Power Up and Initial Configuration

This chapter guides you through a basic controller configuration, which is sufficient for you to access your network. Complex configuration procedures are beyond the scope of this publication and can be found in the modular configuration and command reference publications in the Cisco IOS software configuration documentation set that corresponds to the software release installed on your Cisco hardware.

- Power the controller, on page 1
- Initial controller configuration, on page 2
- Gigabit Ethernet management interface, on page 12
- Save your controller configuration, on page 14
- Verify the initial configuration, on page 14
- Power off the controller safely, on page 15

Power the controller

Before you power on, make sure that:

- The power supply cord is plugged into the power supply inlet.
- All cables are connected.
- Your computer is powered up and connected.

Note Your controller automatically powers UP from the pre-installed image in the factory settings.

For information on how to recover a Cisco Catalyst 9800 controller or the password from ROMMON mode, see:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214012-recovering-a-catalyst-9800-controller-fr.html

Initial controller configuration

Using the Cisco IOS XE CLI - Cisco setup command facility

The **setup** command facility prompts you to enter the information that is needed to configure a controller quickly. The facility takes you through an initial configuration, including wireless configurations.

Note The setup command facility is entered automatically if there is no configuration on the controller when it is booted into Cisco IOS XE.

Note Do not delete *Throughput.txt* file. This file is created when the **license wireless high-performance** command is used on the controller to increase the scale from 250 APs and 5000 clients to 500 APs and 10000 clients. Deleting this file will revert the controller to the previous state of 250 APs and 5000 clients.

You are prompted for wireless configuration after the Day 0 banner.

For information on modifying the configuration after you create it, see the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide and the Cisco Catalyst 9800 Series Wireless Controller Command Reference Guide.

This section includes:

- Configure the device management interface.
- Configure the device management IP.
- Set a static route.
- Configure the management credentials.
- Configure the wireless management interface.
- Choose the deployment mode.
- Configure the system name or hostname.
- Configure credentials for management access on access points.
- Configure the country code.
- Configure the time using an NTP server or manually.
- [Optional] Configure a time zone.
- [Optional] Configure the wireless client density.
- [Optional] Configure AAA servers.
- [Optional] Configure the wireless network settings.
- [Optional] Configure a network name or SSID.

- [Optional] Configure a virtual IP.
- [Optional] Configure an RF network name.
- [Optional] Configure high avalability.

Note Presently, there is no direct method to get back to your previous configuration. Press **Ctrl-C** to restart the configuration and return to the setup without saving the configuration.

Day 0 CLI wizard for the controller

Procedure

Step 1 You can get into the Day 0 setup wizard using the **write erase** command or directly on the Day 0 device.

Step 2 Device management interface setup configures the device management or service port. This interface enables the basic configuration to access the device using the GUI. This is an optional configuration where you can opt to configure only the wireless management interface and not the device management.

```
Configure device management interface?[yes]:
```

Step 3 Device management IP helps access the device using the GUI.

```
 Configure static IP address? [yes]: yes
    Enter the interface IP [GigabitEthernet0]: 10.104.177.128
    Enter the subnet mask [GigabitEthernet0] [255.0.0.0]: 255.255.255.0
```

Step 4 Set a static route to access the device using the GUI.

```
Interface belongs to VRF "Mgmt-intf". Please configure a static route on the VRF
Enter the destination prefix: 0.0.0.0
Enter the destination mask: 0.0.0.0
Enter the forwarding router IP: 10.104.170.1
```

Step 5 Enter the management username and password. This is a mandatory step.

```
Enter the management username: cisco
  Enter the password: ********
  Reenter the password: ********
```

Step 6 Configure the wireless management if you have not configured a device management interface.

```
Basic management setup is now complete. At this point, it is possible to save the above and
continue wireless setup using the webUI (for this, choose 'no' below)

Would you like to continue with the wireless setup? [yes]: yes
```

Note

- If you have not configured the device management, the setup moves to **Step 7** before displaying the above banner.
- You cannot exit the wizard without completing the configuration.

- If you select **Yes**, you need to follow the upcoming steps. Also, you can access the device using the IP configured in **Step 4**.

Step 7 Configure wireless management interface. Wireless management interface is a mandatory configuration.

```
Configuring wireless management interface
  Select interface to be used for wireless management
   1. TenGigabitEthernet0/0/0 [Up]
   2. TenGigabitEthernet0/0/1 [Up]
  Choose the interface to config [1]:
```

Step 8 Enter a VLAN ID.

```
Enter the vlan ID (1-4094): 112
```

Step 9 Configure an IPv4 or IPv6 address.

```
  Configure IPv4 address? [yes]:
    Enter the interface IP TenGigabitEthernet0/0/0 [Up]: 9.11.112.40
    Enter the subnet mask TenGigabitEthernet0/0/1 [Up] [255.0.0.0]: 255.255.255.0
  Configure IPv6 address? [yes]: no
```

Step 10 Configure a VLAN DHCP server and IP address:

```
 Do you want to configure a VLAN DHCP Server? [yes]: yes
   Enter the VLAN DHCP Server IP [TenGigabitEthernet0/0/1]: 9.11.112.45
```

Step 11 (Optional) Set a static route to attach an AP client to the controller. The default options for static route prompts you to configure a default route. However, you can specify a different route as well.

```
 Configure static route? [yes/no]: yes
  Enter the destination prefix [0.0.0.0]:
  Enter the destination mask [0.0.0.0]:
  Enter the forwarding router IP: 9.11.112.1
```

Note

If you configure the device as HA RMI and you haven't configured a default route (that is, source and destination as 0.0.0.0), the wizard asks for the default route information.

```
Basic management setup is now complete. At this point, it is possible to save the above and
continue wireless setup using the webUI(for this, choose 'no' below)

Would you like to continue with the wireless setup? [yes]
```

Step 12 Choose the deployment mode.

```
 Choose the deployment mode
    1. Standalone
    2. Active
    3. Standby
 Enter your selection [1]:
```

Note

You can choose from one of the following deployment modes:

- **Standalone**: In this mode, you do not get to view any high availability pairing information.

- **Active**: In this mode, the controller needs to be configured with all the Day 0 information.
- **Standby**: In this mode, the configuration proceeds to the **High Availability** configuration.

Step 13 Configure the system name or hostname.

```
Enter the hostname [WLC]: ciscowlc
```

Note

This is a mandatory step. The hostname needs to confirm to the RFC standards.

Step 14 (Optional) Configure the login credentials for an AP.

```
Configure credentials for management access on Access Points? [yes]:
  Enter the management username: cisco
  Enter the management password: ****
    Reenter the password: ****
  Enter the privileged mode access password: ****
    Reenter the password: ****
```

Step 15 Configure the country code. You can specify multiple country codes by separating them with a comma.

```
Configure country code for wireless operation in ISO format ? [US]:
```

Step 16 Configure the date and NTP to allow access points to join the controller. You can configure time using an NTP server or manually.

Note

You need to enter time in the following format:

DAY-MONTH-YEAR

```
Configure NTP server ? [yes/no]: no
Enter the day:
Enter the month:
Enter the year:

Configure a NTP server now? [yes]:
Enter ntp server address : 9.11.112.45
Enter a polling interval between 16 and 131072 secs which is power of 2: 16
```

Step 17 (Optional) Configure a timezone.

```
 Configure timezone? [yes]:
  Enter name of timezone: ind
  Enter hours offset from UTC (-23,23): 5
  Enter mins offset from UTC (0,59) [0]: 30
```

Step 18 (Optional) Configure the expected client density.

```
 Configure Wireless client density? [yes]:
  Choose the client density
    1. Low
    2. Typical
    3. High
  Enter your selection [2]: 3
```

Step 19 (Optional) Configure AAA servers.

Note

You can configure a maximum of 6 servers during Day 0 configuration.

```
 Configure AAA servers? [yes]:
  Enter the AAA server address: 9.11.112.46
  Enter the AAA key: ***
Do you want to add more AAA servers? [yes]:
  Enter the AAA server address: 9.11.112.47
  Enter the AAA key: ***
Do you want to add more AAA servers? [yes]: no
```

Note

The AAA servers are required for WPA2 Enterprise. You need to configure AAA only in one place. If you follow **Step 21**, WPA2 Enterprise will not ask for AAA servers in **Step 22**.

Step 20 (Optional) Configure wireless network settings to configure WLAN information for an AP and client join.

```
Configure Wireless network settings? [yes]:
```

Step 21 (Optional) Configure an SSID for client join.

```
Enter the network name or service set identifier (SSID):
Choose the network type
    1. Employee
    2. Guest
```

If you choose **Employee** as the network type, these options are displayed.

```
Choose the security type
    1. WPA Personal
    2. WPA Enterprise
   Enter your selection [2]:
```

If you choose **WPA2 Personal**, you will need to enter a pre-shared key (ASCII).

```
Enter the pre-shared key (ASCII):
```

If you choose **WPA2 Enterprise**, you will be able to add multiple AAA servers.

```
Enter the AAA server address:
Enter the AAA key:
Enter more AAA server details? [yes]
```

If you choose **Guest**, you have these options:

```
Please choose the security type:
1. Webauth
2. Authbypass
3. Consent
4. Webconsent
Enter the security type:
```

Step 22 (Optional) Configure a virtual IP address. The recommended virtual IP address is 192.0.2.1.

```
 Configure virtual IP? [yes]:
  Enter the virtual IP [192.0.6.1]:
```

Step 23 (Optional) Configure an RF network name.

```
Configure RF-Network Name? [yes]:
 Enter the RF-Network Name: ciscorf
```

Step 24 (Optional) Configure High Availability.

If you choose the deployment mode as Active or Standby, you will need to choose from one of the High Availability pairing type:

a. RMI

b. RP-RP

Note
For information on HA pairing types, see **Part: High Availability (High Availability > Information About Redundancy Management Interface)** in *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.18.x*.

```
High Availability configuration
 Please choose the HA pairing type
   1. RMI
   2. RP-RP
 Enter your selection [1]:
```

If you choose RMI+RP, you need to select an interface to be used as redundancy port:

```
Enter the RMI IP for local chassis: 9.11.112.12
Enter the RMI IP for remote chassis: 9.11.112.13
Enter the gateway IP of the last resort: 9.11.112.1
```

Note
If you have not configured a default route earlier, you need to enter the gateway IP of the last resort.

If you choose the deployment mode as Standby, you need to specify the VLAN ID for completing the pairing:

```
Enter the RMI IP for local chassis: 9.11.112.51
Enter the RMI IP for remote chassis: 9.11.112.50
Enter the wireless management VLAN: 112
```

If you choose RP, you need to select an interface to be used as redundancy port:

```
Select interface to be used as redundancy port
  1. TenGigabitEthernet0/0/0 [Up]
  2. TenGigabitEthernet0/0/1 [Up]
 Choose the interface to config [1]: 2
 Enter the local IP:
Enter the subnet mask:
Enter the remote IP:
```

Day 0 web UI wizard for the controller

For information on the Day 0 Web UI, see the Day 0 Express Setup using WebUI section of the *Cisco Catalyst 9800 Wireless Controller Series Web UI Deployment Guide*.

Note After the day 0 wizard configuration, the management interface (Gig0) remains as the source interface for TFTP. In the day 0 wizard configuration the wireless management interface is configured and most of the time this is the interface used for all network traffic.

To change the TFTP source interface to the wireless management interface, use the following command: **ip tftp source-interface vlan** *VLAN-ID*.

Use the Cisco IOS XE CLI

This section shows you how to access the CLI to perform the initial configuration on the controller.

If the system configuration message does not appear, it means a default configuration file was installed on the controller prior to shipping.

Follow these steps to configure the controller.

Procedure

Step 1 Enter **no** when the following system message appears on the controller.

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no
```

Step 2 Press **Return** and continue with the manual configuration.

Several log messages are displayed.

Step 3 Press **Return** to bring up the `WLC>` prompt.

Step 4 Type **enable** to enter privileged EXEC mode.

```
WLC> enable
WLC#
```

Configure the controller hostname

The hostname used in CLI prompts the default configuration filenames. If you do not configure the controller hostname, the controller uses the factory-assigned default hostname **WLC**.

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
WLC> enable
```

Note

Enter your password if prompted.

Step 2 Enter global configuration mode.

Example:

```
WLC# configure terminal
```

Step 3 Specifies or modifies the hostname for the network server.

Example:

```
WLC(config)# hostname myWLC
```

Step 4 (Optional) Returns to privileged EXEC mode.

Example:

```
myWLC(config)# end
```

Enable secret passwords

To provide an additional layer of security, particularly for passwords that cross the network or are stored on a TFTP server, you can use either the **enable password** command or the**enable secret** command. Both commands accomplish the same thing—they allow you to establish an encrypted password that users must enter to access privileged EXEC (enable) mode.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.

Note If you configure the enable secret command, it takes precedence over the enable password command; the two commands cannot be in effect simultaneously.

For more information, see the **Configuring Passwords and Privileges** chapter in the *Cisco IOS Security Configuration Guide*. Also see **Cisco IOS Password Encryption Facts** and **Cisco Guide to Harden Cisco IOS Devices**.

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device# enable
```

Enter your password if prompted.

Step 2 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 3 Specify an additional layer of security over the **enable password** command.

Example:

```
Device(config)# enable secret greentree
```

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

Step 5 Enable privileged EXEC mode.

Example:

```
Device> enable
```

Verify that your new enable or enable secret password works.

Configure the console idle privileged EXEC timeout

By default, the privileged EXEC command interpreter waits 10 minutes to detect user input before timing out.

When you configure the console line, you can also set communication parameters, specify autobaud connections, and configure terminal operating parameters for the terminal that you are using. For more information on configuring the console line, see the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*. In particular, see the *Configuring Operating Characteristics for Terminals* and *Troubleshooting and Fault Management* chapters.

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device> enable
```

Note
Enter your password if prompted.

Step 2 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 3 Configure the console line and start the line configuration command collection mode.

Example:

```
Device(config)# line console 0
```

Step 4 Set the idle privileged EXEC timeout.

Example:

```
Device(config-line)# exec-timeout 0 0
```

Idle privileged EXEC timeout is the interval that the privileged EXEC command interpreter waits until user input is detected.

The example shows how to specify no timeout. Setting the **exec-timeout** value to 0 will cause the controller to never log out once logged in. This could have security implications if you leave the console without manually logging out using the disable command.

Step 5 Return to privileged EXEC mode.

Example:

```
Device(config-line)# end
```

Step 6 Display the running configuration file.

Example:

```
Device# show running-config
```

Verify that you have configured the idle privileged EXEC timeout correctly.

Example

This example shows how to set the console idle privileged EXEC timeout to 2 minutes 30 seconds:

```
line console
exec-timeout 2 30
```

This example shows how to set the console idle privileged EXEC timeout to 30 seconds:

```
line console
exec-timeout 0 30
```

Complete the configuration

When using the Cisco setup command facility, and after you have provided all the information requested by the facility as described in *Using the Cisco setup Command Facility* section, the final configuration appears.

To complete your controller configuration, follow these steps.

Procedure

Step 1 Save the configuration. When the facility prompts you to save the configuration, type yes or no.

- If you answer no, the configuration information you entered is not saved, and you return to the controller enable prompt (**WLC#**). Enter **setup** to return to the System Configuration dialog box.
- If you answer yes, the configuration is saved, and you are returned to the user EXEC prompt (`WLC>`).

```
Use this configuration? {yes/no} : yes
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.

%LINK-3-UPDOWN: Interface GigabitEthernet0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1/0, changed state to up

<Additional messages omitted.>
```

Step 2 Press return to get the `WLC>` prompt when the messages stop appearing on your screen. The `WLC>` prompt indicates that you are now at the CLI. You have just completed the initial controller configuration. Note that this is not the complete configuration.

Step 3 Choose to perform either of the steps.

- Run the setup command facility again, and create another configuration:

```
WLC> enable
Password: password
WLC# setup
```

- Modify the existing configuration or configure additional features by using the CLI:

```
WLC> enable
Password:  password
WLC# configure terminal
WLC(config)#
```

Gigabit Ethernet management interface

The controller provides an Ethernet management port named GigabitEthernet0.

The purpose of this interface is to allow users to perform management tasks on the controller; it is an interface that should not, and often cannot, forward network traffic, but can be used to access the controller through Telnet and SSH to perform management tasks on the controller. The interface is most useful in troubleshooting scenarios when other forwarding interfaces are inactive.

These are the aspects of management Ethernet interface:

- The controller has one management Ethernet interface named GigabitEthernet0.
- IPv4, IPv6, and ARP are the only routed protocols supported for the interface.
- The interface provides a way to access the controller even if forwarding interfaces are not functional, or the Cisco IOS is down.
- The management Ethernet interface is part of its own VRF. See the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide* for more details.

Default gigabit Ethernet configuration

By default, a forwarding VRF is configured for the interface with a special group named Mgmt-intf. This cannot be changed. This isolates the traffic on the management interface away from the forwarding plane. Otherwise, the interface can be configured like other Gigabit Ethernet interfaces for most functions.

For example, the default configuration is:

```
interface GigabitEthernet0
vrf forwarding Mgmt-intf
ip address 200.165.200.225 255.255.255.224
negotiation auto
```

Configure Gigabit Ethernet interfaces

This section shows how to assign an IP address and interface description to an Ethernet interface on your controller.

For comprehensive configuration information on Gigabit Ethernet interfaces, see the **Configuring LAN Interfaces** chapter of the *Cisco IOS Interface and Hardware Component Configuration Guide*.

For information on the interface numbering, see the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
WLC> enable
```

Note
Enter your password if prompted.

Step 2 Display a brief status of the interfaces that are configured for IP.

Example:

```
WLC# show ip interface brief
```

Learn which type of Ethernet interface is on your controller.

Step 3 Enter global configuration mode.

Example:

```
WLC# configure terminal
```

Step 4 Specify the Ethernet interface and enter the interface configuration mode.

Example:

```
WLC(config)# interface GigabitEthernet 0
```

Step 5 Set a primary IP address for an interface.

Example:

```
WLC(config-if)# ip address 172.16.74.3 255.255.255.0
```

Step 6 Enable an interface.

Example:

```
WLC(config-if)# no shutdown
```

Step 7 Return to privileged EXEC mode.

Example:

```
WLC(config)# end
```

Step 8 Display a brief status of the interfaces that are configured for IP.

Example:

```
WLC# show ip interface brief
```

Verify that the interfaces are up and configured correctly.

Note
For comprehensive configuration information about IP routing and IP routing protocols, see the **Configuring IP Routing Protocol-Independent Feature** on **cisco.com**.

Save your controller configuration

This section describes how to avoid losing your configuration at the next system reload or power cycle by saving the running configuration to the startup configuration in NVRAM. The NVRAM provides 32 MB of storage on the controller.

Note

- To aid file recovery and minimize downtime in case of file corruption, we recommend that you save backup copies of the startup configuration file and the Cisco IOS XE software system image file on a server.
- To avoid losing work you have completed, be sure to save your configuration occasionally as you proceed. Use the **copy running-config startup-config** command to save the configuration to NVRAM.

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device> enable
```

Enter your password if prompted.

Step 2 Save the running configuration to the startup configuration.

Example:

```
Device# copy running-config startup-config
```

Verify the initial configuration

Enter these commands in Cisco IOS XE to verify the initial configuration on the controller:

- **show version**: Displays the system hardware version, the installed software version, the names and sources of configuration files, the boot images, and the amount of installed DRAM, NVRAM, and flash memory.
- **show diag all eeprom**: Lists and displays the chassis, slot location, and subslot location details.

- **show interfaces**: Shows if interfaces are operating correctly and if interfaces and line protocols are in the correct state, either up or down.
- **show ip interface brief**: Displays a summary of the interfaces configured for IP protocol.
- **show configuration**: Helps verify if you have configured the correct hostname and password.

After you have completed and verified the initial configuration, the specific features and functions are ready to be configured. See the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

Power off the controller safely

Before you begin

We recommend that before turning off all power to the chassis, you issue the reload command. This ensures that the operating system cleans up all the file systems.

Procedure

Step 1 Slip on the ESD-preventive wrist strap included in the accessory kit.

Step 2 Change the controller **config-register** by running these commands.

```
wlc#
wlc# conf t
wlc(config)# config-register <config-register-number>
```

Note
config-register-number refers to the config register number. The valid range is from 0x0 to 0xFFFF.

You can use *0x2102* as the config register number for the initial deployment.

Step 3 Save the controller configuration with this command.

```
wlc# write memory
```

Step 4 Enter the **reload** command.

Step 5 Confirm the reload command.

```
wlc# reload

Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
Chassis 1 reloading, reason - Reload command
Feb  6 19:50:38.556: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting:
Feb  6 19:5
Initializing Hardware ...
System integrity status: 90170200 21030107
```

Step 6 After confirming the reload command, wait until the system bootstrap message is displayed before powering off the system.

```
System Bootstrap, Version 17.18(1r), DEVELOPMENT SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.
Compiled Wed Apr 30 09:49:11 2025 by ankurath
```

```
Current image running: Boot ROM1
Last reset cause: LocalSoft

CW9800L platform with 33554432 Kbytes of main memory
```