



CHAPTER 8

Managing Controller Software and Configurations

This chapter describes how to manage configurations and software versions on the controllers. It contains these sections:

- [Upgrading Controller Software, page 8-2](#)
- [Transferring Files to and from a Controller, page 8-7](#)
- [Saving Configurations, page 8-17](#)
- [Clearing the Controller Configuration, page 8-17](#)
- [Erasing the Controller Configuration, page 8-18](#)
- [Resetting the Controller, page 8-18](#)

Upgrading Controller Software

When you upgrade the controller's software, the software on the controller's associated access points is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession. Up to 10 access points can be concurrently upgraded from the controller.



Caution

Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image! Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported in software release 4.0.206.0 and later, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Guidelines for Upgrading Controller Software

Follow these guidelines before upgrading your controller to software release 5.0:

- Make sure you have a TFTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP server:
 - Controller software release 5.0 is greater than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the WCS. If you attempt to download the 5.0 controller software and your TFTP server does not support files of this size, the following error message appears: "TFTP failure while storing in flash."
 - If you are upgrading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
 - If you are upgrading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
 - A third-party TFTP server cannot run on the same computer as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.
- You can upgrade or downgrade the controller software only between two releases. To upgrade or downgrade beyond two releases, you must first install an intermediate release. For example, if your controller is running a 4.1 or 4.2 software release, you can upgrade your controller directly to software release 5.0. If your controller is running a 3.2 or 4.0 release, you must upgrade your controller to an intermediate release prior to upgrading to 5.0. [Table 8-1](#) shows the upgrade path that you must follow prior to downloading software release 5.0.



Note

To see the software release that your controller is currently running, click **Monitor** and look at the Software Version field under Controller Summary on the controller GUI or enter **show sysinfo** on the controller CLI.

Table 8-1 Upgrade Path to Controller Software Release 5.0

Current Software Release	Upgrade Path to 5.0 Software
3.2.78.0 or later 3.2 release	Upgrade to a 4.1 release before upgrading to 5.0.
4.0.155.5 or later 4.0 release	Upgrade to a 4.1 or 4.2 release before upgrading to 5.0.
4.1.171.0 or later 4.1 release	You can upgrade directly to 5.0.
4.2.61.0 or later 4.2 release	You can upgrade directly to 5.0.



Note When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 5.0 software. In large networks, it may take some time to download the software on each access point.

- Cisco recommends that you also install the Cisco Unified Wireless Network Controller Boot Software 5.0.148.0 ER.aes file on the controller. This file resolves defect CSCsd52483 and is necessary to ensure proper operation of the controller. The ER.aes file can be installed on all controller platforms. If you do not install this ER.aes file, your controller does not obtain the fix for this defect, and “Error” appears in the Bootloader Version field in the output of the **show sysinfo** command.



Note Unlike previous ER images, a new bootloader file is not loaded when you install the 5.0.148.0 ER.aes file. This is true for all controllers. The 4.2.112.0 ER.aes file is the last ER file to contain a bootloader. If you want the latest bootloader, install the 4.2.112.0 E.aes file. If you want to obtain the fix for CSCsd52483, also install the 5.0.148.0 ER.aes file.



Note The ER.aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (5.0.148.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

**Caution**

If you require a downgrade from one release to another, you may lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.

Using the GUI to Upgrade Controller Software

Follow these steps to upgrade the controller software using the GUI.


Note

Do not install the 5.0 controller software file and the 5.0 ER.aes boot software file at the same time. Install one file and reboot the controller; then install the other file and reboot the controller.

Step 1 Upload your controller configuration files to a server to back them up.


Note

Cisco highly recommends that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Follow these steps to obtain the 5.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes file from the Software Center on Cisco.com:

- a. Click this URL to go to the Software Center:
<http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>
- b. Click **Wireless Software**.
- c. Click **Wireless LAN Controllers**.
- d. Click **Standalone Controllers, Wireless Integrated Routers, or Wireless Integrated Switches**.
- e. Click the name of a controller.
- f. Click **Wireless LAN Controller Software**.
- g. Click a controller software release.
- h. Click the filename (*filename.aes*).
- i. Click **Download**.
- j. Read Cisco's End User Software License Agreement and then click **Agree**.
- k. Save the file to your hard drive.
- l. Repeat steps a. to k. to download the remaining file (either the 5.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes file).

Step 3 Copy the controller software file (*filename.aes*) and the Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes file to the default directory on your TFTP server.

Step 4 Disable the controller 802.11a and 802.11b/g networks.

Step 5 For Cisco WiSMs, shut down the controller port channel on the Catalyst switch to allow the controller to reboot before the access points start downloading the software.

Step 6 Disable any WLANs on the controller.

Step 7 Click **Commands > Download File** to open the Download File to Controller page (see [Figure 8-1](#)).

Step 8 From the File Type drop-down box, choose **Code**.

Step 9 In the IP Address field, enter the IP address of the TFTP server.

Figure 8-1 Download File to Controller Page

The screenshot shows the Cisco GUI interface for downloading a file to a controller. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' tab is active. On the left, a sidebar lists various actions: 'Download File' (highlighted), 'Upload File', 'Reboot', 'Reset to Factory Default', and 'Set Time'. The main content area is titled 'Download file to Controller' and contains a 'File Type' dropdown menu set to 'Code'. Below this is a 'TFTP Server' section with several input fields: 'IP Address' (0.0.0.0), 'Maximum retries' (10), 'Timeout (seconds)' (6), 'File Path', and 'File Name'. There are 'Clear' and 'Download' buttons at the top right of the form area. A vertical ID '230915' is visible on the right edge of the screenshot.

- Step 10** The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work fine without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout field.
- Step 11** In the File Path field, enter the directory path of the software.
- Step 12** In the File Name field, enter the name of the controller software file (*filename.aes*).
- Step 13** Click **Download** to download the software to the controller. A message appears indicating the status of the download.
- Step 14** After the download is complete, click **Reboot**.
- Step 15** If prompted to save your changes, click **Save and Reboot**.
- Step 16** Click **OK** to confirm your decision to reboot the controller.
- Step 17** After the controller reboots, repeat [Step 7](#) to [Step 16](#) to install the remaining file (either the 5.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes file).
- Step 18** Re-enable the WLANs.
- Step 19** For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch.
- Step 20** Re-enable your 802.11a and 802.11b/g networks.
- Step 21** If desired, reload your latest configuration file to the controller.
- Step 22** To verify that the 5.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.
- Step 23** To verify that the Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes file is installed, enter the **show sysinfo** command on the controller CLI and look at the Bootloader Version field. “N/A” appears if the ER.aes file is installed successfully. “Error” appears if the ER.aes file is not installed.

Using the CLI to Upgrade Controller Software

Follow these steps to upgrade the controller software using the CLI.



Note

Do not install the 5.0 controller software file and the 5.0 ER.aes boot software file at the same time. Install one file and reboot the controller; then install the other file and reboot the controller.

Step 1 Upload your controller configuration files to a server to back them up.



Note Cisco highly recommends that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Follow these steps to obtain the 5.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes file from the Software Center on Cisco.com:

- a. Click this URL to go to the Software Center:
<http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>
- b. Click **Wireless Software**.
- c. Click **Wireless LAN Controllers**.
- d. Click **Standalone Controllers, Wireless Integrated Routers, or Wireless Integrated Switches**.
- e. Click the name of a controller.
- f. Click **Wireless LAN Controller Software**.
- g. Click a controller software release.
- h. Click the filename (*filename.aes*).
- i. Click **Download**.
- j. Read Cisco's End User Software License Agreement and then click **Agree**.
- k. Save the file to your hard drive.
- l. Repeat steps a. to k. to download the remaining file (either the 5.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes file).

Step 3 Copy the controller software file (*filename.aes*) and the Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes file to the default directory on your TFTP server.

Step 4 Disable the controller 802.11a and 802.11b/g networks.

Step 5 For Cisco WiSMs, shut down the controller port channel on the Catalyst switch to allow the controller to reboot before the access points start downloading the software.

Step 6 Disable any WLANs on the controller (using the **config wlan disable wlan_id** command).

Step 7 Log into the controller CLI.

Step 8 Enter **ping server-ip-address** to verify that the controller can contact the TFTP server.

Step 9 Enter **transfer download start** and answer **n** to the prompt to view the current download settings. Information similar to the following appears:

```
Mode..... TFTP
Data Type..... Code
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... <directory path>
TFTP Filename..... xxx.aes
```

```
Are you sure you want to start? (y/n) n
Transfer Canceled
```

Step 10 Enter these commands to change the download settings, if necessary:

transfer download mode tftp

transfer download datatype code

transfer download serverip *tftp-server-ip-address*

transfer download filename *filename*

transfer download path *tftp-server-path-to-file*



Note Pathnames on a TFTP server are relative to the server's default or root directory. For example, in the case of the Solarwinds TFTP server, the path is “/”.

Step 11 Enter **transfer download start** to view the updated settings and answer **y** to the prompt to confirm the current download settings and start the software download. Information similar to the following appears:

```
Mode..... TFTP
Data Type..... Code
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... <directory path>
TFTP Filename..... xxx.aes
Are you sure you want to start? (y/n) y
TFTP Code transfer starting.
TFTP receive complete... extracting components.
Writing new bootloader to flash.
Making backup copy of RTOS.
Writing new RTOS to flash.
Making backup copy of Code.
Writing new Code to flash.
TFTP File transfer operation completed successfully.
Please restart the switch (reset system) for update to complete.
```

Step 12 Enter **reset system** to save the code update to non-volatile NVRAM and reboot the controller. The controller completes the bootup process.

Step 13 After the controller reboots, repeat [Step 9](#) to [Step 12](#) to install the remaining file (either the 5.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes file).

Step 14 Enter **config wlan enable** *wlan_id* to re-enable the WLANs.

Step 15 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch.

Step 16 Re-enable your 802.11a and 802.11b/g networks.

Step 17 If desired, reload your latest configuration file to the controller.

Step 18 To verify that the 5.0 controller software is installed, enter **show sysinfo** and look at the Product Version field. To verify that the Boot Software 5.0 ER.aes file is installed, look at the Bootloader Version field. “N/A” appears if the ER.aes file is installed successfully. “Error” appears if the ER.aes file is not installed.

Transferring Files to and from a Controller

Controllers have built-in utilities for uploading and downloading various files. Follow the instructions in these sections to import files using either the controller GUI or CLI:

- [Downloading Device Certificates, page 8-8](#)
- [Downloading CA Certificates, page 8-10](#)
- [Uploading PACs, page 8-12](#)
- [Uploading and Downloading Configuration Files, page 8-13](#)

Downloading Device Certificates

Each wireless device (controller, access point, and client) has its own device certificate. For example, the controller is shipped with a Cisco-installed device certificate. This certificate is used by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authentication. However, if you wish to use your own vendor-specific device certificate, it must be downloaded to the controller.



Note

See the “[Configuring Local EAP](#)” section on page 5-37 for information on configuring local EAP.

Follow the instructions in this section to download a vendor-specific device certificate to the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP server available for the certificate download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.



Note

All certificates downloaded to the controller must be in PEM format.

Using the GUI to Download Device Certificates

Follow these steps to download a device certificate to the controller using the controller GUI.

- Step 1** Copy the device certificate to the default directory on your TFTP server.
- Step 2** Click **Commands > Download File** to open the Download File to Controller page (see [Figure 8-2](#)).

Figure 8-2 Download File to Controller Page

The screenshot shows the Cisco GUI interface for downloading a device certificate. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' tab is active. On the left, a sidebar lists various actions: 'Commands', 'Download File', 'Upload File', 'Reboot', 'Reset to Factory Default', and 'Set Time'. The main area is titled 'Download file to Controller' and contains the following form fields:

- File Type:** A dropdown menu set to 'Vendor Device Certificate'.
- Certificate Password:** A text input field with masked characters (dots).
- TFTP Server:** A section containing several input fields:
 - IP Address:** 10.10.10.4
 - Maximum retries:** 10
 - Timeout (seconds):** 60
 - File Path:** tftpboot/username
 - File Name:** devcert1.pem

At the top right of the form area, there are 'Clear' and 'Download' buttons. A vertical ID number '230921' is visible on the right edge of the screenshot.

- Step 3** From the File Type drop-down box, choose **Vendor Device Certificate**.

- Step 4** In the Certificate Password field, enter the password that was used to protect the certificate.
- Step 5** In the IP Address field, enter the IP address of the TFTP server.
- Step 6** The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work fine without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout field.
- Step 7** In the File Path field, enter the directory path of the certificate.
- Step 8** In the File Name field, enter the name of the certificate.
- Step 9** Click **Download** to download the device certificate to the controller. A message appears indicating the status of the download.
- Step 10** After the download is complete, click **Commands > Reboot > Reboot**.
- Step 11** If prompted to save your changes, click **Save and Reboot**.
- Step 12** Click **OK** to confirm your decision to reboot the controller.

Using the CLI to Download Device Certificates

Follow these steps to download a device certificate to the controller using the controller CLI.

- Step 1** Log into the controller CLI.
- Step 2** Enter **transfer download datatype eapdevcert**.
- Step 3** Enter **transfer download certpassword *password***.
- Step 4** Enter **transfer upload serverip *tftp-server-ip-address***.
- Step 5** Enter **transfer download filename *filename.pem***.
- Step 6** Enter **transfer download start** to view the updated settings; then answer **y** when prompted to confirm the current settings and start the download process. This example shows the download command output:


```
Mode..... TFTP
Data Type..... Vendor Dev Cert
TFTP Server IP..... 10.10.10.4
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /tftpboot/username/
TFTP Filename..... filename.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
Reboot the switch to use the new certificate.
```
- Step 7** Enter **reset system** to reboot the controller.
- Step 8** After the controller reboots, enter **show certificates local-auth** to verify that the certificate is installed.

Downloading CA Certificates

Controllers and access points have a Certificate Authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate may be used by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authentication. However, if you wish to use your own vendor-specific CA certificate, it must be downloaded to the controller.



Note

See the “[Configuring Local EAP](#)” section on page 5-37 for information on configuring local EAP.

Follow the instructions in this section to download CA certificates to the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP server available for the certificate download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.



Note

All certificates downloaded to the controller must be in PEM format.

Using the GUI to Download CA Certificates

Follow these steps to download a CA certificate to the controller using the controller GUI.

- Step 1** Copy the CA certificate to the default directory on your TFTP server.
- Step 2** Click **Commands > Download File** to open the Download File to Controller page (see [Figure 8-3](#)).

Figure 8-3 Download File to Controller Page

The screenshot shows the Cisco GUI interface for downloading a file to the controller. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' tab is active. On the left sidebar, 'Download File' is selected. The main content area is titled 'Download file to Controller' and contains the following fields and options:

- File Type:** Vendor CA Certificate (dropdown menu)
- TFTP Server:**
 - IP Address: 10.10.10.4
 - Maximum retries: 10
 - Timeout (seconds): 60
 - File Path: /tftpboot/username
 - File Name: ca.pem

Buttons for 'Clear' and 'Download' are located at the top right of the form area.

- Step 3** From the File Type drop-down box, choose **Vendor CA Certificate**.
- Step 4** In the IP Address field, enter the IP address of the TFTP server.

- Step 5** The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work fine without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout field.
- Step 6** In the File Path field, enter the directory path of the certificate.
- Step 7** In the File Name field, enter the name of the certificate.
- Step 8** Click **Download** to download the CA certificate to the controller. A message appears indicating the status of the download.
- Step 9** After the download is complete, click **Commands > Reboot > Reboot**.
- Step 10** If prompted to save your changes, click **Save and Reboot**.
- Step 11** Click **OK** to confirm your decision to reboot the controller.
-

Using the CLI to Download CA Certificates

Follow these steps to download a CA certificate to the controller using the controller CLI.

- Step 1** Log into the controller CLI.
- Step 2** Enter **transfer download datatype eapcacert**.
- Step 3** Enter **transfer download serverip *tftp-server-ip-address***.
- Step 4** Enter **transfer download filename *filename.pem***.
- Step 5** Enter **transfer download start** to view the updated settings; then answer **y** when prompted to confirm the current settings and start the download process. This example shows the download command output:
- ```
Mode..... TFTP
Data Type..... Vendor CA Cert
TFTP Server IP..... 10.10.10.4
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /tftpboot/username/
TFTP Filename..... filename.pem
```
- This may take some time.  
Are you sure you want to start? (y/N) y
- TFTP EAP CA cert transfer starting.
- Certificate installed.  
Reboot the switch to use the new certificate.
- Step 6** Enter **reset system** to reboot the controller.
- Step 7** After the controller reboots, enter **show certificates local-auth** to verify that the certificate is installed.
-

## Uploading PACs

Protected access credentials (PACs) are credentials that are either automatically or manually provisioned and used to perform mutual authentication with a local EAP authentication server during EAP-FAST authentication. When manual PAC provisioning is enabled, the PAC file is manually generated on the controller.



### Note

See the “[Configuring Local EAP](#)” section on page 5-37 for information on configuring local EAP.

Follow the instructions in this section to generate and load PACs from the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP server available for the PAC upload. Keep these guidelines in mind when setting up a TFTP server:

- If you are uploading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are uploading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.

## Using the GUI to Upload PACs

Follow these steps to upload a PAC from the controller using the controller GUI.

- Step 1** Click **Commands > Upload File** to open the Upload File from Controller page (see [Figure 8-4](#)).

**Figure 8-4** Upload File from Controller Page

The screenshot shows the Cisco GUI interface for uploading a Protected Access Credential (PAC). The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' tab is active. On the left, a sidebar lists 'Commands' with 'Upload File' highlighted. The main content area is titled 'Upload file from Controller' and contains the following fields:

- File Type:** A dropdown menu set to 'PAC (Protected Access Credential)'.
- User (Identity):** A text input field containing 'username'.
- Validity (in days):** A text input field containing '10'.
- Password:** A text input field with masked characters '...'.
- Confirm Password:** A text input field with masked characters '...'.
- TFTP Server:** A section with three sub-fields:
  - IP Address:** '10.10.10.4'
  - File Path:** 'tftpboot/username'
  - File Name:** 'test.pac'

Buttons for 'Clear' and 'Upload' are located in the top right corner of the form area. A vertical ID number '230922' is visible on the right edge of the screenshot.

- Step 2** From the File Type drop-down box, choose **PAC (Protected Access Credential)**.
- Step 3** In the User field, enter the name of the user who will use the PAC.
- Step 4** In the Validity field, enter the number days for the PAC to remain valid. The default setting is zero (0).
- Step 5** In the Password and Confirm Password fields, enter a password to protect the PAC.

- Step 6** In the IP Address field, enter the IP address of the TFTP server.
  - Step 7** In the File Path field, enter the directory path of the PAC.
  - Step 8** In the File Name field, enter the name of the PAC file. PAC files have a .pac extension.
  - Step 9** Click **Upload** to upload the PAC from the controller. A message appears indicating the status of the upload.
  - Step 10** Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.
- 

## Using the CLI to Upload PACs

Follow these steps to upload a PAC from the controller using the controller CLI.

- Step 1** Log into the controller CLI.
- Step 2** Enter **transfer upload datatype pac**.
- Step 3** Enter **transfer upload pac *username validity password***.
- Step 4** Enter **transfer upload serverip *tftp-server-ip-address***.
- Step 5** Enter **transfer upload filename *manual.pac***.
- Step 6** Enter **transfer upload start** to view the updated settings; then answer **y** when prompted to confirm the current settings and start the upload process. This example shows the upload command output:

```

Mode..... TFTP
TFTP Server IP..... 10.10.10.4
TFTP Path..... /tftpboot/username/
TFTP Filename..... manual.pac
Data Type..... PAC
PAC User..... username
PAC Validity..... 10 days
PAC Password..... password

Are you sure you want to start? (y/N) y

PAC transfer starting.

File transfer operation completed successfully.
```

- Step 7** Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.
- 

## Uploading and Downloading Configuration Files

Prior to upgrading your controller's software, Cisco recommends that you upload your controller's configuration file to a server to back it up. Then after the new controller software is installed, you can download the configuration file to the controller.

**Note**

If you do not back up your controller's configuration file prior to upgrading the controller software, you must manually reconfigure the controller.

In controller software release 4.2 or later, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. Therefore, you cannot download a binary configuration file onto a controller running software release 4.2 or later. However, when you upgrade a controller from a previous software release to 4.2 or later, the configuration file is migrated and converted to XML.

**Note**

Do not attempt to make changes to the configuration file. If you do so and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

## Uploading Configuration Files

You can upload configuration files using either the GUI or the CLI.

### Using the GUI to Upload Configuration Files

Using the controller GUI, follow these steps to upload a configuration file.

- Step 1** Click **Commands > Upload File** to open the Upload File from Controller page (see [Figure 8-5](#)).

**Figure 8-5** Upload File from Controller Page

The screenshot shows the Cisco GUI interface for uploading a configuration file. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' menu is expanded, showing options like 'Download File', 'Upload File', 'Reboot', 'Reset to Factory Default', and 'Set Time'. The 'Upload File' option is selected, leading to the 'Upload file from Controller' page. This page has a 'File Type' dropdown menu set to 'Configuration'. Below it, the 'Configuration File Encryption' checkbox is checked and labeled 'Enabled', with an 'Encryption Key' field containing masked characters. The 'TFTP Server' section contains three input fields: 'IP Address' (10.10.10.4), 'File Path' (tftpboot/username/), and 'File Name' (AS\_4402\_4\_55). There are 'Clear' and 'Upload' buttons at the top right of the form area.

- Step 2** From the File Type drop-down box, choose **Configuration**.
- Step 3** To enable encryption, check the **Configuration File Encryption** check box and enter the encryption key. File encryption ensures that data is encrypted while the configuration file is being uploaded through a TFTP server.
- Step 4** In the IP Address field, enter the IP address of the TFTP server.
- Step 5** In the File Path field, enter the directory path of the configuration file.
- Step 6** In the File Name field, enter the name of the configuration file.

- Step 7** Click **Upload** to upload the configuration file to the TFTP server. A message appears indicating the status of the upload. If the upload fails, repeat the procedure and try again.

### Using the CLI to Upload Configuration Files

Using the controller CLI, follow these steps to upload a configuration file to the controller.

- Step 1** Log into the controller CLI.
- Step 2** Enter **transfer upload datatype config**.
- Step 3** To encrypt the configuration file, do the following:
- Enter **transfer encrypt enable**.
  - Enter **transfer encrypt set-key key**.
- Step 4** Enter **transfer upload serverip tftp-server-ip-address**.
- Step 5** Enter **transfer upload path path**.
- Step 6** Enter **transfer upload filename filename**.
- Step 7** Enter **transfer upload start** to view the updated settings; then answer **y** when prompted to confirm the current settings and start the upload process. This example shows the upload command output:

```
Mode..... TFTP
TFTP Server IP..... 10.10.10.4
TFTP Path..... Config/
TFTP Filename..... AS_4402_4_2_55_8_Config.xml
Data Type..... Config File
Encryption..... Disabled
```

```

*** WARNING: Config File Encryption Disabled ***

```

```
Are you sure you want to start? (y/N) y
```

```
File transfer operation completed successfully.
```

If the upload fails, repeat the procedure and try again.

### Downloading Configuration Files

You can download configuration files using either the GUI or the CLI.

#### Using the GUI to Download Configuration Files

Using the controller GUI, follow these steps to download a configuration file to the controller.

- Step 1** Click **Commands > Download File** to open the Download File to Controller page (see [Figure 8-6](#)).

Figure 8-6 Download File to Controller Page

The screenshot shows the Cisco Wireless LAN Controller GUI. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' tab is active. On the left, a sidebar lists 'Commands' with 'Download File' selected. The main content area is titled 'Download file to Controller' and contains the following fields:

- File Type:** Configuration (dropdown menu)
- Configuration File Encryption Key:** Masked with six dots
- TFTP Server:**
  - IP Address: 10.10.10.4
  - Maximum retries: 10
  - Timeout (seconds): 6
  - File Path: tftpboot/username/
  - File Name: AS\_4402\_4\_55

Buttons for 'Clear' and 'Download' are located at the top right of the form. A vertical ID number '232283' is visible on the right side of the form area.

- Step 2** From the File Type drop-down box, choose **Configuration**.
- Step 3** In the Configuration File Encryption Key field, enter the encryption key that encrypts the data in the configuration file when the file is downloaded.
- Step 4** In the IP Address field, enter the IP address of the TFTP server.
- Step 5** The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work fine without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the configuration file in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the configuration file in the Timeout field.
- Step 6** In the File Path field, enter the directory path of the configuration file.
- Step 7** In the File Name field, enter the name of the configuration file (*filename*).
- Step 8** Click **Download** to download the file to the controller. A message appears indicating the status of the download, and the controller reboots automatically. If the download fails, repeat the procedure and try again.

## Using the CLI to Download Configuration Files

Using the controller CLI, follow these steps to download a configuration file to the controller.

- Step 1** Log into the controller CLI.
- Step 2** Enter **transfer download datatype config**.
- Step 3** To encrypt the configuration file, do the following:
- Enter **transfer encrypt enable**.
  - Enter **transfer encrypt set-key key**.
- Step 4** Enter **transfer download serverip tftp-server-ip-address**.
- Step 5** Enter **transfer download path path**.
- Step 6** Enter **transfer download filename filename**.

- Step 7** Enter **transfer download start** to view the updated settings; then answer **y** when prompted to confirm the current settings and start the download process. This example shows the download command output:

```
Mode..... TFTP
TFTP Server IP..... 10.10.10.4
TFTP Path..... Config/
TFTP Filename..... AS_4402_4_2_55_8_Config.xml
Data Type..... Config File
Encryption..... Disabled
```

```

*** WARNING: Config File Encryption Disabled ***

```

Are you sure you want to start? (y/N) **y**

File transfer operation completed successfully.

If the download fails, repeat the procedure and try again.

## Saving Configurations

Controllers contain two kinds of memory: volatile RAM and NVRAM. At any time, you can save the configuration changes from active volatile RAM to non-volatile RAM (NVRAM) using one of these commands:

- Use the **save config** command. This command saves the configuration from volatile RAM to NVRAM without resetting the controller.
- Use the **reset system** command. The CLI prompts you to confirm that you want to save configuration changes before the controller reboots.
- Use the **logout** command. The CLI prompts you to confirm that you want to save configuration changes before you log out.

## Clearing the Controller Configuration

Follow these steps to clear the active configuration in NVRAM.

- Step 1** Enter **clear config** and enter **y** at the confirmation prompt to confirm the action.
- Step 2** Enter **reset system**. At the confirmation prompt, enter **n** to reboot without saving configuration changes. When the controller reboots, the configuration wizard starts automatically.
- Step 3** Follow the instructions in the [“Using the Configuration Wizard”](#) section on page 4-2 to complete the initial configuration.

## Erasing the Controller Configuration

Follow these steps to reset the controller configuration to default settings:

- 
- Step 1** Enter **reset system**. At the confirmation prompt, enter **y** to save configuration changes to NVRAM. The controller reboots.
- Step 2** When you are prompted for a username, enter **recover-config** to restore the factory default configuration. The controller reboots and the configuration wizard starts automatically.
- Step 3** Follow the instructions in the [“Using the Configuration Wizard” section on page 4-2](#) to complete the initial configuration.
- 

## Resetting the Controller

You can reset the controller and view the reboot process on the CLI console using one of the following two methods:

- Turn the controller off and then turn it back on.
- On the CLI, enter **reset system**. At the confirmation prompt, enter **y** to save configuration changes to NVRAM. The controller reboots.

When the controller reboots, the CLI console displays the following reboot information:

- Initializing the system.
- Verifying the hardware configuration.
- Loading microcode into memory.
- Verifying the operating system software load.
- Initializing with its stored configurations.
- Displaying the login prompt.