputs. The option to enter rule inputs is available only if you entered input parameters when you created a new rule.
- Policy Profiles are created and an audit job can be run.

Auditing Devices

After you create a policy profile, you must choose the devices on which it has to be run. After you choose the devices and schedule an audit, a job with the name of the policy profile name is created. This name defines this job, and can be scheduled periodically. This job name is editable.

- Step 1

After you have created the profiles, click the **Run Compliance Audit** icon.
- The Select Devices window appears.
- Step 2

Select the devices which you wish to audit. Click **Next**.

- Step 3** The Schedule Audit page appears. Enter the schedule details. Against Choose Configuration option, choose the configuration that you want to be applied:
- Use Latest Archived Configuration—If you choose this option, the latest Backup Configuration available in NCCM is used. If the backup configuration is not available, the device is not audited and is marked against non-audited devices.
 - Use Current Device Configuration—If you choose this option, Prime Network polls for the latest configuration from the device and then performs the audit.
- Step 4** Click **Audit**. An audit job is scheduled. You can view the status of an audit job from the Jobs page.

Viewing the Results of an Audit Job and Running Fixes for Violations

The status of scheduled jobs appears on the Jobs page (**Compliance Audit > Jobs**). All audits are logged by Prime Network as jobs.

From this page, you can view the violation details and can also apply a fix. After a job is created, you can set the following preferences for the job:

- Suspend—Can be applied only on jobs that are scheduled for future. You cannot suspend a job that is running.
- Resume—Can be applied only on jobs that have been suspended.
- Reschedule—Using this option, you can reschedule a job that has been scheduled for a different time. Choose a job, and click **Reschedule**. The Compliance Audit Job Rescheduler window opens. Set your preferences. The following options are available against Choose Configuration option:
 - Use Latest Archived Configuration—If you choose this option, the latest Backup Configuration available in NCCM is used.
 - Use Current Device Configuration—If you choose this option, Prime Network polls for the latest configuration from the device and performs the audit.



Note

You might be prompted to enter your device access credentials. This option is enabled if, from the **Prime Network Administration > Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations**, you checked the option **Ask for user credentials when running configuration operations**. This is an enhanced security measure to restrict access to devices.

- Cancel—Using this option, you can cancel a scheduled job.
- View—This option is enabled only for jobs that in Completed state. Using this option, you can view the details of a job, the associated policies and devices.
- Delete—This option deletes a job that has been scheduled. This deletes the listing from the GUI. You cannot delete a job that is running.

All jobs that are completed are listed in the jobs page. The job is flagged a success only if all the devices audited confirm to the policies specified in the profile. The result, otherwise, is displayed as Failure. The job is called a partial success if job contains a mix of both audited and non-audited devices, with the compliance status of audited devices being a success.

You can view the details of the job by clicking the hyperlinked result displayed against each job. When you click the result, the Compliance Job Audit Details window displays the violation details. The Compliance Audit Violation Details window displays the following details:

Table 4-7 Compliance Audit Violation Details- Fields

Field	Description
Job Details and Violations Summary	
Audited/Non-Audited Devices	<p>This displays the number of audited and non-audited devices. For more details on devices, click the hyperlinked count of audited and non-audited devices. Non-audited devices include the count of the following.</p> <ul style="list-style-type: none"> – The devices that were within the scope of the user while scheduling the job, but has since changed. At the time job ran, these devices were not within the scope of the user. – The devices that were down or were not reachable when the job ran. – CPT device not in IOS mode. These devices are not audited because they do not contain running configuration, which is required for Compliance Manager. – Third Party Devices. – Device not in sync with with Compliance server—that is, the device element type is not available in the Compliance server. – Devices of which backup running configuration cannot be fetched from CCM.
Selected Rules	Number of rules selected in a policy at the time the policy profile was created. This may be subset of the total number of rules defined for the policy.
Compliance State	Displays Pass or Fail. All rules in policy for all devices must confirm for the state to display Pass.
Violation Count	This lists the number of distinct violations (for a particular policy, for the number of devices) that were observed in each job. For example, if a particular policy is violated in 100 devices, the violation count is only 1.
Instance Count	Summation of the violation count for all the device. For example, if a particular policy is violated in 100 devices, the instance count is 100.
Highest Severity	The highest severity of the various rules comprising the policy. The highest (as decided at the time of creating rules) is shown. This overrides the lower severity items.
Ignore Count	This is the count of rules ignored due to devices falling outside the scope of platforms defined against the rule.
Violations by Device	
Violations by Device	This window displays the violations at a device level. Select the devices for which require the fix CLI to be applied. Only the devices for which a fix CLI is available can be selected. Click Next.
Preview Fix Commands	
Preview Fix Commands	Select a violation to view the respective CLI for the devices. If two or more options are selected, the CLI is appended. To schedule a fix job, click Next.
Schedule	
Schedule	Schedule to the fix job. The details of the fix job can be viewed from Compliance Audit > Jobs . The job type is Compliance-Fix

You can view the status of a fix job after the job completes. Click the hyperlinked status to view the results of the fix job.

Global Settings and Administration

This topic contains the following sections:

- [Change Configuration Management Global Settings, page 4-61](#)
- [Change Image Management Global Settings, page 4-66](#)
- [Check the Processes, page 4-68](#)
- [Manage Jobs, page 4-68](#)
- [User Authentication and Authorization, page 4-69](#)

Change Configuration Management Global Settings

To open the Configurations global settings page, choose **Configurations > Settings**. [Table 4-8](#) lists all of the global settings you can configure for Configuration Management.

The backup settings you enter here do not affect the manual backups you can perform by choosing **Configurations > Backup**. The backups you perform from that page and the backups you configure on this Settings page are completely independent of each other.



Note

Make sure that the configuration change detection schedule does not conflict with purging, since both processes are database-intensive.

Table 4-8 Configuration Archive Global Settings

Field	Description
Export Settings	
Server Name	DNS-resolvable server name. Note CCM supports export servers with IPv4 or IPv6 address.
Location	The full pathname of the directory to which Prime Network should copy the file on the server specified in the Server Name field.
Username	The login username that Prime Network should use when connecting to the server specified in the Server Name field.
Password	The login password that Prime Network should use when connecting to the server specified in the Server Name field.
Export Protocol	Default export protocol that Prime Network should use when exporting configuration files to another server. The choices are FTP and SFTP. The default is FTP. You can override this protocol while scheduling an export job, if required.
Archive Purge Settings	
Minimum Versions to Retain	Minimum number of versions of each configuration that should be retained in the archive (default is 2).
Maximum Versions to Retain	Maximum number of versions of each configuration that Prime Network should retain (default is 5). The oldest configuration is purged when the maximum number is reached. Configurations marked “do not purge” are not included when calculating this number.

Table 4-8 Configuration Archive Global Settings (continued)

Field	Description
Minimum Age to Purge	Age (in days) at which configurations should be purged (between 5-360).
Configuration Change Purge Settings	
Purge Change Logs after	The age in days at which configuration change notifications (Change Logs) that are sent by devices should be purged. The default is 30 days and the range is 5-360.
Global Settings	
Transport Protocol	<p>Default transport protocol that Prime Network should use when copying configuration files to and from a device. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. Note the following:</p> <ul style="list-style-type: none"> The TFTP source interface on the devices must be able to reach the unit. Otherwise, the configuration management jobs that require TFTP may fail. To use SFTP/SCP for config transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS XR devices, you need to configure the device with K9 security (k9sec) enabled images such that the SSH server is up and running on the device.
Enable Periodic Config Backup	<p>Detect ongoing configuration changes by performing a periodic collection of device information. Use this method if configurations change frequently and those changes are not important to you. CM compares the timestamp for the last configuration change on the archived version with the timestamp on the newer version. If they are different, CM backs the new file to the archive immediately. By default, this is not enabled.</p> <p>You can set up an interval in the range of 1-100 hours. Default value is 72 hours.</p> <p>Note This CM collection is independent of the Prime Network inventory collection.</p>
Enable Periodic Sync for Out of Sync Devices (72 Hours)	(For Cisco IOS only) Enables automatic synchronization of the out-of-sync devices on a periodic basis. Prime Network adds a device to the list of out-of-sync devices whenever the latest version of the startup configuration is not in sync with the latest version of the running configuration file on the device.
Periodic Export Options	
Enable Periodic Config Export	<p>Allows CM to export archived configurations periodically to the export server. You can set up an interval in the range of 1-100 hours to export the archived configurations. The default value for export interval is 24 hours. You can also specify the start time for the periodic export operation.</p> <p>If there are no configuration changes i.e. if the archived configuration is available in the export server, choose one of the following options to indicate how the export job should be performed:</p> <ul style="list-style-type: none"> Export configuration file will all configuration—Overwrite the existing configuration on the export server. Do not export configuration file—Skip configuration export. Export configuration file with reference to previous configuration file—Create a configuration file with only a reference to the file having the actual configuration. <p>Refer to Configuration Export File Type for Device Families, page 4-66, to know more about the type of configuration files exported for different devices.</p>

Table 4-8 Configuration Archive Global Settings (continued)

Field	Description	
Enable Initial Config Syncup	<p>Allows CM to fetch the configuration files from the network devices and archive it whenever a new device is added to Prime Network. If this setting is enabled:</p> <ul style="list-style-type: none"> CM performs the configuration file fetch operation whenever the Prime Network gateway is restarted. The Disable Initial Config Syncup on Restart check box is enabled by default to prevent network device performance issues on subsequent Prime Network gateway restarts. <p>To preserve this setting such that CM fetches the configuration files from network devices on Prime Network gateway restarts, you must uncheck the Disable Initial Config Syncup on Restart check box after enabling the Enable Initial Config Syncup option.</p> <p>Note The “sync up” described here pertains to making sure the archive correctly reflects the network device configurations. This is different from the CM Synchronize operation, where devices are checked to make sure their running and startup configurations are the same.</p> <p>This “sync up” is required in order for Prime Network to populate the Configuration Sync Status dashlet (on the dashboard).</p>	
	Disable Initial Config Syncup on Restart	Check the check box to set Enable Initial Config Syncup to its default setting (not enabled) if Prime Network restarts.
Enable Event-Triggered Config Archive	<p>Detect ongoing configuration changes by monitoring device configuration change notifications. This setting also controls whether Prime Network populates the Configuration Changes in the Last Week and the Most Recent Configuration Changes dashlets (on the dashboard).</p> <p>Use this method if you consider every configuration file change to be significant. When a notification is received, CM backs up the new running configuration file to the archive using one of the following methods.</p> <p>Note If you are using event-triggered archiving, you should also make sure that exclude commands are properly configured. Exclude commands are commands that Prime Network ignores when comparing configurations, and they are controlled from the Settings page. Using this mechanism eliminates unnecessary file backups to the archive.</p>	
	Sync archive on each configuration change	Upon receiving a change notification from a device, immediately backs up the device configuration file to the archive.
	Sync archives with changed configurations every ____ hours and ____ minutes	Upon receiving a change notification from a device, queue the changes and backs up the device configuration files according to the specified schedule.

Table 4-8 Configuration Archive Global Settings (continued)

Field	Description
Device Access Credentials	<p>For enhanced security, and to prevent unauthorized access to devices, you might be asked to enter device credentials. This option is enabled if, from the Prime Network Administration > Global Settings > Security Settings > User Account Settings > Execution of Configuration Operations, you checked the option Ask for user credentials when running configuration operations. By default, the device credentials field is populated with the default VNE credentials. You must change the credentials to the device credentials before you save the settings. System jobs will fail, if the credentials entered are incorrect. If you checked the option Ask for user credentials when running configuration operations from Prime Network Administration, and did not change the settings from the Settings page after making the change, all system jobs that are scheduled to run will fail.</p> <p>If the option Ask for user credentials when running configuration operations (from Prime Network Administration) is not enabled, the default VNE credentials are used. Also, if device credentials are entered in the Settings page, and the option Ask for user credentials when running configuration operations is not enabled from Prime Network Administration GUI, the device credentials you have entered in the Settings page are ignored and the default VNE credentials are used.</p>
Restore Mode Settings	
Restore Mode	<p>Mode for restoring configuration files to a device:</p> <ul style="list-style-type: none"> • Overwrite—Prime Network overwrites the existing configuration on the device with the file you selected from the archive. Check the Use Merge on Failure check box to restore configuration files in merge mode, if overwrite mode fails. • Merge—Prime Network merges the existing running or startup configuration on the device with the configuration present in the version you selected from the archive.
E-mail Settings	
SMTP Host	SMTP server to use for sending e-mail notifications on the status of configuration management jobs to users. If an SMTP host is configured in the Image Management Settings page, the same value will be displayed here by default. You can modify it, if required.
E-mail Id(s)	<p>E-mail addresses of users to send a notification to after the scheduled job is complete. For two or more users, enter a comma-separated list of e-mail IDs. For example:</p> <p>xyz@cisco.com,abc@cisco.com</p> <p>The e-mail IDs configured here will appear by default while scheduling the configuration management jobs. However, you can add/modify the e-mail IDs then.</p>
SMTP Port	SMTP port ID to connect to the host server. The default port is 25.
Email Option	<p>Choose from the following options to specify when you want to send an e-mail notification for CM jobs:</p> <ul style="list-style-type: none"> • All—To send a notification e-mail irrespective of the job result. • Failure—To send a notification e-mail only when the job has failed. • No Mail—Do not send a notification e-mail on the job status. <p>The selected option will appear by default while scheduling CM jobs. However, you can modify the option then.</p>

Table 4-8 Configuration Archive Global Settings (continued)

Field	Description
Exclude Commands	
(Device Selector)	Selected devices to which the exclude commands should be applied (that is, the commands will not be considered when comparing any type of device configuration files). The current selection is highlighted in green. All exclude commands applied to that selection will be listed below the device selector. See Notes on Exclude Commands, page 4-65 .
Category Commands	Comma-separated list of commands to be excluded when comparing device configurations for any devices in this category (for example, all Cisco routers)
Series Commands	Comma-separated list of commands to be excluded when comparing device configurations for any devices in this series (for example, all Cisco 7200 series routers)
Device Commands	Comma-separated list of commands to be excluded when comparing device configurations for any devices of this same device type (for example, all Cisco 7201 routers)

Notes on Exclude Commands

Exclude commands are inherited; in other words, if three exclude commands are specified for Cisco routers, all devices in any of the Cisco router families will exclude those three commands when comparing configuration files.

**Caution**

Exclude commands configured for a device family (such as Cisco 7200 Routers) will be applied to all device types in that family (Cisco 7201, Cisco 7204, Cisco 7204VXR, and so forth).

When you are working in the Exclude Commands GUI, your current selection will be highlighted in green. All exclude commands applied to that selection will be listed below the device selector. When Prime Network compares the router configuration files, it will exclude all of the commands listed in the Device Commands field. If a series is selected (example, Cisco 7200 Series), the commands listed in the Series Commands field will be excluded and so on.

The following procedure describes how to configure exclude commands.

-
- Step 1** Choose **Configurations > Settings**.
- Step 2** In the Exclude Commands area, navigate and choose one of the following (your selection is highlighted in green):
- A device category
 - A device series
 - A device type
- Step 3** Enter a comma-separated list of commands you want to exclude when comparing configuration files for that device category, series, or type. You can also edit an existing list of commands.
- Your entries change to red until they are saved, and all affected device types, series, or categories are indicated in bold font.
- Step 4** If you want a device type to ignore the parent commands (that is, the series and category commands), check the **Ignore Above** check box.
- Step 5** Click **Save** to save your changes.
-

Configuration Export File Type for Device Families

The following table provides the types of configuration files exported for different types of devices.

Device Type	Configuration File Exported	Condition(s)
Cisco IOS device	Only the latest running configuration	If there is no running version, the latest startup configuration is exported
Cisco IOS XR device	Latest running and startup configuration	None
Cisco ASR 5000 series devices	Latest running configuration	If there is no running version, boot configuration is NOT exported
Cisco 7600 device with ACE card	Latest running configuration	If there is no running version, the latest startup configuration is exported
Cisco Nexus device	Latest running configuration	If there is no running version, the latest startup configuration is exported

Change Image Management Global Settings

To open the Image Management global settings page, choose **Images > Settings**. [Table 4-9](#) lists all of the global settings you can configure for Image Management.

Table 4-9 Image Management Global Settings


Field	Description
Transfer Protocol	<p>Default transfer protocol to use when copying images to and from a device. This setting can be overridden when creating a distribution job (for example, if you know a device does not support the default protocol). FTP and TFTP are unsecured.</p> <ul style="list-style-type: none"> The TFTP source interface on the devices must be able to reach the unit. Otherwise, the image management jobs that require TFTP may fail. To use SFTP/SCP for image transfers from a device to a unit, you need to ensure that an SSH server is configured and running on the device, such that the device acts as a server and the unit as a client during the transfer. For Cisco IOS XR devices, you need to configure the device with K9 security (k9sec) enabled images such that the SSH server is up and running on the device. (Cisco IOS XR devices use SFTP, and Cisco IOS devices use SCP).
Flash Properties	In case of insufficient memory, use the Clear Flash option (under Flash Properties). This deletes any one file (other than the running image) and recovers the disk space occupied by the file. This procedure is repeated until adequate space is available in the selected flash.
Warm Upgrade	<p>If Warm Upgrade is checked, a Cisco IOS image can read in and decompress another Cisco IOS image and transfer control to this new image. This functionality reduces the downtime of a device during planned Cisco IOS software upgrades or downgrades. This can be overridden when creating the job.</p> <div>  <p>Note You can perform a warm upgrade only on Cisco IOS devices 12.3(2)T or later, such as 12.4T, 15.0, 15.1T, and for ISR 800/1800/2800/3800 series and 1900/2900/3900 series.</p> </div>

Table 4-9 *Image Management Global Settings (continued)*

Field	Description	
File Locations	Full pathname of directories where images are stored when they are being imported into the Prime Network image repository, or when they are being transferred out of the repository to devices. New directories must be empty and have the proper permissions (read, write, and execute permissions for users).	
	The entries must be full pathnames. In the following default locations, PRIME_NETWORK_HOME is the Prime Network installation directory, normally /export/home/network-user; where network-user is the operating system user for the Prime Network application and an example of network-user is network39.	
	Staging Directory	Location where images from the Prime Network image repository are placed before transferring them out to devices. The default is PRIME_NETWORK_HOME/NCCMComponents/NEIM/staging/.
	Storing Directory	Location where images from an outside source are placed before importing them into the Prime Network image repository (from Cisco.com, from existing devices, or from another file system). The default is PRIME_NETWORK_HOME/NCCMComponents/NEIM/images/.
External Server Details	Details about external server from which images can be imported into repository.	
	Server Name	IP address of the external server (IPv4 or IPv6 addresses supported).
	Image Location	Path where the image is located on the server.
	User Name	Username to access the external server.
	Password	Password to access the external server.
	SSH Port	SSH port ID to connect to the server.
E-mail Settings	Settings for automatic e-mail notifications about the status of jobs.	
	SMTP Host	SMTP server to use for sending e-mail notifications on the status of image management jobs to users. If an SMTP host is configured in the Configuration Management Settings page, the same value will be displayed here by default. You can modify it, if required.
	E-mail Id(s)	E-mail address of the user to send a notification to after the scheduled job is complete. For two or more users, enter a comma-separated list of e-mail addresses. For example: xyz@cisco.com,abc@cisco.com The e-mail IDs configured here will appear by default while scheduling the image management jobs. However, you can add/modify the e-mail IDs then.
	SMTP Port	SMTP port ID to connect to the host server. The default port is 25.
	Email Option	Controls when e-mail notifications for NEIM jobs are sent (can be overridden when creating the job): <ul style="list-style-type: none"> All—Send a notification irrespective of the job result. Failure—Send a notification e-mail only when the job has failed. No Mail—Do not send a notification e-mail on the job status.

Table 4-9 *Image Management Global Settings (continued)*

Field	Description	
Proxy Settings	Details about proxy server to use when importing images from Cisco.com	
	HTTP Proxy	HTTP proxy server to use for downloading images from Cisco.com.
	Port	Port address to use for downloading images from Cisco.com.
Vendor Credentials	Usernames and passwords that can be used to download images from Cisco.com. (See the procedure described in Check the Processes, page 4-68)	

Check the Processes

CCM runs on AVM 77. To check, start, stop, or restart the process, use the following commands:

```
dmctl status
dmctl start
dmctl stop
dmctl restart
```

Manage Jobs

Prime Network redirects you to the Jobs page whenever a CM or image management job is scheduled to run immediately. When a job is created, Cisco Prime Network assigns it a job specification ID and attaches a time stamp, indicating when the job was created. Only the job creator and users with Administrator privileges can change the job settings.

Prime Network also facilitates automatic e-mail notification of the status of the CM and NEIM jobs upon completion based on the e-mail option you set up in the configuration and image management settings. The notification is sent to a list of e-mail IDs configured either in the settings page or while scheduling the job.

Keeps these items in mind when managing jobs:

- All jobs are scheduled based on the server time.
- If you choose two or more jobs and click Reschedule, the option defaults to 'Start as Soon as Possible.' To view the original time and then reschedule, choose only one job and click Reschedule.
- Job properties cannot be edited; you must delete the old job and create a new one.
- Jobs are persisted even if the gateway server is restarted.
- Only the job creators and users with Administrator and Configurator privileges can perform the actions provided on the Jobs page (suspend, resume, reschedule, cancel, delete, refresh).
- Configuration and image management jobs fail under the following conditions:
 - If the device is not under the scope of the user to perform the config or image operation.
 - If the user is not authorized to perform the config or image operation.
 - For Cisco CPT devices, if the device is not in Cisco IOS mode.
- Running jobs cannot be suspended or cancelled; you must let them complete.
- System-generated jobs cannot be modified. To change the settings, go to **Settings > Global Settings > Period Export Options**, and modify the options accordingly.

- Cancel stops all future instances of a job. To stop a job and resume it later, use Suspend and Resume
- To view the history of a job, choose a job and view the history from the History tab at the bottom of the page. You cannot view history of multiple jobs at the same time; choose only one job at a time.

Messages that can be used for debugging are saved in
PRIME_NETWORK_HOME/XMP_Platform/logs/JobManager.log.

User Authentication and Authorization

User Authentication and Authorization

CCM uses the security methods employed by Prime Network. These are described in the [Cisco Prime Network 4.0 Administrator Guide](#)



Note

If authentication fails, check the status of AVM 77 (XMP runtime DM) and Prime Network using Cisco Prime Network Administration. Cisco Prime Network Administration displays AVM 77 only when CCM is installed. For information on how to use Cisco Prime Network Administration, see the [Cisco Prime Network 4.0 Administrator Guide](#).

The GUI-based functions and required roles are listed in [Table 4-10](#). Note that these functions do not perform any actions on devices.

Table 4-10 GUI-Based Access Roles Required to Use CCM

Function	Viewer	Operator	OperatorPlus	Configurator	Administrator
Dashboard					
Access top families	X	X	X	X	X
Configuration Management					
Delete files from archive ¹				X	X
Add, change, delete archive file labels ¹				X	X
Add change, delete archive file comments ¹				X	X
Export files from archive ¹				X	X
Image Management					
View images in repository	X	X	X	X	X
Add images to repository				X	X
Delete images from repository				X	X
Global Tasks					
View jobs	X	X	X	X	X
Administer jobs (suspend, delete, and so forth)				X	X
Change settings				X	X
Compliance Audit					
Creating policies	X	X	—	—	—

Table 4-10 GUI-Based Access Roles Required to Use CCM (continued)

Function	Viewer	Operator	OperatorPlus	Configurator	Administrator
Creating policy profiles	X	X	X	X	—
Executing audit job	X	X	X	X	—
Viewing audit job results	X (user's jobs)	X (user's jobs)	X (OperatorPlus jobs)	X (Configurator jobs)	—
Executing a Fix job Note To execute a fix job, the device-level role of the user must be Configurator or Administrator. The role of the user for a device overrides the role of a user on Prime Network.	X	X	—	—	—
Viewing the fix job results	X	X	—	—	—
Configuration Audit					
Define configuration policies				X	X
Schedule configuration audit				X	X
View configuration audit jobs and audit results			X	X	X
Managing Device Groups					
Create device groups	X	X	X	X	X
Edit device group details				X	X
Delete device groups				X	X

1. Configuration files are filtered according to the device scope of a user.

Table 4-11 lists all of the CCM functions that are that filtered to only show devices in the device scope of a user, along with the role required to perform any functions on those devices.

Table 4-11 Device Scope-Based Roles Required to Use CCM

Function	Viewer	Operator	Operator Plus	Configurator	Administrator
Dashboard					
Access configuration sync status ¹	X	X	X	X	X
Access configuration changes in the last week ¹	X	X	X	X	X
Access most recent configuration changes ¹	X	X	X	X	X
Configuration Management					
View files in archive ¹	X	X	X	X	X

Table 4-11 *Device Scope-Based Roles Required to Use CCM (continued)*

Function	Viewer	Operator	Operator Plus	Configurator	Administrator
Compare files in archive	X	X	X	X	X
Synchronize configurations				X	X
Back up (copy) files from devices to archive			X	X	X
Restore files from archive to devices				X	X
Edit configuration files before restoring them to devices				X	X
View configuration change logs	X	X	X	X	X
Image Management					
Distribute images				X	X
Activate and deactivate images				X	X
Commit image changes				X	X
Rollback images				X	X
Managing Device Groups					
Create device groups				X	X
Edit device group details				X	X
Delete device groups				X	X
Compliance Audit					
Creating policies	X	X	—	—	—
Creating policy profiles	X	X	X	X	—
Executing audit job	X	X	X	X	—
Viewing audit job results	X	X	X	X	—
Executing a Fix job	—	—	—	X	X
Viewing the fix job results	X	X	—	—	—
Configuration Audit					
Define configuration policies				X	X
Schedule configuration audit				X	X
View configuration audit jobs and audit results			X	X	X

1. Although users can view configuration files for devices in their scopes, the actions they can perform on those configuration files are controlled by the GUI-based access roles in [Table 4-10](#).

For information on how Prime Network performs user authentication and authorization, including an explanation of user access roles and device scopes, see the [Cisco Prime Network 4.0 Administrator Guide](#).

