Initial Setup

Cisco WLAN Express Setup

Cisco WLAN Express Setup is a simplified, out-of-the-box installation and configuration interface for Cisco Wireless Controllers. This section provides instructions to set up a controller to operate in a small, medium, or large network wireless environment, where access points can join and together as a simple solution provide various services such as corporate employee or guest wireless access on the network.

There are two methods:

- Wired method
- Wireless method

With this, there are three ways to set up a controller:

- Cisco WLAN Express Setup
- Traditional command line interface (CLI) through serial console
- Updated method using network connection directly to the controller GUI setup wizard

Note Cisco WLAN Express Setup can be used only for the first time in out-of-the-box installations or when controller configuration is reset to factory defaults.

Feature History

- Release 7.6.120.0: This feature was introduced and supported only on Cisco 2500 Series Wireless Controller. It includes an easy-to-use GUI Configuration Wizard, an intuitive monitoring dashboard and several Cisco Wireless LAN best practices enabled by default.
- Release 8.0.110.0: The following enhancements were made:

- Connect to any port: You can connect a client device to any port on the Cisco 2500 Series Wireless Controller and access the GUI configuration wizard to run Cisco WLAN Express. Previously, you were required to connect the client device to only port 2.
- Wireless Support to run Cisco WLAN Express: You can connect an AP to any of the ports on the Cisco 2500 Series Wireless Controller, associate a client device with the AP, and run Cisco WLAN Express. When the AP is associated with the Cisco 2500 Series Wireless Controller, only 802.11b and 802.11g radios are enabled; the 802.11a radio is disabled. The AP broadcasts an SSID named *CiscoAirProvision*, which is of WPA2-PSK type with the key being *password*. After a client device associates with this SSID, the client device automatically gets an IP address in the 192.168.x.x range. On the web browser of the client device, go to http://192.168.1.1 to open the GUI configuration wizard.

Note This feature is not supported on mobile devices such as smartphones and tablet computers.

- Release 8.1: The following enhancements are made:
  - Added support for the Cisco WLAN Express using the wired method to Cisco 5500, Flex 7500, 8500 Series Wireless Controllers and Cisco Virtual Wireless Controller.
  - Introduced the Main Dashboard view and compliance assessment and best practices. For more details, see the controller Online Help.

Configuration Checklist

The following checklist is for your reference to make the installation process easy. Ensure that you have these requirements ready before you proceed:

1. Network switch requirements:
   a. Controller switch port number assigned
   b. Controller assigned switch port
   c. Is the switch port configured as trunk or access?
   d. Is there a management VLAN? If yes, Management VLAN ID
   e. Is there a guest VLAN? If yes, Guest VLAN ID
2. Controller Settings:
   a. New admin account name
   b. Admin account password
   c. System name for the controller
   d. Current time zone
   e. Is there an NTP server available? If yes, NTP server IP address

Note We recommend using a reachable NTP server IP address. APs do not support FQDN in a day0 scenario.

   f. Controller Management Interface:
      1. IP address
      2. Subnet Mask
      3. Default gateway
   g. Management VLAN ID

3. Corporate wireless network
4. Corporate wireless name or SSID
5. Is a RADIUS server required?
6. Security authentication option to select:
   a. WPA/WPA2 Personal
   b. Corporate passphrase (PSK)
   c. WPA/WPA2 (Enterprise)
   d. RADIUS server IP address and shared secret
7. Is a DHCP server known? If yes, DHCP server IP address
8. Guest Wireless Network (optional)
   a. Guest wireless name/SSID
   b. Is a password required for guest?
   c. Guest passphrase (PSK)
   d. Guest VLAN ID
   e. Guest networking
      1. IP address
      2. Subnet Mask
      3. Default gateway
9. Advanced option: Configure RF Parameters for Client Density as Low, Medium, or High.

Preparing for Setup Using Cisco WLAN Express

- Do not auto-configure the controller or use the wizard for configuration.
- Do not use console interface; the only connection to the controller should be client connected to service port.

- Configure DHCP or assign static IP 192.168.1.X to laptop interface connected to service port.

For more information about Cisco WLAN Express, see WLAN Express Setup and Best Practices Deployment Guide.

This section contains the following subsections:

Setting up Cisco Wireless Controller using Cisco WLAN Express (Wired Method)

Procedure

Step 1 Connect a laptop's wired Ethernet port directly to the Service port of the controller. The port LEDs blink to indicate that both the machines are properly connected.

Note It may take several minutes for the controller to fully power on to make the GUI available to the PC. Do not auto-configure the controller.

The LEDs on the front panel provide the system status:

- If the LED is off, it means that the controller is not ready.
- If the LED is solid green, it means that the controller is ready.

Step 2 Configure DHCP option on the laptop that you have connected to the Service port. This assigns an IP address to the laptop from the controller Service port 192.168.1.X, or you can assign a static IP address 192.168.1.X to the laptop to access the controller GUI; both options are supported.

Step 3 Open any one of the following supported web browsers and type http://192.168.1.1 in the address bar.

- Mozilla Firefox version 32 or later (Windows, Mac)
- Microsoft Internet Explorer version 10 or later (Windows)
- Apple Safari version 7 or later (Mac)

Note This feature is not supported on mobile devices such as smartphones and tablet computers.

Step 4 Create an administrator account by providing the name and password. Click **Start** to continue.

Step 5 In the **Set Up Your Controller** box, enter the following details:

a. System Name for the controller

b. Current time zone

c. NTP Server (optional)

Note We recommend using a reachable NTP server IP address. APs do not support FQDN in a day0 scenario.

d. Management IP Address

e. Subnet Mask

f. Default Gateway

g. Management VLAN ID—If left unchanged or set to 0, the network switch port must be configured with a native VLAN 'X0'

Note The setup attempts to import the clock information (date and time) from the computer via JavaScript. We recommend that you confirm this before continuing. Access points rely on correct clock settings to be able to join the controller.

Step 6 In the **Create Your Wireless Networks** box, in the **Employee Network** area, use the checklist to enter the following data:

a) Network name/SSID
b) Security
c) Pass Phrase, if Security is set to WPA/WPA2 Personal
d) DHCP Server IP Address: If left empty, the DHCP processing is bridged to the management interface

Step 7 (Optional) In the **Create Your Wireless Networks** box, in the **Guest Network** area, use the checklist to enter the following data:

a) Network name/SSID
b) Security
c) VLAN IP Address, VLAN Subnet Mask, VLAN Default Gateway, VLAN ID
d) DHCP Server IP Address: If left empty, the DHCP processing is bridged to the management interface

Step 8 In the **Advanced Setting** box, in the **RF Parameter Optimization** area, do the following:

a) Select the client density as Low, Typical, or High.
b) Configure the RF parameters for RF Traffic Type, such as Data and Voice.
c) Change the Service port IP address and subnet mask, if necessary.

Step 9 Click **Next**.

Step 10 Review your settings and then click **Apply** to confirm.

The controller reboots automatically. You will be prompted that the controller is fully configured and will be restarted. Sometimes, you might not be prompted with this message. In this scenario, do the following:

a) Disconnect the laptop from the controller service port and connect it to the Switch port.
b) Connect the controller port 1 to the switch configured trunk port.
c) Connect access points to the switch if not already connected.
d) Wait until the access points join the controller.

RF Profile Configurations

Procedure

Step 1 After a successful login as an administrator, choose **Wireless** > **RF Profiles** to verify whether the Cisco WLAN Express features are enabled by checking that the predefined RF profiles are created on this page.

You can define AP Groups and apply appropriate profile to a set of APs.

Step 2 Choose **Wireless** > **Advanced** > **Network Profile**, verify the client density and traffic type details.

Note We recommend that you use **RF and Network profiles** configuration even if Cisco WLAN Express was not used initially or if the controller was upgraded from a release that is earlier than Release 8.1.

Setting up Cisco Wireless Controller using Cisco WLAN Express (Wireless Method)

This wireless method applies only to Cisco 2500 Series Wireless Controller.

Procedure

Step 1 Plug in a Cisco AP to any one of the ports of Cisco 2500 Series WLC. If you do not have a separate power supply for the AP, you can use Port 3 or Port 4, which supports PoE.

Step 2 After the AP boots up, the AP associates with the WLC and downloads the WLC software.

Step 3 The AP starts provisioning a WPA2-PSK SSID "CiscoAirProvision" with the key "password."

Step 4 Associate a client device to the "CiscoAirProvision" SSID.
The client device is assigned an IP address in the 192.168.x.x range.

Step 5 On the web browser of the client device, go to http://192.168.1.1 to open the GUI configuration wizard.

Default Configurations

When you configure your Cisco Wireless Controller, the following parameters are enabled or disabled. These settings are different from the default settings obtained when you configure the controller using the CLI wizard.

Parameters in New Interface	Default Setting
Aironet IE	Disabled
DHCP Address Assignment (Guest SSID)	Enabled
Client Band Select	Enabled
Local HTTP and DHCP Profiling	Enabled
Guest ACL	Applied. **Note** Guest ACL denies traffic to the management subnet.
CleanAir	Enabled
EDRRM	Enabled
EDRRM Sensitivity Threshold	• Low sensitivity for 2.4 GHz. • Medium sensitivity for 5 GHz.

Parameters in New Interface	Default Setting
Channel Bonding (5 GHz)	Enabled
DCA Channel Width	40 MHz
mDNS Global Snooping	Enabled
Default mDNS profile	Two new services added: • Better printer support • HTTP
AVC (only AV)	Enabled only with following prerequisites: • Bootloader version—1.0.18 Or • Field Upgradable Software version—1.8.0.0 and above **Note** If you upgrade the bootloader after you have setup the Cisco 2500 Series Controller using the GUI Wizard, you have to manually enable AVC on the previously created WLAN.
Management	• Via Wireless Clients—Enabled • HTTP/HTTPS Access—Enabled • WebAuth Secure Web—Enabled
Virtual IP Address	192.0.2.1
Multicast Address	Not configured
Mobility Domain Name	Name of employee SSID
RF Group Name	Default

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.

Configuring the Controller (GUI)

Procedure

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

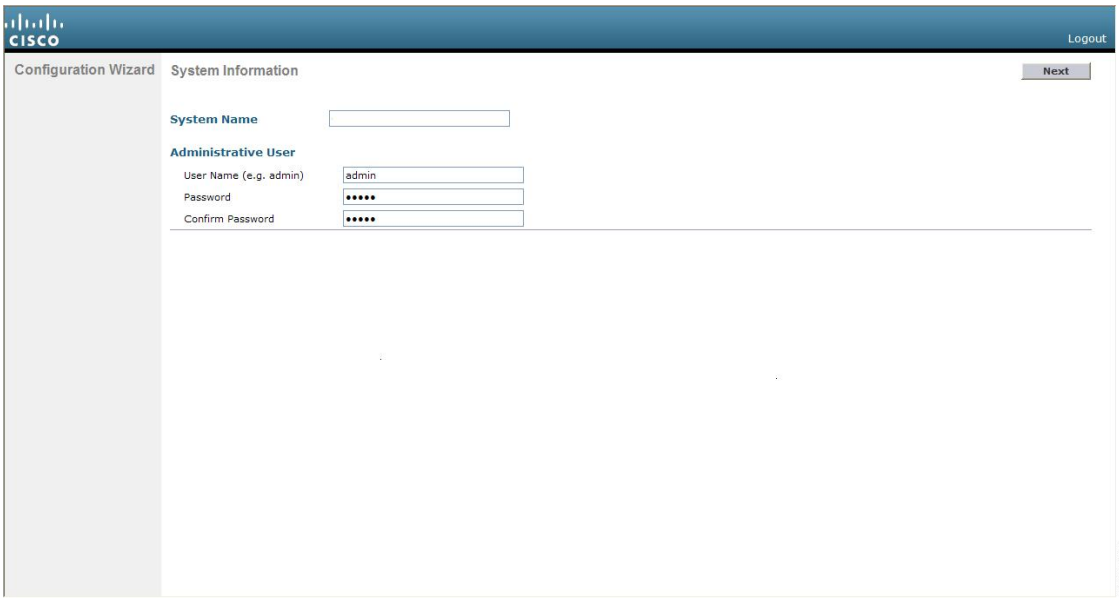
Note With Cisco 2504 Wireless Controller, connect your PC to the port 2 on the controller and configure to use the same subnet.

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

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.

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

Figure 1: Configuration Wizard — System Information Page



Step 3 In the **System Name** field, 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** field, enter the administrative username to be assigned to this controller. You can enter up to 24 ASCII characters. The default username is *admin*.

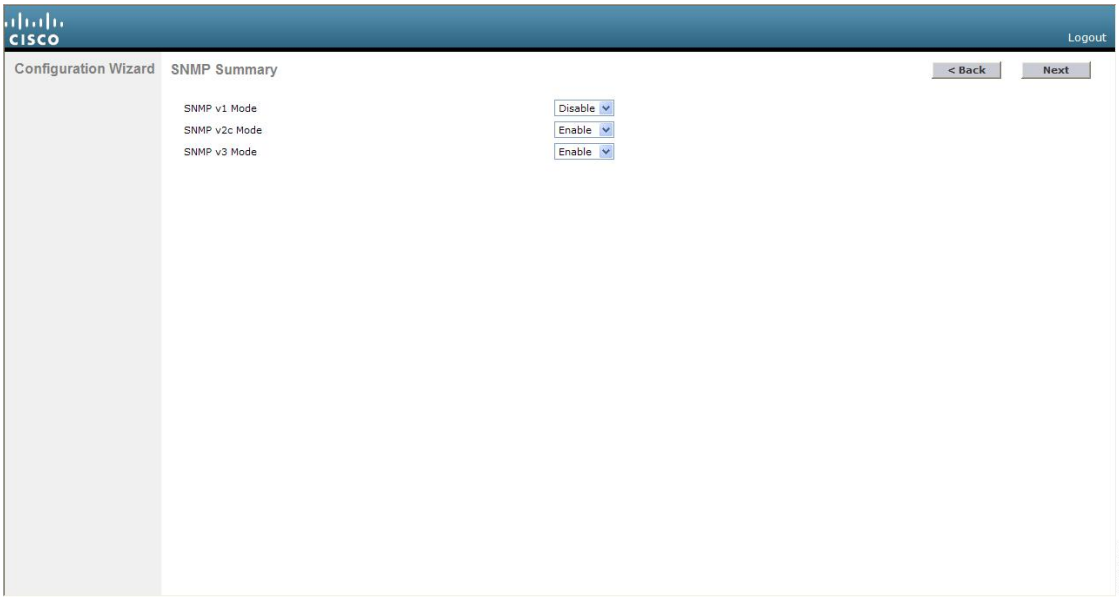
Step 5 In the **Password** and **Confirm Password** boxes, enter the administrative password to be assigned to this controller. You can enter up to 24 ASCII characters. The default password is *admin*.

- 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



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.

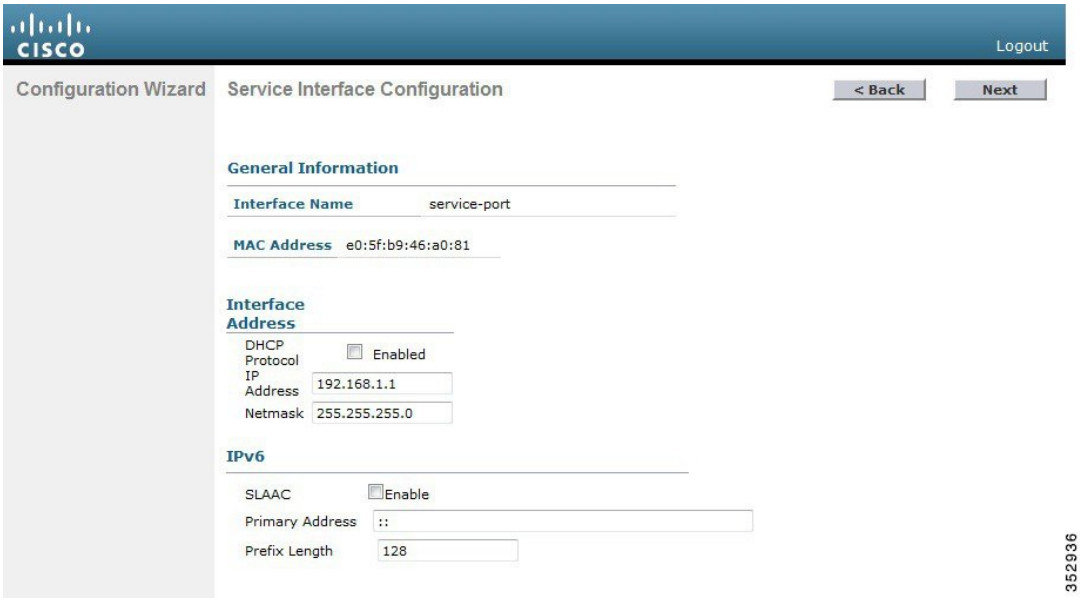
Step 10 Click **Next**.

Step 11 When the following message is displayed, 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



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.

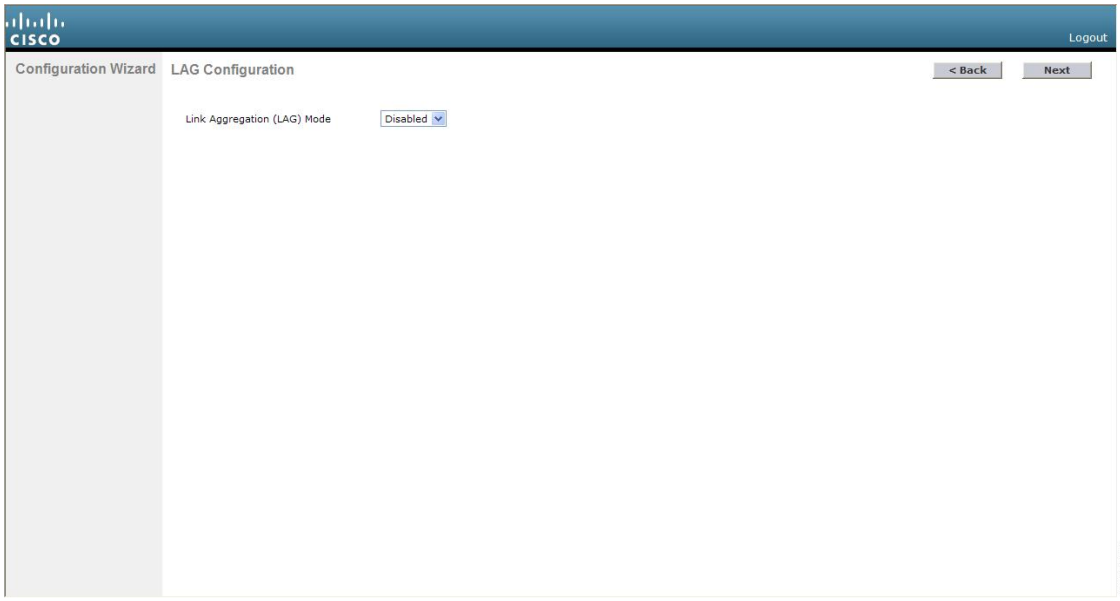
Step 13 Perform one of the following:

- 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.

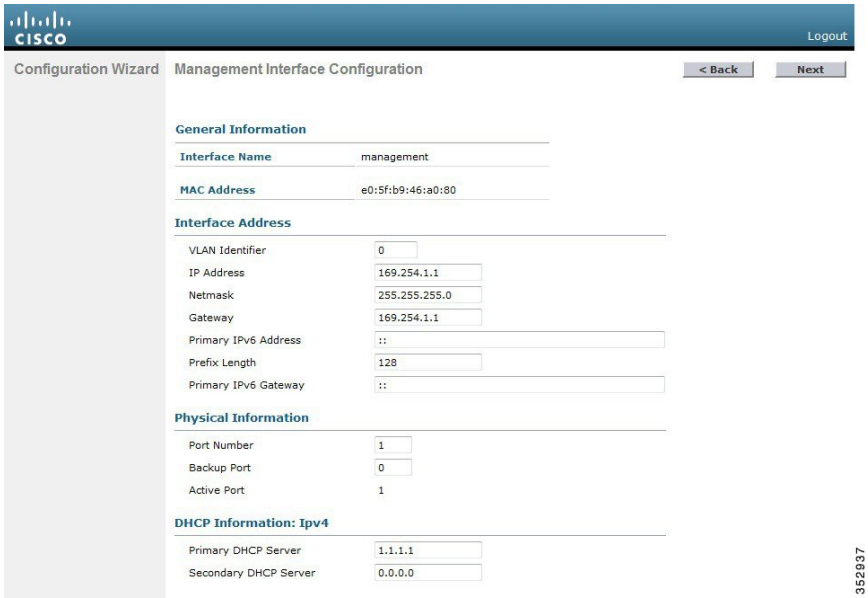
Figure 4: Configuration Wizard—LAG Configuration Page



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

Step 16 Click **Next**.

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



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** field, 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** field, enter the IP address of the management interface.

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

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

Step 21 In the **Port Number** field, 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** field, 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** field, 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** field, 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.

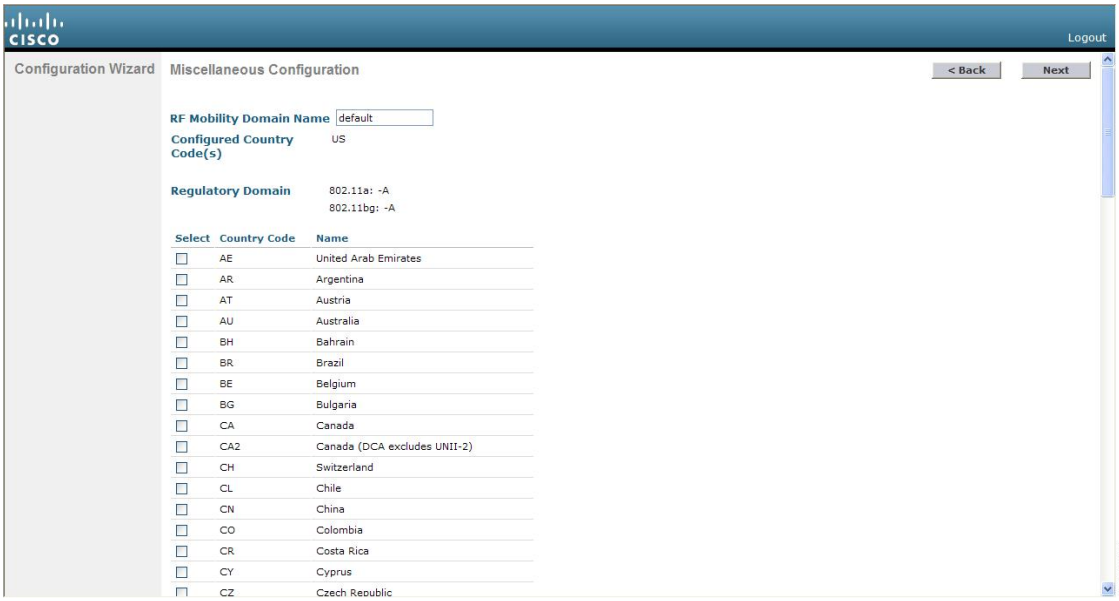
Step 25 Click **Next**. The **AP-Manager Interface Configuration** page is displayed.

Note This screen does not appear for Cisco 5508 controllers 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** field, 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



Step 28 In the **RF Mobility Domain Name** field, 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)** field 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.

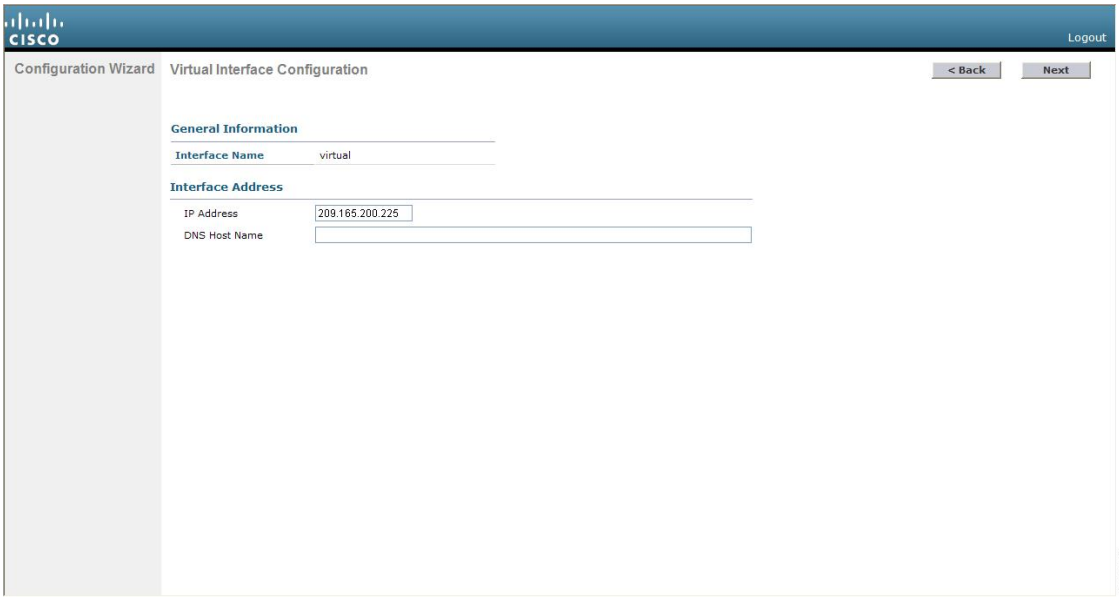
Step 30 Click **Next**.

Step 31 When the following message is displayed, 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



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

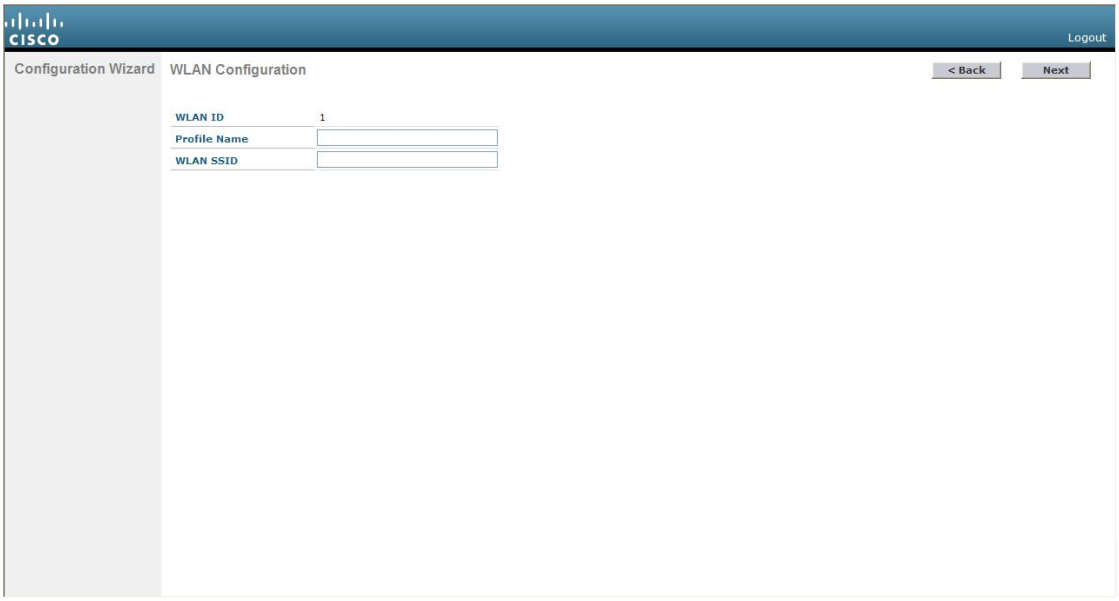
Note The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 33 In the **DNS Host Name** field, 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



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

Step 36 In the **WLAN SSID** field, 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.

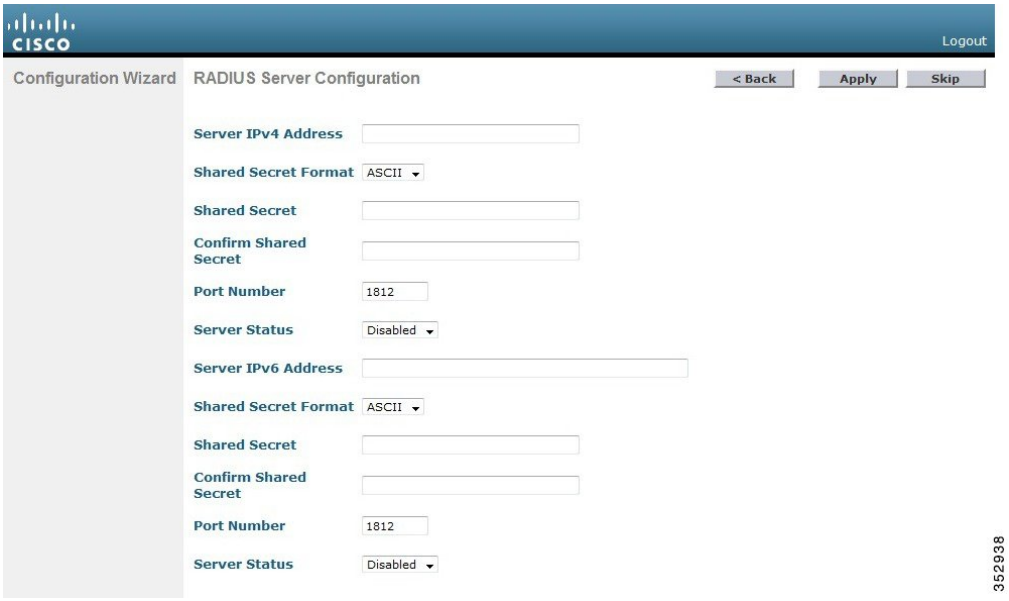
Step 37 Click **Next**.

Step 38 When the following message is displayed, 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



Step 39 In the **Server IP Address** field, 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.

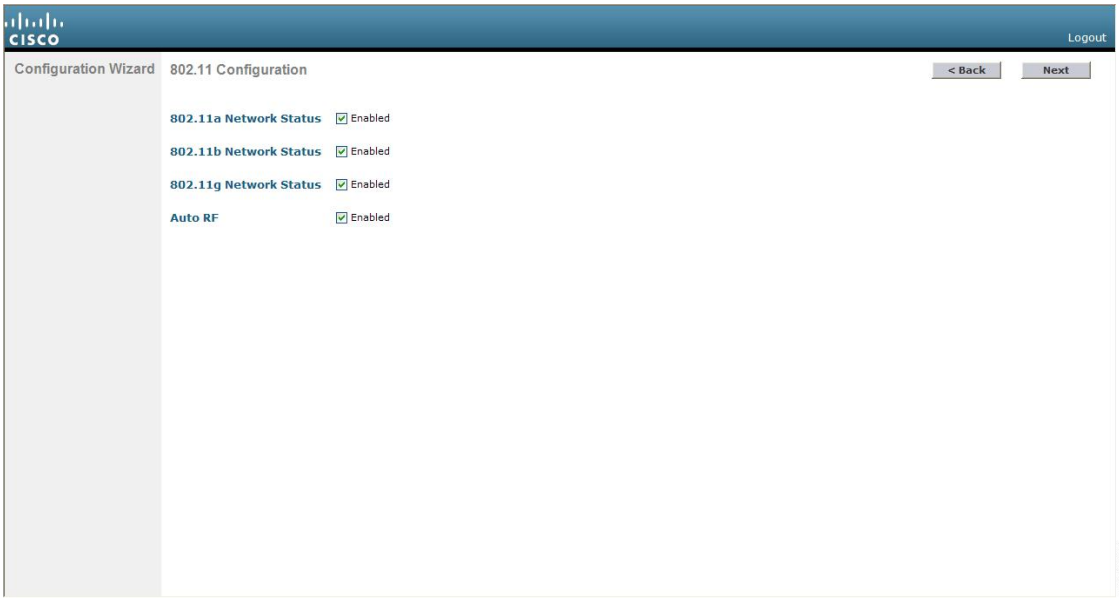
Step 41 In the **Shared Secret** and **Confirm Shared Secret** boxes, enter the secret key used by the RADIUS server.

Step 42 In the **Port Number** field, 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 field set to **Disabled**.

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

Figure 9: Configuration Wizard—802.11 Configuration Page



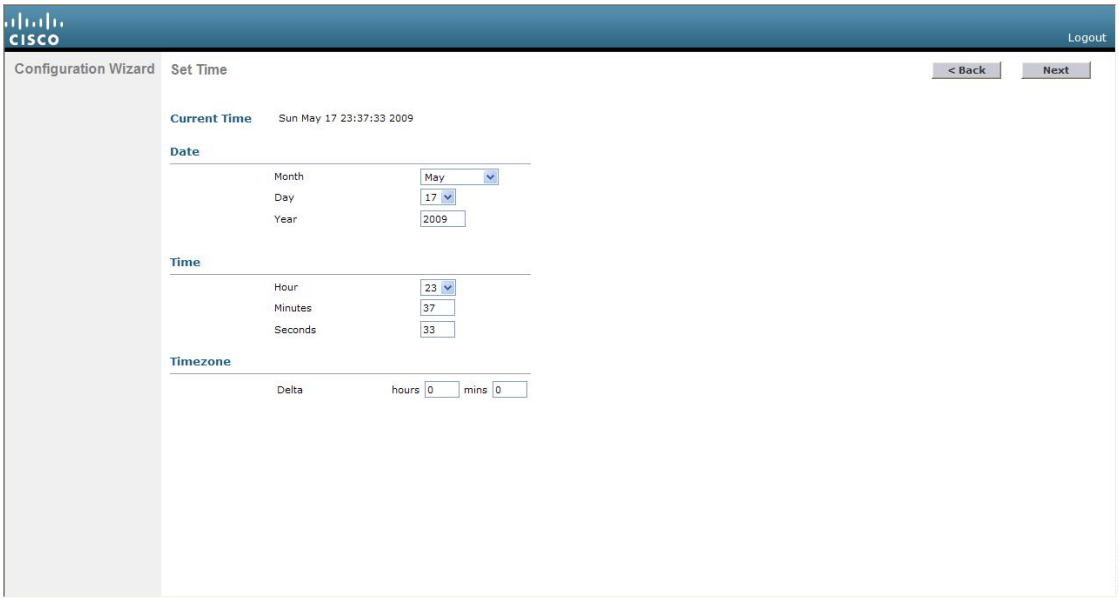
Step 45 To enable the 802.11a, 802.11b, and 802.11g lightweight access point networks, leave the **802.11a Network Status**, **802.11b Network Status**, and **802.11g Network Status** check boxes checked. To disable support for any of these networks, uncheck the check boxes.

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



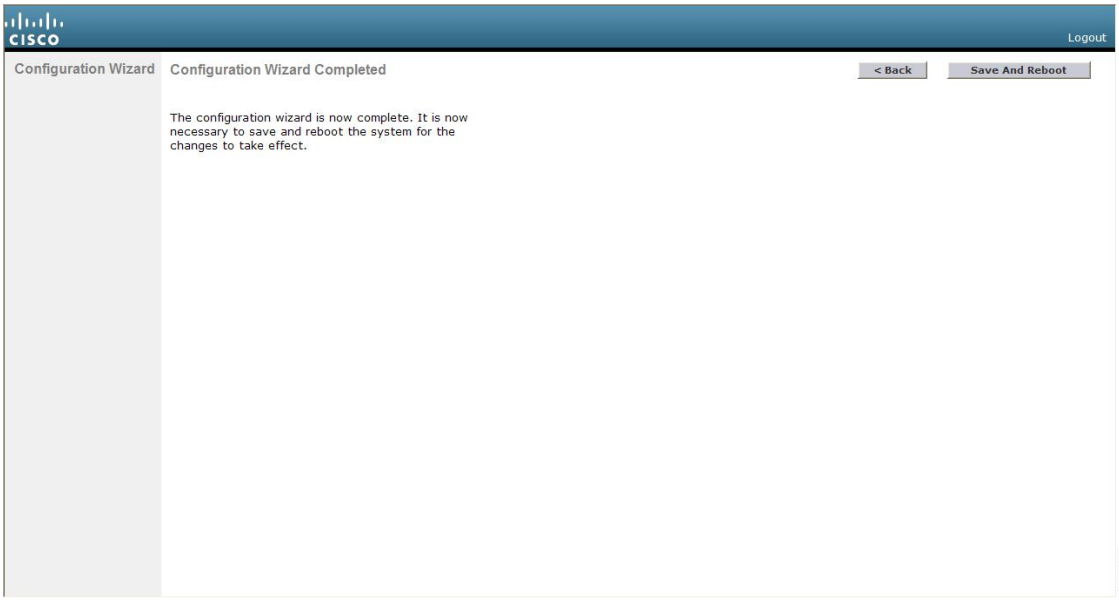
Step 48 To manually configure the system time on your controller, enter the current date in Month/DD/YYYY format and the current time in HH:MM:SS format.

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** field and the local minute difference from GMT in the **Delta Mins** field.

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



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

Step 52 When the following message is displayed, 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 are displayed in brackets after each configuration parameter. The default value is displayed in all uppercase letters.
- If you enter an incorrect response, an appropriate error message is displayed, 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.

Procedure

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.

- 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 is displayed: `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 must 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 .

After 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 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.

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 address*-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-confg'
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.

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.
- Notifications for certificates expiring after the year 2049 are not triggered. This is due to the change in the date format to Generalized time format from the year 2050. Currently UTC time format is used to validate the certificate.

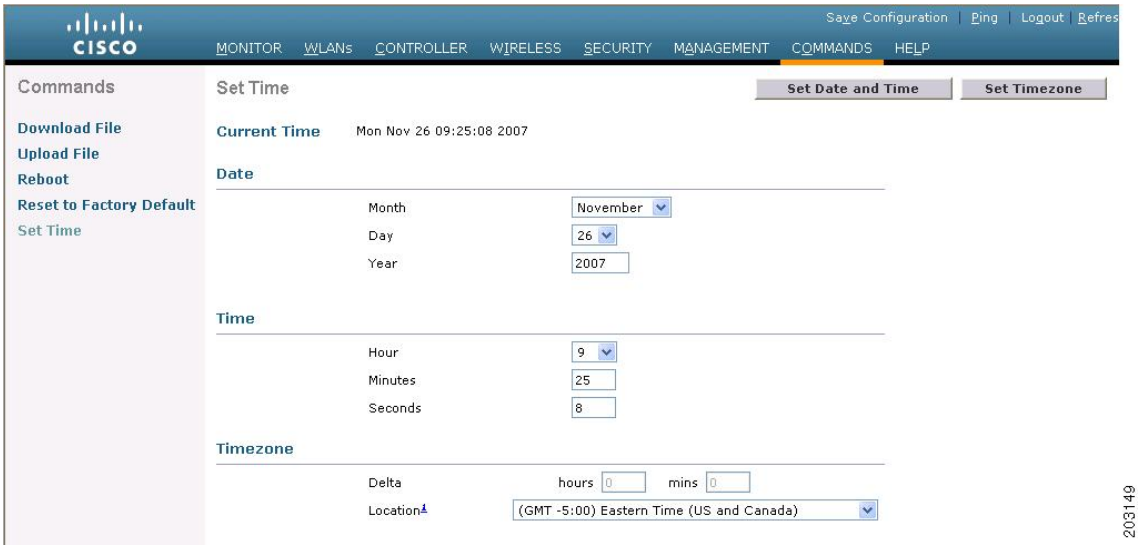
  For more information, see section 4.1.2.5 of the RFC 5280 document at https://tools.ietf.org/html/rfc5280.

Configuring the Date and Time (GUI)

Procedure

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

Figure 12: Set Time Page



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)

Procedure

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 is displayed:

```
Time.................. Thu Apr  7 13:56:37 2011
Timezone delt......... 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.