Commands Tab

This tab on the menu bar enables you to access the controller operating system software management commands. Use the left navigation pane to access the operating system software management parameters.

You can access the following pages from the Commands tab:

- Download File to Controller
- Upload File from Controller
- System Reboot
- Config Boot
- Scheduled Reboot
- Reset to Factory Default
- Set Time
- Login Banner
- Redundancy

You can find controller configuration information in the following sections:

- Using the Configuration Wizard
- Collect the Initial Configuration Settings
- Connecting Your Web Browser to a Controller
- Configuration Wizard System Information
- Service Interface Configuration
- Management Interface Configuration
- Miscellaneous Configuration
- Virtual Interface Configuration
- WLAN Policy Configuration
- RADIUS Server Configuration
- 802.11 Configuration
- Completing the Configuration Wizard

Download File to Controller

Choose **COMMANDS > Download File** to navigate to this page.

This page enables you to download and install new controller operating system software (code), a signature file, or a configuration file to your controller from a local TFTP (trivial file transfer protocol), FTP server, SFTP server, or over HTTP.

Note Follow these guidelines when setting up a TFTP server:

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

To download a file to the controller, follow these steps:

Step 1 From the File Type drop-down list, choose the kind of file that you want to download from the following options:

- Code—You can download an executable image.
- Configuration—If you choose Configuration, also enter the configuration file encryption key that enables the data in the file to be encrypted when the file is downloaded.
- Signature File—A standard signature file exists on the controller by default. You can upload this signature file from the controller, or you can create a custom signature file and download it to the controller or modify the standard signature file to create a custom signature.

  If you are downloading a custom signature file (*.sig), copy it to the default directory on your TFTP server.
- Webauth Bundle—You can download a custom webauth bundle.
- Vendor Device Certificate—When you choose Vendor Device Certificate, also enter the certificate password that is used to protect the certificate.
- Vendor CA Certificate—You can download a vendor CA certificate.
- Login Banner—The login banner is the text that appears in the window before user authentication when you access the controller CLI using Telnet, SSH, or a console port connection. You save the login banner information as a text file (*.txt). The text file cannot be larger than 1296 characters and cannot have more than 16 lines of text.

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

  Note Clearing the controller configuration does not remove the login banner. See the Login Banner topic for information about clearing the login banner file.

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.

Step 2 From the Transfer Mode drop-down list, choose from the following options:

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

Step 3 If you selected **TFTP** from the **Transfer Mode** drop-down list, do the following:

a. In the IP Address (IPv4/IPv6) text box, enter the IPv4/IPv6 address of the TFTP server.

b. In the Maximum Retries text box, enter the maximum number of times the controller should attempt to download the signature file. The valid range is from 1 to 254; the default value is 10.

c. In the Timeout text box, enter the amount of time in seconds before the controller times out while attempting to download the signature file. The valid range is from 1 to 254; the default value is 6.

d. In the File Path text box, enter the file path on the server (default = /).

e. In the File Name text box, enter the name of the file to be transferred.

Note You cannot use special characters such as \ : * ? " < > | for the file path or a filename.

Step 4 If you selected **FTP** or **SFTP** from the **Transfer Mode** drop-down list, do the following:

a. In the IP Address (IPv4/IPv6) text box, enter the IPv4/IPv6 address of the FTP or SFTP server.

b. In the File Path text box, enter the file path on the server (default = /).

c. In the File Name text box, enter the name of the file to be transferred.

d. In the Server Login Username text box, enter the username to log in to the FTP or SFTP server.

e. In the Server Login Password text box, enter the password to log in to the FTP or SFTP server.

f. In the Server Port Number text box, enter the port number on the FTP or SFTP server through which the download occurs. The default value for the FTP server port is 21. The default value for the SFTP server port is 22.

Note The SFTP server must support SSHv2, else the file transfer will fail.

Step 5 If you selected **HTTP** from the **Transfer Mode** drop-down list, do the following:

a. Click **Choose File** and browse to the *.aes* file on the local computer to send to WLC.

Step 6 Click the **Download** button.

The controller downloads and installs the new controller operating system software. This process takes at least three minutes and overwrites your existing code and configuration.

Note You must reboot the controller after the new operating system software is installed.

Buttons

- Clear: Deletes the entries in the data fields.
- Download: Begins the download from the SFTP , FTP or TFTP server; you are prompted to continue.

Upload File from Controller

Choose **COMMANDS > Upload File** to navigate to this page.

This page enables you to upload files from your controller to a local SFTP , FTP or, TFTP server.

Note The SFTP server must support SSHv2, else the file transfer will fail.

You can upload the following files:

- Configuration file—See the Editing Configuration Files topic for information about editing configuration files. The following options are available:
  - Configuration
  - Event Log
  - Message Log
  - Trap Log
  - Crash File
  - Debug-File
  - Signature File
  - PAC (Protected Access Credential)—In the User text box, enter the name of the user who will use the PAC. In the Validity text box, enter the number days for the PAC to remain valid. The default setting is zero (0). In the Password and Confirm Password text boxes, enter a password to protect the PAC.
  - Radio Core Dump
  - Invalid Config—See the Configuration Files with Invalid CLI Commands topic for information about uploading the invalid configuration for analysis.
  - Packet Capture—When a Cisco 5500 Series Controller's data plane crashes, it stores the last 50 packets that the controller received in flash memory. This information can be useful in troubleshooting the crash. When a crash occurs, the controller generates a new packet capture file (*.pcap) file. You can upload the packet capture file from the controller. You can then use Wireshark or another standard packet capture tool to view and analyze the contents of the file.

Note Only Cisco 5500 Series Controllers generate packet capture files. This feature is not available on other controller platforms.

  - Watchdog Crash File
  - Panic Crash File

- Configuration File Encryption—Enable the Configuration File Encryption option and enter the encryption key. File encryption ensures that data is encrypted while uploading or downloading the controller configuration file through a TFTP, SFTP, or FTP server.
- Transfer Mode—Choose the transfer mode from the drop-down list. Available options include FTP, SFTP, and TFTP.

  If you chose TFTP from the Transfer Mode drop-down list, enter the IPv4/IPv6 address of the TFTP server, the file path on the server (default = /), and a name for the file you have selected for upload.

Note The TFTP server cannot run on the same computer as the Cisco Wireless Control System because the Cisco WCS or Cisco Prime Infrastructure and the TFTP server use the same communication port.

If you chose FTP or SFTP from the Transfer Mode drop-down list, enter the IPv4/IPv6 address of the FTP or SFTP server, the file path on the server (default = /), a name for the file you have selected for upload, the username to log in to the SFTP or FTP server, the password to log in to the SFTP or FTP server, and the port number on the SFTP or FTP server through which the download occurs (the default value for the FTP server port is 21, and the default value for the SFTP server port is 22).

When you click Upload, the selected file is uploaded to your TFTP, SFTP, or FTP server and is saved with the same name that you entered in the File Name field.

Editing Configuration Files

When you save the controller's configuration, the controller stores it in XML format in flash memory. When you upload the configuration file to a TFTP, SFTP, or FTP server, the controller converts the file from XML to CLI. You can then read, modify, delete, or add CLI commands to the configuration file in CLI format on the server.

Note To edit the configuration file, you can use either Notepad on Windows or the VI editor on Linux.

When you are finished, save your changes to the configuration file on the server and download the file back to the controller, where it is reconverted to XML format and saved.

Configuration Files with Invalid CLI Commands

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 the **show invalid-config** command on the controller CLI.

Note You can enter this command only before the **clear config** or **save config** command.

If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP, SFTP, or FTP server for analysis.

Buttons

- Clear: Deletes the entries in the data fields are deleted.
- Upload: Begins the file upload to the TFTP, SFTP, or FTP server; you are prompted to continue.

System Reboot

Choose **COMMANDS > Reboot** to navigate to this page.

This page enables you to restart the controller. You are prompted to save your configuration changes in the next page if you have not already saved configuration changes using the Save Configuration Administrative toolbar at the top right of your window.

Buttons

- Reboot: Restarts the controller. You are prompted for confirmation. See the System Reboot > Save? topic.

System Reboot > Save?

Choose **COMMANDS > Reboot** and then click **Reboot** to navigate to this page.

This page prompts you to restart the controller after saving your configuration changes or restart without saving.

Buttons

- Reboot: Restarts the controller after saving your existing applied changes. See the System Reboot > Confirm topic.

System Reboot > Confirm

Choose **COMMANDS > Reboot** and then click **Reboot** to navigate to this page.

This page enables you to confirm the restart of your controller after saving your configuration changes. All system connections are lost so you must open a new session and log back in to the controller.

Buttons

- Reboot: Restarts the controller.

Config Boot

Choose **Commands > Config Boot** to navigate to this page.

This page enables you to configure the primary and backup boot image for the controller.

General

The primary image uses the primary image version on the controller. The primary image is the active image. The backup image uses the backup image version on the controller.

Config Boot Image

Boot enables you to select the image that you want the controller to use while rebooting. You can choose one of the two options provided from the drop-down list: Primary or Backup. Depending on the option that you choose from the drop-down list, the controller takes that image as the active image while rebooting.

Buttons

- Apply: Saves the config boot input to the controller.

Scheduled Reboot

This topic describes how to schedule a reboot of the controller.

Reboot At

Choose **COMMANDS > Scheduled Reboot >Reboot At** and then click the **Reboot** button to navigate to this page.

This page enables you to schedule a reboot of the controller at a specific time. All system connections are lost so you must open a new session and log back into the controller.

You can schedule the following settings for a reboot:

- Current Time—Current time on the controller.
- Date—Date on which you want to schedule the reboot. You can choose the month by using the drop-down lists for the month and the year in the Year text box.
- Time—Time at which you want to schedule the reboot. You can choose the hour from the Hour drop-down list and enter the minutes and seconds in the text boxes provided.
- Image—Type of image that the controller must use when rebooting. The following options are available:
  - Normal—The controller reboots with the current available software image.
  - Interchange—The controller interchanges the software image with the backup image when rebooting.

Buttons

- Save and Reboot: Saves the controller configuration and reboot.
- Reboot without Save: Reboots the controller without saving the configuration.

Reboot In

Choose **COMMANDS > Scheduled Reboot >Reboot In** and click **Reboot** to navigate to this page.

This page enables you to schedule a reboot of the controller in a specific time duration from the current time. All system connections are lost so you must open a new session and log back into the controller.

- Time—Time at which you want to schedule the reboot by setting the hour from the Hour drop-down list and then you can enter the minutes and seconds in the text boxes provided.
- Image—Type of image that the controller must use when rebooting. The following options are available:
  - Normal—The controller reboots with the current available software image.
  - Interchange—The controller interchanges the software image with the backup image when rebooting.

Buttons

- Save and Reboot: Saves the controller configuration and reboot.
- Reboot without Save: Reboots the controller without saving the configuration.

Clear Reboot

Choose **COMMANDS > Scheduled Reboot > Clear Reboot** to navigate to this page.

This page enables you to cancel the scheduled reboot. The following information appears:

- Scheduled Reset Information—Scheduled reset information.
  - Current Time—Current time on the controller.
  - System Reset Time—System reset time.
- Reset System Notify-time—Reset system notification time.
  - Current reset system notify-time—Scheduled notification time (in minutes) before the traps are sent.
  - Notify Time—Notification time (in minutes) before the traps should be sent.

Buttons

- Clear: Clears the scheduled reset information.
- Apply: Applies the current settings.

Reset to Factory Default

Choose **COMMANDS > Reset to Factory Default** to navigate to this page.

This page enables you to reset the controller configuration to the factory default. Resetting the configuration overwrites all applied and saved configuration parameters. You are prompted for confirmation to reset the configuration.

All configuration data files are deleted, and upon reboot, the controller is restored to its original unconfigured state. Resetting the configuration removes all IP configuration and you need a serial connection to restore the base configuration.

Note After confirming the configuration removal, you must reboot the controller and choose **Reboot Without Saving**.

Buttons

- Reset: Returns the configuration to the factory default.

Set Time

Choose **COMMANDS > Set Time** to navigate to this page. This page enables you to configure the following settings for the time and date on the controller:

- Current Time—Current timestamp on the controller.
- Date—The date on the controller
  - Month
  - Day
  - Year
- Time
  - Hour
  - Minutes
  - Seconds
- Timezone
  - Delta—You cannot use this option on the controller GUI. However, if you do so on the controller CLI, the change is reflected in the Delta Hours and Mins fields on the controller GUI.
  - Location—When you choose a time zone that uses Daylight Saving Time (DST), the controller automatically sets its system clock to reflect the time change when DST occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

Login Banner

Choose **COMMANDS > Login Banner** to navigate to this page.

To clear the login banner from the controller, click **Clear**. At the prompt, click **OK** to clear the banner.

Redundancy

Choose **COMMANDS > Redundancy to configure the redundancy parameters and peer network routes:**

- To upload files from the peer controller to a local TFTP server, choose **COMMANDS > Redundancy > Upload Peer**.
- To reset the peer controller, choose **COMMANDS > Redundancy > Reset Peer**.

Redundancy > Upload Peer

Choose **COMMANDS > Redundancy > Upload Peer** to navigate to this page.

This page enables you to upload files from the peer controller to a local TFTP server.

You can upload the following files:

- Configuration file—See the Editing Configuration Files topic for information about editing configuration files. The following options are available:
  - Configuration
  - Event Log
  - Message Log
  - Trap Log
  - Crash File
  - Debug-File
  - Signature File
  - PAC (Protected Access Credential)—In the User text box, enter the name of the user who will use the PAC. In the Validity text box, enter the number days for the PAC to remain valid. The default setting is zero (0). In the Password and Confirm Password text boxes, enter a password to protect the PAC.
  - Radio Core Dump
  - Invalid Config—See the Configuration Files with Invalid CLI Commands topic for information about uploading the invalid configuration for analysis.
  - Packet Capture—When a Cisco 5500 Series Controller's data plane crashes, it stores the last 50 packets that the controller received in flash memory. This information can be useful in troubleshooting the crash. When a crash occurs, the controller generates a new packet capture file (*.pcap) file. You can upload the packet capture file from the controller. You can then use Wireshark or another standard packet capture tool to view and analyze the contents of the file.

Note Only Cisco 5500 Series Controllers generate packet capture files. This feature is not available on other controller platforms.

  - Watchdog Crash File
  - Panic Crash File
- Configuration File Encryption—Enable the Configuration File Encryption option and enter the encryption key. File encryption ensures that data is encrypted while uploading or downloading the controller configuration file through a TFTP, SFTP, or FTP server.
- Transfer Mode—Choose the transfer mode from the drop-down list. Available options include FTP, SFTP, and TFTP. If you chose TFTP from the Transfer Mode drop-down list, enter the IP address of the TFTP server, the file path on the server (default = /), and a name for the file you have selected for upload.

Note The TFTP server cannot run on the same computer as the Cisco Wireless Control System because the Cisco WCS or Cisco Prime Infrastructure and the TFTP server use the same communication port.

If you chose FTP or SFTP from the Transfer Mode drop-down list, enter the IP address of the FTP or SFTP server, the file path on the server (default = /), a name for the file you have selected for upload, the username to log in to the FTP or SFTP server, the password to log in to the FTP or SFTP server, and the port number on the FTP or SFTP server through which the download occurs (the default value for the server port is 21 and the default value for the SFTP server port is 22).

When you click Upload, the selected file is uploaded to your TFTP, SFTP, or FTP server and is saved with the same name that you entered in the File Name field.

Editing Configuration Files

When you save the controller's configuration, the controller stores it in XML format in flash memory. When you upload the configuration file to a TFTP, SFTP, or FTP server, the controller converts the file from XML to CLI. You can then read, modify, delete, or add CLI commands to the configuration file in CLI format on the server.

Note To edit the configuration file, you can use either Notepad on Windows or the VI editor on Linux.

When you are finished, save your changes to the configuration file on the server and download the file back to the controller, where it is reconverted to XML format and saved.

Configuration Files with Invalid CLI Commands

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 the **show invalid-config** command on the controller CLI.

Note You can enter this command only before the **clear config** or **save config** command.

If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP, SFTP, or FTP server for analysis.

Buttons

- Clear: Deletes the entries in the data fields are deleted.
- Upload: Begins the file upload to the TFTP, SFTP, or FTP server; you are prompted to continue.

Redundancy > Reset Peer

Choose **COMMANDS > Redundancy > Reset Peer** to navigate to this page.

This page enables you to reset the peer controller.

Buttons

- Reboot: Resets the peer controller.

Using the Configuration Wizard

When the controller is activated for the first time from the factory, or when it has been rebooted after a Reset to Factory Default, the Web User Interface displays the Web Configuration Wizard. Use the web Configuration Wizard to configure the controller for initial operation.

Complete the following wizard screens to enter the initial controller configuration:

- Collect the Initial Configuration Settings
- Connecting Your Web Browser to a Controller
- Configuration Wizard System Information
- Service Interface Configuration
- Management Interface Configuration
- Miscellaneous Configuration
- Virtual Interface Configuration
- WLAN Policy Configuration
- RADIUS Server Configuration
- 802.11 Configuration
- Redundancy Configuration
- Completing the Configuration Wizard

Collect the Initial Configuration Settings

Collect the following high-level controller parameters.

System Parameters

The system parameters are as follows:

- Controller name
- Supported protocols: 802.11a/n and/or 802.11b/g/n
- New usernames and passwords (optional)

Network (Distribution System) Parameters

The network parameters are as follows:

- Distribution System (network) port static IP address, netmask, and optional default gateway IP address from the network planner.
- Service port static IP address and netmask from the network planner (optional).
- Distribution System physical port (1000Base-T, 1000BASE-SX, or 10/100BASE-T). The 1000Base-SX (UNUSED PRODUCT) provides a 100/1000 Mbps wired connection to a network through an 850nM (SX) fiber-optic link using an LC physical connector.
- Distribution System port VLAN assignment (optional).
- Distribution System port Web and Secure Web mode settings, enabled or disabled.

- Distribution System port Spanning Tree Protocol: enabled/disabled, 802.1D/fast/off mode per port, path cost per port, priority per port, bridge priority, forward delay, hello time, maximum age.

WLAN Parameters

The WLAN parameters are as follows:

- VLAN assignments
- Layer 2 Security settings
- Layer 3 Security settings
- QoS assignments

Mobility Parameters

Specify the Mobility Settings for the controller by providing a mobility group name. This step is optional.

RADIUS Parameters

Specify the RADIUS parameters.

SNMP Parameters

Specify the SNMP parameters.

Other Parameters

Other Port and Parameter Settings: Service port, Radio Resource Management (RRM), third-party APs, Serial/CLI Console port, 802.3x Flow Control, and System Logging.

Other Actions

Collect all files that may need uploading or downloading to the controller, including the latest operating system code.

Connecting Your Web Browser to a Controller

To connect your web browser to the controller, follow these steps:

Note For the Initial GUI Configuration Wizard only, you cannot access the controller using IPv6 address.

Step 1 Temporarily configure your web browser device with a 192.168.1.2 IP address. Connect your web browser to the controller front panel service port, either using a crossover Ethernet cable or through an Ethernet hub or controller.

Note In case of Cisco WLC 2500, connect your PC to the port 2 on the controller and configure to use the same subnet.

Step 2 Type 192.168.1.1 into the address line of your web browser to log into the web user interface as described in the Commands Tab topic. The web server built into the controller responds with the login prompt.

Step 3 Enter admin and admin as the login and password, respectively. The controller displays the Configuration Wizard System Information page, in which you will configure the controller name and administrative user login.

Configuration Wizard System Information

To configure the wizard, follow these steps:

Step 1 On the Configuration Wizard System Information page, enter the controller name.

Step 2 Also in the Configuration Wizard page, enter a new administrative username and password. The default is admin and admin, respectively.)

Step 3 Click **Next** to have the controller save your inputs and display the Service Interface Configuration page, in which you will configure the Service Port Interface.

Service Interface Configuration

To configure the service interface, follow these steps:

Step 1 Click the DHCP Protocol **Enable** box when the Service Port Interface is to obtain an IP address from a DHCP server. When the Service Port Interface is to use a fixed IP address, leave this box unselected.

Step 2 The IP Address box contains the current Service Port Interface IP address. If desired, enter a different Service Port Interface IP address.

Step 3 The Netmask box contains the current Service Port IP netmask. If desired, enter a different Service Port Interface IP netmask.

Step 4 Click **Next** to have the controller save your inputs and display the Management Interface Configuration page, in which you will configure the Management Interface.

Management Interface Configuration

To configure the management interface, follow these steps:

Caution Do not configure wired clients in the same VLAN or subnet of the service port on the network. If you configure wired clients on the same subnet or VLAN as the service port, you will not be able to access the management interface.

Step 1 Enter a Management Interface VLAN assignment.

The VLAN Identifier box contains the current VLAN assignment (0 if untagged). If desired, enter a different Management Interface VLAN assignment (or 0 if untagged).

Step 2 Enter the Management Interface IP address.

The IP Address text box contains the current Management Interface IP address. If desired, enter a different Management Interface IP address.

Step 3 Enter a Management Interface netmask.

The Netmask text box contains the current Management Interface netmask. If desired, enter a different management interface netmask.

Step 4 Enter the Management Interface Gateway in the Gateway text box.

The Gateway text box contains the default Management Interface gateway. If desired, enter a different Management Interface gateway.

Step 5 Enter the Management Interface Physical Port in the Port Number text box text box.

The Port Number text box contains the current Management Interface physical port. If desired, enter a different Management Interface physical port.

Step 6 Enter the Primary DHCP Server IP address.

The Primary DHCP Server text box contains the default Management Interface primary DHCP server IP address. If necessary, enter a valid primary DHCP server IP address for the Management Interface.

Step 7 Enter the secondary DHCP server box.

The Secondary DHCP Server text box contains the default Management Interface secondary DHCP server IP address. If necessary, enter a valid secondary DHCP server IP address for the Management Interface.

Step 8 Click **Next** to have the controller save your inputs and display the Miscellaneous Configuration page, in which you will configure some Cisco WLAN Solution parameters.

Redundancy Configuration

To configure High Availabilty between two controllers, follow these steps:

Step 1 Configure the management IP address of both the controllers.

Note Before enabling redundancy, ensure that the management IP address of both the controllers are in the same subnet.

Step 2 Enter yes to enable HA.

Step 3 Configure the primary and secondary unit.

Step 4 Configure the Redundant Management and Peer Redundant Management IP address.

Note Both the interfaces should be in same subnet as the Management interface.

Miscellaneous Configuration

To perform the miscellaneous configuration, follow these steps:

Step 1 Enter the RF Mobility Domain Name.

The RF Mobility Domain Name text box contains the default RF Mobility Domain Name. If desired, enter a different RF mobility domain name.

Step 2 Enter the country code in the Country Code text box.

The Country Code text box contains the current country code. If desired, enter a different country code.

Step 3 Click **Next** to have the controller save your inputs and display the Virtual Interface Configuration page, in which you will configure the Virtual Interface parameters.

Virtual Interface Configuration

To configure the virtual interface, follow these steps:

Step 1 Enter the IP address.

The IP Address text box contains the default Virtual Interface IP address. Enter a different virtual interface IP address. Note that the Virtual Interface uses any fictitious, unassigned IP address (such as 192.0.2.1), to be used by Layer 3 Security and Mobility managers.

Step 2 Enter the DNS host name.

The DNS Host Name text box contains a space for a Web Auth ID Certificate DNS Host Name. If the controller uses an externally-generated Web Auth ID Certificate that includes a DNS Host Name, enter the DNS Host Name here.

Step 3 Click **Next** to have the controller save your inputs and display the WLAN Policy Configuration page, in which you will configure the WLAN 1 parameters.

WLAN Policy Configuration

To configure the WLAN policy, follow these steps:

Note Refer to the Editing WLANs page for a description of these parameters.

Step 1 Enter the WLAN SSID in the WLAN SSID text box.

The WLAN SSID text box contains the current WLAN 1 SSID. If desired, enter a different SSID.

Step 2 Enter the radio policy you want to adopt in the Radio Policy text box.

The Radio Policy text box contains the default bands controlled by the WLAN 1 policy. If desired, enter a different WLAN 1 policy: 802.11a only, 802.11g only, 802.11b/g only, 802.11a/g only, or All.

Step 3 Enter the admin status in the Admin Status text box.

The Admin Status text box contains the default administrative status (unselected, or disabled). If desired, enable the WLAN 1 policy by selecting the **Admin Status** box.

Step 4 Enter the session timeout value in the Session Timeout text box.

The Session Timeout text box contains the default 802.11 session timeout (0, or no timeout). If desired, enter a different 802.11 session timeout in minutes.

Step 5 Enter the QoS value in the Quality of Service text box.

The Quality of Service (QoS) text box contains the default QoS status (Silver, or Best Effort QoS). If desired, enter a different QoS: Platinum = Voice, Gold = Video, Bronze = Background, or leave as Silver = Best Effort. VoIP clients should be set to Platinum, Gold or Silver, while low-bandwidth clients can be set to Bronze.

Step 6 Set the AAA Override status.

The Allow AAA Override text box contains the default AAA Override status (unselected, or disabled). If desired, enable AAA Override by selecting the **AAA Override** box.

Step 7 Set the Blacklist Exclusion List Timeout.

The Blacklist Exclusion List Timeout text box contains the default client Exclusion List (blacklist) timeout status (selected, or enabled). If desired, disable Exclusion List (Blacklist) Timeout by unselecting the **Blacklist Timeout** box.

Step 8 Enter the number of seconds a client is added to the Exclusion List (blacklisted) after you fail to authenticate three consecutive times.

Step 9 Set the DHCP Server Override.

The DHCP Server Override text box contains the current status (unselected or disabled). If desired, enable DHCP Server Override by selecting the Override box.

Step 10 Set the DHCP Addr. Assignment.

The DHCP Addr. Assignment Required text box contains the current status (unselected or not required). If desired, enable DHCP Address Assignment Required parameter by selecting the **Required** box.

Step 11 Enter the Interface Name.

The Interface Name text box contains the current WLAN 1 Interface (management). Leave this setting unchanged.

Step 12 Enter the Layer 2 Security.

The Layer 2 Security text box contains the default Layer 2 Security setting (802.1X). If desired, select a different Layer 2 Security setting: None, WPA, 802.1X, Static WEP, Cranite, or Fortress. Refer to the Editing WLANs page for a description of these parameters and the related parameters that can be set for Layer 2 Security.

Step 13 Enter the Layer 3 Security.

The Layer 3 Security text box contains the default Layer 3 Security setting (None). If desired, select a different Layer 3 Security setting: None, IPSec, or VPN Pass Through. Refer to the Editing WLANs page for a description of these parameters and the related parameters that can be set for Layer 3 Security.

Step 14 Click **Next** to have the controller save your inputs and display the RADIUS Server Configuration page, in which you will configure the RADIUS server parameters.

RADIUS Server Configuration

If you do not want to configure a RADIUS server at this time, click **Skip** to ignore this section, and continue with the 802.11 Configuration section. If you do want to configure a RADIUS server, continue with this section.

To configure a RADIUS server, follow these steps:

Step 1 Enter the RADIUS server IP.

If required, enter a RADIUS server IP address.

Step 2 Enter the RADIUS Server Shared Secret password in the Shared Secret and Confirm Shared Secret text box.

Step 3 Enter the communication port number in the Port Number text box.

The Port Number text box contains the default communication port number (1812). If required, enter a different, unused communication port number.

Step 4 Set the RADIUS server status.

The Server Status text box contains the default RADIUS server status (Disabled). If desired, enable the RADIUS configuration by choosing **Enabled**.

Step 5 Click **Apply** to have the controller save your inputs and display the 802.11 Configuration page, in which you will activate or deactivate the different 802.11 bands and the Radio Resource Management (RRM) (RRM software).

802.11 Configuration

To configure 802.11 parameters, follow these steps:

Step 1 Set the 802.11a network status by selecting the **Network Status** check box.

The 802.11a Network Status check box contains the current status (unselected = disabled). If desired, select the box to activate the 802.11a Network in the Cisco WLAN Solution.

Step 2 Set the 802.11b network status by selecting the **Network Status** check box.

The 802.11b Network Status check box contains the current status (unselected = disabled). If desired, select the **Network Status** check box to activate the 802.11b Network in the Cisco WLAN Solution.

Step 3 Set the 802.11g network status by selecting the **Network Status** check box.

The 802.11g Network Status check box contains the current status (unselected = disabled). If desired, select the **Network Status** check box to activate the 802.11g Network in the Cisco WLAN Solution.

Step 4 Select the **Radio Resource Management** check box to enable RRM.

The Radio Resource Management check box contains the current Radio Resource Management, or Radio Resource Management, status (selected = enabled). If desired, unselect the box to disable the Radio Resource Management dynamic channel number and transmit power level assignment functions.

Step 5 Click **Next** to have the controller save your inputs and display the Configuration Wizard Completed page, in which the controller saves your changes in nonvolatile RAM and reboots the controller.

Completing the Configuration Wizard

To complete the configuration, follow these steps:

Step 1 Click the **Save and Reboot** button to have the controller save your changes in nonvolatile RAM and reboot. The operating system prompts you to confirm the operation.

Step 2 Click **OK** to continue. You have configured the controller using the Web User Interface.