



Configuring Controller Settings

This chapter describes how to configure settings on the controllers. This chapter contains these sections:

- [Using the Configuration Wizard, page 4-2](#)
- [Managing the System Time and Date, page 4-5](#)
- [Configuring a Country Code, page 4-5](#)
- [Enabling and Disabling 802.11 Bands, page 4-7](#)
- [Configuring Administrator Usernames and Passwords, page 4-7](#)
- [Configuring RADIUS Settings, page 4-7](#)
- [Configuring SNMP Settings, page 4-8](#)
- [Enabling 802.3x Flow Control, page 4-8](#)
- [Enabling System Logging, page 4-8](#)
- [Enabling Dynamic Transmit Power Control, page 4-9](#)
- [Configuring Multicast Mode, page 4-9](#)
- [Configuring the Supervisor 720 to Support the WiSM, page 4-10](#)
- [Using the Wireless LAN Controller Network Module, page 4-13](#)

Using the Configuration Wizard

This section describes how to configure basic settings on a controller for the first time or after the configuration has been reset to factory defaults. The contents of this chapter are similar to the instructions in the quick start guide that shipped with your controller.

You use the configuration wizard to configure basic settings. You can run the wizard on the CLI or the GUI. This section explains how to run the wizard on the CLI.

This section contains these sections:

- [Before You Start, page 4-2](#)
- [Resetting the Device to Default Settings, page 4-3](#)
- [Running the Configuration Wizard on the CLI, page 4-4](#)

Before You Start

You should collect these basic configuration parameters before configuring the controller:

- System name for the controller
- 802.11 protocols supported: 802.11a and/or 802.11b/g
- Administrator usernames and passwords (optional)
- Distribution System (network) port static IP Address, netmask, and optional default gateway IP Address
- Service port static IP Address and netmask (optional)
- Distribution System physical port (1000BASE-T, 1000BASE-SX, or 10/100BASE-T)



Note Each 1000BASE-SX connector provides a 100/1000 Mbps wired connection to a network through an 850nm (SX) fiber-optic link using an LC physical connector.

- Distribution System port VLAN assignment (optional)
- Distribution System port Web and Secure Web mode settings: enabled or disabled
- Distribution System port Spanning Tree Protocol: enabled/disabled, 802.1D/fast/off mode per port, path cost per port, priority per port, bridge priority, forward delay, hello time, maximum age
- WLAN Configuration: SSID, VLAN assignments, Layer 2 Security settings, Layer 3 Security settings, QoS assignments
- Mobility Settings: Mobility Group Name (optional)
- RADIUS Settings
- SNMP Settings
- NTP server settings (the wizard prompts you for NTP server settings only when you run the wizard on a wireless controller network module installed in a Cisco Integrated Services router)
- Other port and parameter settings: service port, Radio Resource Management (RRM), third-party access points, console port, 802.3x flow control, and system logging

Resetting the Device to Default Settings

If you need to start over during the initial setup process, you can reset the controller to factory default settings.

**Note**

After resetting the configuration to defaults, you need a serial connection to the controller to use the configuration wizard.

Resetting to Default Settings Using the CLI

Follow these steps to reset the configuration to factory default settings using the CLI:

-
- Step 1** Enter **reset system**. At the prompt that asks whether you need to save changes to the configuration, enter **Y** or **N**. The unit reboots.
 - Step 2** When you are prompted for a username, enter **recover-config** to restore the factory default configuration. The Cisco Wireless LAN Controller reboots and displays this message:

```
Welcome to the Cisco WLAN Solution Wizard Configuration Tool
```
 - Step 3** Use the configuration wizard to enter configuration settings.
-

Resetting to Default Settings Using the GUI

Follow these steps to return to default settings using the GUI:

-
- Step 1** Open your Internet browser. The GUI is fully compatible with Microsoft Internet Explorer version 6.0 or later on Windows platforms.
 - Step 2** Enter the controller IP address in the browser address line and press **Enter**. An Enter Network Password window appears.
 - Step 3** Enter your username in the User Name field. The default username is *admin*.
 - Step 4** Enter the wireless device password in the Password field and press **Enter**. The default password is *admin*.
 - Step 5** Browse to the **Commands/Reset to Factory Defaults** page.
 - Step 6** Click **Reset**. At the prompt, confirm the reset.
 - Step 7** Reboot the unit and do not save changes.
 - Step 8** Use the configuration wizard to enter configuration settings.
-

Running the Configuration Wizard on the CLI

When the controller boots at factory defaults, the bootup script runs the configuration wizard, which prompts the installer for initial configuration settings. Follow these steps to enter settings using the wizard on the CLI:

-
- Step 1** Connect your computer to the controller using a DB-9 null-modem serial cable.
- Step 2** Open a terminal emulator session using these settings:
- 9600 baud
 - 8 data bits
 - 1 stop bit
 - no parity
 - no hardware flow control
- Step 3** At the prompt, log into the CLI. The default username is *admin* and the default password is *admin*.
- Step 4** If necessary, enter **reset system** to reboot the unit and start the wizard.
- Step 5** The first wizard prompt is for the system name. Enter up to 32 printable ASCII characters.
- Step 6** Enter an administrator username and password, each up to 24 printable ASCII characters.
- Step 7** Enter the service-port interface IP configuration protocol: **none** or **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**.
- Step 8** If you entered **none** in step 7 and need to enter a static IP address for the service port, enter the service-port interface IP address and netmask for the next two prompts. If you do not want to use the service port, enter **0.0.0.0** for the IP address and netmask.
- Step 9** Enter the management interface IP Address, netmask, default router IP address, and optional VLAN identifier (a valid VLAN identifier, or **0** for untagged).
- Step 10** Enter the Network Interface (Distribution System) Physical Port number. For the controller, the possible ports are 1 through 4 for a front panel GigE port.
- Step 11** Enter the IP address of the default DHCP Server that will supply IP Addresses to clients, the management interface, and the service port interface if you use one.
- Step 12** Enter the LWAPP Transport Mode, **LAYER2** or **LAYER3** (refer to the Layer 2 and Layer 3 LWAPP Operation chapter for an explanation of this setting).
- Step 13** Enter the Virtual Gateway IP Address. This address can be any fictitious, unassigned IP address (such as 1.1.1.1) to be used by Layer 3 Security and Mobility managers.
- Step 14** Enter the Cisco WLAN Solution Mobility Group (RF group) name.
- Step 15** Enter the WLAN 1 SSID, or network name. This is the default SSID that lightweight access points use to associate to a controller.
- Step 16** Allow or disallow Static IP Addresses for clients. Enter **yes** to allow clients to supply their own IP addresses. Enter **no** to require clients to request an IP Address from a DHCP server.
- Step 17** If you need to configure a RADIUS Server, enter **yes**, and enter the RADIUS server IP address, the communication port, and the shared secret. If you do not need to configure a RADIUS server or you want to configure the server later, enter **no**.

Step 18 Enter a country code for the unit. Enter **help** to list the supported countries.

**Note**

When you run the wizard on a wireless controller network module installed in a Cisco Integrated Services Router, the wizard prompts you for NTP server settings. The controller network module does not have a battery and cannot save a time setting. It must receive a time setting from an NTP server when it powers up.

Step 19 Enable and disable support for 802.11b, 802.11a, and 802.11g.

Step 20 Enable or disable radio resource management (RRM) (auto RF).

When you answer the last prompt, the controller saves the configuration, reboots with your changes, and prompts you to log in or to enter **recover-config** to reset to the factory default configuration and return to the wizard.

Managing the System Time and Date

You can configure the controller to obtain the time and date from an NTP server or you can configure the time and date manually.

Configuring Time and Date Manually

On the CLI, enter **show time** to check the system time and date. If necessary, enter **config time mm/dd/yy hh:mm:ss** to set the time and date.

To enable Daylight Saving Time, enter **config time timezone enable**.

Configuring NTP

On the CLI, enter **config time ntp server-ip-address** to specify the NTP server for the controller. Enter **config time ntp interval** to specify, in seconds, the polling interval.

Configuring a Country Code

Controllers are designed for use in many countries with varying regulatory requirements. You can configure a country code for the controller to ensure that it complies with your country's regulations.

**Note**

Controllers running software release 3.2 or earlier do not have the ability to control access points in more than one regulatory domain.

On the CLI, enter **config country code** to configure the country code. Enter **show country** to check the configuration.

**Note**

The controller must be installed by a network administrator or qualified IT professional and the proper country code must be selected. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality.

Table 4-1 lists commonly used country codes and the 802.11 bands that they allow. For a complete list of country codes supported per product, refer to www.cisco.com or <http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html>.

Table 4-1 Commonly Used Country Codes

Country Code	Country	802.11 Bands Allowed
US	United States of America	802.11b, 802.11g, and 802.11a low, medium, and high bands
USL	US Low	802.11b, 802.11g, and 802.11a low and medium bands (used for legacy 802.11a interface cards that do not support 802.11a high band)
AU	Australia	802.11b, 802.11g, and 802.11a
AT	Austria	802.11b, 802.11g, and 802.11a
BE	Belgium	802.11b, 802.11g, and 802.11a
CA	Canada	802.11b and 802.11g
DK	Denmark	802.11b, 802.11g, and 802.11a
FI	Finland	802.11b, 802.11g, and 802.11a
FR	France	802.11b, 802.11g, and 802.11a
DE	Germany	802.11b, 802.11g, and 802.11a
GR	Greece	802.11b and 802.11g
IE	Ireland	802.11b, 802.11g, and 802.11a
IN	India	802.11b and 802.11a
IT	Italy	802.11b, 802.11g, and 802.11a
JP	Japan	802.11b, 802.11g, and 802.11a
KR	Republic of Korea	802.11b, 802.11g, and 802.11a
LU	Luxembourg	802.11b, 802.11g, and 802.11a
NL	Netherlands	802.11b, 802.11g, and 802.11a
PT	Portugal	802.11b, 802.11g, and 802.11a
ES	Spain	802.11b, 802.11g, and 802.11a
SE	Sweden	802.11b, 802.11g, and 802.11a
GB	United Kingdom	802.11b, 802.11g, and 802.11a

Enabling and Disabling 802.11 Bands

You can enable or disable the 802.11b/g (2.4-GHz) and the 802.11a (5-GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g and 802.11a are enabled.

On the CLI, enter **config 80211b disable network** to disable 802.11b/g operation on the controller. Enter **config 80211b enable network** to re-enable 802.11b/g operation.

Enter **config 80211a disable network** to disable 802.11a operation on the controller. Enter **config 80211a enable network** to re-enable 802.11a operation.

Configuring Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information.

On the CLI, enter **config mgmtuser add *username password* read-write** to create a username-password pair with read-write privileges. Enter **config mgmtuser add *username password* read-only** to create a username-password pair with read-only privileges. Usernames and passwords are case-sensitive and can contain up to 24 ASCII characters. Usernames and passwords cannot contain spaces.

To change the password for an existing username, enter **config mgmtuser password *username new_password***

To list configured users, enter **show mgmtuser**.

Configuring RADIUS Settings

If you need to use a RADIUS server for accounting or authentication, follow these steps on the CLI to configure RADIUS settings for the controller:

-
- Step 1** Enter **config radius acct *ip-address*** to configure a RADIUS server for accounting.
 - Step 2** Enter **config radius acct *port*** to specify the UDP port for accounting.
 - Step 3** Enter **config radius acct *secret*** to configure the shared secret.
 - Step 4** Enter **config radius acct *enable*** to enable accounting. Enter **config radius acct *disable*** to disable accounting. Accounting is disabled by default.
 - Step 5** Enter **config radius auth *ip-address*** to configure a RADIUS server for authentication.
 - Step 6** Enter **config radius auth *port*** to specify the UDP port for authentication.
 - Step 7** Enter **config radius auth *secret*** to configure the shared secret.
 - Step 8** Enter **config radius auth *enable*** to enable authentication. Enter **config radius acct *disable*** to disable authentication. Authentication is disabled by default.
 - Step 9** Use the **show radius acct statistics**, **show radius auth statistics**, and **show radius summary** commands to verify that the RADIUS settings are correctly configured.
-

Configuring SNMP Settings

Cisco recommends that you use the GUI to configure SNMP settings on the controller. To use the CLI, follow these steps:

-
- Step 1** Enter **config snmp community create** *name* to create an SNMP community name.
 - Step 2** Enter **config snmp community delete** *name* to delete an SNMP community name.
 - Step 3** Enter **config snmp community accessmode ro** *name* to configure an SNMP community name with read-only privileges. Enter **config snmp community accessmode rw** *name* to configure an SNMP community name with read-write privileges.
 - Step 4** Enter **config snmp community ipaddr** *ip-address ip-mask name* to configure an IP address and subnet mask for an SNMP community.
 - Step 5** Enter **config snmp community mode enable** to enable a community name. Enter **config snmp community mode disable** to disable a community name.
 - Step 6** Enter **config snmp trapreceiver create** *name ip-address* to configure a destination for a trap.
 - Step 7** Enter **config snmp trapreceiver delete** *name* to delete a trap.
 - Step 8** Enter **config snmp trapreceiver ipaddr** *old-ip-address name new-ip-address* to change the destination for a trap.
 - Step 9** Enter **config snmp trapreceiver mode enable** to enable traps. Enter **config snmp trapreceiver mode disable** to disable traps.
 - Step 10** Enter **config snmp syscontact** *syscontact-name* to configure the name of the SNMP contact. Enter up to 31 alphanumeric characters for the contact name.
 - Step 11** Enter **config snmp syslocation** *syslocation-name* to configure the SNMP system location. Enter up to 31 alphanumeric characters for the location.
 - Step 12** Use the **show snmpcommunity** and **show snmptrap** commands to verify that the SNMP traps and communities are correctly configured.
 - Step 13** Use the **show trapflags** command to see the enabled and disabled trapflags. If necessary, use the **config trapflags** commands to enable or disable trapflags.
-

Enabling 802.3x Flow Control

802.3x Flow Control is disabled by default. To enable it, enter **config switchconfig flowcontrol enable**.

Enabling System Logging

System logging is disabled by default. Enter **show syslog** to view the current syslog status. Enter **config syslog** to send a controller log to a remote IP Address or hostname.

Enabling Dynamic Transmit Power Control

When you enable Dynamic Transmit Power Control (DTPC), access points add channel and transmit power information to beacons. (On access points that run Cisco IOS software, this feature is called world mode.) Client devices using DTPC receive the information and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there. DTPC is enabled by default.

Enter this command to disable or enable DTPC:

```
config {802.11a | 802.11bg} dtpc {enable | disable}
```

Configuring Multicast Mode

If your network supports packet multicasting you can configure the multicast method that the controller uses. The controller performs multicasting in two modes:

- Unicast mode—In this mode the controller unicasts every multicast packet to every access point associated to the controller. This mode is inefficient but might be required on networks that do not support multicasting.
- Multicast mode—In this mode the controller sends multicast packets to an LWAPP multicast group. This method reduces overhead on the controller processor and shifts the work of packet replication to your network, which is much more efficient than the unicast method.

Understanding Multicast Mode

When you enable multicast mode, the controller does not become a member the multicast group. When the controller receives a multicast packet from the wired LAN, the controller encapsulates the packet using LWAPP and forwards the packet to the LWAPP multicast group address. The controller always uses the management interface for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the interface on which clients receive multicast traffic. From the access point perspective, the multicast appears to be a broadcast to all SSIDs.

When the source of the multicast is a wireless client, the multicast packet is unicast to the controller. In this case the controller makes two copies of the packet. One copy is the raw Ethernet packet that the controller sends out to the interface for the wireless LAN on which the client is associated, enabling the receivers on the wired LAN to receive the multicast traffic. The second copy of the packet is LWAPP-encapsulated and is sent to the multicast group. In this case the source of the multicast also receives the multicast packet, which helps the wireless client receive the multicast source.

Guidelines for Using Multicast Mode

Follow these guidelines when you enable multicast mode on your network:

- The Cisco Unified Wireless Network solution uses some IP address ranges for specific purposes, and you should keep these ranges in mind when configuring a multicast group:
 - 224.0.0.0 through 224.0.0.255—Reserved link local addresses
 - 224.0.1.0 through 238.255.255.255—Globally scoped addresses
 - 239.0.0.0 through 239.255.255.255—Limited scope addresses

- When you enable multicast mode on the controller you also must configure an LWAPP multicast group address on the controller. Access points subscribe to the LWAPP multicast group using IGMP.
- Cisco 1100, 1130, 1200, 1230, and 1240 access points use IGMP versions 1, 2, and 3. However, Cisco 1000 series access points use only IGMP v1 to join the multicast group.
- Multicast mode works only in Layer 3 LWAPP mode.
- Access points in monitor mode, sniffer mode, or rogue detector mode do not join the LWAPP multicast group address.
- When using Multiple controllers on the network, make sure that the same multicast address is configured on all the controllers.
- Multicast mode does not work across intersubnet mobility events such as guest tunneling, site-specific VLANs, or interface override using RADIUS. However, multicast mode does work in these subnet mobility events when you disable the layer 2 IGMP snooping/CGMP features on the wired LAN.
- The controller drops any multicast packets sent to the UDP port numbers 12222, 12223, and 12224. Make sure the multicast applications on your network do not use those port numbers.

Enabling Multicast Mode

Multicasting is disabled by default. Use the commands in [Table 4-2](#) to configure multicast mode on the controller CLI.

Table 4-2 CLI Commands for Configuring Multicast Mode

Command	Multicast Mode
config network multicast global {enable disable}	Enable or disable multicasting
config network multicast mode unicast	Configure the controller to use the unicast method to send multicast packets
config network multicast mode multicast <i>multicast-group-ip-address</i>	Configure the controller to use the multicast method to send multicast packets to an LWAPP multicast group.

You can also enable multicast mode on the Configure > Switch IP System General page on the WCS interface.

Configuring the Supervisor 720 to Support the WiSM

When you install a WiSM in a Cisco Catalyst 6500 switch, you must configure the Supervisor 720 to support the WiSM. When the supervisor detects the WiSM, the supervisor creates 10 GigabitEthernet interfaces, ranging from *Gigslot/1* to *Gigslot/8*. For example, if the WiSM is in slot 9, the supervisor creates interfaces *Gig9/1* through *Gig9/8*. The first eight GigabitEthernet interfaces must be organized into two etherchannel bundles of four interfaces each. The remaining two GigabitEthernet interfaces are used as service-port interfaces, one for each controller on the WiSM. You must manually create VLANs to communicate with the ports on the WiSM.

**Note**

The WiSM is also supported on Cisco 7600 Series Routers running only Cisco IOS Release 12.2(18)SXF5.

General WiSM Guidelines

Keep these general guidelines in mind when you add a WiSM to your network:

- The switch ports leading to the controller service port are automatically configured and cannot be manually configured.
- The switch ports leading to the controller data ports should be configured as edge ports to avoid sending unnecessary BPDUs.
- The switch ports leading to the controller data ports should not be configured with any additional settings (such as port channel or SPAN destination) other than settings necessary for carrying data traffic to and from the controllers.
- The WiSM controllers support Layer 3 LWAPP mode, but they do not support Layer 2 LWAPP mode.

**Note**

Refer to [Chapter 3](#) for information on configuring the WiSM's ports and interfaces.

Configuring the Supervisor

Log into the switch CLI and, beginning in Privileged Exec mode, follow these steps to configure the supervisor to support the WiSM:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>vlan</i>	Create a VLAN to communicate with the data ports on the WiSM and enter interface config mode.
Step 3	ip address <i>ip-address gateway</i>	Assign an IP address and gateway to the VLAN.
Step 4	ip helper-address <i>ip-address</i>	Assign a helper address to the VLAN.
Step 5	end	Return to global config mode.
Step 6	interface port-channel 1	Configure a port-channel to bundle the automatically created Gigabit interfaces 1-4 into an etherchannel.
	a. switchport trunk encapsulation dot1q	Configure the previously created port-channel interfaces as trunk ports. For the native VLAN on the ports, configure the VLAN that you created for communicating with the WiSM data ports.
	b. switchport trunk native vlan <i>vlan</i>	
	c. switchport mode trunk	
	d. end	Return to global config mode.

	Command	Purpose
Step 7	interface port-channel 2	Configure a port-channel to bundle the automatically created Gigabit interfaces 5-8 into an etherchannel.
	a. switchport trunk encapsulation dot1q	Configure the second port-channel as the first.
	b. switchport trunk native vlan <i>vlan</i>	
	c. switchport mode trunk	
	d. end	Return to global config mode.
Step 8	interface GigabitEthernet9/1-4	Establish a separate Gigabit etherchannel for the first controller on the WiSM. For the native VLAN on the ports, configure the VLAN that you created for communicating with the WiSM data ports.
	a. switchport trunk encapsulation dot1q	Configure the previously created port-channel interfaces as trunk ports. For the native VLAN on the ports, configure the VLAN that you created for communicating with the WiSM data ports.
	b. switchport trunk native vlan <i>vlan</i>	
	c. switchport mode trunk	
	d. channel-group 1 mode on	Bind the physical GigabitEthernet interfaces to the logical port-channel interface.
Step 9	interface GigabitEthernet9/5-8	Establish a separate Gigabit etherchannel for the second controller on the WiSM. For the native VLAN on the ports, configure the VLAN that you created for communicating with the WiSM data ports.
	a. switchport trunk encapsulation dot1q	Configure the second group of GigabitEthernet interfaces as the first.
	b. switchport trunk native vlan <i>vlan</i>	
	c. switchport mode trunk	
	d. channel-group 2 mode on	Bind the physical GigabitEthernet interfaces to the logical port-channel interface.
Step 10	interface <i>vlan</i>	Create a VLAN to communicate with the service ports on the WiSM.
Step 11	ip address <i>ip-address gateway</i>	Assign an IP address and gateway to the VLAN.
Step 12	end	Return to global config mode.
Step 13	wism service-vlan <i>vlan</i>	Configure the VLAN that you created in step 10 to communicate with the WiSM service ports.
Step 14	end	Return to global config mode.
Step 15	show wism status	Verify that the WiSM is operational.

Using the Wireless LAN Controller Network Module

Keep these guidelines in mind when using a wireless LAN controller network module (CNM) installed in a Cisco Integrated Services Router:

- The controller network module does not support IPSec. To use IPSec with the CNM, configure IPSec on the router in which the CNM is installed. Click this link to browse to IPSec configuration instructions for routers:

http://www.cisco.com/en/US/tech/tk583/tk372/tech_configuration_guides_list.html

- The controller network module does not have a battery and cannot save a time setting. It must receive a time setting from an NTP server when it powers up. When you install the module the configuration wizard prompts you for NTP server information.
- To access the CNM bootloader, Cisco recommends that you reset the CNM from the router. If you reset the CNM from a CNM user interface the router might reset the CNM while you are using the bootloader.

When you reset the CNM from a CNM interface you have 17 minutes to use the bootloader before the router automatically resets the CNM. The CNM bootloader does not run the Router Blade Configuration Protocol (RBCP), so the RBCP heartbeat running on the router times out after 17 minutes, triggering a reset of the CNM.

If you reset the CNM from the router, the router stops the RBCP heartbeat exchange and does not restart it until the CNM boots up. To reset the CNM from the router, enter this command on the router CLI:

```
service-module wlan-controller 1/0 reset
```

