



CHAPTER 9

Managing Software Images Using Software Management

Manually upgrading your devices to the latest software version can be an error-prone, and time-consuming process. To ensure rapid, reliable software upgrades, Software Management automates the steps associated with upgrade planning, scheduling, downloading, and monitoring.

This chapter contains:

- [Setting Up Your Environment](#)
- [Software Repository](#)
- [Software Distribution](#)
- [Using Software Management Job Browser](#)
- [Understanding User-supplied Scripts](#)
- [Locating Software Management Files](#)

Using Software Management, you can:

- Set up your Software Management preferences.
 - You can specify information such as the directory where images are stored, and the pathname of the user-supplied script to run before and after each device software upgrade.
 - You can enable and define the protocol order for Software Management tasks. You can also enable the Job Based Password option for Software Management tasks.
 - You can specify if the images on Cisco.com should be included during image recommendation of the device. Also specify the Cisco.com filters so that only the images that match the filter criteria are selected.
- Analyze software upgrades
 - You can generate Upgrade Analysis reports that help you determine prerequisites for a new software deployment.
 - These reports analyze the proposed images to determine the hardware upgrades (device access, boot ROM, Flash memory, RAM, and NVRAM and boot Flash, if applicable) required before you can perform the software upgrade.
 - See [Upgrade Analysis](#) for further details.

- Perform In Service Software Upgrade (ISSU)

LMS supports the In Service Software Upgrade (ISSU) process that allows Cisco IOS software images to be updated without rebooting the device. This process increases network availability and reduces downtime caused by planned software upgrades.

See [Support for In Service Software Upgrade](#) for further details.
- Import images into the software repository

You can determine the images missing from your repository and import them into the software repository.

You can also keep the repository up-to-date and periodically synchronize the repository with the images running on your network devices.

You can also schedule an image import for a later, more convenient time.

See [Adding Images to the Software Repository](#) for further details.
- Distribute software images to groups of devices

Depending on system complexity, you can configure upgrades for groups of devices to the same software image or to different software images.

You can specify these groups manually, using your groups and search criteria. You can also use some other selection criterion, such as the current software version or hardware type to specify the groups.

You can run the device upgrades job sequentially or in parallel. After upgrading the devices, you can also specify the reboot order.

See [Software Distribution](#) for further details.
- Distribute images as patches to group of devices

Depending on system complexity, you can configure upgrades for groups of devices to the patch software images.

You can specify these groups manually, using your groups and search criteria. You can also use some selection criterion, such as the current software version or hardware type.

You can run the device upgrades job sequentially or in parallel. After upgrading the devices, you can also specify the reboot order.

See [Patch Distribution](#) for further details.
- Reduce errors by using a recommended image

Software Management checks the current software version, Flash device size, DRAM size, boot ROM version. Software Management also checks any device type specific software and hardware requirements for compatibility. Software Management checks and recommends a best-fit image for a device.

See [Understanding Upgrade Recommendations](#) for further details.
- Schedule image upgrade jobs

You can schedule image upgrades to occur immediately or at a later, more convenient time. Optionally, you can integrate software upgrade scheduling into your internal change approval process.

After an upgrade, you can:

- Undo the upgrade and roll back to the previous image

Software Management tracks the image history of each device so that if you upgrade to a new image, you have a record of what has been installed on the device. This information allows you to undo the upgrade and roll back to the previous image, if necessary.

A Change Audit record is logged for this task. You can generate the Standard Change Audit report. See *Reports Management with Cisco Prime LAN Management Solution 4.2* for more information.

See [Undo a Successful Distribution Job](#) for further details.

- Retry the upgrade on devices that failed in a previous job

You can also retry a job for devices that failed the upgrade process. For example, you may need to do this because of a configuration error or a bad network connection.

You can retry the job and include only those devices that were not upgraded previously.

See [Retry a Failed Distribution Job](#) for further details.

- Track job progress and job history information

Software Management generates detailed job reports. These reports display the status of each software upgrade and a detailed job log. They also keep track of job and device operations and job history information.

See [Using Software Management Job Browser](#) for further details.

- Track software bugs

You can view the known catastrophic or severe bugs in the software running on the devices supported by Software Management using Locate Device Report (**Reports > Cisco.com > Locate Device Report**).

See *Reports Management with Cisco Prime LAN Management Solution 4.2* for further details.

- Set the debug mode for Software Management application

You can set the debug mode for Software Management application in the Log Level Settings dialog box (**Admin > System > Debug Settings > Config and Image Management Debugging settings**).

See *Administration of Cisco Prime LAN Management Solution 4.2* for further details.

- The supported IOS image version is 11.x and later.

For list of supported devices in the Software Management application, see:

- Supported Image Import Features for Software Management

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

- Supported Image Distribution Features for Software Management

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

Setting Up Your Environment

This section lists all prerequisites for using the Software Management in LMS.

- [Requirements on LMS Server](#)
- [Logging Into Cisco.com](#)
- [Configuring Devices for Upgrades](#)
- [Using Job Approval for Software Management](#)

Requirements on LMS Server

The following are the prerequisites:

- Make sure you have a directory or file system location with enough space to store the software images.
- Verify that you have the appropriate privilege level to access Software Management options. You can view the Permission Report (**Reports > System > Users > Permission**) to know the various privilege levels.
- 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 web site.
- If your system is behind a firewall, configure the proxy URL to access the Internet from the installed system. You can do this using **Admin > System > Cisco.com Settings > Proxy Server Setup**.

You can enter Cisco.com credentials when you use the Software Management tasks.

See [Logging Into Cisco.com](#) for further details.

Mandatory Setup Tasks

- Add the device passwords to the Device and Credentials database. You can add these credentials using **Inventory > Device Administration > Add / Import / Manage Devices**. Also, see [Configuring Telnet and SSH Access](#) for further details.
- Use the **Admin > System > System Preferences** option to enter the name of your SMTP server. You have to configure the SMTP server to send e-mails.

We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (**Admin > System > System Preferences**). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.

- If you plan to enable a remote file copy (RCP) or secure copy server as the active file transfer server, see [Configuring RCP](#) or [Configuring SCP](#) for further details.
- Set or change your Software Management preferences. See *Administration of Cisco Prime LAN Management Solution 4.2* for further details.

Optional Setup Tasks

- Make a baseline of your network images by importing images from the Software Management-supported devices in your network into your software image repository.
To do this, go to **Configuration > Tools > Software Image Management > Software Repository** and click **Add** and select **Device**.
- Schedule the Synchronization report to run periodically. This is used to determine whether any images running on Software Management-supported devices are not in the software image repository.
To generate the report, go to **Configuration > Tools > Software Image Management > Repository Synchronization**.
- If you use the Job Approval option to approve or reject jobs, you must create one or more approver lists and enable Job Approval. See *Administration of Cisco Prime LAN Management Solution 4.2* to enable Job Approval.

Logging Into Cisco.com

Login privileges are required for all Software Management tasks that access Cisco.com.

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 web site.

To download the cryptographic images on Cisco.com through Software Management tasks, you must have a Cisco.com account with cryptographic access.

To get the access you must have a Cisco.com account. You can register by going to the following URL:
<http://tools.cisco.com/RPF/register/register.do>

After getting the Cisco.com account:

-
- Step 1** Go to the following URL: <http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y>
The Enter Network Password dialog box appears.
- Step 2** Log in with your Cisco.com account.
The Encryption Software Export Distribution Authorization Form page appears.
- Step 3** Select your software from the list box and click **Submit**.
The Encryption Software Export Distribution Authorization Form appears.
- Step 4** Review and complete the Encryption Software Export Distribution Authorization form and click **Submit**.
The Cisco Encryption Software: Crypto Access Granted message appears.



Note

It takes approximately 4 hours to process your application. You cannot download the software until the entitlement process is complete. You will not receive any notification for this.

On LMS Server, you can enter Cisco.com credentials for Individual user Cisco.com credentials.

You can enter your individual Cisco.com credentials when you perform any Software Management tasks that need access to the Cisco.com server.

If your Cisco.com username and password have not been added to the LMS database, enter your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, the credentials are valid only for that session.

If your Cisco.com username and password have been added to the LMS database, then Cisco.com login dialog box appears with the information that is available in the LMS database.

If you are accessing Cisco.com over a proxy server, you must enter the proxy server details in the Proxy Server Setup dialog box (**Admin > System > Cisco.com Settings > Proxy Server Setup**).

Using Job Approval for Software Management

You can enable Job Approval for Software Management tasks, (**Configuration > Job Browsers > Job Approval**), which means all jobs require approval before they can run.

Only users with Approver permissions can approve Software Management jobs. Jobs must be approved before they can run if Job Approval is enabled on the system.

The following Software Management tasks require approval if you have enabled Job Approval:

- Adding images to Software Repository (**Configuration > Tools > Software Image Management > Software Repository > Add**) using:
 - Cisco.com
 - Device
 - URL
 - Network (Use Out-of-sync Report)
- Distributing software images (**Configuration > Tools > Software Image Management > Software Distribution**) using any one of these methods:
 - Distributing by Devices [Basic]
 - Distributing by Devices [Advanced]
 - Distributing by Images
 - Remote Staging and Distribution

If you have enabled Approval for Software Management tasks, then in the Job Schedule and Options dialog box, you get these two options:

- Maker Comments—Approval comments for the job approver.
- Maker E-Mail—E-mail ID of the job creator.

See *Administration of Cisco Prime LAN Management Solution 4.2* for more details on creating and editing approver lists, assigning approver lists, setting up Job Approval, and approving and rejecting jobs.

Software Repository

The Software Repository Management window displays the images that are available in the Software Management repository.

This section contains:

- [Software Repository Synchronization](#)
- [Scheduling a Synchronization Report](#)
- [Viewing a Synchronization Report](#)
- [Removing a Synchronization Report Job](#)
- [Adding Images to the Software Repository](#)
- [Synchronizing Software Image Status With Cisco.com](#)
- [Deleting Images From the Software Repository](#)
- [Exporting Images from Software Repository](#)
- [Searching for Images from Software Repository](#)
- [Software Image Attributes](#)

The Software Repository Management window contains the following fields, buttons, and the entry in the TOC:

- [Software Repository Management Window Fields](#)
- [Software Repository Management Window Buttons and TOC Entry](#)

Table 9-1 Software Repository Management Window Fields

Fields	Description
File Name	File name of the software image. Click on the File Name to edit the image attributes. See Editing and Viewing the Image Attributes .
Image Family	Name of the image family.
Image Type	Type of the images (SYSTEM_SW, SUPERVISOR, SUPERVISOR2_6000, SUPERVISOR6000, BOOT_LOADER, ATM_WBPVC, etc.).
Version	Software version number.
Size	Image size in megabytes.
Status	Status of the image on Cisco.com. See Synchronizing Software Image Status With Cisco.com .
Updated at	Date and time the image was checked into the repository.
Comments	Comments, typically used to track the reason for adding the image to the repository.

Table 9-2 lists and describes the buttons and TOC entries in the Software Repository Management Window.

Table 9-2 Software Repository Management Window Buttons and TOC Entry

Buttons and TOC Entry	Description
Software Repository Synchronization (TOC entry)	Keep the software repository up to date. See: <ul style="list-style-type: none"> • Software Repository Synchronization • Scheduling a Synchronization Report • Viewing a Synchronization Report • Removing a Synchronization Report Job
Filter (Button)	Filter and search images. See Searching for Images from Software Repository .
Add (Button)	Add images to the repository. See Adding Images to the Software Repository .
Delete (Button)	Delete images from the repository. See Deleting Images From the Software Repository .
Export (Button)	Export images from Repository. See Exporting Images from Software Repository .
Update Status (Button)	Update the status of the images. See Synchronizing Software Image Status With Cisco.com .

Software Repository Synchronization

The Synchronization report shows the Software Management-supported devices that are running software images not available in the software image repository.

Using this option you can view and schedule the synchronization report.



Note

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

Select **Configuration > Tools > Software Image Management > Software Repository Synchronization**.

The Software Repository Synchronization dialog box that appears contains the following:

Table 9-3 Software Repository Synchronization Dialog Box

Fields/Buttons	Description
Job Id	Unique number assigned to the job when it is created.
Next Run	Time and date of the next instance of Synchronization Report job.

Table 9-3 Software Repository Synchronization Dialog Box (continued)

Fields/Buttons	Description
View Report	You can view the synchronization report. This report displays the Software Management-supported devices that are running software images not available in the software image repository. See Viewing a Synchronization Report for further details.
Schedule	You can schedule a Synchronization report. You can also reschedule an existing Synchronization report. See Scheduling a Synchronization Report for further details.
Remove Job	You can remove the scheduled synchronization report job. See Removing a Synchronization Report Job for further details.

Scheduling a Synchronization Report

To schedule or reschedule a Synchronization report:

-
- Step 1** Go to **Configuration > Tools > Software Image Management > Software Repository Synchronization**. The Software Repository Synchronization dialog box appears.
- Step 2** Click **Schedule**. The Job Schedule for Out-of-sync Report dialog box appears.
- Step 3** Enter the following information:

Field	Description
Scheduling	
Run Time	<p>You can specify when you want to run the Image Out-of-Sync Report job.</p> <p>To do this, select one of these options from the drop-down menu:</p> <ul style="list-style-type: none"> Daily—Runs daily at the specified time. Weekly—Runs weekly on the day of the week and at the specified time. Monthly—Runs monthly on the day of the month and at the specified time. <p>The subsequent instances of periodic jobs will run only after the earlier instance of the job is complete.</p> <p>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2 only if the earlier instance of the November 1 job has completed.</p> <p>If the 10.00 a.m. November 1 job has not been completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.</p>
Date	Select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	<p>The system default job description, <i>SoftwareImages Out Of Synch Report</i> is displayed.</p> <p>You cannot change this description.</p>
E-mail	<p>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job.</p> <p>You can enter multiple e-mail addresses separated by commas.</p> <p>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences).</p> <p>We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.</p>

- Step 4** Click **Submit**.

If the job was scheduled successfully, the notification dialog box is displayed with the Job ID. You can check the status of your scheduled synchronization job by selecting **Configuration > Tools > Software Image Management > Jobs**.

Viewing a Synchronization Report

To view a synchronization report:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository Synchronization**.

The Software Repository Synchronization dialog box appears.

Step 2 Click **View Report**.

The Image Out-of-sync Report window appears.

Removing a Synchronization Report Job

To remove a Synchronization Report job:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository Synchronization**.

The Software Repository Synchronization dialog box appears.

Step 2 Click **Remove Job**.

A confirmation dialog box shows that the synchronization report job is removed successfully.

Step 3 Click **OK**.

Adding Images to the Software Repository

Your software image repository should contain copies of software images running on all Software Management-supported devices in your network. Use the following options to populate and maintain your software repository:

- Add Image to Software Repository using the Cisco.com option downloads images for devices in LMS from Cisco.com to the software repository.

See [Adding Images to the Software Repository From Cisco.com](#).

- Add Image to Software Repository using the Device option
 - Imports images from selected Cisco devices to the software repository.
 - Imports software from Flash cards on a live device to the software repository.

See [Adding Images to the Software Repository From Devices](#).

- Add Image to Software Repository using the File System option imports an image from a directory accessible from the LMS server.

See [Adding Images to the Software Repository From a File System](#).

- Add Image to Software Repository using the URL option downloads images from the URL you specify.
See [Adding Images to the Software Repository From a URL](#).
- Add Image to Software Repository using the Network option creates a baseline of all Software Management-supported devices in your network, and imports these images into your software repository.
See [Adding Images to the Software Repository From the Network](#).

Adding Images to the Software Repository From Cisco.com

Use this option to download software images from Cisco.com into the software image repository.

- Contact your channel partner or enter a request on the main Cisco web site. If you do not have a user account and password on Cisco.com.
See [Logging Into Cisco.com](#).
- Access the Cisco.com web site to make sure that the releases for the images you plan to download are stable.
- Determine the approximate number and size of the images you want to download. The number of images you can download at a time can vary depending on Cisco.com load, image sizes, network load, and LMS server load.



Note

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

To add images from Cisco.com:

-
- Step 1** Select **Configuration > Tools > Software Image Management > Software Repository**.
The Software Repository Management dialog box appears.
 - Step 2** Click **Add**. Do not select any images from Software Repository Management window.
The Image Source dialog box appears.
 - Step 3** Select **Cisco.com**.
The Cisco.com and Proxy Server Credential Profile dialog box appears.
 - Enter your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.
 - You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:
Admin > System > Cisco.com Settings > Proxy Server Setup
 - After entering the credential information, Click **OK**.
 - Step 4** Click **Next**.
The Device Selection dialog box appears.

Step 5 Select the device from the Device Selection dialog box, and click **Next**.

If you do not want to select any devices, click **Next**.

If you select devices from this list, they identify a subset of device software images. This helps you narrow your options on subsequent screens.

The Add Images from Cisco.com dialog box appears. This dialog box has several sections from which you select combinations of device platforms, software release versions, and software subset images.

See *Inventory Management with Cisco Prime LAN Management Solution 4.2* for information on how to use the Device Selector.

Step 6 Select the images to download. Work from left to right and from top to bottom:

a. From the Select a Device/Platform section, select a device or device family.

If you select an individual device, the device family, Cisco IOS release, and required Flash and RAM sizes appear.

For IPX/IGX/BPX/MGX devices, the system software release appears.

A list of available software versions for that device appears in the top middle section.

b. From the Software Versions section, select a software version.

If you are unsure of the subset image you need, see the Release Notes on Cisco.com.

- For IPX/IGX/BPX platforms, both switch software and all applicable module firmware images appear.
- For MGX platforms, system releases appear.

A list of available subset images for the selected software version appear in the top right frame.

c. From the Software Subset Images section, select a subset image.

The subset image is added to the Images to be Added table in the bottom section.

For IPX/IGX/BPX/MGX devices, there are no subset images. Select the item that appears in this section to complete image selection.

Step 7 Continue adding images to the list.

The images that you have added appear in the Images to be Added table. This table contains the following information:

- Devices/Platforms—Name of the device or platform.
- Version—Software version that you have selected.
- Subset—Subset image information.

Step 8 Click **Next** when the list contains all image combinations to download.

Software Management verifies that the images in the Image list run in the selected devices and displays the status in the Add Images from Cisco.com dialog box. The Add Images from Cisco.com dialog box contains:

Field	Description
Device/Platform	Lists the device details that you have selected.
Selected Version and Subset	Displays the image details.
Image Requirements	Displays the required hardware (RAM and Flash) details.

Field	Description
Download	<p>Select the image you want to download.</p> <p>By default, the check boxes are selected for the images that have passed the verification.</p> <p>You can choose not to add an image by deselecting that check box.</p>
Pass/Fail	<p>Results of image verification.</p> <ul style="list-style-type: none"> • Pass—Device has the minimum required memory and Flash memory. • Fail—Device does not have enough memory or Flash memory. <p>Images that fail verification on one device could work on another. Therefore, you can download a failed image by selecting the Download check box.</p>

Step 9 Select the images to add to the image repository in the Add Images from Cisco.com dialog box and click **Next**.

The Job Control Information dialog box appears.

Step 10 Enter the following in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	<p>You can specify when you want to run the Image Import (from Cisco.com) job.</p> <p>To do this, select one of these options from the drop-down menu:</p> <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected Once for Run Type, select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	<p>Enter the e-mail address to which the job sends messages at the beginning and at the end of the job.</p> <p>You can enter multiple e-mail addresses separated by commas.</p> <p>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences).</p> <p>We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.</p>
Comments	Enter additional information about this job.

Field	Description
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 11 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name that you have selected. It also displays the file size of the image.

Step 12 Click **Finish**.

If the job was scheduled successfully, the notification dialog box appears with the Job ID.

To check the status of your scheduled synchronization job, select **Configuration > Tools > Software Image Management > Jobs**.

Adding Images to the Software Repository From Devices

Use this procedure to add software images from Cisco devices to the software repository.

Software Management downloads images from more than one device in parallel. You must ensure that software repository has enough free space to accommodate at least 20 images.

The image import from device option is not available for all the devices. Find the devices from which you can download images in the Supported Image Import Features for the Software Management table on Cisco.com.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

**Note**

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

To add images from devices:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**.

Do not select any images from Software Repository Management window.

The Image Source dialog box appears.

Step 3 Select **Device**, and click **Next**.

The Device Selection dialog box appears in the Add Images from Device window.

See *Inventory Management with Cisco Prime LAN Management Solution 4.2* for information on how to use the Device Selector.

Step 4 Select the devices that contain the images to add to the software repository.**Step 5** Click **Next**.

Software Management retrieves the images, analyzes them according to the selected image type, and displays a report that contains:

Field	Description
Image	Images available on your device.
Available At	Location where the image is available on your device.
Device	Name of the device as managed by LMS.
Size	Image size in bytes.
Errors	Click on the link for details.

By default, the check boxes of the images that are not in the software repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 6 Click **Next**.

The Job Control Information dialog box appears.

Step 7 Enter the following in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from Device) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected Once for Run Type, select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.

Field	Description
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 8 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This description is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name that you have selected. The field also displays the file size of the image.

Step 9 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job select **Configuration > Tools > Software Image Management > Jobs**.

Adding Images to the Software Repository From a File System

Use the following procedure to add software images from a file system to the software repository.

You have to know the directory name in which the image files are stored before importing the images from the File System to the software repository.



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

To add images from file system:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add..**

Do not select any images from the Software Repository Management window.

The Image Source dialog box appears in the Add Images window.

Step 3 Click **File System**, and click **Next**.

The Add Image From Local File System dialog box appears.

Step 4 Enter the full pathname of the source file or directory.

Or

- a. Click **Browse** to search for the directory name.
The Server Side File Browser dialog box appears.
- b. Select either the file or the directory on the LMS server.
- c. Click **OK**.

Step 5 Click **Next**.

The Image Attributes dialog box appears with this information:

- **Filename**—Filename as it appears in filesystem directory.
You cannot add an image if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.
- **Image Type**—Image type, determined from the filename. If the image type is not correct, select the correct type from the drop-down list box.

Software Management tries to determine the image type from the filename. If it cannot determine the image type (for example, if the image has been renamed using a nonstandard name), it labels the image type as `Unknown`.

By default, the check boxes of the images that are not in the software repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 6 Click **Next**.

The Image Attributes window appears with the following information for verification:

Field	Description	Usage Notes
File Name	Filename as it appears in filesystem directory	You cannot add images if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.
Size	Size of file in bytes.	None.
Image Family	Device family name.	None.
Image Type	Image type, determined from the filename.	Software Management tries to determine the image type from the filename. If it cannot determine the image type (for example, if the image has been renamed to a nonstandard name), it labels the image type as <code>Unknown</code> . You must select an image type from an available option before you can add the file to the repository.
Version	Version of the image	None.
Errors	Click on the link for details.	None.

Step 7 Click **Finish**.

A pop up window appears for you to enter a description.

Step 8 Either:

- Click **OK**.

The Software Repository Management window appears with the newly added images. The description that you have entered appears in the Comments column in the Software Repository Management window.

Or

- Click **Cancel**.

The Software Repository Management window appears with the newly added images. The Comments column in the Software Repository Management window will be blank for this task.



Note

The import from File System may take more time if you have selected many images.

Adding Images to the Software Repository From a URL

Use the following procedure to add software images from a URL to the software repository.



Note

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

To add images from URL:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management window appears.

Step 2 Click **Add**.

Do not select any images from the Software Repository Management window.

The Image Source dialog box appears in the Add Images window.

Step 3 Click **URL**, and click **Next**.

The Add Image From URL dialog box appears.

Step 4 Enter the URL details.

For example: `http://servername:portnumber/file_location/`

Where,

- *servername* is the name of the server where the image resides.
- *portnumber* is the http port number.
- *file_location* is the image location on the server. The *file_location* can be swimtemp or htdocs folder.

For example,

If the image is in swimtemp, then the URL is `http://servername:portnumber/swimtemp/image_file`

If the image is in the htdocs, then the URL is `http://servername:portnumber/image_file`

The web server must be running on the destination machine. You can use only HTTP URLs. The remote server should not have any authentication.

Step 5 Click **Next**.

The Job Control Information dialog box appears.

Step 6 Enter the following information in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from URL) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected Once for Run Type, select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You cannot enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 7 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This description is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name that you have selected. It also displays the file size of the image.

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Adding Images to the Software Repository From the Network

This option allows you to import running images from all Software Management-supported devices in your network into the software image repository.

Use this option to create a baseline of the image in your network and populate the software image repository. Use the Synchronize report option to review the Software Management supported devices are running images that are not in the Software Repository.

**Note**

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

You must locate your device in the Supported Image Import Features for Software Management table on Cisco.com. This is because the image baseline capabilities might not be available yet for all devices.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

To add images from network:

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Click **Add**. Do not select any images from the Software Repository Management window.

The Image Source dialog box appears.

Step 3 Select **Network**, and click **Next**.

Software Management checks the devices on your network and the software images running on those devices.

To run this check faster, select **Use generated Out-of-sync Report** to find the images that are not in the Software Images repository.

You should generate an Out-of-sync Report before selecting this option. The running images in the network that are not in the Software Repository, appear in the Network Baseline dialog box.

If you have not selected the Use generated Out-of-sync Report option, all running images that are not in the Software Repository appear in the Network Baseline dialog box.

The Network Baseline dialog box contains the following information:

Field	Description
File Name	Filename as it appears in filesystem directory. You cannot add an image if a file with the same name already exists in the software repository or if the minimum required attributes cannot be retrieved.
Size	Image size in bytes.
Available at	Location where the image is available on your device.
Error	Click on the link to review the details.

By default, the check boxes of the images that are not in the Software Repository are selected. You can choose not to add an image by deselecting the corresponding check box.

Step 4 Select/deselect the images and click **Next**.

The Job Control Information dialog box appears.

Step 5 Enter the following information in the Job Control Information dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Import (from Network) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	If you have selected Once for Run Type, select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.

Step 6 Click **Next**.

The Image Import Work Order dialog box appears with the following information:

Field	Description
Job Description	Displays the job description. This description is what you entered while scheduling the job.
Work Order	Displays the details of the device name and image name that you have selected. It also displays the file size of the image.

Step 7 Click **Finish**.

If the job was scheduled successfully, the notification dialog box appears with the Job ID.

To check the status of your scheduled synchronization job, select **Configuration > Tools > Software Image Management > Jobs**.

Synchronizing Software Image Status With Cisco.com

You can check if the software images that are in your software repository are valid images using the Update Status button in the Software Repository Management window.

The Status table column is updated with the following status:

- Not Deferred—Displayed when this image is a valid image.
- Deferred—Displayed when this image is not supported and not available to be downloaded from Cisco.com.

This image is not recommended by Software Management.

- Software Advisory Notice—Displayed when this image has some issues. You can download this image from Cisco.com.

This image may be recommended by Software Management. However, you have to read the Software Advisory Notice before importing or upgrading your device.

- Unknown—Displayed when you have added images to the repository for the first time, using any one of these methods:
 - Add Images by Devices
 - Add Images by File system
 - Add Images by URL
 - Add Images from Network

Use the Update Status button to update the status field.

- Not available—Displayed when information is not available on Cisco.com.

Read the software release notes on Cisco.com for more details.

**Note**

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

To synchronize Software Image Status with Cisco.com:

-
- Step 1** Select **Configuration > Tools > Software Image Management > Software Repository**.
The Software Repository Management dialog box appears.
- Step 2** Select the images for which you want to know the status and click **Update Status**.
The Cisco.com login dialog box appears.
- If your Cisco.com username and password have not been added to the LMS database, enter your Cisco.com username and password, click **OK**. If you enter Cisco.com credentials in this workflow then the credentials are valid only for that session.
 - If your Cisco.com username and password have been added to the LMS database, the Cisco.com login dialog box appears with the information that is available in the LMS database. Click **OK**.
- A confirmation message appears that Image Status was retrieved from Cisco.com successfully.
- Step 3** Click **OK**.
Review the Status table column in the Software Repository Management window.
-

Deleting Images From the Software Repository

To delete software images from the software repository:



Note

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

-
- Step 1** Select **Configuration > Tools > Software Image Management > Software Repository**.
The Software Repository Management dialog box appears.
- Step 2** Select the images that you want to delete, then click **Delete**.
A confirmation message appears, `The selected images will be deleted.`
- Step 3** Click **OK**.
The Software Repository Management window reappears with the selected images deleted.
-

Exporting Images from Software Repository

To export software images from the Software Repository:

-
- Step 1** Select **Configuration > Tools > Software Image Management > Software Repository**.
The Software Repository Management dialog box appears.
- Step 2** Select images that you want to export, then click **Export**.
A confirmation message appears, The selected images will be exported.
- Step 3** Click **OK**.
The Select directory to export window appears.
- Step 4** Click on **Browse** to select a directory to which you want to export the selected images.
The Server Side File Browser dialog box appears.
- Step 5** Choose the required directory and click **OK**.
The Image Directory field in the Select directory to export window displays the directory location that you had selected.
- Step 6** Click **Next**.
A progress bar appears indicating the progress of the export of images.
The Export Images Summary Report appears, after the image export is completed with the following details:
- Number of Selected Images
 - Target Directory
 - Summary
- Step 7** Click **Finish**.
You have successfully exported the images to the selected directory.
-

Searching for Images from Software Repository

To search software images from the software repository:



Note

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

Step 1 Select **Configuration > Tools > Software Image Management > Software Repository**.

The Software Repository Management dialog box appears.

Step 2 Select one of the following from the Filter by drop-down list:

- File Name
- Image Family
- Image Type
- Version
- Size
- Updated At

You cannot use wildcard characters. However, you can filter based on the first character.

For example: If you have images with file names `c3640-i-mz.112-24.P.bin`, `c3640-i-mz.112-25.P.bin`, `cat5000-sup.5-5-18.bin`, and `cat5000-supg.6-4-10.bin`.

If you select File Name as the Filter by option and enter the value as `c3`. The filter result displays only `c3640-i-mz.112-24.P.bin` and `c3640-i-mz.112-25.P.bin` images.

Step 3 Click **Filter**.

The Software Repository Management window appears with the filtered image details.

Software Image Attributes

To ensure that Software Management is using the most current information about an image, you should keep the image attributes up to date. Software Management uses image attribute information to:

- Recommend the appropriate image for a given device

When you distribute an image from the software repository to a device, Software Management uses the image attributes to recommend an image.
- Notify you when a Flash memory or DRAM upgrade is required (upgrade analysis)

When you distribute an image from the Software Repository to a device, Software Management compares the current Flash memory and DRAM attributes with the Flash memory and DRAM requirements for the new image.

The following sections contain:

- [Understanding Software Image Attributes](#)
- [Understanding Default Attribute Values](#)
- [Finding Missing Attribute Information](#)
- [Editing and Viewing the Image Attributes](#)

Understanding Software Image Attributes

To ensure that Software Management is using the most current information about an image, keep the image attributes updated.

If you do not have all the image attribute information when you add the image to the Software Repository, you must edit the attributes when the information becomes available.



Note

The auto fill of the Minimum NVRAM, Minimum RAM and Minimum Bootflash image attributes is applicable only for IOS.

The attributes for software images are:

Table 9-4 Software Image Attributes

Attribute	Description	Usage Notes
Minimum RAM	Minimum RAM required.	Select it from the list of options.
Minimum Flash	Minimum Flash memory required.	Select it from the list of options.
Minimum Boot ROM Version	Minimum bootstrap version required.	Enter text in standard Cisco IOS format: a.b(c).
Minimum system software version	Minimum system software version required on the device to upgrade the microcode image (MICA portware, Microcom firmware, CIP microcode only)	Enter text in standard Cisco IOS format: a.b(c).
Minimum supervisor version	Minimum software image version required on supervisor engine module. Cisco Switches can contain any number of modules such as, ATM, FDDI/CDDI, etc. These modules can run different images. There are some interdependencies among the software images that can run on the supervisor engine module and the ATM, FDDI/CDDI, and Token Ring modules residing on the same device chassis.	Enter text in standard Cisco IOS format: a.b(c).
Minimum NVRAM	Minimum NVRAM required to run image on Supervisor Engine III.	Select from list of options.

Understanding Default Attribute Values

The Unknown attribute option has different meanings for different image attributes.

Attribute	Description
RAM	If you select Unknown , Software Management computes the RAM value.
Flash Size	If Min.Flash is unknown, it is ignored. If the image size is unknown, the required Flash size to copy the image cannot be determined and the image cannot be used for upgrade.
Boot ROM Version	If you select Unknown , no value is stored in this field and the image can run with any boot ROM image version.

Finding Missing Attribute Information

When you import an image from another filesystem, the image might not contain all the attribute information that Software Management requires.

You can find the missing attribute information in the following ways:

- Read the Release Notes on Cisco.com or the documentation CD-ROM.
- Review the image attribute information that is available along with the images, when you download the images from Cisco.com.

You can update the missing attribute information in the Edit/View Image Attributes dialog box.

See [Editing and Viewing the Image Attributes](#) for further details.

Editing and Viewing the Image Attributes

LMS allows you to edit and view image attributes.



Note

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

To edit the software images attributes:

-
- Step 1** Select **Configuration > Tools > Software Image Management > Software Repository**.
The Software Repository Management dialog box appears.
 - Step 2** Click the **File Name**.
The Edit/View Image Attributes dialog box displays attributes for the selected image type.
 - Step 3** Make your changes in the available editable fields.
For editable image attributes, you will get either a drop-down list or text fields that you can edit.

Step 4 Either:

- Click **Update**, if you have updated the image attributes.
The Software Repository Management dialog box appears after updating the attributes.
Or
 - Click **OK**, if you have not updated the image attributes.
The Software Repository Management dialog box appears without updating the attributes.
-

Software Distribution

Software Distribution allows you to distribute images in your network and to analyze and determine the impact and prerequisites for new software images before distribution.

This section contains:

- [Upgrade Analysis](#)
- [Software Distribution Methods](#)
- [Patch Distribution](#)
- [Remote Staging and Distribution](#)
- [Understanding Upgrade Recommendations](#)

Upgrade Analysis

Before planning a software image upgrade, you must determine the prerequisites of the new software images. You can analyze these by using,

- Cisco.com (See [Planning an Upgrade From Cisco.com.](#))
- Repository (See [Planning an Upgrade From Repository.](#))

This section contains:

- [Understanding the Upgrade Analysis Report](#)
- [Support for In Service Software Upgrade](#)
- [Planning the Upgrade](#)
- [Configuring Devices for Upgrades](#)
- [Scheduling the Upgrade](#)

Planning an Upgrade From Cisco.com

Use the Cisco.com Upgrade Analysis option to determine the impact to and prerequisites for a new software deployment using images that reside in Cisco.com.

This option allows you to identify only images that meet certain criteria. It then analyzes the images to determine the required hardware upgrades (boot ROM, Flash memory, RAM, and access).

This option helps you answer questions such as:

- Does the device have sufficient RAM to hold the new software?
- Have the minimum ROM version requirements been met?
- Is the Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device to the Device and Credential Repository?
- Have I performed an upgrade path and NVRAM analysis on my Catalyst devices?
- Does the module firmware on my IPX/IGX/BPX devices need to be upgraded?



Note

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

To upgrade from Cisco.com:

Step 1 Select **Configuration > Tools > Software Image Management > Upgrade Analysis**.

The Select Upgrade Source dialog box appears.

Step 2 Select **Cisco.com** and click **Go**.

The Device Selection dialog box appears.

Step 3 Select the devices to analyze, then click **Next**.

See *Administration of Cisco Prime LAN Management Solution 4.2* for information on how to use the Device Selector.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

a. Enter your Cisco.com username and password.

If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

Admin > System > Cisco.com Settings > Proxy Server Setup

b. Click **OK** after entering the credential information.

The Cisco.com Upgrade Analysis dialog box appears with the following information:

Field	Description
Device	Name of the device
Running Image	Running image of the device

Field	Description
Image Options	Available images. Select the Image options from the drop-down list.
Error	Click on the link to review the details.

- Step 4** Click **Finish** to update the upgrade path information.
The Upgrade Analysis Report appears in a new browser window.
See [Understanding the Upgrade Analysis Report](#) for details.

Planning an Upgrade From Repository

Use the Repository Upgrade Analysis option to analyze images in your software repository and determine the impact to and prerequisites for a new software deployment. The option produces the Upgrade Analysis report, which shows the required boot ROM, Flash memory, RAM, and access.

This option helps you answer such questions as:

- Does the device have sufficient RAM to hold the new software?
- Have the minimum ROM version requirements been met?
- Is the Flash memory large enough to hold the new software?
- Do I need to add Telnet access information for the device to the Device and Credential Repository?
- Does the module firmware on my IPX/IGX/BPX devices need to be upgraded?



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

To upgrade from repository:

- Step 1** Select **Configuration > Tools > Software Image Management > Upgrade Analysis**.
The Select Upgrade Source dialog box appears.
- Step 2** Select **Repository**, then click **Go**.
The Repository Upgrade Analysis dialog box appears.
- Step 3** From the list, select the image to analyze, then select the devices to upgrade, then click **Run Report**.
The Upgrade Analysis Report window appears.
See [Understanding the Upgrade Analysis Report](#) for details.

Understanding the Upgrade Analysis Report

The Upgrade Analysis report summarizes the impact to and prerequisites for a new software deployment for the selected devices. It is generated by the Cisco.com Upgrade Analysis ([Planning an Upgrade From Cisco.com](#)) and Repository Upgrade Analysis ([Planning an Upgrade From Repository](#)) options.

The information that is shown in this report depends on the device type you have selected. See these tables to understand the Upgrade Analysis Report, [Table 9-5](#) and [Table 9-6](#).

Locate your device in the Supported Image Import Features for Software Management table on Cisco.com. For some devices the upgrade analysis option may not be available yet.

Table 9-5 Upgrade Analysis Report Columns

Column	Description
Device Information	Running Image Name, Running Image Version, BootROM Version, Running Image Feature, and Device Family
Boot ROM Upgrade	Any boot ROM upgrade required
Flash Upgrade	Any Flash upgrade required
RAM Upgrade	Any RAM upgrade required
Telnet Access	Any Telnet information required
Boot Flash Upgrade	Any boot Flash upgrade required
NVRAM Upgrade	Any NVRAM upgrade required
Module Firmware Upgrade	Firmware upgrade requirements for each service module in device.
Firmware Compatibility	Indicates whether the selected firmware image is compatible with the switch software image running on the device.

The following table ([Table 9-6](#)) maps the Upgrade Analysis Report to the supported device types:

- Optical Networking
- Routers and Switches
- Storage Networking

The Upgrade Analysis from Cisco.com and Repository are not supported for these device types because the required information for the upgrade analysis is not provided by the device:

- Universal Gateways and Access Servers
- Content Networking
- DSL and Long Reach Ethernet (LRE)
- Optical Networking
- Security and VPN
- Broadband Cable
- Voice and Telephony
- Network Management
- Wireless
- Cisco Interfaces and Modules

Table 9-6 Upgrade Analysis Report Based on Device Type

Upgrade Analysis Report Columns	Device Type: Routers and Optical Networking	Device Type: Switches	Device Type: Storage Networking
Boot ROM Upgrade	Supported	Not supported	Not supported
Flash Upgrade	Supported	Not supported	Not supported
RAM Upgrade	Supported	Supported	Supported
Telnet Access	Supported	Not supported	Supported
Boot Flash Upgrade	Not supported	Supported	Not supported
NVRAM Upgrade	Not supported	Supported	Not supported
Module Firmware Upgrade	Supported. See the Supported Image Distribution Features for Software Management table on Cisco.com for the router's device list that supports Module Firmware Upgrade. http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html	Supported. This is applicable for the following devices: <ul style="list-style-type: none"> • IPX/IGX/BPX device switch • MGX system 	Not supported
Firmware Compatibility	Not supported	Supported. This is applicable for the following devices: IPX/IGX/BPX device firmware	Not supported

In addition to this information, you can use the Go To drop-down list to navigate to particular device analysis report.

Button	Description
Export to File (Icon)	Exports the analysis report in CSV or PDF format.
Print (Icon)	Generates a format that can be printed.

Support for In Service Software Upgrade

LMS supports In Service Software Upgrade (ISSU) process. This process allows Cisco IOS software images to be updated without rebooting the device. This increases network availability and reduces downtime caused by planned software upgrades.

To perform the image upgrade using this ISSU process, the running image and the upgrade image must be ISSU capable and should be available in the flash memory.

The ISSU image upgrade process may fail if:

- The running or the upgrade image is not available in the flash memory
- The running image is deleted because of flash cleanup operation performed while the job is running.

ISSU support is available only for the following devices:

- Cisco Catalyst 6000 Series IOS Dual Chassis (VSS) Switches
- Cisco Catalyst 6000 Series Dual Supervisor Switches

ISSU process can be applied to the following distribution methods:

- By devices [Basic]
- By image
- Use remote staging

To perform this ISSU image upgrade process:

- Select **Reboot immediately after downloading** in the Job Schedule and Options page of the Device Distribution flow.
- You can also customize the configurations available in the `Issuconf.properties` file located at:
 - `NMSROOT/MDC/tomcat/webapps/rme/WEB-INF/conf/swim` (On Solaris and Soft Appliance)
 - `NMSROOT\MDC\tomcat\webapps\rme\WEB-INF\conf\swim` (On Windows)

`NMSROOT` is the LMS install directory.

You can configure the following properties in the `Issuconf.properties` file:

Variable	Description
RBTConfig	Configure the rollback timer. By default, the value of this variable is set as NO. If you configure the value as yes , then rollback will happen for the value set in the variable <i>RollBackTime</i> .
RollBackTime	Enter the rollback timer (value in minutes). By default, the rollback time is set as 45. To consider the value for rollback timer you must set the RBTConfig value as yes .
IssuSupImgVer	The ISSU supported version of the running image. For ISSU upgrade support, the value for this variable must be an ISSU capable image version such as sxi . This value can either match the version of the running image completely, or partially. For example, 12.2(33)SXI, or SXI.

The running software image version in the device must match the version configured in the `Issuconf.properties`.

If the running image or the upgrade image is not an ISSU capable image, or the version of the image is wrongly configured for the variable “`IssuSupImgVer`” in the `Issuconf.properties` file, then ISSU upgrade process will not happen and LMS proceeds with the normal upgrade process.

For example, if the running image version is 12.2(33)SXI, which is ISSU capable, and the version entered for the variable “`IssuSupImgVer`” is 12.2(33)SXH, then ISSU upgrade will not happen and LMS proceeds with normal upgrade process.

To fix this issue, you must provide the proper version for the variable “`IssuSupImgVer`” that is ISSU capable. For example, 12.2(33)SXI, or SXI.

Software Distribution Methods

You can distribute images to the devices in your network, using any of these options:

- Distribute by Devices [Basic]:

This option enables you to select devices and perform software image upgrades to those devices. Software Management checks the current image on the device and recommends a suitable image and the appropriate image storage for distribution.

See [Distributing by Devices \[Basic\]](#)

- Distribute by Devices [Advanced]:

This option enables you to enter the software image and storage media for the device that you want to upgrade.

The selected image and storage media is validated and verified for dependencies and requirements based on the device information that you entered when you added devices to the Device Credentials Repository.

See [Distributing by Devices \[Advanced\]](#)

- Distribute by Images:

This option enables you to select a software image from the software image repository and use it to perform an image upgrade on suitable devices in your network. This option is useful when you have to distribute the same image to multiple devices.

See [Distributing by Images](#).

- Remote Staging and Distribution:

This option enables you to select a software image, store it temporarily on a device and then use this stored image to upgrade suitable devices in your network. This option is helpful when the LMS server and the devices (including the remote stage device) are distributed across a WAN.

See [Remote Staging and Distribution](#).

You can run the device upgrades job sequentially or in parallel. After the devices upgrade, you can also specify the reboot order. You can specify these options in the Job Schedule and Options dialog box.

During the image upgrade, Software Management:

- Checks the amount of Flash memory on the device. If Flash memory needs to be erased before the new system image is loaded and erasing is allowed, it erases the Flash memory. Before erasing the Flash, a warning message appears `Flash memory will be erased`.
- Performs MD5 Checksum check of the image when it is downloaded from Cisco.com directly. It also performs image size check once the image is copied to a device, to check if there was any network transfer issue. These are the image consistency checks performed by Software Management.
- Provides a running log of the upgrade job.
- E-mails a report on the results to the specified addresses after completing the upgrade.
- Inserts boot commands to activate the upgraded image.
- Reboots the device if the Reboot Schedule option has been set to Reboot Immediately.
- RAM value is not checked. Hence, distribution proceeds without any errors even if the RAM value is unknown.
- Min.Flash is ignored, if Min.Flash is unknown.
- Image cannot be used for upgrade, if Flash size is unknown.

After you schedule an image upgrade, you can use Software Management Job Browser (**Configuration > Job Browsers > Software Image Management**) to review, retry, or cancel a job.

After a successful distribution job, Software Management triggers

- An inventory and a configuration collection.
- A Change Audit log. You can generate a Change Audit Standard Report in the Report Generator window (**Reports > Audit > Change Audit > Standard**).

This section contains:

- [Planning the Upgrade](#)
- [Configuring Devices for Upgrades](#)
- [Scheduling the Upgrade](#)
- [Authorizing a Distribution Job](#)
- [Distributing by Devices \[Basic\]](#)
- [Distributing by Devices \[Advanced\]](#)
- [Distributing by Images](#)

Planning the Upgrade

Planning the upgrade typically involves these phases:

- [Identifying Possible Changes](#)
- [Satisfying the Prerequisites](#)
- [Maintaining Your Software Image Repository](#)
- [Testing the New Images](#)

Identifying Possible Changes

Identifying which devices at your site might require software upgrades consists of these phases:

- Determine whether an upgrade is required

You can learn about new features or fixes in different ways.

You use the Browse Bugs option (**Reports > Cisco.com > Bug Summary**) to summarize the software image bugs for the devices in your network.

You can schedule a Browse Bugs job to run at regular intervals. This will help you determine any bugs related to current running images on the devices.

If you find a bug in your software, call the Technical Assistance Center (TAC) to know the status of the bug.

Your sales engineer or channel partner notifies you of new features that might be appropriate for your site.

You check Cisco.com periodically to review new release notes, bug-fix documentation, and marketing bulletins.

- Retrieve information about the upgrade

Go to Cisco.com to read the most recent product Release Notes or bug-fix documentation. This information will help you determine the software image version you need.

- Determine whether the upgrade is really necessary

After you determine the version you need, you can list the current software version numbers for your managed devices.

You can generate this using (**Reports > Inventory > Software**)

Satisfying the Prerequisites

Run Cisco.com Upgrade Analysis or Repository Upgrade Analysis to determine the prerequisites for a new software deployment. See [Upgrade Analysis](#) for further details.

In addition, you need to answer questions such as:

- Have you supplied the minimum requirements such as the minimum device configuration requirements for each device? See [Meeting Minimum Device Requirements](#) for further details.
- Is the device running from Flash (RFF)?
- Does the device have multiple Flash partitions?
- Does the Supervisor board require a new software image?
- Have you satisfied the additional requirements for the devices?
See [Configuring Devices for Upgrades](#) for further details.

Maintaining Your Software Image Repository

- Use the Adding Images to the Repository > Network option to import running images from all Software Management-supported devices in your network into the repository.
See [Adding Images to the Software Repository From the Network](#) for further details.
- Since you can download new images to a device without using Software Management, eventually the software image repository might not reflect the images that are running on your network devices.

To keep the repository current:

- Review all software images in the repository.
See [Software Repository](#) for further details.
- Schedule the Synchronization report to run periodically.
See [Scheduling a Synchronization Report](#) for further details.
- Retrieve additional images from Cisco.com, another device, or a file system on your server.
See [Adding Images to the Software Repository](#) for further details.
- Download Cisco images from Cisco.com during a scheduled distribution job.

Testing the New Images

To confirm the stability of your network after upgrades, test the new software images before you perform a full-scale deployment.

You cannot roll back software upgrades for supervisor modules on Catalyst 5000 series switches. Therefore, test the new images for these devices thoroughly before deploying them on your network.

Configuring Devices for Upgrades

This section lists all the required tasks that have to be performed on Cisco devices. This section also captures the following information:

- [Meeting Minimum Device Requirements](#)
- [Meeting Additional Device Requirements](#)
- [Additional SFB Checks](#)
- [Configuring Telnet and SSH Access](#)
- [Configuring SCP](#)

- [Configuring RCP](#)
- [Configuring TFTP](#)
- [Configuring HTTP](#)
- [Meeting Microcode and Modem Firmware Requirements](#)

Meeting Minimum Device Requirements

Before you can upgrade software images, you must meet the following requirements:

Category	Requirements
Device configuration	Device must be configured with SNMP read-write community string. There should not be any access list on the device that will disable TFTP transfers from the workstation.
IOS and ONS devices	For the device to be rebooted using the SNMP protocol, you must configure the <code>snmp-server system-shutdown</code> command on the device.
SFB devices	See Additional SFB Checks for further details.
RSP 7000 or 7500 devices running Cisco IOS version 11.x or later	See Additional SFB Checks for further details.
Microcode images	See Meeting Microcode and Modem Firmware Requirements for further details.
Inventory	SNMP read-write community string must be in Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices).
tftpboot directory space	Must have enough space for all concurrent jobs, which could include image distribution, image import, config file scan, and so on.

Meeting Additional Device Requirements

Before you upgrade, you must meet the following additional device requirements:

- Make sure you have Telnet access to upgrade the devices. Before you upgrade, add the Enable mode password (see [Configuring Telnet and SSH Access](#)) and access information for each device to the Device and Credential Repository.
See the Software Management Functional Supported Device tables on Cisco.com for the devices list that requires Telnet access.
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html
- To perform the upgrade, the device must be rebooted to RxBoot mode using SNMP. Do this even if you have selected the Do not reboot option when scheduling the upgrade. This procedure is applicable only to RFF devices.

- Configure PIX Firewall for SNMP and telnet access. For LMS to manage these devices, you must enter these commands on the device, in the config mode:
 1. `config terminal`
 2. `snmp -server host hostname`
 3. `snmp -server community community name`
 4. `telnet ip 255.255.253.255 inside interface`
 5. `write mem`

Additional SFB Checks

Software Management validates the image upgrades at the time the job is scheduled. For SFB devices, Software Management also verifies that:

- IP routing is enabled on the device.
- The ethernet interface that connects LMS to the device has an IP address assigned to it and is routing IP protocol.
- If the device is configured with Frame Relay subinterfaces, the device software version is 11.1 or higher.
- The ROM monitor code version is 5.2 or higher.

Configuring Telnet and SSH Access

Before you schedule the upgrade, use the Device and Credentials (**Inventory > Device Administration > Add / Import / Manage Devices**) option to add or change passwords and access information.

When you select the SSH protocol for the Software Management, the underlying transport mechanism checks whether the device is running SSHv2.

If so, it tries to connect to the device using SSHv2.

If the device does not run SSHv2 and runs only SSHv1 then it connects to the device through SSHv1.

If the device runs both SSHv2 and SSHv1, then it connects to the device using SSHv2.

If a problem occurs while connecting to the device using SSHv2, then it does not fall back to SSHv1 for the device that is being accessed.

See the Software Management Functional Supported Device tables on Cisco.com for the devices list that requires Telnet and SSH access.

http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html

- Telnet password
 - If the Telnet password is configured on your device, you might need this password for basic login access.
 - Enter the Telnet password in the *Primary Credential Password* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).
- Local user name
 - If the device is configured with the local username and password, you must enter this information when you log in. In Telnet mode, for catalyst devices, the local user name is not applicable, so you must leave this field blank. In secure shell (SSH) mode, for catalyst devices, you must enter this information.

Enter the Local User name in the *Primary Credential Username* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- Local user password

If the device is configured with the local username and password, you must enter this information when you log in.

If TACACS is configured, the application uses the TACACS information.

If the parent TACACS server is down and the local username and password are present, the application uses this information instead.

Enter the Local user password in the *Primary Credential Password* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- TACACS username and password

If the device is configured for TACACS, you must enter the TACACS username and password. The application will try to use this information first for login access.

Enter the TACACS username and password in the *Primary Credential Username* and *Primary Credential Password* fields in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- Enable secret password

The enable secret password takes precedence over the enable password in Cisco IOS Release 11.x and later. Use this password to make changes when running in regular Cisco IOS mode. If the service password-encryption is enabled, enable secret passwords are more secure than enable passwords.

Enter the Enable password in the *Primary Credential Enable Password* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- Enable password

Since some versions of BOOT ROM mode do not recognize the enable secret password or if enable secret is not configured on the device, you must use the enable password to load Flash memory.

Enter the Enable password in the *Primary Credential Enable Password* field in the Add Credential Template dialog box (**Inventory > Device Administration > Add / Import / Manage Devices**).

- Enable TACACS

Sometimes the device is configured for enable TACACS. In this case, you must provide the TACACS user name and password information for enable access.



Note The TACACS user name and password must be same as the Local user name and password. You cannot configure different user names and passwords for user mode and enable mode for the device.

Some useful URLs on configuring SSHv2 are:

- Configuring Secure Shell on Routers and Switches Running Cisco IOS:
<http://www.cisco.com/warp/public/707/ssh.shtml>
- How to Configure SSH on Catalyst Switches Running Catalyst OS:
http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a0080094314.shtml
- Configuring the Secure Shell Daemon Protocol on CSS:
http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/css11500series/v8.20/configuration/security/guide/sshd.html
- Configuration Examples and TechNotes:
http://www.cisco.com/en/US/tech/tk583/tk617/tech_configuration_examples_list.html

Configuring SCP

You can use the SCP protocol to transfer the software images. While using SCP protocol, the LMS server acts like a client and the device acts like a server.

To configure the LMS server as an SCP client, you must enter the SSH credentials. See [Configuring Telnet and SSH Access](#) for further details.

For Cisco Catalyst 2900XL, 2970, 2960, 3550, 3560, 3750, and 3750E switches, if you are upgrading the .tar images using SCP protocol, you must configure the SCP username and password.

The minimum supported version of the running image should be 12.2(25) SEC and should have the SCP protocol support.

In this case, LMS server acts like a SCP server and the device acts like a client.

To configure SCP username and password:

Step 1 Go to **Admin > System > System Preferences**.

The System Preferences dialog box appears.

Step 2 Enter the following information:

Field	Description
SCP User	<p>Enter the user name.</p> <p>For Solaris and Soft Appliance:</p> <ul style="list-style-type: none"> You must specify a user name that has SSH authorization. SCP uses this authorization for transferring the images. <p>For Windows:</p> <ul style="list-style-type: none"> The username you have entered here is taken for transferring images using SCP protocol.
SCP Password	<p>Enter the password.</p> <p>For Solaris and Soft Appliance:</p> <ul style="list-style-type: none"> You must specify a password that has SSH authentication. SCP uses this authentication for transferring the images. <p>For Windows:</p> <ul style="list-style-type: none"> The password you have entered here is used for authentication while transferring images using SCP protocol.
SCP Verify Password	Re-enter the password to verify.

Step 3 Click **Apply** after making the changes.

Step 4 To cancel the changes, click **Cancel**.

Configuring RCP

You can use the RCP protocol to transfer the software images. The LMS server acts like a RCP server and the device acts like a client.

Configuring RCP involves the following:

- [Configuring RCP on Solaris and Soft Appliance](#)
- [Configuring RCP on Windows](#)
- [Selecting RCP as the Active File Transfer Method on Solaris and Soft Appliance and Windows](#)
- [Configuring Cisco IOS Software Devices to Allow RCP Transactions](#)

Configuring RCP on Solaris and Soft Appliance

Configuring RCP on Solaris and Soft Appliance, involves the following:

- [Creating the RCP Remote User Account](#)
- [Enabling the RCP Daemon](#)

Creating the RCP Remote User Account

To use RCP, you must create a user account on the system to act as the remote user to authenticate the RCP commands issued by devices. This user account must own an empty `.rhosts` file in its home directory to which the user, `casuser` has write access.

You can choose the name of this user account because you can configure the LMS server to use any user account.

The default user account name is `cwuser`. The examples in this procedure use the default name `cwuser`. If you choose to use a different name, substitute that name for `cwuser`.

To create and configure the RCP remote user account, follow these steps while logged in as root:

-
- Step 1** To add a user account named `cwuser` to the system, enter:
- ```
useradd -m -c "user account to authenticate remote copy operations" \ cwuser
```
- Step 2** Navigate to the `cwuser` home directory.
- Step 3** Create the `.rhosts` file, by entering:
- ```
# touch .rhosts
```
- Step 4** Change the owner of the `.rhosts` file, by entering:
- ```
chown cwuser:casusers .rhosts
```
- Step 5** Change the permissions of the `.rhosts` file, by entering:
- ```
# chmod 0664 .rhosts
```

If you did not use the default user name `cwuser`, use the user account that you created as the RCP remote user account.

- a. Login to the server as admin.
 - b. Select **Admin > System > System Preferences**.
The View / Edit System Preferences dialog box appears.
 - c. Enter the name of the user account that you created in the RCP User field, then click **Apply**.
-

Enabling the RCP Daemon

To add and configure standard Solaris and Soft Appliance RCP server software:

-
- Step 1** Log in as superuser.
- Step 2** Edit the `/etc/inetd.conf` file using a text editor.
- Look in the file `/etc/inetd.conf` for the line that invokes `rshd`. If the line begins with a pound sign (`#`), remove the pound sign with a text editor. Depending on your system, the line that invokes the `rshd` server might look similar to:


```
shell stream tcp nowait root /usr/sbin/in.rshd in.rshd
```
 - Save the changes to the edited file and exit the text editor.

Step 3 Go to the UNIX prompt, enter the following to display the process identification number for the *inetd* configuration:

```
# /usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root 119 1 0 12:56:14 ? 0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the *inetd* configuration.

Step 4 Enable your system to read the edited */etc/inetd.conf* file, enter:

```
# kill -HUP 119
```

where *119* is the process identification number identified in Step 3.

Step 5 Verify that *rsmd* is enabled by entering:

```
# netstat -a | grep shell
```

which should return output similar to:

```
*.shell *.* 0 0 0 0 LISTEN
```

Configuring RCP on Windows

During LMS installation, the RCP server is configured.

Selecting RCP as the Active File Transfer Method on Solaris and Soft Appliance and Windows

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

The View/Edit Preferences dialog box appears.

Step 2 Select the **Protocol Order**.

Step 3 Click **Apply**.

Configuring Cisco IOS Software Devices to Allow RCP Transactions

Given here is a basic configuration in a router that can handle RCP transactions from the LMS server.

```
calvi# show running configuration
```

```
Building configuration...
```

```
Current configuration:
```

```
!
```

```
version 11.3 service timestamps debug uptime
```

```
service timestamps log uptime
```

```
service password-encryption
```

```
!
```

```
hostname calvi
```

```
!
```

```
boot system c2500-is-1.113-11a.T1.bin 255.255.255.255
```

```
enable password 7 1106170043130700
```

```
!
```

```
username cwuser password 7 000C1C0A05
```

```
ip rcmd rcp-enable
ip rcmd remote-host cwuser 172.17.246.221 cwuser enable
ip rcmd remote-username cwuser
!
!
process-max-time 200
!
interface Loopback0
 ip address 5.5.5.5 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0
 description Connection to Backbone
 ip address 172.17.246.4 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 no ip address
 no ip mroute-cache shutdown
 no cdp enable

!
interface Serial1
 no ip address
 no ip mroute-cache shutdown
 no cdp enable
!
interface Async1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.246.1
!
logging monitor informational
snmp-server community private RW
snmp-server community public RO
snmp-server enable traps snmp
snmp-server host 172.17.246.117 traps public

!
line con 0
 exec-timeout 0 0
 password 7 0504080A754D4205
 login
line 1 8
 exec-timeout 0 0
```

```
login
transport input all
line aux 0
password 7 06090124184F0515
login
line vty 0 4
exec-timeout 0 0
password 7 06090124184F0515
login
!
```

where:

- `username cwuser password 7 000C1C0A05` creates the username `cwuser` on the router. You must choose a password for this user.
- `ip rcmd rcp-enable` enables RCP service on the device.
- `ip remote-host cwuser 172.17.246.221 cwuser enable` The remote system where you install LMS has the IP address 172.17.246.221 and the local definition of the user, `cwuser`. This command allows `cwuser` to issue the `copy` command on the network device.
- `ip rcmd remote-username cwuser` configures use of the remote user name at the request of a remote copy. At the initiation of the remote copy operation in the network device, for example, in `Add Images to Library`, the device uses the `cwuser` name to authenticate against the LMS server.

Configuring TFTP

You can use the Trivial File Transfer Protocol (TFTP) protocol to transfer the software images. The LMS server acts like a TFTP server and the device acts like a client.

Configuring TFTP on Windows

During LMS installation, the `tftpboot` directory is created under the directory in which LMS is installed (the default is `SystemDrive:\Program Files\CSCOpX`).

Configuring TFTP on Solaris and Soft Appliance

A file transfer server must be installed on your system. You must enable a TFTP server because it is the default file transfer server type.

During Software Management installation, if the installation tool cannot find a TFTP server, it tries to add one. If the installation tool cannot find or create a TFTP server, you must install and enable the TFTP server. Verify that a `/tftpboot` directory exists, as explained in the following sections.

- [Enabling the TFTP Daemon](#)
- [Creating the /tftpboot Directory](#)

Enabling the TFTP Daemon

If you are using standard Solaris and Soft Appliance software, you can add and configure the TFTP server (TFTPD).

Step 1 Log in as superuser.

Step 2 Edit the `/etc/inetd.conf` file using a text editor.

- Look in the file `/etc/inetd.conf` for the line that invokes TFTPD. If the line begins with a pound sign (#), remove the pound sign with your text editor. Depending on your system, the line that invokes the TFTP server might look similar to:

```
tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

- Save the changes to the edited file and exit your text editor.

Step 3 Go to the UNIX prompt, enter the following command to display the process identification number for the `inetd` configuration:

```
# /usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root 119 1 0 12:56:14 ? 0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the `inetd` configuration.

Step 4 Enable your system to read the edited `/etc/inetd.conf` file, enter:

```
# kill -HUP 119
```

where `119` is the process identification number identified in Step 3.

Step 5 Verify that TFTP is enabled by entering either:

```
# netstat -a
```

or

```
# grep tftp
```

which should return output similar to:

```
*.tftp Idle
```

or enter:

```
# /opt/CSCOpX/bin/mping -s tftp localhost_machine_name
```

which returns the number of modules sent and received, for example:

```
sent:5 rcvd:5 . . .
```

If the output shows that zero modules were received, TFTP is not enabled. Repeat these steps, beginning with Step 1, to make sure you have enabled TFTP.

Creating the `/tftpboot` Directory

LMS uses the `/tftpboot` directory when transferring files between the LMS server and network devices. The files are removed after the transfer is complete. However, multiple jobs (for example, image distribution, image import, or config file scan) could be running at the same time.

Each of these jobs requires its own space. Software image sizes, for example, can be up to 20 MB. To ensure that jobs run successfully, make sure there is sufficient space available in the `/tftpboot` directory.

If the /tftpboot directory does not exist on your system, you must create it:

-
- Step 1** Enter:
- ```
mkdir /tftpboot
```
- Step 2** Make sure all users have read, write, and execute permissions to the /tftpboot directory by entering:
- ```
# chmod 777 /tftpboot
```
- The /tftpboot directory now exists and has the correct permissions.
-

Configuring HTTP

No configuration on device is required for this protocol.

Meeting Microcode and Modem Firmware Requirements

The following minimum system software versions are required to support microcode and modem firmware upgrades. However, different versions of these image types might require different versions of system software.

Software Management does not check for compatibility and dependence between each microcode version and system software version. It merely warns the user to check this information by consulting a technical representative or the compatibility matrix published on Cisco.com.

MICA Portware Image Types

Device	Minimum System Software Version
AS5200	Cisco IOS version 11.3(2)T Bootloader version 11.2(11)P
AS5300	Cisco IOS version 11.2(9)XA
3640	Cisco IOS version 11.2(12)P

Microcom Firmware Image Types

Device	Minimum System Software Version
AS5200	Cisco IOS version 11.2(10a)P Bootloader version 11.2(11)P
AS5300	Cisco IOS version 11.1(14)AA

CIP Microcode Image Types

Supported for Cisco IOS versions 11.x and later.

Scheduling the Upgrade

Scheduling an upgrade consists of:

- Selecting the devices to upgrade

Use Software Management's scheduling features to schedule the upgrade for one device or a series of devices.

Software Management downloads images from more than one device in parallel. You must ensure that the tftpboot directory (*NMSROOT/tftpboot* (On Solaris and Soft Appliance), and *NMSROOT\tftpboot* (On Windows)) has enough free space to accommodate at least 20 images.

- Determining any limitations or requirements for the selected devices

For example, SFB devices have several upgrade requirements and limitations.

- Updating the inventory

Since Software Management uses the inventory to make image and Flash memory recommendations, be sure that your current inventory reflects the correct device information.

For some devices such as 6400 NRP1, 801, and 802, etc., Software Management contacts devices to get the Flash information.

- Configuring file transfer protocol order

Before scheduling a software upgrade job, set the protocol order for configuration file transfer.

For fetching configuration from device, the protocol settings of Configuration Management are used. Software Management uses the same protocol for fetch and download of configurations. You can set the Configuration Management protocol order using **Admin > Collection Settings > Config > Config Collection Settings**.

For better performance, set *tftp* as the first protocol.

- Determining the upgrade and execution order

Based on your network topology and to minimize the impact on your network, you can schedule the upgrades job either sequentially or in parallel.

For example, if devices A, B, and C are networked sequentially, then you must upgrade device C first, then device B, then device A. If you upgrade device B first, you might no longer have access to device C.

- Determining the upgrade schedule

For most devices, you can schedule the software to:

- Distribute the software to the device and reload the device immediately.
- Distribute the software only. You will perform the reloads manually.

The following devices are always rebooted immediately after the software is downloaded:

- Single Flash bank devices
- FDDI/CDDI, ATM, and Token Ring modules on Catalyst switches

- Checking the Work Order report

The Work Order report contains such information as the state of the software running on the device and the new software, the operations that will be performed during the upgrade procedure, and any important notes that you should be aware of before the upgrade begins.

Authorizing a Distribution Job

The Job Approval approval option allows you to require job upgrade approvals before running a scheduled job. It enforces the approval process by sending job requests through e-mail to people on the approver list.

To set up the authorization process:

- Select the appropriate Job Approval options.
- Make sure one or more approver lists exist.
- Make sure the upgrade job identifies an approver list.
- Make sure the approver is a member of that approver list.

See *Administration of Cisco Prime LAN Management Solution 4.2* for more details on creating and editing approver lists, assigning approver lists, setting up Job Approval, and approving and rejecting jobs.

Distributing by Devices [Basic]

You can use the Distribute by Devices option to schedule device-centric upgrade jobs.

Software Management recommends any software images available on LMS server and Cisco.com, if this option is selected by you (**Admin > Network > Software Image Management > View/Edit Preferences**).

To do this, select the devices first and distribute suitable images to them. After the distribution job is complete, you can use the Software Management Job Browser window to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade



Note

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

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.

You can also download the images from Cisco.com. You must ensure that you have the access to download the images from Cisco.com.

- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the images by device in Basic mode:

Step 1 Select **Configuration > Tools > Software Image Management > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **By device [Basic]** and click **Go**. The Select Devices dialog box appears.

Step 3 Select the devices, then click **Next**.

The Cisco.com and Proxy Server Credential Profile dialog box appears.

a. Enter your Cisco.com username and password.

If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

Admin > System > Cisco.com Settings > Proxy Server Setup

- Click **OK** after entering the credential information.

The software management analyzes the required images that are available in your software repository and on Cisco.com. It then recommends the appropriate image for distribution.

See [Understanding Upgrade Recommendations](#) for details on how Software Management recommends image for various Cisco device types.

The Distribute By Devices dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Image Options	Details of the recommended image.
Storage Options	Details of recommended image storage information.
Errors	Click on the underlined Error message to review the details.

Notation Descriptions

- An asterisk (*) at the beginning of the field indicates the recommended image or partition by Software Management. If there is no asterisk at the beginning of the field, it indicates that an appropriate image or partition could not be found but the displayed selections might work.
- A '^' means that the image resides in Cisco.com but not in your software image repository. When you select an image in Cisco.com to distribute to a network device, the image is first added to the image repository, then downloaded to the device.
- A superscript '1' refers to read-only Flash memory.
- A superscript '2' refers to the Flash partition that holds the running image when a device is running from Flash (RFF).

Step 4 Select the devices to which you want to distribute images and click **Next**.

The Distribute By Devices window appears with these details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Image	Image information that you have selected.

Field	Description
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 5 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: <ul style="list-style-type: none"> • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).

Field	Description
Perform distribution in Non-Installed mode	This option is available only if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If the running image is in the repository, select this option to place a copy in the TFTP server directory. Uses this copy of image if reboot with new image fails. Note the following about this option: <ul style="list-style-type: none"> Option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. Backup image is not deleted after upgrade. It remains in TFTP server directory so that the device can find it any time it reboots
Backup current running image	Select to back up the running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do <i>not</i> select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices) are ignored.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: <ul style="list-style-type: none"> Sequential—Job runs on the devices, sequentially. You can define this sequence. Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: <ol style="list-style-type: none"> Click Execution Order. The Execution Order dialog box appears. Use the Up and Down arrows to order your device list. Click Done.

Field	Description
Reboot	<p>Select the reboot order for the devices. This can be either Parallel or Sequential.</p> <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Boot Order. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click Done.

Step 7 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Distributing by Devices [Advanced]

You can use the Distribute by Devices option to schedule device-centric upgrade jobs.

The selected image and storage media is validated and verified for dependencies and requirements based on the device information that you have provided at the time of adding devices to the Device and Credential Repository and the device data that is collected by the inventory.

The images that you want to distribute must be available in the Software repository.

You can use this method to upgrade the System software on all Software Management supported devices. You can also upgrade module software on those modules which have a management IP address.

The modules/interfaces that do not have a management IP address cannot be upgraded using this method.

The input file that contains the details of the device and image must be available at this location:

On Solaris and Soft Appliance:

`/var/adm/CSCOPx/files/rme/swim/advdistinput`

On Windows:

`NMSROOT\files\rme\swim\advdistinput`

Where *NMSROOT* is the LMS installed directory.

After the distribution job is complete, you can use the Software Management Job Browser window to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade



Note

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

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device. You should have verified whether the necessary software images are present in the image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the images by device in Advance mode:

Step 1 Select **Configuration > Tools > Software Image Management > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **By device [Advanced]**, then click **Go**.

The Expert Distribution dialog box appears.

Step 3 Click **Browse**.

The Server Side File Browser dialog box appears.

Step 4 Select the file and click **OK**.

The input file that contains the details must be available at this location:

On Solaris and Soft Appliance:

`/var/adm/CSCOPx/files/rme/swim/advdistinput`

On Windows:

`NMSROOT\files\rme\swim\advdistinput`

Where *NMSROOT* is the LMS installed directory.

The selected file must contain the information in CSV format and all the fields are mandatory:

device-display-name,image-in-repository,storedestination,moduleidentifier

- *device-display-name*—Name of the device as entered in Device and Credential Repository.
- *image-in-repository*—Image name as in the software image repository.

- *storagedestination*—Image storage destination
- *moduleidentifier*—Module identifier number. This is applicable only for Catalyst devices. For other devices, you must enter 0.

You can identify the device module number using Inventory Detailed Device Report (**Reports > Inventory > Detailed Device**). In the Detailed Device Report, the *Slot Number* column in the *Module Information* table provides you the Module Identifier Number.

For example, for a Cisco Router:

```
Rtr1750,c1700-sy56i-mz.121-24.bin,flash:1,0
```

For a Cisco Catalyst device:

```
cat5500-10.100.38.17,cat5000-supg.6-4-10.bin,bootflash:,1
```

Step 5 Do either of the following:

- Check the Skip Verification checkbox if you want to postpone the verification to the job execution stage.

If you have checked the Skip Verification checkbox, go to [Step 7](#).

Or

- Click **Verify** if you want the verification to take place during the job scheduling stage itself.

If you have clicked **Verify**, go to [Step 6](#).

Step 6 When you click Verify, the Expert Distribution window is updated with the following device details:

Field	Description
Device	Name of the device as specified in the input file.
Image	Name of the image as specified in the input file.
Storage Destination	Image storage information as specified in the input file.
Module Number	Module identifier number as specified in the input file.
Result	Click on the link to review the details.

Step 7 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 8 Enter the following information in the Job Schedule and Options dialog box:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (by device [Advanced]) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: <ul style="list-style-type: none"> Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. Applies to Supervisor Engine I, II, and III only. Line cards reboot automatically. Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is available only if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Note the following about this option: <ul style="list-style-type: none"> Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated. Applies to Supervisor Engine III only.
Use current running image as tftp fallback image	If the running image is in the repository, select this option to place a copy in the TFTP server directory. Uses this copy of image if reboot with new image fails. Note the following about this option: <ul style="list-style-type: none"> Applies to Supervisor Engine I, II, and III only. Option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. Backup image is not deleted after upgrade. It remains in TFTP server directory so that the device can find it any time it reboots

Field	Description
Back up current running image	Select to back up the running image in software image repository before upgrading. Applies to Supervisor Engine I, II, and III only. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do <i>not</i> select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to Telnet to the devices at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices) are ignored.
Execution	Select the job execution order for the devices. This can be either Parallel or Sequential: <ul style="list-style-type: none"> Sequential—Job runs on the devices, sequentially. You can define this sequence. Parallel—Job runs on a batch of 15 devices at the same time. If you have selected Sequential: <ol style="list-style-type: none"> Click Execution Order. The Execution Order dialog box appears. Use the Up and Down arrows to order your the device list. Click Done.
Reboot	Select the reboot order for the devices. This can be either Parallel or Sequential. If you have selected Sequential: <ol style="list-style-type: none"> Click Boot Order. The Boot Order dialog box appears. Use the Up and Down arrows to order your devices list. Click Done.

Step 9 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)

- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 10 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Distributing by Images

You can use the Distribute by Images option to schedule image-centric upgrade jobs. To do this, you must first select an image and then distribute it to applicable devices.

After the distribution job is complete, you can use the Job Details report to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade



Note

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

You cannot use this procedure to upgrade:

- MICA portware
- Microcom firmware
- CIP microcode
- Bootloader for IOS
- Catalyst modules other than the Supervisor module

Before You Begin

Before you begin distributing the images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device. You should have verified whether the necessary software images are in the image repository.
See [Planning the Upgrade](#) for further details.
- Considered the effect of the upgrade on your network and your network users.
See [Scheduling the Upgrade](#) for further details.
- Supplied the information required by Software Management for each device.
See [Configuring Devices for Upgrades](#) for further details.

To distribute images by image:

Step 1 Select **Configuration > Tools > Software Image Management > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **By image**, then click **Go**.

The Select Image And Devices dialog box appears.

Step 3 Select:

- a. An image from the software image repository.
- b. Devices that need upgrading

Step 4 Click **Next**.

The Device Recommendation dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Recommended Storage	Details of recommended image storage information.
Error	Click on the link to review the details.

Notation Descriptions

- An asterisk (*) at the beginning of the field indicates the recommended partition by Software Management. If there is no asterisk at the beginning of the field indicates, an appropriate partition could not be found but the displayed selections might work.
- A superscript '1' refers to read-only Flash memory.

Step 5 Select the devices you want to upgrade, then click **Next**.

The Image Centric Distribution Verification window appears. This window displays the following information:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Software management recommends the Flash partition with the maximum free space in each device. You can override the recommendation and select another partition from the drop-down box.

Step 6 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 7 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (by image) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none">• Immediate—Runs this job immediately.• Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: <ul style="list-style-type: none"> Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. Line cards reboot automatically. Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following: <ul style="list-style-type: none"> This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.

Field	Description
On error, halt processing of subsequent devices	<p>Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device.</p> <p>For sequential execution, if you do <i>not</i> select this option, upgrade for next device begins.</p> <p>For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed.</p> <p>See the Job Summary page for details.</p>
Enable Job Password	<p>Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution.</p> <p>The credentials that you enter here are used for this particular Software Management job.</p> <p>The credentials that you have entered in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices) are ignored.</p>
Execution	<p>Select the job execution order for the devices. This can be either Parallel or Sequential:</p> <ul style="list-style-type: none"> • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Execution Order. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click Done.
Reboot	<p>Select the reboot order for the devices. This can be either Parallel or Sequential.</p> <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Boot Order. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click Done.

Step 8 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.

- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verification warnings generated during image distribution (if applicable).

Step 9 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your job, select **Configuration > Tools > Software Image Management > Jobs**.

Support for IOS Software Modularity

Software Management provides support for Cisco IOS Software Modularity Images. The Cisco IOS Software Modularity Images combine subsystems into individual processes and enhances the memory architecture in order to provide the process level fault isolation and subsystem In-Service Software Upgrade (ISSU) capability.

Traditionally, IOS Software images are distributed by:

- Copying the image to disk.
- Updating boot commands and rebooted.

The IOS Software Modularity images can be run in this mode as well. This is called Cisco IOS Software Modular non-install mode (also known as binary mode).

Software Management supports distribution of Patches and Maintenance Packs. This distribution is accomplished by the use of Cisco IOS Software Modularity Images. Software Modularity enhances the IOS infrastructure to allow selective system maintenance through individual patch upgrades. See [Patch Distribution](#) for more details.

Patches

A patch is a single fix that may affect one or more subsystems. Patches can only be installed to a search root, where a base image exists. Patches are released for a particular base image version and device platform.

Maintenance Pack

A Maintenance Pack includes one or more patches. This pack is applied like a Patch. Maintenance Packs are released for a particular base image version and device platform.



Note

Software Management does not support downloading Patches/Maintenance Packs from Cisco.com. The reason is that these images are available in an external URL. You have to manually download patches from the external URL and add the same to Software Repository.

Modes of Distribution

There are two modes of distribution of Software Modularity images to devices:

- Non Installed Mode

This process involves the distribution of images by copying of the IOS Software Modularity images to the hard disk of the device, updating the boot commands and rebooting the OS on the device. You can run the Cisco IOS Software Modularity Images in this mode and so it is also called IOS Software Modularity non-install mode. It is also known as binary mode.

- Installed Mode

According to this mode the IOS Software Modularity image is extracted/uncompressed to a compact Flash with a well defined directory structure. The installed mode provides the advantage of accomodating the point fix capabilities of Software Modularity.



Note

Software Management checks the current image on the device and recommends a suitable image and the appropriate image storage for distribution. Software Management only recommends Maintenance Pack Images for devices. It does not recommend patches for devices.

Cisco IOS Software Modularity base images support:

- Import of Image from Cisco.com
- Import of Image from device
- Import of Image form File System
- Import of Image from Network
- Cisco.comUpgrade Analysis
- Distribution of Images
- Software Repository Synchronization

Support for Import of Image from device, Import of Image from Network and Software Repository Synchronization is applicable only for devices running IOS Software Modularity images in non-installed mode.

The population of Flash files on Cisco-Flash-MIB is not done on the devices running IOS Software Modularity image versions 12.2(18)SXF4 and 12.2(18)SXF5 and so these image versions are not supported by Software Management. The minimum IOS Software Modularity image version supported by Software Management is 12.2(18)SXF6.

Patch Distribution

You can distribute patches simultaneously to applicable devices. Patch distribution does not require reboot of the entire OS on a device. You can install patches only to a search root where a base image exists. Patches, once installed, must be activated to come to effect on the running system.

**Note**

You can apply Patches or Maintenance Packs to a device only if the device is running IOS Software Modularity Images in installed mode.

Software Management verifies:

- Patches against the base image and device platform to ensure compatibility. If the patches are incompatible then those patches are rejected.
- Whether the target patch already exists on the device.

Patch Distribution Methods

You can distribute patch images to the devices in your network, using any of these methods:

- Distribute by Devices

This method enables you to select devices and perform patch upgrades to those devices.

See [Patch Distribution - by Devices](#).

- Distribute by Patch

This method enables you to select a patch image from the Software Repository and use it to perform a patch upgrade on suitable devices in your network. This option is useful when you have to distribute the same patch image to multiple devices.

See [Patch Distribution - by Patch](#).

Patch Distribution - by Devices

You can use the Distribute by Devices option to schedule device-centric patch upgrade jobs.

Software Management recommends any Maintenance Pack software images available in the Repository.

**Note**

Currently Software Management does not support importing of patch images from Cisco.com. You need to import patch images into local filesystem and then import into repository by using Import from file system. See [Adding Images to the Software Repository From a File System](#) for more details.

Before You Begin

Before you begin distributing the patch images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the patch images by device:

Step 1 Select **Configuration > Tools > Software Image Management > Patch Distribution**.

The Patch Distribution Method dialog box appears.

Step 2 Select **By devices** and click **Proceed**.

The Patch Distribute by Devices dialog box appears. The Device Selector lists all the available devices.

Step 3 Select the devices, then click **Next**.

If any of the selected device is not in install mode, an error message is displayed:

```
Device is not in installed mode or not patchable
```

Unselect the device that is not in installed mode and continue.

The software management analyzes the required patch images that are available in your software repository and lists the applicable patch images for each device selected. You can select one or more required patches from the list for each device by using the Ctrl key.

You should select at least one patch for each selected device. If you do not select a patch for a device, an error message is displayed.

```
You should select atleast one patch image for each selected device.
```

Ensure that you select at least one patch for each selected device and continue.

The Patch Distribute By Devices dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Patch type, chassis model, and software version on device.
Patches Options	Details of the patch.
Storage Location	Details of the storage location of the selected patch image.
Errors	Click on the underlined Error message to review the details.

Step 4 Select the devices as well as the patch images you wish to distribute to the selected devices and click **Next**.

The Patch Distribute By Devices window appears with these details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Patch	Patch information that you have selected.
Selected Slot	Image storage information from where the current base image is running.
Verification Result	Click on the link to review the details.

Step 5 Click **Next**. The Job Schedule and Options dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Patch Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none">• Immediate—Runs this job immediately.• Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.

Field	Description
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	<p>Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas.</p> <p>Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences).</p> <p>We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.</p>
Comments	Enter additional information about this job.
Job Options	
Activate Patches	Select if you want to activate the patches immediately after download.
Reboot if it needs.	Select if the patch activation requires a reboot. Unselect if the patch activation does not require a reboot.
On error, stop processing subsequent devices	<p>Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device.</p> <p>For sequential execution, if you do <i>not</i> select this option, upgrade for the next device begins.</p> <p>For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed.</p> <p>See the Job Summary page for details.</p>
Enable Job Password	This option is checked, when the user name, password and enable password are provided for the job.
User Name	Enter the username for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Password	Enter the password for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Enable Password	Re-enter the password for confirmation purpose.
Execution	<p>Select the job execution order for the devices. This can be either Parallel or Sequential:</p> <ul style="list-style-type: none"> • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Execution Order. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click Done.

Field	Description
Reboot	<p>Select the reboot order for the devices. This can be either Parallel or Sequential.</p> <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Boot Order. <p>The Boot Order dialog box appears.</p> <ol style="list-style-type: none"> 2. Use the Up and Down arrows to order your devices list. 3. Click Done.

Step 7 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Patches selected for the upgrade.
- Job Approval information.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verify warnings generated during patch distribution (if applicable).

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Patch Distribution - by Patch

You can use the Distribute by Patch option to schedule patch upgrade jobs.



Note

Currently Software Management does not support importing of patch images from Cisco.com. You need to import patch images into local filesystem and then import into repository by using Import from file system. See [Adding Images to the Software Repository From a File System](#) for more details.

Before You Begin

Before you begin distributing the patch images, you should have:

- Prepared for this upgrade. You should have met all of the prerequisites for loading the software on the device and also verified whether the necessary software images are present in the software image repository.
- Considered the effect of the upgrade on your network and your network users.
- Supplied the information required by Software Management for each device.

To distribute the patch images by device:

Step 1 Select **Configuration > Tools > Software Image Management > Patch Distribution**.

The Patch Distribution Method dialog box appears.

Step 2 Select **By Patch** and click **Proceed**.

The Distribute by Patch dialog box appears.

Step 3 Select a patch from the Image Selection pane and devices from the Device Selection pane, and click **Next**.

The Distribute By Patch - Recommendations dialog box appears with the following information:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of the storage location of the selected patch image.
Errors	Click on the underlined Error message to review the details.

Step 4 Select the devices as well as the patch images you wish to distribute to the selected devices and click **Next**.

The Distribute By Patch - Verification window appears with these details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information from where the current base image is running.
Verification Result	Click on the link to review the details.

Step 5 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 6 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Patch Distribution (by device [Basic]) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule the job.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter the additional information about this job.
Job Options	
Activate Patches	Select if you want to activate the patches immediately after download.
Reboot if it needs	Select if the patch activation requires a reboot. Unselect if the patch activation does not require a reboot.
On error, stop processing subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to the next device. For sequential execution, if you do <i>not</i> select this option, upgrade for the next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	This option is checked, when the user name, password and enable password are provided for the job.
User Name	Enter the username for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Password	Enter the password for the distribution job. The credentials that you enter here are used for this particular Software Management job.
Enable Password	Re-enter the password for confirmation purpose.

Field	Description
Execution	<p>Select the job execution order for the devices. This can be either Parallel or Sequential:</p> <ul style="list-style-type: none"> • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Execution Order. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click Done.
Reboot	<p>Select the reboot order for the devices. This can be either Parallel or Sequential.</p> <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Boot Order. The Boot Order dialog box appears. 2. Use the Up and Down arrows to order your devices list. 3. Click Done.

Step 7 Click **Next** after you finish entering the job information details.

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Patches selected for the upgrade.
- Job Approval information.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Verify warnings generated during patch distribution (if applicable).

Step 8 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Remote Staging and Distribution

The Remote Staging and Distribution option helps you to upgrade multiple devices over a WAN.

You can perform remote staging and distribution by any one of the methods:

- External FTP server
- External TFTP server
- Remote Staging Device

In this workflow, a managed device or external TFTP server or FTP server is used to stage an image temporarily. The staged image is then used to upgrade devices that are connected by LAN to the Remote Stage device or external TFTP server or FTP server. If you use this method, you do not have to copy a similar image, multiple times across the WAN.

After the image distribution job is completed using a managed device as a remote stage device, the configuration changes made to the Remote Stage device are automatically reversed and the staged image is deleted from the Remote Stage device.

After the distribution job is complete, you can use the Software Image Management Job Browser to:

- Undo an upgrade and roll back to the previous image
- Retry devices that failed a previous upgrade

This section contains:

- [Using External FTP Server](#)
- [Using External TFTP Server](#)
- [Using Remote Stage Device](#)



Note

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

Supported Remote Stage Devices

The device that is used as the Remote Stage must have enough free Flash space to copy the selected image.

See the Supported Image Distribution Features for Software Management table on Cisco.com for Remote Staging devices list.

Before You Begin

Before you begin distributing the images, you should:

- Prepare for this upgrade. You should have met all of the prerequisites for loading the software on the device or external TFTP server or FTP server. You should also verified whether the necessary software images are in the image repository.
- Manually copy the software image to the External TFTP server or FTP server. This is if you are using the External TFTP/FTP server as the Staging Server.
- Consider the effect of the upgrade on your network and your network users.
- Supply the necessary information required by Software Management for each device.
- Decide on the device or external TFTP server or FTP server that you will use as the Remote Stage device or server.

- Ensure that the Telnet or SSH protocols are functioning properly if you are planning to distribute the images to devices using an External FTP server. The connection protocol for running FTP commands on the device can be either Telnet or SSH.



Note For the devices that supports remote staging using external FTP Server, see [Supported Devices for FTP](#).

To distribute images using Remote Staging:

Step 1 Select **Configuration > Tools > Software Image Management > Software Distribution**.

The Distribution Method dialog box appears.

Step 2 Select **Use remote staging** and click **Go**.

The Remote Staging and Distribution dialog box appears.

Step 3 Select any of the following:

- **Using External FTP Server** to use an external FTP server as the staging server.
For more information, see [Using External FTP Server](#).
- **Using External TFTP Server** to use an external TFTP server as the staging server.
For more information, see [Using External TFTP Server](#).
- **Using Remote Stage Device** to use a device as the remote staging device.
For more information, see [Using Remote Stage Device](#).

Using External FTP Server

LMS Software Management uses the External FTP server option to upgrade software images in one or more devices. When you select this option, you must enter the FTP credentials and image location.

The FTP copy command is arrived at based on the FTP credentials that you enter. Software Management uses Telnet or SSH protocol to connect to the devices and deploy the FTP `copy` command. This command gets the software images from the specified location in the FTP server.

Only WLSE and NAM devices support image distribution using External FTP server.

For more information, see [Supported Devices for FTP](#).

If you have selected Using External FTP server option:

Step 1 Enter the following FTP credentials in their applicable text boxes:

Field	Description
FTP Server Name	Name of the FTP server
FTP User Name	FTP Username to access the External FTP server.
FTP Password	FTP Password to access the External FTP server.
Image Location	Location of the image in the FTP server directory. These images will be used by Software Management to upgrade the software images on the selected devices.

Software Management will validate the FTP credentials and image location only while the job is running; not while the job is being scheduled.

If you have selected Using External TFTP server option, proceed to the [TFTP Wizard](#).

Step 2 Click **Next**.

The Remote Staging and Distribution dialog box appears.

Step 3 Select:

- a. An image from the Image Selection pane.
- b. Click on **Select Applicable Devices** button to automatically select the applicable devices

Or

Manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see [Unsupported Software Images](#).

Step 4 Click **Next**.

If you have selected Using External TFTP server option, proceed to the [TFTP Wizard](#).

The External FTP Server Details dialog box appears with the following details:

Field	Description
IP Address	IP Address of the External FTP server.
Selected Image	Image name that you have selected for distribution.
Errors	Error information.

Step 5 Click **Next**.

If you have selected Using External TFTP server option, proceed to the [TFTP Wizard](#).

The Device Recommendation dialog box appears with the following details:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of recommended image storage information.
Errors	Error information.

Step 6 Click **Next**.

If you have selected Using External TFTP server option, proceed to the [TFTP Wizard](#).

The Remote Devices Verification dialog box appears with the following details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.

Field	Description
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 7 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 8 Enter the following information. If you have selected Using External TFTP server option, proceed to the [TFTP Wizard](#).

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (using remote staging) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent from the LMS E-mail ID.
Comments	Enter the additional information about this job.
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: <ul style="list-style-type: none"> • Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. • Line cards reboot automatically. • Does not apply to PIX devices managed through Auto Update Server (AUS).

Field	Description
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the FTP server directory. Uses this copy if reboot with new image fails. Note the following: <ul style="list-style-type: none"> This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. Backup image is not deleted after upgrade. It remains in FTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do <i>not</i> select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.
Enable Job Password	Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution. The credentials that you enter here are used for this particular Software Management job. The credentials that you have entered in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices) are ignored. You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See <i>Administration of Cisco Prime LAN Management Solution 4.2</i> for more details.

Field	Description
Execution	<p>Select the job execution order for the devices. This can be either Parallel or Sequential:</p> <ul style="list-style-type: none"> • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Execution Order. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click Done.
Reboot	<p>Select the reboot order for the devices. This can be either Parallel or Sequential.</p> <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Boot Order. The Boot Order dialog box appears. 2. Use the Up and the Down arrows to order your devices list. 3. Click Done.

- Step 9** Click **Next** after you finish entering the job information details. If you have selected Using External TFTP server option, proceed to the [TFTP Wizard](#).

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External FTP server.
- Verification warnings generated during image distribution (if applicable).

- Step 10** Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Supported Devices for FTP

Table 9-7 Supported Devices for FTP

Device Family	Device	SysObject ID
NAM	NAM X6380	1.3.6.1.4.1.9.5.1.3.1.1.2.223
	NAM1	1.3.6.1.4.1.9.5.1.3.1.1.2.914
	NAM2	1.3.6.1.4.1.9.5.1.3.1.1.2.291
	NM NAM	1.3.6.1.4.1.9.1.562
	NME NAM	1.3.6.1.4.1.9.1.826
WLSE	WLSE	1.3.6.1.4.1.9.1.459
	WLSE	1.3.6.1.4.1.9.1.630
	WLSE	1.3.6.1.4.1.9.1.631
	WLSE 1153	1.3.6.1.4.1.9.1.752
Cisco Catalyst 3750 Series Switches	CatalystIOS37XXStack	1.3.6.1.4.1.9.1.516
	Catalyst3750ME	1.3.6.1.4.1.9.1.574
	WS.C3750G.12S.SD	1.3.6.1.4.1.9.1.688
	WS.C3750E.24TD	1.3.6.1.4.1.9.1.789
	WS.C3750E.48TD	1.3.6.1.4.1.9.1.790
	WS.C3750E.48PD	1.3.6.1.4.1.9.1.791
	WS.C3750E.24PD	1.3.6.1.4.1.9.1.792
	catalyst375024	1.3.6.1.4.1.9.1.511
	catalyst375048	1.3.6.1.4.1.9.1.512
	catalyst375024TS	1.3.6.1.4.1.9.1.513
	catalyst375024T	1.3.6.1.4.1.9.1.514
	catalyst375048PS	1.3.6.1.4.1.9.1.535
	catalyst3750G24PS	1.3.6.1.4.1.9.1.602
	catalyst3750G48PS	1.3.6.1.4.1.9.1.603
	catalyst3750G48TS	1.3.6.1.4.1.9.1.604
	catalyst3750G24TS1U	1.3.6.1.4.1.9.1.624
catalyst375024FS	1.3.6.1.4.1.9.1.656	
Cisco Intelligent Gigabit Ethernet Switch Module (IEGSM)	ciscoIGESM	1.3.6.1.4.1.9.1.592
	ciscoIGESMSFP	1.3.6.1.4.1.9.1.660

Table 9-7 Supported Devices for FTP

Device Family	Device	SysObject ID
Cisco Catalyst 3560,C3560E Series Switches	CatalystIOS3560G.24PS	1.3.6.1.4.1.9.1.614
	CatalystIOS3560G.24TS	1.3.6.1.4.1.9.1.615
	CatalystIOS3560G.48PS	1.3.6.1.4.1.9.1.616
	CatalystIOS3560G.48TS	1.3.6.1.4.1.9.1.617
	CatalystIOS3560.24PS.S	1.3.6.1.4.1.9.1.563
	CatalystIOS3560.48PS	1.3.6.1.4.1.9.1.564
	CatalystIOS3560.24TS	1.3.6.1.4.1.9.1.633
	CatalystIOS3560.48TS	1.3.6.1.4.1.9.1.634
	WS.C3560E.24TD	1.3.6.1.4.1.9.1.793
	WS.C3560E.48TD	1.3.6.1.4.1.9.1.794
	WS.C3560E.24PD	1.3.6.1.4.1.9.1.795
	WS.C3560E.48PD	1.3.6.1.4.1.9.1.796
	WS.C3560.8PC	1.3.6.1.4.1.9.1.797
	WS-C3560E-12D-S	1.3.6.1.4.1.9.1.930
	WS-C3560E-12SD-E	1.3.6.1.4.1.9.1.956
	WS-C3560-12PC-S	1.3.6.1.4.1.9.1.1015
Cisco Blade Switches (CBS)	CBS3030Del	1.3.6.1.4.1.9.1.749
	CBS3020	1.3.6.1.4.1.9.1.748
	CBS3040	1.3.6.1.4.1.9.1.784
	CBS1100	1.3.6.1.4.1.9.1.946
	CBS3110	1.3.6.1.4.1.9.1.947
	CBS3120	1.3.6.1.4.1.9.1.948
	CBS3130	1.3.6.1.4.1.9.1.949
	CBS3012	1.3.6.1.4.1.9.1.999
	CBS3012I	1.3.6.1.4.1.9.1.1000
	CBS3132	1.3.6.1.4.1.9.1.920
	CBS3110G-S	1.3.6.1.4.1.9.1.909
	CBS3110X-S	1.3.6.1.4.1.9.1.910
	CBS3110G-S-I	1.3.6.1.4.1.9.1.911
	CBS3110X-S-I	1.3.6.1.4.1.9.1.912
	CBS3125G-S	1.3.6.1.4.1.9.1.1001
	CBS3120G-S	1.3.6.1.4.1.9.1.918
	CBS3125X-S	1.3.6.1.4.1.9.1.1002
	CBS3120X-S	1.3.6.1.4.1.9.1.919
CBS3130G-S	1.3.6.1.4.1.9.1.921	
CBS3130X-S	1.3.6.1.4.1.9.1.922	

Table 9-7 Supported Devices for FTP

Device Family	Device	SysObject ID
Cisco Catalyst 2960 Series Switches	Catalyst296024	1.3.6.1.4.1.9.1.694
	Catalyst296048	1.3.6.1.4.1.9.1.695
	Catalyst2960G24	1.3.6.1.4.1.9.1.696
	WS-C2960G-48TC-L	1.3.6.1.4.1.9.1.697
	Catalyst296024TT	1.3.6.1.4.1.9.1.716
	Catalyst296048TT	1.3.6.1.4.1.9.1.717
	Catalyst29608TC	1.3.6.1.4.1.9.1.798
	Catalyst2960G8TC	1.3.6.1.4.1.9.1.799
	C2960-24-S	1.3.6.1.4.1.9.1.929
	C2960-24TC-S	1.3.6.1.4.1.9.1.928
	C2960-48TC-S	1.3.6.1.4.1.9.1.927
	C2960-24PC-L	1.3.6.1.4.1.9.1.950
	C2960-24LT-L	1.3.6.1.4.1.9.1.951
	C2960PD-8TT-L	1.3.6.1.4.1.9.1.952
	C2960P	1.3.6.1.4.1.9.1.1006
	C2960	1.3.6.1.4.1.9.1.1005
Cisco Catalyst 3550 Series Switches	Catalyst355012T	1.3.6.1.4.1.9.1.368
	Catalyst355024switch	1.3.6.1.4.1.9.1.366
	Catalyst355048switch	1.3.6.1.4.1.9.1.367
	Catalyst355012G	1.3.6.1.4.1.9.1.431
	Catalyst355024DC	1.3.6.1.4.1.9.1.452
	Catalyst355024FX	1.3.6.1.4.1.9.1.453
	Catalyst355024PWR	1.3.6.1.4.1.9.1.485
Cisco PIX Series Security Appliances	PIX 535	1.3.6.1.4.1.9.1.675
	PIX 525	1.3.6.1.4.1.9.1.676
	PIX 515	1.3.6.1.4.1.9.1.678
	PIX 515E	1.3.6.1.4.1.9.1.451
	PIX 515EFirewall	1.3.6.1.4.1.9.1.677

Table 9-7 Supported Devices for FTP

Device Family	Device	SysObject ID
Cisco Adaptive Security Appliances (ASA)	ASA5510	1.3.6.1.4.1.9.1.773
	ASA5520	1.3.6.1.4.1.9.1.671
	ASA5520	1.3.6.1.4.1.9.1.670
	ASA5510	1.3.6.1.4.1.9.1.669
	ASA5505	1.3.6.1.4.1.9.1.745
	ASA5550	1.3.6.1.4.1.9.1.763
	ASA5540	1.3.6.1.4.1.9.1.673
	ASA5580	1.3.6.1.4.1.9.1.672
	ASA5550	1.3.6.1.4.1.9.1.753
	ASA5540	1.3.6.1.4.1.9.1.914
	ASA5580	1.3.6.1.4.1.9.1.915

Using External TFTP Server

If you have selected Using External TFTP server option:

Step 1 Enter the external TFTP server IP address in the Enter TFTP IP Address text box.

Step 2 Click **Next**.

The Remote Staging and Distribution dialog box appears.

Step 3 Select:

- a. An image from the Image Selection pane.
- b. Click on **Select Applicable Devices** button to automatically select the applicable devices

Or

Manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see [Unsupported Software Images](#).

Step 4 Click **Next**.

The External TFTP Server Details dialog box appears with the following details:

Field	Description
IP Address	IP Address of the External TFTP server.
Selected Image	Image name that you have selected for distribution.
Errors	Error information.

Step 5 Click **Next**.

The Device Recommendation dialog box appears with the following details:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of recommended image storage information.
Errors	Error information.

Step 6 Click **Next**.

The Remote Devices Verification dialog box appears with the following details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 7 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 8 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (using remote staging) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Comments	Enter the additional information about this job.

Field	Description
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: <ul style="list-style-type: none"> Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. Line cards reboot automatically. Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following: <ul style="list-style-type: none"> This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do <i>not</i> select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.

Field	Description
Enable Job Password	<p>Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution.</p> <p>The credentials that you enter here are used for this particular Software Management job.</p> <p>The credentials that you have entered in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices) are ignored.</p> <p>You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See <i>Administration of Cisco Prime LAN Management Solution 4.2</i> for more details.</p>
Execution	<p>Select the job execution order for the devices. This can be either Parallel or Sequential:</p> <ul style="list-style-type: none"> • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Execution Order. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click Done.
Reboot	<p>Select the reboot order for the devices. This can be either Parallel or Sequential.</p> <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Boot Order. The Boot Order dialog box appears. 2. Use the Up and the Down arrows to order your devices list. 3. Click Done.

Step 9 Click **Next** after you finish entering the job information details

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External TFTP/FTPserver.
- Verification warnings generated during image distribution (if applicable).

Step 10 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Using Remote Stage Device

If you have selected Remote Stage device option:

Step 1 Go to the Select Remote Stage Device pane, select a device that you want to use as the remote stage device. Ensure that you select a device that supports remote staging.

If you select a device that does not support remote staging, an error message is displayed.

Step 2 Click **Next**.

The Remote Staging and Distribution dialog box appears.

Step 3 Select:

- a. An image from the Image Selection pane.
- b. Click **Select Applicable Devices** to automatically select the applicable devices

or

Manually select the devices that need an upgrade from the Devices to be Upgraded pane.

For more information on the unsupported images for Remote Staging and Distribution, see [Unsupported Software Images](#).

Step 4 Click **Next**.

The Remote Stage and Image Upgrade Details dialog box appears with the following details:

Field	Description
Remote Stage Name	Name of the remote stage device that you want to use as a remote stage.
Selected Image	Image name that you have selected for distribution.
Storage Options	Image storage information

Step 5 Click **Next**.

If the Remote Stage verification fails, check if the Remote Stage device has enough free space and restart the software distribution from the beginning.

The Device Recommendation dialog box appears. This displays the following details:

Field	Description
Device Information	Name of the device. Click on the device name to launch the Troubleshooting page.
Module Information	Image type, chassis model, and software version on device.
Storage Options	Details of recommended image storage information.

Step 6 Click **Next**.

The Remote Devices Verification dialog box appears with the following details:

Field	Description
Device	Name of the device
Selected Module	Module information that you have selected.
Selected Slot	Image storage information that you have selected.
Verification Result	Click on the link to review the details.

Step 7 Click **Next**.

The Job Schedule and Options dialog box appears.

Step 8 Enter the following information:

Field	Description
Scheduling	
Run Type	You can specify when you want to run the Image Distribution (using remote staging) job. To do this, select one of these options from the drop-down menu: <ul style="list-style-type: none"> • Immediate—Runs this job immediately. • Once—Runs this job once at the specified date and time.
Date	Select the date and time (hours and minutes) to schedule.
Job Info	
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.
E-mail	Enter e-mail addresses to which the job sends messages at the beginning and at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Admin > System > System Preferences). We recommend that you configure the LMS E-mail ID in the View / Edit System Preferences dialog box (Admin > System > System Preferences). When the job starts or completes, an e-mail is sent with the LMS E-mail ID as the sender's address.
Comments	Enter the additional information about this job.

Field	Description
Maker E-Mail	Enter the e-mail ID of the job creator. This is a mandatory field. This field is displayed only if you have enabled Job Approval for Software Management.
Maker Comments	Enter comments for the job approver. This field is displayed only if you have enabled Job Approval for Software Management.
Job Options	
Reboot immediately after download	Choose not to reboot (and reboot manually later) or to reboot immediately after download. You cannot select this option, if you have selected the Do not insert new boot commands into the configuration file option. Note the following about this option: <ul style="list-style-type: none"> Does not apply to Cisco IOS SFB 2500/1600/5200 devices. These devices always reboot immediately. Line cards reboot automatically. Does not apply to PIX devices managed through Auto Update Server (AUS).
Perform distribution in Non-Installed mode	This option is only available if the selected devices have IOS Software Modularity images running. This option allows you to choose whether you want to install the images in Installed or Non-Installed mode. By default Software Management distributes images in Installed mode.
Do not insert new boot commands into configuration file	Do not insert boot commands into configuration file to reboot with new image. You cannot select this option, if you have selected the Reboot immediately after download option. Does not apply to Cisco IOS SFB 2500/1600/5200 devices. Configuration file for these is always updated.
Use current running image as tftp fallback image	If running image is in repository, select option to place a copy in the TFTP server directory. Uses this copy if reboot with new image fails. Note the following: <ul style="list-style-type: none"> This option is subject to your platform restrictions to boot over connection to server. Check your platform documentation. Backup image is not deleted after upgrade. It remains in TFTP server directory so that device can find it any time it reboots
Back up current running image	Select to back up running image in software image repository before upgrading. Line cards do not support upload.
On error, halt processing of subsequent devices	Select to stop the job if a download or reboot error on a device or a module occurs. The default is to continue to next device. For sequential execution, if you do <i>not</i> select this option, upgrade for next device begins. For parallel execution, upgrade occurs in batches. On completion of the ongoing batch, subsequent devices are not processed. See the Job Summary page for details.

Field	Description
Enable Job Password	<p>Enter the password for the distribution job. This password is used to connect to the devices using Telnet at the time of distribution.</p> <p>The credentials that you enter here are used for this particular Software Management job.</p> <p>The credentials that you have entered in the Device and Credentials database (Inventory > Device Administration > Add / Import / Manage Devices) are ignored.</p> <p>You are allowed to provide a password in this field only if you have selected the Enable Job Based Password in the View / Edit Preferences dialog box. See <i>Administration of Cisco Prime LAN Management Solution 4.2</i> for more details.</p>
Execution	<p>Select the job execution order for the devices. This can be either Parallel or Sequential:</p> <ul style="list-style-type: none"> • Sequential—Job runs on the devices, sequentially. You can define this sequence. • Parallel—Job runs on a batch of 15 devices at the same time. <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Execution Order. The Execution Order dialog box appears. 2. Use the Up and Down arrows to order your the device list. 3. Click Done.
Reboot	<p>Select the reboot order for the devices. This can be either Parallel or Sequential.</p> <p>If you have selected Sequential:</p> <ol style="list-style-type: none"> 1. Click Boot Order. The Boot Order dialog box appears. 2. Use the Up and the Down arrows to order your devices list. 3. Click Done.

Step 9 Click **Next** after you finish entering the job information details

The Software Distribution Work Order dialog box appears with these details:

- Summary of the job information.
- State of the running image on the device.
- Image selected for the upgrade.
- Job Approval information.
- Whether Flash memory will be erased before the new image is loaded.
- Operations that will be performed during the upgrade procedure.
- Whether the bootloader will be upgraded. (For a bootloader upgrade.)
- Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device.
- Details of the Remote Stage device or the External TFTP server.
- Verification warnings generated during image distribution (if applicable).

Step 10 Click **Finish**.

The notification window appears with the Job ID.

To check the status of your scheduled job, select **Configuration > Tools > Software Image Management > Jobs**.

Unsupported Software Images

During remote staging, there maybe software images running on the devices selected for remote staging, but some of them may not get listed as available images. This is because, some software images do not support Remote Staging and Distribution.

The following below lists the software images that do not support Remote Staging and Distribution:

- CSS_SW FDDI_CDDI
- ATM_WTALL
- ATM_WBPVC
- CIP
- CSS_11000_SW
- C6KMODULE_MWAM_SW
- PATCH_SW
- ONS15530
- TOKENRING
- ATM_WBLANE
- BOOT_LOADER
- C6KMODULE_MWAM_SW
- CSS_11500_SW
- CSS_11000_SW
- C2500
- C1600
- BLADERUNNER
- ATM_WTOKEN
- MICA MICROCOM
- NAM_APPL_SW
- SPA_FPD_SW
- CSS_11500_SW
- ONS15540

Understanding Upgrade Recommendations

This section describes how Software Management recommends image for the various Cisco device types:

- [Upgrade Recommendation for Cisco IOS Devices](#)
- [Upgrade Recommendation for Catalyst Devices](#)
- [Upgrade Recommendation for VPN 3000 Series](#)
- [Upgrade Recommendation for Catalyst 1900/2820](#)
- [Upgrade Recommendation for Other Device Types](#)

Upgrade Recommendation for Cisco IOS Devices

To determine the recommended software images for Cisco IOS devices, Software Management:

1. Lists all images in the software repository that can run on the device. For example, C7000 images run on 7000 and 7010 devices, IGS images run on 25xx devices, and so on.
2. Removes all listed images that require:
 - More RAM or Flash memory than is available on the device.
 - A newer boot ROM than the one on the device.

If RAM is UNKNOWN, it is not considered in any comparison operation (image filtering). However, you are warned during the subsequent task.

3. Recommends an image whose feature subset matches the image running on the device.
 - Any images that support all current features and include some additional ones, take precedence over images that match exactly.
 - If more than one image is either a superset or an exact match of the running image, the latest version takes precedence over earlier versions.
4. Removes the images from recommendation if the images Min.Flash size requirement is not met by the device.

If Min.Flash required is UNKNOWN, it is not considered in any comparison operation (image filtering).

If Flash Size is UNKNOWN, the image cannot be used for upgrade.

See the IOS Software Release documentation on Cisco.com to know the Min.Flash size.

5. Depending on the image feature list, Software Management recommends an image whose image version is lower than the current running image version.
6. Recommends to filter out the images that are larger in size than the flash available on the device.
7. Recommends Flash partitions on the device along with the storage details, if you are upgrading the Boot Loader image.

This algorithm might recommend images that are older than the one running on the device.

To ensure that only newer images are recommended, select **Admin > Network > Software Image Management > View/Edit Preferences**. In the View/Edit Preferences dialog box, select the Include images higher than running image checkbox, then click **Apply**.

Upgrade Recommendation for Catalyst Devices

For Catalyst device upgrades, Software Management typically recommends the latest version images in the software repository.

For default RAM requirements for Supervisor Engine I and Supervisor Engine III, however, Software Management uses:

Module Type and Version	Default RAM (MB)
Supervisor Engine III	32
Supervisor version 2.1 up to (but not including) 3.1	8
Supervisor version 3.1.1 and later	16
Maintenance release versions 3.1 and 3.2 with “Sup8M” in filename	8

For supervisor versions 3.1 to 3.2, when the image repository or Cisco.com has both 8 MB of RAM and regular images available, Software Management also checks the device RAM:

1. If the RAM can be determined and the available RAM is greater than 16 MB:
 - a. Software Management recommends the latest regular supervisor image where the RAM requirement is less than the available RAM.
 - b. If no regular image with matching RAM requirements is available, it recommends the latest version of the 8-MB images.
 - c. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).
2. If the RAM can be determined and the available RAM is less than 16 MB:
 - a. Software Management recommends the highest image version for which the RAM requirement is less than 16 MB.
 - b. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).
3. If the RAM cannot be determined:
 - a. Software Management recommends the latest regular image.
 - b. If no regular image is available, it recommends the latest 8-MB image.
 - c. If there is still no matching image, it recommends the latest image version that has no RAM requirements (where the RAM requirement is set to DEFAULT_SIZE).

The minimum RAM in the image attributes file supersedes these guidelines.

For example, if a supervisor engine module is running the version 3.1 maintenance release (8 MB RAM) but the RAM in the image attributes was changed to 16 MB, Software Management uses the value in the attributes file.

Upgrade Recommendation for VPN 3000 Series

Software Management recommends the latest version of the image in the software image repository. If the device is a VPN 3005 Concentrator, it recommends the VPN 3005 System software images in the repository.

Upgrade Recommendation for Catalyst 1900/2820

For Catalyst 1900/2820 Enterprise version device upgrades, Software Management typically recommends the latest version of images in the software repository.



Note

For Catalyst 1900/2820 Series devices, Software Management recommends images with version numbers greater than 8.0(0) because the older versions do not support the Command Line Interface. Non-Enterprise versions of the Catalyst 1900/2820 are not supported in Software Management.

Upgrade Recommendation for Other Device Types

For the following device types, Software Management recommends the latest version of the image in the software image repository:

- PIX Firewall Devices

If you are running PIX image version 7.0 or later, while recommending the image, Software Management will also recommend the storage details of the device.

- Content Service Switches
- Aironet AP Series
- Optical Switch Series
- Network Analysis Module Series
- Content Engines

Using Software Management Job Browser

Using this window you can view all your scheduled Software Management jobs.

The Software Management Job Browser contains the following fields and buttons:

- [Software Management Job Browser Fields](#)
- [Software Management Job Browser Buttons](#)

This section contains:

- [Changing the Schedule of a Job](#)
- [Retry a Failed Distribution Job](#)
- [Undo a Successful Distribution Job](#)
- [Stopping a Job](#)
- [Deleting Jobs](#)

The Software Management Job Browser displays the following details for a job:

Table 9-8 Software Management Job Browser Fields

Field	Description
Job ID	<p>Unique number assigned to the job when it is created.</p> <p>Click to display a summary of job details and schedule options.</p> <p>See Understanding the Software Management Job Summary for further details.</p>
Job Type	Type of job such as Import Images, Distribute Images.
Status	<p>Job states:</p> <ul style="list-style-type: none"> • Successful—Job completed successfully • Failed—Failed job. Click on the Job ID to view the job details. The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed. For example, If the status displays Failed(5), then the count of devices that had failed is 5. • Running—Job still running. • Pending—Job scheduled to run. • Stopped—Running job stopped by you. • Missed Start—Job could not run for some reason at the scheduled time. For example, if the system was down when the job was scheduled to start, when the system comes up again, the job does not run. This is because the scheduled time for the job has elapsed. The status for the specified job will be displayed as Missed Start. • Approved—Job approved by an approver • Rejected—Job rejected by an approver. Click on the Job ID to view the rejection details. • Waiting for Approval—Job waiting for approval.
Description	Job description as entered at the time of creation.
Owner	User who created the job.
Scheduled At	Start time of the scheduled job.
Completed At	End time of the scheduled job.
Schedule Type	<p>Type of the scheduled job:</p> <ul style="list-style-type: none"> • Immediate • Once

Table 9-9 Software Management Job Browser Buttons

Buttons	Description
Edit	Reschedules the job. You can change the schedule only for jobs that are in the Pending, Waiting for Approval or the Approved status. See Changing the Schedule of a Job .
Retry	Retry the failed job. You can retry only failed distribution jobs. See Retry a Failed Distribution Job .
Undo	Undo a successful job. You can undo only successful distribution jobs. See Undo a Successful Distribution Job . However, you cannot undo a successful software distribution job scheduled for NAM devices. If you still try to Undo this job, an error message is displayed indicating that the Undo operation is not supported for NAM devices.
Stop	Stops a scheduled job. You can Stop only jobs that are either in the Pending or the Running status. See Stopping a Job .
Delete	Delete the jobs. See Deleting Jobs .
Refresh (Icon)	Click on this icon to refresh the Software Management Job Browser Window.

Changing the Schedule of a Job

You can change the schedule only for jobs that are either in the Pending, Waiting for Approval or the Approved status.



Note

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

To change the schedule of a job:

-
- Step 1** Select **Configuration > Tools > Software Image Management > Jobs**.
The Software Management Job Browser dialog box appears.
 - Step 2** Select either a pending or an approved job.
 - Step 3** Click **Edit**.
The Change Job Schedule dialog box appears.

Step 4 Change the schedule.

Step 5 Click **Submit**.

Retry a Failed Distribution Job

You can retry only failed distribution jobs.



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

To retry a Job:

Step 1 Select **Configuration > Tools > Software Image Management > Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select a failed distribution job.

Step 3 Click **Retry**.

The Retry Upgrade dialog box appears with the following information:

Field	Description
Device Information	Name of the device
Module	Device module
Pre-upgrade Image	Image name that was running before the upgrade.
Selected Image	Image name that is selected for distribution.
Running Image	Image name that is currently running on the device.
Errors	Click on the underlined Error message to review the details.

Step 4 Click **Next**.

Continue entering the information for this job as you would for a new distribution depending on your previous distribution selection:

- [Distributing by Devices \[Basic\]](#)
- [Distributing by Devices \[Advanced\]](#)
- [Distributing by Images](#)
- [Remote Staging and Distribution](#)

Undo a Successful Distribution Job

You can undo only successful Distribution jobs.



Note

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

To undo a job:

Step 1 Select **Configuration > Tools > Software Image Management > Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select a successful distribution job.

Step 3 Click **Undo**.

The Undo Upgrade dialog box appears with the following information:

Field	Description
Device	Name of the device
Module	Device module
Pre-upgrade Image	Image name which was running before the upgrade.
Post-upgrade Image	Image name after completing the upgrade.
Running Image	Image name that is currently running on the image.
Errors	Click on the underlined Error message to review the details.

Step 4 Click **Next**.

Continue entering the information for this job as you would for a new distribution. This depend on what you selected earlier in the Distribution Method window:

- [Distributing by Devices \[Basic\]](#)
- [Distributing by Devices \[Advanced\]](#)
- [Distributing by Images](#)
- [Remote Staging and Distribution](#)

Stopping a Job

You can stop only jobs that are either in the Pending or the Running status.

The job stops only after the current task is complete. During this time, the Software Management Job Browser window displays the job status as Running.



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

To stop a job:

Step 1 Select **Configuration > Tools > Software Image Management > Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select either a pending or a running job.

Step 3 Click **Stop**.

A confirmation box shows that the selected job will be stopped.

Step 4 Click **OK**.

A message appears that the selected job has been stopped.

After the job is stopped, the Pending job status changes to Stopped. The Running job status changes temporarily to Stop Initiated and then to Stopped.

Deleting Jobs

To delete jobs:



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

Step 1 Select **Configuration > Tools > Software Image Management > Jobs**.

The Software Management Job Browser dialog box appears.

Step 2 Select the jobs.

Step 3 Click **Delete**.

A confirmation box shows that the selected jobs will be deleted.

Step 4 Click **OK**.

Understanding the Software Management Job Summary

From the Software Management Job Browser, you can learn more about one job by viewing its details. You can view this details by clicking the Job ID on the Software Management Job Browser window.



Note

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

The Software Management Job Details window contains the following information:

Page/Folder	Description
Work Order	<p>Select a device to view the summary of the job:</p> <ul style="list-style-type: none"> • If there is more than one device, the software distribution order. • The state of the running image on the device. • The image selected for the upgrade. • Whether Flash memory will be erased before the new image is loaded. • Operations that will be performed during the upgrade procedure. • For a bootloader upgrade, whether the bootloader will be upgraded. • The Job Approval information. • Information you should know before the upgrade begins. For instance, if the Image Subset feature has changed on the device, you might need to reconfigure the device. • Details of the Remote Stage device (if applicable). • Verification warnings generated during image distribution (if applicable).
Job Results	<p>Select a device to view the complete job result. It displays information on:</p> <ul style="list-style-type: none"> • The job status, start time and end time. • The job completion status on the devices you have selected. For example, number of successful devices where the job is executed successfully. • The import/upgrade mode (parallel or sequential) • The protocol order used for image transfer and configuration tasks. • How the job was processed.
Summary[On Job Complete]	<p>Displays the summary of the completed job</p> <p>For software distribution jobs, the summary contains details about the device, image type, running image name, upgrade image name, upgrade storage location, and image distribution status.</p> <p>For software import jobs, the summary contains details about device, image name, storage location, and import status of the image.</p> <p>The Job Summary is not generated for Image Out-Of-Sync Report job.</p>

Understanding User-supplied Scripts

User-supplied scripts are run before and after each device upgrade, for example:

- The preupgrade script can check whether the device is accessible.
- The preupgrade script can check whether any users are connected to the access server. If the script finds that some users are connected, it can decide whether to disable the connections before upgrading.
- The post-upgrade script can check whether the upgrade was successful. Depending on the return value, Software Management either halts or continues with the rest of the upgrade.

The following sections contain:

- [Script Requirements](#)
- [Script Parameters](#)
- [Sample Script](#)

Script Requirements

- In the Edit Preferences dialog box (**Admin > Network > Software Image Management > View/Edit Preferences**), enter:
 - Enter the shell scripts (*.sh) on UNIX and batch files (*.bat) on Windows.

On UNIX, the scripts should have read, write, and execute permissions for the owner (casuser) and read and execute permissions for group casusers. That is, the script should have 750 permission.

On Windows, the script should have read, write, and execute permissions for casuser/Administrator.

The other users should have only read permission. You must ensure that the scripts contained in the file has permissions to execute from within the *casuser* account.
 - The script files *must* be available at this location:

On Solaris and Soft Appliance:
/var/adm/CSCOpX/files/scripts/swim

On Windows:
NMSROOT\files\scripts\swim
 - User script timeout

Software Management waits for the time specified before concluding that the script has failed.
- Software Management verifies that:
 - The script has write and execute permissions for the user *casuser*.
 - Only users logged in as Administrator, root, or *casuser* have write and execute permissions.



Caution

The script should not write output to the system console. The script can write the output to a file. Writing the script output to the system console can cause the Software Management job to hang.

Script Parameters

Software Management passes a parameter indicating whether the script is running before or after the upgrade. If the script does not intend to perform any pre-upgrade check, the script can return an exit value of zero and perform checks in the post-upgrade. See the [Sample Script](#) for reference.

The parameters provided to the script by Software Management are in the form of environment variables.

The server environment variables such as *PATH*, *SystemRoot*, etc., are not passed on to the script by Software Management. You have to set the relevant environment variables within the script. See the [Sample Script](#) for reference.

See Adding Devices to the Device and Credential Repository section in the *Inventory Management with Cisco Prime LAN Management Solution 4.2* for further information on device hostname, device name (device name), SNMP v2 community strings, etc.

The different parameters are described in the table below:

Variable	Description
CRM_SCRIPT_CONTEXT	This variable is used to determine if the script has to be invoked before or after image upgrade. If you set the variable to, <ul style="list-style-type: none"> PRE-DOWNLOAD—Script is invoked by Software Management prior to image upgrade. POST-DOWNLOAD—Script is invoked by Software Management post image upgrade.
NMSROOT	LMS installed directory.
TMPDIR	Directory provided to LMS to create temporary files.
CRM_DEV_NAME	Name of Device Name as entered in Device and Credential Repository.
CRM_SNMP_V2_RWCOMMUNITY	SNMP version 2 read-write community string.
CRM_SNMP_V2_ROCOMMUNITY	SNMP version 2 read only community string.
CRM_SNMP_V3_ENGINE_ID	SNMP version 3 Engine ID
CRM_SNMP_V3_USER_ID	User ID configured for SNMP version 3 protocol access on the device.
CRM_SNMP_V3_PASSWORD	SNMP version 3 password for the user ID.
CRM_ENABLE_PASSWORD	Enable password.
CRM_PRIMARY_USERNAME	Primary user name configured on the device.
CRM_PRIMARY_PASSWORD	Primary password configured on the device.
CRM_DEV_MGMT_IP_ADDR	IP address provided in Device and Credential Repository for management.

Sample Script

The sample script illustrates how to use this option before the upgrade to see if the device is accessible and after the upgrade to see whether it was successful.

The *sample.bat* file contains:

```
c:\progra~1\cscopx\bin\perl c:\progra~1\cscopx\files\scripts\swim\samplescript.pl
```

The *samplescript.pl* file contains:

```
#!/usr/bin/perl
BEGIN
{
use lib "$ENV{NMSROOT}/objects/perl5/lib/Net";

}
use Net::Telnet;
#my $output="";
## The following Environment variables are not passed on by Software Image Management
## Need to set these variables for the script to work as expected
$ENV{'Path'}="C:\\PROGRA~1\\CSCOPx\\MDC\\tomcat\\bin;C:\\PROGRA~1\\CSCOPx\\MDC\\Apache;C:\\PROGRA~1\\CSCOPx\\MDC\\jre\\bin;C:\\PROGRA~1\\CSCOPx\\MDC\\bin;C:\\PROGRA~1\\CSCOPx\\lib\\jre\\bin\\server;C:\\PROGRA~1\\CSCOPx\\objects\\db\\win32;C:\\PROGRA~1\\CSCOPx\\bin;c:\\cscopx\\lib\\jre\\bin\\server;c:\\cscopx\\lib\\jre141\\bin\\server;C:\\WINNT\\system32;C:\\WINNT;C:\\WINNT\\System32\\Wbem;C:\\Program Files\\Common Files\\Adaptec Shared\\System;c:\\progra~1\\cscopx;c:\\progra~1\\cscopx\\bin;";
$ENV{'TEMP'}=$ENV{'TMPDIR'};
$ENV{'TMP'}=$ENV{'TMPDIR'};
$ENV{'SystemRoot'}="C:\\WINNT";
##### Required Environment variables are set #####
my $prmpchar = '/>/i';
$filename = $ENV{'CRM_DEV_NAME'} . '.txt';
if ($ENV{'CRM_SCRIPT_CONTEXT'} eq 'PRE-DOWNLOAD') {
open OUTFILE, "> $filename" or die "Can't open file";
print OUTFILE %ENV;

my $host = $ENV{'CRM_DEV_MGMT_IP_ADDR'};
my $pwd = $ENV{'CRM_PRIMARY_PASSWORD'};
print OUTFILE $host;
print OUTFILE $pwd;
$telnet = new Net::Telnet(Input_Log=>"inp.txt");
$prev = $telnet->host($host);
print OUTFILE $prev;
print OUTFILE "Conntecting to Host...";
$telnet->open($host);
print OUTFILE "Connected ...";
$telnet->dump_log("dmp.txt");
$telnet->waitfor('/Username: $/i');
$telnet->print($ENV{'CRM_PRIMARY_USERNAME'});
$telnet->waitfor('/Password: $/i');
$telnet->print($pwd);
print OUTFILE "Password send";
($output) = $telnet->waitfor('/#$/i');
print OUTFILE "Returned after waitfor";
print OUTFILE $output;
$telnet->print('terminal length 0');
$telnet->waitfor('/#$/i');
$telnet->print('sh ver');
($output) = $telnet->waitfor('/#$/i');
print OUTFILE $output;
### If the device is not running the expected Image, return 1
### so that Software Image Management application does not proceed.
if ($output =~ m/Version 12.2\.(27\)/) {
print OUTFILE "Required Software running on Device, Allow to proceed with Upgrade\n"
```

```

    }
else
{
    print OUTFILE "Upgrade stopped, Device not running desired Image";
    close OUTFILE;
    exit(1);
}
close OUTFILE;
## A return vale of zero(0) allows the Software Image Management application to proceed
exit(0);
}
if ($ENV{'CRM_SCRIPT_CONTEXT'} eq "POST-DOWNLOAD") {
my $hostnew = $ENV{'CRM_DEV_MGMT_IP_ADDR'};
my $pwdnew = $ENV{'CRM_PRIMARY_PASSWORD'};
open OUTFILE, ">>$filename" or die "Can't open file";
print OUTFILE "=====  

POST DOWNLOAD RESULTS  

=====";
$telnet = new Net::Telnet(Input_Log=>"inpl.txt");
$telnet->dump_log("dmpo.txt");
$telnet->open($hostnew);
$telnet->waitfor('/Username: $/i');
$telnet->print($ENV{'CRM_PRIMARY_USERNAME'});
$telnet->waitfor('/Password: $/i');
$telnet->print($pwdnew);
($opt) = $telnet->waitfor('/#$/i');
$telnet->print('terminal length 0');
$telnet->waitfor('/#$/i');
$telnet->print('sh ver');
($opt) = $telnet->waitfor('/#$/i');
if ($opt =~ m/Version 12.3\ (10a\)/) {
    print OUTFILE "Required Software running on Device, Upgrade Successful\n";
}
}
print OUTFILE $opt;
close OUTFILE;
exit(0);
}

```

Locating Software Management Files

This table shows the locations of some of the Software Management directories and log files that describe what is happening in the system.

Contents	Operating System	Location
Software Management User Interface/job creation debug log file	Solaris and Soft Appliance	/var/adm/CSCOPx/log/swim_debug.log
	Windows	<i>NMSROOT</i> \log\swim_debug.log Where <i>NMSROOT</i> is the LMS installed directory.
Software Management job execution debug log files. You can set the debug mode for Software Management application in the Log Level Settings dialog box (Admin > System > Debug Settings > Config and Image Management Debugging Settings)	Solaris and Soft Appliance	/var/adm/CSCOPx/files/rme/jobs/swim/ <i>job-id</i> /swim_debug.log
	Windows	<i>NMSROOT</i> \files\rme\jobs\swim\ <i>job-id</i> \swim_debug.log Where <i>NMSROOT</i> is the LMS installed directory.

