Managing Controller Software and Configurations

Upgrading the Controller Software

When you upgrade the controller software, the software on the access points associated with the controller is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.

Caution Do not power down the controller or any access point during this process; otherwise, the software image could be corrupted. 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 the controller software release, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Guidelines and Restrictions for Upgrading Controller Software

The following are some of the general guidelines and restrictions that are applicable when upgrading the controller software. For any release-specific restrictions, see the relevant release notes.

For correct interoperability among Cisco Wireless infrastructure, including but not limited to mobility among controllers, AP compatibility, see the *Cisco Wireless Solutions Software Compatibility Matrix* at:

https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

- For every software upgrade, see the corresponding release notes for any caveats, considerations, or possible interim upgrades required to upgrade your controller to the desired release of software.

- We recommend that you have a backup of your configuration in an external repository before any software upgrade activity.
- The upgrade of the controller software, with a fast connection to your TFTP, SFTP, or FTP file server, can take approximately 15 to 25 minutes or less from the start of the software transfer to reboot of controller (might take longer if the upgrade also includes a Field Upgrade Software installation during the same maintenance window). The time required for the upgrade of the associated APs might vary from one network to another, due to a variety of deployment-specific factors, such as number of APs associated with controller, speed of network connectivity between a given AP and the controller, and so on.
- We recommend that, during the upgrade process, you do not power off controller or any AP associated with the controller.
- Controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Download Software area in Cisco.com.
- The objects under the SNMP table bsnAPIfDot11CountersEntry like bsnAPIfDot11RetryCount, bsnAPIfDot11TransmittedFrameCount, and so on, per SNMP MIB description, are defined to use the index as 802.3 (Ethernet) MAC address of the AP. However, the controller sends the AP radio MAC address in snmpget, getnext, and getbulk. This is because the snmpwalk returns index using base radio MAC address instead of the AP Ethernet MAC address.
- You can reduce the network downtime using the following options:
  - You can predownload the AP image.

    For more information about predownloading the AP image, see the "Predownloading an Image to an Access Point" section.
  - For FlexConnect access points, use the FlexConnect Efficient AP upgrade feature to reduce traffic between the controller and the AP (main site and the branch).

    For more information about configuring FlexConnect AP upgrades, see the Configuring FlexConnect AP Upgrades for FlexConnect APs section.

Upgrading Controller Software (GUI)

Before you begin

Before upgrading the controller software, we recommend that you consult relevant release notes for any release-specific restrictions.

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

Note We highly recommend that you back up your configuration files of the controller prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Get the controller software image by following these steps:

a) Browse to http://www.cisco.com/cisco/software/navigator.html.

b) Choose **Wireless** > **Wireless LAN Controller**.

The following options are available: **Integrated Controllers and Controller Modules**, **Mobility Express**, and **Standalone Controllers**.

c) Depending on your controller platform, click one of the above options.
d) Click the controller model number or name. The Download Software page is displayed.
e) Click a controller software release. The software releases are labeled as follows to help you determine which release to download:

Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.

Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

f) Choose a software release number.
g) Click the filename (*filename*.aes).
h) Click **Download**.
i) Read Cisco's End User Software License Agreement and then click **Agree**.
j) Save the file to your hard drive.
k) Repeat steps *a* through *k* to download the remaining file.

Step 3 Copy the controller software image (*filename*.aes) to the default directory on your TFTP or FTP server.

Note In Release 8.1 and later releases, transfer over HTTP is also supported.

Note In 8.3, 8.4, and 8.5 releases, for Cisco 2504 WLC, 5508 WLC, and WiSM2, the Cisco WLC software image is split into two images: Base Install Image and Supplementary AP Bundle Image. Therefore, to upgrade to 8.3, 8.4, or 8.5 release, you must repeat Step 2 through Step 14 to complete the installation of both Base Install Image and Supplementary AP Bundle Image.

Download the Supplementary AP Bundle Image only if you are using any of these APs: AP80x, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, and/or Cisco Aironet 1600 APs.

Step 4 (Optional) Disable the 802.11 networks.

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 5 Choose **Commands > Download File** to open the **Download File to Controller** page.

Step 6 From the **File Type** drop-down list, choose **Code**.

Step 7 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)
- **HTTP** (available in 8.1 and later releases)

Step 8 In the **IP Address** field, enter the IP address of the server.

Step 9 (Optional) If you are using a TFTP server, the default values of 10 retries for the Maximum Retries text field, and 6 seconds for the Timeout text field should work correctly 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 10 In the **File Path** field, enter the directory path of the software.

Step 11 In the **File Name** field, enter the name of the controller software file (*filename*.aes).

Step 12 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the FTP server.

b) In the **Server Login Password** field, enter the password to log into the FTP server.

c) In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 13 Click **Download** to download the software to the controller. A message is displayed indicating the status of the download.

Note In 8.3, 8.4, and 8.5 releases, for Cisco 2504 WLC, 5508 WLC, and WiSM2, the Cisco WLC software image is split into two images: Base Install Image and Supplementary AP Bundle Image. Therefore, to upgrade to 8.3, 8.4, or 8.5 release, you must repeat Step 2 through Step 14 to complete the installation of both Base Install Image and Supplementary AP Bundle Image.

Download the Supplementary AP Bundle Image only if you are using any of these APs: AP80x, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, and/or Cisco Aironet 1600 APs.

Step 14 (Optional) After the download is complete, you can choose to predownload the image to your access points. For more information, see the "Predownloading an Image to an Access Point" section.

Step 15 Click **Reboot** to reboot the controller.

Step 16 If prompted to save your changes, click **Save and Reboot**.

Step 17 Click **OK** to confirm.

Step 18 After the controller reboots, repeat step 6 to step 16 to install the remaining file.

Step 19 For Cisco WiSM2, reenable the controller port channel on the Catalyst switch.

Step 20 If you have disabled the 802.11 networks, reenable them.

Step 21 To verify the controller software version, choose **Monitor** on the controller GUI and see **Software Version** in the Controller Summary area.

Upgrading Controller Software (CLI)

Before you begin

Before upgrading the controller software, we recommend that you consult relevant release notes for any release-specific restrictions.

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

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

Step 2 Get the controller software image by following these steps:

a) Browse to http://www.cisco.com/cisco/software/navigator.html.

b) Choose **Wireless** > **Wireless LAN Controller**.

The following options are available: **Integrated Controllers and Controller Modules**, **Mobility Express**, and **Standalone Controllers**.

c) Depending on your controller platform, click one of the above options.
d) Click the controller model number or name. The Download Software page is displayed.
e) Click a controller software release. The software releases are labeled as follows to help you determine which release to download:

Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.

Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

f) Choose a software release number.
g) Click the filename (*filename*.aes).
h) Click **Download**.
i) Read Cisco's End User Software License Agreement and then click **Agree**.
j) Save the file to your hard drive.
k) Repeat steps *a* through *k* to download the remaining file.

Step 3 Copy the controller software image (*filename*.aes) to the default directory on your TFTP or FTP server.

Note In Release 8.3, for Cisco 2504 WLC, 5508 WLC, and WiSM2, the Cisco WLC software image is split into two images: Base Install Image and Supplementary AP Bundle Image. Therefore, to upgrade to Release 8.3 or later supported releases, you must repeat Step 2 through Step 11 to complete the installation of both Base Install Image and Supplementary AP Bundle Image.

Download the Supplementary AP Bundle Image only if you are using any of these APs: AP80x, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, and/or Cisco Aironet 1600 Series APs.

Step 4 Log onto the controller CLI.

Step 5 On the controller CLI over Telnet or SSH, enter the **ping server-ip-address** command to verify that the controller can contact the TFTP or FTP server.

Step 6 (Optional) Disable the 802.11 networks by entering this command:

config 802.11{**a** | **b**} **disable network**

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 7 View current download settings by entering the **transfer download start** command. Press **n** at the prompt to view the current download settings.

Step 8 Change the download settings, if necessary by entering these commands:

- **transfer download mode** {**tftp** | **ftp** | **sftp**}
- **transfer download datatype code**
- **transfer download serverip** *server-ip-address*
- **transfer download filename** *filename*
- **transfer download path** *server-path-to-file*

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

(Optional) If you are using a TFTP server, also enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

If you are using an FTP server, also enter these commands:

- **transfer download username** *username*
- **transfer download password** *password*
- (Optional) **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 9 View the current updated settings by entering the **transfer download start** command. Press **y** at the prompt to confirm the current download settings and start the software download.

Step 10 (Optional) After the download is complete, you can choose to predownload the image to your access points. For more information, see the "Predownloading an Image to an Access Point" section.

Step 11 Save the code update to nonvolatile NVRAM and reboot the controller by entering this command:

reset system

The controller completes the bootup process.

Step 12 After the controller reboots, repeat Steps 7 through 11 to install the remaining file.

Step 13 For Cisco WiSM2, re-enable the controller port channel on the Catalyst switch.

Step 14 If you have disabled the 802.11 networks in Step 6, reenable them by entering this command:

config 802.11{a | b} enable network

Step 15 To verify the controller software that is installed, enter the **show sysinfo** command and see Product Version.

Step 16 (Optional) To verify the Cisco Unified Wireless Network Controller Boot Software file that is installed on the controller, enter the **show sysinfo** command on the controller CLI and see Recovery Image Version or Emergency Image Version.

Note If a Cisco Unified Wireless Network Controller Boot Software ER.aes file is not installed, Recovery Image Version or Emergency Image Version show 'N/A.'

Predownloading an Image to an Access Point

To minimize network outages, you can download an upgrade image to the access point from the controller without resetting the access point or losing network connectivity. Previously, you would download an upgrade image to the controller and reset it, which causes the access point to go into discovery mode. After the access

point discovers the controller with the new image, the access point downloads the new image, resets, goes into discovery mode, and rejoins the controller.

You can now download the upgrade image to the controller and then download the image to the access point while the network is still operational. You can also schedule a reboot of the controller and access points, either after a specified amount of time or at a specific date and time. When both devices are up, the access point discovers and rejoins the controller.

Concurrent Controller to AP Image Upgrade

This table lists the controllers and their maximum concurrent AP image download support.

Controller	Maximum Number of Concurrent AP Image Download Supported
Cisco 2504 Wireless Controller	75
Cisco 5508 Wireless Controller	500
Cisco 5520 Wireless Controller	1000
Cisco Flex 7510 Wireless Controller	1000
Cisco 8510 Wireless Controller	1000
Cisco 8540 Wireless Controller	1000
Cisco WiSM2	500
Cisco vWLC	1000

Flash Memory Requirements on Access Points

This table lists the Cisco AP models and the minimum amount of free flash memory required for the predownload process to work:

Cisco AP	Minimum Free Flash Memory Required
3700(I/E)	16 MB
3600(I/E)	14 MB
3502(I/E)	14 MB
2700(I/E)	16 MB
2602(I/E)	14 MB
1700(I/E)	16 MB
1602(I/E)	12 MB
1262	14 MB
1142	12 MB

Note

- The required flash memory can vary based on the radio type and the number of antennas used.
- This predownload feature is not supported on 1242 and 1131 Cisco AP models.
- Cisco AP1142 has 32 MB of total flash memory and can support the predownload feature.
- During the predownloading of image to APs, some APs do not have enough memory to keep the current radio firmware available. After the image has been predownloaded, these APs have the image only on flash memory and no other memory is available to host the current image or version radio firmware. The APs that have this limitation are as follows: Cisco Aironet 700, 1140, 1260, 1520, 1530, 1550, 1600, 3500, and 3600 Series APs.

  For more information about this limitation, see CSCvg41698.
- As part of the fix for CSCvb75682, if the flash memory of Cisco Aironet 1700, 2700, and 3700 Series APs is less than 10 Mb and a recovery image is present, the backup images in these APs are deleted.

Access Point Predownload Process

The access point predownload feature works as follows:

- The controller image is downloaded.
  - (Optional) The primary image becomes the backup image of the controller and the downloaded image becomes the new primary image. Change the current boot image as the backup image by using the **config boot backup** command to ensure that if a system failure occurs, the controller boots with the last working image of the controller.
  - Start the AP image predownload procedure for all joined APs or a specific AP, by entering the **config ap image predownload primary** {**all** | *ap-name*} command.
  - The upgrade image is downloaded as the backup image on the APs. You can verify this by using the **show ap image all** command.
  - Change the boot image to primary image manually using the **config boot primary** command and reboot the controller for the upgrade image to be activated.

    or
  - You issue a scheduled reboot with the **swap** keyword. The **swap** keyword has the following importance: The swapping occurs to the primary and backup images on the access point and the currently active image on controller with the backup image.
  - When the controller reboots, the access points are disassociated and eventually come up with an upgraded image. Once the controller responds to the discovery request sent by an access point with its discovery response packet, the access point sends a join request.
- The actual upgrade of the images occur. The following sequence of actions occur:
  - During boot time, the access point sends a join request.
  - The controller responds with the join response with the image version that the controller is running.
  - The access point compares its running image with the running image on the controller. If the versions match, the access point joins the controller.

- If the versions do not match, the access point compares the version of the backup image and if they match, the access point swaps the primary and backup images and reloads and subsequently joins the controller.
- If the primary image of the access point is the same as the controller image, the access point reloads and joins the controller.
- If none of the above conditions are true, the access point sends an image data request to the controller, downloads the latest image, reloads, and joins the controller.

Note Normally, when upgrading the image of an AP, you can use the preimage download feature to reduce the amount of time the AP is unavailable to serve clients. However, it also increases the downtime because the AP cannot serve clients during an upgrade. The preimage download feature can be used to reduce this downtime. However, in the case of a branch office set up, the upgrade images are still downloaded to each AP over the WAN link, which has a higher latency.

A more efficient way is to use the FlexConnect AP Image Upgrade feature. When this feature is enabled, one AP of each model in the local network first downloads the upgrade image over the WAN link. For more information about FlexConnect AP upgrades, see the "FlexConnect AP Image Upgrades" chapter.

Guidelines and Restrictions for Predownloading an Image to an Access Point

- The 2600, 3500, and 3600 AP models can store only a single image in the flash. When you reboot the AP (without rebooting the controller after a pre-download), it will download the current image from the controller as the current image will be overwritten by the pre-downloaded image in the flash.
- The maximum number of concurrent predownloads is limited to half the number of concurrent normal image downloads. This limitation allows new access points to join the controller during image downloading.
- If you reach the predownload limit, then the access points that cannot get an image sleep for a time between 180 to 600 seconds and then reattempt the predownload.
- Before you predownload, you should change the active controller boot image to the backup image to ensure that if the controller reboots for some reason, it comes back up with the earlier running image, not the partially downloaded upgrade image.
- This predownload feature is not supported on 1242 and 1131 Cisco AP models.
- When the system time is changed by using the **config time** command, the time set for a scheduled reset is not valid and the scheduled system reset is canceled. You are given an option either to cancel the scheduled reset before configuring the time or retain the scheduled reset and not configure the time.
- All the primary, secondary, and tertiary controllers should run the same images as the primary and backup images. That is, the primary image of all three controllers should be X and the secondary image of all three controllers should be Y or the feature is not effective.

  Having different versions of the controller software running on primary, secondary, and tertiary controllers adds unnecessary and protracted delays to APs failing over and joining the other available controllers in an N+1 setup. This is due to the APs being forced to download different image versions when failing over to a secondary or tertiary controller, and joining back to their primary controller when it is available.

- At the time of the reset, if any AP is downloading the controller image, the scheduled reset is canceled. The following message appears with the reason why the scheduled reset was canceled:

```
%OSAPI-3-RESETSYSTEM_FAILED: osapi_task.c:4458 System will not reset
as software is being upgraded.
```

- Predownloading a 7.2 or later version of image on a Cisco Aironet 1240 access point is not supported when upgrading from a previous controller release. If predownloading is attempted to the Cisco Aironet 1240 access point, the AP gets disconnected.
- There are two images for the1550 Mesh AP - 1550 with 64 MB memory and 1550 with 128 MB memory. During the controller upgrade to 7.6 and higher versions, the AP images are downloaded and there are two reboots.
- If you upgrade from a release that is prior to Release 7.5 directly to Release 7.6.X or a later release, the predownload process on Cisco AP2600 and AP3600 fails. After the controller is upgraded to Release 7.6.X or a later release, the new image is loaded on Cisco AP2600 and AP3600. After the upgrade to a Release 7.6.X image, the predownload functionality works as expected. The predownload failure is only a one-time failure.
- If you upgrade from 8.2 to 8.4 release, the predownload process on Cisco AP1700, AP2700, or AP3700 fails with the following error message:

  ```
  Not enough free space to download.
  ```

  After the controller is reloaded with 8.4, the backup image version still shows up as 3.0.
- If an AP is in the process of downloading a software image, the status of the download is not shown on the controller CLI. During the image download process, any configuration performed on the AP via the controller CLI is not applied. Therefore, we recommend that you do not perform any configuration on the AP via the controller CLI if an image download on the AP is in progress.

Predownloading an Image to Access Points—Global Configuration (GUI)

To predownload an image to the APs, you must perform the following steps after upgrading your controller software image and before you reboot the controller for the new image to take effect.

Step 1 To configure the predownloading of access point images globally, choose **Wireless** > **Access Points** > **Global Configuration** to open the **Global Configuration** page.

Step 2 In the **AP Image Pre-download** section, perform one of the following:

- To instruct all the access points to predownload a primary image from the controller, click **Download Primary** under the AP Image Pre-download.
- To instruct all the access points to swap their primary and backup images, click **Interchange Image**.
- To download an image from the controller and store it as a backup image, click **Download Backup**.
- To terminate the predownload operation, click **Abort Predownload**.

Step 3 Click **OK**.

Step 4 Click **Apply**.

Predownloading an Image to Access Points (CLI)

To predownload an image to the APs, you must perform the following steps after upgrading your controller software image and before you reboot the controller for the new image to take effect.

Step 1 Specify APs that will receive the predownload image by entering one of these commands:

- Specify APs for predownload by entering this command:

  config ap image predownload {**primary** | **backup**} {*ap_name* | **all**}

  The primary image is the new image; the backup image is the existing image. APs always boot with the primary image.

- Swap an AP's primary and backup images by entering this command:

  config ap image swap {*ap_name* | **all**}

- Display detailed information on APs specified for predownload by entering this command:

  show ap image {**all** | *ap-name*}

The output lists APs that are specified for predownloading and provides for each AP, primary and secondary image versions, the version of the predownload image, the predownload retry time (if necessary), and the number of predownload attempts. The output also includes the predownload status for each device. The status of the APs is as follows:

- None—The AP is not scheduled for predownload.
- Predownloading—The AP is predownloading the image.
- Not supported—The AP (1120, 1230, and 1310) does not support predownloading.
- Initiated—The AP is waiting to get the predownload image because the concurrent download limit has been reached.
- Failed—The AP has failed 64 predownload attempts.
- Complete—The AP has completed predownloading.

Step 2 Set a reboot time for the controller and the APs.

Use one of these commands to schedule a reboot of the controller and APs:

- Specify the amount of time delay before the devices reboot by entering this command:

  reset system in *HH*:*MM*:*SS* **image** {**swap** | **no-swap**} **reset-aps** [**save-config**]

  Note The **swap** operand in the **reset** command will result in the swapping of the primary and backup images on both the controller and the AP and sets the default flag on the next controller reboot.

  The controller sends a reset message to all joined APs, and then the controller resets.

- Specify a date and time for the devices to reboot by entering this command:

  reset system at *YYYY-MM-DD HH*:*MM*:*SS* **image** {**swap** | **no-swap**} **reset-aps** [**save-config**]

  The controller sends a reset message to all joined APs, and then the controller resets.

  Note The **swap** operand in the **reset** command will result in the swapping of the primary and backup images on both the controller and the AP.

- (Optional) Set up an SNMP trap message that announces the upcoming reset by entering this command:

reset system notify-time *minutes*

The controller sends the announcement trap *the configured number of minutes* before the reset.

- Cancel the scheduled reboot by entering this command:

  reset system cancel

  Note If you configure reset times and then use the **config time** command to change the system time on the controller, the controller notifies you that any scheduled reset times will be canceled and must be reconfigured after you set the system time.

Use the **show reset** command to display scheduled resets.

Information similar to the following appears:

```
System reset is scheduled for Apr 08 01:01:01 2010.
Current local time and date is Apr 07 02:57:44 2010.
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

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 a Login Banner File

You can download a login banner file using either the GUI or the CLI. The login banner is the text that appears on the page before user authentication when you access the controller GUI or CLI using Telnet, SSH, or a console port connection.

You save the login banner information as a text (*.txt) file. The text file cannot be larger than 1296 characters and cannot have more than 16 lines of text.

Note The ASCII character set consists of printable and nonprintable characters. The login banner supports only printable characters.

Here is an example of a login banner:

```
Welcome to the Cisco Wireless Controller!
Unauthorized access prohibited.
Contact sysadmin@corp.com for access.
```

Follow the instructions in this section to download a login banner to the controller through the GUI or CLI. However, before you begin, make sure that you have a TFTP or FTP server available for the file download. Follow these guidelines when setting up a TFTP or FTP server:

- If you are downloading through the service port, the TFTP or FTP 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 or FTP server can be on the same or a different subnet because the distribution system port is routable.

Downloading a Login Banner File (GUI)

Step 1 Copy the login banner file to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the **Download File to Controller** page.

Step 3 From the **File Type** drop-down list, choose **Login Banner**.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 5 In the **IP Address** field, enter the IP address of the server type you chose in Step 4.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work correctly without any adjustment. However, you can change these values.

Step 6 (Optional) 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 login banner file.

Step 8 In the **File Name** field, enter the name of the login banner text (*.txt) file.

Step 9 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the FTP server.
b) In the **Server Login Password** field, enter the password to log into the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the login banner file to the controller. A message appears indicating the status of the download.

Downloading a Login Banner File (CLI)

Step 1 Log onto the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Download the controller login banner by entering this command:

transfer download datatype login-banner

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

transfer download serverip server-ip-address

Step 5 Specify the name of the config file to be downloaded by entering this command:

transfer download path server-path-to-file

Step 6 Specify the directory path of the config file by entering this command:

transfer download filename *filename.txt*

Step 7 (Optional) If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands:

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 9 View the download settings by entering the **transfer download start** command. Enter **y** when prompted to confirm the current settings and start the download process.

Clearing the Login Banner (GUI)

Step 1 Choose **Commands** > **Login Banner** to open the Login Banner page.

Step 2 Click **Clear**.

Step 3 When prompted, click **OK** to clear the banner.

To clear the login banner from the controller using the controller CLI, enter the **clear login-banner** command.

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 MIC device certificate.

Note For more information about configuring local EAP, see the "Configuring Local EAP" section.

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 or FTP server available for the certificate download. Follow these guidelines when setting up a TFTP or FTP server:

- If you are downloading through the service port, the TFTP or FTP 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 or FTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

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

Note Clients using Microsoft Windows 10 with default (zero-touch config) supplicant fail to connect to controller when there is no CA certificate to validate the server certificate. This is because the supplicant does not pop up a window to accept the server certificate and silently rejects the 802.1X authentication. Therefore, we recommend that you do either of the following:

- Manually install a third-party CA certificate on the AAA server, which the clients using Microsoft Windows 10 can trust.
- Use any other supplicant, such as Cisco AnyConnect, which pops up a window to trust or not trust the server certificate. If you accept the trust certificate, then the client is authenticated.

Downloading Device Certificates (GUI)

Step 1 Copy the device certificate to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

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

Step 4 In the Certificate Password text box, enter the password that was used to protect the certificate.

Step 5 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 6 In the IP Address text box, enter the IP address of the server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 7 Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

Step 8 In the File Path text box, enter the directory path of the certificate.

Step 9 In the File Name text box, enter the name of the certificate.

Step 10 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log into the FTP server.
b) In the Server Login Password text box, enter the password to log into the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 11 Click **Download** to download the device certificate to the controller. A message appears indicating the status of the download.

Step 12 After the download is complete, choose **Commands** > **Reboot** > **Reboot**.

Step 13 If prompted to save your changes, click **Save and Reboot**.

Step 14 Click **OK** to confirm your decision to reboot the controller.

Downloading Device Certificates (CLI)

Step 1 Log onto the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the type of the file to be downloaded by entering this command:

transfer download datatype eapdevcert

Step 4 Specify the certificate's private key by entering this command:

transfer download certpassword *password*

Step 5 Specify the IP address of the TFTP or FTP server by entering this command:

transfer download serverip *server-ip-address*

Step 6 Specify the name of the config file to be downloaded by entering this command:

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

Step 7 Specify the directory path of the config file by entering this command:

transfer download filename *filename.pem*

Step 8 (Optional) If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 9 If you are using an FTP server, enter these commands (skip this step if you are not using FTP server):

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 10 View the updated settings by entering the **transfer download start** command. Answer **y** when prompted to confirm the current settings and start the download process.

Step 11 Reboot the controller by entering this command:

reset system

Uploading Device Certificates

Uploading Device Certificates (GUI)

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **IPSec Device Certificate**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 4 In the IP Address text box, enter the IP address of the server.

Step 5 In the File Path text box, enter the directory path of the certificate.

Step 6 In the File Name text box, enter the name of the certificate.

Step 7 If you are using an FTP server, follow these steps (skip this step if you are not using FTP server):

a) In the Server Login Username text box, enter the username to log on to the FTP server.
b) In the Server Login Password text box, enter the password to log on to the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21. For SFTP, the default value is 22.

Step 8 Click **Upload** to upload the CA certificate from the controller. A message appears indicating the status of the upload.

Step 9 After the upload is complete, choose **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.

Uploading Device Certificates (CLI)

Step 1 Log on to the controller CLI.

Step 2 Specify the type of the file to be uploaded by entering this command:

transfer upload datatype ipsecdevcert

Step 3 Specify the transfer mode used to upload the file by entering this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

transfer upload serverip *server-ip-address*

Step 5 Specify the directory path of the file by entering this command:

transfer upload path *server-path-to-file*

Step 6 Specify the name of the file to be uploaded by entering this command:

transfer upload filename *filename*

Step 7 If you are using an FTP server, enter these commands (skip this step if you are not using FTP server):

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter for is 21. For SFTP, the default value is 22.

Step 8 View the updated settings by entering the **transfer upload start** command. Answer y when prompted to confirm the current settings and start the upload process.

Step 9 Reboot the controller by entering the **reset system** command.

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 want to use your own vendor-specific CA certificate, it must be downloaded to the controller.

Note For more information about configuring local EAP, see the "Configuring Local EAP" section.

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

- If you are downloading through the service port, the TFTP or FTP 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 or FTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

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

Download CA Certificates (GUI)

Step 1 Copy the CA certificate to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the File Type drop-down list, choose **Vendor CA Certificate**.

Step 4 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 5 In the IP Address text box, enter the IP address of the server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 6 Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

Step 7 In the File Path text box, enter the directory path of the certificate.

Step 8 In the File Name text box, enter the name of the certificate.

Step 9 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log on to the FTP server.
b) In the Server Login Password text box, enter the password to log on to the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the CA certificate to the controller. A message appears indicating the status of the download.

Step 11 After the download is complete, choose **Commands** > **Reboot** > **Reboot**.

Step 12 If prompted to save your changes, click **Save and Reboot**.

Step 13 Click **OK** to confirm your decision to reboot the controller.

Downloading CA Certificates (CLI)

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:

transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the type of the file to be downloaded by entering this command:

transfer download datatype eapdevcert

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

transfer download serverip *server-ip-address*

Step 5 Specify the directory path of the config file by entering this command:

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

Step 6 Specify the name of the config file to be downloaded by entering this command:

transfer download filename *filename*

Step 7 (Optional) If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands (skip this step if you are not using FTP server):

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 9 View the updated settings by entering the **transfer download start** command. Answer y when prompted to confirm the current settings and start the download process.

Step 10 Reboot the controller by entering the **reset system** command.

Uploading CA Certificates

Uploading CA Certificates (GUI)

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **IPSec CA Certificate**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 4 In the **IP Address** field, enter the IP address of the server.

Step 5 In the **File Path** field, enter the directory path of the certificate.

Step 6 In the **File Name** field, enter the name of the certificate.

Step 7 (Optional) If you are using an FTP server, follow these steps (skip this step if you are not using FTP server):

a) In the **Server Login Username** field, enter the username to log on to the FTP server.
b) In the **Server Login Password** field, enter the password to log on to the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21. For SFTP, the default value is 22.

Step 8 Click **Upload** to upload the CA certificate from the controller. A message appears indicating the status of the upload.

Step 9 If prompted to save your changes, click **Save**.

Uploading CA Certificates (CLI)

Step 1 Log on to the controller CLI.

Step 2 Specify the type of the file to be uploaded by entering this command:

transfer upload datatype ipseccacert

Step 3 Specify the transfer mode used to upload the file by entering this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:

transfer upload serverip *server-ip-address*

Step 5 Specify the directory path of the file by entering this command:

transfer upload path *server-path-to-file*

Step 6 Specify the name of the file to be uploaded by entering this command:

transfer upload filename *filename*

Step 7 (Optional) If you are using an FTP server, enter these commands (skip this step if you are not using FTP server):

- **transfer upload username** *username*

- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21. For SFTP, the default value is 22.

Step 8 View the updated settings by entering the **transfer upload start** command. Answer y when prompted to confirm the current settings and start the upload process.

Step 9 Reboot the controller by entering the **reset system** command.

Uploading PACs for EAP-FAST

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.

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 or FTP server available for the PAC upload. Follow these guidelines when setting up a TFTP or FTP server:

- If you are uploading through the service port, the TFTP or FTP 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 or FTP server can be on the same or a different subnet because the distribution system port is routable.

This section contains the following subsections:

Uploading PACs (GUI)

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, 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 of days for the PAC to remain valid. The default setting is zero (0).

Step 5 In the **Password** and **Confirm Password** text boxes, enter a password to protect the PAC.

Step 6 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 7 In the **IP Address (IPv4/IPv6)** field, enter the IPv4/IPv6 address of the server.

Step 8 In the **File Path** field, enter the directory path of the PAC.

Step 9 In the **File Name** field, enter the name of the PAC file. PAC files have a .pac extension.

Step 10 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the FTP server.
b) In the **Server Login Password** field, enter the password to log into the FTP server.

c) In the **Server Port Number** field, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 11 Click **Upload** to upload the PAC from the controller. A message appears indicating the status of the upload.

Step 12 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 PACs (CLI)

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to upload the config file by entering this command:

transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 3 Upload a Protected Access Credential (PAC) by entering this command:

transfer upload datatype pac

Step 4 Specify the identification of the user by entering this command:

transfer upload pac *username validity password*

Step 5 Specify the IP address of the TFTP or FTP server by entering this command:

transfer upload serverip *server-ip-address*

Note The server supports both, IPv4 and IPv6.

Step 6 Specify the directory path of the config file by entering this command:

transfer upload path *server-path-to-file*

Step 7 Specify the name of the config file to be uploaded by entering this command:

transfer upload filename *manual*.pac.

Step 8 If you are using an FTP server, enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 9 View the updated settings by entering the **transfer upload start** command. Answer y when prompted to confirm the current settings and start the upload process.

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.

Backing Up and Restoring Controller Configuration

We recommend that you upload your controller's configuration file to a server to back it up. If you lose your configuration, you can then download the saved configuration to the controller.

Caution Do not download a configuration file to your controller directly that was uploaded from a different controller platform. For example, a Cisco 5508 controller does not support the configuration file from a Cisco 2504 controller. To properly convert the configuration files from one controller platform to another, use the WLC Config Converter tool available at https://cway.cisco.com/tools/WirelessConfigConverter/.

Note While controller configuration backup is in progress, we recommend you do not initiate any new configuration or modify any existing configuration settings. This is to avoid corrupting the configuration file.

Follow these guidelines when working with configuration files:

- Any CLI with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup. A configuration may be rejected if the validation fails. A configuration may fail if you have an invalid CLI. For example, if you have a CLI where you try to configure a WLAN without adding appropriate commands to add the WLAN.
- A configuration may be rejected if the dependencies are not addressed. For example, if you try to configure dependent parameters without using the add command. The XML validation may succeed but the configuration download infrastructure will immediately reject the configuration with no validation errors.
- An invalid configuration can be verified by using the **show invalid-config** command. The **show invalid-config** command reports the configuration that is rejected by the controller either as part of download process or by XML validation infrastructure.

  Note You can also read and modify the configuration file via a text editor, to correct any incorrect configuration commands. After you are done, you can save the changes and once again try the configuration download to the controller in question.

- A wireless client that connects to the controller when Management over Wireless has been enabled can still conduct an upgrade using the newer HTTP transfer method.

Uploading Configuration Files

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

Uploading the Configuration Files (GUI)

Step 1 Choose **Commands** > **Upload File** to open the **Upload File from Controller** page.

Step 2 From the **File Type** drop-down list, choose **Configuration**.

Step 3 (Optional) Encrypt the configuration file by checking the **Configuration File Encryption** check box and entering the encryption key in the **Encryption Key** field.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 5 In the **IP Address** field, enter the IP address of the server.

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.

Step 8 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the FTP server.
b) In the **Server Login Password** field, enter the password to log into the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 9 Click **Upload** to upload the configuration file to the server. A message appears indicating the status of the upload. If the upload fails, repeat this procedure and try again.

Uploading the Configuration Files (CLI)

Step 1 Specify the transfer mode used to upload the configuration file by entering this command:
transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 2 Specify the type of file to be uploaded by entering this command:
transfer upload datatype config

Step 3 (Optional) Encrypt the configuration file by entering these commands:

- **transfer encrypt enable**
- **transfer encrypt set-key** *key*, where *key* is the encryption key used to encrypt the file.

Step 4 Specify the IP address of the server by entering this command:
transfer upload serverip *server-ip-address*

Step 5 Specify the directory path of the configuration file by entering this command:
transfer upload path *server-path-to-file*

Step 6 Specify the name of the configuration file to be uploaded by entering this command:
transfer upload filename *filename*

Step 7 If you are using an FTP server, enter these commands to specify the username and password used to log into the FTP server and the port number through which the upload occurs:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 8 Initiate the upload process by entering this command:

transfer upload start

Step 9 When prompted to confirm the current settings, answer **y**.

Information similar to the following appears:

```
Mode..................................... TFTP
TFTP Server IP........................... 224.0.0.1
TFTP Path................................ Config/
TFTP Filename............................ AS_5520_x_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 this procedure and try again.

Downloading Configuration Files

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

Downloading the Configuration Files (GUI)

Step 1 Choose **Commands** > **Download File** to open the **Download File to Controller** page.

Step 2 From the **File Type** drop-down list, choose **Configuration**.

Step 3 If the configuration file is encrypted, check the **Configuration File Encryption** check box and enter the encryption key used to decrypt the file in the **Encryption Key** field.

Note The key that you enter here should match the one entered during the upload process.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP**

Step 5 In the **IP Address** field, enter the IP address of the server.

If you are using a TFTP server, the default values of 10 retries and 6 seconds for the **Maximum Retries** and **Timeout** fields should work correctly without any adjustment. However, you can change these values.

Step 6 (Optional) 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 7 In the **File Path** field, enter the directory path of the configuration file.

Step 8 In the **File Name** field, enter the name of the configuration file.

Step 9 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** field, enter the username to log into the FTP server.
b) In the **Server Login Password** field, enter the password to log into the FTP server.
c) In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 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 this procedure and try again.

Downloading the Configuration Files (CLI)

Note The controller does not support incremental configuration downloads. The configuration file contains all mandatory commands (all interface address commands, mgmtuser with read-write permission commands, and interface port or LAG enable or disable commands) required to successfully complete the download. For example, if you download only the **config time ntp server** *index server_address* command as part of the configuration file, the download fails. Only the commands present in the configuration file are applied to the controller, and any configuration in the controller prior to the download is removed.

Step 1 Specify the transfer mode used to download the configuration file by entering this command:
transfer download mode {**tftp** | **ftp** | **sftp**}

Step 2 Specify the type of file to be downloaded by entering this command:
transfer download datatype config

Step 3 If the configuration file is encrypted, enter these commands:

- **transfer encrypt enable**
- **transfer encrypt set-key** *key*, where *key* is the encryption key used to decrypt the file.

Note The key that you enter here should match the one entered during the upload process.

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:
transfer download serverip *server-ip-address*

Step 5 Specify the directory path of the configuration file by entering this command:
transfer download path *server-path-to-file*

Step 6 Specify the name of the configuration file to be downloaded by entering this command:
transfer download filename *filename*

Step 7 (Optional) If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands to specify the username and password used to log into the FTP server and the port number through which the download occurs:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 9 View the updated settings by entering this command:

transfer download start

Step 10 When prompted to confirm the current settings and start the download process, answer **y**.

Information similar to the following appears:

```
Mode............................................. TFTP
TFTP Server IP................................... 224.0.0.1
TFTP Path........................................ Config/
TFTP Filename.................................... AS_5520_x_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 this procedure and try again.

Saving Configurations

Controllers contain two types of memory: volatile RAM and NVRAM. At any time, you can save the configuration changes from active volatile RAM to nonvolatile RAM (NVRAM). You are prompted to save your configuration automatically whenever you initiate a reboot of the controller or log out of a GUI or a CLI session. The following are some examples of the corresponding commands:

- **save config**—Saves the configuration from volatile RAM to NVRAM without resetting the controller.
- **reset system**—Prompts you to confirm that you want to save configuration changes before the controller reboots.
- **logout**—Prompts you to confirm that you want to save configuration changes before you log out.

Editing Configuration Files

When you save the controller's configuration, the controller stores it in XML format in flash memory. Controller software release 5.2 or later releases enable you to easily read and modify the configuration file by converting it to CLI format. When you upload the configuration file to a TFTP/FTP/SFTP server, the controller initiates the conversion from XML to CLI. You can then read or edit the configuration file in a CLI format on the server. When you are finished, you download the file back to the controller, where it is reconverted to an XML format and saved.

Step 1 Upload the configuration file to a TFTP/FTP/SFTP server by performing one of the following:

- Upload the file using the controller GUI.
- Upload the file using the controller CLI.

Step 2 Read or edit the configuration file on the server. You can modify or delete existing CLI commands and add new CLI commands to the file.

Note To edit the configuration file, you can use your text editor of choice such as Notepad or Wordpad on Windows platforms, VI editor on Linux, and so forth.

Step 3 Save your changes to the configuration file on the server.

Step 4 Download the configuration file to the controller by performing one of the following:

- Download the file using the controller GUI.
- Download the file using the controller CLI.

The controller converts the configuration file to an XML format, saves it to flash memory, and then reboots using the new configuration. CLI commands with known keywords and proper syntax are converted to XML while improper CLI commands are ignored and saved to flash memory. Any CLI commands that have invalid values are replaced with default values. To see any ignored commands or invalid configuration values, enter this command:

show invalid-config

Note You cannot execute this command after the **clear config** or **save config** command.

Step 5 If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP or FTP server for analysis. To do so, perform one of the following:

- Upload the invalid configuration using the controller GUI. Follow the instructions in the Uploading Configuration Files (GUI) section but choose **Invalid Config** from the **File Type** drop-down list in *Step 2* and skip *Step 3*.
- Upload the invalid configuration using the controller CLI. Follow the instructions in the Uploading Configuration Files (CLI) section but enter the transfer **upload datatype invalid-config command** in *Step 2* and skip *Step 3*.

Step 6 The controller does not support the uploading and downloading of port configuration CLI commands. If you want to configure the controller ports, enter these commands:

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}—Enables or disables the up and down link traps for a specific controller port or for all ports.

- **config port adminmode** {*port* | **all**} {**enable** | **disable**}—Enables or disables the administrative mode for a specific controller port or for all ports.

Step 7 Save your changes by entering this command:

save config

Clearing the Controller Configuration

Step 1 Clear the configuration by entering this command:

clear config

Enter **y** at the confirmation prompt to confirm the action.

Step 2 Reboot the system by entering this command:

reset system

Enter **n** to reboot without saving configuration changes. When the controller reboots, the configuration wizard starts automatically.

Step 3 Follow the instructions in the Configuring the Controller-Using the Configuration Wizard section to complete the initial configuration.

Erasing the Controller Configuration

Step 1 Reset the configuration by entering this command:

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, restore the factory-default settings by entering this command:

recover-config

The controller reboots and the configuration wizard starts automatically.

Step 3 Follow the instructions in the Configuring the Controller-Using the Configuration Wizard section 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.