CHAPTER 7

Change and Configuration Management Administration

These topics provide administrative information on Change and Configuration Management:

- Configuring Global Settings for Configuration Management, page 7-1—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.
- Configuring Global Settings for Image and Package Management, page 7-7—How to use the Image Management Settings page to specify the default transfer protocol, staging and storing locations, and credentials for accessing a vendor website.
- Administration and Security, page 7-11—How Change and Configuration Management 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 Change and Configuration Management by reading Setup Tasks to Perform Before Using Change and Configuration Management, page 1-6.

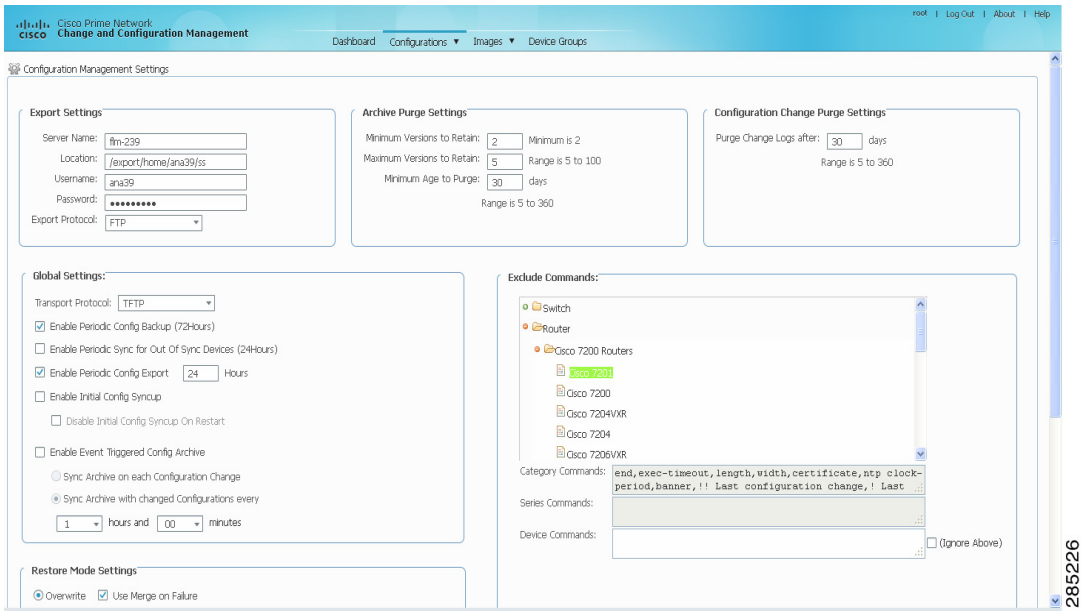
Configuring Global Settings for Configuration Management

These topics explain how to configure:

- Export settings to use when a user wants to export a configuration file to another server.
- Purging policies for change logs and configuration files in the archive. When Prime Network purges the configuration archive, it follows the policies that are defined on this page. These policies are applied to all types of configurations (admin, startup, and running). Configurations that are marked “do not purge” are never purged, regardless of the purging policies. By default, five versions of each file type are retained.
- Global settings including default transport protocol, config sync, export, and backup options, default restore mode, and e-mail settings. If you plan to use event-triggered archiving, you should also make sure that logging is properly configured on devices, as specified in Setup Tasks to Perform Before Using Change and Configuration Management, page 1-6.
- Exclude commands that Prime Network should ignore when comparing configurations.

Figure 7-1 shows the Configuration Management Settings page. You can open this page by choosing **Configurations > Settings**. The red text indicates changes that were made but have not been saved.

Figure 7-1 Configuration Management Settings Page



Export Settings

The Export Settings in Table 7-1 specify the defaults that Prime Network should use when a user exports a file to another server. Files can be exported from the Archives page; see Exporting Configuration Files, page 3-14.

Table 7-1 Export Settings for Configuration Management

Field	Description
Server Name	DNS-resolvable server name. **Note** Change and Configuration Management 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

The Archive Purge Settings in Table 7-2 control when Prime Network should delete files from the CM archive. These settings apply to all types of configuration files (startup, running, and admin). Configurations that are marked “do not purge” are never purged, regardless of the purging policies.

A file that exceeds the allowed age will not be purged if doing so would bring the number of versions below the minimum versions. In other words, if the minimum number of versions that must be in the archive is two, Change and Configuration Management will *not* purge the file even if one of the versions exceeds the allowed age.

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

Table 7-2 Archive Purge Settings for Configuration Management

Field	Description
Minimum Versions to Retain	The minimum number of versions of each configuration that should be retained in the archive. The default is two. This prevents a user from deleting a configuration file if there are only two versions in the archive.
Maximum Versions to Retain	The maximum number of versions of each configuration that Prime Network should retain. The oldest configuration is purged when the maximum number is reached. The default is five. Configurations marked “Do Not Purge” are not included when calculating this number.
Minimum Age to Purge	The age (in days) at which configurations should be purged. The permitted range is 5-360. Prime Network does not purge configuration files unless there are more than two versions of the files in the archive.

Configuration Change Purge Settings

The Configuration Change Purge setting in Table 7-3 controls when configuration Change Logs should be purged from the Prime Network database. These logs contain the configuration changes displayed on the Dashboard and on the Configuration Change Logs page.

Table 7-3 Configuration Change Purge Settings for Configuration Management

Field	Description
Purge Change Logs after	The age (in days) at which configuration change notifications that are sent by devices should be purged. The default is 30 days.

Global Settings

The Global Settings in Table 7-4 control the following:

- Default transport protocol
- When Prime Network should retrieve configuration files from devices and copy them (back them up) to the archive
- When Prime Network should export archived configurations to an export server
- Mode of restoring configuration files to devices

- E-mail IDs to which to send a notification after a scheduled configuration management job is complete

By default, none of the following settings are enabled.

Note The 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.

Table 7-4 Global Settings for Configuration Management

Field	Description
Transport Protocol Global Settings	
Transport Protocol	Default transport protocol that Prime Network should use when copying configuration files to and from a device. The choices are TFTP, SCP/SFTP, or FTP. The default is TFTP.
Configuration Backup Global Settings	
Enable Periodic Config Backup (72Hours)	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. When a change is detected, CM backs the new file to the archive immediately. By default, this is not enabled. **Note** This CM collection is independent of the Prime Network inventory collection.
Enable Periodic Sync for Out of Sync Devices (24Hours)	(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.
Enable Periodic Config Export	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. If there are no configuration changes i.e. if the archived configuration is available in the export server, the periodic export job is skipped.

Table 7-4 Global Settings for Configuration Management (continued)

Field	Description	
Enable Initial Config Syncup	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: • 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. 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. **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. This "sync up" is required in order for Prime Network to populate the Configuration Sync Status dashlet (on the dashboard).	
	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	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). 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. **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. This is addressed in Exclude Commands, page 7-6.	
	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 7-4 Global Settings for Configuration Management (continued)

Field	Description
Restore Mode	Choose from one of the following options to specify the mode of restoring configuration files to devices: • 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.
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)	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: `xyz@cisco.com,abc@cisco.com` 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.
SMTP Port	SMTP port ID to connect to the host server. The default port is 25.
Email Option	Choose from the following options to specify when you want to send an e-mail notification for CM jobs: • 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. The selected option will appear by default while scheduling CM jobs. However, you can modify the option then.

Exclude Commands

The Exclude Commands specify any commands that Prime Network should ignore when comparing device configurations files of any type. Exclude commands are inherited; in other words, if three exclude commands are specified for Cisco routers, all devices is 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. For example, in Figure 7-1, a Cisco 7201 router is selected. 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.

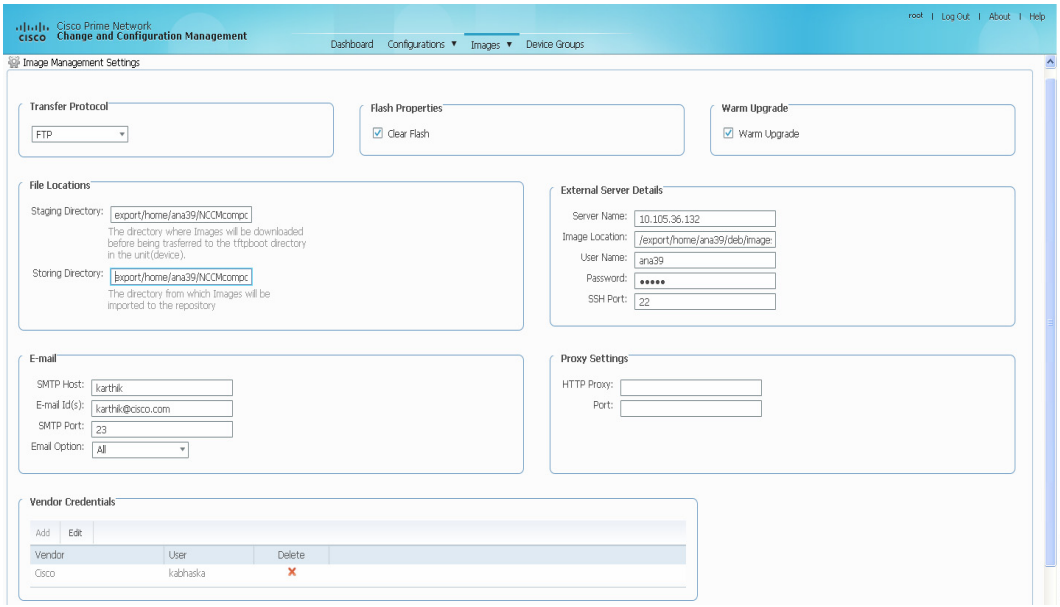
Step 5 Click **Save** to save your changes.

Configuring Global Settings for Image and Package Management

These topics explain how to configure:

Figure 7-2 shows an example of the Image Management Settings page. You can open this page by choosing **Images > Settings**.

Figure 7-2 Image Management Settings Page



Transfer Protocol

The default transfer protocol that Change and Configuration Management should use when copying images to and from a device. Supported protocols are:

- TFTP (unsecured)
- SFTP/SCP (secured; Cisco IOS XR devices use SFTP, and Cisco IOS devices use SCP)
- FTP (unsecured)

You can override this protocol when creating a distribution job (for example, if you know that a device does not support the default protocol).

Flash Properties

You can clear the disk space on a storage location before distributing the image or package if there is insufficient memory in the storage device. Check the **Clear Flash** check box to free the flash memory space for distribution of images or packages.

Warm Upgrade

Cisco Prime Change and Configuration Management provides a warm upgrade facility for Cisco IOS devices, by which one 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. For more information on the warm upgrade feature, see Warm Upgrade (For Cisco IOS only), page 1-3.

If you select this check box, the warm upgrade option is enabled by default for distribution and activation of Cisco IOS images. However, you can override this option while scheduling the distribution and activation jobs.

File Locations

The File Locations settings specify the 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.

If you are creating a new directory, make sure the directory is empty and has 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.

Field	Description	Default Location
Staging Directory	Location where images from the Prime Network image repository are placed before transferring them out to devices.	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).	PRIME_NETWORK_HOME/NCCMComponents/NEIM/images/

External Server Details

You can set up the details of an external server from which you can import images to the Prime Network image repository.

Field	Description
Server Name	IP address of the external server. **Note** Change and Configuration Management supports external servers with IPv4 or IPv6 address.
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

You can set up the SMTP server and e-mail IDs to send automatic e-mail notifications regarding the status of image management jobs to users.

Field	Description
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	Choose from the following options to specify when you want to send an e-mail notification for NEIM jobs: • 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. The selected option will appear by default while scheduling NEIM jobs. However, you can modify the option then.

Proxy Settings

You can set up the proxy server details to use while importing images to the archive from Cisco.com.

Field	Description
HTTP Proxy	HTTP proxy server to use for downloading images from Cisco.com.
Port	The port address to use for downloading images from Cisco.com.

Vendor Credentials

The Vendor Credentials settings specify the usernames and passwords that can be used to download images from Cisco.com. (See the procedure described in Obtaining Cisco.com Login Privileges, page 7-11).

- To add a new user, click **Add** and enter the username and password. (Cisco is the only supported vendor in this release.) The username and password must match those for the Cisco.com account.
- To change the username and password, click **Edit** and enter the new username and password. The new username and password must match those for the Cisco.com account.
- To delete a user, click the delete icon (red **X**) next to the username.

Click **Save**.

Obtaining Cisco.com Login Privileges

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.
```

Administration and Security

These topics address the administration and security aspects of Change and Configuration Management.

Database Information

All device configuration files and repository images are kept in the Prime Network database. Device configuration files are stored in readable format (as received from the device). Software images are stored in binary format.

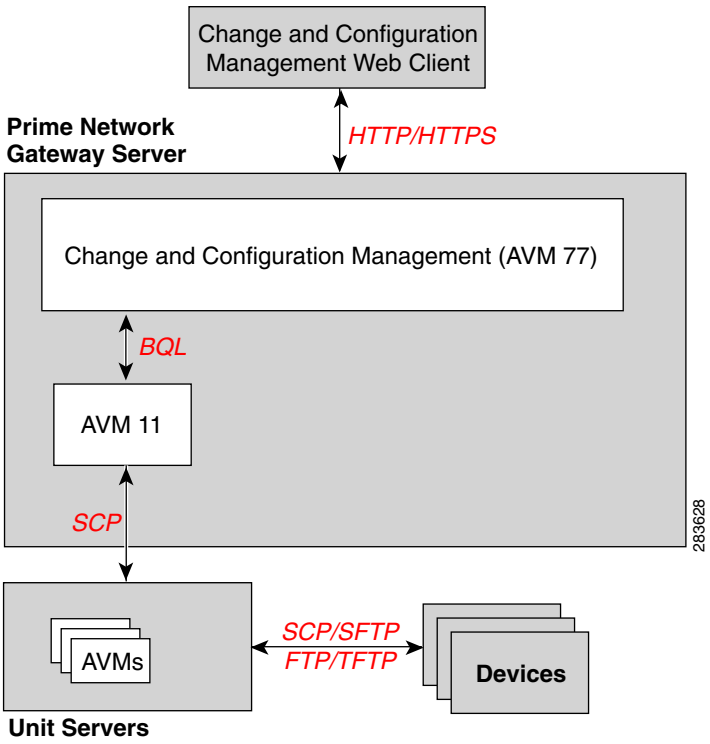
Change and Configuration Management data is stored in the *network-user*_**xmp** schema (where *network-user* is the operating system user for the Prime Network application when it is installed; and an example of *network-user* is network39). For information on how to change the database password, see the *Cisco Prime Network 3.9 Administrator Guide*.

Change and Configuration Management can be installed on a Prime Network installation that uses an encrypted connection to the database, but the connection used by Change and Configuration Management will not be encrypted.

Communication Security

Figure 7-3 provides a simplified illustration of the methods and protocols that Prime Network, Change and Configuration Management, and devices use to communicate with each other. (For information on the Prime Network communication architecture, see the *Cisco Prime Network 3.9 Administrator Guide*.)

Figure 7-3 Communication Security in Change and Configuration Management



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

User Authentication and Authorization (Access Roles and Device Scopes)

Change and Configuration Management performs user authentication and authorization using the methods and rules configured on the Prime Network gateway.

- *User authentication* can be controlled locally (by Prime Network) or externally by an LDAP application. Change and Configuration Management will use the method as it is configured on the gateway.
- *User authorization* is managed according to the *user access roles* and *device scopes* that were assigned to the user when the user account was created on the Prime Network gateway. The user access role determines the actions the user can perform in the Change and Configuration Management GUI. The device scope determines which devices the user can access and manage.

A user can have different access roles: one that controls the GUI-based operations they are allowed to perform, and another that controls the devices they can view and to what degree they can manage those devices. The first is configured when user accounts are created and is called the user access role. The second is configured when a device scope is assigned to the user account.

Here is an example:

- A user may have the OperatorPlus access role which controls all *GUI functions* they can perform. The user would be prevented from configuring the export directory for configuration files because that function requires the Configurator access role. (Note that this function does not perform anything on a specific device.)
- The user may have the Configurator role for the device *scopes* that are assigned to them. That controls all *device-based functions* the user can perform. If the user wanted to distribute a software image to a device in their scope, they would be permitted to do so.

Note The name of the current user is displayed at the top right of the Change and Configuration Management GUI window. See Basics of the Change and Configuration Management GUI, page 1-13, for an example.

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 Change and Configuration Management is installed. For information on how to use Cisco Prime Network Administration, see the *Cisco Prime Network 3.9 Administrator Guide*.

The GUI-based functions and required roles are listed in Table 7-5. Note that these functions do not perform any actions on devices.

Table 7-5 GUI-Based Access Roles Required to Use Change and Configuration Management

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
Managing Device Groups					
Create device groups	X	X	X	X	X

Table 7-5 GUI-Based Access Roles Required to Use Change and Configuration Management

Function	Viewer	Operator	OperatorPlus	Configurator	Administrator
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 7-6 lists all of the Change and Configuration Management 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 7-6 Device Scope-Based Roles Required to Use Change and Configuration Management

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
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

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 7-5.

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 3.9 Administrator Guide*.

Data Purging

To maintain system stability, CM data is purged according to the settings you specify in the Configuration Management Settings page. All other data are purged using to the Prime Network settings and schedule. For information on how Prime Network performs data purging, see the *Cisco Prime Network 3.9 Administrator Guide*.

Checking, Stopping, and Restarting the Change and Configuration Management Processes

Change and Configuration Management runs on AVM 77. To check, start, stop, or restart the process, use the following commands:

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

Log Files

Table 7-7 provides a list of the Change and Configuration Management log files which contain messages that can be used for debugging. PRIME_NETWORK_HOME is the 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).

Table 7-7 Change and Configuration Management Log Files

Log File	Description
PRIME_NETWORK_HOME/Main/logs/77.log	Manages Change and Configuration Management processes in Prime Network
PRIME_NETWORK_HOME/XMP_Platform/logs/ConfigArchive.log	CM activities log file
PRIME_NETWORK_HOME/XMP_Platform/logs/JobManager.log	Job Manager activities log file
PRIME_NETWORK_HOME/XMP_Platform/logs/NEIM.log	NEIM log file
PRIME_NETWORK_HOME/XMP_Platform/logs/NccmGUI.log	Change and Configuration Management GUI log file

Log files are archived and purged according to the settings on the Prime Network gateway. For more information, see the *Cisco Prime Network 3.9 Administrator Guide*.