Managing Configuration

Resetting the Controller to Default Settings

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

This section contains the following subsections:

Resetting the Controller to Default Settings (GUI)

Procedure

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.

Resetting the Controller to Default Settings (CLI)

Procedure

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.

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.

Procedure

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

Related Topics

Uploading Configuration Files, on page 6
Downloading Configuration Files, on page 8

Clearing the Controller Configuration

Procedure

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.

Restoring Passwords

Before you begin

Ensure that you are accessing the controller CLI through the console port.

Procedure

Step 1 After the controller boots up, enter **Restore-Password** at the User prompt.

Note For security reasons, the text that you enter does not appear on the controller console.

Step 2 At the Enter User Name prompt, enter a new username.

Step 3 At the Enter Password prompt, enter a new password.

Step 4 At the Re-enter Password prompt, reenter the new password. The controller validates and stores your entries in the database.

Step 5 When the User prompt reappears, enter your new username.

Step 6 When the Password prompt appears, enter your new password. The controller logs you in with your new username and password.

Rebooting 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 the **reset system** command. At the confirmation prompt, press **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 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.

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.

Related Topics

Editing Configuration Files, on page 2

Uploading the Configuration Files (GUI)

Procedure

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)

Procedure

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.

Related Topics

Editing Configuration Files, on page 2

Downloading the Configuration Files (GUI)

Procedure

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.

Procedure

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.

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)

Procedure

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)

Procedure

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)

Procedure

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 Diagnostic Support Bundle

Some commonly collected diagnostic information of various types can be made available in a single bundle that you can upload from controller. The diagnostic information that you can include in the bundle are core files, crash files, **show run-config** and **config** commands, msglog, and traplog.

Uploading Diagnostic Support Bundle (GUI)

Procedure

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

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

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

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

Step 4 In the **IP Address (IPv4/IPv6)** field, enter the IPv4/IPv6 address of the server.

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

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

Step 7 If you are using an FTP or SFTP server, follow these steps:

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

Step 8 Click **Upload** to upload the diagnostic bundle from the controller.

Uploading Diagnostic Support Bundle (CLI)

Procedure

Step 1 Log on to the controller CLI.

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

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

Step 3 Upload the diagnostic support bundle by entering this command:

transfer upload datatype support-bundle

Step 4 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 5 Specify the directory path of the bundle file by entering this command:

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

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

transfer upload filename *file-name*

Step 7 If you are using an FTP or SFTP 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 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.

Password Encryption

Controllers encrypt most of the passwords that are stored in the configuration file, using Advanced Encryption Standard-128 (AES-128). The encryption is hardcoded. To choose between the encrypted or the plain text method of storing passwords, use this command:

config switchconfig secret-obfuscation {**enable** | **disable**}

With secret obfuscation in enabled state, all the secrets from plain text are converted to encrypted values by using the hard-coded encryption key. This type of encryption is called type-7 encryption. If you disable secret obfuscation, all the secrets are converted from encrypted values to plain text passwords by using hard-coded encryption key. This type of encryption is called type-0 encryption. Secret obfuscation is enabled by default.

A disadvantage with type-7 encryption is that the passwords can be recovered from the hard-coded key value. There is a need for a stronger encryption method in which the key value can be configured. After you configure secret obfuscation, you can provide an extra level of encryption method that is called type-6. The type-6 method of encryption takes the configurable key along with AES-128 and stores the passwords. This stores all the secrets along with the configurable master key. You can change the key value from time to time to avoid decryption of passwords.

By default, type-6 encryption and password encryption are disabled.

The master key is encrypted with a device certificate private key. The master key length should be between 16 to 127 alphanumeric characters. We recommend that you use at least three of the following four classes in the password:

- Lowercase letters
- Uppercase letters
- Digits
- Special characters

The following applications use the type-6 encryption method:

- Local Net user
- RADIUS (Authentication, Accounting, and DNS)
- TACACS+ (Authentication, Accounting, Authorization, and DNS)
- IPSec secrets
- LDAP
- Local EAP
- SXP
- WPA2 PSK
- Local management user

This section contains the following subsections:

Guidelines and Restrictions for Password Encryption

- It is not possible to roll back configurations that contain type-6 encrypted passwords.
- You can enable the type-6 encryption only after configuring the master key.
- It is not possible to modify a master key if type-6 encryption method is enabled. You must disable the type-6 encryption method and then modify the master key.
- To downgrade from a release that supports this feature to an earlier release that does not support it, we recommend that you decrypt all type-6 passwords to type-7, or disable password encryption.
- To move the configuration from one device to another device, we recommend that you do either of the following:
    - Decrypt the configuration file before porting it to another device.

- Configure the same master key on the device to which the configuration is to be applied.

Note You will be prompted with a warning message to ensure that the same master key is applied on the controller where the configuration is downloaded with type-6 encryption enabled. If not, you will have to clear the configuration to recover the controller.

- If the stored encrypted key is not readable, a print is made available on the console or the CLI session. You can use the print to initiate a clear configuration action to recover the controller.
- Configuration for type-6 method is not available for the Cisco WLAN Express method of setting up controllers.
- The type-6 encryption key configuration always follows a strong password check.

Note You can perform a check for strong passwords by entering the **config switchconfig strong-pwd** command.

- For FlexConnect group local users: It is not possible to enable type-6 encryption through modification in the configuration file. That is, uploading type-7 encrypted data, enabling type-6 via the CLI, and then downloading the configuration file again is not supported.

Configuring Password Encryption (CLI)

Procedure

Step 1 Enable secret obfuscation by entering this command:

config switchconfig secret-obfuscation enable

Step 2 Configure the master key that is used to encrypt all the secrets by entering this command:

config switchconfig password-encryption key *ascii-value*

The master key can range between 16 to 127 alphanumeric characters.

Step 3 Enable type-6 password encryption with the master key by entering this command:

config switchconfig password-encryption enable

Step 4 View the status of type-6 encryption by entering this command:

show switchconfig