



# Updating Device Firmware

You can use the WLSE to upgrade the firmware on one or more access points, either as a scheduled operation or on demand. The firmware options on the WLSE are:

- Upgrading IOS and non-IOS access points.
- Converting non-IOS access points to IOS.
- Displaying firmware versions supported by the WLSE and updating the firmware versions support on the WLSE.

The topics in this section are:

Topic	Reference
Overview	<a href="#">About Firmware Upgrades, page 5-2</a>
Managing normal firmware upgrades:	
<ul style="list-style-type: none"> <li>• Downloading images to the WLSE or a remote TFTP server</li> </ul>	<a href="#">Managing Firmware Images, page 5-5</a>
<ul style="list-style-type: none"> <li>• Running firmware jobs</li> </ul>	<a href="#">Managing Firmware Jobs, page 5-14</a>
Converting Cisco Aironet 1200 and Aironet 350 access points from non-IOS to IOS firmware	<a href="#">Converting Access Points to IOS, page 5-35</a>
Viewing and updating the WLSE's firmware support data	<a href="#">Viewing and Updating Firmware Versions that the WLSE Supports, page 5-14</a>

**Note**

One or both of the firmware subtabs may not be visible to some users. Your login determines whether you can view and use WLSE options.

## About Firmware Upgrades

The topics covered in this section are:

- [How Firmware Upgrades Work, page 5-2](#)
- [Recommendations For Running Firmware Upgrades, page 5-3](#)

For overview information on converting non-IOS access points to IOS, see [Converting Access Points to IOS, page 5-35](#)

## How Firmware Upgrades Work

To use the firmware upgrade feature, you must:

1. Download the firmware image to the WLSE and import it to the WLSE or import the image directly from Cisco.com. You can also download images to a remote TFTP server.
2. Configure the upgrade job.
3. Schedule the upgrade job or run it immediately.

Usually when a firmware job runs, the WLSE instructs each access point in the upgrade job to download the new firmware from the WLSE. You may want to initiate a TFTP download from a server other than the WLSE if your access points are locally remotely.

After an access point downloads new firmware, it reboots. The WLSE tries to contact the access point periodically after the reboot until it verifies that the device has resumed normal operation. The WLSE assumes the upgrade is successful if the access point reboots successfully.

The WLSE usually initiates the download and reboot by using an SNMP set operation. For older non-IOS APs that do not support such SNMP operations, you can use HTTP to initiate the download. In that case, each access point in the job must have the WLSE configured as the TFTP server. It is recommended that you migrate to newer access point firmware and use SNMP instead of HTTP.

## Recommendations For Running Firmware Upgrades

The topics in this section concern the number of devices to include in firmware jobs and the amount of time it takes to run a job:

- [Number of Devices in a Job, page 5-3](#)
- [How Much Time to Allocate, page 5-3](#)
- [Calculating the Estimated Time, page 5-4](#)

### Number of Devices in a Job

Because the WLSE firmware upgrade feature is multi-threaded with up to 20 allotted threads, it can upgrade as many as twenty access points simultaneously. For example, a firmware upgrade job with 100 devices will begin by upgrading twenty devices, one thread per device. When a device upgrade completes, its thread will start on a new device immediately, even if the other firmware upgrade tasks are in progress.

### How Much Time to Allocate

When calculating the amount of time it takes to upgrade an access point, the factors to consider are:

- How long does it take to download the firmware via TFTP?

The TFTP download is dependent on network performance. If you have high latency issues or a congested network, allow extra time for the download.

- How long does it take for the access point to reboot and load the new firmware?

The amount of time to reboot and load new firmware is usually constant. However, if the access point uses DHCP to get an IP address or retrieve a configuration file when it comes up after a reboot, this time is also affected by network performance.

Here are some other factors that might influence firmware upgrade times:

- In some cases, you may need to change the WLSE firmware upgrade timeout setting to get accurate upgrade job status (see [Firmware jobs over slow links do not succeed.](#), page 10-28). The default setting is usually adequate, but in cases where there are congested and high latency links, the timeout usually needs to be increased.
- If you have access points deployed remotely, consider using the TFTP staging server option, especially if the remote site is at the other end of a slow WAN link or behind a firewall. When you configure the WLSE upgrade job, you select the remote TFTP server option and input the remote TFTP server address.

## Calculating the Estimated Time

Suppose a WLAN administrator plans to upgrade 200 AP1100 access points. After preliminary testing, it is determined that it takes approximately 5 minutes over a 100 Mbps Ethernet network to upgrade one access point. In this example, 100 Mbps is the slowest connection that the upgrade process will need to traverse and because the upgrade will be done late at night, network congestion will probably not cause delays in the upgrade. Therefore, a rough estimate of the amount of time needed for the upgrade might be:

$$(200 \text{ APs} / 20 \text{ threads}) * 5 \text{ minutes per AP} = 50 \text{ minutes}$$

Consider adding a safety factor into the equation. In this example, the WLAN administrator might want to add an additional 45 minutes, in case one device rejects the new firmware and a separate upgrade needs to be started after the first upgrade job completes.

The estimated change window formula can be calculated as follows:

$$T = (n / 20) * t + s$$

where:

- T is the total time for the change window
- n is the number of devices in the upgrade job
- t is the estimated time to upgrade a single device
- s is the safety factor.

In this formula, T is often a constant defined by IT policies. For example, many campuses allow for a change window of no more than two hours. If you determine that it will take more than T to upgrade the access points, plan the upgrades in phases, each of which can be completed well within the change window. It is always a good idea to plan upgrades conservatively. One conservative way to use this formula is to use the firmware upgrade timeout setting as your value for t.

## Managing Firmware Images

The options under the Images subtab allow you to:

- View images downloaded to the WLSE—See [Viewing Images Downloaded to the WLSE, page 5-6](#).
- Edit images on the WLSE—See [Editing Image Details on the WLSE, page 5-6](#).
- Delete images from the WLSE—See [Deleting Images from the WLSE, page 5-8](#).
- Download images to the WLSE—See [Importing Images to the WLSE, page 5-8](#).
- 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 5-13](#).

### Related Topics

- [Managing Firmware Jobs, page 5-14](#)
- [Converting Access Points to IOS, page 5-35](#)
- [About Firmware Upgrades, page 5-2](#)

## Viewing Images Downloaded to 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 5-6](#)

## 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 as described in [Table 5-1 on page 5-7](#).

**Table 5-1** 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>
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><b>Note</b> 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"> <li>• Official format—12.2(4)JA1</li> <li>• Cisco.com format—12.2.4-JA1</li> </ul>
Size	Size of the image (read-only field).
Description	This field is blank by default.

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

Click **Reset** to cancel your edits.

#### Related Topics

- [Deleting Images from the WLSE, page 5-8](#)
- [Viewing and Updating Firmware Versions that the WLSE Supports, page 5-14](#)

## 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 and deleted from the WLSE.
- 

### Related Topics

- [Viewing Images Downloaded to the WLSE, page 5-6](#)
- [Editing Image Details on the WLSE, page 5-6](#)

## 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 5-9](#).
- Download images to the WLSE directly from Cisco.com—see [Importing Images Directly from Cisco.com to the WLSE, page 5-11](#).

### Related Topics

- [Viewing Images Downloaded to the WLSE, page 5-6](#)
- [Editing Image Details on the WLSE, page 5-6](#)

## 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>
- You can also locate images on Cisco.com by selecting **Products and Services > Network Management Cisco Works > Wireless LAN Solution Engine > Software Center**.



---

**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**.

- Step 2** Select **Firmware > Images > Import > From Desktop**. Enter information as described in [Table 5-2 on page 5-10](#).

Table 5-2 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><b>Note</b> 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"> <li>• Official format—12.2(4)JA1</li> <li>• Cisco.com format—12.2.4-JA1</li> </ul> <p><b>Note</b> If you are importing an image to convert non-IOS access points to IOS, see <a href="#">Converting Access Points to IOS, page 5-35</a> for information about the images for conversion and how to enter the version.</p>
File Location	<p>Enter the path to the image on the desktop or click <b>Browse</b>.</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 <a href="#">Editing Image Details on the WLSE, page 5-6</a>.</p>
Overwrite Existing Image	<p>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.</p>

**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 5-14](#).

## 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.



### Note

The special images for converting non-IOS access points to IOS are not available for import directly from CCO to the WLSE. Use the special conversion procedures in [Converting Access Points to IOS, page 5-35](#).

### Procedure

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

**Table 5-3** *Cisco.com Import Window*

Field	Description
Cisco.com Username	Your Cisco.com username.
Cisco.com Password	Your Cisco.com password
Proxy IP/Hostname <sup>1</sup>	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	

Table 5-3 Cisco.com Import Window (continued)

Field	Description
Proxy Username	The username and password for contacting the proxy server (if required on your network).
Proxy Password	

- 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 5-9](#)).

**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.
```

- If a “connectivity failed” message appears, make sure that domain name service (DNS) is configured on the WLSE and DNS can resolve the cisco.com domain name.

**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 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 5-6](#).

**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 **Overwrite Existing Images** 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 **Overwrite Existing Image** 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 5-14](#).

---

## 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 from Cisco.com:

- Go to the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

- Navigate to the images by selecting **Products and Services > Network Management CiscoWorks > Wireless LAN Solution Engine > Software Center**.

The image file must reside in the main directory for TFTP access on the server (usually the /tftpboot directory).

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 5-14](#). You specify the TFTP server and provide the filename when you specify job options (for more information, see [5. Set Options, page 5-20](#)).

## Viewing and Updating Firmware Versions that the WLSE Supports

You can:

- Import support for new versions by selecting **Administration > System > New Version Support**. See [Updating Supported Firmware Versions, page 8-38](#).
- View version support by selecting **Administration > System > Firmware Supported Versions**. See [Viewing Supported Firmware Versions, page 8-39](#).

## Managing Firmware Jobs

The Jobs subtab allows you to:

- Create firmware jobs—See [Creating and Running a Firmware Job, page 5-15](#).  
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 5-35](#) before creating a firmware job.
- View a list of firmware jobs—See [Viewing Job Status Information, page 5-28](#).

- Filter the list of firmware jobs—See [Filtering Jobs](#), page 5-30.
- Edit firmware jobs—See [Editing a Job](#), page 5-31.
- Copy firmware jobs—see [Copying a Job](#), page 5-32.
- Delete firmware jobs—See [Deleting a Job](#), page 5-31.
- View firmware jobs details—See [Viewing Job Run Details](#), page 5-32.

### Related Topics

[Managing Firmware Images](#), page 5-5

## 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 routine upgrades of the firmware on IOS and non-IOS access points.

Use the procedure in [Converting Access Points to IOS](#), page 5-35 to convert access points 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**.



---

**Note** Each job name (configuration, firmware, or AP radio scan) must be unique.

---

For other 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 a firmware job. For information on these choices, see [Job Creation Tasks, page 5-16](#).
- 

## Job Creation Tasks

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 5 in any order.

It is recommended that you download the latest version support file before beginning a firmware job. If the image is not recognized; however, you can still proceed by ignoring the warnings that are displayed in Step 6, Save the Job. For information about versions currently supported by the WLSE and downloading the support file to update the supported versions, see [Firmware Version Support, page 8-37](#).

1. **Job Name**—See [1. Name the Job and Select the Protocol, page 5-17](#).
2. **Select Image**—See [2. Select the Image, page 5-18](#).
3. **Select Devices**—See [3. Select Devices, page 5-18](#).
4. **Schedule Job**—See [4. Schedule the Job, page 5-19](#).
5. **Options**—See [5. Set Options, page 5-20](#).
6. **Save the Job and Finish**—After completing tasks 1 through 5, you can save the job. After you save the job, it will run if it is an immediate job. If it is scheduled for a later time, it will be added to the schedule of jobs—See [6. Save the Job and Finish, page 5-22](#).



### 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



**Note** Each job name (configuration, firmware, or AP radio scan) must be unique.

### Procedure

**Step 1** Select **JOB NAME** from the left 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** Enter the data described in [Table 5-4 on page 5-17](#).

**Table 5-4 Job Name Parameters**

Field	Description
Job Name	Enter a name for the job. For guidelines on naming jobs, see <a href="#">Appendix A, “Naming Guidelines.”</a>
Description	Enter a description of the job. For guidelines on entering descriptions, see <a href="#">Appendix A, “Naming Guidelines.”</a>
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.  <b>Note</b> After a job runs once, the protocol cannot be changed. To change the protocol, make a copy of the job and select a different protocol. For information on copying a job, see <a href="#">Copying a Job, page 5-32</a> .

**Step 3** Go to the next step, Select Image. See [2. Select the Image, page 5-18](#).

## 2. Select the Image

### Procedure

---

- Step 1** Select **SELECT IMAGE** from the left pane.
- 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 5-8](#).

- Step 3** From the menu in the left pane, go to the next step, Select Devices. See [3. Select Devices, page 5-18](#).
- 

## 3. Select Devices

### Procedure

---

- Step 1** Select **SELECT DEVICES** from the left pane. 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** Select devices from the device selector or use Search. For information on using the device selector or search, see [Using the Device Selector and Search, page 1-9](#).

**Step 3** Expand the folder for the group that contains the devices you want to include in the job. Then click the 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 3-97](#).

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

- 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 <<.

**Step 7** Go to the next step, Schedule Job. See [4. Schedule the Job, page 5-19](#).

---

#### Related Topics

[Managing Groups, page 3-97](#)

## 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** Select **SCHEDULE JOB** from the left pane.



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

---

**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** Go to the next task, Set Options. See [5. Set Options, page 5-20](#).

---

## 5. Set Options

In this task, you can select email notification (optional) and specify the remote server (if you are uploading the image from a remote TFTP server instead of uploading from the WLSE).

### Procedure

---

**Step 1** Select **OPTIONS** in the left pane.

**Step 2** **Email settings**

If you want to be notified by email when the job finishes, enter the following information in this section.

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

Field	Description
<b>On completion, mail to</b>	Enter a comma-separated list of email addresses to be notified when the job completes.
<b>Email only if job fails</b>	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 8-35](#).

**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 5-6 on page 5-21](#). For information about storing images on the remote TFTP server, see [Using a Remote TFTP Server for Updating Devices, page 5-13](#).

**Table 5-6 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 (usually the /tftpboot directory).

**Step 4** Go to the last task, [6. Save the Job and Finish, page 5-22](#).

## 6. Save the Job and Finish

### Procedure

---

**Step 1** Select **SAVE** from the left pane.

The Save window shows information about the job and the results of the validation tests that the WLSE runs on all firmware jobs. The window may contain warnings or errors:

- A warning usually indicates one of the following problems. You can go back and edit your job choices or choose to proceed in spite of warnings.
  - The action is not advisable; for example, you are downgrading the image version on the devices.
  - You selected an image version that is unknown to the WLSE.

For information about versions currently supported by the WLSE or updating the versions supported by the WLSE, see [Firmware Version Support, page 8-37](#).

- Errors indicate that the job will always fail for those devices.




---

**Note** For more information about the messages in the Save window, see [About the Save Window, page 5-25](#).

---

**Step 2** Click **Save**.

- If there are no errors or warnings, the job runs or is scheduled and the Job Summary window appears. Go to Step 3 for more information.
- If there are uncorrected errors or warnings, the Save Confirmation window appears. Proceed as follows:




---

**Note** To remove all of your settings for the job, click **Clear**.

---

– **If there are only warnings:**

Desired Action	Steps
Apply image to all devices, including those with warnings.	Click <b>Yes</b> . The Job Summary window appears.
Skip devices with warnings and only apply image to devices without warnings.	Click <b>No</b> . The Job Summary window appears.
Correct warnings before proceeding.	<ol style="list-style-type: none"> <li>1. Click <b>Cancel</b>. The Save window appears.</li> <li>2. Return to job choices, make corrections, and save job again.</li> </ol>

– **If there are warnings and errors:**

Desired Action	Steps
Skip devices with errors. Apply image to all other devices, including those with warnings.	Click <b>Yes</b> . The Job Summary window appears. <b>Note</b> Image will <i>not</i> be applied to devices with errors.
Skip devices with warnings or errors. Apply image to all other devices.	Click <b>No</b> . The Job Summary window appears. <b>Note</b> Image will <i>not</i> be applied to devices with errors.
Correct warnings or errors before proceeding.	<ol style="list-style-type: none"> <li>1. Click <b>Cancel</b>. The Save window appears.</li> <li>2. Return to the job choices, make corrections, and save the job again.</li> </ol>

– **If there are only errors:**

Desired Action	Steps
Skip devices with errors. Apply image to all other devices.	Click <b>OK</b> . The Job Summary window appears. <b>Note</b> Image will <i>not</i> be applied to devices with errors.
Correct errors before proceeding.	<ol style="list-style-type: none"> <li>1. Click <b>Cancel</b>. The Save window appears.</li> <li>2. Return to job choices, make corrections, and save job again.</li> </ol>

- Step 3** When the job is ready to run, the Job Summary window displays the following information and the main Jobs window appears. All new jobs are added to the list of jobs, and immediate jobs start running. For more information about the main Jobs window, see [Viewing Job Status Information, page 5-28](#).

**Table 5-7 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.

- Step 4** 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 5** For information about job status, see [Viewing Job Status Information, page 5-28](#).

To view the status of jobs at any time, select **Firmware > Jobs**.

#### Related Topics

- [Deleting a Job, page 5-31](#)
- [Viewing Job Status Information, page 5-28](#)
- [Viewing Job Run Details, page 5-32](#)

## About the Save Window

The Save window shows information on the firmware job, including errors and warnings. Messages indicate whether the job has passed the validation tests. For the meaning of the messages, see [Table 5-9 on page 5-26](#).

**Table 5-8 Save Window**

Information type	Description
Image selected, Version, and Device type	Image name, image version, and device type that you selected when creating the job.  Usage notes about this image version may also appear.
Duration estimate	Maximum amount of time required to complete the job is indicated by the following message:  <i>This job can take as long as xx minutes to complete.</i>
Image version validation	Whether the image version is valid for the selected device type. This field is marked <i>Warning</i> if the image is not recognized.  For information on importing updated information on supported firmware versions and viewing information on versions supported by the WLSE, see <a href="#">Updating Supported Firmware Versions, page 8-38</a> and <a href="#">Viewing Supported Firmware Versions, page 8-39</a> .
Image known bugs validation	Any major caveats for this image.
Job protocol validation	Whether the selected job protocol (HTTP or SNMP) is valid for this device.  <b>Note</b> 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.
Device-Image validation	Whether the selected image is valid for this device: <ul style="list-style-type: none"> <li>• <i>Error</i> if the image is not valid for the selected device type.</li> <li>• <i>Warning</i> if the image is not recognized by the WLSE.</li> <li>• <i>Information</i> if the same image is already installed on the devices.</li> </ul>

Messages in the Save window show the status of each item that is tested by the job validation process:

**Table 5-9 Messages in the Save Window**

Message Type	Description and Solution
<i>Passed</i>	No problems were found.
<i>Information</i>	No problems were found, but there is information you might want to know. For example, the image version you selected is already installed on the device.
<i>Warning</i>	<p>The operation is permitted but may not be advisable; for example, downgrading to an earlier image.</p> <p>The image will not be applied to devices that have warnings, unless you choose to ignore warnings. A popup window will be displayed after you click <b>Save</b> in this window and you can decide whether to ignore warnings.</p> <p>The warning messages are:</p> <ul style="list-style-type: none"> <li>• Device is running a software version that is not currently supported by WLSE—The WLSE does not recognize this software version. You can click <b>Yes</b> when prompted to ignore warnings.</li> <li>• Selected image version has an older version the one currently existing on the device—You are attempting to downgrade the device firmware. You can click <b>Yes</b> when prompted to ignore warnings.</li> <li>• Selected firmware image version is the same as the image running on the device—You can click <b>Yes</b> when prompted to ignore warnings.</li> </ul>

Table 5-9 Messages in the Save Window (continued)

Message Type	Description and Solution
<i>Error</i>	<p>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.</p> <ul style="list-style-type: none"> <li>• Selected image may not valid for device type—The image is not valid for the type of device you selected; for example, you are trying to apply an AP1100 image to an AP350. Remove this device from the job or verify that the image was imported as the appropriate device type.</li> <li>• Select image may not be valid for device type, not supported—Firmware upgrade is not supported for this type of device; for example, the device is a switch. Remove the device from the job.</li> <li>• SNMP/HTTP protocol not supported for firmware upload on device—Remove the device from the job.</li> <li>• Telnet/SSH credentials are not provided to reboot this device during upgrade, please add them to WLSE before creating the job—An IOS device’s Telnet or SSH credentials were not added to the WLSE; therefore, the device cannot be rebooted after the upgrade. You must add the credentials under <b>Devices &gt; Discover &gt; Device Credentials</b> before you can upgrade this device. For more information, see <a href="#">Enter Telnet and SSH Usernames and Passwords—IOS Access Points, page 3-33</a>.</li> </ul>

## Using the Functions in the Main Jobs Window

To check job status, view job details, filter the job list, edit jobs, copy jobs, or delete jobs, select **Firmware > Jobs**. The main jobs window appears.

Job data is retained for 30 days by default. To change the retention period, see [Managing Polling Parameters, page 3-87](#).



### Note

Your login determines whether you can use the following options.

- To check the status of jobs, see [Viewing Job Status Information, page 5-28](#).
- To filter the list of jobs, see [Filtering Jobs, page 5-30](#).
- To edit a job, see [Editing a Job, page 5-31](#).
- To delete a job, see [Deleting a Job, page 5-31](#).
- To see the details of a job, see [Viewing Job Run Details, page 5-32](#).

### Related Topics

[Creating and Running a Firmware Job, page 5-15](#)

## Viewing Job Status Information

For information about specific job states, see [Job Status Information and Job Run Log Messages, page 5-33](#).

### 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. <b>Note</b> 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** The following options are provided:
- Filter jobs—See [Filtering Jobs, page 5-30](#).
  - Edit a job—See [Editing a Job, page 5-31](#).
  - Delete a job—See [Deleting a Job, page 5-31](#).
  - Copy a job—See [Table 5-9 on page 5-32](#).
  - View job run details—See [Viewing Job Run Details, page 5-32](#).
- Step 5** To refresh the screen, click **Refresh**.
- 

### Related Topics

[Using the Functions in the Main Jobs Window, page 5-27](#)

## 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

[Using the Functions in the Main Jobs Window, page 5-27](#)

## 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 Creation Tasks, page 5-16](#).
- 

### Related Topics

[Using the Functions in the Main Jobs Window, page 5-27](#)

## 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

[Using the Functions in the Main Jobs Window, page 5-27](#)

## 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 Enter a name for the job in the popup window. The copy will be unscheduled. To schedule it, select the job and click Edit Job.

### Related Topics

[Using the Functions in the Main Jobs Window, page 5-27](#)

## 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.
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 and click **Show Run Details**.

**Step 5** To view the job run log, click **Job Run Log**. A window displays all the details for the selected job number. For information on the messages in the job run log, see [Job Status Information and Job Run Log Messages, page 5-33](#).

**Step 6** To refresh the table, click **Refresh**.

#### Related Topics

[Using the Functions in the Main Jobs Window, page 5-27](#)

## Job Status Information and Job Run Log Messages

This section provides information about:

- [Job Status “Not Verified”, page 5-33](#)
- [Job Run Log Messages, page 5-34](#)

### Job Status “Not Verified”

If a job ends with the status “not verified,” or fails because of timeouts caused by slow 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 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 the job failed, increase the value of the **Device Reboot Wait Timeout** parameter and run the job again.
- If the job is timing out and failing because the access point and WLSE are connected through a slow link (less than 1.544 Mbps), first 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.

## Job Run Log Messages

For a normal, successful firmware upgrade, the job run log contains messages similar to the following:

```
Device: 110.80.cisco.com Initiating firmware upgrade.
Device: 110.80.cisco.com Uploading new firmware image, please wait.
Device:110.80.cisco.com Upload completed, proceeding to reboot
AccessPoint.
Device: 110.80.cisco.com Waiting for firmware update confirmation.
Device: 110.80.cisco.com Attempting to confirm version installed.
Device: 110.80.cisco.com Actual version is 12.2(11)JA1, expected
version is 1.2.211-JA1.
Device: 110.80.cisco.com Firmware update completed successfully.
```

The following error messages may appear in the job run log.

**Table 5-10 Error Messages—Firmware Job Run Log**

Message	Meaning
SNMP error while initiating firmware upgrade. SNMP write community string was not provided or is incorrect.	The job failed. Enter the correct write community string in <b>Devices &gt; Device Credentials</b> . For more information about the required community strings, see <a href="#">Setting Up Devices, page 3-5</a> .
SNMP error while confirming version for <code>access_point</code> . Device could have been rebooting. See the documentation on how to increase the Job Timeout Properties.	The job may or may not have failed. See job status. Also, see the job timeout information in <a href="#">Job Status “Not Verified”, page 5-33</a> .

# 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.

**Caution**

The conversion job might fail if the non-IOS access point does not have at least 4 MB (DRAM) of free space. To check the free space in the device, use the CLI command `vxdiag_memshow`. You can free up space by temporarily removing the 11a radio. For more information, see the access point documentation on Cisco.com.

This section contains the following topics:

- Overview information—see [About Conversion, page 5-35](#).
- Step-by-step conversion procedure—see [Conversion Procedure, page 5-37](#).

## About Conversion

This section contains the following topics:

- [Overview: Converting Non-IOS Access Points, page 5-35](#)
- [Converting Cisco Aironet 1200 and 1220 Access Points, page 5-36](#)
- [Converting Cisco Aironet 350 Access Points, page 5-37](#)

## Overview: Converting Non-IOS Access Points

There are two options for converting non-IOS access points to IOS:

- You can download the Cisco Aironet Conversion Tool (CAC Tool) from Cisco.com, and convert one access point at a time.
- You can use the WLSE, which can convert multiple access points to IOS.

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.

Conversion takes more time than normal upgrades because:

- Conversion images are larger than normal images.
- The access point must be rebooted twice during a conversion, while it is rebooted only once during normal upgrades.

The WLSE automatically converts most of the non-IOS configuration data to IOS-style configuration. However, certain key data are not automatically converted and must be specified as part of the upgrade job. Therefore, when you use WLSE to convert to IOS, you must define a non-IOS configuration template that includes the following parameters: HSRP configuration, LEAP configuration, User Manager configuration AAA server configurations, WEP key configuration, and per-VLAN security settings. This template is assigned to the devices during the upgrade process.

The WLSE has an internal timeout parameter for firmware upgrades. If the WLSE is unable to communicate successfully with the access point within the period specified by the timeout, it will declare the upgrade job unverified.

## Converting Cisco Aironet 1200 and 1220 Access Points

After conversion, a Cisco Aironet 1200 becomes a Cisco Aironet 1210, and a Cisco Aironet 1220 becomes a Cisco Aironet 1230. As a result, the following changes occur:

- The sysOID after conversion is the same as the sysOID of an access point with native IOS.
- Software images listed in the WLSE Supported Device Table for 1210 and 1230 access points will now apply to the converted access points.
- Converted devices will be placed in different system groups.

The Cisco Aironet 1200 and 1220 access points to be converted must be running 11.56, 12.01T1, or 12.02T1 non-IOS (VxWorks) firmware. The upgrade images are:

Image Name	IOS Version after Conversion
AP1200-Cisco-IOS-Upgrade-Image-v1.img	Cisco IOS Release 12.2(11)JA
AP1200-Cisco-IOS-Upgrade-Image-v1.1.img	Cisco IOS Release 12.2(11)JA1

## Converting Cisco Aironet 350 Access Points

After conversion, Cisco Aironet 350 access points will be removed from the AP350 system group and placed in the AP350-IOS group. The Cisco Aironet 350 access points to be converted must be running 11.23T, 12.01T1, or 12.02T1 non-IOS (VxWorks firmware). The upgrade image is:

Image Name	IOS Version after Conversion
AP350-Cisco-IOS-Upgrade-Image-v1.img	Cisco IOS Release 12.2(13)JA

## Conversion Procedure

The major tasks in the conversion process are listed in [Table 5-11 on page 5-37](#).



### Note

An estimate of the time required to complete the firmware job is displayed during the last task, [4. Create and Run the Conversion Job, page 5-43](#).

**Table 5-11 Quick Reference for Converting an Access Point to IOS**

Task	Reference	
1	Configure the access points to be converted.	<a href="#">1. Configure Access Points To Be Converted, page 5-38.</a>
2	Configure the WLSE by downloading a special conversion image to your local system, importing it into the WLSE, and entering the community strings for all access points to be converted. <b>Note</b> Downloading the image directly from Cisco.com is not supported for the conversion images.	<a href="#">2. Configure the WLSE for IOS Conversions, page 5-38.</a>
3	Create a template for the conversion.	<a href="#">3. Create a Conversion Template, page 5-40.</a>
4	Create and schedule the conversion job.	<a href="#">4. Create and Run the Conversion Job, page 5-43.</a>

## 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.

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

a. 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 5-38](#).

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

---

Next, configure the WLSE. See [2. Configure the WLSE for IOS Conversions, page 5-38](#).

## 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>

For information on the images to use for conversion, see [Converting Cisco Aironet 1200 and 1220 Access Points, page 5-36](#) or [Converting Cisco Aironet 350 Access Points, page 5-37](#).

**Step 2** Import the image:

- a. Download the image to the desktop from Cisco.com. You can download firmware images from the following URL:

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



**Note** Conversion images cannot be imported directly from CCO because these images lack an appropriate version identifier.



**Note** Use of a remote TFTP server is not supported for conversion jobs.

- b. Import the image to the WLSE by selecting **Firmware > Images > Import > From Desktop**.
- c. For converting AP 350s, make sure you select AP 350 from the Device Type list. Do not select AP350-IOS.



**Caution**

The Version field must be set correctly. Otherwise, the image will be incompatible with the access points that you are converting.

Image	Version <sup>1</sup>
AP1200-Cisco-IOS-Upgrade-Image-v1.img	12.2(11)JA
AP1200-Cisco-IOS-Upgrade-Image-v1.1.img	12.2(11)JA1
AP350-Cisco-IOS-Upgrade-Image-v1.img	12.2(13)JA

1. You can also enter the image version as 12.2.

- d. For more information about downloading and importing firmware, see [Importing Images to the WLSE, page 5-8](#).

- 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 5-38](#).

For more information on entering community strings on the WLSE, see [Enter SNMP Communities, page 3-56](#).

---

Next, create a conversion template on the WLSE; see [3. Create a Conversion Template, page 5-40](#).

### 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 the access point is configured correctly after the conversion.

All other parameters 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 but 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 5-38](#).

---

- 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 5-12 on page 5-42](#). 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 during the last task. These messages will not prevent the firmware jobs from running successfully.

---

**Table 5-12 Other Conversion Template Settings**

Template Choice	Setting
Association > VLANs	<ul style="list-style-type: none"> <li>• Enter WEP Key 1 through WEP Key 4.</li> <li>• Select the size of each WEP key.</li> </ul>
11a Radio > Data Encryption	<ul style="list-style-type: none"> <li>• Enter Encryption Key 1 through Encryption Key 4.</li> <li>• Select the Transmit Key.</li> <li>• Select the Key Size for each encryption key.</li> </ul>
Security > Local AP/Client Security	<ul style="list-style-type: none"> <li>• Enter Encryption Key 1 through Encryption Key 4.</li> <li>• Select the Transmit Key.</li> <li>• Select the Key Size for each encryption key.</li> </ul>
Security > Authentication Server	<ul style="list-style-type: none"> <li>• Enter server name or IP address.</li> <li>• Select Server Type.</li> <li>• Enter Port, Share Secret, Retran Int, Max Retran.</li> <li>• Specify EAP Auth, MAC Auth, User Auth, and MIP Auth.</li> </ul>

**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 4-1](#).

After you create the template, you can create and run the firmware job; see [4. Create and Run the Conversion Job, page 5-43](#).

## 4. Create and Run the Conversion Job

For more details on the steps in this procedure, see the complete descriptions in [Job Creation Tasks, page 5-16](#).

To create, save, and run the conversion job:

---

**Step 1** Select **Firmware > Jobs**.

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



---

**Note** Each job name (configuration, firmware, or AP radio scan) must be unique.

---

**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 **Options**. To specify job options:

- a. (Optional) In the Email settings section, you can specify email notification upon completion of the job.
- b. The Remote Server option cannot be used for conversion jobs.
- c. 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.

---

**Step 7** Click **Save** to validate the job settings, view a job summary, and run the job immediately or add it to the list of scheduled jobs.

The Save window shows information about the job. For details about the messages in this window, see [Table 5-8 on page 5-25](#).

If there are warning or error messages in the Save window, the job will fail or only succeed on some of the devices. Edit your job choices and click **Save** in the left pane.

**Step 8** When the job is ready to run, click **Save** in the Save window. The Job Summary page displays basic information about the job, and the job will run immediately or will be added to the job list.

**Step 9** To check job status, select **Firmware > Jobs**.

- 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*.




---

**Note** A job status of “not verified” does not always mean the job failed. The WLSE may have timed out before confirming that the job succeeded. For more information, see [Job Status Information and Job Run Log Messages, page 5-33](#).

---

- 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 successfully:

- All access points in the job will be rebooted.
- An inventory will run automatically.
- The access points will be in the managed state.

- Cisco Aironet 1200 access points that were converted will be removed from the AP 1200 system group and placed in the AP 1210 group. Cisco Aironet 1220 access points will be in the AP 1230 group. Cisco Aironet 350 access points will be in the AP 350-IOS group.
-

