

Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide

First Published: 2019-04-04

Last Modified: 2022-12-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface vii

About this Guide vii

Conventions vii

Related Documentation viii

CHAPTER 1

Overview of Cisco Catalyst 9800-L Wireless Controller 1

Summary of Cisco Catalyst 9800-L Wireless Controller Features 2

Platform Components 3

Cisco Catalyst 9800-L Wireless Controller Front Panel 3

Front Panel LEDs: Definitions of States 4

Cisco Catalyst 9800-L Wireless Controller Rear Panel 5

CHAPTER 2

Prepare Your Site for Installation 7

Installation Guidelines and Safety Warnings 7

Unpacking and Inspecting the Controller 9

Package Contents 10

Requirements Tools and Information 10

Choosing a Physical Location 10

CHAPTER 3

Install the Cisco Catalyst 9800-L Wireless Controller 13

Mount the controller 13

Mounting the Controller on Desktop or Shelf 13

Mounting the Controller on a Wall 15

Rack Mounting the Controller 17

Connecting the Controller Console Port 24

Management Ethernet Port Cable Connection 24

Installing a Security Lock 25

CHAPTER 4 **Install the Power Supply 27**

Overview on Power Supply 27

Installation Guidelines 30

Installing an AC Power Supply 30

Finding the Power Supply Serial Number 30

CHAPTER 5 **Remove and Replace Internal Components 31**

Remove and replace the battery 31

Remove the battery 31

Replace the battery 33

CHAPTER 6 **Power Up and Initial Configuration 35**

Powering Up the Controller 35

Initial controller configuration 36

Using the Cisco IOS XE CLI - Cisco setup command facility 36

Day 0 CLI wizard for the controller 37

Day 0 Web UI Wizard for the Controller 42

Using the Cisco IOS-XE CLI—Manual Configuration 42

Configuring the Controller Hostname 43

Configuring the Enable and Enable Secret Passwords 43

Configuring the Console Idle Privileged EXEC Timeout 44

Completing the Configuration 45

Gigabit Ethernet Management Interface Overview 46

Default Gigabit Ethernet Configuration 47

Configuring Gigabit Ethernet Interfaces 47

Saving Your Controller Configuration 48

Verifying the Initial Configuration 49

Powering Off the Controller Safely 49

CHAPTER 7 **License Information 51**

Evaluation license 51

View license information 51

View the Cisco IOS license level 51

CHAPTER 8 **Factory Reset** 53

Information About Factory Reset 53

Prerequisites for Performing Factory Reset 53

Performing Factory Reset 53

APPENDIX A **Controller Specifications** 55

Physical specifications 55

Environmental specifications 55

Power specifications 56



Preface

This preface describes this guide and provides information about the conventions used in this guide, and related documentation. It includes the following sections:

- About this Guide, on page vii
- Conventions, on page vii
- Related Documentation, on page viii

About this Guide

This guide is designed to help experienced network administrators install and minimally configure Cisco Catalyst 9800-L Wireless Controller.

Conventions

This document uses the following conventions for notes, cautions, and safety warnings. Notes and cautions contain important information that you should know.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. Cautions contain information about something you might do that could result in equipment damage or loss of data.

Warning Safety warnings appear throughout this guide in procedures that, if performed incorrectly, can cause physical injuries. A warning symbol precedes each warning statement.

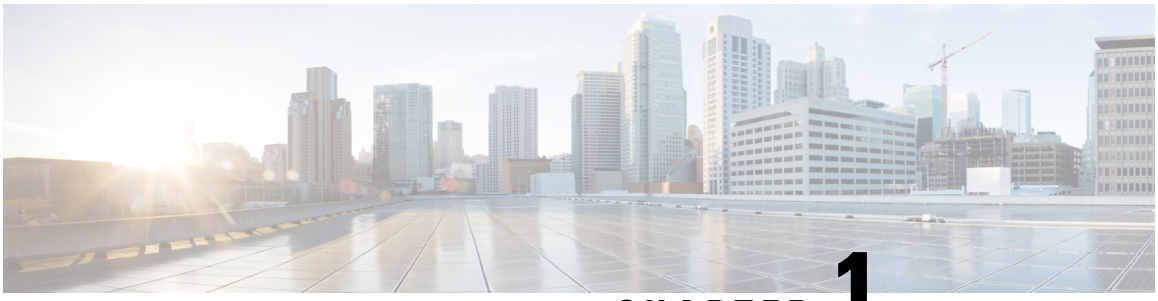
Related Documentation

- For information about the Cisco Catalyst 9800-L Wireless Controller, see:

  https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

- For information about the *Regulatory Compliance and Safety Information—Cisco Wireless 9800L Controller*, see:

  https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/9800-L/regulatory/RCSI-0419-book.pdf



CHAPTER 1

Overview of Cisco Catalyst 9800-L Wireless Controller

Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features from Cisco 3504 Wireless Controller.

The following are the two variations of the controller:

- Cisco Catalyst 9800-L Copper Series Wireless Controller (9800-L-C RJ45).
- Cisco Catalyst 9800-L Fiber Series Wireless Controller (9800-L-F SFP).

For more information about features and benefits, see the *Cisco Catalyst 9800-L Wireless Controller datasheet*.

Figure 1: Cisco Catalyst 9800-L Copper Series Wireless Controller (9800-L-C RJ45)

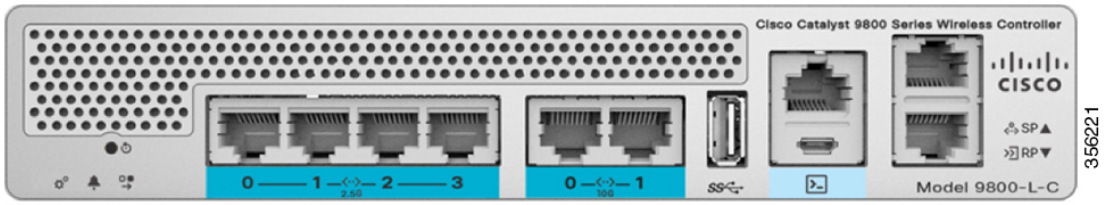
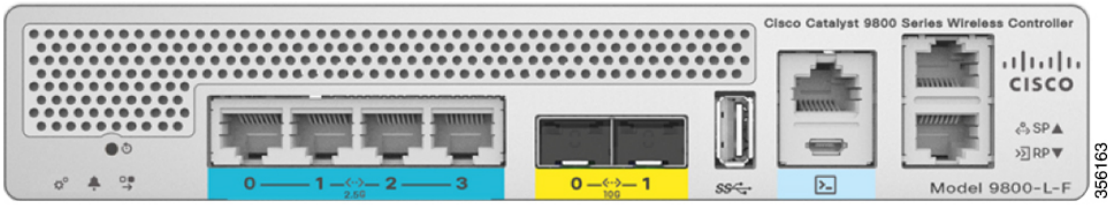


Figure 2: Cisco Catalyst 9800-L Fiber Series Wireless Controller (9800-L-F SFP)



- Summary of Cisco Catalyst 9800-L Wireless Controller Features, on page 2
- Platform Components, on page 3

Summary of Cisco Catalyst 9800-L Wireless Controller Features

Table 1: Cisco Catalyst 9800-L Wireless Controller Features

Feature	Description
Chassis Height	One rack-unit (1RU)
Throughput	5 Gbps
Number of APs supported	250
Number of clients supported	5000
Processor	Intel Broadwell-NE DE—8-core, 2 GHz
Memory Options	• Control/Data Plane Memory—16GB DDR4 • Boot Flash—8MB • Bulk Flash—32GB eMMC
Redundancy, Service Ports	2x 1GE Cu
Data Ports	2x 1G/2.5G/5G/10G Cu (or) 2x 1G/10G Fiber, 4x 1G/2.5G Cu
Storage Temperature	–13° F to 158° F (–25° C to 70° C)
Operating Temperature	32° F to 104° F (0° C to 40° C) **Note** The maximum temperature is derated by 1.0° C for every 1000 ft (305 m) of altitude above sea level.
Storage Humidity	0% to 95% RH non-condensing
Operating Humidity	10% to 95% RH non-condensing
Operational Altitude	0 to 10,000 ft (3048m)
Power Adapter	110W single 12V output adapter (C9800-AC-110W)

Platform Components

Cisco Catalyst 9800-L Wireless Controller Front Panel

Figure 3: Cisco Catalyst 9800-L Wireless Controller Front Panel View

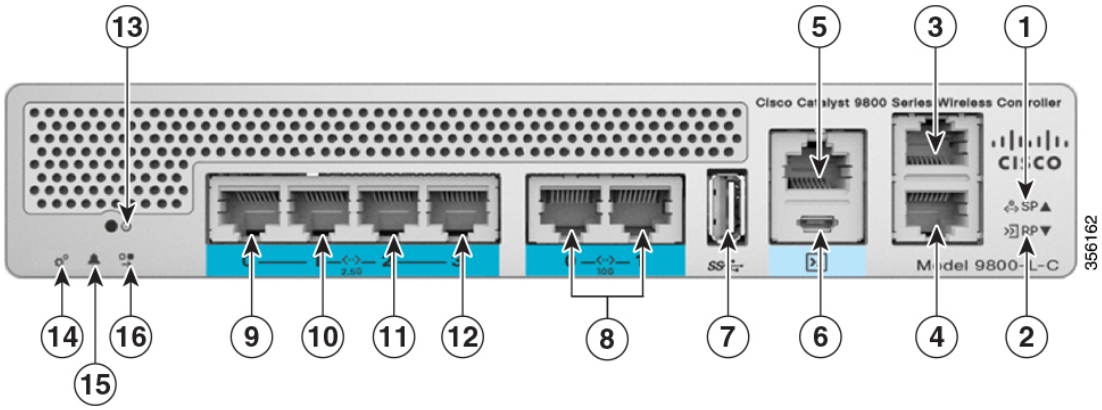


Table 2: Cisco Catalyst 9800-L Wireless Controller Front Panel Components

1	Service Port LED
2	Redundancy Port LED
3	Service Port (SP) (RJ-45) for out-of-band management
4	Redundancy Port (RP) (RJ-45). **Note** The redundancy ports can be connected back to back or via an L2 switch.
5	CPU console port, which is an RJ-45 RS-232 and micro-B USB serial console port. The default RJ-45 se 9600, N, 8, 1. The boot-loader supports baud rates of 1200, 2400, 4800, 9600, 19200, 38400, 57600, and baud-rate recovery mechanism is not available; however, the bootloader ensures that the stored baud rate the allowed values before setting the baud rate. If a nonstandard value is detected, the baud rate will defa Micro-B USB serial connection takes precedence over RJ-45 when both connections are made. **Note** If the Micro-B USB console port is used, the CPU console port that supports RJ-45 connector is ignored. the two ports are ever active.
6	Micro USB Type-B console port that can be used to perform software updates in addition to the already av namely HTTP, TFTP, FTP, and SFTP. **Note** If you connect both the Micro USB Type-B console port and the CPU console port, then USB port takes CPU console port is ignored as only one of the two ports are ever active.

7	Type A 3.0 USB port used to perform software updates in addition to already available transfer mode, namel FTP, and SFTP.
8	2x 10 G/mGig ports. This mGig port supports speeds of 10G, 5G, 2.5G, and 1G. **Note** In a High Availability environment, it is not possible to change the configured port speed.
9, 10, 11, and 12	mGig ports. These mGig ports support only 2.5G and 1G speeds. Gigabit Ethernet ports 1,2, 3, and 4 are RJ-45 connector form-factors. These ports are designed so that 1500 (per the 802.3 specification) is met between chassis ground and any Ethernet signal. **Note** The ports can be used for infra-switch connection using multiple an AP-Manager or data interface.
13	Reset button • Pushing the Reset button for less than 10 seconds will reload the controller. • Pushing the Reset button for more than 10 seconds will erase the startup configuration in NVRAM of th
14	System LED that determines if the system is powered up and booted.
15	Alarm LED that determines a status or error occurred. The status or error is posted on the console screen.
16	High Availability LED

Front Panel LEDs: Definitions of States

Table 3: System LED Indicators

Color	Description
Off	System not receiving power. System crash Firmware upgrade Temperature error
Blinking Green	System boot
Red	Controller error. For example, an internal voltage error exists.

Table 4: Alarm LED Indicators

Color	Description
Blinking Green	Controller image upgrade

Color	Description
Red	Controller error. For example, a temperature error exists. **Note** When only one TenGig port is connected, an alarm is triggered and the Alarm LED remains on and red. This does not occur when only one mGig port is connected.

Note The Cisco Catalyst 9800-L Wireless Controller has an external power adapter.

The Alarm Bell LED is illuminated **red**, if the **10-G** uplink ports are not connected to the switch. This does not mean a system or hardware failure. When the interfaces are disabled in the controller, the **red** light remains off even when the controller is not connected.

Table 5: High Availability LED Indicators

Color and State	Description
Green	On: HA active
Green	Slow blinking: HA standby hot
Amber	Slow blinking: HA standby cold
Amber	Fast linking: HA maintenance

Cisco Catalyst 9800-L Wireless Controller Rear Panel

Figure 4: Cisco Catalyst 9800-L Wireless Controller Rear Panel View

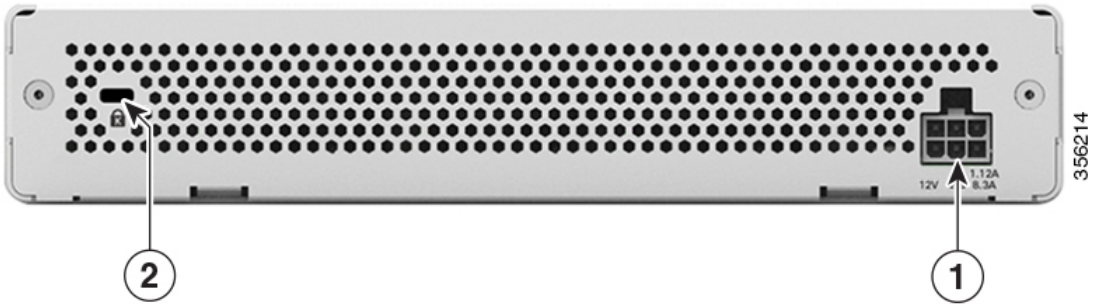
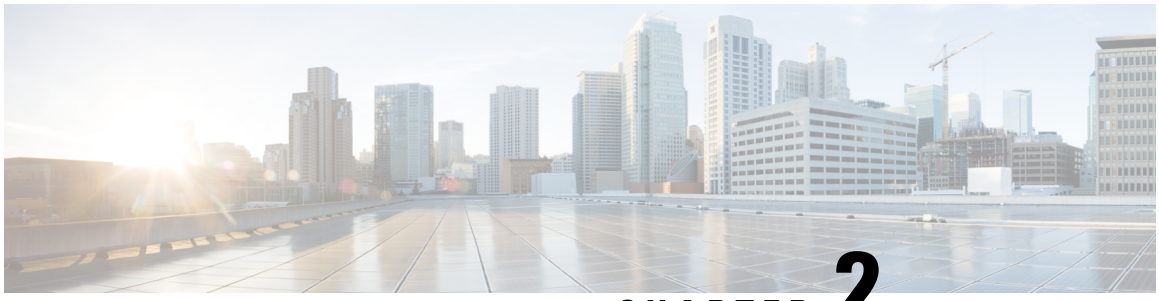


Table 6: Cisco Catalyst 9800-L Wireless Controller Rear Panel Components

1	External 110W, single output 12VDC power adapter (C9800-AC-110W).

2	Kensington security slot



CHAPTER 2

Prepare Your Site for Installation

This section describes how to prepare your site for installation:

- Installation Guidelines and Safety Warnings, on page 7
- Unpacking and Inspecting the Controller, on page 9
- Package Contents, on page 10
- Requirements Tools and Information, on page 10
- Choosing a Physical Location, on page 10

Installation Guidelines and Safety Warnings

This section includes the basic installation guidelines and safety warning statements. Read this section before you start the installation procedure. Translations of the warning statements appear in the RCSI guide on Cisco.com.

- The operating environment must be within the ranges listed in the "Environmental Specifications" section.
- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures. Make sure that the cabling is safely away from other devices that might damage the cables.
- Airflow around the device and through the vents is unrestricted
- Humidity around the device does not exceed 95 percent.
- Altitude at the installation site is not greater than 10,000 feet.
- Do not place any items on the top of the device.
- For 10/100/1000 fixed ports, the cable length from a switch to a connected device cannot exceed 328 feet (100 meters).
- Clearance to the front and rear panel meets these conditions:
    - Front-panel LEDs can be easily read.
    - Access to ports is sufficient for unrestricted cabling.



Warning To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 40° C (104° F). The maximum temperature is derated by 1.0° C for every 1000 ft (305 m) of altitude above sea level. **Statement 1047**



Warning To prevent airflow restriction, allow clearance around the ventilation openings to be at least 50 mm (5 cm). **Statement 1076**



Warning Read the installation instructions before connecting the system to the power source. **Statement 1004**.



Warning Ultimate disposal of this product should be handled according to all national laws and regulations. **Statement 1040**.



Warning No user-serviceable parts inside. Do not open. **Statement 1073**.



Warning Installation of the equipment must comply with local and national electrical codes. **Statement 1074**.



Warning **Hot surface. Statement 1079**.



Warning Connect the unit only to DC power source that complies with the Safety Extra-Low Voltage (SELV) requirements in IEC 60950 based safety standards. **Statement 1033**.



Warning Class 1 laser product. **Statement 1008**

Warning Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard.

Fiber type and Core diameter (µm)	Wavelength (nm)	Max. Power (mW)
SM 11	1200 - 1400	39 - 50
MM 62.5	1200 - 1400	150
MM 50	1200 - 1400	135
SM 11	1400 - 1600	112 - 145

1056

Warning Pluggable optical modules comply with IEC 60825-1 Ed. 3 and 21 CFR 1040.10 and 1040.11 with or without exception for conformance with IEC 60825-1 Ed. 3 as described in Laser Notice No. 56, dated May 8, 2019. **Statement 1255**.

Unpacking and Inspecting the Controller

Follow these steps to unpack the Cisco Catalyst 9800-L Wireless Controller and prepare it for operation:

Procedure

Step 1 Remove the controller from its container and save all the packaging material.

Step 2 Compare the shipment to the equipment list provided by your Cisco customer service representative. Verify that you have all the items.

Step 3 Check for damage and report discrepancies or damage, if any, to your Cisco customer service representative. Before speaking to the representative, have the following information ready:

- Invoice number of shipper (see the packing slip)
- Model and serial number of the damaged unit
- Description of damage

- Effect of damage on the installation

Package Contents

Each Cisco Catalyst 9800-L Wireless Controller package contains the following items:

- One Cisco Catalyst 9800-L Wireless Controller
- One Power supply and power cord (power cord option configurable)
- Optional licenses will be pre-installed on controller at factory, if selected
- Cisco Catalyst 9800-L Wireless Controller software pre-loaded on the controller (software option configurable)
- Four adhesive rubber feet pieces

Requirements Tools and Information

You will need the following tools and information before you can install the controller:

- Wireless controller hardware
  - Controller with factory-supplied power cord and mounting hardware
  - Network, operating system service network, access point cables, and adapter are required
- Command-line interface (CLI) console
  - Serial terminal emulator on CLI console (PC or laptop)
  - Use either RJ-45 console cable or Micro USB Type-B cable to connect CLI console and controller

Choosing a Physical Location

You can install the controller almost anywhere, but it is more secure and reliable if you install it in a secure equipment room or wiring closet. For maximum reliability, mount the controller while following these guidelines:

- Make sure you can reach the controller and all cables attached to it.
- Make sure that water or excessive moisture cannot get into the controller.
- To prevent airflow restriction, allow clearance around the ventilation openings to be at least 50 mm (5 cm).
- Verify that the ambient temperature remains between 32° F to 104° F (0° C to 40° C).

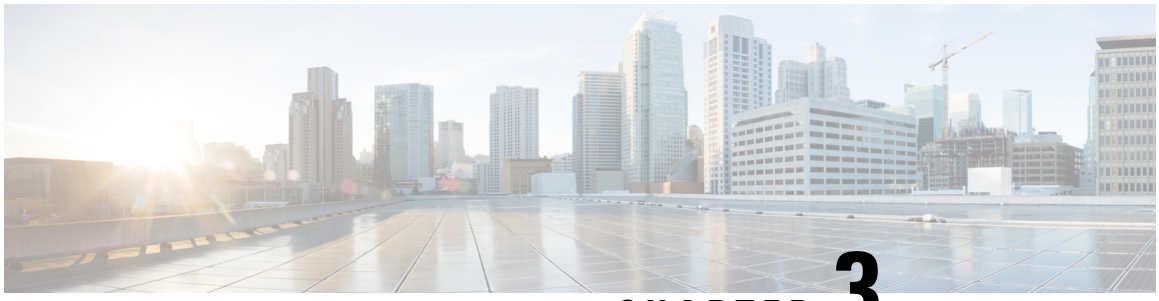
- Make sure that the controller is within 328 ft. (100 m) of equipment connected to the 10/100/1000 Mbps Ethernet ports.
- Make sure that the power supply adapter and the power cord can reach a 100 to 240 VAC grounded electrical outlet.
- Make sure that at least two rack-units space is available for rack tray kit, if you are installing the controller in a rack.



Warning This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. **Statement 1024**.



Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 20A. **Statement 1005**.



CHAPTER 3

Install the Cisco Catalyst 9800-L Wireless Controller

This chapter describes how to install the Cisco Catalyst 9800-L Wireless Controller.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. **Statement 1071**

SAVE THESE INSTRUCTIONS

- Mount the controller, on page 13
- Connecting the Controller Console Port, on page 24
- Management Ethernet Port Cable Connection, on page 24
- Installing a Security Lock, on page 25

Mount the controller

This section describes the various mounting options for the controller:

Mounting the Controller on Desktop or Shelf

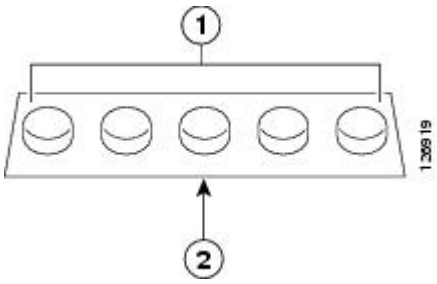
Before mounting the controller on a desktop or shelf, install the rubber feet located in accessory kit shipped with the controller.

To install the rubber feet to the controller, follow these steps:

Procedure

Step 1 Locate the rubber feet on the black adhesive strip that is shipped with the controller.

Figure 5: Identifying the Rubber Feet

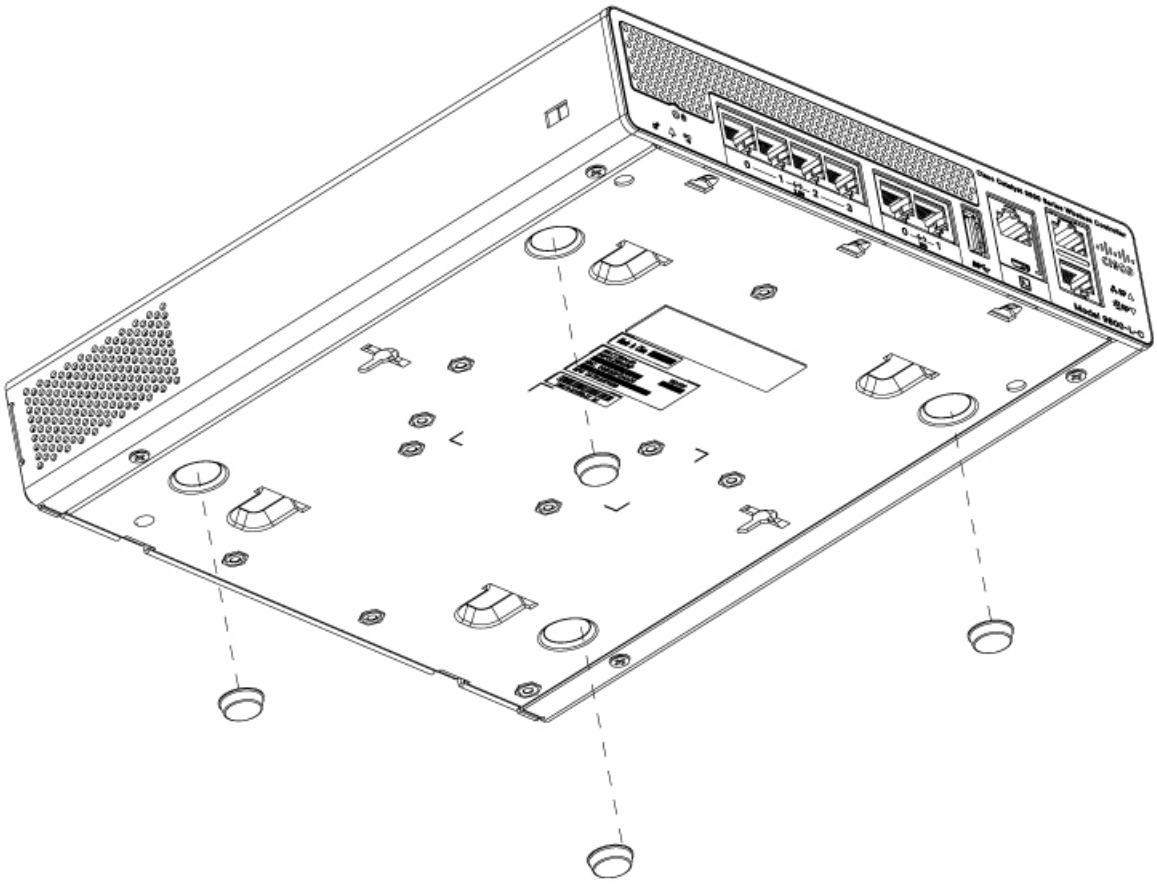


1	Rubber feet	2	Black adhesive strip

Step 2 Place the controller upside down, on a smooth, flat surface.

Step 3 Peel off the rubber feet from the black adhesive strip and press them adhesive-side down onto the bottom four corners of the controller, see the figure below:

Figure 6: Attaching the Rubber Feet



Step 4 Place the controller right-side up on a flat, smooth, secure surface.

Step 5 Connect the interface cables.

Mounting the Controller on a Wall

Note Do not wall-mount the device with its front panel facing up. Following safety regulations, wall-mount the device with its front panel facing down or to the side to prevent airflow restriction and to provide easier access to the cables.

Warning Read the wall-mounting carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system. **Statement 378**.

Note Wall mounting screws are not supplied. Installer must supply proper screws in accordance with local codes.

Controller wall mount holes located on the bottom of the enclosure fit standard #6 or M3 Pan Head screw. The type of screw used to mount to wall should follow local guidelines for wall type and material.

To mount the controller on a wall using mounting screws, follow these steps:

Procedure

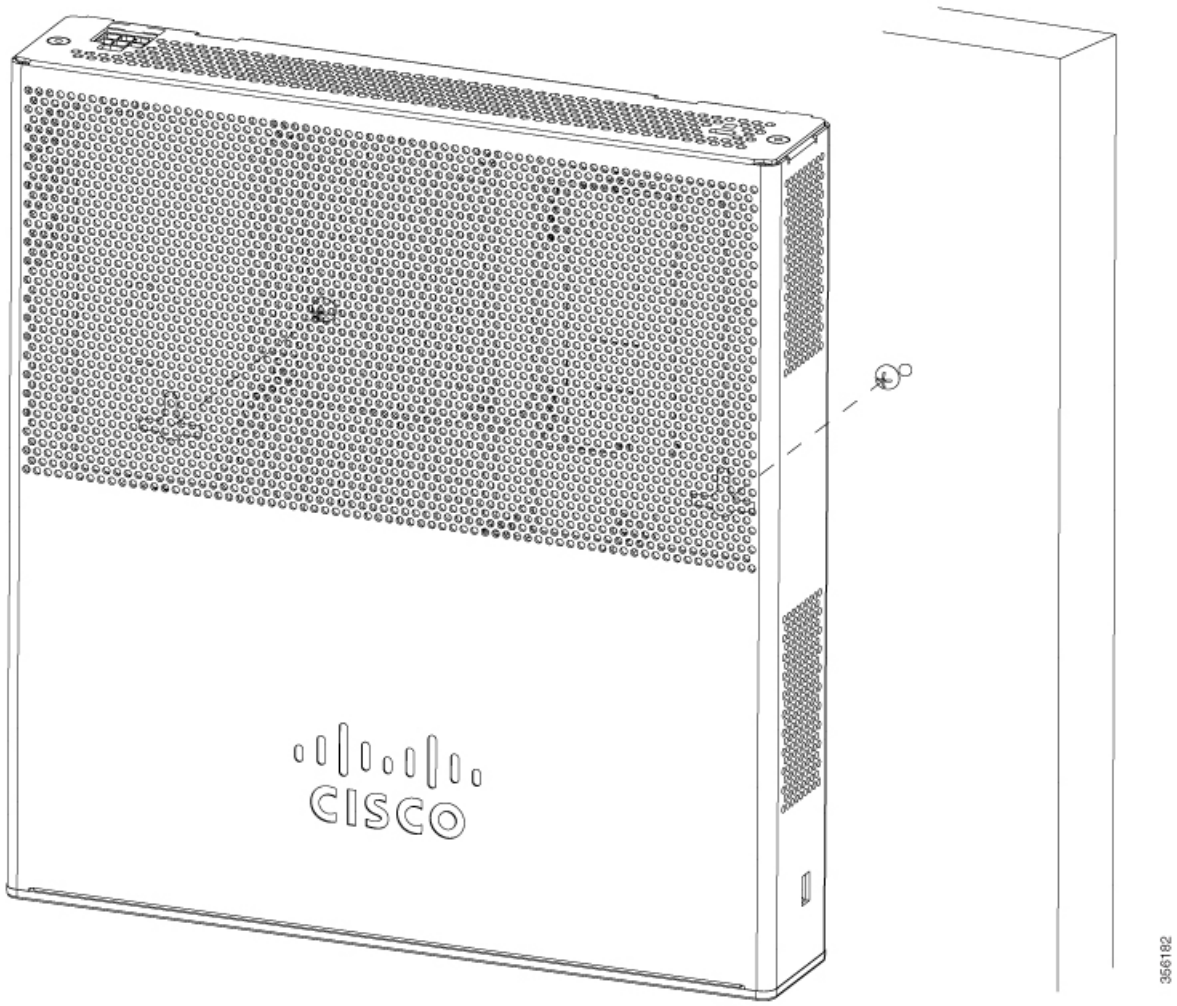
Step 1 Mark the location of the mounting screws on the wall. Use the mount hole locations on the back of the controller for placement of the mounting screws. Mounting screw spacing is 6 1/8 inch (155.4 mm).

Step 2 Install two screws and tighten until the top of the screws are 1/8 inch (3 mm) from the wall (leaving enough room for the back panel to slide onto the screws firmly).

Step 3 Place the controller onto the mounting screws and slide it down until it lock into place, as shown in figure below:

Note
The front panel of the controller should be facing down.

Figure 7: Place the Controller on the Mounting Screws



Step 4 After the controller is mounted on the wall, perform the following tasks to complete the installation

- Connecting the Controller Console Port
- Securing the Power Adapter Cable
- Connecting to the Network

Step 5 For configuration instructions about using the CLI setup program, see the (Link to Running the Bootup script section).

Rack Mounting the Controller

Warning To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Statement 1006

Warning Take care when connecting units to the supply circuit so that wiring is not overloaded. **Statement 1018**.

To mount the controller in a 19-inch equipment rack, you can order an optional Optional Rack Mount kit (C9800-RMNT= Cisco Catalyst 9800-L Wireless Controller Rack Mount Tray).

The rack-mount tray is designed for 19 racks and uses two rack-units spaces. To rack-mount the controller, perform the following steps:

Procedure

Step 1 Remove the four rubber feet if previously installed.

Step 2 Slide the Cisco Catalyst 9800-L Wireless Controller in position such that the 4-tray tabs align and latch into the bottom of the unit as it is pushed in place. The front of the Cisco Catalyst 9800-L Wireless Controller should be flush against the front edge of the tray. A nylon latch in the center of the tray snaps into and locks the Cisco Catalyst 9800-L Wireless Controller in place.

Figure 8: Placing the Controller on the Rack Mount Tray

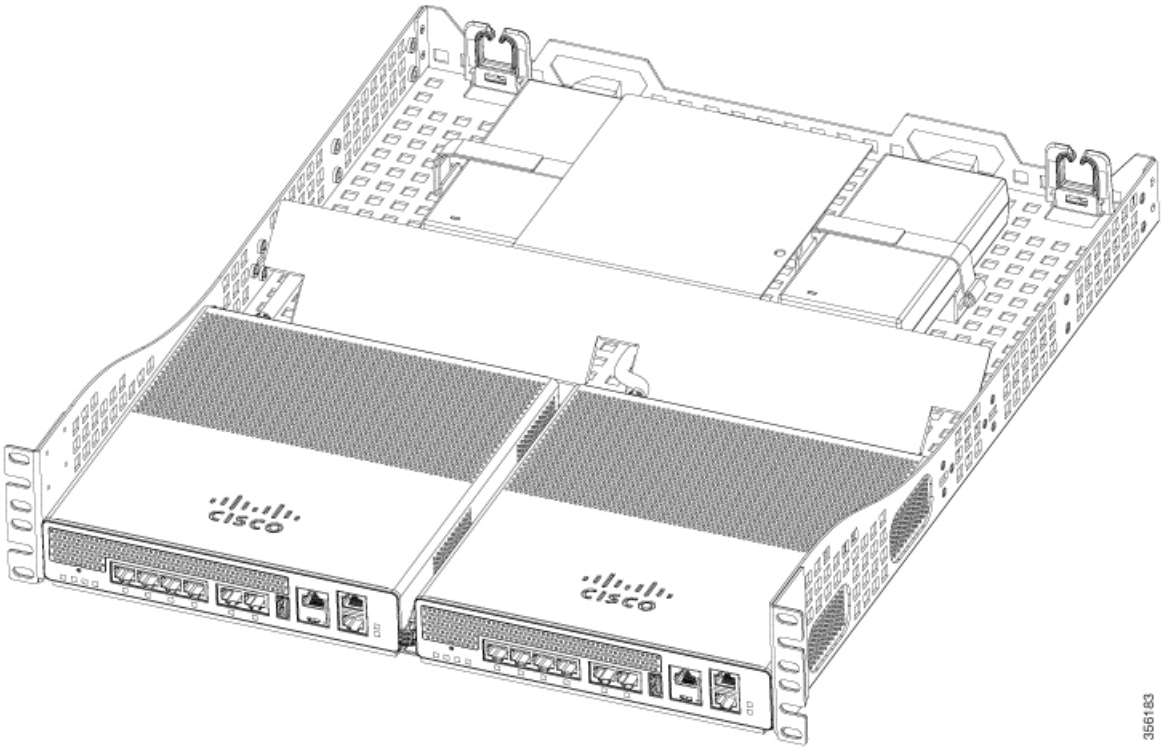
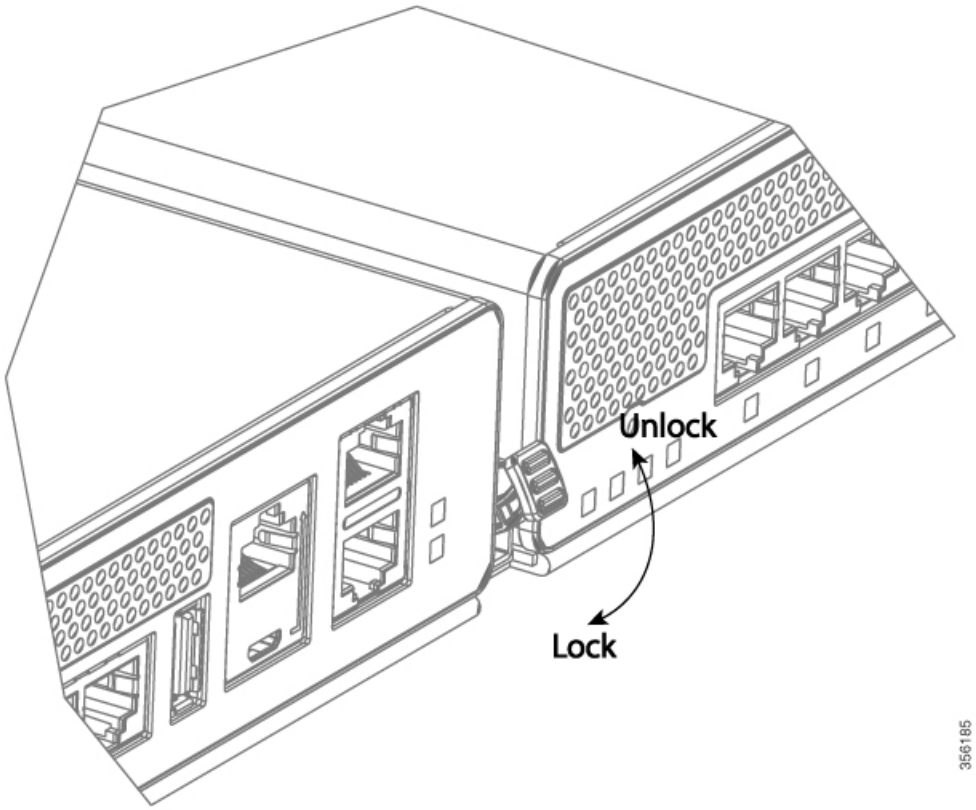
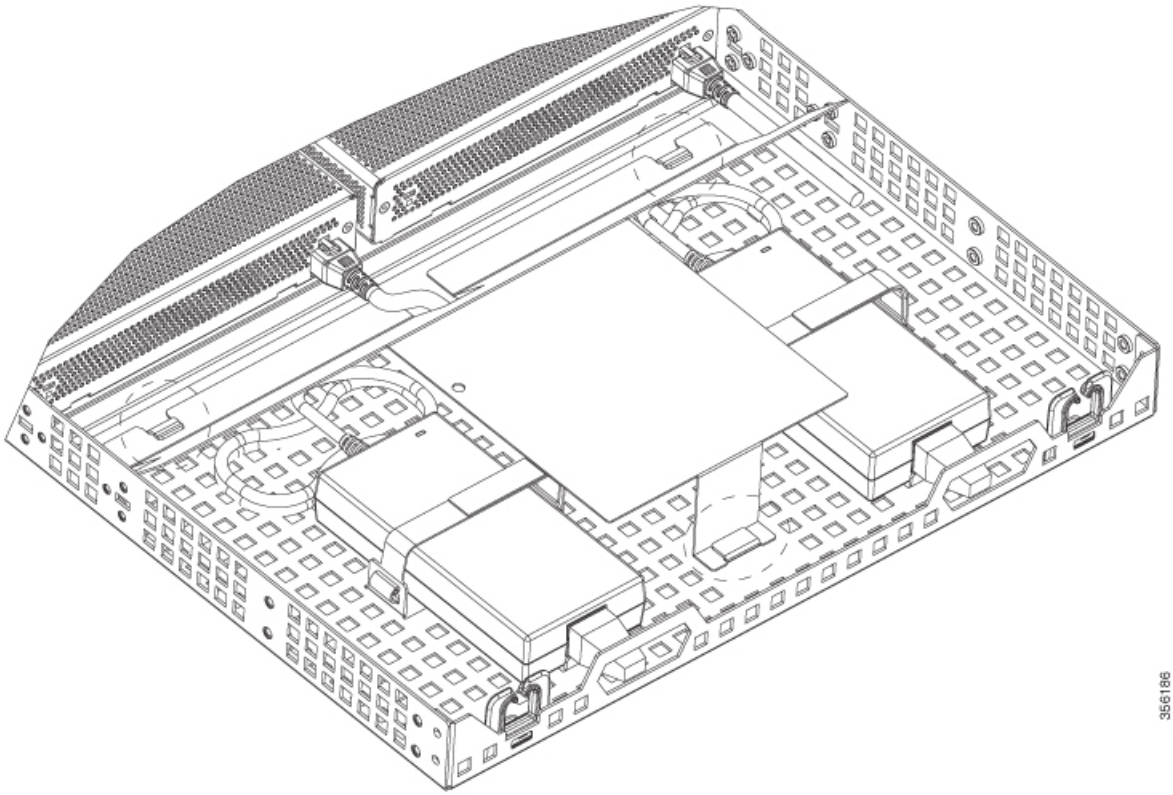


Figure 9: Close-up View of Center Latch Securing Controllers in a Rack



Step 3 Remove power supply baffle in rear tray. Baffles secure with tabs circled.

Figure 10: Power Supply Baffle



Step 4 Place the power adapters between either of the two tabs in the rear of the tray and use the provided velcro straps to secure them.

Step 5 Route the AC wiring through the cable management clips.

Step 6 Re-install and secure tabs on power supply baffle, coil extra cables, and locate them under the baffle.

Note
This is an hot air baffle.

Step 7 Attach the rack mount tray to the rack using the supplied screws and brackets, as shown in figures below:

Figure 11: Attaching the Rack Mount Tray to a Front Post Rack

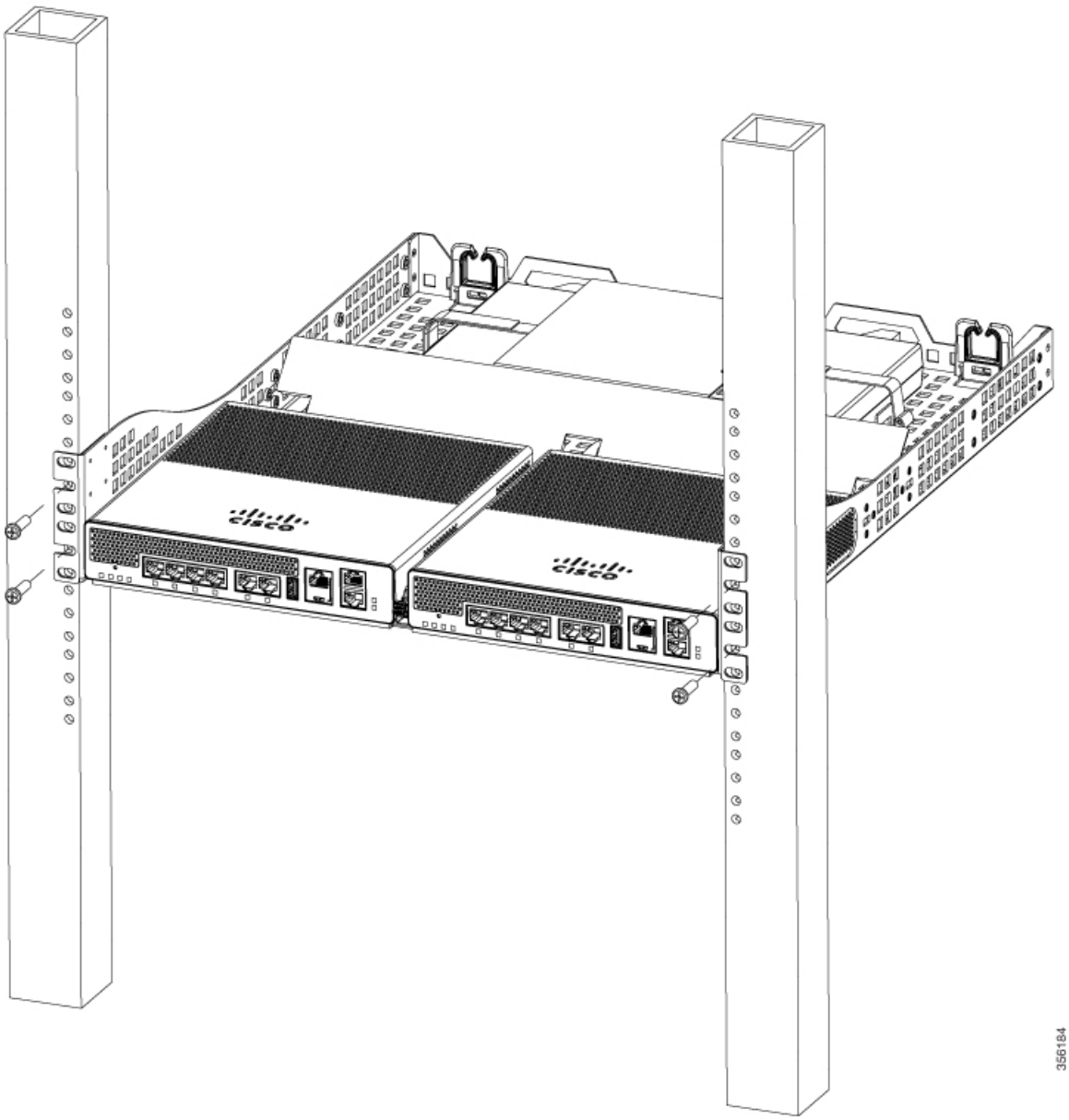
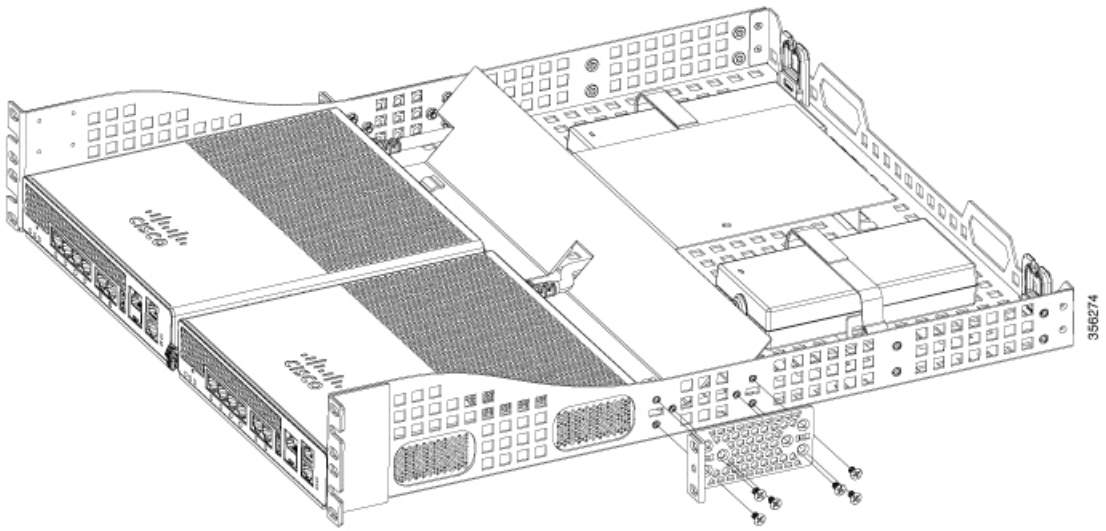
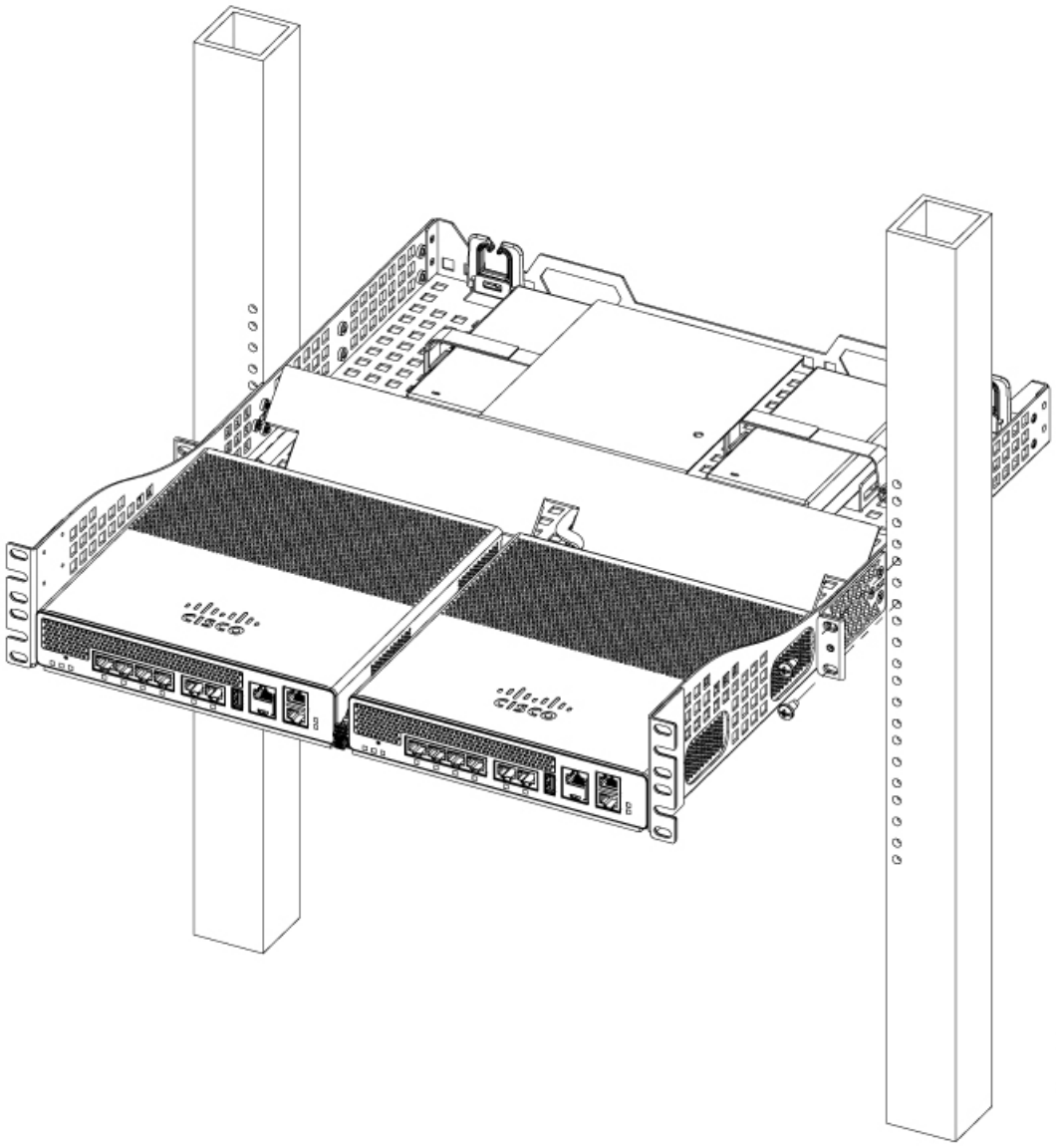


Figure 12: Installing the Rack Mount Tray to a Center Post Rack



Note
Install the center mount brackets to both sides of the tray.

Figure 13: Installing the Rack Mount Tray to a Center Post Rack



To remove the chassis from the rack, remove the screws that attach the chassis to the rack, and then remove the chassis.

Step 8 (optional): If required install the rear rack mount bracket for additional stability on four-post racks.

Include optional orderable rear rack mount adapter kit: C4948E-BKT-KIT= C49xxE front and rear mount brackets.

Connecting the Controller Console Port

Note Install the USB device driver before establishing a physical connection between the controller and the PC using the USB Console cable plugged into the USB serial port, otherwise the connection will fail.

Procedure

Step 1 Perform either one of the following tasks:

- Connect the end of the console cable with the RJ-45 connector to the console port on the controller.
- Connect a Micro USB Type-B cable to the Micro USB console port. If you are using the USB serial port for the first time on a Windows-based computer, ensure that you have installed the USB driver.

Note
It is not possible to use both the Micro USB console port and the CPU console port concurrently. If both the ports are connected, the USB port takes precedence over the CPU console port.

Step 2 If you are using a standard Cisco DB-9 console cable, connect the end of the cable with the DB-9 connector (or USB Type-A) to the terminal or PC. If your terminal or PC has a console port that does not accommodate a DB-9 connector, you must provide an appropriate adapter for that port.

Step 3 To communicate with the controller, start a terminal emulator application. This software should be configured with the following parameters:

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

Management Ethernet Port Cable Connection

Before you begin

Caution To comply with Class A emission requirements, a shielded Ethernet cable must be used for the connection

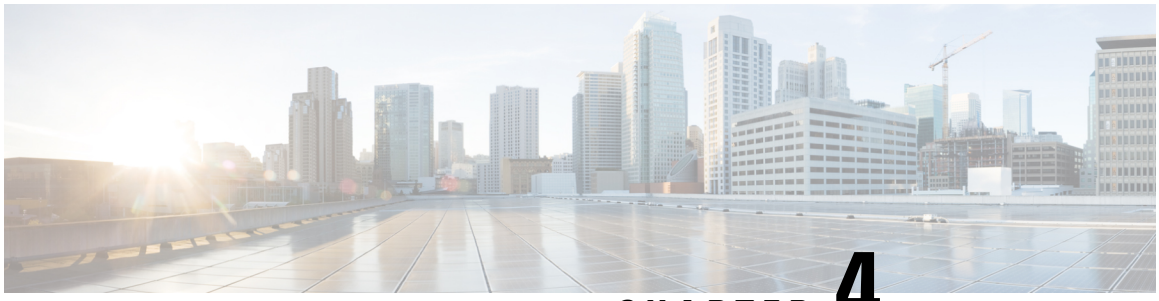
Procedure

Step 1 Insert an Ethernet RJ-45 cable into the MGMT port.

Step 2 Insert the other end of the RJ-45 cable to your management device or network.

Installing a Security Lock

The controller has a security slot on the back panel. You can install an optional customer-supplied Kensington lock, such as the type that is used to secure a laptop computer, to secure the controller. See the "Cisco Catalyst 9800-L Wireless Controller Rear Panel" section for the location of the security lock.



CHAPTER 4

Install the Power Supply

This chapter describes how to install the power supply.

The controller can be powered using one power supply unit.

The power supply do not have an on/off switch and can only be powered down by removing AC input.

- Overview on Power Supply, on page 27
- Installation Guidelines, on page 30
- Installing an AC Power Supply, on page 30
- Finding the Power Supply Serial Number, on page 30

Overview on Power Supply

The following table describes the external power supply.

Table 7: Power Supply Adapter Part Number and Description

Part Number	Description
C9800-AC-110W	110W AC power supply

The 110W AC power supply is an autoranging unit that supports input voltages between 100 and 240 VAC.

The power supply adapter uses an 18- AWG power cord for connection to an AC power outlet.

Figure 14: 110W AC Power Cord



A 6-pin latching DC connector supplies power to the controller.

Figure 15: 6-Pin Latching DC Connector



Figure 16: DC Power Cord



Verifying Connections

To verify if the power supply adapter is connected to the power outlet, first turn on the power, then check the LED status.

Figure 17: LED Location



The following table describes the LED status of the power supply adapter.

Table 8: Power Supply Adapter LED and Description

Power Supply Adapter LED	Description
Off (LED is off)	No input power.
Green	Input power present.

Installation Guidelines

This section includes the basic installation guidelines for installing a power supply. Read this section before you start the installation procedure. Translations of the warning statements appear in the RCSI guide on Cisco.com.

Observe these guidelines when installing a power supply:

- A power supply that is only partially connected to the controller can disrupt the system operation.

Warning Installation of the equipment must comply with local and national electrical codes. **Statement 1074**

Warning Only trained and qualified personnel should be allowed to install, replace, or service this equipment. **Statement 1030**.

Installing an AC Power Supply

Procedure

Step 1 Connect the power cord to the power supply and to an AC power outlet. Turn on the power at the power source.

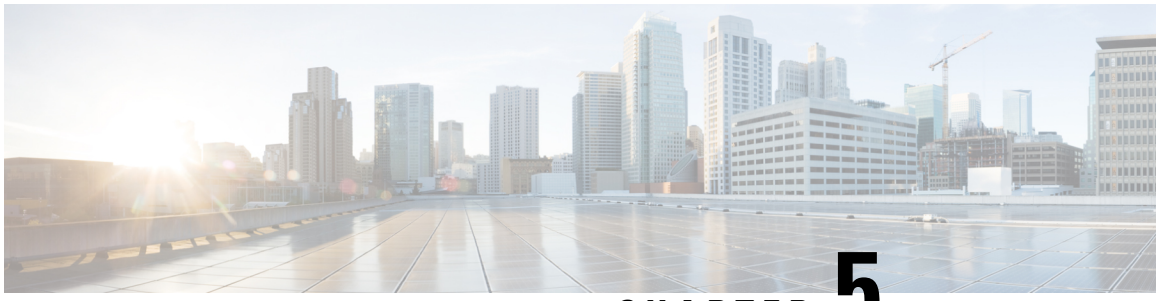
Step 2 Plug the DC cord into the controller.

Step 3 Confirm that the power supply PS OK LED is green.

Finding the Power Supply Serial Number

If you contact Cisco Technical Assistance regarding a power supply, you need to know the serial number.

You can find the serial number printed on the external power adapter.



CHAPTER 5

Remove and Replace Internal Components

- Remove and replace the battery, on page 31

Remove and replace the battery

These instructions are provided in order to comply with the EU Battery Replaceability Requirement.

- This product was not specifically designed for battery replacement in the field.
- It is recommended that, whenever possible, follow the standard repair or return process for battery issues.

Caution Always wear an ESD-preventive wrist strap and ensure that it makes good contact with your skin when you remove or install the internal modules. Connect the equipment end of the wrist strap to the metal part of the chassis.

Remove the battery

Use this procedure to access and remove the battery from the controller.

Note Follow proper electrostatic discharge (ESD) precautions before handling the battery or device.

Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to channel unwanted ESD voltages safely to ground. To guard against ESD damage and shocks, the wrist strap and cord must operate effectively.

Warning Statement 1015—Battery Handling

To reduce risk of fire, explosion or leakage of flammable liquid or gas:

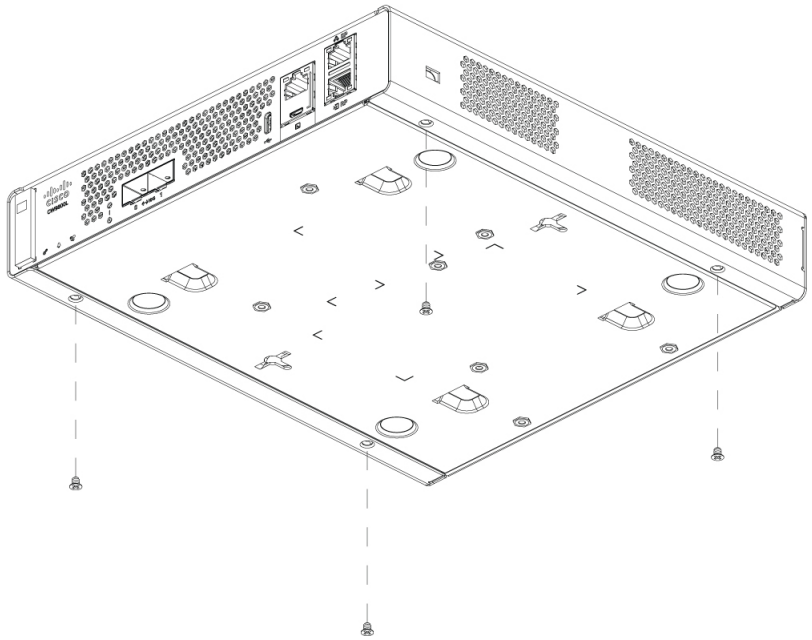
- Replace the battery only with the same or equivalent type recommended by the manufacturer.
- Do not dismantle, crush, puncture, use sharp tool to remove, short external contacts, or dispose of in fire.
- Do not use if battery is warped or swollen.

Procedure

Step 1 Read the Safety Warnings section, and disconnect the power supplies before you remove the battery.

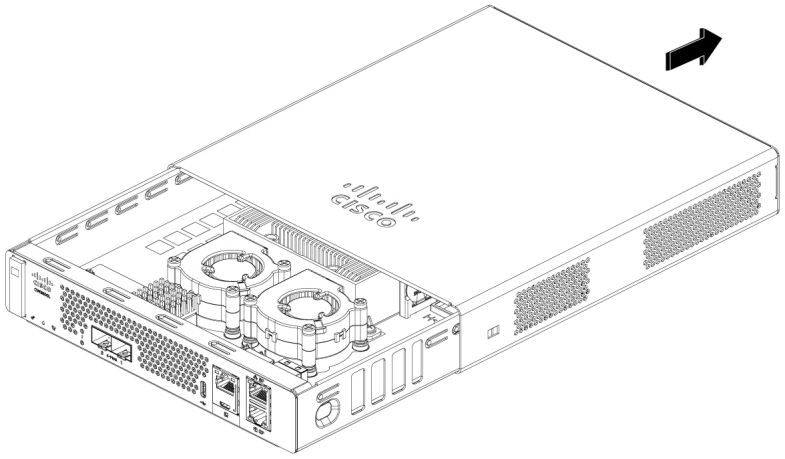
Step 2 Remove the screws from the wrap-around cover on the underside of the controller.

Figure 18: Remove the screws from the wrap-around cover



Step 3 Slide the cover off the base.

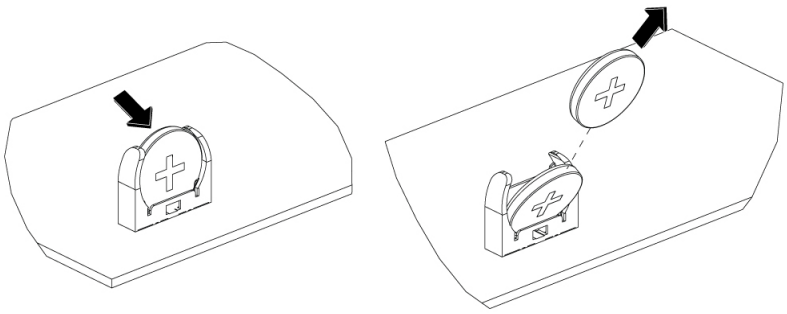
Figure 19: Slide the cover off the base



Step 4 Pivot the battery in the direction shown.

Step 5 Pull the battery out of the holder at an angle.

Figure 20: Remove the battery



Replace the battery

Use this procedure to replace the battery and secure the controller cover.

Before you begin

The battery is a BR2032 type. You should only replace batteries with the same or an equivalent type recommended by the manufacturer.

- Panasonic BR-2032/BN

Note Follow proper electrostatic discharge (ESD) precautions before you handle the battery or the device.

Procedure

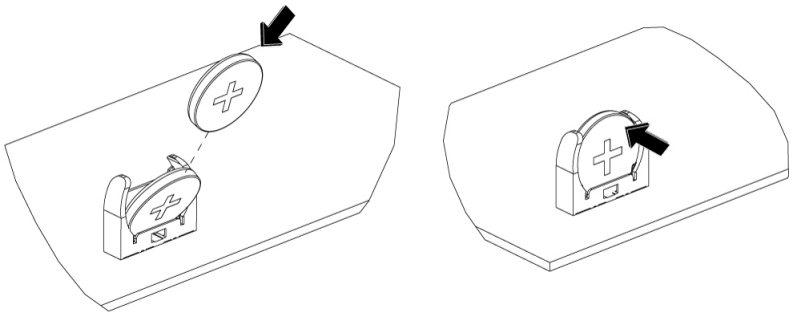
Step 1 Read the safety warnings and disconnect the power supplies before you replace the battery.

Step 2 Orient the battery with the positive side facing up, as shown.

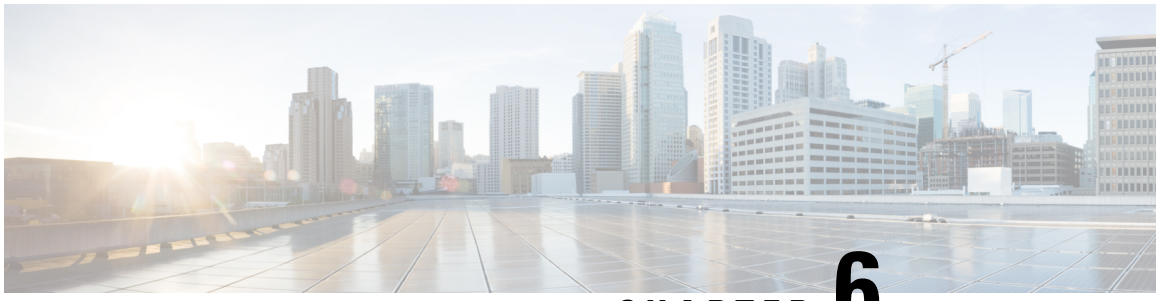
Step 3 Insert the edge of the battery into the battery holder at an angle.

Step 4 Rotate the battery into the holder, and press down until the battery is seated firmly.

Figure 21: Install the battery



Step 5 Replace the cover, and secure it with the screws.



CHAPTER 6

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.

- Powering Up the Controller, on page 35
- Initial controller configuration, on page 36
- Gigabit Ethernet Management Interface Overview, on page 46
- Saving Your Controller Configuration, on page 48
- Verifying the Initial Configuration, on page 49
- Powering Off the Controller Safely, on page 49

Powering Up 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 Catalyst 9800 controller or the password from ROMMON mode, see the following link:

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 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*.

Using the Cisco IOS-XE CLI—Manual Configuration

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#
```

Configuring 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `WLC> enable`	Enables privileged EXEC mode. **Note** Enter your password if prompted.
Step 2	**configure terminal** **Example:** `WLC# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `WLC(config)# hostname myWLC`	Specifies or modifies the hostname for the network server.
Step 4	**end** **Example:** `myWLC(config)# end`	(Optional) Returns to privileged EXEC mode.

Configuring the Enable and 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 **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 the **Cisco IOS Password Encryption Facts** tech note and the **Cisco Guide to Harden Cisco IOS Devices** tech note.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. **Note** Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**enable secret** *password* **Example:** `Device(config)# enable secret greentree`	Specifies an additional layer of security over the **enable password** command.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Verify that your new enable or enable secret password works.

Configuring 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. **Note** Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**line console 0** **Example:** `Device(config)# line console 0`	Configures the console line and starts the line configuration command collection mode.
Step 4	**exec-timeout** *minutes* [*seconds*] **Example:** `Device(config-line)# exec-timeout 0 0`	Sets the idle privileged EXEC timeout, which 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	**end** **Example:** `Device(config-line)# end`	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Device# show running-config`	Displays the running configuration file. Verify that you have configured the idle privileged EXEC timeout correctly.

Example

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

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

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

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

Completing 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 The facility prompts you to save the configuration.

- 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 When messages stop appearing on your screen, press Return to get the `WLC>` prompt.

Step 3 The `WLC>` prompt indicates that you are now at the command-line interface (CLI).

You have just completed an initial controller configuration. Note that this is not a complete configuration. At this point, you have two choices:

- 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 Overview

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.

The following aspects of the management Ethernet interface should be noted:

- 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 as follows:

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

Configuring 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `WLC> enable`	Enables privileged EXEC mode. **Note** Enter your password if prompted.
Step 2	**show ip interface brief** **Example:** `WLC# show ip interface brief`	Displays a brief status of the interfaces that are configured for IP. Learn which type of Ethernet interface is on your controller.
Step 3	**configure terminal** **Example:** `WLC# configure terminal`	Enters global configuration mode.
Step 4	**interface GigabitEthernet 0** **Example:** `WLC(config)# interface GigabitEthernet 0`	Specifies the Ethernet interface and enters the interface configuration mode.
Step 5	**ip address** *ip-address mask* **Example:** `WLC(config-if)# ip address 172.16.74.3 255.255.255.0`	Sets a primary IP address for an interface.

	Command or Action	Purpose
Step 6	**no shutdown** **Example:** `WLC(config-if)# no shutdown`	Enables an interface.
Step 7	**end** **Example:** `WLC(config)# end`	Returns to privileged EXEC mode.
Step 8	**show ip interface brief** **Example:** `WLC# show ip interface brief`	Displays a brief status of the interfaces that are configured for IP. 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**.

Saving 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

Note 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. **Note** Enter your password if prompted.

	Command or Action	Purpose
Step 2	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves the running configuration to the startup configuration.

Verifying the Initial Configuration

Enter the following 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*.

Note When bit errors occur due to memory failure, you get to view the following logs:

```
"EDAC MC0: 1 UE INTERAL ERROR on unknown memory (channel:<channel-number> csrow:0
page:<address> offset:<address> grain:1 - MBE)
Kernel panic - not syncing: UE INTERAL ERROR on unknown memory (channel:<channel-number>
csrow:0 page:<address> offset:<address> grain:1 - MBE)"
```

Recommended Action:

Check if your Cisco Catalyst 9800-L Wireless Controller is affected by checking the serial number against the affected Serial#. If your controller is affected, you will need to initiate a Return Merchandise Authorization (RMA).

Powering 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 issuing the following 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 config register number *0x2102* as the best case for initial deployment.

Step 3 Save the controller configuration using the following command:

```
wlc# write memory
```

Step 4 Enter the **reload** command.

Step 5 Confirm the reload command:

```
wlc# reload

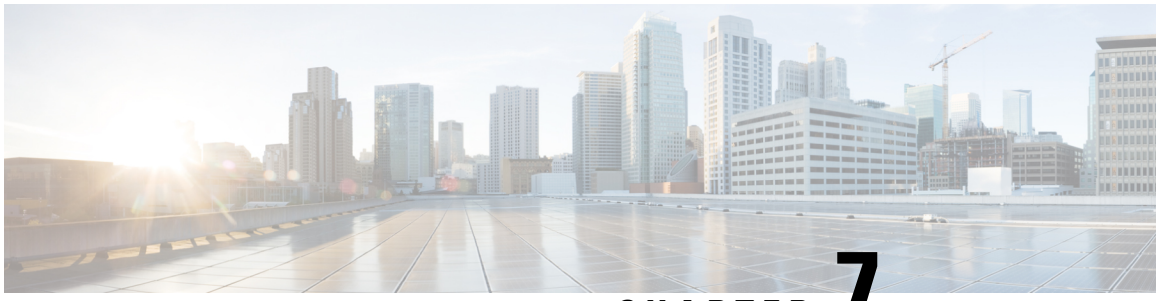
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]
Chassis 1 reloading, reason - Reload command
Feb  6 19:50:38.556: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting:
Feb  6 19:5
Initializing Hardware ...
System integrity status: 90170200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

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

```
System Bootstrap, Version 12.2($v)
[$copy_name 101], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2019  by cisco Systems, Inc.
Compiled Mon 04/15/2019  6:19:54.88 by arcmaitr

Current image running: Boot ROM0
Last reset cause: LocalSoft

The values of MSR  0x198h = 00001400 and MSR 0x199h = 00001400 for KATAR
ME is in reserved state
C9800-L-X-K9 platform with 16777216 Kbytes of main memory
```



CHAPTER 7

License Information

- Evaluation license, on page 51
- View license information, on page 51
- View the Cisco IOS license level, on page 51

Evaluation license

The wireless controller operates on evaluation mode when the device is not registered. The evaluation mode is for 90 days. After the expiry of the evaluation period, if the wireless controller is not registered to a smart account, the wireless controller will start displaying syslog evaluation expiration messages. These error messages are purely for informational purpose only and will not affect the functionality of the wireless controller.

The number of APs supported on the wireless controller when the wireless controller is on EVAL mode will be equal to the capacity of the wireless controller and the wireless controller will be fully operational. No other license is required to use the wireless controller in evaluation mode.

For more information on license information, see *Configure Cisco Wireless Licenses*.

View license information

Use the **show license udi** command to determine the Universal Device Identifier (UDI) information of your chassis. This may be required at the time of purchasing a new license.

This example displays sample output from the **show license udi** command:

```
Device#show license udi
UDI: PID:CW9800L,SN:XXXXXXXXXXX
Device#
```

View the Cisco IOS license level

Use the **show version** command to determine the Cisco IOS license level in the controller.

Example:

```
Device# show version | section License
```

```
licensed under the GNU General Public License ("GPL") Version 2.0.  The
documentation or "License Notice" file accompanying the IOS-XE software,
License Type: Smart License is permanent
License Level: adventerprise
AIR License Level: AIR DNA Advantage
```

Table 9: Show version command output description

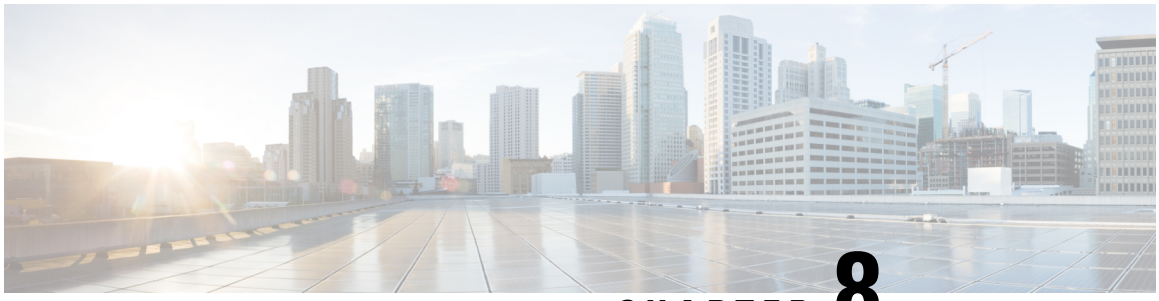
Field name	Description
License Level: adventerprise	Indicates the current Cisco IOS license code level.
License Type: Smart License is permanent	Indicates the type of license that is used. This example shows that the Cisco Smart license is used that provides floating licenses for your user account. Other license types could be: Permanent (purchased) license or an Evaluation 60-day license.
AIR License Level: AIR DNA Advantage	Indicates the AIR network advantage license level.

Use the **show running-config** command or the **show startup-config** command to view the license-level information. This example displays sample output from the **show running-config** command:

```
Device# show running-config
.
.
.
license boot level adventerprise
```

Table 10: show running-config Command Output Description

Field name	Description
license boot level adventerprise	Indicates the current requested Cisco lOS license level to boot.



CHAPTER 8

Factory Reset

- Information About Factory Reset, on page 53
- Prerequisites for Performing Factory Reset, on page 53
- Performing Factory Reset, on page 53

Information About Factory Reset

Factory reset removes all the customer-specific data that has been added to a device since the time of its shipping. The erased data includes configurations, log files, boot variables, core files, and credentials such as Federal Information Processing Standard-related (FIPS-related) keys.

The device returns to its default license configuration after a factory reset.

Note The factory reset is performed through an IOS CLI. A copy of the running image is backed up and restored after the reset.

Prerequisites for Performing Factory Reset

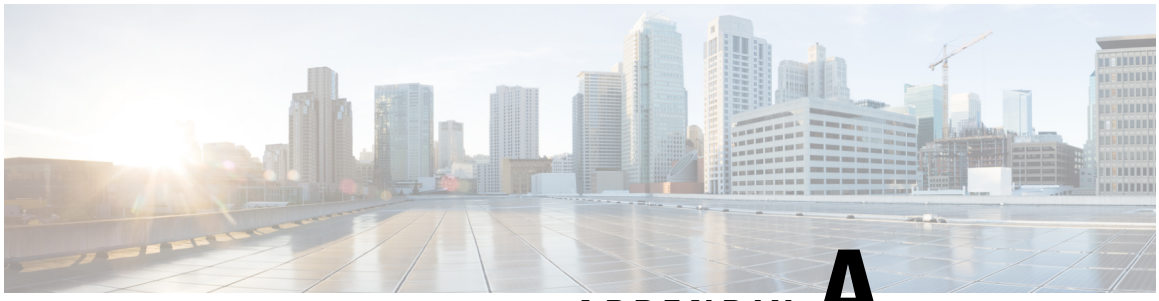
- Ensure that all the software images, configurations, and personal data are backed up.
- Ensure that there is uninterrupted power supply when the factory reset is in progress.
- Ensure that you take a backup of the current image.

Performing Factory Reset

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password, if prompted.
Step 2	**factory-reset all secure 3-pass** **Example:** `Device# factory-reset all secure 3-pass`	Removes sensitive data from all the partitions that are currently being cleaned up by the **factory-reset all** command. From Cisco IOS-XE 17.10 onwards, the following are the three passes to erase data in disk partitions: • Write 0s • Write 1s • Write a random byte **Note** The factory reset takes 3 to 6 hours to be completed.



APPENDIX A

Controller Specifications

This appendix lists the technical specifications for the controller.

- Physical specifications, on page 55
- Environmental specifications , on page 55
- Power specifications, on page 56

Physical specifications

Table 11: Physical specifications

Description	Specification
Width	8.5 in. (215.9 mm)
Depth	9 in. (228.6 mm)
Height	1.73 in. (43.94 mm)
Weight	4.4 lbs (2 kg)

Environmental specifications

Table 12: Environmental specifications

Description	Specification
Storage Temperature	–13° F to 158° F (–25° C to 70° C)
Operating Temperature	32° F to 104° F (0° C to 40° C) **Note** The maximum temperature is derated by 1.0° C for every 1000 ft (305 m) of altitude above sea level.

Description	Specification
Storage Humidity	0% to 95% RH non-condensing
Operating Humidity	5% to 90% RH non-condensing
Operational Altitude	0 to 10,000 ft (3048m) at 30° C

Power specifications

Table 13: AC power supply specifications

Description	Specification
AC input voltage	100 to 240 VAC
Frequency	50 to 60 Hz
Maximum output power	110 W
Adapter	C9800-AC-110W

Table 14: Heat dissipation and power consumption specifications

Description	Specification
Maximum heat dissipation (with 2-ports .3at)	48 W
Maximum power consumption (with 2-ports .3at)	98 W