Using Image Manager

Image Manager is a tool to simplify the distribution and management of images on internal and edge firewall devices in your network. It enables you to:

- Download and maintain a repository of different types and versions of images
- Evaluate images
- Analyze impact of upgrading images to the devices in the network
- Prepare for and plan an upgrade
- Reliably upgrade devices, with sufficient fallback and recovery mechanisms built in to ensure minimal network downtime

This chapter contains the following topics:

- Getting Started with Image Manager, page 70-1
- Working with Images, page 70-7
- Working with Bundles, page 70-11
- Working with Devices, page 70-14
- About Image Updates on Devices Using Image Manager, page 70-18
- Working with Jobs, page 70-30
- Troubleshooting Image Management, page 70-35

Getting Started with Image Manager

Image Manager contains sections that are used for managing your images, working with the devices that you will need to update, and performing image installations on those devices.

For more information on these areas of Image Manager, see the following topics:

- Working with Images, page 70-7
- Working with Bundles, page 70-11
- Working with Devices, page 70-14
- Working with Jobs, page 70-30

Before working with Image Manager, you should review the sections that follow:

- the platforms that are supported by this feature,
- the configuration settings you can change to control how the feature works, and

- the steps that are necessary to ensure your devices are configured to work with Image Manager.

This section contains the following topics:

- Image Manager Supported Platforms and Versions, page 70-2
- Device Configurations supported by Image Manager, page 70-2
- Image Manager Supported Image Types, page 70-3
- Administrative Settings for Image Manager, page 70-4
- Bootstrapping Devices for Image Manager, page 70-6

Image Manager Supported Platforms and Versions

Image Manager is available only for ASA devices. The following devices support Image Manager:

- All legacy ASA models—ASA 5505/10/20/40/50/80
- ASA 5585
- ASA 5512/15/25/35/45/55
- ASA-SM module for Catalyst 6K

The following devices are not supported and are filtered out in the devices tab of the Image Manager unified view:

- PIX firewall
- FWSM blade
- ASA device managed by AUS
- Devices unmanaged in Security Manager
- Other device types—IPS and Routers

Image Manager supports image upgrade for ASA device version from 7.x onwards. The target image version that can be used to upgrade is not restricted. Image upgrade to the highest ASA version supported in Security Manager 4.4, that is ASA version 9.0(1) and 9.1(1), has been tested.

Warning **Image downgrade is not restricted, but is done at your own risk. Image Manager does not validate downgrade cases.**

Device Configurations supported by Image Manager

In addition to supporting image updates on standalone ASA devices, Image Manager manages the filesystem and supports seamless image update for ASA devices specially configured for high availability and scalability. Following configurations are supported:

- **Multiple context mode**—ASA in multiple context mode where a single ASA can be partitioned into multiple virtual devices/firewalls. Refer to *http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/ha_contexts.html*. Each of these virtual firewalls are represented in CSM as independent devices. When Image Manager updates the image on the physical unit hosting these virtual devices, it updates device properties of all virtual devices with the new image information.

- **Failover configuration**—Two identical ASA devices configured to failover for high availability. They can be configured to be in Active/Active or Active/Standby failover. Refer to *http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/ha_overview.html*. Image update on an Active/Active failover pair is not supported in Image Manager. In order to use Image Manager to update the images on an Active/Active failover pair, the Active/Active failover pair has to temporarily be converted to Active/Standby by making all the failover groups active on one unit, and the corresponding failover groups standby on the other unit. After upgrade, you can convert the failover pair back to Active/Active.
- **Cluster configuration**—Multiple ASAs (up to 8 ASAs) can be grouped together as a single logical unit called a **cluster** for achieving increased throughput and redundancy. The purpose of clustering devices is to simplify manageability and to increase processing speed. By using clusters you are able to scale to a multitude of simultaneous connections that work together to load balance the connections. Clustering feature has been introduced starting from ASA version 9.0(1). For more information see *http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/ha_cluster.html*.

Note Clustering is only supported on ASA 5580 and ASA 5585.

Starting from CSM 4.4, Security Manager supports Clustering. In Configuration manager and Image Manager, all the devices/members in a cluster or a failover pair are managed as a single device. That is, when you change the configuration on a cluster's master device, the change is automatically made to all the devices in the cluster. Similarly, Image Manager updates image on each of the physical unit that is part of failover or cluster in a single operation.

Image Manager Supported Image Types

Image Manager supports the following types of images:

- ASA System software
- ASDM image
- VPN images [includes Cisco Secure Desktop (CSD), AnyConnect, and Hostscan]
- SSLVPN Plug-in images (For example: RDP, SSH, ICA, and others)

Image Manager completely manages the ASA system software and the ASDM images on the ASA devices, i.e., it performs loading of the image, activating the image by modifying configuration, and even reloading the device if required to complete the image upgrade process.

Image Manager does not support the ASA–CX images. This includes both the system images, for example asacx-sys-9.1.1-1.pkg, and also the boot images, for example asacx-5500x-boot-9.1.1-1.img. Using Image Manager, you cannot add any CX images to the Image Manager repository and cannot push any CX images to the device .

Handling of SSL VPN Images

Image Manager only reliably copies SSL VPN images to the ASA device. No configuration or activation commands are added for SSL VPN images by Image Manager. The configuration of the images must still be done using Configuration Manager.

The following files are not managed in Image Manager and have to be configured and deployed from Configuration Manager as in earlier versions of Security Manager:

- CSD Configuration XML

- AnyConnect Client Profile files
- DAP Configuration XML
- Full Customization XML files

After the SSL VPN images have been copied to the device using Image Manager, the remote access VPN policies must be configured in Configuration Manager to make use of these images. The Remote Access VPN policies that must be configured are located at the following paths in Configuration Manager:

- **CSD Package**—Remote Access VPN > Dynamic Access > Cisco Secure Desktop group box
- **HostScan Package**—Remote Access VPN > Dynamic Access > Cisco Secure Desktop group box
- **Anyconnect Image**—Remote Access VPN > SSL VPN > Other Settings > Client Settings tab
- **Plug-ins**—Remote Access VPN > SSL VPN > Other Settings > Plug-in tab

The SSL VPN binary files must be present on the device flash before you reference them in VPN policy. If not, Security Manager will present an activity validation warning informing the user of the preference to use Image Manager to push these files reliably to the device before deploying the configuration. If the user ignores the activation warning and goes ahead, Configuration Manager defaults to the old behavior and pushes the images or files as was done in the earlier versions of Security Manager before deploying the configuration referring to these files. But the user cannot leverage the following advantages of using Image Manager for copying these files:

1. Capability to use external disks like disk1 to copy the files. Configuration Manager only copies the files to disk0 and does not recognize or support external disks.
2. Image Manager preempts errors during the image copy by validating that there is enough free space on the disk to copy the selected images and does not allow creation of a job unless there is sufficient space is to copy the images. User can make space by using the Image Manager to delete unwanted images.

Note Image Manager does not validate the compatibility of the SSL VPN files that are pushed to the ASA. But Configuration Manager will complain when incompatible files are referenced in the Remote Access VPN policies.

Administrative Settings for Image Manager

Image Manager introduces new administrative settings. These administrative settings must be configured as part of Configuration Manager.

Configuring Cisco.com Certificates

Beginning with version 4.4, Security Manager has a certificate trust management feature. This feature helps you with improved handling of Cisco.com certificates. For detailed documentation of this feature, refer to Certificate Trust Management, page 10-17.

To configure administrative settings for Image Manager, do the following:

Step 1 Go to **Configuration Manager > Tools > Security Manager Administration**.

The Cisco Security Manager - Administration page appears.

Step 2 Configure workflow settings:

Tip Refer to the Configuration Manager documentation for workflow control setting information.

a. Select **Workflow**.

b. To require that Install Jobs be approved explicitly by an assigned approver before they are installed on devices, select **Require Deployment & Install Image Approval**. If you select this option, make sure you configure appropriate email notification settings. For more information, see the Workflow Page, page 11-55.

c. Click **Save.**

Step 3 Configure debug settings:

a. Select **Debug Options** and from the drop-down list for Image Manager Debug Level, select the debug level you want.

Tip The levels include: Severe, Error, Warning, Info and Debug. The default log level is Error.

Note The log files are stored as follows:

- The server logs are located at: ***%NMSROOT%\MDC\log\operation\vmssharedsvcs.log*** and ***%NMSROOT%\MDC\tomcat\logs\stdout.log***
- The client logs are located at: ***<Client Install Dir>\logs*.log***

b. Click **Save.**

Step 4 Configure Cisco.com credentials:

a. Select **Image Manager**.

The Image Manager page appears.

b. If you have credentials to connect to Cisco.com configured already at Tools > Security Manager Administration > IPS Updates > Update Server and wish to reuse the same for Image Manager, then check the **Use IPS Updates Settings** check box. This is also the default behavior.

Note Only Cisco.com is supported, not Local Server.

c. On the Image Manager page, deselect the **Use IPS Updates Settings** check box if you want to specify a set of credentials for Image Manager explicitly.

The fields on the Image Manager page become operable.

d. Complete the following fields:

- Username
- Password
- Confirmation

e. Optionally, complete the Proxy Server Settings to configure a proxy, if required.

1. Select the **Enable Proxy** check box.
2. Complete the following fields to define the proxy:

- IP or Hostname
- Port
- Username
- Password
- Confirmation (of Password)

f. Click **Test Connection** test connectivity to Cisco.com with the configured settings.

g. Click **Save**.

Step 5 Configure Purge Interval for Image Install Jobs

a. Select Image Manager.

b. Enter a purge value to specify how many days should pass between purges, in the Purge Jobs Older Than field.

Note Pressing the Purge Now button immediately purges the Image Installation jobs satisfying the Purge Interval criteria.

Step 6 Configure Image Backup Settings

a. Select Image Manager.

b. To include the repository as part of the standard backup, select **Include Repository**.

Caution Ensure that you have sufficient hard disk space on the Security Manager server as the image files consume a lot of space.

Note You can click the Reset button to reset the values to the last saved values before the current change.

c. Click **Save**.

Step 7 Click **Close** to close the Administration window.

Bootstrapping Devices for Image Manager

The bootstrapping in Image Manager is essentially the same as that which you perform in Configuration Manager for ASA devices.

To bootstrap a device for Image Management, do the following:

Step 1 Configure HTTPS on the device(s) to manage ASA in Security Manager.

a. Ensure that the HTTP server is enabled.

b. Add the Security Manager server IP address as an allowed host for HTTP management on the device.

Step 2 Ensure that the configuration register setting is set to boot with the image list in the running configuration.

a. Register value: 0x1,0x3,0x5, 0x7, 0x9

Note Register value: 0x1 is the recommended setting.

b. Do not set to boot to **rommon** mode. (Otherwise device will not be rebooted and the image upgrade will be aborted.)

Step 3 In Security Manager, go to Tools > Security Manager Administration > Device Communication > SSL Certificate Parameters. In the SSL Certificate Parameters area, set PIX/ASA/FWSM Device Authentication Certificates to Do not use certificate authentication.

Step 4 Ensure that there is sufficient space in the flash memory of the device(s) to hold the images you intend to load.

Tip If necessary, you can delete other images you do not intend to use from the device(s).

Step 5 We recommend that you unmanage the Boot-Image/Configuration policy for ASA, as follows:

a. In Security Manager, navigate to Tools > Administration > Policy Management.

b. Uncheck the Boot Image/Configuration policy selection.

Note Image Manager configures boot image and ASDM image as part of the image installation job. So, if the Boot Image/Configuration policy is not unmanaged, then any configuration deployment after the image installation will remove these boot commands added by Image Manager. To prevent this, the Boot Image/Configuration policy should be unmanaged in Security Manager. This can be done from Security Manager administration settings -> Device Exception Settings -> Firewall Policies node.

Step 6 We recommend that the device not be set as a priority monitored device in HPM.

Step 7 Ensure that all configuration changes on the device are submitted and deployed.

Working with Images

Image Manager provides access to images on Cisco.com as well as images on your network. When an image shows a location of Repository, it means that image has already been downloaded (either from Cisco.com or from a local file system). Conversely, an image that shows location as Cisco.com has not been downloaded into the repository. Navigating to the Repository Images in the Images section of the selector enables you to examine a list of all the images. You can also filter, sort, and search the images available. Filtering, in particular, is a good way to navigate within Image Manager. Beginning with all images, you can use the headings in the main repository view to locate images by a variety of attributes including name, version, and type.

Image Manager does not manage ASA-CX images. Any CX images available on Cisco.com will not be shown in Image Manager for download. You also cannot add any CX images from the file-system.

Note Only images that are downloaded to the Image Repository can be used for image upgrade jobs.

Note Beginning with Security Manager release 4.4, when Security Manager contacts Cisco.com to update images or to check on the availability of image updates, an additional certificate validation is performed. The update or download fails if you have not accepted the most recent certificate. You must retrieve, view, and accept the most recent certificate before you can proceed with other operations. For more information on the certificates, see Managing Device Communication Settings and Certificates, page 9-4.

This section contains the following topics:

- View All Images, page 70-8
- Download Images to the Repository, page 70-9

View All Images

When you first open Image Manager, or when you select All Images from the selector, the system displays a complete list of images. This list includes both those images in the repository as well as those on Cisco.com (which have not yet been downloaded). Some of the VPN image files are bundled with the Security Manager installation and are shown in the repository from the first time onwards. Image Manager will display a warning about credentials not being configured when the Image Manager client is launched for the first time, or until the credentials are configured under Security Manager administration settings for Image Manager.

Note In earlier releases of Security manager, only the prepackaged SSL-VPN images already existing in the Image Manager repository could be seen. If you do not have a repository connection, beginning with Security Manager release 4.4, on a freshly installed Security Manager, Image Manager shows not only the prepackaged SSL-VPN images in the repository, but also lists supported ASA images available on Cisco.com. The prepackaged files are available at: `CSMRoot>\MDC\athena\ccometadata`. Thus, even if you do not have initial connectivity to Cisco.com, you can view the latest images that are available at the time of release of the Security Manager. You have to have Cisco.com connectivity and should configure credentials to Cisco.com to either check for the latest updates on Cisco.com or to download the images from Cisco.com, or both. This prepackaged information about image availability enables users not having Cisco.com connectivity to still view the latest images available on Cisco.com (at least the ones published on Cisco.com by the Security Manager release). This also lets you view compatible images for a particular device type/platform.

This view can be re-ordered by any of the listed image attributes. For example, you can list the images by size. The attributes that you can sort on include:

- Download State - This is the first column and is shown as icons. The icons are actionable, and you can double-click the icon in this column to start the download of an image from Cisco.com, or to abort an ongoing image download, or to delete an image from the repository. Note that the icons change during each of these actions. (A green arrow indicates an image on Cisco.com, a red cross indicates an image that has already been downloaded, and another icon indicates that a download is in progress.)
- Image (name)

- Type
- Version
- Location
- Size
- Description
- Comments (you can add and edit comments for an image).

To view all images, do the following:

Step 1 Check for new images available on Cisco.com

a. Configure the credentials for reaching Cisco.com by navigating to Tools > Security Manager Administration > Image Manager.

b. In the upper right corner, click the double arrow **Check for Updates** icon.

c. Ensure that the CCO account has permissions to download crypto images. Otherwise, navigate to the link and accept the agreement, and then retry the operation.

The system displays "***Updating***" while it checks for updates. When finished, it reads: ***Last updated at: <timestamp>***, and you can view the new images available in the All Images view.

Step 2 If you have not already accepted the most recently issued Cisco.com certification, the system notifies you that you must retieve, view, and accept the latest certificate before any communication with Cisco.com by Image Manager can occur.

Step 3 Click **All Images** in the selector.

The system displays the image list.

Step 4 To re-order the list, click on any of the column headings.

The list of images is reordered according to the selected attribute.

Step 5 To filter the list, use the Image Manager's search window to enter a key string. For example, you could enter the digits of a version number.

Note Also, you can use the filter settings in some of the column headings to filter the list shown.

Download Images to the Repository

You can download images to the repository either from Cisco.com or from a local file system.

Note Beginning with version 4.4, Security Manager has a certificate trust management feature. This feature helps you with improved handling of Cisco.com certificates. For detailed documentation of this feature, refer to Certificate Trust Management, page 10-17. You must have accepted the latest certificate from the image download site on Cisco.com to proceed. The certificate of the site from which the image is to be downloaded may be different from the site that is contacted for "Check for updates" to obtain the latest meta-data information about images. Thus, even if you have accepted the certificate from the

"Image Meta-data Locator" URL, the image download may fail with an error to accept the certificate of the image download URL. You must retrieve and accept the certificate from the download URL given in the error message to proceed with the image download.

Tip Images can also be downloaded from the Compatible Images tab. For details see Manage Images on a Device, page 70-15.

To add an image file to your Security Manager repository, do the following:

Step 1 To download images from Cisco.com, do the following:

a. From the All Images view double-click the **Start Download** icon in the first column.

Tip Ensure that the credentials to Cisco.com are configured and you have authorization to download the images.

Note Image Manager displays an error message if the image to be downloaded already exists in the repository. The system skips the download when the file name and checksum are identical.

The Downloads window appears showing the progress of the download.

Tip The progress icons may change as the download progresses. A green check icon with the word Deployed indicates success. A red X icon indicates failure. In case of failures, you can view the cause of the failure for that image in the Downloads window. You can double click the message to view the complete details of the error.

b. When completed, select Repository Images and view the image in the listing.

Tip You can also select multiple images and download them all at once by right-clicking them and using the context-sensitive menu.

Tip By sorting the list on Update Time, you can easily view the most recent image.

Step 2 To download images from a local file system, do the following:

a. From the toolbar in the Repository Images view, click the **Download image from file system** icon (found on the far left).

The Download from File System dialog box appears.

b. Use the Browse feature to select the Import location and to select the image to be imported.

c. Click **OK**.

d. Click **OK** in the Download image from file system dialog box.

e. Observe the progress of the download.

Note If the image to be downloaded already exists in the repository, the system displays an error.

f. When completed, select a device group in Security Manager and view the image in the listing.

Tip By sorting the list on Update Time, you can easily view the most recent image.

g. Alternatively, you can download an image file using the drag-and-drop method. For example, you can drag one or more files from your desktop and simply drop it on the Image Manager application.

Working with Bundles

Bundles are groups of compatible images that you define. You can use bundles to simplify repetitive operations, by grouping images that are pre-validated to work together as a logical group. For example, you might define bundles that reflect ASA and ASDM pairs to ensure that you deploy both types in a single operation. The following types of images can be part of a bundle:

- ASA system software
- ASDM image
- VPN images (including csd, AnyConnect, Hostscan)
- Plug-ins (including rdp, ssh, ica, owa, and others)

Multiple system software images cannot be included in the same bundle.

Caution The Image Manager does not stop you from adding incompatible images as part of a bundle. You must determine this compatibility. The ASA and ASDM Compatibility matrix is located at: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html#wp42231.

Tip Throughout Image Manager there are operations where you can choose to apply an image, multiple images, or a (predefined) bundle of images.

This section contains the following topics:

- Creating Bundles, page 70-11
- View Images by Bundle, page 70-12
- Renaming Bundles, page 70-13
- Deleting Bundles, page 70-13
- Deleting Images from Bundles, page 70-13

Creating Bundles

You can define bundles of images to simplify your Image Manager. Bundles are particularly useful when you have a group of images upon which you regularly operate.

To create a bundle, do the following:

Step 1 From the Bundles heading in the selector, click the **Add Bundle** (plus sign) icon.

Step 2 In the Create Bundle dialog box that opens, enter the name for the new bundle.

Step 3 Click **OK**.

The bundle is listed under the Bundles heading in the selector.

Step 4 From the Images section of the selector, select an image to be bundled. Then click on the Release Notes tab. Finally, examine the compatibility table in the applicable release notes to ensure there are no conflicts with the other images to be bundled.

Caution The Image Manager does not stop you from adding incompatible images as part of a bundle. It is the responsibility of the user to determine this compatibility. The ASA and ASDM Compatibility matrix is located at: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html#wp42231.

Step 5 With compatibility determined, drag and drop each image onto the bundle.

Note Multiple system software images cannot be included in the same bundle.

Tip You can select a range of images to drag and drop by selecting the first image in the range and then, with the Shift key pressed, selecting the last image in the range. You can select multiple images by clicking those images while keeping the Ctrl key pressed. You can also select a range of images and then add additional images to your selection by using the Ctrl key method. To move multiple images to a bundle, drag using the right mouse button.

View Images by Bundle

You can view the images that have been added to a bundle.

To view the images in a bundle, do one of the following:

Step 1 To view the images contained within all bundles:

a. Under the Bundles heading in the selector, click the top-level Bundles folder.

All the bundles are listed, together with the images contained within each.

b. You can expand or collapse any of the bundles to make viewing easier. To expand all bundles or collapse all bundles, use the Expand All and Collapse All buttons at the top of the main window.

Step 2 To view the images for a specific bundle:

a. Under the Bundles heading in the selector, select a bundle.

The list of images for the selected bundle is displayed in the main window.

Step 3 To view a particular bundle:

a. In the Bundles section of the selector, click **Search** (the magnifier icon).

b. Enter the bundle name in the search field under the Bundles banner.

The list of bundles displays only the specified bundle.

Renaming Bundles

Bundles can easily be renamed to provide better organization or to more accurately reflect the contents of the bundle.

To rename a bundle, do the following:

Step 1 From the Bundles heading in the selector, select a bundle.

Step 2 Right-click the bundle name and, from the drop-down list, select **Rename Bundle**.

The Rename Bundle dialog box appears.

Step 3 Type the new bundle name.

Step 4 Click **OK.**

The new bundle name appears in the selector under Bundles.

Deleting Bundles

Bundles that are no longer needed can be deleted.

To delete a bundle, do the following:

Step 1 Select the bundle.

Step 2 From the Bundles heading in the selector, click **Delete** (the red X icon). Alternatively, right click on the selected bundle and select **Delete Bundle**.

Deleting Images from Bundles

If you wish to change the contents of a bundle, you can delete any of the images that are defined as part of a bundle.

To delete images from bundle, do the following:

Step 1 Select the bundle.

Step 2 Right-click on the image(s) to be removed.

Step 3 Select **Delete Image from Bundle**. Alternatively, click the Delete button at the top of the table.

Working with Devices

The following topics explain how to work with devices in Image Manager.

Note For a cluster, only the master node supports the download of files from storage.

This section contains the following topics:

- Viewing Device Inventory, page 70-14
- Manage Images on a Device, page 70-15
- View Device Memory, page 70-16
- Configuring the Image Install Location, page 70-17

Viewing Device Inventory

You can use the Device Summary page to quickly view the devices on your network and their attributes.

Within the selector panel on the left is an area called Devices. From that area you can display all devices by selecting All (or you could select a location or group of devices you have defined). After you have chosen the scope of device selection, the corresponding devices are displayed in the upper panel of the Device Summary page. The upper window of the Device Summary page displays the following attributes, as applicable, for each device:

- Device Display name
- Mode (for example, Standalone, Active-Active. Active-Standby, Cluster)
- System SW Version
- ASDM Version
- AnyConnect Version
- Secure Desktop Version
- Hostscan Version

The Device Summary table includes a Mode column. This column specifies such modes as Cluster, Standalone, Active-Active, and Active-Standby.

For configurations in which multiple physical devices are grouped together, as in failover and cluster configuration, each physical unit/ member has its own file system. And these file systems can be different. The details of the file systems of each physical device/ member are viewable within Image Manager.

Details of individual cluster members, including storage and image status, are shown in the Security Manager user interface. During discovery of image management inventory data, details are discovered regarding each cluster member's storage and running image details.

When a Failover or Cluster device is selected in the Device Summary page, the individual physical members in the group are displayed in the middle Device View table. The Device View table for Cluster device displays the following information about the cluster members:

- **Name**—Device or cluster member name.
- **ID**—Cluster Member ID.
- **Status**—Role of the member in the cluster. For example, Cluster Master or Cluster Slave.

- **Serial Number**—
- **RAM Size**—
- **Running OS Version**—Version of OS on the particular member
- **CCL IP**—Cluster Link IP address
- **CCL MAC**—Cluster Link MAC address

The Device View table for a *Failover device* has columns that include Name, Status (for example Standby or Active), Serial Number, RAM size, and Running OS Version. The Failover Device table lists these elements by Primary and Secondary devices for the failover pair nodes.

When you select a particular device in the device summary page, then the lower window displays the following tabbed pages for the details of that device.

- **Summary**—Display Name, Device Type, IP Address, Hostname, Domain Name, Serial Number, Running OS Version, Target OS Version, RAM, Failover Mode, Image Install Location
- **Compatible Images**—Images compatible to the device—Image, Type, Version, Location, Size, Description, Comment.
- **History**—Chronological view of Image Installation Jobs and Configuration Deployment Jobs that have been executed on the device—Job Name, Changed By, State, Last Action, Tickets

When you select a particular member of a failover or cluster device in the middle Device View, the lower window displays the following tabbed details for that physical device.

- **Summary**—Running OS Version, Target OS Version, RAM
- **Storage**—The number and capacity of flash memory units. Name, Size, Path, Type, Disk Usage
- **Running Images**—The images presently operating. Name, Type, Version, Path, Size

Manage Images on a Device

You can use the Image Management tool to review, download, and remove the images on the ASA device(s) you select.

To review, download, or remove ASA images on a device, do the following:

Step 1 Select a device group from the Devices area of the selector panel.

The main window displays the Device Summary. The Device summary lists the devices and the associated system software versions.

Tip Alternatively, you can select the search function (magnifier icon) from the Devices banner and then enter the device name in the search field that appears.

Step 2 From the upper pane of the Device Summary page, select a device.

Note If a particular device is part of a cluster, you can navigate through the cluster to view device details.

The lower pane displays details of the selected device.

Step 3 Select the Storage tab in the lower pane and then check the amount of free space listed under Disk Usage.

Note If a particular device is part of a cluster, you can navigate through the cluster to view device storage details.

Tip The device may have more than one storage area, for example, disk1. Be sure to scroll down to see secondary (flash) storage capacity.

Step 4 Note the available disk space on the device.

Step 5 To remove one or more images from the device to free up space, select one or more images in the Storage Tab and click **Delete** at the top of the Storage Tab.

Tip Alternatively, you can select one or more images, right-click and click Delete.

Tip If you delete an image that is currently active and is being referenced, Image Manager displays a warning message.

Step 6 To download an image from the device, select the image and click **Download** at the top of the Storage tab. Select the location on the local file system to which to download the image and click **OK**.

Note For a cluster device, download of images is only supported on the Cluster master. Similarly, for a failover device, download of images is only supported on the active device in the pair.

A dialog appears showing the progress of the download from the device. After the download is completed, the downloaded image is shown in Explorer.

Step 7 Select the Compatible Images tab in the lower pane.

The system displays images that are compatible to the device.

Step 8 To install the compatible image(s) onto the device do the following:

a. Select the image to be added to the device.

b. Double-click the download icon.

The image is downloaded to the repository.

c. Select the image and then select **Install** from the context menu.

The Install wizard appears and the system installs the image. Please see Install Compatible Images on Devices, page 70-28 for details.

View Device Memory

You can use Image Manager to determine the memory capacity and application of a device in your network.

Note Only physical devices can display memory capacity, clusters do not.

To view the details of the memory on a device, do the following:

Step 1 From the Devices area of the selector panel, choose the device to examine.

Details of the selected device appear in upper window of the Device Summary page.

Step 2 In the upper panel, examine the RAM listing.

Caution Image Manager warns you if there is insufficient RAM on a device to load the new image. However, the system does not stop you from performing such an image upgrade. (This is in contrast with Configuration deployment, where the deployment job stops if there is insufficient RAM.)

Configuring the Image Install Location

ASA devices have a default flash (disk0) where all the images reside. By default, Image Manager copies images to disk0 of the ASA device. When the ASA device is configured with an external disk (that is, disk1), Image Manager allows you to choose between the two disks, disk0 or disk1, when loading images on the ASA device.

Note The capability to load images on an external disk is very useful for storing large images such as those for AnyConnect and CSD, as disk0 can run out of space quickly with even a few of these larger images.

For configuring Image Manager to use the external disk, do the following:

Step 1 Select the device from the Devices area of the selector.

Step 2 View the Summary information on the right pane.

The available disks on the device are listed in the Image Install Location drop-down list. For a device with external disk, disk0 and disk1 would be listed.

Step 3 Select the external disk, disk1, from the Image Install Location drop-down list and click **Apply**.

All future image installation jobs for the device will load the images to disk1.

Tip The configuration of the external disk can be verified by performing an image install operation. After the job is complete, view the contents of disk1 in the Storage tab of the device in Image Manager. It should list the newly installed images.

Note For cluster and failover devices, if all the physical member devices do not have the disk that is selected as the Image Install location, then there will be a validation error when you try to install images on the cluster or failover device. You need to select the Image Install location to be a disk that is present on every member device in the cluster or the failover to proceed with installing images.

About Image Updates on Devices Using Image Manager

How does Image Manager update images on an ASA device?

Image Manager follows the standard documented procedure to upgrade the stand-alone ASA devices with several built-in checks to ensure reliable image upgrade. Please refer to: http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008067e9f9.shtml#maintask2 for the procedure for image upgrade.

Note You must have accepted the latest Cisco.com certificate to enable Image Manager to interface with cisco.com. You must accept the certificate from both the "Image Meta-data locator" site and the download site of the images to start downloading images successfully (see Image Manager Page, page 11-29).

Image Manager uses the HTTPS protocol to copy images to the ASA device, performs configuration changes to activate the new image (ensuring fallback to the older image in case of any error), and finally reloads the device if required, with the new image.

How does Image Manager update images on an ASA configured for failover?

Updating the images in an Active/Standby failover pair is accomplished by creating an image upgrade job on the active device of the pair, and then running the image upgrade job.

Note Image update on an Active/Active failover pair is not supported in Image Manager. The Active/Active failover pair has to be converted to Active/Standby by making all the failover groups active on one unit, and the corresponding failover groups standby on the other unit. Only then can Image Manager update the image on the pair of devices.

To upgrade devices in an Active/Active failover pair:

1. Manually convert the pair to active/standby by forcing all the failover groups on one device to be **active** and on the other device to be **standby**.

Note Do not discover the devices in Security Manager.

Note For additional details on how to convert an active/active failover pair to active/standby, see http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080b20f35.shtml#Actact.

2. Create an image upgrade job on the active device of the pair, and run the image upgrade job.
3. After the upgrade has occurred, manually convert the pair back to active/active configuration, as existed before the upgrade, by making the required failover groups active on one unit and the remaining failover groups to be active on the other physical unit.
4. Rediscover in Security Manager only the device inventory for the unit that was converted to standby.

Image Manager follows the zero-downtime upgrade procedure as detailed at: http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080b20f35.shtml. The image is copied to both the units and then configuration change is done to activate the image that is synced to both units. First the standby is reloaded via the active unit and after ensuring that the standby has been upgraded successfully to the new version, the current active is reloaded. After both the units are upgraded to the new version, the failover pair or cluster upgrade is marked successful.

There are restrictions for image upgrade in failover ASA pair. We recommend that, while performing image upgrades on a failover ASA pair or cluster using Image Manager, you ensure the following restrictions are satisfied:

- The two units in a failover configuration should have the same major (first number) and minor (second number) software version.
- **Maintenance Release**: You can upgrade from any maintenance release to any other maintenance release within a minor release. For example, you can upgrade from 7.0(1) to 7.0(4) without first installing the maintenance releases in between.
- **Minor Release**: You can upgrade from a minor release to the next minor release. **You cannot skip a minor release.** For example, you can upgrade from 7.0 to 7.1. Upgrading from 7.0 directly to 7.2 is not supported for zero-downtime upgrades; you must first upgrade to 7.1
- **Major Release**: You can upgrade from the last minor release of the previous version to the next major release. For example, you can upgrade from 7.9 to 8.0, assuming that 7.9 is the last minor version in the 7.x release.

How does Image Manager update images on an ASA cluster?

Image updates follow the procedure previously established for hitless upgrades that ensures that all members of a cluster are upgraded to a new version in a single user operation without affecting traffic flow. During an image upgrade:

- Slave cluster members are first loaded with the new image from the master. Images are copied to all members of a cluster while being connected only to the master. Such propagation through a cluster does not require switchovers of each device to master status and, thereby, minimizes traffic disruption.
- Configuration is changed on the master to add the boot command to load with the new image. The configuration, once changed on the master, automatically gets synced on all the slave units.
- All the slave cluster members reboot with the new image sequentially via the cluster master.
- All the slave cluster members come online and rejoin the cluster.
- The cluster master is then made into a slave (with the next slave member taking over the cluster master role).
- Via the new master, the old master is reloaded with the new image.

This procedure for image update followed by Image Manager ensures minimal switchovers and minimal disruption of traffic.

Device State Changes During and After Image Update

Image upgrade is a critical operation and hence there is a need to depict visually, and inform users of, all image update operations. Thus, three new device states have been introduced:

- **Upgrade In Progress**—The device is put into this state whenever an image install job starts on the device. This state is automatically reset by the system after the image update operation is completed on the device.
- **Maintenance**—The device is put into Maintenance state when the image install job fails on the device and the device becomes unreachable after the image install operation. You need to manually reset this state to normal/operational state after taking necessary steps to bring back the device online by manually correcting issues due to upgrade or by rolling back the image.
- **Configuration Required**—For certain cases of image upgrade (like from ASA 8.2 to ASA 8.3), there are significant changes in the device configuration as part of the image upgrade which renders the policy configuration model in Security Manager incompatible with the device configuration. In such cases, even if the image upgrade operation may be successful, you must perform some operations, like rediscovery of device, to ensure that after upgrade, Security Manager's configuration policy model and the device configuration are in tandem. Thus, after an image upgrade, if some additional configuration is required to be made in Configuration Manager to make the device operational, the device is put into *Configuration Required* state. Even in the case where VPN images are deployed using Image Manager, the device is put into *Configuration Required* state since this requires the user to configure these images in the VPN policies using Configuration Manager. The *Configuration Required* state indicates that there are changes to be done in Configuration Manager to make the device functional in Security Manager after the image update operation. You can make the suggested changes and, after you are satisfied with your configuration changes, you can manually bring the device back to *Operational* state.

Note Refer to the Troubleshooting Image Management, page 70-35 for more scenarios that can put the device in the Configuration Required mode.

Whenever the device state is changed to any of these three states, the state is indicated in the device selector with an explicit icon. This change in device state can be seen in both Configuration Manager and Image Manager. The normal state of the device when there is no image update operation on the device is the *Operational* state.

Tip To manually reset the device state to normal or *Operational* status, select the device(s) in the device selector in Configuration Manager or Image Manager, right click, and select Make Device Operational.

This section contains the following topics:

- Validating a Proposed Image Update on a Device, page 70-21
- Using the Image Installation Wizard to Install Images on Devices, page 70-24
- Install Bundled Images on Devices, page 70-28
- Install Compatible Images on Devices, page 70-28
- Install Images on Selected Devices, page 70-29

Validating a Proposed Image Update on a Device

You can validate the image update job on one or more devices prior to actually performing it. The following list details the various validations that are performed:

- Insufficient disk space on the ASA device to accommodate the selected images.

  An error is displayed in this case. You must navigate to the Storage tab for that device and delete one or more images to make space. Then retry the upgrade validation operation.

  Note The disk space on each of the members in the Cluster and both active and standby units in a Failover are evaluated for sufficient space to accommodate the selected images. When a single member or device does not have sufficient space, an error is displayed and you cannot proceed to creating a job on the device. You must navigate to the Storage tab for that particular member and make space by deleting one or more unwanted images.

- Insufficient RAM on the device to run the new image as recommended in: Release Notes for the Cisco ASA 5500 Series, 8.4(x).

  Note Image Manager will warn you if there is insufficient RAM on the device to load the new image. However, this will not stop you from performing an image upgrade. This is in contrast with Configuration deployment, wherein the deployment job stops if there is insufficient RAM.

- If the flash device (disk0 or disk1) that is selected for Image Install Location is not present on any of the devices/members in cluster/failover setup, then an error is displayed and the job is aborted.
- Configuration changes that have been submitted but not yet deployed to the device. These changes need to be deployed before starting the image update job. Otherwise, the configuration changes may become incompatible with the upgraded image version on the device.
- Warn if the selected image(s) is (are) incompatible with the device type, for example, if non-SMP images are selected for ASA 5585 device types.

  Note This warning only occurs when you are using the drag-and-drop method. For other flows, the incompatible images/devices are filtered out in step 2 of the Image Install Wizard.

  Note This validation was skipped in CSM 4.3 if Check for updates is not performed due to the unavailability of meta-data information about images on Cisco.com compatible with MDF IDs. In CSM 4.4, the meta-data information are prepackaged with CSM install and hence even if Check for updates is not performed, Image manager will validate the compatibility of images for device types and warn the user when an incompatible image-device combination is chosen.

- Warn if the device is being updated to a version that is unsupported on Security Manager.
- Warn if the new image version is the same as or lower than the version running on the device.
- An image upgrade to ASA Version 8.3 from any lower version would require the device to be re-discovered in Security Manager. There were major changes in the NAT configuration introduced in ASA version 8.3 that are incompatible with previous ASA versions. Likewise, there were major

changes to the NAT policy model in Security Manager for Version 8.3. Hence, when a device is upgraded to ASA 8.3, that device is put into the Configuration Required state to indicate to the Configuration user that some changes are required in Configuration Manager to make the device operational. After rediscovering the device in Security Manager, the user can right-click the device in the device tree and select Make Device Operational to bring it back to normal state.

- An image upgrade from ASA Version 8.3.x to 8.4.2 or higher also requires rediscovery of the device in Security Manager because of incompatible changes in PAT configuration in ASA Version 8.4.2. In this case also, the device state is changed to the Configuration Required state after the image upgrade.
- An image upgrade from ASA Version 8.x to 9.0.1 or higher requires rediscovery of the device in Security Manager because of incompatible changes in Unified access rules, inspection, and NAT rules.
- An image upgrade from ASA Version 7.x to 8.x introduces major changes in the SSLVPN configuration both on the device and in Security Manager. Because of these incompatible changes, the device must be deleted from Security Manager after the image upgrade and then added again. The device is put into the Configuration Required state to notify the user to act upon these warnings.
- Any VPN image, such as an AnyConnect, CSD, or Hostscan image, being loaded using Image Manager warns the user if the existing VPN image was part of a shared policy being assigned to the current device or other devices. A warning is issued to also copy the new image to all the devices to which the shared policy is assigned so that the shared policy can be updated for all the devices seamlessly without the loss of policy sharing.
- Warn when the standby unit in a failover pair in not reachable. This is an error that will cause the job to be aborted.
- Warning for upgrade of Active/Standby failover pair. The version being upgraded should comply with the recommendations listed at: ASA/PIX: How to Use the CLI to Upgrade the Software Image on a Failover Pair.

  Note The same warnings are also applicable for an ASA in cluster configuration.

- Warning for upgrade of Active/Active failover pair that the image update job will be aborted unless the pair is converted to Active/Standby (that is, if all the failover groups are active on one physical unit).

Note Additional validations are required for a "device" that is a designated cluster master. In addition to a check that is similar to that for Active/Standby Failover, there is also a check that the cluster image is compatible with supported platforms. A cluster cannot be downgraded to a version less than 9.x.

To validate an image installation, do the following:

Step 1 From the File menu, select **Validate.**

The Validate Image Assignments window opens.

Step 2 Click **Add Assignment**.

The Image Assignment window opens.

Step 3 In the Image Assignment window, from the drop-down list, select either:

- Select Images and Assign to Devices

- Select Devices and Assign to Images

Tip The same result is obtained by assigning images to devices or by assigning devices to images.

Step 4 Select one or more items (images or devices) by moving them to the window on the right.

Tip You can use pre-defined bundles rather than images by clicking **Bundles** and selecting the bundle.

Step 5 Click **Next** and assign the other item (images or devices).

The Confirm Assignments window appears.

Step 6 Examine and confirm the assignments that you have specified.

Tip You can continue to add or remove assignments, as required.

Step 7 Click **Finish.**

The Validate Assignments window appears.

Step 8 Click **Start Validation**.

The validation status of the assignment is shown in the Validation column. It shows either Warning or Successful or Error.

Step 9 Click on the display of Warning or Successful or Error.

A lower pane window opens.

Step 10 According to the validation status, do one of the following:

- **Error**—Examine the potential reasons for the error and correct as necessary.
- **Warning**—Examine the potential reasons for the warning and correct as necessary.
- **Successful**—No action required.

Tip Be sure to display and examine all the errors or warnings by using the window slider bar on the right.

Step 11 After addressing the warnings or errors shown, you can proceed to create the job using the Image Install wizard.

Step 12 Optionally, you can right-click on an assignment element in the Validate Image Assignments window and modify or delete it before proceeding.

Step 13 You can also right-click on an assignment and select **Copy Table**. This copies the assignment details and the validation status and notes. You can then paste the contents to Notepad or another program as a CSV file to be used as reference.

Using the Image Installation Wizard to Install Images on Devices

You can use this feature to create a job to assign and install images on devices. An assignment is simply an association of an image and a device that defines an installation job.

Note If you have the workflow function enabled, you must perform the additional steps described for obtaining authorization before you can accomplish installation.

Note You can choose to operate upon any arbitrary set of devices.

To create a job to install images on devices, do the following:

Step 1 Go to Files > Open Image Installation Wizard.

The Image Installation Wizard dialog box appears.

Tip The Image Installation Wizard can be invoked in several ways. In addition to invoking the Wizard from the menu, as described here, you can invoke it when you do any one of the following things: (1) install images by the drag-and-drop method; (2) right-click on a device or bundle; or (3) select a device, navigate to the Compatible Image tab, select one or more images from the table, right-click, and select the **Install** option.

Step 2 On the lower left, click **Add Assignment**.

The Image Assignments dialog box appears.

Step 3 From the drop-down list on the top, select whether you want to assign images to devices, or devices to images.

Step 4 Move items (devices or images) from the list on the left to the selected items list on the right. Then click **Next**. You can also select bundles, instead of images, by clicking the Bundles tab.

Tip When pairing images and devices to define assignments, you can proceed with images and then devices, or devices and then images. The order of this selection does not matter.

Step 5 Review the assignment definition in the Confirm Assignments dialog box and click **Finish.**

Tip At this point you can choose to add additional assignment pairs, as desired, by clicking **Add Assignment**.

Step 6 When you are finished defining assignments, click **Start Validation.** Wait until the system displays Validation Complete.

Step 7 Examine the status in the Validation column on the Assignments tab of the Wizard dialog box. It shows either Warning or Successful or Error.

Step 8 Determine what steps are necessary according to the status:

- **Error**—Examine the potential reasons for the error and correct as necessary.
- **Warning**—Examine the potential reasons for the warning and correct as necessary.

- **Successful**—No action required.

Step 9 Right-click on the assignment for more options:

- **Move Up/Move Down**—Select these options for a multi-device job when you want to change the order in which the devices will get updated. This feature can be used to order or sequence the devices when the Install Images to Devices job option is set to Sequential.
- **Delete/Delete All**—You choose these options to remove one or all devices from the image upgrade job.
- **Copy Table**—Use this to copy the warning messages to some text editor or spreadsheet program for reference.
- **Test File copy**—Use this option to check whether files can be copied between Security Manager Image repository and ASA device flash using https protocol.

Tip Be sure to display and examine all the errors or warnings by using the windows slider bar on the right.

Step 10 If you want the installation job scheduled for a particular time, select the **Schedule** tab and specify the date and time.

Step 11 To set properties of the installation job, select the **Properties** tab.

a. Edit the **Name**, if desired. (The default is Image install Job—<timestamp>)

b. Edit the **Description**, if desired.

c. Select a **Ticket ID**, if desired.

Tip Starting from release 4.4, Ticket ID field in Image Manager has been decoupled from Config Manager. It is now just a 'tag' and can be any arbitrary string. Ticket ID field is an editable combo box with auto completion that shows tickets created earlier both in Image Manager and Configuration Manager. Also, there is no dependency on Ticketing mode in Configuration Manager for Ticket ID field. Ticket ID is an optional field and can be left blank. Global search in Configuration Manager also supports tickets used in Image Manager and lists the Image Installation jobs with which the ticket is associated.

d. Set the **On Error** option. (Default is Stop Installation, alternative is Continue Operation.)

e. Set the **Backup Current Image** option. (Default is Yes, alternative is No.)

Tip This is only applicable for system software images

f. Set the **Install images to devices in** option. (Default is parallel, alternative is Sequential.)

g. Select one of three operations:
   - Install image and reboot device
   - Install image but do not reboot device
   - Only copy image onto devices

h. If you are using Workflow, you can optionally configure the following approval options:

Tip These are located in the top frame in Job properties for the job.

- **Action**—
- Approve
- Reject
- Deploy
- Submit

If you reject a job, the status is set to Rejected, after which you discard the job. When you discard a job the status is shown as Discarded and all the job's action buttons are disabled.

If you approve a job, the status is set to Approved. Then, you must click Deploy to start the image upgrade job.

Tip You can the check running commentary by selecting the Details tab. and clicking **Show Progress**.

After you deploy a job, the job status is shown as either Deployed or Failed. The History tab in the bottom pane (for the selected job) only is activated in WF mode and displays one of two job action flows:

- Creating/ Edit-In-use/ Submitted/ Rejected/ Discarded
- Creating/Edit-In-use/ Submitted/ Approved/ Deploying/ Deployed (or Failed)
- **Submit the job**—This is checked by default
- **Approver email**—The email address list of approvers
- **Submitter email**—The email address of the person submitting the job

i. You can change job properties by clicking **Edit.**

j. Refer to Viewing Install Jobs, page 70-31 for additional job viewing options.

Step 12 Click **Install**.

The Jobs page appears and the install job is shown with its status as Deploying.

Note If a schedule was selected for the job, the job state is shown as Scheduled. The job will start deploying at the scheduled time and, at that time, the job state changes to Deploying.

Note If workflow is enabled for Image Install Jobs, then the job state is changed to either Submitted or Edit-in-Use. In this mode, the job can be deployed only after it has been approved. Please refer to Image Installation Job Approval Workflow, page 70-34 for details on the job states in the workflow mode.

Tip You can halt the job by clicking **Abort**. Please see Aborting an Image Installation Job, page 70-32 for important information about aborting an installation job.

You can discard a job before the scheduled run time by clicking **Discard**.

Step 13 When the job starts deploying, notice the change in the state of the devices to *Update in progress* state in the device tree in Configuration Manager and Image Manager. A green progress icon appears beside the device in the device tree.

Step 14 View the details of the job and its progress while it is in deploying state. Please see Viewing Install Jobs, page 70-31 for details.

Step 15 Wait for the job to complete.

The job state is changed to *Deployed* if all the devices are successfully updated. The job state is changed to *Failed* if one or more devices failed in the job.

Step 16 Notice the change in state of the device(s) in the device tree after the job is complete.

If the image update is successful and there are no further configuration changes required in Configuration Manager, the device will be moved back to *Operational* state. If there are configuration changes required on the device after the update, then device is moved to *Configuration Required* state. Clicking on the device in the device tree brings up a balloon tip with details of the state and actions to be taken to move the device state back to *Operational*.

If the image update fails on the device and the device is rendered unreachable during the image update operation, the device is put to *Maintenance* state.

Step 17 Verifying the image update:

a. Click on the device in the device tree in Image Manager.

b. Go to the Summary tab to view the updated Running OS version.

c. Go to the Running Images tab to view the new running images after the image update.

d. Select the device in Configuration Manager.

e. Right-click the device and select **Device Properties**.

f. Notice the new image version updated in Running OS Version field.

g. Go to **Configuration Manager > Manage > Configuration Archive**.

h. From the device CLI, enter ***sh ver***

The updated OS version should be displayed.

i. Select the device in the left device tree.

j. View the Configuration Archive versions in the right pane and notice the latest entry with the Archival Source as *Image Manager*.

k. Select the archived entry and click **View.**

l. Compare this entry with the previous archived version to view the configuration changes made by Image Manager during image update. You can view the boot commands being prepended for the new ASA system software image and/or ASDM image command being added for the new ASDM image.

m. Email notification will be sent to configured recipients with the status of the Image Upgrade job if email notification is configured in Image Manager administration settings.

Step 18 If the device is set to *Configuration Required* or *Maintenance* state after the image update operation, follow the steps below to complete the post-image update requirements to make the device functional from Configuration Manager:

a. Click on the device in the device tree in Configuration Manager or Image Manager.

A balloon tip appears showing the device information.

b. View the contents of the balloon tip. Review the reason for the device being set to the *Configuration Required* or *Maintenance* state. Review also the recommended actions to be taken.

c. Perform the recommended actions.

d. Right-click the device in the device tree and select **Make Device(s) Operational**.

The device is moved to *Operational* state and the icon beside the device in the device tree is removed.

Install Bundled Images on Devices

You can use the Image Manager tool to assign and install compatible images that are grouped as bundles. Bundles simplify repetitive operations and can ensure consistent actions are taken on a group of devices.

To selectively install an image bundle on a device or device group, do the following:

Step 1 Drag and drop the bundle onto a device or device group.

The Install images on devices dialog box appears with device and images in the bundle pre-assigned. If the bundle is dropped onto a device group, all the devices in the group are automatically selected and assigned to the images in the bundle.

Step 2 Investigate any assignment validation errors or warnings listed in the Install images on devices dialog box.

Tip You can choose to schedule the job and also modify the default properties for the job. Please see Using the Image Installation Wizard to Install Images on Devices, page 70-24 for details on scheduling a job and configuring job properties.

Step 3 When your warnings are corrected (or you determine them to be insignificant), click **Install.**

Note Alternatively, you can right-click a bundle and select **Install** to launch the Image Installation wizard with the bundle pre-selected. You can then choose the devices and click **Install** to install the bundle on the selected devices.

Install Compatible Images on Devices

You can use Image Manager to install compatible images on devices.

To selectively install one or more compatible images on a device or device group, do the following:

Step 1 Select a device in the Devices area of the selector and navigate to the Compatible Images tab.

Step 2 Select one or more Repository images in the Compatible Images tab.

Step 3 Right-click a selected image and click **Install**.

The Image Installation wizard appears with the selected images pre-assigned or moved to the right pane in the Select Image page.

Step 4 Click **Next**.

The Select Devices page of the wizard is displayed.

Step 5 Select the devices to which you want to install, and then click **Next**.

The Confirm Assignments page of the wizard is displayed.

Step 6 Confirm the devices and images assignments, and then click **Finish**.

The Install images on selected devices dialog box appears with the devices and image(s) assigned.

Step 7 Click **Start Validation** in the upper-right corner of the Assignments tab. Investigate any assignment validation errors or warnings listed in the Install images on devices dialog box.

Tip You can choose to schedule the job and also modify the default properties for the job. Please see Using the Image Installation Wizard to Install Images on Devices, page 70-24 for details on scheduling a job and configuring job properties.

Step 8 When your warnings are corrected (or you determine them to be insignificant), click **Install**.

The image installation job is created. Please see Using the Image Installation Wizard to Install Images on Devices, page 70-24 for the remaining steps to monitor the job progress and verify the image update.

Note Alternatively, to install one or more images on a device or device group, you can drag multiple images from the Repository view and drop them onto a device or device group. Then, click **Install** to install the selected image(s) on the selected device(s).

Install Images on Selected Devices

You can use Image Manager to upgrade the images on a set of devices that you select.

To install images on a selected set of devices, do the following:

Step 1 Select a device group in the Devices area of the selector.

Step 2 View the listing of devices in the group in the right pane.

Step 3 Select one or more devices from the list.

Tip Use the Shift and Control keys to select multiple devices.

Step 4 Right-click a selected device and click **Install**.

The Image Installation wizard appears with the selected devices pre-assigned or moved to the right pane in the Select Devices page.

Step 5 Click **Next**.

The Select Images page of the wizard is displayed.

Step 6 Select the images you want to install, and then click **Next**.

Tip You can also select a bundle in the Bundles tab.

The Confirm Assignments page of the wizard is displayed.

Step 7 Confirm the devices and images assignments, and then click **Finish**.

The Install Images on selected devices dialog box appears with the devices and image(s) assigned.

Step 8 Click **Start Validation** in the upper-right corner of the Assignments tab. Investigate any assignment validation errors or warnings listed in the Install images on devices dialog box.

Tip You can choose to schedule the job and also modify the default properties for the job. Please see Using the Image Installation Wizard to Install Images on Devices, page 70-24 for details on scheduling a job and configuring job properties.

Step 9 When your warnings are corrected (or you determine them to be insignificant), click **Install**.

The image installation job is created. Please see Using the Image Installation Wizard to Install Images on Devices, page 70-24 for the remaining steps to monitor the job progress and verify the image update.

Working with Jobs

This section details the set of functions that assists in the performance of the image installation jobs. An image installation job may be immediately run, or it may be scheduled to run at a specified time and date. As Image Manager jobs tend to be time-consuming, the job management functions enable you to perform these operations in the background. Image Manager incorporates an optional ticketing system that enables you to easily locate a job or jobs by means of a unique Ticket ID.

You should understand that the details of a particular job are defined and validated before being run.

This section contains the following topics:

- Viewing Image Installation Job Summary, page 70-31
- Viewing Install Jobs, page 70-31
- Aborting an Image Installation Job, page 70-32
- Retry a Failed Image Install Job, page 70-33
- Roll Back a Deployed Job, page 70-33
- Image Installation Job Approval Workflow, page 70-34

Viewing Image Installation Job Summary

You can use the Image Manager tool to monitor image installation and deployment jobs. You can view the history and status of jobs that Image Manager has performed, as well as the summary, details, or history of any particular job.

Note Comprehensive details of job state changes are available in Configuration Manager (see Job States in Non-Workflow Mode, page 8-4 or Job States in Workflow Mode, page 8-6). For an Audit Report navigate to Configuration Manager > Manage > Audit Report.

To view a summary of image installation jobs, do the following:

Step 1 In the selector, under Jobs, click **Install Jobs**.

The main window displays the Jobs list in the upper pane.

Step 2 Examine the details of the Jobs list, which may include:

- **Name**—The name of the job. By default the name includes a time stamp.
- **Last Action**—Date of the last action.
- **Status**—Whether the job has deployed, failed, or is underway.
- **Changed By**—Who started the job.
- **Description**—Job description.
- **Schedule**—Job schedule.
- **Ticket ID(s)**—Tickets are just tags attached to Image Manager job to track changes. These tickets may be tickets created in Configuration Manager, but are not mandated to be so.

Step 3 Optionally, you can find and select a single job about which more information is then displayed in the lower pane. This includes:

- Summary
- Details
- History

Tip While viewing the lower pane Details tab, you can select a device and then view a log of the job in the lower right pane.

Note These are dockable windows. You can customize the default view.

Viewing Install Jobs

You can view the details associated with a particular Image Management job.

To view the details associated with a job, do the following:

Step 1 In the selector, under Jobs, click **Install Jobs**.

Tip The Status column in the Jobs selector indicates whether a job is Submitted, Approved, Deployed, In Progress, or Failed.

The main window displays the Jobs list in the upper pane.

Step 2 Select a job to examine.

Tip To find a particular job, you can sort the Jobs list by any of the column headings, including Name, Last Action (chronology), Status (e.g., Deployed, Failed), Description, and so forth. You can also find a particular job by using the search window to enter a filtering string.

Note The location of the jobs folder is CSM-ROOT\files\vms\jobs directory.

Step 3 Examine job summary information by clicking **Summary** in the lower pane.

The lower pane displays job summary information including Image Management Job Name, Devices to be Deployed, Devices Deployed Successfully, and Devices Deployed with Errors.

Step 4 Examine job summary details by clicking **Details** in the lower pane.

Details of the Devices, New Image, Old Image, and the device status are displayed.

Step 5 Examine the Commentary on the devices in the job by clicking on the vertical **Commentary** tab on the far right. This shows the progress of the image install operation on the device.

Step 6 Examine the Transcript of the devices in the job by clicking on the vertical **Transcript** tab on the far right. This shows the chronology of the commands executed on the device and their responses.

Step 7 Examine job history details by clicking **History** in the lower pane. This shows the history of the transition in the job state.

Note This information is visible only in the workflow mode.

Aborting an Image Installation Job

You can abort an image installation job by clicking **Abort** from the Jobs page. This option is effective only for multi-device jobs:

Note If the job involves a single device, then Abort will have no effect after the job begins and the job will always run to completion.

- If the Sequential option is selected, then all the devices on which the job has not yet started will be aborted.

- If Parallel is selected, then all the devices till that batch will undergo image upgrade. All devices from the next batch onwards will be aborted.

Retry a Failed Image Install Job

If your attempts to deploy an image to one or more devices fails, you can retry the job. However, you should retry the entire job and not attempt to simply continue from a failed step.

To retry a failed job, do the following:

Step 1 To determine that an installation job has failed, go to the Jobs section in the selector and click **Install Jobs**.

The Jobs page appears.

Step 2 Determine the status of the job in question by examining the Status column.

Tip A green check icon with the word Deployed indicates success. A red X icon indicates failure.

Step 3 Investigate possible reasons for job failure.

Step 4 Select the failed image install job from the job list and click **Retry** from the toolbar atop the upper pane.

The Install Images on Devices window appears. You can observe the validation warnings as you would in a normal install job.

Step 5 As required, you can change the images, devices, schedule, or job properties to be used.

Step 6 From within the Install Images on Devices window click **Install.**

Step 7 Determine that the retried attempt is successful by observing the newly created job.

Roll Back a Deployed Job

You can roll back the changes from a deployed image installation job.

To roll back a Deployed job, do the following:

Step 1 From the job list, select the image install job to be rolled back and click **Rollback** from the toolbar atop the upper pane.

The Install Images on Devices window appears. You can observe the validation warnings as you would in a normal install job.

Step 2 As required, you can change the images, devices, schedule, or job properties to be used in the rollback.

Step 3 From within the Install Images on Devices window click **Install**.

Step 4 Determine that the rollback attempt is successful by monitoring the newly created job.

Image Installation Job Approval Workflow

Image update is a critical operation that has the potential to cause downtime for devices and your network. Hence, change control and management for image install operations is crucial. Change management for image installation jobs is done using the Deployment Workflow framework of Configuration Manager. This ensures that all image installation jobs need to be approved before getting executed or deployed.

To use workflow with image installation jobs, do the following:

Step 1 Enable workflow for image installation jobs:

a. In Configuration Manager, select **Tools > Security Manager Administration > Workflow**.

b. If workflow is not already enabled, select **Enable Workflow**.

c. Select **Require Deployment & Install Image Approval**.

d. Configure the email address of the person responsible for approving the image installation job in the Job/Schedule Approver field. For more information, see Workflow Page, page 11-55.

e. Click **Save** and then **Close**.

f. Launch Image Manager and navigate to **Install Jobs**. Notice the new buttons available in the Menu bar for job state transitions in workflow mode: Submit, Approve, Reject, and Deploy.

Step 2 To create and execute an image installation job with workflow enabled:

a. Use any of the previously documented procedures to create an image installation job. See About Image Updates on Devices Using Image Manager, page 70-18.

Note There is an additional option in the Properties tab to Submit the Job. Check this option to automatically submit the job for approval after creation of the job.

b. Once the image installation job is created, note the state of the job in the Image Install Jobs View.

c. Select the job and click **Submit** to submit the job for approval if automatic submit option was not selected while creating the job.

The job Approver (user with Approver role/privileges) receives an email notification to approve the job.

d. The Approver can log in to Security Manager, launch Image Manager, and navigate to the job.

e. The Approver clicks **Approve** to approve the job after reviewing the details of the upgrade, that is, image being upgraded to, job properties, schedule, and so on.

Job state is changed to *Approved*. The creator of the job receives an email that the job has been approved. Now the job can be deployed.

f. If the Approver is not convinced after reviewing the job details, he can choose to reject the job by clicking **Reject**.

The job state is moved to *Rejected*. The creator of the job receives an email that job has been rejected. A rejected job will not be deployed.

Note A rejected job will not be deployed. It can be edited and resubmitted for approval or it has to be discarded.

g. Once the job is approved, the job can be deployed by clicking **Deploy**.

   The job state is changed to *Deploying* and image install job execution is started.

h. If the job is rejected or any other changes are required to be made for a job, the job can be edited by clicking **Edit**.

   The Image Assignments page of the wizard showing all the devices and images is displayed. The user can modify the Job Properties, schedule and even delete some device-to-image assignments and submit the job for approval again by clicking **Submit**.

i. If a job has not started executing, then the user can dismiss the job by clicking **Discard**.

   The job is moved to *Discarded* state. A discarded job does not execute and cannot be edited or moved to any other state.

j. If the changed job is acceptable to the approver, he can approve the job this time and the job can be deployed as mentioned above.

k. Once the deploying job completes execution it will be moved to *Deployed* state if the image installation is successful or it will be moved to *Failed* state if the image installation operation fails.

Troubleshooting Image Management

This section addresses steps you can take to troubleshoot Image Management in response to particular symptoms.

No data for devices in Image Manager, after Security Manager upgrade. Any one of the following operations that first contacts the device will collect the image inventory for the device:

- Rediscover the device choosing to discover only Device Inventory
- Perform a live deployment to device
- Perform an Image Install operation to the device

Image Download from Cisco.com Fails

- Go to Configuration Manager > Tools > Security Manager Administration.
- Select Image Manager.
- Click **Test Connection** to ensure the server is reachable.
- Check ***%NMSROOT%/MDC/athena/config/****-CCOMetaData.xml*** for error in downloading metadata information for particular MDF IDs.

Update or Image Download fails due to certificate mismatch, unavailability, expiration, or other cause.

- Employ the recommended actions cited by the error message. Use the failed download URL from the error message to retrieve the certificate.
- View the stored certificate at ***%NMSROOT%/MDC/certificates/*.ser*** (Serialized object--file contents are unintelligible and cannot be viewed in any editor.)

Image Download from Cisco.com Fails with Message: "User not authorized to download file"

- Go to Configuration Manager > Tools > Security Manager Administration.
- Select Image Manager.
- Click **Test Connection** to ensure the server is reachable.

- Register your acceptance of the Cisco Encryption Software Usage Handling and Distribution Policy.

Tip The policy is found at: http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y.

Image Download from Cisco.com is Slow

- Ensure proxy is configured
- Trace route from Security Manger to Cisco.com

Check for Updates Fails

Go to the Security Manager administrative settings page and test connectivity to Cisco.com. Check ***%NMSROOT%/MDC/athena/config/****-CCOMetaData.xml*** for an error in downloading metadata information for particular MDF IDs.

Message: "User not authorized to download file." Go to the Security Manager administrative settings page and test connectivity to Cisco.com. Accept the crypto agreement at http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y

Image Download from External File System or Network Fileshare Fails

- Check that you have proper permissions/credentials for the external file system or fileshare.
- Open the fileshare on the client, drag the image and drop it on Image Manager.

Image Install Wizard does not Show Compatible Images

- Image Manager uses the information on Cisco.com to determine the compatibility of the images for the MDF IDs. Please download the latest images available on cisco.com by performing 'Check for Updates'. If the image is available on Cisco.com and listed as compatible for the platform, you should now be able to view these images for the device in the Image Install Wizard and also in the Compatible Images tab for the device.
- Even the Compatible Images tab for the device may not show some images that are actually compatible to the device.
- If you still don't see the images in the Install Wizard, either because you do not have Cisco.com connectivity or images are not updated on Cisco.com for that platform, you can use the drag and drop procedure to install the images on the device. You would be warned that the image is not compatible, but you can still go ahead and install the image by dragging the image and dropping it on to the device and creating a job.

Image Copy Failure –"HTTP 413 Error"

- Right-click **Device** in Image Manager > Test File Copy To Device
- Check Error Message in vmssharedsvcs.log
- If you encounter an HTTP 413 error, split the job to contain a smaller number of images in one job

Image Copy Failure –"Not enough space on disk"

- Check Device > Storage View for files on device and free space in the Image Install Location.
- If Device > Storage View shows files, then delete files from Storage to make space and retry.
- If Device > Storage View does not show files, either because it is a greenfield device or it is a Security Manager upgrade setup, rediscover only the device inventory on the device and then delete files from Storage view to make space.

Image Install Job failure –Error: "Invalid flash device"

- Check if flash exists on the device:
  - Right-click on device in IM > Test File Copy to Device
  - Connect to device, and check whether it is a multiple-context device that is being managed as a single context device in Security Manager
  - Rediscover the device selecting to discover **System Context**. Then, retry the image install job.

Image Upgrade Job on Active/Standby pair fails

- Error: ***"This host is not the 'active' device in the failover pair"***- Ensure that the failover pair is managed in Security Manager via the IP address of the active device in the failover pair and not the IP address of the standby device.
- Error: ***"Secondary device is not in standby-ready state"*** - Ensure that the devices in the failover pair are up and the standby device is in standby-ready state. Job will abort if standby device is in failed state

Image Install Job failure –Error: "SWIM1114: Device could not be reached after upgrade"

- Manually check if device is reachable. Solution: After image upgrade, device has to be re-added in Security Manager or change the Admin option to "Do not check certificate authentication"
- Check whether Tools > Admin > Device Communication > SSL Certificate Parameters > PIX/ASA/FWSM Device Authentication Certificates is set to "Retrieve while adding devices."
- After image upgrade, ensure the device has been re-added in Security Manager. Otherwise, change the Admin option to "Do not check certificate authentication."

Note You must have accepted the latest Cisco.com certificate to enable Image Manager to interface with cisco.com. You must accept the certificate from both the "Image Meta-data locator" site and the download site of the images to start downloading images successfully (see Image Manager Page, page 11-29).

No data for devices in Image Manager after Security Manager upgrade

- Rediscover the device choosing to discover only Device Inventory
- Perform a live deployment to device
- Perform an image install operation to the device

Trying to retry or rollback a job fails

- Check if any of the devices in the job are deleted from Security Manager
- Check if none of the images to be retried or rolled back to are unavailable in Security Manager. Add the images to the Security Manager repository and retry the operation