



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 8-6](#)
- [Saving Configurations, page 8-12](#)
- [Clearing the Controller Configuration, page 8-12](#)
- [Erasing the Controller Configuration, page 8-13](#)
- [Resetting the Controller, page 8-13](#)

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. 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 4.1 from a previous release:

- 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 4.1 is greater than 32 megabytes (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 tftpd, Cisco tftp, and the TFTP server within the WCS. If you attempt to download the 4.1 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.
 - 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.
- If your controller is running software release 3.2.195.10(or a later 3.2 release) or 4.0.206.0 (or a later 4.0 release), you can upgrade your controller directly to software release 4.1. If your controller is running an earlier 3.2 or 4.0 release, you must upgrade your controller to an intermediate release prior to upgrading to 4.1. [Table 8-1](#) shows the upgrade path that you must follow prior to downloading software release 4.1.



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.

Table 8-1 Upgrade Path to Controller Software Release 4.1

Current Software Release	Upgrade Path to 4.1 Software
3.2.78.0	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 4.1.
3.2.116.21	
3.2.150.10	
3.2.171.6	
3.2.193.5	If your controller is configured with the new J3 country code, upgrade to 3.2.195.10 (or a later 3.2 release). If your controller is not configured for the new J3 country code, you can upgrade to 3.2.195.10 (or a later 3.2 release) or to 4.0.206.0 (or a later 4.0 release).
3.2.195.10 (or later 3.2 release)	You can upgrade directly to 4.1.
4.0.155.5	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 4.1.
4.0.179.11	
4.0.206.0 (or later 4.0 release)	You can upgrade directly to 4.1.



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 4.1 software. In large networks, it may take some time to download the software on each access point.

- Due to some enhancements that were made to the bootloader software for some controllers, you must install the Cisco Unified Wireless Network Controller Boot Software 4.1 _ER.aes image on the controller either before or after installing the 4.1 .aes file.



Note Refer to the Release Notes for your specific 4.1 release to see which controllers require the _ER.aes image.

- Cisco recommends the following sequence when performing an upgrade:
 - Upload your controller configuration files to a server to back them up.
 - Disable the controller 802.11a and 802.11b/g networks.
 - Upgrade your controller to the latest software release, following the instructions in this section.
 - Re-enable your 802.11a and 802.11b/g networks.
 - If desired, reload your latest configuration file to the controller.

**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.

- Step 1** Obtain the desired controller software release from the Software Center on Cisco.com: <http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>
- Step 2** Copy the software file (*filename.aes*) to the default directory on your TFTP server.
- Step 3** Click **Commands > Download File** to access the Download File to Controller page (see [Figure 8-1](#)).

Figure 8-1 Download File to Controller Page

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

- File Type:** A dropdown menu currently set to 'Code'.
- TFTP Server:** A section containing several input fields:
 - IP Address:** 0.0.0.0
 - Maximum retries:** 10
 - Timeout (seconds):** 6
 - File Path:** An empty text input field.
 - File Name:** An empty text input field.
- Buttons:** 'Clear' and 'Download' buttons are located in the top right corner of the form area.

A vertical ID number '230915' is visible on the right side of the screenshot.

- Step 4** From the File Type drop-down box, choose **Code**.
- Step 5** In the IP Address field, enter the IP address of the TFTP server.
- Step 6** In the Maximum Retries field, enter the maximum number of times that the TFTP server attempts to download the software.
- Step 7** In the Timeout field, enter the amount of time (in seconds) that the TFTP server attempts to download the software.
- Step 8** In the File Path field, enter the directory path of the software.
- Step 9** In the File Name field, enter the name of the software (*filename.aes*).
- Step 10** Click **Download** to download the software to the controller. A message appears indicating the status of the download.
- Step 11** After the download is complete, click **Reboot**.
- Step 12** If prompted to save your changes, click **Save and Reboot**.
- Step 13** Disable the WLANs and then repeat this procedure to install the *_ER.aes* file.
- Step 14** Re-enable the WLANs.

Using the CLI to Upgrade Controller Software

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

- Step 1** Obtain the desired controller software release from the Software Center on Cisco.com:
<http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml>
- Step 2** Copy the software file (*filename.aes*) to the default directory on your TFTP server.
- Step 3** Log into the controller CLI.
- Step 4** Enter **ping** *server-ip-address* to verify that the controller can contact the TFTP server.
- Step 5** 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 6** Enter these commands to change the download settings:

```
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 7** 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 8** Enter **reset system** to save the code update to non-volatile NVRAM and reboot the controller. The controller completes the bootup process
- Step 9** Disable the WLANs (using the **config wlan disable wlan_id** command) and then repeat this procedure to install the `_ER.aes` file.
- Step 10** Enter **config wlan enable wlan_id** to re-enable the WLANs.
-

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 8-6](#)
- [Downloading CA Certificates, page 8-8](#)
- [Uploading PACs, page 8-10](#)

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-TLS and EAP-FAST (when not using PACs) 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 5-24](#) 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.
- 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 access 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 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, a sidebar lists 'Commands' with sub-options: 'Download File', 'Upload File', 'Reboot', 'Reset to Factory Default', and 'Set Time'. The main content area is titled 'Download file to Controller' and contains the following 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 with 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. The Cisco logo is in the top left corner. A vertical ID '230921' is on the right edge.

- 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** In the Maximum Retries field, enter the maximum number of times that the TFTP server attempts to download the certificate.
- Step 7** In the Timeout field, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.
- Step 8** In the File Path field, enter the directory path of the certificate.
- Step 9** In the File Name field, enter the name of the certificate.
- Step 10** Click **Download** to download the device certificate to the controller. A message appears indicating the status of the download.
- Step 11** After the download is complete, click **Commands > Reboot > Reboot**.
- Step 12** If prompted to save your changes, click **Save and Reboot**.

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-TLS and EAP-FAST (when not using PACs) 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 5-24](#) 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.
- 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 access 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, 'Commands' is selected, and 'Download File' is highlighted. The main content area is titled 'Download file to Controller' and contains the following fields:

- 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** In the Maximum Retries field, enter the maximum number of times that the TFTP server attempts to download the certificate.
- Step 6** In the Timeout field, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.
- 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 CA 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**.

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 5-24](#) 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.
- 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 access the Upload File from Controller page (see [Figure 8-4](#)).

Figure 8-4 Upload File from Controller Page

The screenshot shows the Cisco GUI for uploading a Protected Access Credential (PAC). The navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' menu is open, and 'Upload File' is selected. The main content area is titled 'Upload file from Controller' and contains the following fields:

- File Type:** A drop-down 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 (dots).
- Confirm Password:** A text input field with masked characters (dots).
- TFTP Server:** A section with three fields:
 - IP Address:** '10.10.10.4'
 - File Path:** 'tftpboot/username'
 - File Name:** 'test.pac'

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

- 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 ftp-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.
-

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.

