Managing Configuration

- Resetting the Cisco WLC to Default Settings, page 1
- Saving Configurations, page 2
- Editing Configuration Files, page 3
- Clearing the Controller Configuration, page 4
- Erasing the Controller Configuration, page 4
- Resetting the Controller, page 4
- Transferring Files to and from a Controller, page 5

Resetting the Cisco WLC to Default Settings

Information About Resetting the Controller to Default Settings

You can return the controller to its original configuration by resetting the controller to factory-default settings.

Resetting the Controller to Default Settings (GUI)

Step 1 Start your Internet browser.

Step 2 Enter the controller IP address in the browser address line and press **Enter**. An Enter Network Password dialog box appears.

Step 3 Enter your username in the User Name text box. The default username is *admin*.

Step 4 Enter the wireless device password in the Password text box and press **Enter**. The default password is *admin*.

Step 5 Choose **Commands** > **Reset to Factory Default**.

Step 6 Click **Reset**.

Step 7 When prompted, confirm the reset.

Step 8 Reboot the controller without saving the configuration.

Step 9 Use the configuration wizard to enter configuration settings. See the Configuring the Controller- Using the Configuration Wizard section section for more information.

Resetting the Controller to Default Settings (CLI)

Step 1 Enter the **reset system** command. At the prompt that asks whether you need to save changes to the configuration, enter **N**. The unit reboots.

Step 2 When you are prompted for a username, enter the **recover-config** command to restore the factory-default configuration. The controller reboots and displays this message:

```
Welcome to the Cisco WLAN Solution Wizard Configuration Tool
```

Step 3 Use the configuration wizard to enter configuration settings. See the Configuring the Controller- Using the Configuration Wizard section for more information.

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 nonvolatile RAM (NVRAM) using one of these 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 either Notepad or WordPad on Windows or the VI editor on Linux.

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.

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:

Backing Up and Restoring Cisco WLC Configuration

We recommend that you upload your Cisco WLC'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.

Note We recommend that you do not download a configuration file to your Cisco WLC that was uploaded from a different Cisco WLC platform. For example, a Cisco 5508 Controller does not support the configuration file from a Cisco 2504 Controller, and a Cisco 5520 WLC does not support the configuration file from a Cisco 5508 WLC.

Note While Cisco WLC 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.

- The FTP or the TFTP servers for transfer of configuration, image, and so on, must be reachable over a wired connection. The transfer cannot be performed over one of the wireless clients of the Cisco WLC. If you try to use a wireless client of the Cisco WLC, you are prompted with a system message saying that the server is not reachable. However, if you use a wireless client that is associated with another Cisco WLC, the FTP or the TFTP servers are reachable.

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 Encrypt the configuration file by selecting the **Configuration File Encryption** check box and entering the encryption key in the Encryption Key text box.

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.

Step 6 In the File Path text box, enter the directory path of the configuration file.

Step 7 In the File Name text box, 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 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 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 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................................... 10.10.10.4
TFTP Path........................................ Config/
TFTP Filename.................................... AS_4402_4_2_55_8_Config.xml
Data Type........................................ Config File
Encryption....................................... Disabled

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

Are you sure you want to start? (y/N) Y
File transfer operation completed successfully.
```

If the upload fails, repeat 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, select the **Configuration File Encryption** check box and enter the encryption key used to decrypt the file in the Encryption Key text box.

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** (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 configuration file in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the configuration file in the Timeout text box.

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

Step 8 In the File Name text box, 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 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 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 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.................................. 10.10.10.4
TFTP Path....................................... Config/
TFTP Filename................................... AS_4402_4_2_55_8_Config.xml
Data Type....................................... Config File
Encryption...................................... Disabled

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

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

File transfer operation completed successfully.
```

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

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.
- 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 Clearing the controller configuration does not remove the login banner. See the Clearing the Login Banner (GUI) section for information about clearing the login banner using the controller GUI or CLI.

Note The controller can have only one login banner file. If you download another login banner file to the controller, the first login banner file is overwritten.

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** (available in 7.4 and later releases)

Step 5 In the IP Address text box, 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 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 login banner file.

Step 8 In the File Name text box, 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 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 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 into 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 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.

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.

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.
- 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.

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** text box, enter the name of the user who will use the PAC.

Step 4 In the **Validity** text box, 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)** text box, enter the IPv4/IPv6 address of the server.

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

Step 9 In the **File Name** text box, 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** 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 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.