Getting Started

- Configuring the Controller Using the Configuration Wizard, on page 1
- Connecting the Console Port of the Controller, on page 1
- Configuring the Controller (GUI), on page 2
- Configuring the Controller—Using the CLI Configuration Wizard, on page 13
- Using the Controller GUI, on page 16
- Loading an Externally Generated SSL Certificate, on page 19
- Loading an Externally Generated SSL Certificate, on page 19
- Loading an SSL Certificate (GUI), on page 20
- Loading an SSL Certificate (CLI), on page 21
- Using the Controller CLI, on page 22
- Using the AutoInstall Feature for Controllers Without a Configuration, on page 25
- Information About the AutoInstall Feature, on page 26
- Restrictions on AutoInstall, on page 27
- Managing the Controller System Date and Time, on page 30
- Telnet and Secure Shell Sessions, on page 35
- Managing the Controller Wirelessly, on page 40

Configuring the Controller Using the Configuration Wizard

The configuration wizard enables you to configure basic settings on the controller. You can run the wizard after you receive the controller from the factory or after the controller has been reset to factory defaults. The configuration wizard is available in both GUI and CLI formats.

Connecting the Console Port of the Controller

Before you can configure the controller for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip).

Note On Cisco 5500 Series Controllers, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller's USB console port and the other end of the cable into the PC's USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.

Step 1 Connect one end of a null-modem serial cable to the controller's console port and the other end to your PC's serial port.

Step 2 Start the PC's VT-100 terminal emulation program.

Step 3 Configure the terminal emulation program for these parameters:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

Step 4 Plug the AC power cord into the controller and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet.Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self test verification) and basic configuration.

If the controller passes the power-on self test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.

Configuring the Controller (GUI)

Step 1 Connect your PC to the service port and configure it to use the same subnet as the controller.

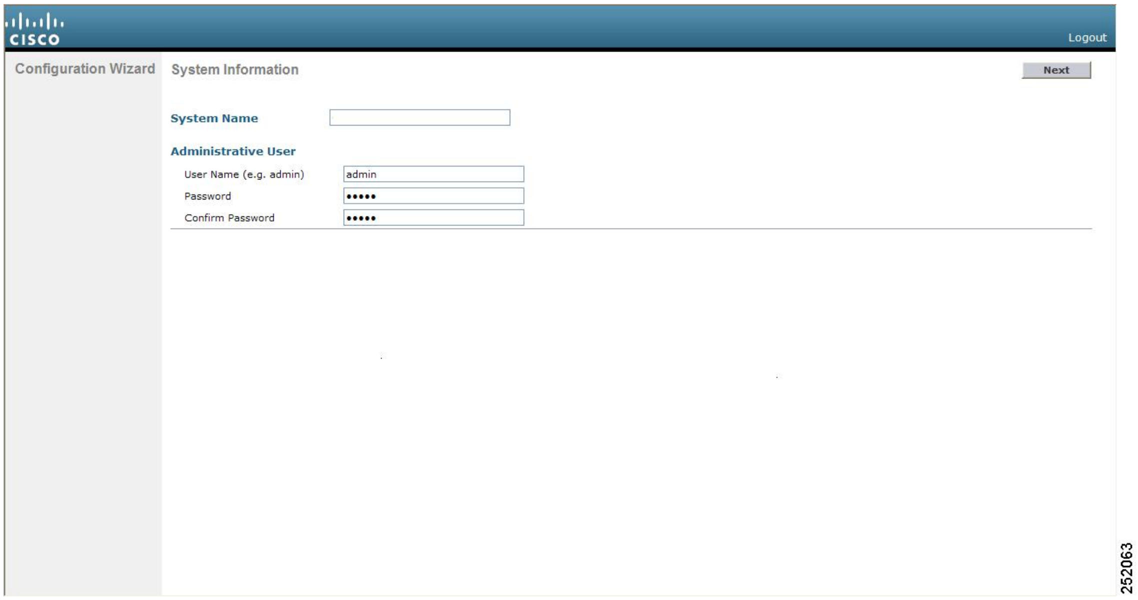
Note In case of Cisco 2504 Wireless Controller, connect your PC to the port 2 on the controller and configure to use the same subnet.

Step 2 Browse to http://192.168.1.1. The configuration wizard appears.

Note You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled. The default IP address to connect to the service port interface is 192.168.1.1.

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

Figure 1: Configuration Wizard — System Information Page



System Information

System Name □

Administrative User

User Name (e.g. admin)	admin
Password	•••••
Confirm Password	•••••

Step 3 In the **System Name** box, enter the name that you want to assign to this controller. You can enter up to 31 ASCII characters.

Step 4 In the **User Name** box, enter the administrative username to be assigned to this controller. You can enter up to 24 ASCII characters. The default username is *admin*.

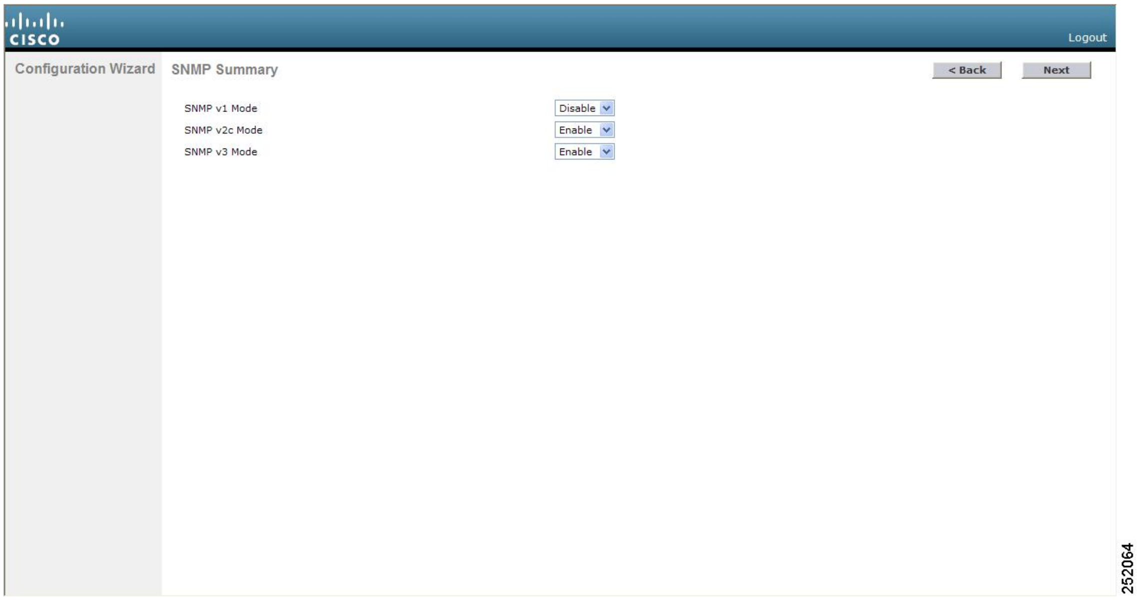
Step 5 In the **Password** and **Confirm Password** boxes, enter the administrative password to be assigned to this controller. You can enter up to 24 ASCII characters. The default password is *admin*.

Starting in release 7.0.116.0, the following password policy has been implemented:

- The password must contain characters from at least three of the following classes:
    - Lowercase letters
    - Uppercase letters
    - Digits
    - Special characters
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 6 Click **Next**. The **SNMP Summary** page is displayed.

Figure 2: Configuration Wizard—SNMP Summary Page



SNMP Summary

SNMP v1 Mode: Disable
SNMP v2c Mode: Enable
SNMP v3 Mode: Enable

Step 7 If you want to enable Simple Network Management Protocol (SNMP) v1 mode for this controller, choose **Enable** from the **SNMP v1 Mode** drop-down list. Otherwise, leave this parameter set to **Disable**.

Note SNMP manages nodes (servers, workstations, routers, switches, and so on) on an IP network. Currently, there are three versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3.

Step 8 If you want to enable SNMPv2c mode for this controller, leave this parameter set to **Enable**. Otherwise, choose **Disable** from the **SNVP v2c Mode** drop-down list.

Step 9 If you want to enable SNMPv3 mode for this controller, leave this parameter set to **Enable**. Otherwise, choose **Disable** from the **SNVP v3 Mode** drop-down list.

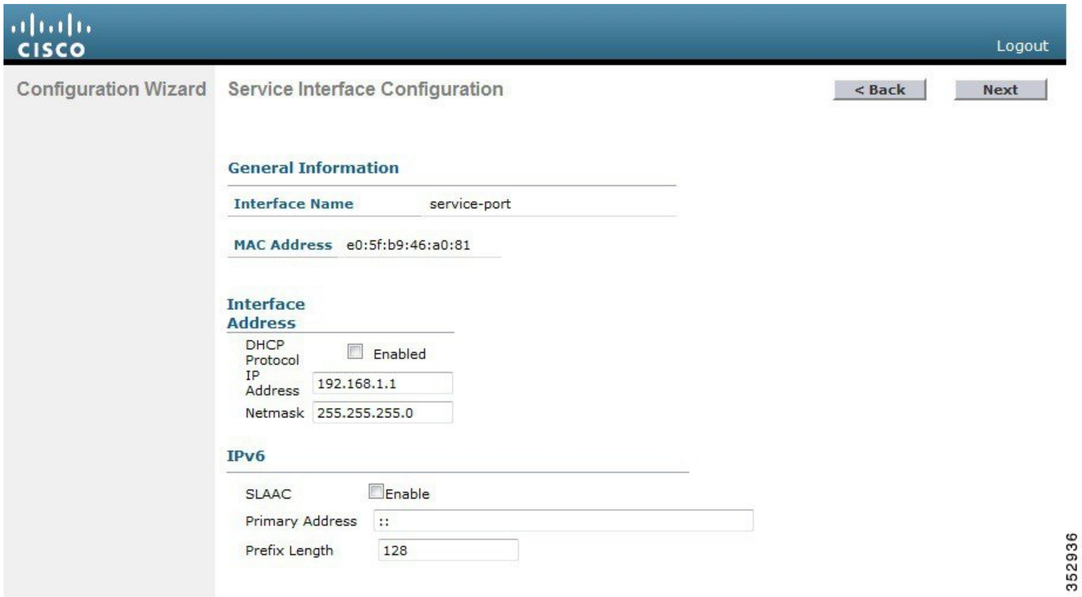
Step 10 Click **Next**.

Step 11 When the following message appears, click **OK**:

```
Default values are present for v1/v2c community strings.
Please make sure to create new v1/v2c community strings once the system comes up.
Please make sure to create new v3 users once the system comes up.
```

The **Service Interface Configuration** page is displayed.

Figure 3: Configuration Wizard-Service Interface Configuration Page



Service Interface Configuration

General Information

Interface Name service-port

MAC Address e0:5f:b9:46:a0:81

Interface Address

DHCP Protocol □ Enabled

IP Address 192.168.1.1

Netmask 255.255.255.0

IPv6

SLAAC □ Enable

Primary Address ::

Prefix Length 128

Step 12 If you want the controller’s service-port interface to obtain an IP address from a DHCP server, check the **DHCP Protocol Enabled** check box. If you do not want to use the service port or if you want to assign a static IP address to the service port, leave the check box unchecked.

Note The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

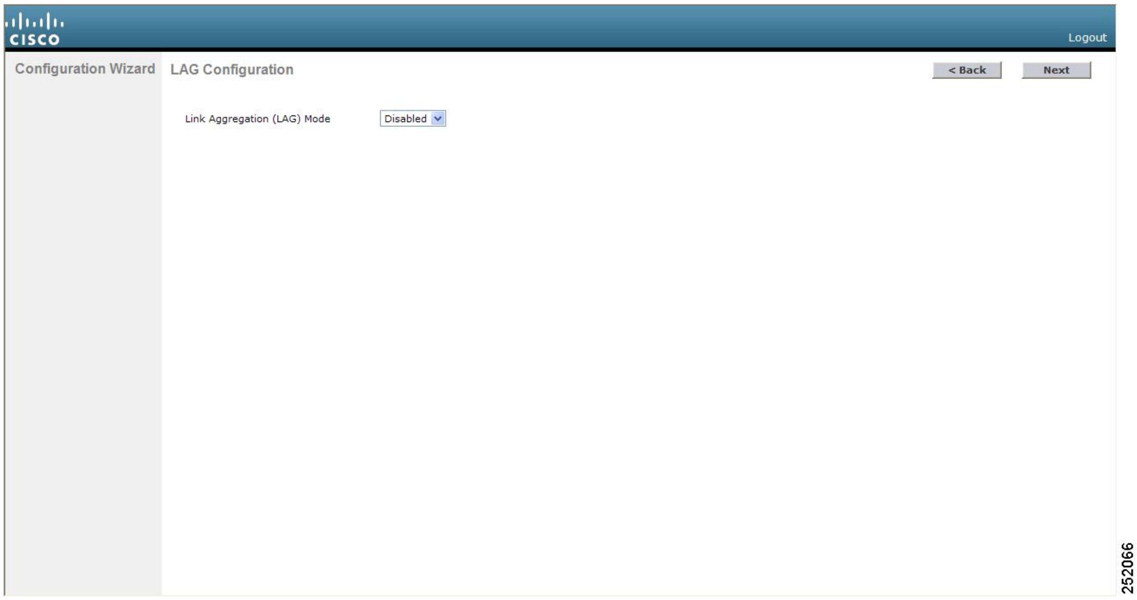
Step 13 Perform one of the following:

- If you enabled DHCP, clear out any entries in the IP Address and Netmask text boxes, leaving them blank.
- If you disabled DHCP, enter the static IP address and netmask for the service port in the IP Address and Netmask text boxes.

Step 14 Click **Next**.

The **LAG Configuration** page is displayed.

Figure 4: Configuration Wizard—LAG Configuration Page

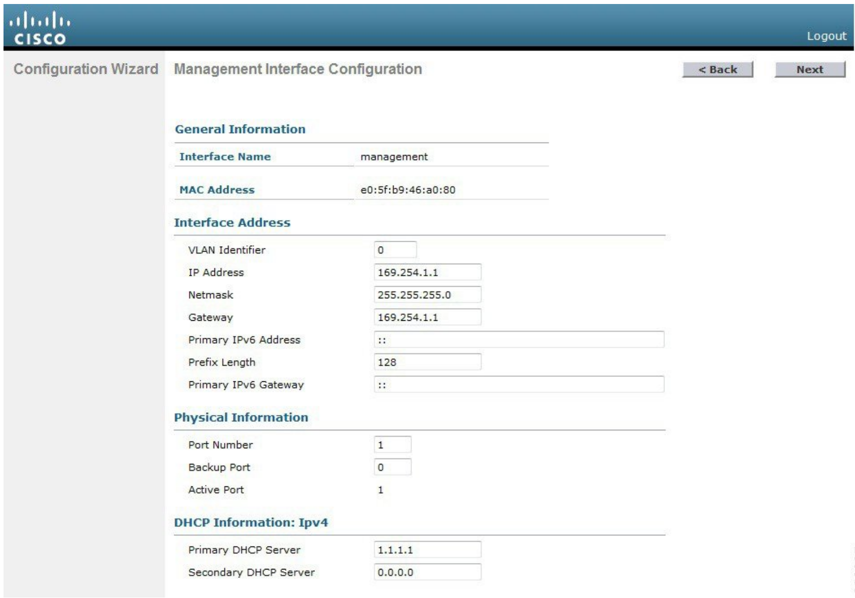


Link Aggregation (LAG) Mode: Disabled

Step 15 To enable link aggregation (LAG), choose **Enabled** from the Link Aggregation (LAG) Mode drop-down list. To disable LAG, leave this text box set to **Disabled**.

Step 16 Click **Next**.

The **Management Interface Configuration** page is displayed.



General Information

Interface Name	management
MAC Address	e0:5f:b9:46:a0:80

Interface Address

VLAN Identifier	0
IP Address	169.254.1.1
Netmask	255.255.255.0
Gateway	169.254.1.1
Primary IPv6 Address	::
Prefix Length	128
Primary IPv6 Gateway	::

Physical Information

Port Number	1
Backup Port	0
Active Port	1

DHCP Information: Ipv4

Primary DHCP Server	1.1.1.1
Secondary DHCP Server	0.0.0.0

Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.

Step 17 In the **VLAN Identifier** box, enter the VLAN identifier of the management interface (either a valid VLAN identifier or **0** for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

Step 18 In the **IP Address** box, enter the IP address of the management interface.

Step 19 In the **Netmask** box, enter the IP address of the management interface netmask.

Step 20 In the **Gateway** box, enter the IP address of the default gateway.

Step 21 In the **Port Number** box, enter the number of the port assigned to the management interface. Each interface is mapped to at least one primary port.

Step 22 In the **Backup Port** box, enter the number of the backup port assigned to the management interface. If the primary port for the management interface fails, the interface automatically moves to the backup port.

Step 23 In the **Primary DHCP Server** box, enter the IP address of the default DHCP server that will supply IP addresses to clients, the controller’s management interface, and optionally, the service port interface.

Step 24 In the **Secondary DHCP Server** box, enter the IP address of an optional secondary DHCP server that will supply IP addresses to clients, the controller’s management interface, and optionally, the service port interface.

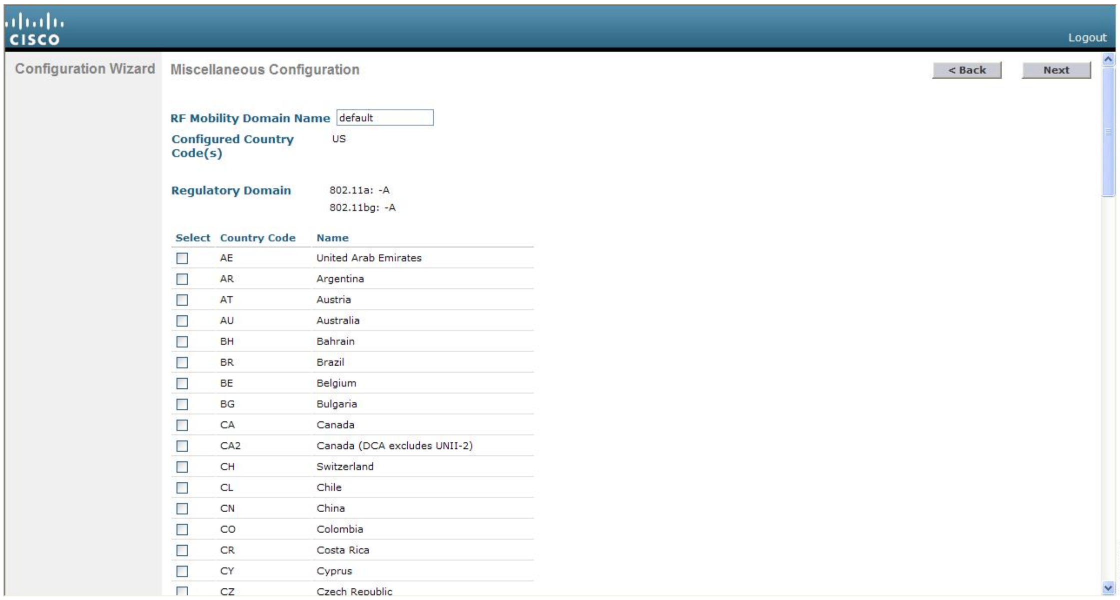
Step 25 Click **Next**. The **AP-Manager Interface Configuration** page is displayed.

Note This screen does not appear for Cisco 5508 WLCs because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 26 In the **IP Address** box, enter the IP address of the AP-manager interface.

Step 27 Click **Next**. The **Miscellaneous Configuration** page is displayed.

Figure 5: Configuration Wizard—Miscellaneous Configuration Page



Miscellaneous Configuration

RF Mobility Domain Name: default

Configured Country Code(s): US

Regulatory Domain: 802.11a: -A
802.11bg: -A

Select	Country Code	Name
□	AE	United Arab Emirates
□	AR	Argentina
□	AT	Austria
□	AU	Australia
□	BH	Bahrain
□	BR	Brazil
□	BE	Belgium
□	BG	Bulgaria
□	CA	Canada
□	CA2	Canada (DCA excludes UNII-2)
□	CH	Switzerland
□	CL	Chile
□	CN	China
□	CO	Colombia
□	CR	Costa Rica
□	CY	Cyprus
□	CZ	Czech Republic

Step 28 In the **RF Mobility Domain Name** box, enter the name of the mobility group/RF group to which you want the controller to belong.

Note Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

Step 29 The **Configured Country Code(s)** box shows the code for the country in which the controller will be used. If you want to change the country of operation, check the check box for the desired country.

Note You can choose more than one country code if you want to manage access points in multiple countries from a single controller. After the configuration wizard runs, you must assign each access point joined to the controller to a specific country.

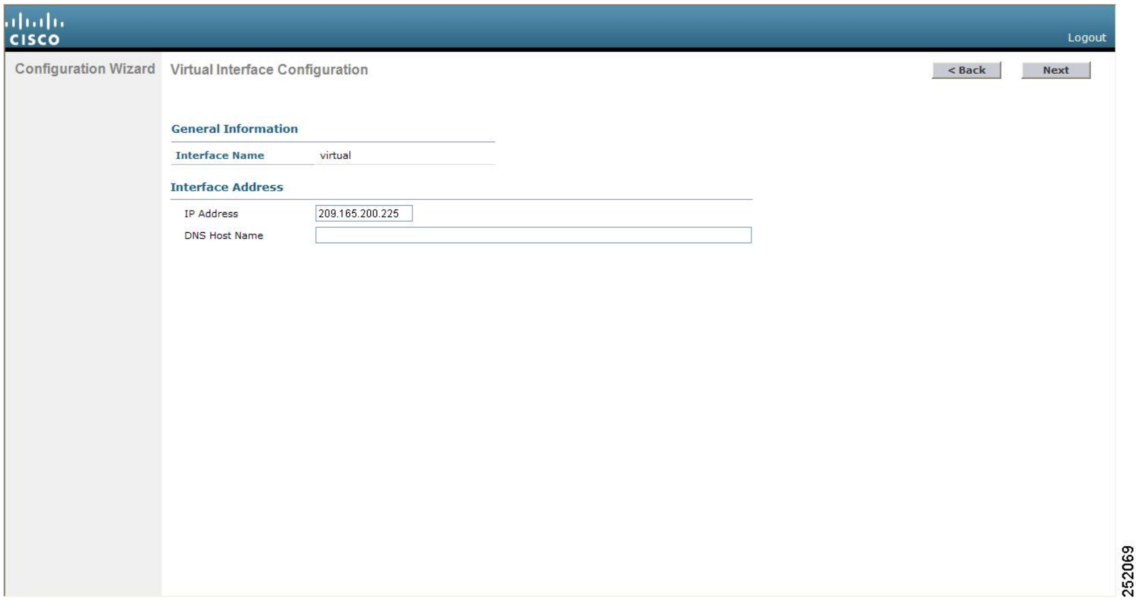
Step 30 Click **Next**.

Step 31 When the following message appears, click **OK**:

```
Warning! To maintain regulatory compliance functionality, the country code
setting may only be modified by a network administrator or qualified IT professional.
Ensure that proper country codes are selected before proceeding.?
```

The **Virtual Interface Configuration** page is displayed.

Figure 6: Configuration Wizard — Virtual Interface Configuration Page



Virtual Interface Configuration

General Information

Interface Name virtual

Interface Address

IP Address 209.165.200.225

DNS Host Name

Step 32 In the **IP Address** box, enter the IP address of the controller's virtual interface. You should enter a fictitious, unassigned IP address.

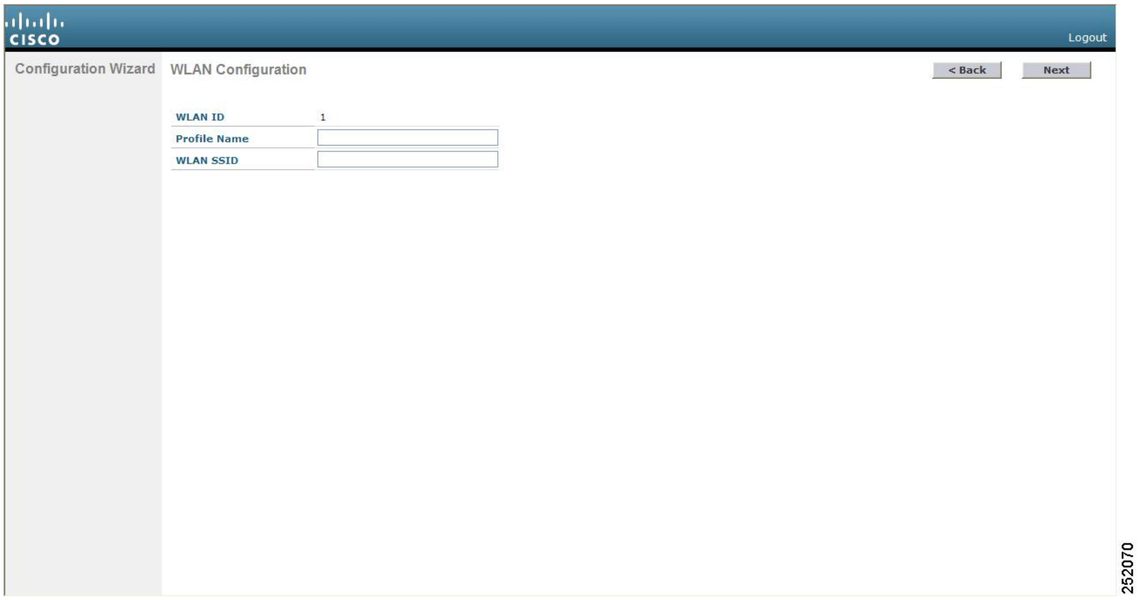
Note The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 33 In the **DNS Host Name** box, enter the name of the Domain Name System (DNS) gateway used to verify the source of certificates when Layer 3 web authorization is enabled.

Note To ensure connectivity and web authentication, the DNS server should always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then the same DNS hostname must be configured on the DNS servers used by the client.

Step 34 Click **Next**. The **WLAN Configuration** page is displayed.

Figure 7: Configuration Wizard — WLAN Configuration Page



Configuration Wizard

WLAN Configuration

WLAN ID	1
Profile Name	
WLAN SSID	

Step 35 In the **Profile Name** box, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN.

Step 36 In the **WLAN SSID** box, enter up to 32 alphanumeric characters for the network name, or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

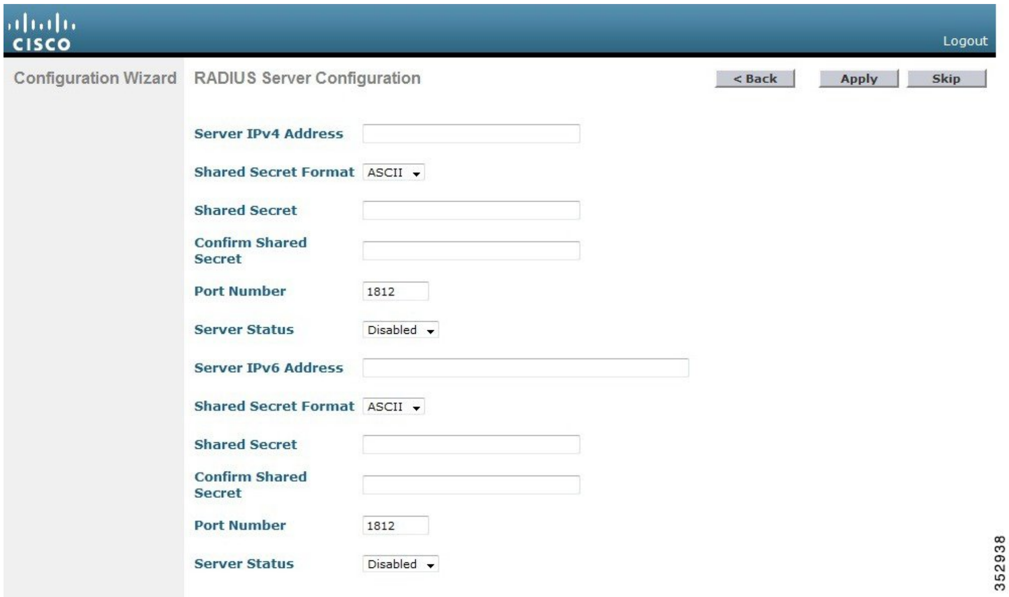
Step 37 Click **Next**.

Step 38 When the following message appears, click **OK**:

```
Default Security applied to WLAN is: [WPA2(AES)][Auth(802.1x)]. You can change
this after the wizard is complete and the system is rebooted.?
```

The **RADIUS Server Configuration** page is displayed.

Figure 8: Configuration Wizard-RADIUS Server Configuration Page



RADIUS Server Configuration

Server IPv4 Address	
Shared Secret Format	ASCII
Shared Secret	
Confirm Shared Secret	
Port Number	1812
Server Status	Disabled
Server IPv6 Address	
Shared Secret Format	ASCII
Shared Secret	
Confirm Shared Secret	
Port Number	1812
Server Status	Disabled

Step 39 In the **Server IP Address** box, enter the IP address of the RADIUS server.

Step 40 From the **Shared Secret Format** drop-down list, choose **ASCII** or **Hex** to specify the format of the shared secret.

Note Due to security reasons, the RADIUS shared secret key reverts to ASCII mode even if you have selected HEX as the shared secret format from the Shared Secret Format drop-down list.

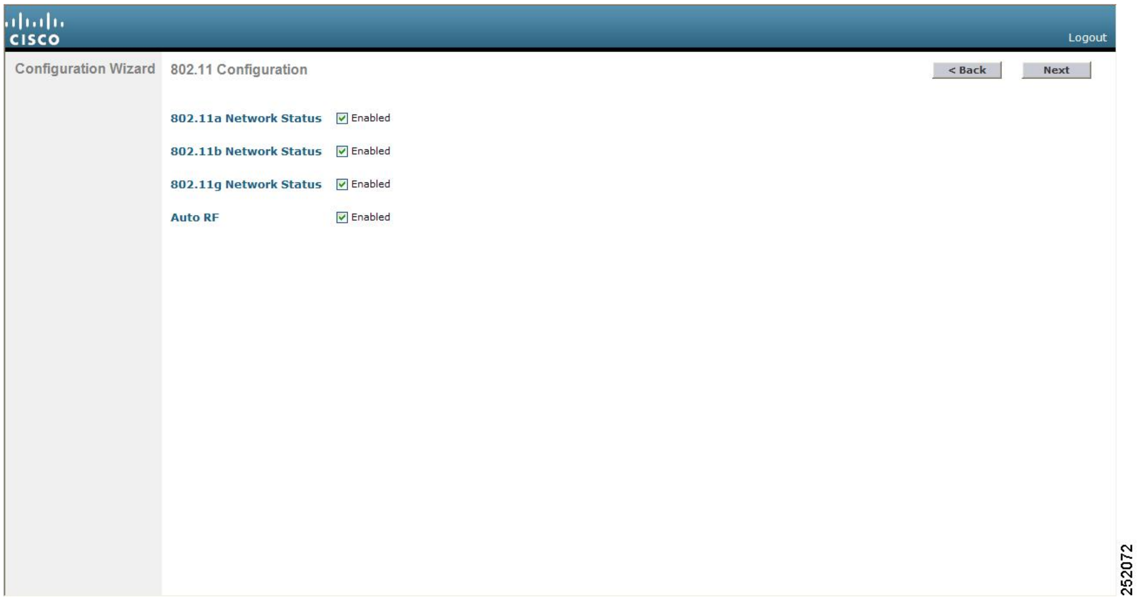
Step 41 In the **Shared Secret** and **Confirm Shared Secret** boxes, enter the secret key used by the RADIUS server.

Step 42 In the **Port Number** box, enter the communication port of the RADIUS server. The default value is 1812.

Step 43 To enable the RADIUS server, choose **Enabled** from the **Server Status** drop-down list. To disable the RADIUS server, leave this box set to **Disabled**.

Step 44 Click **Apply**. The **802.11 Configuration** page is displayed.

Figure 9: Configuration Wizard—802.11 Configuration Page



Configuration Wizard

802.11 Configuration

802.11a Network Status ☑ Enabled

802.11b Network Status ☑ Enabled

802.11g Network Status ☑ Enabled

Auto RF ☑ Enabled

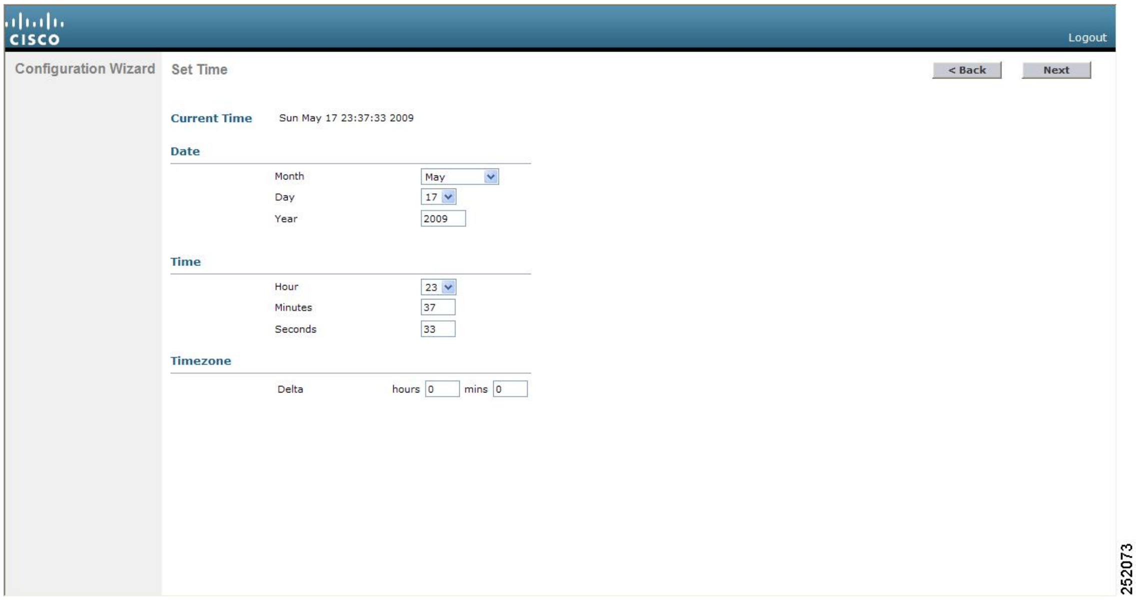
Step 45 To enable the 802.11a, 802.11b, and 802.11g lightweight access point networks, leave the **802.11a Network Status**, **802.11b Network Status**, and **802.11g Network Status** check boxes checked. To disable support for any of these networks, uncheck the check boxes.

Step 46 To enable the controller's radio resource management (RRM) auto-RF feature, leave the **Auto RF** check box selected. To disable support for the auto-RF feature, uncheck this check box.

Note The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and transmit power assignment, for the group.

Step 47 Click **Next**. The **Set Time** page is displayed.

Figure 10: Configuration Wizard — Set Time Screen



Set Time

Current Time Sun May 17 23:37:33 2009

Date

Month	May
Day	17
Year	2009

Time

Hour	23
Minutes	37
Seconds	33

Timezone

Delta hours 0 mins 0

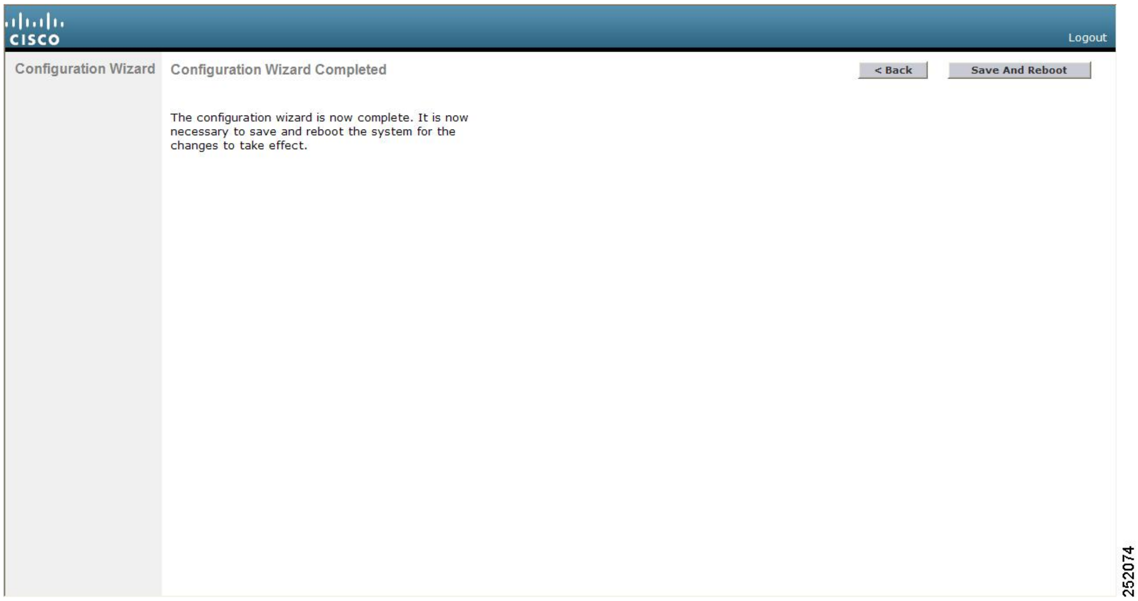
Step 48 To manually configure the system time on your controller, enter the current date in Month/DD/YYYY format and the current time in HH:MM:SS format.

Step 49 To manually set the time zone so that Daylight Saving Time (DST) is not set automatically, enter the local hour difference from Greenwich Mean Time (GMT) in the **Delta Hours** box and the local minute difference from GMT in the **Delta Mins** box.

Note When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/–). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as –8.

Step 50 Click **Next**. The **Configuration Wizard Completed** page is displayed.

Figure 11: Configuration Wizard—Configuration Wizard Completed Page



Configuration Wizard Completed

The configuration wizard is now complete. It is now necessary to save and reboot the system for the changes to take effect.

Step 51 Click **Save and Reboot** to save your configuration and reboot the controller.

Step 52 When the following message appears, click **OK**:

```
Configuration will be saved and the controller will be
rebooted. Click ok to confirm.?
```

The controller saves your configuration, reboots, and prompts you to log on.

Configuring the Controller—Using the CLI Configuration Wizard

Before you begin

- The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.
- If you enter an incorrect response, the controller provides you with an appropriate error message, such as “Invalid Response”, and returns you to the wizard prompt.
- Press the **hyphen** key if you ever need to return to the previous command line.

Step 1 When prompted to terminate the AutoInstall process, enter **yes**. If you do not enter **yes**, the AutoInstall process begins after 30 seconds.

Note The AutoInstall feature downloads a configuration file from a TFTP server and then loads the configuration onto the controller automatically.

Step 2 Enter the system name, which is the name that you want to assign to the controller. You can enter up to 31 ASCII characters.

Step 3 Enter the administrative username and password to be assigned to this controller. You can enter up to 24 ASCII characters for each.

Starting in release 7.0.116.0, the following password policy has been implemented:

- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 4 If you want the controller's service-port interface to obtain an IP address from a DHCP server, enter **DHCP**. If you do not want to use the service port or if you want to assign a static IP address to the service port, enter none.

Note The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

Step 5 If you entered none in *Step 4*, enter the IP address and netmask for the service-port interface on the next two lines.

Step 6 Enable or disable link aggregation (LAG) by choosing yes or NO.

Step 7 Enter the IP address of the management interface.

Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.

Step 8 Enter the IP address of the management interface netmask.

Step 9 Enter the IP address of the default router.

Step 10 Enter the VLAN identifier of the management interface (either a valid VLAN identifier or 0 for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

Step 11 Enter the IP address of the default DHCP server that will supply IP addresses to clients, the management interface of the controller, and optionally, the service port interface. Enter the IP address of the AP-manager interface.

Note This prompt does not appear for Cisco 5508 WLCs because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 12 Enter the IP address of the controller's virtual interface. You should enter a fictitious unassigned IP address.

Note The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 13 If desired, enter the name of the mobility group/RF group to which you want the controller to belong.

Note Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

Step 14 Enter the network name or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

Step 15 Enter YES to allow clients to assign their own IP address or no to require clients to request an IP address from a DHCP server.

Step 16 To configure a RADIUS server now, enter YES and then enter the IP address, communication port, and secret key of the RADIUS server. Otherwise, enter no. If you enter no, the following message appears: “Warning! The default WLAN security policy requires a RADIUS server. Please see the documentation for more details.”

Step 17 Enter the code for the country in which the controller will be used.

Note Enter help to view the list of available country codes.

Note You can enter more than one country code if you want to manage access points in multiple countries from a single controller. To do so, separate the country codes with a comma (for example, US,CA,MX). After the configuration wizard runs, you need to assign each access point joined to the controller to a specific country.

Step 18 Enable or disable the 802.11b, 802.11a, and 802.11g lightweight access point networks by entering **YES** or **no**.

Step 19 Enable or disable the controller’s radio resource management (RRM) auto-RF feature by entering **YES** or **no**.

Note The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and transmit power assignment, for the group.

Step 20 If you want the controller to receive its time setting from an external Network Time Protocol (NTP) server when it powers up, enter **YES** to configure an NTP server. Otherwise, enter **no**.

Note The controller network module installed in a Cisco Integrated Services Router does not have a battery and cannot save a time setting. Therefore, it must receive a time setting from an external NTP server when it powers up.

Step 21 If you entered **no** in *Step 20* and want to manually configure the system time on your controller now, enter **YES**. If you do not want to configure the system time now, enter **no**.

Step 22 If you entered **YES** in *Step 21*, enter the current date in the MM/DD/YY format and the current time in the HH:MM:SS format.

After you have completed *step 22*, the wizard prompts you to configure IPv6 parameters. Enter **yes** to proceed.

Step 23 Enter the service port interface IPv6 address configuration. You can enter either **static** or **SLAAC**.

- If you entered, **SLAAC**, then IPv6 address is autoconfigured.
- If you entered, **static**, you need to enter the IPv6 address and its prefix length of the service interface.

Step 24 Enter the IPv6 address of the management interface.

Step 25 Enter the IPv6 address prefix length of the management interface.

Step 26 Enter the gateway IPv6 address of the management interface .

Once the management interface configuration is complete, the wizard prompts to configure IPv6 parameters for RADIUS server. Enter **yes**.

Step 27 Enter the IPv6 address of the RADIUS server.

Step 28 Enter the communication port number of the RADIUS server. The default value is 1812.

Step 29 Enter the secret key for IPv6 address of the RADIUS server.

Once the RADIUS server configuration is complete, the wizard prompts to configure IPv6 NTP server. Enter **yes**.

Step 30 Enter the IPv6 address of the NTP server.

Step 31 When prompted to verify that the configuration is correct, enter **yes** or **NO**.

The controller saves your configuration when you enter **yes**, reboots, and prompts you to log on.

Using the Controller GUI

A browser-based GUI is built into each controller.

It allows up to five users to simultaneously browse into the controller HTTP or HTTPS (HTTP + SSL) management pages to configure parameters and monitor the operational status for the controller and its associated access points.

For detailed descriptions of the Controller GUI, see the Online Help. To access the online help, click **Help** on the Controller GUI.

- The Cisco WLC GUI is supported on the following web browsers:
    - Microsoft Internet Explorer 10 or a later version (Windows)
    - Mozilla Firefox, Version 32 or a later version (Windows, Mac)
    - Google Chrome, Version 38.x or a later version (Windows, Mac)
    - Apple Safari, Version 7 or a later version (Mac)

Note We recommend that you enable the HTTPS interface and disable the HTTP interface to ensure more robust security.

Restrictions on using Controller GUI

Follow these guidelines when using the controller GUI:

- The controller Web UI is compatible with the following web browsers
    - Microsoft Internet Explorer 11 and later versions
    - Mozilla Firefox 32 and later versions
- To view the Main Dashboard that is introduced in Release 8.1.102.0, you must enable JavaScript on the web browser.

Note Ensure that the screen resolution is set to 1280x800 or more. Lesser resolutions are not supported.

- You can use either the service port interface or the management interface to access the GUI.
- You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled.
- Click **Help** at the top of any page in the GUI to display online help. You might need to disable your browser's pop-up blocker to view the online help.

Logging On to the GUI

Note Do not configure TACACS+ authentication when the controller is set to use local authentication.

Step 1 Enter the IP address in your browser's address bar. For a secure connection, enter **`https://ip-address`**. For a less secure connection, enter **`https://ip-address`**.

Step 2 When prompted, enter a valid username and password, and click **OK**.

The **Summary** page is displayed.

Note The administrative username and password that you created in the configuration wizard are case sensitive.

Logging out of the GUI

Step 1 Click **Logout** in the top right corner of the page.

Step 2 Click **Close** to complete the log out process and prevent unauthorized users from accessing the controller GUI.

Step 3 When prompted to confirm your decision, click **Yes**.

Enabling Web and Secure Web Modes

This section provides instructions to enable the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate.

You can configure web and secure web mode using the controller GUI or CLI.

This section contains the following subsections:

Enabling Web and Secure Web Modes (GUI)

Step 1 Choose **Management** > **HTTP-HTTPS**.

The **HTTP-HTTPS Configuration** page is displayed.

Step 2 To enable web mode, which allows users to access the controller GUI using "http://*ip-address*," choose **Enabled** from the **HTTP Access** drop-down list. Otherwise, choose **Disabled**. The default value is Disabled. Web mode is not a secure connection.

Step 3 To enable secure web mode, which allows users to access the controller GUI using "https://*ip-address*," choose **Enabled** from the **HTTPS Access** drop-down list. Otherwise, choose **Disabled**. The default value is Enabled. Secure web mode is a secure connection.

Step 4 In the **Web Session Timeout** field, enter the amount of time, in minutes, before the web session times out due to inactivity. You can enter a value between 10 and 160 minutes (inclusive). The default value is 30 minutes.

Step 5 Click **Apply**.

Step 6 If you enabled secure web mode in Step 3, the controller generates a local web administration SSL certificate and automatically applies it to the GUI. The details of the current certificate appear in the middle of the **HTTP-HTTPS Configuration** page.

Note If desired, you can delete the current certificate by clicking **Delete Certificate** and have the controller generate a new certificate by clicking **Regenerate Certificate**. You have the option to use server side SSL certificate that you can download to controller. If you are using HTTPS, you can use SSC or MIC certificates.

Step 7 Click **Save Configuration**.

Enabling Web and Secure Web Modes (CLI)

Step 1 Enable or disable web mode by entering this command:

config network webmode {**enable** | **disable**}

This command allows users to access the controller GUI using "http://*ip-address*." The default value is disabled. Web mode is not a secure connection.

Step 2 Enable or disable secure web mode by entering this command:

config network secureweb {**enable** | **disable**}

This command allows users to access the controller GUI using "https://*ip-address*." The default value is enabled. Secure web mode is a secure connection.

Step 3 Enable or disable secure web mode with increased security by entering this command:

config network secureweb cipher-option high {**enable** | **disable**}

This command allows users to access the controller GUI using "https://*ip-address*" but only from browsers that support 128-bit (or larger) ciphers. The default value is disabled.

When high ciphers is enabled, SHA1, SHA256, SHA384 keys continue to be listed and TLSv1.0 is disabled. This is applicable to webauth and webadmin but not for NMSP.

Step 4 Enable or disable SSLv2 for web administration by entering this command:

config network secureweb cipher-option sslv2 {**enable** | **disable**}

If you disable SSLv2, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The default value is disabled.

Step 5 Enable 256 bit ciphers for a SSH session by entering this command:

config network ssh cipher-option high {**enable** | **disable**}

Step 6 [Optional] Disable telnet by entering this command:

config network telnet{**enable** | **disable**}

Step 7 Enable or disable preference for RC4-SHA (Rivest Cipher 4-Secure Hash Algorithm) cipher suites (over CBC cipher suites) for web authentication and web administration by entering this command:

config network secureweb cipher-option rc4-preference {**enable** | **disable**}

Step 8 Verify that the controller has generated a certificate by entering this command:

show certificate summary

Information similar to the following appears:

```
Web Administration Certificate................. Locally Generated
Web Authentication Certificate................. Locally Generated
Certificate compatibility mode:................ off
```

Step 9 (Optional) Generate a new certificate by entering this command:

config certificate generate webadmin

After a few seconds, the controller verifies that the certificate has been generated.

Step 10 Save the SSL certificate, key, and secure web password to nonvolatile RAM (NVRAM) so that your changes are retained across reboots by entering this command:

save config

Step 11 Reboot the controller by entering this command:

reset system

Loading an Externally Generated SSL Certificate

This section describes how to load an externally generated SSL certificate.

Loading an Externally Generated SSL Certificate

You can use a supported transfer method such as TFTP server to download an externally generated SSL certificate to the controller. Follow these guidelines for using TFTP:

- If you load the certificate through the service port, the TFTP server must be on the same subnet as the controller because the service port is not routable, or you must create static routes on the controller. Also, if you load the certificate through the distribution system network port, the TFTP server can be on any subnet.

- A third-party TFTP server cannot run on the same PC as the Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.

Note Chained certificates are supported for web authentication and management certificate.

CSR compliance with RFC-5280

With all parameters in CSR aligned with RFC-5280, there are some restrictions as follows:

- *emailAddress* in CSR can only be 128 characters long.
- If the CSR is generated using the CLI, the maximum number of characters (of all input combined for CSR) is limited to 500 including **config certificate generate csr-*****.

Related Documentation

Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC—https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html

Loading an SSL Certificate (GUI)

Step 1 Choose **Security** > **Web Auth** > **Certificate**.

Step 2 On the **Web Authentication Certificate** page, check the **Download SSL Certificate** check box.

Note On the controller GUI, only TFTP transfer mode is used. You can use other methods such as FTP, and so on, on the controller CLI.

Step 3 In the **Server IP Address** field, enter the IP address of the TFTP server.

Step 4 In the **Maximum Retries** field, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 5 In the **Timeout** field, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 6 In the **Certificate File Path** field, enter the directory path of the certificate.

Step 7 In the **Certificate File Name** field, enter the name of the certificate (webadmincert_name.pem).

Step 8 (Optional) In the **Certificate Password** field, enter a password to encrypt the certificate.

Step 9 Save the configuration.

Step 10 Choose **Commands** > **Reboot** > **Reboot** > **Save and Reboot** to reboot the controller for your changes to take effect,

Loading an SSL Certificate (CLI)

The procedure described in this section is similar for both webauthcert and webadmincert installation, with the difference being in the download of the datatype.

Step 1 Use a password to encrypt the HTTPS certificate in a .PEM-encoded file. The PEM-encoded file is called a web administration certificate file (`webadmincert_name.pem`).

Step 2 Move the `webadmincert_name.pem` file to the default directory on your TFTP server.

Step 3 To view the current download settings, enter this command and answer **n** to the prompt:

transfer download start

Information similar to the following appears:

```
Mode........................................... TFTP
Data Type...................................... Admin Cert
TFTP Server IP................................. xxx.xxx.xxx.xxx
TFTP Path...................................... <directory path>
TFTP Filename..................................
Are you sure you want to start? (y/n) n
Transfer Canceled
```

Step 4 Use these commands to change the download settings:

transfer download mode *tftp*

transfer download datatype *webadmincert*

transfer download serverip *TFTP_server IP_address*

transfer download path *absolute_TFTP_server_path_to_the_update_file*

transfer download filename *webadmincert_name.pem*

Step 5 To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, enter this command:

transfer download certpassword *private_key_password*

Step 6 To confirm the current download settings and start the certificate and key download, enter this command and answer **y** to the prompt:

transfer download start

Information similar to the following appears:

```
Mode........................................... TFTP
Data Type...................................... Site Cert
TFTP Server IP................................. xxx.xxx.xxx.xxx
TFTP Path...................................... directory path
TFTP Filename.................................. webadmincert_name
Are you sure you want to start? (y/n) y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

Step 7 To save the SSL certificate, key, and secure web password to NVRAM so that your changes are retained across reboots, enter this command:

save config

Step 8 To reboot the controller, enter this command:

reset system

Using the Controller CLI

A Cisco UWN solution command-line interface (CLI) is built into each controller. The CLI enables you to use a VT-100 terminal emulation program to locally or remotely configure, monitor, and control individual controllers and its associated lightweight access points. The CLI is a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulation programs to access the controller.

Note For more information about specific commands, see the *Cisco Wireless Controller Command Reference* for relevant releases at:

https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-command-reference-list.html

Logging on to the Controller CLI

You can access the controller CLI using either of the following methods:

- A direct serial connection to the controller console port
- A remote session over the network using Telnet or SSH through the preconfigured service port or the distribution system ports

For more information about ports and console connection options on controllers, see the relevant controller platform's installation guide.

Using a Serial or USB Console Connection on Cisco WLC

On Cisco 5508 WLCs, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller's USB console port and the other end of the cable into the PC's USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.

See the Telnet and Secure Shell Sessions section for information on enabling Telnet sessions.

Using a Local Serial Connection

Before you begin

You need these items to connect to the serial port:

- A computer that is running a terminal emulation program such as Putty, SecureCRT, or similar
- A standard Cisco console serial cable with an RJ45 connector

To log on to the controller CLI through the serial port, follow these steps:

Step 1 Connect console cable—Connect one end of a standard Cisco console serial cable with an RJ45 connector to the controller's console port and the other end to your PC's serial port.

Step 2 Configure terminal emulator program with default settings:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

Note The controller serial port is set for a 9600 baud rate and a short timeout. If you would like to change either of these values, run the **config serial baudrate** *value* and **config serial timeout** *value* to make your changes. If you set the serial timeout value to 0, serial sessions never time out.

If you change the console speed to a value other than 9600, the console speed used by controller will be 9600 during boot and will only change upon the completion of boot process. Therefore, we recommend that you do not change the console speed, except as a temporary measure on an as-needed basis.

Step 3 Log on to the CLI—When prompted, enter a valid username and password to log on to the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note The default username is admin, and the default password is admin.

The CLI displays the root level system prompt:

(Cisco Controller) >

Note The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the **config prompt** command.

Using a Remote Telnet or SSH Connection

Before you begin

You need these items to connect to a controller remotely:

- A PC with network connectivity to either the management IP address, the service port address, or if management is enabled on a dynamic interface of the controller in question
- The IP address of the controller
- A VT-100 terminal emulation program or a DOS shell for the Telnet session

Note By default, controllers block Telnet sessions. You must use a local connection to the serial port to enable Telnet sessions.

Note The **aes-cbc ciphers** are not supported on WLC. The SSH client which is used to log in to the WLC should have minimum a non-aes-cbc cipher.

Step 1 Verify that your VT-100 terminal emulation program or DOS shell interface is configured with these parameters:

- Ethernet address
- Port 23

Step 2 Use the controller IP address to Telnet to the CLI.

Step 3 When prompted, enter a valid username and password to log into the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note The default username is admin, and the default password is admin.

The CLI displays the root level system prompt.

Note The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the **config prompt** command.

Logging Out of the CLI

When you finish using the CLI, navigate to the root level and enter **logout**. The system prompts you to save any changes you made to the volatile RAM.

Note The CLI automatically logs you out without saving any changes after 5 minutes of inactivity. You can set the automatic logout from 0 (never log out) to 160 minutes using the **config serial timeout** command.

To prevent SSH or Telnet sessions from timing out, run the **config sessions timeout***0* command.

Navigating the CLI

- When you log into the CLI, you are at the root level. From the root level, you can enter any full command without first navigating to the correct command level.

- If you enter a top-level keyword such as **config**, **debug**, and so on without arguments, you are taken to the submode of that corresponding keyword.
- `Ctrl + Z` or entering **exit** returns the CLI prompt to the default or root level.
- When navigating to the CLI, enter **?** to see additional options available for any given command at the current level.
- You can also enter the space or tab key to complete the current keyword if unambigious.
- Enter **help** at the root level to see available command line editing options.

The following table lists commands you use to navigate the CLI and to perform common tasks.

Table 1: Commands for CLI Navigation and Common Tasks

Command	Action
help	At the root level, view system wide navigation commands
?	View commands available at the current level
command ?	View parameters for a specific command
exit	Move down one level
Ctrl + Z	Return from any level to the root level
save config	At the root level, save configuration changes from active working RAM to nonvolatile RAM (NVRAM) so they are retained after reboot
reset system	At the root level, reset the controller without logging out
logout	Logs you out of the CLI

Using the AutoInstall Feature for Controllers Without a Configuration

When you boot up a controller that does not have a configuration, the AutoInstall feature can download a configuration file from a TFTP server and then load the configuration onto the controller automatically.

If you create a configuration file on a controller that is already on the network (or through a Prime Infrastructure filter), place that configuration file on a TFTP server, and configure a DHCP server so that a new controller can get an IP address and TFTP server information, the AutoInstall feature can obtain the configuration file for the new controller automatically.

When the controller boots, the AutoInstall process starts. The controller does not take any action until AutoInstall is notified that the configuration wizard has started. If the wizard has not started, the controller has a valid configuration.

If AutoInstall is notified that the configuration wizard has started (which means that the controller does not have a configuration), AutoInstall waits for an additional 30 seconds. This time period gives you an opportunity to respond to the first prompt from the configuration wizard:

```
Would you like to terminate autoinstall? [yes]:
```

When the 30-second terminate timeout expires, AutoInstall starts the DHCP client. You can terminate the AutoInstall task even after this 30-second timeout if you enter **Yes** at the prompt. However, AutoInstall cannot be terminated if the TFTP task has locked the flash and is in the process of downloading and installing a valid configuration file.

Note The AutoInstall process and manual configuration using both the GUI and CLI of controller can occur in parallel. As part of the AutoInstall cleanup process, the service port IP address is set to 192.168.1.1 and the service port protocol configuration is modified. Because the AutoInstall process takes precedence over the manual configuration, whatever manual configuration is performed is overwritten by the AutoInstall process.

Information About the AutoInstall Feature

When you boot up a controller that does not have a configuration, the AutoInstall feature can download a configuration file from a TFTP server and then load the configuration onto the controller automatically.

If you create a configuration file on a controller that is already on the network (or through a Prime Infrastructure filter), place that configuration file on a TFTP server, and configure a DHCP server so that a new controller can get an IP address and TFTP server information, the AutoInstall feature can obtain the configuration file for the new controller automatically.

When the controller boots, the AutoInstall process starts. The controller does not take any action until AutoInstall is notified that the configuration wizard has started. If the wizard has not started, the controller has a valid configuration.

If AutoInstall is notified that the configuration wizard has started (which means that the controller does not have a configuration), AutoInstall waits for an additional 30 seconds. This time period gives you an opportunity to respond to the first prompt from the configuration wizard:

```
Would you like to terminate autoinstall? [yes]:
```

When the 30-second termination timeout expires, AutoInstall starts the DHCP client. You can terminate the AutoInstall task even after this 30-second timeout if you enter **Yes** at the prompt. However, AutoInstall cannot be terminated if the TFTP task has locked the flash and is in the process of downloading and installing a valid configuration file.

Note The AutoInstall process and manual configuration using both the GUI and CLI of Cisco WLC can occur in parallel. As part of the AutoInstall cleanup process, the service port IP address is set to 192.168.1.1 and the service port protocol configuration is modified. Because the AutoInstall process takes precedence over the manual configuration, whatever manual configuration is performed is overwritten by the AutoInstall process.

Restrictions on AutoInstall

- In Cisco 5508 WLCs, the following interfaces are used:
  - eth0—Service port (untagged)
  - dtl0—Gigabit port 1 through the NPU (untagged)
- AutoInstall is not supported on Cisco 2504 WLC.

Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server

AutoInstall attempts to obtain an IP address from the DHCP server until the DHCP process is successful or until you terminate the AutoInstall process. The first interface to successfully obtain an IP address from the DHCP server registers with the AutoInstall task. The registration of this interface causes AutoInstall to begin the process of obtaining TFTP server information and downloading the configuration file.

Following the acquisition of the DHCP IP address for an interface, AutoInstall begins a short sequence of events to determine the host name of the controller and the IP address of the TFTP server. Each phase of this sequence gives preference to explicitly configured information over default or implied information and to explicit host names over explicit IP addresses.

The process is as follows:

- If at least one Domain Name System (DNS) server IP address is learned through DHCP, AutoInstall creates a /etc/resolv.conf file. This file includes the domain name and the list of DNS servers that have been received. The Domain Name Server option provides the list of DNS servers, and the Domain Name option provides the domain name.
- If the domain servers are not on the same subnet as the controller, static route entries are installed for each domain server. These static routes point to the gateway that is learned through the DHCP Router option.
- The host name of the controller is determined in this order by one of the following:
  - If the DHCP Host Name option was received, this information (truncated at the first period [.]) is used as the host name for the controller.
  - A reverse DNS lookup is performed on the controller IP address. If DNS returns a hostname, this name (truncated at the first period [.]) is used as the hostname for the controller.
- The IP address of the TFTP server is determined in this order by one of the following:
  - If AutoInstall received the DHCP TFTP Server Name option, AutoInstall performs a DNS lookup on this server name. If the DNS lookup is successful, the returned IP address is used as the IP address of the TFTP server.
  - If the DHCP Server Host Name (sname) text box is valid, AutoInstall performs a DNS lookup on this name. If the DNS lookup is successful, the IP address that is returned is used as the IP address of the TFTP server.

  - If AutoInstall received the DHCP TFTP Server Address option, this address is used as the IP address of the TFTP server.
  - AutoInstall performs a DNS lookup on the default TFTP server name (cisco-wlc-tftp). If the DNS lookup is successful, the IP address that is received is used as the IP address of the TFTP server.
  - If the DHCP server IP address (siaddr) text box is nonzero, this address is used as the IP address of the TFTP server.
  - The limited broadcast address (255.255.255.255) is used as the IP address of the TFTP server.

- If the TFTP server is not on the same subnet as the controller, a static route (/32) is installed for the IP address of the TFTP server. This static route points to the gateway that is learned through the DHCP Router option.

Selecting a Configuration File

After the hostname and TFTP server have been determined, AutoInstall attempts to download a configuration file. AutoInstall performs three full download iterations on each interface that obtains a DHCP IP address. If the interface cannot download a configuration file successfully after three attempts, the interface does not attempt further.

The first configuration file that is downloaded and installed successfully triggers a reboot of the controller. After the reboot, the controller runs the newly downloaded configuration.

AutoInstall searches for configuration files in the order in which the names are listed:

- The filename that is provided by the DHCP Boot File Name option
- The filename that is provided by the DHCP File text box
- *host name*-confg
- *host name*.cfg
- *base MAC addres*s-confg (for example, 0011.2233.4455-confg)
- *serial number*-confg
- ciscowlc-confg
- ciscowlc.cfg

AutoInstall runs through this list until it finds a configuration file. It stops running if it does not find a configuration file after it cycles through this list three times on each registered interface.

Note

- The downloaded configuration file can be a complete configuration, or it can be a minimal configuration that provides enough information for the controller to be managed by the Cisco Prime Infrastructure. Full configuration can then be deployed directly from the Prime Infrastructure.
- AutoInstall does not expect the switch connected to the controller to be configured for either channels. AutoInstall works with a service port in LAG configuration.
- Cisco Prime Infrastructure provides AutoInstall capabilities for controllers. A Cisco Prime Infrastructure administrator can create a filter that includes the host name, the MAC address, or the serial number of the controller and associate a group of templates (a configuration group) to this filter rule. The Prime Infrastructure pushes the initial configuration to the controller when the controller boots up initially. After the controller is discovered, the Prime Infrastructure pushes the templates that are defined in the configuration group. For more information about the AutoInstall feature and Cisco Prime Infrastructure, see the Cisco Prime Infrastructure documentation.

Example: AutoInstall Operation

The following is an example of an AutoInstall process from start to finish:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Filename ==> 'abcd-confg'
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Server IP ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'service-port' - setting DHCP yiaddr ==> 172.19.29.253
AUTO-INSTALL: interface 'service-port' - setting DHCP Netmask ==> 255.255.255.0
AUTO-INSTALL: interface 'service-port' - setting DHCP Gateway ==> 172.19.29.1
AUTO-INSTALL: interface 'service-port' registered
AUTO-INSTALL: interation 1 -- interface 'service-port'
AUTO-INSTALL: DNS reverse lookup 172.19.29.253 ===> 'wlc-1'
AUTO-INSTALL: hostname 'wlc-1'
AUTO-INSTALL: TFTP server 1.100.108.2 (from DHCP Option 150)
AUTO-INSTALL: attempting download of 'abcd-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: interface 'management' - setting DHCP file ==> 'bootfile1'
AUTO-INSTALL: interface 'management' - setting DHCP TFTP Filename ==> 'bootfile2-config'
AUTO-INSTALL: interface 'management' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[1] ==> 1.100.108.3
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[2] ==> 1.100.108.4
AUTO-INSTALL: interface 'management' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'management' - setting DHCP yiaddr ==> 1.100.108.238
AUTO-INSTALL: interface 'management' - setting DHCP Netmask ==> 255.255.254.0
AUTO-INSTALL: interface 'management' - setting DHCP Gateway ==> 1.100.108.1
AUTO-INSTALL: interface 'management' registered
AUTO-INSTALL: TFTP status - 'Config file transfer failed - Error from server: File not
found' (3)
AUTO-INSTALL: attempting download of 'wlc-1-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... updating configuration.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... storing in flash.' (2)
```

```
AUTO-INSTALL: TFTP status - 'System being reset.' (2)
Resetting system
```

Managing the Controller System Date and Time

You can configure the controller system date and time at the time of configuring the controller using the configuration wizard. If you did not configure the system date and time through the configuration wizard or if you want to change your configuration, you can follow the instructions in this section to configure the controller to obtain the date and time from a Network Time Protocol (NTP) server or to configure the date and time manually. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

You can also configure an authentication mechanism between various NTP servers.

Information About Controller System Date and Time

You can configure the controller system date and time at the time of configuring the controller using the configuration wizard. If you did not configure the system date and time through the configuration wizard or if you want to change your configuration, you can follow the instructions in this section to configure the controller to obtain the date and time from a Network Time Protocol (NTP) server or to configure the date and time manually. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

You can also configure an authentication mechanism between various NTP servers.

Restrictions on Configuring the Controller Date and Time

- If you are configuring wIPS, you must set the controller time zone to UTC.
- Cisco Aironet lightweight access points might not connect to the controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.
- You can configure an authentication channel between the controller and the NTP server.

Configuring the NTP/SNTP Server to Obtain the Date and Time (CLI)

Use these commands to configure an NTP/SNTP server to obtain the date and time:

Procedure

- To specify the NTP/SNTP server for the controller, enter this command:

  config time ntp server *index ip-address*

- (Optional) To specify the polling interval (in seconds), enter this command:

  config time ntp *interval*

- To enable or disable NTP/SNTP server authentication, enter these commands:

  - **config time ntp auth enable** *server-index key-index*—Enables NTP/SNTP authentication on a given NTP/SNTP server.
  - **config time ntp key-auth add** *key-index* **md5** {**ascii** | **hex**} *key*—Adds an authentication key. By default MD5 is used. The key format can be ASCII or hexadecimal.
  - **config time ntp key-auth delete** *key-index*—Deletes authentication keys.
  - **config time ntp auth disable** *server-index*—Disables NTP/SNTP authentication.
  - **show ntp-keys**—Displays the NTP/SNTP authentication related parameter.

- To delete an NTP server IP address or DNS server from the controller, enter this command:

  config time ntp delete *NTP_server index*

Configuring NTP/SNTP Authentication (GUI)

Step 1 Choose **Controller > NTP > Servers** to open the **NTP Servers** page.

Step 2 Click **New** to add an NTP server.

Step 3 Choose a server priority from the **Server Index (Priority)** drop-down list.

Step 4 Enter the NTP server IPv4/IPv6 address in the **Server IP Address (IPv4/IPv6)** text box.

Step 5 Enable NTP server authentication by checking the **NTP Server Authentication** check box.

Step 6 Click **Apply**.

Step 7 Choose **Controller** > **NTP** > **Keys**.

Step 8 Click **New** to create a key.

Step 9 Enter the key index in the **Key Index** text box.

Step 10 Choose the key format from the **Key Format** drop-down list.

Step 11 Enter the key in the **Key** text box.

Step 12 Click **Apply**.

Configuring NTP/SNTP Authentication (CLI)

Note By default, MD5 is used.

- **config time ntp auth enable** *server-index key-index*
- **config time ntp auth disable** *server-index*
- **config time ntp key-auth add key-index md5** *key-format key*
- Delete an authentication key by entering this command:

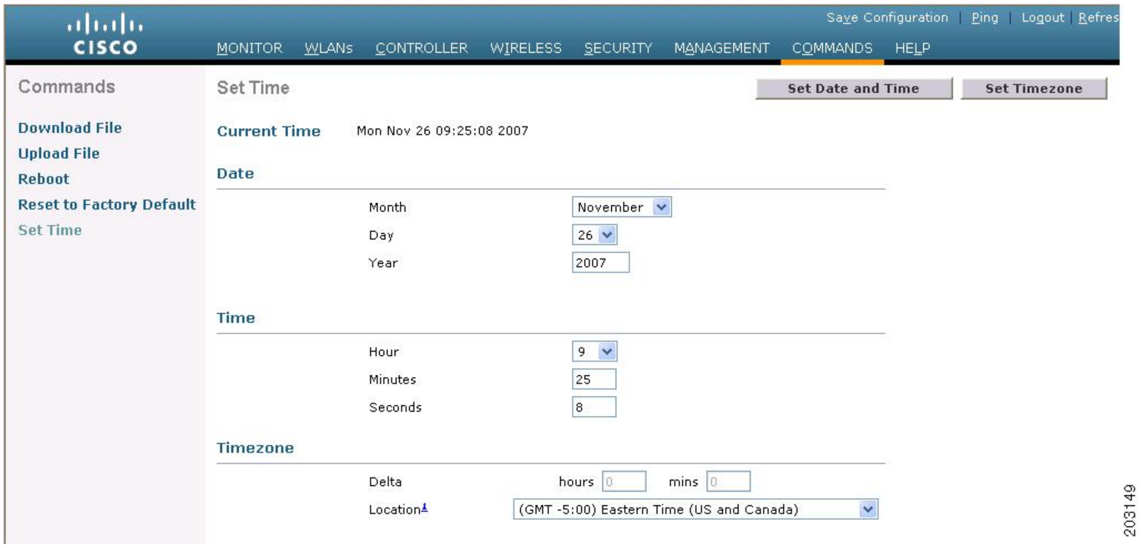
  config time ntp key-auth delete *key-index*
- View the list of NTP/SNTP key Indices by entering this command:

  show ntp-keys

Configuring the Date and Time (GUI)

Step 1 Choose **Commands > Set Time** to open the **Set Time** page.

Figure 12: Set Time Page



Set Time

Current Time Mon Nov 26 09:25:08 2007

Date

Month November

Day 26

Year 2007

Time

Hour 9

Minutes 25

Seconds 8

Timezone

Delta hours 0 mins 0

Location[1] (GMT -5:00) Eastern Time (US and Canada)

The current date and time appear at the top of the page.

Step 2 In the **Timezone** area, choose your local time zone from the **Location** drop-down list.

Note 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.

Note You cannot set the time zone delta on the controller GUI. However, if you do so on the controller CLI, the change is reflected in the **Delta Hours** and **Mins** boxes on the controller GUI.

Step 3 Click **Set Timezone** to apply your changes.

Step 4 In the **Date** area, choose the current local month and day from the **Month** and **Day** drop-down lists, and enter the year in the **Year** box.

Step 5 In the **Time** area, choose the current local hour from the **Hour** drop-down list, and enter the minutes and seconds in the **Minutes** and **Seconds** boxes.

Note If you change the time zone location after setting the date and time, the values in the Time area are updated to reflect the time in the new time zone location. For example, if the controller is currently configured for noon Eastern time and you change the time zone to Pacific time, the time automatically changes to 9:00 a.m.

Step 6 Click **Set Date and Time** to apply your changes.

Step 7 Click **Save Configuration**.

Configuring the Date and Time (CLI)

Step 1 Configure the current local date and time in GMT on the controller by entering this command:

config time manual *mm/dd/yy hh:mm:ss*

Note When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8:00 a.m. Pacific time in the United States, you would enter 16:00 because the Pacific time zone is 8 hours behind GMT.

Step 2 Perform one of the following to set the time zone for the controller:

- Set the time zone location in order to have Daylight Saving Time (DST) set automatically when it occurs by entering this command:

  config time timezone location *location_index*

  where *location_index* is a number representing one of the following time zone locations:

  a. (GMT-12:00) International Date Line West

  b. (GMT-11:00) Samoa

  c. (GMT-10:00) Hawaii

  d. (GMT-9:00) Alaska

  e. (GMT-8:00) Pacific Time (US and Canada)

  f. (GMT-7:00) Mountain Time (US and Canada)

  g. (GMT-6:00) Central Time (US and Canada)

  h. (GMT-5:00) Eastern Time (US and Canada)

  i. (GMT-4:00) Atlantic Time (Canada)

  j. (GMT-3:00) Buenos Aires (Argentina)

k. (GMT-2:00) Mid-Atlantic

l. (GMT-1:00) Azores

m. (GMT) London, Lisbon, Dublin, Edinburgh (default value)

n. (GMT +1:00) Amsterdam, Berlin, Rome, Vienna

o. (GMT +2:00) Jerusalem

p. (GMT +3:00) Baghdad

q. (GMT +4:00) Muscat, Abu Dhabi

r. (GMT +4:30) Kabul

s. (GMT +5:00) Karachi, Islamabad, Tashkent

t. (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi

u. (GMT +5:45) Katmandu

v. (GMT +6:00) Almaty, Novosibirsk

w. (GMT +6:30) Rangoon

x. (GMT +7:00) Saigon, Hanoi, Bangkok, Jakarta

y. (GMT +8:00) Hong Kong, Beijing, Chongqing

z. (GMT +9:00) Tokyo, Osaka, Sapporo

aa. (GMT +9:30) Darwin

ab. (GMT+10:00) Sydney, Melbourne, Canberra

ac. (GMT+11:00) Magadan, Solomon Is., New Caledonia

ad. (GMT+12:00) Kamchatka, Marshall Is., Fiji

ae. (GMT+12:00) Auckland (New Zealand)

Note If you enter this command, the controller automatically sets its system clock to reflect DST when it occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

- Manually set the time zone so that DST is not set automatically by entering this command:

  config time timezone *delta_hours delta_mins*

  where *delta_hours* is the local hour difference from GMT, and *delta_mins* is the local minute difference from GMT.

  When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/–). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as –8.

  Note You can manually set the time zone and prevent DST from being set only on the controller CLI.

Step 3 Save your changes by entering this command:

save config

Step 4 Verify that the controller shows the current local time with respect to the local time zone by entering this command:

show time

Information similar to the following appears:

```
Time.................................... Thu Apr  7 13:56:37 2011
Timezone delta........................... 0:0
Timezone location....................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata

NTP Servers
    NTP Polling Interval........................     3600

     Index     NTP Key Index     NTP Server       NTP Msg Auth Status
    -------  ---------------------------------------------------------------
       1              1           209.165.200.225      AUTH SUCCESS
```

Note If you configured the time zone location, the Timezone Delta value is set to “0:0.” If you manually configured the time zone using the time zone delta, the Timezone Location is blank.

Telnet and Secure Shell Sessions

Telnet and Secure Shell Sessions

Telnet is a network protocol used to provide access to the controller’s CLI. Secure Shell (SSH) is a more secure version of Telnet that uses data encryption and a secure channel for data transfer. You can use the controller GUI or CLI to configure Telnet and SSH sessions.

This section contains the following subsections:

Restrictions

- When the tool **Putty** is used as an SSH client to connect to the controller running versions 8.6 and above, you may observe disconnects from **Putty** when a large output is requested with paging disabled. This is observed when the controller has lots of configurations and/ or has a high count of APs and clients. We recomend you to use alternate SSH clients in such situations.
- In Release 8.6, controllers are migrated from OpenSSH to libssh, and libssh does not support these key exchange (KEX) algorithms: *ecdh-sha2-nistp384* and *ecdh-sha2-nistp521*. Only *ecdh-sha2-nistp256* is supported.

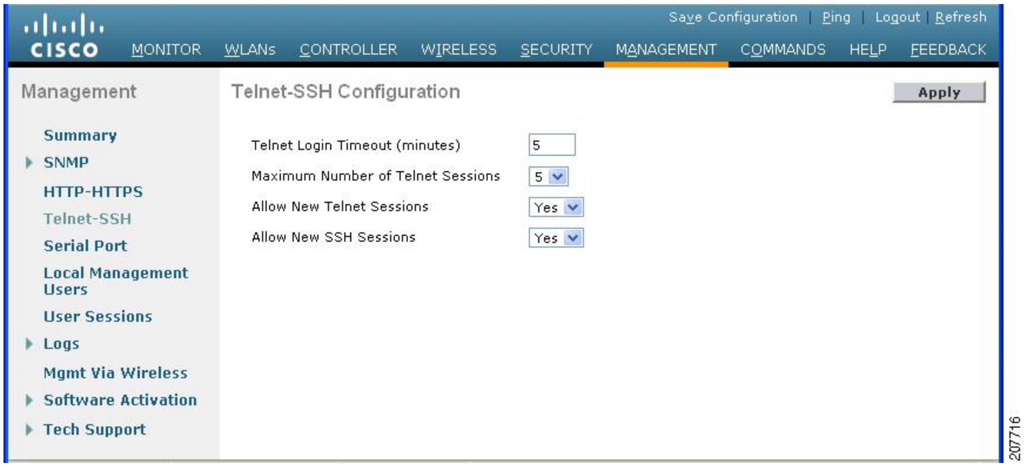
Restrictions on Telnet and SSH

- Only the FIPS approved algorithm aes128-cbc is supported when using SSH to control WLANs.
- The controller does not support raw Telnet mode.

Configuring Telnet and SSH Sessions (GUI)

Step 1 Choose **Management** > **Telnet-SSH** to open the Telnet-SSH Configuration page.

Figure 13: Telnet-SSH Configuration Page



Telnet-SSH Configuration

Telnet Login Timeout (minutes) 5

Maximum Number of Telnet Sessions 5

Allow New Telnet Sessions Yes

Allow New SSH Sessions Yes

Step 2 In the **Telnet Login Timeout** text box, enter the number of minutes that a Telnet session is allowed to remain inactive before being terminated. The valid range is 0 to 160 minutes (inclusive), and the default value is 5 minutes. A value of 0 indicates no timeout.

Step 3 From the **Maximum Number of Sessions** drop-down list, choose the number of simultaneous Telnet or SSH sessions allowed. The valid range is 0 to 5 sessions (inclusive), and the default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

Step 4 To forcefully close current login sessions, choose **Management** > **User Sessions** > **close** from the CLI session drop-down list.

Step 5 From the **Allow New Telnet Sessions** drop-down list, choose **Yes** or **No** to allow or disallow new Telnet sessions on the controller. The default value is No.

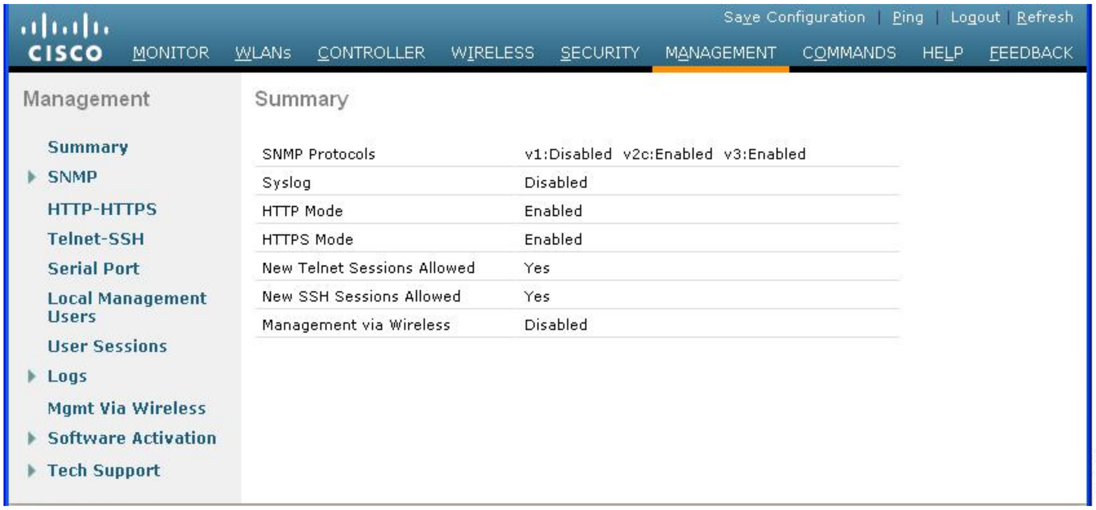
Step 6 From the \ drop-down list, choose **Yes** or **No** to allow or disallow new SSH sessions on the controller. The default value is Yes.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Step 9 To see a summary of the Telnet configuration settings, choose **Management** > **Summary**. The Summary page appears.

Figure 14: Summary Page



Summary

SNMP Protocols	v1:Disabled v2c:Enabled v3:Enabled
Syslog	Disabled
HTTP Mode	Enabled
HTTPS Mode	Enabled
New Telnet Sessions Allowed	Yes
New SSH Sessions Allowed	Yes
Management via Wireless	Disabled

This page shows whether additional Telnet and SSH sessions are permitted.

Configuring Telnet and SSH Sessions (CLI)

Step 1 Allow or disallow new Telnet sessions on the controller by entering this command:

config network telnet {**enable** | **disable**}

The default value is disabled.

Step 2 Allow or disallow new SSH sessions on the controller by entering this command:

config network ssh {**enable** | **disable**}

The default value is enabled.

Note Use the **config network ssh cipher-option high** {**enable** | **disable**} command to enable sha2 which is supported in WLC.

Step 3 (Optional) Specify the number of minutes that a Telnet session is allowed to remain inactive before being terminated by entering this command:

config sessions timeout *timeout*

where *timeout* is a value between 0 and 160 minutes (inclusive). The default value is 5 minutes. A value of 0 indicates no timeout.

Step 4 (Optional) Specify the number of simultaneous Telnet or SSH sessions allowed by entering this command:

config sessions maxsessions *session_num*

where *session_num* is a value between 0 and 5 (inclusive). The default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

Step 5 Save your changes by entering this command:

save config

Step 6 You can close all the Telnet or SSH sessions by entering this command:

config loginsession close {*session-id* | *all*}

The *session-id* can be taken from the **show login-session** command.

Managing and Monitoring Remote Telnet and SSH Sessions

Step 1 See the Telnet and SSH configuration settings by entering this command:

show network summary

Information similar to the following appears:

```
RF-Network Name............................. TestNetwork1
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Shell (ssh).......................... Enable
Telnet.................................. Disable
...
```

Step 2 See the Telnet session configuration settings by entering this command:

show sessions

Information similar to the following appears:

```
CLI Login Timeout (minutes)............ 5
Maximum Number of CLI Sessions....... 5
```

Step 3 See all active Telnet sessions by entering this command:

show login-session

Information similar to the following appears:

```
ID    User Name     Connection From   Idle Time    Session Time
-- ---------------  ---------------  ------------  ------------
00    admin        EIA-232       00:00:00      00:19:04
```

Configuring Telnet Privileges for Selected Management Users (GUI)

Using the controller, you can configure Telnet privileges to selected management users. To do this, you must have enabled Telnet privileges at the global level. By default, all management users have Telnet privileges enabled.

Note SSH sessions are not affected by this feature.

Step 1 Choose **Management** > **Local Management Users**.

Step 2 On the **Local Management Users** page, select or unselect the **Telnet Capable** check box for a management user.

Step 3 Save the configuration.

Configuring Telnet Privileges for Selected Management Users (CLI)

Procedure

- Configure Telnet privileges for a selected management user by entering this command:

  config mgmtuser telnet *user-name* {**enable** | **disable**}

Troubleshooting Access Points Using Telnet or SSH

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller.

- The **upgrade** command cannot be used when a Telnet or SSH session is enabled.

Troubleshooting Access Points Using Telnet or SSH (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the **All APs** page.

Step 2 Click the name of the access point for which you want to enable Telnet or SSH.

Step 3 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

Step 4 Select the **Telnet** check box to enable Telnet connectivity on this access point. The default value is unchecked.

Step 5 Select the **SSH** check box to enable SSH connectivity on this access point. The default value is unchecked.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Troubleshooting Access Points Using Telnet or SSH (CLI)

Step 1 Enable Telnet or SSH connectivity on an access point by entering this command:

config ap {**telnet** | **ssh**} **enable** *Cisco_AP*

The default value is disabled.

Note Disable Telnet or SSH connectivity on an access point by entering this command: **config ap** {**telnet** | **ssh**} **disable** *Cisco_AP*

Step 2 Save your changes by entering this command:

save config

Step 3 See whether Telnet or SSH is enabled on an access point by entering this command:

show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 5
Cisco AP Name.................................... AP33
Country code..................................... Multiple Countries:US,AE,AR,AT,AU,BH
Reg. Domain allowed by Country................... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 2
MAC Address...................................... 00:19:2f:11:16:7a
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.22.8.133
IP NetMask....................................... 255.255.248.0
Gateway IP Addr.................................. 10.22.8.1
Domain...........................................
Name Server......................................
Telnet State..................................... Enabled
Ssh State........................................ Enabled
...
```

Managing the Controller Wirelessly

You can monitor and configure controllers using a wireless client. This feature is supported for all management tasks except uploads from and downloads to the controller.

Before you can open the GUI or the CLI from a wireless client device, you must configure the controller to allow the connection.

Enabling Wireless Connections (GUI)

Step 1 Log onto the GUI.

Step 2 Choose **Management** > **Mgmt Via Wireless** page.

Step 3 Enable the Controller Management to be accessible from wireless clients.

Step 4 Click **Apply**.

Enabling Wireless Connections (CLI)

Step 1 Log onto the CLI.

Step 2 Enter the **config network mgmt-via-wireless enable** command.

Step 3 Use a wireless client to associate to a lightweight access point connected to the controller.

Step 4 On the wireless client, open a Telnet session to the controller, or browse to the controller GUI.