



Updating Device Firmware

The options under the Firmware tab allow you to:

- Import firmware images (for access points and wireless bridges) to the WLSE and manage the firmware stored on the WLSE. If you need to update devices in remote locations, you can store images on a TFTP server instead of storing them on the WLSE. See [Managing Firmware Images, page 4-2](#).
- Run firmware jobs to update firmware on devices. See [Managing Firmware Jobs, page 4-11](#).
- Convert Cisco Aironet 1200 access points from non-IOS to IOS firmware. For information on conversion, see [Converting Access Points to IOS, page 4-30](#).

You can also display firmware versions supported by the WLSE and import a file that updates the firmware versions supported by the WLSE. These options are located under **Administration > System**. For more information, see [Viewing and Updating Supported Firmware Versions, page 4-11](#).



Note

One or both of the firmware subtabs may not be visible to some users.

Managing Firmware Images

The options under the Images subtab allow you to:

- View images—See [Viewing Images on the WLSE](#), page 4-2.
- Edit images—See [Editing Image Details on the WLSE](#), page 4-3.
- Delete images—See [Deleting Images from the WLSE](#), page 4-5.
- Download images to the WLSE—See [Importing Images to the WLSE](#), page 4-5.

You can also download images to a remote TFTP server if you are updating devices that are located remotely—See [Using a Remote TFTP Server for Updating Devices](#), page 4-10.

Related Topics

- [Managing Firmware Jobs](#), page 4-11
- [Converting Access Points to IOS](#), page 4-30

Viewing Images on the WLSE

You can view the list of images stored on the WLSE and view image details.

Procedure

Step 1 Select **Firmware > Images**. The Imported Firmware Images selector shows the images that have been imported into the WLSE.

Step 2 To view the list of available images for a type of device, expand its folder.



Note Images that you download to the WLSE are automatically listed in the Firmware Images selector.

Step 3 To view details on an image, select the image. The Image Details window opens, showing the image name, image version, image size, and a description.

Related Topics

[Editing Image Details on the WLSE, page 4-3](#)

Editing Image Details on the WLSE

Procedure

-
- Step 1** Select **Firmware > Images**.
- Step 2** Expand the folder that contains the image you want to edit, then select the image. The Image Details window opens.
- Step 3** You can edit the image name, image version, device type, and description:

Table 4-1 *Image Details*

Field	Description
Name	By default, the name of the image file or of the image file in a zipped file.
Device Type	<p>The device type to which the firmware applies. Be careful when entering the version; proper uploading of firmware to devices requires accurate version information. You can enter the version in uppercase or lowercase characters.</p> <p>If you change the device type of an image, the image is removed from the former device type folder and added to the new one. For example, if you change the device type from AP340 to AP350, the image is removed from the AP340 folder and added to the AP350 folder.</p>

Table 4-1 Image Details (continued)

Field	Description
Version	<p>Edit the image version. Be careful when editing the version; proper uploading of firmware to devices requires accurate version information. You can enter the version in uppercase or lowercase characters. If you change the device type of an image, the image is removed from the former device type folder and added to the new one. For example, if you change the device type from AP340 to AP350, the image is removed from the AP340 folder and added to the AP350 folder.</p> <p>Note To prevent errors when importing, do not rename IOS images.</p> <p>There are several valid formats for image version. You must retain all of the digits and letters and the first decimal point must be present. For example:</p> <ul style="list-style-type: none"> • Official format—12.2(4)JA1 • Cisco.com format—12.2.4-JA1 <p>Note If you are importing an image for non-IOS to IOS conversion, the version you enter <i>must be 12.2</i>. Otherwise, the image will be incompatible with the Cisco Aironet 1200 access points that you are converting.</p>
Size	Size of the image (read-only field).
Description	This field is blank by default.

Step 4 When you finish editing, click **Save**.

Related Topics

[Deleting Images from the WLSE, page 4-5](#)

Deleting Images from the WLSE

Procedure

- Step 1** Select **Firmware > Images**.
- Step 2** Expand the folder that contains the image you want to delete, then select the image. The Image Details window opens.
- Step 3** Click **Delete**, then click **OK**. The image is deleted from the list of images in the folder.
-

Related Topics

- [Viewing Images on the WLSE, page 4-2](#)
- [Editing Image Details on the WLSE, page 4-3](#)

Importing Images to the WLSE

This option allows you to:

- Download images to the WLSE from the desktop—see [Importing Images from the Client System Desktop to the WLSE, page 4-6](#).
- Download images to the WLSE directly from Cisco.com—see [Importing Images Directly from Cisco.com to the WLSE, page 4-8](#).

Related Topics

- [Viewing Images on the WLSE, page 4-2](#)
- [Editing Image Details on the WLSE, page 4-3](#)

Importing Images from the Client System Desktop to the WLSE

Procedure

- Step 1** Download the desired firmware images to your client system from Cisco.com. You can download firmware images from the following URL:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>



Note Only the combined images from Cisco.com are supported for importing to the WLSE. If you download an image component from another site and then try to import a component, the operation will fail.

For information about supported versions of images, see the Supported Devices document on Cisco.com and the Firmware Supported Versions table in **Administration > System > Firmware Supported Versions**. For more information on supported firmware versions, see [Viewing Supported Firmware Versions, page 6-111](#) and [Updating Supported Firmware Versions, page 6-111](#).

- Step 2** Select **Firmware > Images > Import > From Desktop**. Enter information as described in [Table 4-2 on page 4-7](#).

Table 4-2 Desktop Import Window

Field	Description
Device Type	Select the device type from the list.
Version	<p>Enter the image version. Be careful when entering the version; proper uploading of firmware to devices requires accurate version information. You can enter the version in uppercase or lowercase characters. If you change the device type of an image, the image is removed from the former device type folder and added to the new one. For example, if you change the device type from AP340 to AP350, the image is removed from the AP340 folder and added to the AP350 folder.</p> <p>Note To prevent errors when importing, do not rename IOS images.</p> <p>There are several valid formats for image version. You must retain all of the digits and letters and the first decimal point must be present. For example:</p> <ul style="list-style-type: none"> • Official format—12.2(4)JA1 • Cisco.com format—12.2.4-JA1 <p>Note If you are importing an image for non-IOS to IOS conversion, the version you enter <i>must be 12.2</i>. Otherwise, the image will be incompatible with the Cisco Aironet 1200 access points that you are converting.</p>
File Location	<p>Enter the path to the image on the desktop or click Browse.</p> <p>Images for Cisco Aironet 350 wireless bridges may be named as images for access points (that is, names begin with <i>AP</i>). To avoid confusion, you can rename these images (see Editing Image Details on the WLSE, page 4-3.)</p>
Overwrite Existing Image	Select this if you are importing an image that is already stored on the WLSE. Otherwise, the image import will fail if the same image is already stored on the WLSE.

Step 3 Click **Import**. *Do not close the popup window until you receive a message that the import was successful or the import failed.*

If the import is successful, a confirmation message appears and the image is saved on the WLSE.

If the import fails, an error message appears. The import may fail for one of the following reasons:

- The image you are trying to import is not valid. An error message appears.
- There is insufficient space on the WLSE to store images.
- You specified an image that already exists in the image library and you did not select the Overwrite Existing Image checkbox in Step 2.
- For an IOS image, you renamed the file or the file is not recognized.

Step 4 Repeat Steps 2 and 3 to import more images.

Step 5 For information on uploading firmware to access points and bridges, see [Managing Firmware Jobs, page 4-11](#).

Importing Images Directly from Cisco.com to the WLSE

The first time you attempt to download firmware for IOS access points from Cisco.com, an error message is displayed and you must acknowledge that you have the required cryptography permissions. See the following procedure for the text of the message.

Procedure

Step 1 Select **Firmware > Images > Import > From Cisco.com**. Complete the following:

Table 4-3 Cisco.com Import Window

Field	Description
Cisco.com Username	Your Cisco.com username.
Cisco.com Password	Your Cisco.com password
Proxy IP/Hostname ¹	The IP address of the proxy server used to mediate between the web browser and Cisco.com. The proxy port used by the proxy server (if required on your network).
Proxy Port	
Proxy Username	The username and password for contacting the proxy server (if required on your network).
Proxy Password	

1. Some proxy server software does not work properly while importing firmware from Cisco.com. If you have problems using your proxy server with this feature, download the firmware image to your desktop from Cisco.com and import the image from the desktop (see [Importing Images from the Client System Desktop to the WLSE, page 4-6](#)).

Step 2 To clear all of your entries in the window, click **Clear**.

Step 3 To proceed with image download, click **Login**. The Import window changes to allow you to select the device type.

If the following message appears under Image Details and you are downloading IOS images, log in to Cisco.com and provide the required information. After that, you can proceed to download IOS images.

```
Error while selecting or displaying image details.  
Please log into cisco.com at  
http://www.cisco.com/cgi-bin/Software/Crypto/crypto_main.pl  
and make sure your username has acknowledged cryptography  
permissions for downloading IOS Aironet images.
```

Step 4 Click the device type; the firmware versions available on Cisco.com are displayed. Select a firmware version; the image details are displayed,



Note Images for Cisco Aironet 350 wireless bridges are listed in the Import window as Cisco Aironet 350 access point images (that is, the names begin with *AP*). To avoid confusion, you can rename these images after importing them. For more information, see [Editing Image Details on the WLSE, page 4-3](#).

Step 5 To add the image to the Selected Images list, click **Add**.

Step 6 Repeat steps 4 and 5 to add more images.

Step 7 To remove an image from the Selected Images list, click **Remove**.

Select the Overwrite Existing Images checkbox if you are importing an image version that is already stored on the WLSE. Otherwise, the image import will fail if the same version is already stored on the WLSE.

Step 8 Click **Import**. The Import Status window appears. *Do not close this window until you receive a message that either says the import was successful or the import failed.*

If the import is successful, a confirmation message appears and the image is saved on the WLSE.

If the import fails, an error message appears. The import may fail for one of the following reasons:

- The image you are trying to import is not valid. In that case, an error message appears.
- There is insufficient space on the WLSE to store images.
- You specified an image that already exists in the image library and you did not select the **Overwrite Existing Image** checkbox in Step 7.
- This is the first time you have tried to download software that has cryptographic features. You will be directed to log into Cisco.com and fill out a form to provide more information about your organization.

Step 9 Click **Refresh** to refresh the Import Status window; click **Close** to close it.

Step 10 For information on uploading firmware to access points and bridges, see [Managing Firmware Jobs, page 4-11](#).

Using a Remote TFTP Server for Updating Devices

You can download firmware images to a TFTP server and then upload them to access points and bridges. This method of uploading may be quicker than uploading from the WLSE if you have a slow link between the WLSE and the access points and bridges in your network.

To download firmware images, go to the following URL:

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

To make sure you are downloading a supported firmware release, see the list of supported devices and firmware versions at **Administration > System > Firmware Supported Versions**.

Use the normal procedure for creating firmware jobs described in [Managing Firmware Jobs, page 4-11](#). You specify the TFTP server and provide the filename in the last step, finish the job (for more information, see [5. Finish the Job—Validation, page 4-17](#)).

Viewing and Updating Supported Firmware Versions

You can view the firmware versions supported by the WLSE and import support for new versions.

Select **Administration > System > New Version Support** and **Administration > System > Firmware Supported Versions**.

For more information, see [Updating Supported Firmware Versions, page 6-111](#) and [Viewing Supported Firmware Versions, page 6-111](#).

Managing Firmware Jobs

The Jobs subtab allows you to:

- Create firmware jobs—See [Creating and Running a Firmware Job, page 4-11](#).
If you are using a firmware job to convert non-IOS access points to IOS, follow the procedures in [Converting Access Points to IOS, page 4-30](#) before creating a firmware job.
- View a list of firmware jobs—See [Checking Job Status, page 4-24](#).
- Filter the list of firmware jobs—See [Filtering Jobs, page 4-26](#).
- Edit firmware jobs—See [Editing a Job, page 4-26](#).
- Delete firmware jobs—See [Deleting a Job, page 4-27](#).
- View firmware jobs details—See [Viewing Job Run Details, page 4-28](#).

Related Topics

[Managing Firmware Images, page 4-2](#)

Creating and Running a Firmware Job



Note

After a new image is downloaded to an access point, the access point will automatically reboot.

Use the following procedure to create firmware jobs for upgrading the firmware on IOS and non-IOS access points.

Use the procedure in [Converting Access Points to IOS, page 4-30](#) to create and run a firmware job for converting an access point to IOS.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Firmware > Jobs**.
- Step 2** Enter a name for the job and click **Create Job**.
For guidelines on job names, see [Appendix A, “Naming Guidelines.”](#)
- Step 3** The window refreshes with the Job Creation menu in the left pane and the Job Name dialog box in the right pane.
- Step 4** Select the numbered choices in the left pane to create and run the firmware jobs. For information on these choices, see [Job Choices, page 4-12](#).
-

Job Choices

When you create or edit a firmware upload job, the following tasks appear in the left pane of the Jobs window. All tasks must be completed whether you are uploading images from the WLSE or from a remote TFTP server. You can omit scheduling the job and edit the job later to provide a schedule. You can complete tasks 1 through 4 in any order.

1. **Job Name**—See [1. Name the Job and Select the Protocol, page 4-13](#).
2. **Select Image**—See [2. Select the Image, page 4-14](#).
3. **Select Devices**—See [3. Select Devices, page 4-14](#).
4. **Schedule Job**—See [4. Schedule the Job, page 4-16](#).
5. **Finish**—After completing tasks 1 through 4, you validate and save the job—See [5. Finish the Job—Validation, page 4-17](#).

**Caution**

Clicking on a any subtab (for example, Jobs or Images) before you have saved your entries in the Jobs window will cause the window to reset and you will lose all the information you entered.

1. Name the Job and Select the Protocol

Procedure

Step 1 Click **Job Name**.



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Step 2 Enter the data described in [Table 4-4 on page 4-13](#).

Table 4-4 Job Name Parameters

Field	Description
Job Name	Enter a name for the job. For guidelines on naming jobs, see Appendix A, “Naming Guidelines.”
Description	Enter a description of the job. For guidelines on entering descriptions, see Appendix A, “Naming Guidelines.”
Protocol	Select the protocol to be used for the job: HTTP or SNMP. For IOS firmware upgrades and conversions from non-IOS firmware to IOS firmware, you must select SNMP. Note After a job runs once, the protocol cannot be changed. To change the protocol, make a copy of the job. For information on copying a job, see Copying a Job, page 4-28 .

- Step 3** From the menu in the left pane, go to the next step, Select Image. See [2. Select the Image, page 4-14](#).
-

2. Select the Image

Procedure

- Step 1** Click **Select Image**.
- Step 2** Expand the device folder and select the image you want to upload. The Image Detail window opens.



Note If you are converting Cisco Aironet 1200 access points from non-IOS firmware to IOS firmware, you must select a special upgrade image (for example, AP1200-Cisco-IOS-Upgrade-v1). Do not use a regular IOS image upgrade file.

If the desired image does not appear in the tree, you must import it to the WLSE unless the image is located on a remote TFTP server. For more information, see [Importing Images to the WLSE, page 4-5](#).

- Step 3** From the menu in the left pane, go to the next step, Select Devices. See [3. Select Devices, page 4-14](#).
-

3. Select Devices

Procedure

- Step 1** Click **Select Devices**. All managed devices are listed in the Device selector in the middle pane.



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Step 2 To search for devices:

- a. From the list in the search area located in the middle pane, select a method for searching:

Method	Description
Device name	Enter device name to search for any device.
IP address	Enter IP address to search for any device.
APs based on client MAC	Enter a client MAC address to search for both IOS and non-IOS access points. Finds only access points that are associated with the specified client.
APs based on client IP	Enter a client IP address to search for non-IOS access points <i>only</i> . Finds only access points that are associated with the specified client.

- b. Enter the IP address, name, or MAC address. You can use an asterisk (*) as a wildcard to denote numbers and letters; for example, *AP or 172.*.*.*
- c. Click **Search**. The matching devices appear in the Search Results folder in the device selector.

Step 3 To select devices for image upload, expand a folder that contains the devices you want to include in the job. Then click the device group folder. The group and all its devices are added to the Available Devices list.

For more information on device grouping, see [Managing Groups, page 6-56](#).

Step 4 From the Available Devices list, select a group or individual devices, then click **Add**.

- The devices you selected are moved to the Selected Devices list.



Note Device that are moved to the Selected list are removed from the Available Devices list. You can repopulate the Selected list by clicking on the group again.

- The devices in the Selected Devices list box will receive the image you selected.

Step 5 To add devices from other groups, repeat steps 3 and 4.

- Step 6** To remove devices, select them from the Selected Devices list, then click **Remove**.
- Step 7** From the menu in the left pane, go to the next step, Schedule Job. See [4. Schedule the Job, page 4-16](#).
-

Related Topics

[Managing Groups, page 6-56](#)

4. Schedule the Job

When scheduling a firmware job, you can select Run Now to start the job in 2 minutes, or you can schedule the job for a future date and time.

**Note**

You can save a job without scheduling it. You can edit the job later to add the scheduling information. To edit a job, select **Firmware > Jobs**; then select the job from the list and click **Edit Job**.

Procedure

- Step 1** Click **Schedule Job**.

**Note**

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

- Step 2** Schedule the job as follows:

- To run the job now, select the **Run Now** checkbox. The job will begin running immediately.

**Note**

Selecting this option ignores any date and time that you enter from the Start Date and Start Time lists.

- To schedule the job for a later date and time, select the month, day, and year from the Start Date lists and select the hour and minutes from the Start Time lists.
- Step 3** From the menu in the left pane, select the next task, Finish. See [5. Finish the Job—Validation, page 4-17](#).

5. Finish the Job—Validation

Before validating a job, you must name the job and select the protocol, select the image, select the devices, and schedule the job.

To validate the job, save it, and add it to the list of scheduled jobs:

Procedure

- Step 1** Click **Finish** in the left pane to complete job creation. The Finish dialog consists of the [Email settings section](#), [Remote server settings section](#), [Warnings section](#), [IOS Security Parameters section](#), and [Validate and Save section](#). The following steps describe how to complete each section.
- Step 2** **Email settings section**

If you want email notification of job completion, enter the following information in this section:

Table 4-5 *Email Notification Settings for Firmware Jobs*

Field	Description
On completion, mail to	Enter a comma-separated list of email addresses to be notified when the job completes.
Email only if job fails	Select this checkbox if you want recipients to be notified only if the job fails.



Tip If email notification is not working, you may need to set up the mail route by specifying an SMTP server. See [Configuring the Mail Route, page 6-104](#).

Step 3 Remote server settings section

If images will be uploaded to devices from a remote TFTP server (instead of being uploaded from the WLSE), enter the information described in [Table 4-6 on page 4-18](#). For information about storing images on the remote TFTP server, see [Using a Remote TFTP Server for Updating Devices, page 4-10](#).

Table 4-6 Remote TFTP Server Settings for Firmware Jobs

Field	Description
Use remote server	Select this checkbox to upload the image from a TFTP server. The remote server must have a tftp server running.
Remote server IP address	Enter the IP address of the TFTP server or select a server from the list of recently used servers. Every time you enter a remote server IP address, the address will be added to the Recently used servers list.
Recently used servers	
Remote server firmware image filename	The filename of the firmware image file on a remote server. The image file must reside in the main directory for TFTP access on the server.

Step 4 Warnings section

If warnings are detected for any devices during validation (Step 6), the job will fail for those devices unless you select the **Ignore Warnings** checkbox. If you prefer not to ignore warnings while the job runs, you can correct the warning conditions instead and then validate again.

Step 5 IOS Security Parameters section

Note This section appears only if you have chosen a special image for converting a Cisco Aironet 1200 access point from non-IOS to IOS. For the procedure to convert access points to IOS, see [Converting Access Points to IOS, page 4-30](#).

Step 6 Validate and Save section

- a. Click **Validate** to verify that the job will run successfully. If you missed one or more of the numbered steps in the left pane, error messages are displayed (for example, *Devices not Selected*). Correct these errors and click **Validate** again. The Job Validation Summary window opens. For more information on this window, see [Job Validation Summary Window Details, page 4-21](#).

**Note**

It is recommended that you always validate a job before saving it. Also, you should check the image release notes on Cisco.com for the latest caveat information on the image.

**Note**

If any fields in the Job Validation Summary window are marked *Error*, the job will fail for those devices unless you correct the error situation.

- b. Click **Save** to add the job to the list of scheduled jobs or run the job now, depending on whether you scheduled the job for a later time or chose Run Now in the scheduling screen. The screen refreshes and the Job Save Summary window shows the following information:

Table 4-7 Job Save Summary Window

Field	Description
Name	Name of the job.
Description	Job description, if any.
Image	Name of the image selected for the job.
Devices	Names of the devices selected for the job.
Groups	Names of groups selected for the job.
Schedule	Scheduled date and time for the job, or <i>No Schedule</i> if the job has not been scheduled.



Note After the image is downloaded to the device, the device will be rebooted. Non-IOS devices will be rebooted by using SNMP. IOS devices will be rebooted by using SSH. If the attempt to reboot by using SSH fails, the device will be rebooted using Telnet.

Step 7 To view the status of the job, select **Firmware > Jobs**. For more information, see [Checking Job Status, page 4-24](#).

Step 8 If a job ends with the status of “not verified,” or fails because of timeouts caused by slow network links, you can change the values of the job properties parameters in the WLSE and rerun the job.



Note A status of “not verified” does not always mean that the job has failed. The WLSE may have timed out before verifying whether the job succeeded.

To change job properties parameters that affect timeouts, access the WLSE through the following URL:

`http://your_wlse:1741/debug/jobprops.jsp`

where *your_wlse* is the name of the WLSE.

- If the job ended as “not verified” and it failed, increase the value of the **Device Reboot Wait Timeout** parameter and run the job again.
- If the job timed out and failed because the access point and WLSE are connected through a slow link (less than 1.544 Mbps, increase the value of the **Per device job operation timeout** parameter. For example, for a 56 kbps link, the recommended value is 2400 seconds (40 minutes). For a 128 kbps link, the recommended value is 1200 seconds (20 minutes). Then, run the job again. Run the job again.

Related Topics

- [Deleting a Job, page 4-27](#)
- [Checking Job Status, page 4-24](#)
- [Viewing Job Run Details, page 4-28](#)

Job Validation Summary Window Details

The Job Validation Summary window shows information on the firmware job, including errors and warnings.

Table 4-8 Job Validation Summary Window

Field	Description
Image Selected, Version, and Device Type	The image name, image version, and device type that you selected when creating the job.
Image version validation	Whether the image version is valid. This field is marked <i>Warning</i> if the image is not recognized. If the image is not recognized because it was released after the WLSE software was released, return to the Finish screen and select Ignore Warnings. For information on importing updated information on supported firmware versions and viewing information on versions supported by the WLSE, see Updating Supported Firmware Versions, page 6-111 and Viewing Supported Firmware Versions, page 6-111 .
Duration estimate	The maximum amount of time required to complete the job.
Image known bugs validation	Whether there are any major caveats for this image.

Table 4-8 Job Validation Summary Window (continued)

Field	Description
Job protocol validation	<p>Whether the job protocol (HTTP or SNMP) you selected is supported on this device.</p> <p>Note Firmware upgrade via SNMP is supported for firmware versions 11.08T and later. SNMP is required for IOS firmware upgrades and conversions from non-IOS to IOS.</p>
Device-Image validation	<p>Whether the image you selected is valid for this device. This field is marked <i>Error</i> if:</p> <ul style="list-style-type: none"> The image is not valid for the type of device you selected. An IOS device's Telnet or SSH credentials were not added to the WLSE, and the device cannot be rebooted after the upgrade. You must add the credentials before you can create the job. For information, see Enter Telnet and SSH Usernames and Passwords—IOS Access Points, page 6-11. You did not select a template for an IOS conversion job. <p>This image is marked <i>Warning</i> if:</p> <ul style="list-style-type: none"> The image is not recognized. An IOS device's Telnet or SSH username was not added to the WLSE, and the device might not reboot after the upgrade. If the access point is configured not to ask for the username during login, the job can continue if you select the Ignore Warnings option in the Finish dialog. If the access point will ask for the username, you must add it before the job will run. For information, see Enter Telnet and SSH Usernames and Passwords—IOS Access Points, page 6-11.

Comments in the Job Validation Summary fields show the status of each item:

- Passed*—No problems were found.
- Information*—No problems were found, but there is information you might want to know. For example, if the image version you selected already installed on the device.
- Warning*—The operation is permitted but may not be advisable; for example, downgrading to an earlier image.

The selected image will not be applied to devices that have warnings associated with them, unless you deal with the warnings before saving the job. Use one of the following methods to deal with the warnings:

- Edit your job choices to fix the problems that caused the warnings.
- Select the **Ignore Warnings** checkbox in the Warnings section of the Finish dialog box. By default, warnings are not ignored.



Note If you are doing a conversion from non-IOS to IOS, warnings will be issued if you have not specified all the recommended parameters. These warnings can be safely ignored.

- *Error*—The operation is not permitted. The image will not be applied to devices that have errors associated with them. It is recommended that you eliminate the errors before saving the job. If you save a job with errors, the corresponding devices will be ignored during the job run.

You will receive an error if you do not enter credentials when converting non-IOS devices to IOS.

Overview: Using Job Functions

To check job status, filter jobs, edit jobs, and view job details, select **Firmware > Jobs**.

Job data is retained for 30 days by default. To change the retention period, see [Managing System Parameters, page 6-107](#).



Note

Your login determines whether you can use the following options.

- To check the status of jobs, see [Checking Job Status, page 4-24](#).
- To filter the list of jobs, see [Filtering Jobs, page 4-26](#).
- To edit a job, see [Editing a Job, page 4-26](#).
- To delete a job, see [Deleting a Job, page 4-27](#).
- To see the details of a job, see [Viewing Job Run Details, page 4-28](#).

Related Topics

[Creating and Running a Firmware Job, page 4-11](#)

Checking Job Status**Procedure**

Step 1 Select **Firmware > Jobs**.

Step 2 From the Job State list, select the type of job whose status you want to check. The window refreshes and the jobs are displayed.

The information displayed depends on which Job State you selected: [Scheduled](#), [Unscheduled](#), [Running](#), or [All](#).

- Scheduled

Field	Description
Job Name	The job name.
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is the time the job ran.
Last Run Status	The status of the last run.

- Unscheduled

Field	Description
Job Name	The job name.
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is the time the job ran.
Last Run Status	The status of the last run.

- Running

Field	Description
Job Name	The job name.
Job Start Time	The time the job started.
Percent Complete	The percent of the job that has completed running.
Next Schedule	Firmware jobs are not recurring.

- All

Field	Description
Job Name	The job name.
Job State	The state of the job. Note A job in the DidNotStart state must be rescheduled.
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is when the job ran.
Last Run Status	The status of the job the last time it ran.

Step 3 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 4 You can do any of the following:

- Filter jobs—See [Filtering Jobs](#), page 4-26.
- Edit a job—See [Editing a Job](#), page 4-26.
- Delete a job—See [Deleting a Job](#), page 4-27.
- Copy a job—See [Table 4-8 on page 4-28](#).
- View job run details—See [Viewing Job Run Details](#), page 4-28.

Step 5 To refresh the screen, click **Refresh**.

Related Topics

[Overview: Using Job Functions, page 4-23](#)

Filtering Jobs

Use this option to display a limited set of jobs, making it easier to search for a particular job by name.

Procedure

Step 1 Select **Firmware > Jobs**.

Step 2 Click **Filter Job**.

Step 3 Enter the name, or part of the name. You can use % as a wildcard: for example, entering %name% displays all the jobs that contain the word “name.”

Step 4 Click **Apply filter**. The Job window refreshes and the matching jobs are displayed in the Jobs list.



Note The filter remains in effect until the page is refreshed.

Related Topics

[Overview: Using Job Functions, page 4-23](#)

Editing a Job

Use this option to edit jobs from the displayed list of jobs.



Note If you have deleted the image that was associated with the job you are editing, the job will show that no image has been selected.

Procedure

- Step 1** Select **Firmware > Jobs**.
 - Step 2** From the list of jobs, select the job that you want to edit.
 - Step 3** Click **Edit Job**.
 - Step 4** Select choices in the Job Creation Menu. For descriptions of the choices, see [Job Choices, page 4-12](#).
-

Related Topics

[Overview: Using Job Functions, page 4-23](#)

Deleting a Job

Use this option to delete jobs from the displayed list of jobs. Jobs that are scheduled, unscheduled, completed, or did not start can be deleted. Jobs that are running cannot be deleted.

Procedure

- Step 1** Select **Firmware > Jobs**.
 - Step 2** From the list of jobs, select the job that you want to delete.
 - Step 3** Click **Delete Job**.
 - Step 4** Click **OK** in the popup windows.
-

Related Topics

[Overview: Using Job Functions, page 4-23](#)

Copying a Job

Use this option to copy a job. You can use this option to change the protocol in a job that has already run.



Note

If you have deleted the image associated with the job that you want to copy, the job will show that no image has been selected.

Procedure

- Step 1** Select **Firmware > Jobs**.
- Step 2** From the list of jobs, select the job that you want to copy.
- Step 3** Click **Copy Job**.
- Step 4** Click **OK** in the popup window.

Related Topics

[Overview: Using Job Functions, page 4-23](#)

Viewing Job Run Details

Use this option to view details about a job.

Procedure

- Step 1** Select **Firmware > Jobs**.
- Step 2** From the All Jobs table displayed in the **Firmware > Jobs** window, select a job, then click **Job Run Detail**.
- Step 3** The details window shows the following:

Field	Description
Select Run	Select a job to see its details.
Job Start Time	The time the job started.

Field	Description
Job End Time	The time the job ended.
Job Status	The status of the job.
Percent Complete	The percent of the job that completed.

- Step 4** To view details for a particular job run, select the job, click **Show Run Details**. For more information on this table, see [Job Run Details Table, page 4-29](#).
- Step 5** To view the job run log, click **Job Run Log**. A window displays all the details for the selected job number.
- Step 6** To refresh the table, click **Refresh**.

Related Topics

[Overview: Using Job Functions, page 4-23](#)

Job Run Details Table

The Job Runs Details table displays the following information:

Field	Description
Device Name	The name of the device.
Start Time	The time the job started.
End Time	The time the job ended.
Status	The status of the job.

To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Related Topics

[Overview: Using Job Functions, page 4-23](#)

Converting Access Points to IOS



Caution

After you convert a non-IOS access point to IOS, you cannot reverse the process. The access point cannot be converted back to non-IOS firmware.

The Cisco Aironet 1200 access points to be converted must be running 11.54T, 11.56, 12.01T1, or 12.02T1 non-IOS (VxWorks) firmware.

Conversion from non-IOS to IOS firmware requires a special upgrade image (for example, AP1200-Cisco-IOS-Upgrade-v1). Do not use a regular IOS image upgrade file. For more information on managing firmware images on the WLSE, see [Managing Firmware Images, page 4-2](#).

The major tasks in the conversion process are:

Table 4-9 Major Tasks for Converting an Access Point to IOS

Task	Reference
1 Configure the access points to be converted.	1. Configure Access Points To Be Converted, page 4-31.
2 Configure the WLSE by downloading the special conversion image and entering the community string for each access point to be converted.	2. Configure the WLSE for IOS Conversions, page 4-32.
3 Create a template for the conversion.	3. Create a Conversion Template, page 4-33.
4 Create and schedule the conversion job.	4. Create and Run the Conversion Job, page 4-35.

1. Configure Access Points To Be Converted

For each non-IOS access point to be converted, make sure the access point is configured properly for conversion:

Procedure

Step 1 After an image is uploaded to an access point, the access point is rebooted. If you are using [DHCP](#) to assign IP addresses to the access points to be converted, make sure that the IP addresses do not expire during the time required to run the firmware job and reboot the access points.

You can set the DHCP lease period accordingly or use the DHCP reservation feature. The WLSE firmware module provides IP and MAC addresses for the reservation feature.

An estimate of the time required to complete a firmware job is displayed during the job validation phase of job creation—see [4. Create and Run the Conversion Job, page 4-35](#).

Step 2 Log in to each access point and set the following:

a. Under **Setup > FTP Settings**:

- Set the File Transfer Protocol to TFTP.
- Set the Default File Server to the WLSE's IP address.

b. Under **Setup > Express Setup**, set the SNMP admin community string.

This creates a user under **Setup > Security > User Information** whose username is the community string.

You will need this community string for the next task, [2. Configure the WLSE for IOS Conversions, page 4-32](#).

c. Select the user created in Step 2b. Under Capability Settings, select **Firmware**.

After you have configured the access points, configure the WLSE. See [2. Configure the WLSE for IOS Conversions, page 4-32](#).

2. Configure the WLSE for IOS Conversions

On the WLSE, import the image and make sure access point community strings are entered:

Procedure

-
- Step 1** Locate the special conversion image on Cisco.com at the following URL:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
 Conversion images have names similar to AP1200-Cisco-IOS-Upgrade-v1.
- Step 2** Import the image by first downloading it to the desktop.



Note You cannot import conversion images directly from Cisco.com.

- To import the image, select **Administration > Firmware > Images > Import > From Desktop**. For more information about downloading and importing firmware, see [Importing Images to the WLSE, page 4-5](#).



Note Make sure the Version field is *set to 12.2*. Otherwise, the image will be incompatible with the Cisco Aironet 1200 access points that you are converting.

- If you are using a remote TFTP server for the conversion job (recommended if you have a slow link between the WLSE and the access points), download the image to the TFTP server.

- Step 3** Select **Administration > Discover > Device Credentials > SNMP Communities**.

Make sure the community strings for all access points to be converted are entered into the SNMP Communities table. These are the community strings you entered in [1. Configure Access Points To Be Converted, page 4-31](#).

For more information on entering community strings on the WLSE, see [Enter SNMP Community Strings for All Devices, page 6-7](#).

Next, create a conversion template on the WLSE; see [3. Create a Conversion Template, page 4-33](#).

3. Create a Conversion Template

Create a *non-IOS* template that contains the security parameters for the level of security that you require.

It is necessary to set these security parameters because the parameters set on the access point might have write-only permissions. During the firmware conversion job, write-only parameters cannot be extracted from the access point. Therefore, such parameters must be re-entered by applying a template so they are set on the access point after the conversion.

All other parameters that are set on the access points will retain their values after conversion. If you set parameters in the conversion template in addition to those described in the following procedure, the extra parameters will be ignored.

To create the conversion template.

Procedure

- Step 1** Select **Configure > Templates**.
- Step 2** Select **non-IOS**.
- Step 3** Enter a unique name. See [Naming Guidelines, page A-1](#) for details.
- Step 4** Click **Create New**.
- Step 5** From the left pane, select **Security > Local Admin Access > Add Users** and set the following parameters.



Caution

You must set the following three parameters in the template. Otherwise, the conversion will fail and you will have to log in to each access point and configure it manually.

- a. Enter a User Identifier (any integer, not 0). If you want to set the same user name on all the access points to be converted and do not know which user identifiers are already in use, enter a very high value (such as 2000).

- b. Enter the User Name. After conversion, this username will be the Telnet user name and the read/write community string on the access points. These credentials are necessary for the WLSE to communicate with the access points.



Note This user name must be the same as the community string you entered on the WLSE in [2. Configure the WLSE for IOS Conversions, page 4-32](#).

- c. Enter a password. After conversion, this password will be the Telnet user password on the access points.

Step 6 Using the choices in the left pane, set the necessary parameters from [Table 4-10 on page 4-34](#). The parameters you set depend on the level of security that you need on your access points.



Note When you validate the conversion job, any parameters listed in the table that are not set in the template will cause informational messages. These messages will not prevent the firmware jobs from running successfully.

Table 4-10 Other Conversion Template Settings

Template Choice	Setting
Association > VLANs	<ul style="list-style-type: none"> Enter WEP Key 1 through WEP Key 4. Select the size of each WEP key.
11a Radio > Data Encryption	<ul style="list-style-type: none"> Enter Encryption Key 1 through Encryption Key 4. Select the Transmit Key. Select the Key Size for each encryption key.
Security > Local AP/Client Security	<ul style="list-style-type: none"> Enter Encryption Key 1 through Encryption Key 4. Select the Transmit Key. Select the Key Size for each encryption key.

Table 4-10 Other Conversion Template Settings (continued)

Template Choice	Setting
Security > Authentication Server	<ul style="list-style-type: none"> • Enter server name or IP address. • Select Server Type. • Enter Port, Share Secret, Retran Int, Max Retran. • Specify EAP Auth, MAC Auth, User Auth, and MIP Auth.

Step 7 Select **Preview** to see your changes before you apply them.

Step 8 Select **Finish** to save the template.

For more information about configuration templates, see [Using the Templates, page 3-1](#).

After you create the template, you can create and run the firmware job; see [4. Create and Run the Conversion Job, page 4-35](#).

4. Create and Run the Conversion Job

For more details on the steps in this procedure, see the complete descriptions in [Job Choices, page 4-12](#).

To create, validate, and run the conversion job:

Step 1 Select **Firmware > Jobs**.

Step 2 Enter a name for the job and an optional description. Select **SNMP**.

Step 3 Click **Select Image**. Expand the device folder and select the special conversion image.

Step 4 Click **Select Devices**.

a. Expand the folder that contains the access points to be converted.

b. From the Available Devices list, select a group or individual devices and click **Add**.

Step 5 Click **Schedule Job**.

- To run the job right after you finish the job creation process, select **Run Now**.
- To schedule the job for later, select the date and time.

Step 6 Click **Finish**. To specify job options and validate all job choices:

- (Optional) In the Email settings section, you can specify email notification upon completion of the job.
- Complete the Remote server settings section if you are uploading the image from a remote TFTP server instead of from the WLSE.
- In the Warnings section, select **Ignore Warnings**. Otherwise, any warnings will cause the job to fail.
- In the IOS Security Parameters section, enter the enable password and select the conversion template from the Select Config Template list.



Note

This section appears only if you selected a valid conversion image in [Step 3](#). If it does not appear, return to Select Image and select the correct image.

- In the Validate and Save section, click **Validate**. You should always validate jobs before saving them.
 - If any fields are marked *Error*, the job will fail. You must correct error situations before saving the job.
 - If any fields are marked *Warning* and you did not select **Ignore Warnings** in [Step 6](#), the job will fail. You must select **Ignore Warnings** before saving the job.
 - Informational messages can be ignored.

For a detailed description of the Job Validation Summary window, see [Job Validation Summary Window Details, page 4-21](#).

- Click **Save** to run the job or add it to the list of scheduled jobs.

Step 7 To check the job status, select **Firmware > Jobs**. If a conversion job fails, the status shown will be “not verified.”

Step 8 If the job status is “not verified”:

- First, *check the access points* to find out if they have been converted to IOS.
- If they have not been converted, run the job again.

- If they have been converted, *do not run the job again*.

Step 9 If the job status is “failed,” you can increase the value of the **Vxworks to IOS** time out parameter and run the job again.

To change this parameter, access the WLSE through the following URL:

http://your_wlse:1741/debug/jobprops.jsp

where *your_wlse* is the name of the WLSE.

Step 10 After the job finishes:

- All access points in the job will be rebooted.
 - An inventory will run and the access points will be in the managed state.
 - Cisco Aironet 1200 access points that were converted will be removed from the AP 1200 group and placed in the AP 1210 group.
-

