Introduction to 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 Network Element Image Management (NEIM) function.

These topics provide an overview of the features that Change and Configuration Management provides, some initial setup tasks you must perform, and how to start the GUI.

- Features of Cisco Prime Network Change and Configuration Management, page 1-1
- Setup Tasks to Perform Before Using Change and Configuration Management, page 1-6
- Launching the GUI and GUI Basics, page 1-9

Features of Cisco Prime Network Change and Configuration Management

The following topics provide an introduction to the features of Change and Configuration Management:

- Configuration Management, page 1-2
- Network Element Image Management, page 1-2
- Supporting Functions, page 1-3
- Supported Devices, page 1-5
- SDR Support, page 1-5
- IPv6 and Firewall Support, page 1-5
- ACE Module Support (For Cisco 7600 Series Routers only), page 1-5
Configuration Management

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

- Changes are detected when doing the periodic collection of device configurations; this is called periodic archiving. 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.
- Changes are detected 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 1-7).

Configuration file copies are stored in a configuration archive (the CM archive), from which you can compare configurations, restore configuration files to devices, edit the configuration files before restoring them, and for Cisco IOS devices, synchronize running and startup configuration files. Configuration files in the archive are stored in readable format, as received from the device. Significant configuration files can be labelled using the labeling facility of CM, and you can mark configurations so that purging them is prevented by CM.

For information on how to use the configuration management GUI, see Managing Configurations, page 3-1.

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. For information on Change Logs, see:

- Configuration Changes in the Last Week, page 2-3, which describes the change logs that are displayed in the dashboard.
- Viewing Configuration Change Logs, page 3-24, which describes the change logs that are displayed in the Configurations Change Logs page.

Note: These Change Logs are different from the logs that record configuration and image management activities. Configuration and image management logs are described in Log Files, page 7-17.

Network Element Image Management

Network Element Image Management (NEIM) ensures rapid, reliable software upgrades, and automates the steps associated with upgrade planning and monitoring. 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. 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 where images are stored in binary format.

For information on how to use the NEIM GUI, see Managing Software Images, page 4-1.
Supporting Functions

Change and Configuration Management provides the following functions:

- Job Management, page 1-3
- Automatic E-mail Notifications, page 1-3
- Warm Upgrade (For Cisco IOS only), page 1-3
- User-Defined Device Grouping, page 1-4
- FTP support for Cisco IOS devices, page 1-4
- CM and NEIM Settings, page 1-4

Job Management

A job management GUI interface allows you to schedule the CM and NEIM tasks to happen immediately or at a future time. The GUI also provides additional details on each job, including a results report with details about all operations that were part of a job.

For information on how to use the job GUI, see Managing Change and Configuration Management Jobs, page 6-1.

Automatic E-mail Notifications

Change and Configuration Management facilitates automatic e-mail notification of the status of the CM and NEIM jobs upon completion. You can configure the e-mail address of the recipients either in the settings page or while scheduling the job. You can also specify when you want to send the e-mail by using the following options:

- 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.

A notification e-mail is sent to the specified users with details such as job ID, job type, job result—Success or Partial Success, job scheduled and completion date and time, owner, and comments, if any. The e-mail also provides the list of successful and unsuccessful tasks, if any with the device name and a summary.

Note

A notification e-mail is sent only if SMTP host and port are configured in the CA or NEIM settings. For more information, see Configuring Global Settings for Configuration Management, page 7-1 and Configuring Global Settings for Image and Package Management, page 7-9. Automatic e-mail notification of job results is not applicable for jobs pertaining to download of images from file system or Cisco.com.

Warm Upgrade (For Cisco IOS only)

The Warm Upgrade feature provides the capability for a Cisco IOS image to read and decompress another Cisco IOS image and then transfer control to this new image. This functionality reduces the downtime of a device during planned Cisco IOS software upgrades or downgrades.

Prior to the Warm Upgrade feature, a Cisco IOS image normally transfers control to ROM monitor mode (ROMMON) to perform a Cisco IOS software upgrade or downgrade. ROMMON, along with the help of the boot loader image, carries out the required upgrade or downgrade procedures. While this process is in progress, the networking device will be down.
With the introduction of the Warm Upgrade feature, packet forwarding will continue while the new Cisco IOS image is read and decompressed. The device is down only when the current image is overwritten with the new image, and the new image loads and reconfigures the operating system.

Change and Configuration Management allows you to activate the warm upgrade feature while scheduling image distribution and activation.

**User-Defined Device Grouping**

Change and Configuration Management supports user-defined device grouping. You can create a static or dynamic group with a specific set of devices, so all CM and NEIM operations can be performed for the devices collectively with ease.

For more information on user-defined device grouping, see Managing User-Defined Device Groups, page 5-2.

**FTP support for Cisco IOS devices**

For Cisco IOS devices, Change and Configuration Management supports FTP mode for all config and image transfers. You need to configure the username and password for the unit that manages the device by using the following commands:

```
ip ftp username username
ip ftp password password
```

If you have not configured these commands, the FTP transfers will fail.

However, adding FTP credentials of the unit to the device may not be safe if the network is not secure. Hence, 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.
- Restrict FTP configuration such that the “Prime Network Unit User” has read-write access only to the $PRIME_NETWORK_HOME/tftp directory ($ANAHOME/tftp directory) and hence does not have access to unwanted files outside the home directory.

**CM and NEIM Settings**

Both CM and NEIM have their own Settings pages to control the global and administrative behavior of the CM and NEIM features.

- For CM, this includes the default transport protocol, purging policy, export settings, configuration backup, sync, and restore settings, e-mail settings, and exclude commands (commands not to be considered when Change and Configuration Management compares configurations). For more information, see Configuring Global Settings for Configuration Management, page 7-1.
- For NEIM, this includes the default transfer protocol, flash and warm upgrade settings, staging and storing directories, external server settings, e-mail settings, proxy settings, and vendor credentials. For more information, see Configuring Global Settings for Image and Package Management, page 7-9.

In addition, user actions are restricted according to user access role and assigned device scopes. Users must have Configurator privileges on a device (through their device scope) to perform any of the advanced CA and NEIM tasks. More details are provided in Change and Configuration Management Administration, page 7-1.
Chapter 1  Introduction to Change and Configuration Management

Features of Cisco Prime Network Change and Configuration Management

Supported Devices

For a list of the device series and software supported by Change and Configuration Management, see Supported Devices for Change and Configuration Management, page A-1.

SDR Support

Change and Configuration Management provides Secure Domain Router (SDR) support. SDRs perform routing functions in the same manner as a physical router, but share resources with the rest of the system. Prime Network VNE layer identifies if a given Cisco IOS XR device is an SDR parent (owner) or child (non-owner). Based on this, the following CM and NEIM operations are supported for SDRs:

- Package management life cycle in parent and child SDRs.
- Commit and rollback operations in parent SDRs.
- Collection of running and admin configurations in parent SDRs.
- Collection of only running configuration in child SDRs.

IPv6 and Firewall Support

CM and NEIM functions run smoothly on a combination of network and devices with IPv6 addresses. Both the device and the unit must be configured with an IPv6 address to work. Note the following:

- IPv6 support is not available for Cisco IOS XR devices and Cisco Nexus 5000 and Cisco Nexus 7000 series devices.
- For Cisco IOS devices with IPv6 address, the CM and NEIM operations will work only in FTP mode.

The NEIM and CM functions run on units and gateway in a deployment environment in which the units are located behind firewalls and possibly Network Address Translation (NAT). You need not open special ports for the units to initiate communications. However, if a gateway is behind a firewall, that firewall will need ports opened for communications to the gateway. 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.

ACE Module Support (For Cisco 7600 Series Routers only)

You can perform CM and NEIM operations at the module level for Cisco 7600 series routers with Application Control Engine (ACE) cards. Prime Network provides the following support for Cisco 7600 series routers with ACE cards:

- Configuration Management—Configuration files are collected, archived, and displayed for the ACE cards as part of the parent Cisco 7600 series device.
- Image Management—Upgrade and downgrade of images are supported for the ACE cards.

Note

To perform the configuration archive operations (backup and restore) on the ACE module, you need to use the same credentials used for accessing the parent Cisco 7600 supervisor module. Change and Configuration Management supports only TFTP for configuration and image transfers on ACE cards.
Setup Tasks to Perform Before Using Change and Configuration Management

Before using Change and Configuration Management, perform the following prerequisite tasks:

- Prime Network Setup Tasks, page 1-6
- Configuration Management Setup Tasks, page 1-7
- NEIM Setup Tasks, page 1-8

Prime Network Setup Tasks

Verify the following:

1. Verify that Change and Configuration Management is installed. The installation process is described in *Cisco Prime Network 3.8 Installation Guide*. Change and Configuration Management is an optional installable Prime Network component that can be installed at a later time. The guide includes information about supported browsers, ports that must be available, and so forth.

To check if Change and Configuration Management 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, Change and Configuration Management is installed and running.

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

2. Make sure that pop-up windows are enabled on the Firefox and Internet Explorer browsers. For instructions, see the *Cisco Prime Network 3.8 Installation Guide*.

3. For NEIM, verify that the gateway has sufficient space for the storing and staging directories (see Configuring Global Settings for Image and Package Management, page 7-9).

4. 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 3.8 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.)

5. 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 3.8 Administrator Guide*.

6. SNMP read-write community in Cisco Prime Network Administration must match that on the devices.

7. Ensure reachability from Prime Network units to devices and vice versa.

8. Prime Network AVM 11 (gateway), AVM 77 (Prime Network web server), and AVM 83 (Prime Network TFTP server) must be up and running. To use AVM 83 for Change and Configuration Management, make sure the server port 69 is free and available. For more information, see the Cisco Prime Network Server, TCP, and UDP Ports section in the *Cisco Prime Network 3.8 Installation Guide*.

9. Make sure you have performed all of the device configuration prerequisites for adding VNEs. These commands are described in the *Cisco Prime Network 3.8 Administrator Guide*.
Chapter 1  Introduction to Change and Configuration Management

Setup Tasks to Perform Before Using Change and Configuration Management

Configuration Management Setup Tasks

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 (described in Configuring Global Settings for Configuration Management, page 7-1).

1. Configure the transport protocol that Prime Network will use between the device and the gateway. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. Note the following:
   - 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.

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.

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 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. This will minimize server workload.

      **Note** The periodic setting is recommended.

      If every change is considered significant, use event-driven backups.

   c. For event-driven archiving, should information be copied to the archive immediately upon receiving a change, or should changes be queued and then copied at a certain interval (every 1-24 hours)? 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.

5. Configure when configuration files should be purged from the archive. You should consider:
   - How big are the configuration files?
   - How often are changes made to devices?

6. Consider exporting files from the archive on a regular basis so you can free up disk space while keeping a permanent record of historical archives. You can export files from the GUI. To use this function, set up the export settings. You will need the server name, full pathname, username, and password.

7. Specify the default mode of restoring configuration files to the devices.

8. Configure the SMTP server and e-mail IDs to send notifications on the status of configuration management jobs to users.
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).

**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

The following are the NEIM prerequisites, all of which are controlled by the Image Management Settings page (described in Table 7-4 Configuring Global Settings for Image and Package Management, page 7-9).

1. Configure the transport protocol that Prime Network will use between the device and the gateway. The options are TFTP, SFTP/SCP, and FTP. The default is TFTP. 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. 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 `network38`).

3. Use the **Clear Flash** option to clear the disk space on a storage location before distributing the image or package if there is insufficient memory in the storage device.

4. Enable the warm upgrade facility to reduce the downtime of a device during planned Cisco IOS software upgrades or downgrades.

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). 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 `network38`).

6. 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.

7. Configure the SMTP server and e-mail IDs to send notifications on the status of image management jobs to users.

8. Configure the proxy server details to use while importing images to the archive from Cisco.com.

9. If you plan to download files from Cisco.com, configure the necessary vendor credentials to connect to Cisco.com.
Launching the GUI and GUI Basics

These topics explain the following:
- How To Launch the Change and Configuration Management GUI, page 1-9
- Basics of the Change and Configuration Management GUI, page 1-12

How To Launch the Change and Configuration Management GUI

You can launch the Change and Configuration Management GUI by entering the server name in a web browser or by launching the GUI from Cisco Prime Network Vision or Cisco Prime Network Web Server. By default, the GUI session is terminated after 30 minutes of inactivity and you will be redirected to the login page.

Change and Configuration Management runs on AVM 77 (Prime Network web server), so that AVM must be running. To check, start, stop, or restart the process, use the following commands:

dmctl status
dmctl start
dmctl stop
dmctl restart

Prime Network Change and Configuration Management requires some additional time to initialize after the Prime Network installation, or if Prime Network has been restarted using the dmctl command (which is described in the Cisco Prime Network 3.8 Administrator Guide). If you cannot log into the browser and you see an error message related to the Tomcat Server, the problem is this delay. Retry the operation after a few minutes.

Security Certificate Exception

When you launch the Change and Configuration Management GUI for the first time, the browser displays a security certificate error indicating that the connection is untrusted. To launch the Change and Configuration Management GUI, you must proceed further and confirm the Secure Socket Layer (SSL) security certificate exception within 90 seconds; otherwise the connection will be timed out.

Launch the GUI from a Web Browser

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

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

where:
- gateway-IP is the IP address for the Prime Network gateway server.
- 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. For more information, see Enabling and Disabling Port 8080 Manually, page 1-10.

You can log in using the same username and password that you use to log into any of the Prime Network clients.

For information on supported browsers and minimum screen resolution, see the Cisco Prime Network 3.8 Installation Guide.
Enabling and Disabling Port 8080 Manually

To enable port 8080 manually:

**Step 1**
Run the following commands:
```
$ cd $NCCM_HOME/scripts/
$ ./nccmHTTP.csh enable
```

**Step 2**
Stop and then start Change and Configuration Management by using the following commands, for the change to take effect:
```
$ dmctl stop
$ dmctl start
```

To disable port 8080 manually:

**Step 1**
Run the following commands:
```
$ cd $NCCM_HOME/scripts/
$ ./nccmHTTP.csh disable
```

**Step 2**
Stop and then start Change and Configuration Management by using the following commands, for the change to take effect:
```
$ dmctl stop
$ dmctl start
```

Launch the GUI from Cisco Prime Network Vision

Cisco Prime Network Vision provides launch points for Change and Configuration Management. You can use the main menu and choose Tools > Change and Config Mgmnt, as shown in Figure 1-1.

**Note**
However, for Internet Control Message Protocol (ICMP) VNEs, you cannot launch Change and Configuration Management from Cisco Prime Network Vision.

For information on the Prime Network Vision GUI, see the Cisco Prime Network 3.8 User Guide.
You can also launch it from a device in a Network Vision List or Map view. This will bring you directly to the CM or NEIM page, and will display contextual information for the device you choose. Figure 1-2 shows what happens when you right-click a device. From here, you can choose Image Mgmt or Config Mgmt.

Figure 1-2  Launching the GUI from Cisco Prime Network Vision—Method 2
Launch the GUI from Cisco Prime Network Web Server

To launch the GUI from the Cisco Prime Network web server, enter the following URL in the address bar, where gateway-IP is the IP address for the Prime Network web server:

https://gateway-IP:8043

The Prime Network web server home page is displayed. Click on the Prime Network Change and Configuration Management hyperlink as shown in Figure 1-3.

Figure 1-3 Launching the GUI from Prime Network Web Server

You can log in using the same username and password that you use to log into any of the Prime Network clients.

For information on supported browsers and minimum screen resolution, see the Cisco Prime Network 3.8 Installation Guide.

Note We recommend that you log out from the Change and Configuration Management GUI before closing the browser, so more users can connect to the application with the same username.

Basics of the Change and Configuration Management GUI

Figure 1-4 shows the Change and Configuration Management 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 1-4 Change and Configuration Management Dashboard

Figure 1-5 shows what is displayed when you choose **Images > Repository**. This is the Prime Network Repository page, which displays the available filters for that page.

You can move between the dashboard, CM, NEIM, and device groups functions by choosing one of them from the top control bar. You can choose the various CM and NEIM functions from the respective drop-down menus on the control bar.

The top right corner provides some GUI controls. From here, you can identify the user who is logged into this session, as shown in Figure 1-6. You can also log out, launch the online help, and get version information about Prime Network Change and Configuration Management.

Sometimes, while using Microsoft Internet Explorer 8.0 or 9.0 with a low system resolution, the buttons on the footer of the content area may not be displayed properly. To overcome this issue, minimize and then maximize the browser.
Prime Network user authentication and authorization information applies to Change and Configuration Management as well. For information on the required access roles to use the GUI features, see User Authentication and Authorization (Access Roles and Device Scopes), page 7-14. For information on how Prime Network performs user authentication, see the Cisco Prime Network 3.8 Administrator Guide.

**Figure 1-6 Change and Configuration Management GUI Controls**

Using Special Characters in the GUI Fields

Change and Configuration Management does not support certain special characters while entering a name or description in the GUI fields.

For all the editable fields in the GUI:
- Valid characters are a-z, A-Z, 0-9, ., -, _
- Invalid characters are `,~,!,@,#,$,%,^, &,*,(,),+,=\,{|},:,;,?,>,<,/
- No leading spaces are allowed.

For the Find string in Device Configuration Viewer, valid characters are a-z, A-Z, 0-9, ‘, “, ~, !, @, %, #, &, ., -, _, {, }, :, ;, >, <, and /.