Cisco Catalyst Wireless 9163E Access Point Hardware Installation and Deployment Guide

First Published: 2024-01-19

Last Modified: 2024-03-21

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.

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 3

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

This guide provides instructions to install your Cisco Access Point and provides links to resources that can help you configure it. This guide also provides mounting instructions and troubleshooting information.

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

All user documentation for the Cisco Catalyst 9163E Series Access Points is available at the following URL:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9163e-access-point/model.html

For detailed information and guidelines for configuring and deploying your access point in a wireless network, see the following documentation:

- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, at the following URL:

  https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html

- Video Series: Best Practices for Installing Outdoor Wireless Access Points at the following URL:

  https://www.cisco.com/go/ap-best-practices-videos

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

CHAPTER 1

About Cisco Catalyst Wireless 9163E Access Point

Introduction to Cisco Catalyst Wireless 9163E Access Point

Cisco Catalyst Wireless 9163E Access Point is a Wi-Fi 6E technology-based 2x2 tri-band outdoor enterprise-class 802.11ax access point. The AP supports full interoperability with leading 802.11ax and 802.11ac clients and a hybrid deployment with other APs and controllers.

The AP hardware is supported on the following platforms:

- Cisco Catalyst Center (formerly Cisco DNA Center) on-premises
- Cisco Catalyst stack
- Meraki cloud-based stack

The Cisco Catalyst Wireless 9163E Access Point data sheet provides a full listing of the AP's features and specifications at:

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9163e-access-point/nb-06-cat-9163e-series-access-ds-cte-en.html

Supported Wireless Controller Platforms

The following Cisco Catalyst 9800 Wireless Controllers with Cisco IOS XE 17.12.3 or a later release software supports Cisco Catalyst Wireless 9163E Access Points:

- Cisco Catalyst 9800-80
- Cisco Catalyst 9800-40
- Cisco Catalyst 9800-L
- Cisco Catalyst 9800-CL

Note This AP model does not support the Cisco Embedded Wireless Controller as an active EWC or a subordinate AP.

Cisco Catalyst Wireless 9163E Access Point Features

Cisco Catalyst 9800 wireless controller-based products support Cisco Catalyst Wireless 9163E Access Points. The following are the key features of the AP:

Hardware:

- 2x2 Triple–Band Triple–Concurrent radio—2.4-GHz, 5-GHz, and 6-GHz radios
- 1x1 Tri-Band scanning radio
- Integrated GNSS receiver
- External GNSS port
- Integrated Bluetooth Low Energy (BLE) radio enables IoT use cases like location tracking and wayfinding.
- The AP has the following external interfaces:
    - 1x100/1000/2500 Multigigabit Ethernet (PoE-IN)
    - Recovery push button
    - One multicolor LED status indicator. For information about the colors of the LED status indicator, see Checking the Access Point LEDs, on page 42.

Software:

- The scanning radio can perform advanced radio frequency (RF) spectrum analysis, and deliver features such as next-generation CleanAirPro, Wireless Intrusion Prevention System (WIPS), and Dynamic Frequency Selection (DFS) detection.
- Cisco CleanAir Pro technology enhanced with 160-MHz channel support. CleanAir Pro delivers proactive, high-speed spectrum intelligence across 20, 40, 80, and 160-MHz-wide channels to combat performance issues from wireless interference.
- MU-MIMO technology for uplink and downlink.
- OFDMA-based scheduling for both uplink and downlink.
- A new power savings mode called Target Wake Time (TWT) allows clients to stay asleep and wake up only at prescheduled (target) times to exchange data with the AP. This mode provides significant energy savings for battery-operated devices.
- Cisco Catalyst Center support enables Cisco Spaces, Apple FastLane, Cisco Identity Services Engine (ISE), and Meraki Health intelligent optimization and assurance.
- Optimized AP Roaming to ensure client devices associate with the AP in their coverage range, offering the fastest data rate available.

- Spatial Reuse (also known as Basic Service Set [BSS] coloring) allows the AP and their clients to differentiate between BSS, thus permitting simultaneous transmissions.
- Intelligent Capture probes the network and gives Cisco Catalyst Center in-depth analysis.

The AP supports the following operational modes:

Table 1: Access Point Supported Operational Modes

Mode	Information
Local mode	This is the default mode for the AP. In this mode, the AP serves clients. In local mode, the AP creates two CAPWAP tunnels for the controller, one for management and the other for data traffic. This is known as central switching because the data traffic is switched (bridged) from the AP to the controller.
Cisco FlexConnect mode	In FlexConnect mode, the data traffic is switched locally and is not sent to the controller. In this mode, the AP behaves like an autonomous AP, but is managed by the controller. Here, the AP continues to function even if the connection to the controller is lost.
Monitor mode	In the monitor mode, the AP is excluded from handling data traffic between clients and infrastructure. The AP acts as a dedicated sensor for location-based services (LBS), rogue AP detection, and Intrusion Detection System (IDS). When the AP is in monitor mode, it actively monitors the airwaves and typically does not serve clients.
Sniffer mode	In the wireless sniffer mode, the AP starts sniffing the air on a given channel. It captures and forwards all the clients' packets on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). This includes information about the time stamp, signal strength, packet size, and so on. **Note** In the sniffer mode, the server where the data is sent and the controller management VLAN must reside on the same VLAN. Otherwise, an error is displayed.

AP Model Numbers and Regulatory Domains

Table 2: AP Model Numbers and Regulatory Domains

AP Type	Model Number	Details
AP for outdoor environments, with external antennas	CW9163E-A CW9163E-B CW9163E-E CW9163E-F CW9163E-I CW9163E-Q CW9163E-R CW9163E-Z CW9163E-ROW CW9163E-MR	The AP has four external antenna ports, an external GNSS port and an internal GNSS antenna. This is a stand-alone unit that can be wall or pole mounted.

Note Using the AP's 6 GHz spectrum outdoors requires the Automatic Frequency Coordination (AFC) feature. The AFC feature provides permitted power levels and frequencies for outdoor Wi-Fi 6E APs at the installed location.

You must verify whether the AP model you have is approved for use in your country. To verify approval and to identify the regulatory domain that corresponds to a particular country, see http://www.cisco.com/go/aironet/compliance. Not all regulatory domains have been approved. As and when they are approved, the compliance list is updated.

Antennas and Radios

The CW9163E-x AP model has four N-type antenna ports supporting self-identifying antennas (SIA), and a GNSS antenna supporting SubMiniature version A (SMA) male port.

- CW-ANT-O1-NS-00: These are omnidirectional antennas recommended for 360-degree radio coverage.
- CW-ANT-D1-NS-00: This is a wide-beam directional antenna.
- CW-ANT-GPS2-S-00: An L1/L5 band GNSS optimizing antenna to enhance location precision for Standard Power AFC requirements.

For more information about the supported antennas and the radio bands they operate at, see the Supported External Antennas section.

CHAPTER 2

Hardware Features

This section describes the hardware features of the CW9163E-x models:

- Access Point Views, Ports, and Connectors, on page 5
- Supported External Antennas, on page 7
- Power Sources, on page 9

Access Point Views, Ports, and Connectors

Cisco Catalyst Wireless 9163E Series Outdoor AP has various externally accessible ports and connectors that you can use to install antennas on the AP. For information about connectors and ports for this AP, see Connectors and Ports on the AP, on page 5.

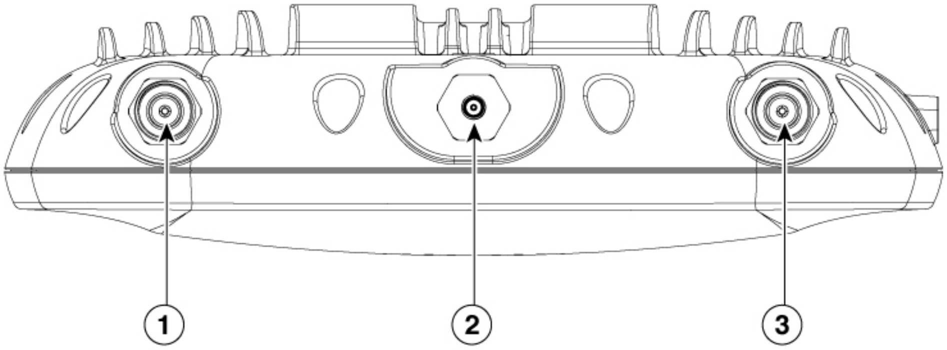
Note The illustrations in this document show all the available connections for the AP. The connector plugs seal the unused connection ports to ensure that the AP is watertight. Liquid-tight adapters are provided for connector openings. You can install the adapters before or after deploying the AP.

Connectors and Ports on the AP

The following illustrations show the different connectors and ports available on the base and sides of the AP.

Connectors and Ports on the Top

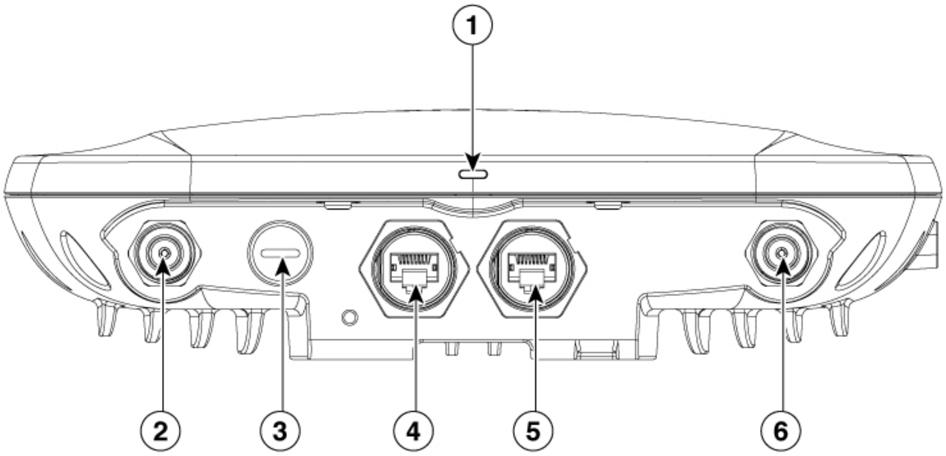
Figure 1: CW9163E Top Connectors and Ports



1	Port A This port supports 6-GHz + SIA. Yellow band	3	Port B This port supports a 6-GHz antenna only. Clear band
2	SMA connector port This port connects to the GNSS antenna only.		

Connectors and Ports on the Base

Figure 2: CW9163E Base Connectors and Ports

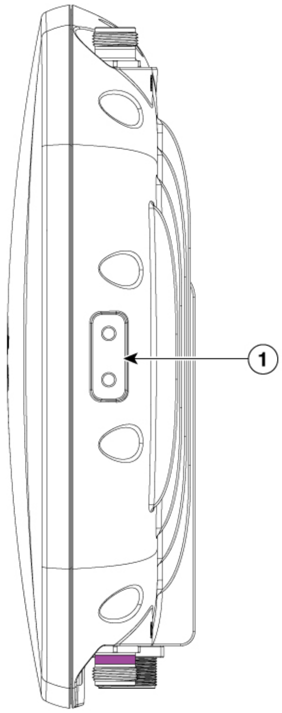


1	LED	4	Console Port If the port is not used, do not remove the covering plug. Otherwise, it might lead to water leaking into the AP.

2 🟧	Port C 2.4-GHz and 5-GHz antenna Orange band	5 2.5G	2.5G mGig PD (PoE-IN) Ethernet port If the port is not used, do not remove the covering plug. Otherwise, it might lead to water leaking into the AP.
3 ⟲	Reset button (covered with a cap)	6 🟪	Port D 2.4-GHz and 5-GHz + SIA antenna Purple band

Connectors and Ports on the Sides

Figure 3: Right–Side Connectors



1 ⏚	Grounding Pad

Supported External Antennas

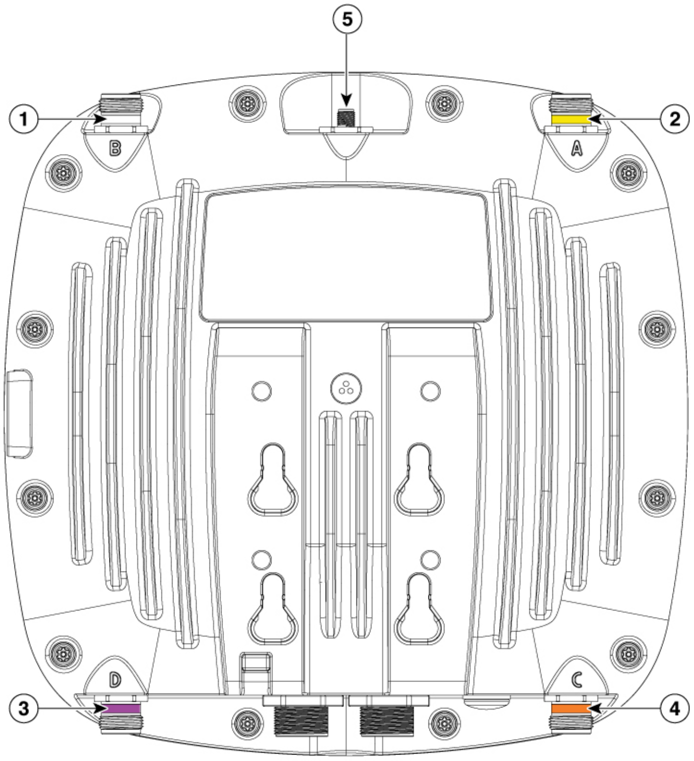
The CW9163E AP supports a combination of 2.4-GHz, 5-GHz, and 6-GHz SIA, depending on the port they are installed on.

The supported Cisco Antennas are:

- CW-ANT-O1-NS-00
- CW-ANT-D1-NS-00
- CW-ANT-GPS2-S-00

Note The AP operates with supported Cisco antennas only on all ports.

The following table lists the CW9163E AP supporting external antennas:



1 🟦	Port B Supports 6-GHz band	4 🟧	Port C Supports 2.4-GHz and 5-GHz bands
2 🟨	Port A Supports 6-GHz band, SIA	5	Port 5 L1/L5 Band
3 🟪	Port D Supports 2.4-GHz and 5-GHz bands, SIA		

Table 3: CW9163E Access Point Supported 6-GHz External Antennas

PID	2.4–GHz Antenna Gain (dBi)	5–GHz Antenna Gain (dBi)	6–GHz Antenna Gain (dBi)	Antenna Type
CW-ANT-O1-NS-00	4	8	8	Direct Attach Omni Directional Antenna, Tri-band
CW-ANT-D1-NS-00	8	9	9	Wall or Pole Attach Wide-beam Directional Antenna, Tri-band

Table 4: CW9163E Access Point Supported External Antennas

PID	Antenna Gain (dBi)	Antenna Type
CW-ANT-GPS2-S-00	2	Wall or Pole Attach, AFC compliant, GNSS Antenna with 10-ft. integrated cable

For installation instructions and detailed information on any of these antennas, refer to the antenna guide at:

http://www.cisco.com/c/en/us/support/wireless/aironet-antennas-accessories/products-installation-guides-list.html

Use of Non-Cisco Antennas

RF connectivity and compliance of third-party antennas is the user’s responsibility. Cisco does not recommend any third-party antennas, and the Cisco Technical Assistance Center will not be able to provide any support for third-party antennas. Cisco’s FCC Part 15 compliance is only guaranteed with Cisco antennas or antennas that are of the same design and gain as Cisco antennas.

Power Sources

You can power the CW9163E AP with Power over Ethernet (PoE) and select power injectors. For more information, see Powering the Access Point, on page 28.

Warning **Statement 1033—**Safety Extra-Low Voltage (SELV)—IEC 60950/ES1–IEC 62368 DC Power Supply

To reduce the risk of electric shock, connect the unit to a DC power source that complies with the SELV requirements in IEC 60950-based safety standards or ES1 and PS1 requirements in IEC 62368-based safety standards or to a Class 2 power supply.

Caution For PoE options and their corresponding modes of operation, see Table 9: Cisco Catalyst Wireless 9163E AP Reduced Power Feature Matrix, on page 29.

Caution When the AP is installed outdoors or in a wet or damp location, the AC branch circuit powering the AP should be provided with ground fault protection (GFCI), as required by Article 210 of the National Electrical Code (NEC).

Power Injectors

CW9163E AP supports the following power injector models:

- AIR-PWRINJ7=
- AIR-PWRINJ6=
- IW-PWRINJ-60RGDMG=
- MA-INJ-6
- MA-INJ-4

Note The MA-INJ-4 power injector is at the End of Life (EOL) stage. Customers who already own these injectors may continue to use them with CW9163E AP.

Caution When the AP is installed outdoors or in a wet or damp location, the AC branch circuit powering the AP should be provided with ground fault protection (GFCI), as required by Article 210 of the National Electrical Code (NEC).

Ethernet (PoE) Ports

The AP supports an Ethernet uplink port (also for PoE-In). The Ethernet uplink port on the AP uses an RJ-45 connector (with weatherproofing) to link the AP to the 100BASE-T, 1000BASE-T, or 2.5GBASE-T network. The Ethernet cable is used to send and receive Ethernet data and optionally supply inline power from the power injector or a suitably powered switch port.

Tip The AP senses the Ethernet and power signals and automatically switches internal circuitry to match the cable connections.

The Ethernet cable must be a *shielded*, outdoor rated, Category 5e (CAT 5e) or better cable. The AP senses the Ethernet and power signals and automatically switches internal circuitry to match the cable connections.

CHAPTER 3

Installing the Access Point

Installing an AP involves the following high-level tasks:

- Unpacking the Package, on page 11
- Preparing the AP for Installation, on page 15
- Performing a Preinstallation Configuration (Optional), on page 16
- Mounting the Access Point, on page 18

Unpacking the Package

Package Contents

Each AP package contains the following items:

- One CW9163E Outdoor AP
- Ground lug and screws with lock washers
- MA-MNT-MR-16 mounting plate
- CAT 6/6A RJ45 Ethernet port termination plug
- Anticorrosion sealant
- Mounting straps
- Cisco product documentation and pointer card

Unpacking the Access Point

To unpack the AP, follow these steps:

Procedure

Step 1 Unpack and remove the AP and the accessory kit from the shipping box.

Step 2 Return the packing material to the shipping container and save it for future use.

Step 3 Verify that you have received the following items:

- The access point
- Accessory kit (Ethernet port termination plug, ground lug kit)
- MA-MNT-MR-16 Mounting bracket
- CW-ACC-KIT1-00 accessory kit, only if you have ordered this optional accessory kit along with the AP.

If any item is missing or damaged, contact your Cisco representative or reseller for instructions.

Optional Tools and Hardware from Cisco

Depending on what you ordered, the following optional equipment may be part of your shipment:

- Cisco Orderable Accessories, on page 12
- Spare part kit containing extra cable glands, power connector, ground lug, and so on. (CW-ACC-KIT1-00)

Additional Tools and Hardware Required for Installation

You must independently procure the following tools and materials, which might be required during the various stages of installing the AP:

- Ground lug crimping tool (Panduit CT-720 with CD-720-1 die)
- #2 Phillips Screwdriver
- 5–mm Hex driver or Allen wrench
- Adjustable wrench or 28–mm box wrench
- 6-AWG copper ground wire
- 10–mm open-end or box wrench
- 13–mm box-end wrench or socket set
- 16–mm box-end wrench or socket set
- CAT6/6A cable of 0.2 to 0.35 inch (5 to 9 mm) diameter
- Ethernet RJ-45 connector and installation tool
- Ground rod, as required by local regulations

Cisco Orderable Accessories

Order the following accessories separately from Cisco:

- AP-mounting brackets to mount the CW9163E AP.

Mounting Brackets	Description
AIR-MNT-VERT1	Vertical mount to a wall or 2 to 5 inch (51 to 127 mm) diameter pole
MA-MNT-MR-16	Vertical mount to a wall or 2.5 to 3.9 inch (63.5 to 99.06 mm) diameter pole

- Accessory kits

Accessory Kit	Description
CW-ACC-KIT1-00	This kit contains the following items: • Ground lug (Qty: 1) • Grounding screws (Qty: 2) • CAT 6/6A Ethernet port plug and gland assembly (Qty: 5) • GNSS antenna cap (Qty: 1) • RJ45 port dust cap (Qty: 2) • Reset port cap (Qty: 2) • Waterproof N-type antenna caps (Qty: 4)
AIR-ACC245LA-N=	Lightning Arrestor kit

- Supported power injectors.

Power Source	Description
AIR-PWRINJ6=	30 W rated single-port PoE injector
AIR-PWRINJ7=	65 W rated single-port PoE injector (802.3bt), mGig Ethernet
IW-PWRINJ-60RGDMG=	37 W rated power injector
MA-INJ-4	30 W rated single-port PoE injector **Note** This power injector is in End of Life (EoL) stage.
MA-INJ-6	60 W rated PoE injector (802.3bt), mGig Ethernet

Preinstallation Checks and Installation Guidelines

Because the AP is a radio device, it is susceptible to common causes of interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

- Thoroughly review the information provided in Installing the Access Point, on page 11.
- Install the AP in an area where structures, trees, or hills do not obstruct radio signals to and from the AP.

- We recommend that you install the AP no higher than 40 feet to support the wireless clients on the ground. Mounting all the APs at the same height provides the best throughput.

Note To calculate path loss and determine how far apart to install the APs, consult an RF planning expert.

Before you begin the installation process, ensure the following:

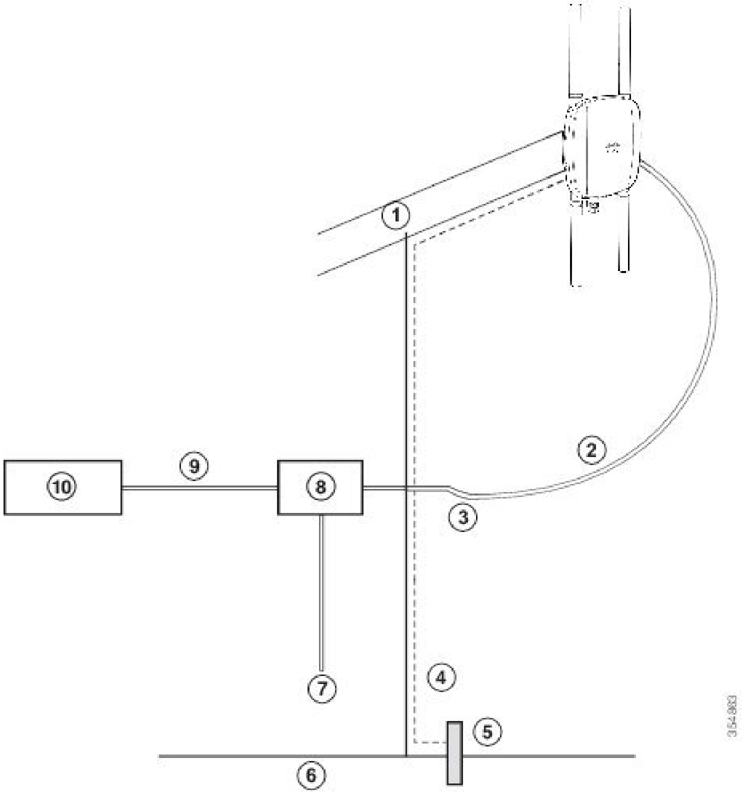
- Perform a site survey. For more information, see Performing Site Surveys, on page 62.
- Your network infrastructure devices must be operational and properly configured.
- Your controllers must be connected to switch trunk ports.
- Your switch must be configured with untagged access ports for connecting your APs.
- A DHCP server configured with Option 43 must be reachable by your AP, or the controller information must be manually configured in the AP. For information about configuring DHCP Option 43, see http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html
- Become familiar with the AP installation components. See Typical Access Point Installation Components, on page 14.
- Familiarize yourself with the best practices video series to install the Cisco outdoor wireless access points. See

  https://www.cisco.com/c/en/us/td/docs/wireless/access_point/outdoor/video/ap-best-practices.html

Typical Access Point Installation Components

The Cisco Catalyst Wireless 9163E Series Outdoor is designed to be installed in an outdoor environment, such as the exterior roof overhang of a tall building or a streetlight pole. Carefully review the Figure 4: Components in a Typical Access Point Installation, on page 15 to become familiar with the system components, connectors, indicators, cables, system interconnection, and grounding.

Figure 4: Components in a Typical Access Point Installation



1	Building roof overhang	6	Ground
2	Shielded outdoor-rated Ethernet (CAT6 or better) cable[1]	7	Power cord
3	Water drip loop	8	Power injector
4	6-AWG copper grounding wire [1]	9	Shielded Ethernet (CAT6 or better) cable[1]
5	Ground rod[1]	10	Controller (through a switch)

[1] Independently sourced by the user.

Preparing the AP for Installation

Before you mount and deploy the AP, we recommend that you perform a site survey (or use the site planning tool) to determine the best location to install your AP.

You should have the following information about your wireless network on hand:

- AP locations
- AP-mounting options: To a vertical wall or pole

Note The AP can be mounted in various orientations. Depending on the orientation, you may have to purchase additional mounting hardware. For more information, see the Mounting the Access Point, on page 18 section.

- AP power options: 802.3at (PoE+), 802.3af (PoE), and 802.3bt
- Operating temperature:
  - Without solar derating: -40° to 149℉ (-40° to 65℃) and 131℉ (55℃)
  - With solar derating: -40° to 131℉ (-40° to 55℃) and 131℉ (55℃)
- Console access using the console port

  We recommend that you use a console cable that is one meter or less in length.

  Note The AP may face issues while booting if you use an unterminated console cable (not plugged into any device or terminal) or a console cable that is more than one meter in length.

We recommend that you prepare a site map showing AP locations so that you can record the device MAC addresses from each location and return them to the person who is planning or managing your wireless network.

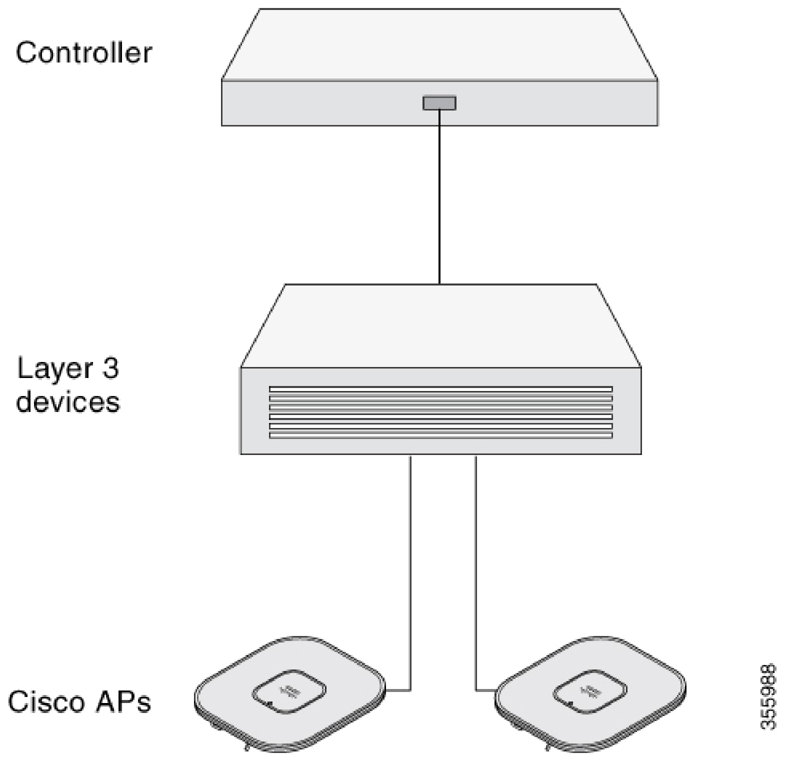
Performing a Preinstallation Configuration (Optional)

Performing the following procedures ensures that the AP installation and the initial operation proceed as expected. This procedure is optional.

Note If your controller is configured properly, you can install the AP in its final location and connect it to the network from there. For additional information, see Deploying the Access Point in a Wireless Network, on page 42.

The preinstallation configuration setup is illustrated in Figure 5: Preinstallation Configuration Setup, on page 17:

Figure 5: Preinstallation Configuration Setup



To perform preinstallation configuration, follow these steps:

Procedure

Step 1 Ensure that the Cisco Controller Distribution System port is connected to the network. Use the procedure for the CLI or the GUI interface, as described in the release-appropriate *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

a) Ensure that the AP has Layer 3 connectivity to the Cisco Controller Management and AP-Manager interfaces.

b) Configure the switch to which the AP should be attached. See the release-specific *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide* for the release your controller is running on.

c) Set the controller as the primary controller so that the new AP always joins it.

d) Ensure that you have enabled DHCP on the network.

The AP must receive its IP address through DHCP.

Note The DHCP server assigns an IP address to an 802.11AX Cisco AP only if a default router (gateway) is configured on the DHCP server (enabling the AP to receive its gateway IP address) and the gateway ARP is resolved.

e) Ensure that the network is configured not to block the CAPWAP UDP ports.

f) The AP must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address.

For other methods, refer to the product documentation. For more information, see Configuring DHCP Option 43, on page 57.

Note The AP requires a Gigabit Ethernet (GbE) link to prevent the Ethernet port from becoming a bottleneck for traffic because wireless traffic speeds exceed the transmit speeds of a 10/100 Ethernet port.

Step 2 Apply power to the AP.

a) When the AP attempts to connect to the controller, the LED cycles through an off, green, and red sequence, taking up to five minutes.

Note If the AP remains in this mode for more than five minutes, the AP is unable to find the primary controller. Check the connection between the AP and the primary controller and ensure they are on the same subnet.

b) If the AP shuts down, check the power source.

c) After the AP finds the primary controller, it attempts to download the software image if the AP software release differs from the controller release version. While this is happening, the status LED blinks blue.

d) If the software image download is successful, the AP reboots.

Step 3 Configure the AP 802.11AX network settings using the controller CLI, controller GUI, or Cisco Catalyst Center.

Step 4 If the preinstallation configuration is successful, the status LED is green, indicating normal operation.

Disconnect the AP and mount it at the location you intend to deploy it on the wireless network.

Step 5 If the AP does not indicate normal operation, turn it off and repeat the preinstallation configuration.

Note When you are installing a Layer 3 AP on a different subnet than the controller, ensure the following:

- Ensure that a DHCP server is reachable from the subnet on which you want to install the AP.
- The subnet has a route back to the controller, and ensure that the route back to the controller has the destination UDP ports 5246 and 5247 open for CAPWAP communications.
- Ensure that the route back to the primary, secondary, and tertiary controllers allows IP packet fragments.
- Ensure that the AP and the controller have a static 1-to-1 NAT to an outside address if address translation is used. (Port Address Translation is not supported.).

Mounting the Access Point

This section provides instructions to mount the AP. Personnel mounting the AP must have knowledge of the wireless AP, bridging techniques, and grounding methods.

Choosing a Mounting Kit

Access Point Mounting Kit

You can mount the AP vertically to a wall or a pole that best fits the installation application.

AP Mounting Kit[2]	Purpose
MA-MNT-MR-16	Fixed mounting kit for vertical mounting on a wall or for pole of diameter 2.5 to 3.9 inch (63.5 to 99.06 mm). See: Wall Mounting the AP using the Meraki Kit, on page 20 Pole Mounting the AP using the Meraki Kit, on page 22
AIR-MNT-VERT1=	Fixed mounting kit for vertical mounting on a wall or for pole of diameter 2 to 3.9 inch (51 to 99.06 mm). See: Wall Mounting the AP using the Cisco Kit, on page 23 Pole Mounting the AP using the Cisco Kit, on page 26

[2] Mount the AP using no less than four screw holes on a bracket.

Note

- When mounting an AP vertically, ensure that the AP is oriented with the LED indicators pointing down.
- Mount the AP in such a way that all antenna ports and the console port are visible and accessible for future use.

Mounting Antenna

The procedure to install the supported antenna to the AP.

Antenna	Purpose
CW-ANT-O1-NS-00	Installing the Omnidirectional Antenna, on page 32
CW-ANT-D1-NS-00	Wall Mounting the CW-ANT-D1-NS-00 Antenna Pole Mounting the CW-ANT-D1-NS-00 Antenna
CW-ANT-GPS2-S-00	Mounting kit to install the GNSS antenna on a wall or pole of diameter 2.5 to 3.9 inch (63.5 to 99.06 mm). See: Wall Mounting the GNSS Antenna, on page 33 Pole Mounting the GNSS Antenna, on page 34

Note

- Align the AP's omnidirectional antennas vertical to the ground.
- Align the AP's directional antenna such that the main beam is parallel to or tilted down toward the horizon.

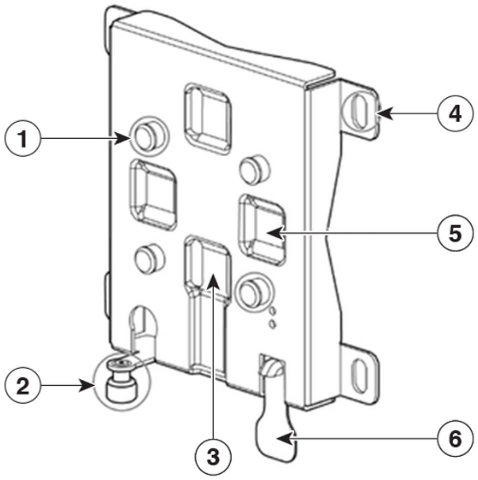
Wall Mounting the AP using the Meraki Kit

The MA-MNT-MR-16 mounting kit contains a mounting bracket for wall mounting or pole mounting.

You can use the mounting bracket as a template to mark the mounting holes' positions for your installation, install the mounting bracket, and then attach the AP to the bracket.

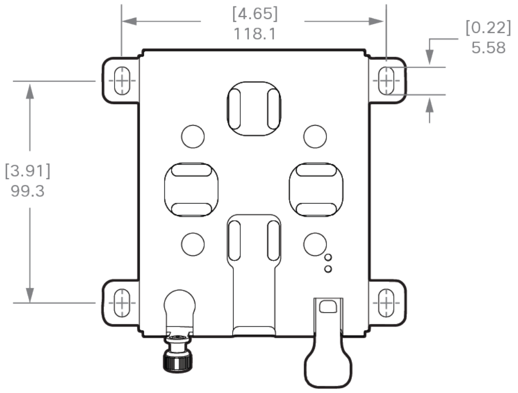
Caution The mounting wall, attaching screws, and wall anchors must support a 50-lb (22.7–kg) static weight.

Figure 6: Mounting Bracket for Wall and Pole Mounting



1	One of four keyhole lugs to mount the AP	4	Bracket mount holes for fastening the bracket to the wall
2	Mount plate security screw	5	One of four slots for steel band clamps, used for pole mounting (horizontal)
3	One of four slots for steel band clamps, used for pole mounting (vertical)	6	AP release tab

Figure 7: Mounting Bracket Dimensions



Before you begin

Ensure that you have the following materials before beginning to mount the AP to a wall:

Table 5: Material Required to Mount Access Point to a Wall using MA-MNT-MR-16 Kit

Materials Required	Supplied in the Kit?
Wall Mount Bracket	Yes
Ground lug and screws (provided with the access point)	Yes
Crimping tool for ground lug, Panduit CT-720 with CD-720-1 die	No
Four wall mounting screws	No
Four wall anchors (specified for all material)	No
Drill bit for wall anchors	No
Electric drill and standard screwdriver	No
#6 AWG ground wire	No
Shielded outdoor-rated Ethernet (CAT6 or better) cable	No
Grounding block	No
Grounding rod	No
10–mm box-end wrench or socket set	No

Procedure

Step 1 Use the mounting bracket as a template to mark four screw-hole locations on the mounting wall.

Step 2 Use four screws and, if required, wall anchors to attach the mounting plate to the mounting surface. These screws and anchors are to be sourced independently.

Note
- You can use an exterior-grade plywood backboard to mount the AP to stucco, cement, or drywall.
- The mounting wall, attaching screws, and wall anchors must support a 50-lb (22.7 kg) static weight.

Step 3 Slide and align the AP mounting holes against the mounting bracket such that the four keyhole lugs on the mounting bracket are inserted into the keyhole slots on the AP.

An audible click confirms that the AP is securely locked to the mounting bracket.

Note The AP should be mounted with the status LED on the base facing downwards.

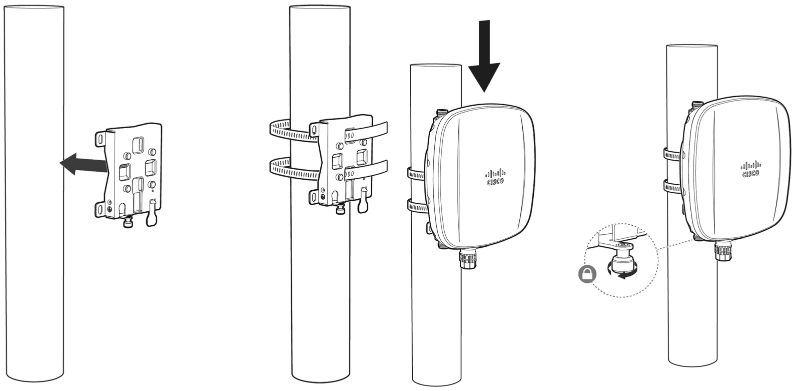
Step 4 Tighten the mounting plate security screw.

Step 5 Proceed with installing antennas, connecting the data cables, grounding the AP, powering, and configuring the AP.

Pole Mounting the AP using the Meraki Kit

The MA-MNT-MR-16 mounting kit contains a mounting bracket used for wall mounting and pole mounting. This kit can be used to install the AP on a pole or mast. It supports metal, wood, or fiberglass poles of 2.5 to 3.9 inch (63.5 to 99.06 mm) in diameter.

Figure 8: AP Mounted on a Pole



Before you begin

Ensure that you have the following materials before beginning to mount the AP to a pole:

Table 6: Materials Needed to Mount the AP on a Vertical Pole using MA-MNT-MR-16 Kit

Materials Required	Supplied in the Kit?
One wall mount bracket	Yes

Materials Required	Supplied in the Kit?
Two stainless steel band clamps (adjustable to 2.5 to 3.9 inch (63.5 to 99.06 mm).	Yes
10–mm box-end wrench	No
A flathead screwdriver	No
Outdoor-rated shielded Ethernet cable	No
Ground lug (provided with the access point)	Yes
Ground block and rod	No
Crimping tool for ground lug, Panduit CT-720 with CD-720-1 die	No
#6 AWG ground wire	No

Procedure

Step 1 Select a mounting location on the pole to mount the AP.

You can attach the AP to a pole having a diameter of 2.5 to 3.9 inch (63.5 to 99.06 mm).

Step 2 Hold the bracket up against the pole and slide the two band straps through the top and bottom sets of mounting slots on the mounting bracket.

Step 3 Wrap the band straps around the pole and lock them.

Lightly tighten the clamps using a 10 mm wrench or Phillips head screwdriver. Only tighten them enough to keep the bracket from sliding down the pole.

Step 4 Align the AP mounting holes against the mounting bracket such that the keyhole slots on the back of the AP are inserted into the keyhole lugs on the mounting bracket.

Ensure that the AP is seated correctly on the keyhole lugs. An audible click confirms that the AP is securely locked to the mounting bracket.

Note The AP should be mounted with the status LED on the base facing downwards.

Step 5 Place the AP in its final position.

Tighten the band clamps with the wrench or a screwdriver so that the AP does not slide on the pole. Ensure that the clamps are tight enough not to let the AP move.

Step 6 Tighten the mount plate security screw.

Step 7 Proceed with installing antennas, connecting the data cables, grounding the AP, powering, and configuring the AP.

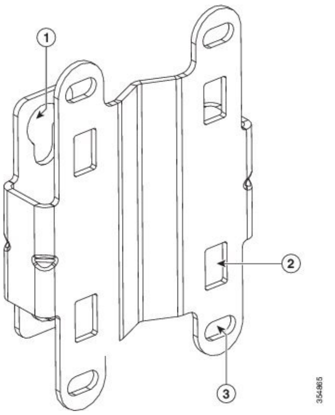
Wall Mounting the AP using the Cisco Kit

The AIR-MNT-VERT1= mounting kit contains a mounting bracket for wall mounting or pole mounting.

You can use the mounting bracket as a template to mark the mounting holes' positions for your installation, install the mounting bracket, and then attach the AP to the bracket.

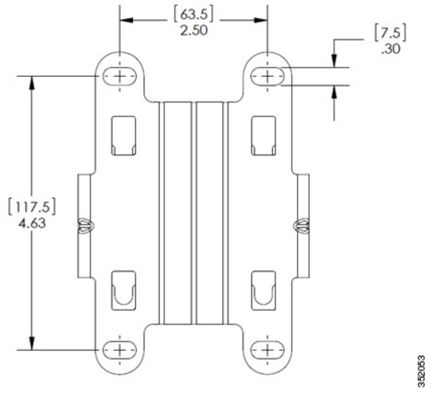
Caution The mounting wall, attaching screws, and wall anchors must support a 50-lb (22.7–kg) static weight.

Figure 9: Mounting Bracket for Wall and Pole Mounting



1	One of four keyhole slots to mount the AP.
2	One of four slots for steel band clamps is used for pole mounting only.
3	Bracket mount holes are used to fasten the bracket to the wall. You can use bolts of up to 1/4” or 6 mm in diameter.

Figure 10: Mounting Bracket Dimensions



Before you begin

Ensure that you have the following materials before beginning to mount the AP to a wall:

Table 7: Material Required to Mount Access Point to a Wall using AIR-MNT-VERT1= Kit

Materials Required	Supplied in the Kit?
Ground lug and screws (provided with the access point)	Yes
Wall Mount Bracket	Optional, Cisco orderable accessory
Four M6 x 12–mm Hex-head Bolts	Yes
Crimping tool for ground lug, Panduit CT-720 with CD-720-1 die	No
Four wall mounting screws	No
Four wall anchors (specified for all material)	No
Drill bit for wall anchors	No
Electric drill and standard screwdriver	No
#6 AWG ground wire	No
Shielded outdoor-rated Ethernet (CAT6 or better) cable	No
Grounding block	No
Grounding rod	No
10–mm box-end wrench or socket set	No

Procedure

Step 1 Use the mounting bracket as a template to mark four screw-hole locations on the mounting wall. The mounting bracket screw hole locations are shown in Figure 9: Mounting Bracket for Wall and Pole Mounting, on page 24. The dimensions of the mounting bracket are shown in Figure 10: Mounting Bracket Dimensions, on page 24.

Step 2 Use four screws and, if required, wall anchors to attach the mounting plate to the mounting surface. These screws and anchors are to be sourced independently.

Note
- You can use an exterior-grade plywood backboard to mount the AP to stucco, cement, or drywall.
- The mounting wall, attaching screws, and wall anchors must support a 50-lb (22.7 kg) static weight.

Step 3 Screw an M6 x12–mm bolt into each of the four support bolt holes on the back of the AP. Do not screw the bolt all the way in, but leave a gap of approximately 0.13 inch (3.3 mm).

Step 4 Position the AP against the mounting bracket such that the four support bolts on the back of the AP slot are inserted into the keyhole slots on the mounting bracket.

Step 5 Slide the AP down to sit securely in the keyhole slots on the mounting bracket.

An audible click confirms that the AP is securely locked to the mounting bracket.

Note The AP should be mounted with the status LED on the base facing downwards.

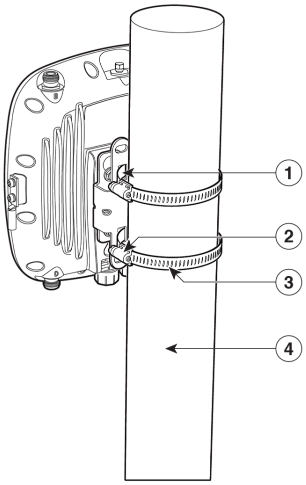
Step 6 Using a 10–mm wrench, tighten the four bolts that connect the AP to the bracket to 40 lbf-in (4.5 Nm) of torque.

Step 7 Proceed with installing antennas, connecting the data cables, grounding the AP, powering, and configuring the AP.

Pole Mounting the AP using the Cisco Kit

The AIR-MNT-VERT1= mounting kit contains a mounting bracket used for both wall mounting and pole mounting. This kit can be used to install the AP on a pole or mast. It supports metal, wood, or fiberglass poles of 2 to 3.9 inch (51 to 99.06 mm) in diameter.

Figure 11: AP Mounted on a Pole



1	One of four M6 keyhole slots for mounting the AP on the bracket.
2	Top and bottom sets of band clamp slots for passing the clamps through.
3	Top and bottom steel band clamps
4	Pole (wood, metal, or fiberglass), 2 to 3.9 inch (51 to 99.06 mm) diameter

Before you begin

Ensure that you have the following materials before beginning to mount the AP to a pole:

Table 8: Materials Needed to Mount the AP on a Vertical Pole using AIR-MNT-VERT1= Kit

Materials Required	Supplied in the Kit?
One wall mount bracket	Optional Cisco orderable accessory
Four M6 x12 mm hex head bolts	Yes

Materials Required	Supplied in the Kit?
Two stainless steel band clamps (adjustable 2 to 3.9 inch (51 to 99.06 mm)	Yes
10–mm box-end wrench	No
Outdoor-rated shielded Ethernet cable	No
Ground lug (provided with the access point)	Yes
Ground block and rod	No
Crimping tool for ground lug, Panduit CT-720 with CD-720-1 die	No
#6 AWG ground wire	No

Procedure

Step 1 Select a mounting location on the pole to mount the AP. You can attach the AP to a pole having a diameter of 2.5 to 3.9 inch (63.5 to 99.06 mm).

Step 2 Hold the bracket up against the pole and slide the two band straps through the top and bottom sets of mounting slots on the mounting bracket.

Step 3 Wrap the band straps around the pole, lock them, and then lightly tighten the clamps using a 10 mm wrench or Phillips head screwdriver. Only tighten them enough to keep the bracket from sliding down the pole.

Step 4 Screw an M6 bolt into each of the four bolt holes on the backside of the AP. Do not screw the bolt in all the way. Leave a gap of about 0.13 inch (3.3 mm).

Step 5 Position the four bolts on the AP into the bracket keyhole slots.

Ensure that the AP is seated correctly in the slots. An audible click confirms that the AP is securely locked to the mounting bracket.

Note The AP should be mounted with the status LED on the base facing downwards.

Step 6 Using a 10–mm wrench, tighten the four bolts that connect the AP to the bracket to 40 lbf-in (4.5 Nm) of torque.

Step 7 Place the AP in its final position. Tighten the band clamps with the wrench or the screwdriver so that the AP does not slide on the pole. Ensure that the clamps are tight enough not to let the AP move.

Step 8 Proceed with installing antennas, connecting the data cables, grounding the AP, powering, and configuring the AP.

Grounding the Access Point

The AP must be grounded before connecting power.

In all outdoor installations, you must follow these steps to ground the case properly:

Procedure

Step 1 If using insulated 6-AWG copper ground wire, strip the insulation required for the grounding lug.

Step 2 Use the appropriate crimping tool to crimp the bare 6-AWG copper ground wire to the supplied grounding lug.

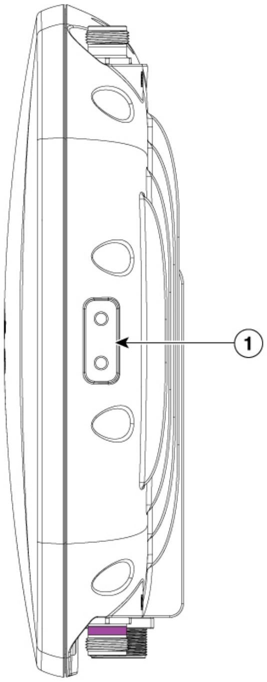
Note The grounding lug and hardware used must comply with local and national electrical codes.

Step 3 Open the anti-corrosion sealant (supplied) and apply a liberal amount over the metal surface called the Ground Pad, where the ground strap screw holes are located.

Step 4 Connect the grounding lug to the AP grounding screw holes using the supplied two Phillips head screws (M4 x10–mm) with lock washers. Tighten the grounding screw with 22 to 24 lb-in (2.5 to 2.7 Nm) of torque.

Step 5 If necessary, strip the other end of the ground wire and connect it to a reliable earth ground, such as a grounding rod or an appropriate grounding point on a metal streetlight pole that is grounded.

Figure 12: Position of the Ground Pad on the Right Side of the AP



1	Ground pad, where the ground strap screw holes are located.

Powering the Access Point

The AP supports Power-over-Ethernet (PoE) based power sources.

The AP is powered via the PoE input from an inline power injector. Depending on the configuration and regulatory domain, the required power for full operation is 802.3at.

Table 9: Cisco Catalyst Wireless 9163E AP Reduced Power Feature Matrix

SKU	PoE-in/DC Input	Radio 0	dBm	Radio 1	dBm	Radio 2	dBm	Scan Radio	Ethernet mGig	BLE	GNSS
		SS	Per Path	SS	Per Path	SS	Per Path				
		2.4-GHz radio		5-GHz Primary radio		6-GHz Primary radio					
CW9163E	.3af (15.4W)	1x1	17	1x1	17	disabled	—	disabled	1G	N	Y
	.3at (30W)	2x2	22	2x2	22	2x2	AFC assigned	enabled	2.5G	Y	Y

Connecting a Power Injector

The AP supports the following power injectors:

Table 10: Supporting Power Injectors

Power Source	Description
AIR-PWRINJ6=	30 W rated single-port PoE injector
AIR-PWRINJ7=	65 W rated single-port PoE injector (802.3bt), mGig Ethernet
IW-PWRINJ-60RGDMG=	37 W rated power injector
MA-INJ-4	30 W rated single-port PoE injector **Note** This power injector is in End of Life (EoL) stage.
MA-INJ-6	60 W rated PoE injector (802.3bt), mGig Ethernet

The power injector provides with DC voltage to the AP over the Ethernet cable and supports a total end-to-end Ethernet cable length of 100 m (328 ft) from the switch to the AP.

When an optional power injector powers your AP, follow these steps to complete installation:

Procedure

Step 1 Before connecting the PoE to the AP, ensure that the AP is grounded (see Grounding the Access Point, on page 27).

Step 2 Identify the components needed for the installation, see the Typical Access Point Installation Components, on page 14.

Step 3 Connect a CAT6 or better Ethernet cable from your wired LAN network to the power injector.

Note The installer is responsible for ensuring that powering the AP from this type of power injector is allowed by local and/or national safety and telecommunications equipment standards.

Step 4 Ensure that the antennas are connected and that the grounding cable is attached to the AP before you apply power to the AP.

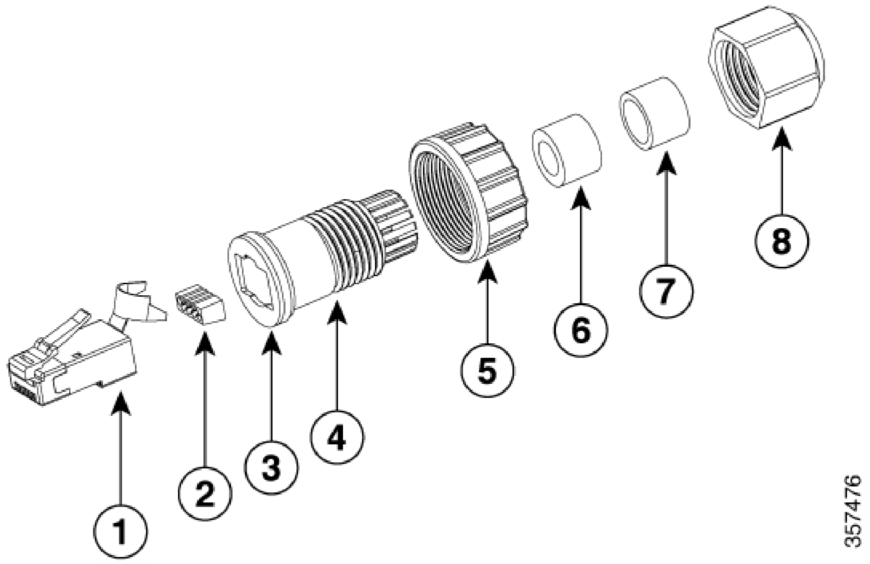
Step 5 Connect a shielded outdoor-rated Ethernet (CAT6 or better) cable between the power injector and the AP's PoE-in connector.

Step 6 Connect the Ethernet cable to the AP PoE-In port.

Connecting an Ethernet Cable to the Access Point

Installing a CAT 6/6A Ethernet Cable and Gland Assembly to the Access Point

Figure 13: CAT 6/6a Cable Gland Assembly



1	CAT 6/6A RJ45 Plug	5	Screw nut
2	RJ45 wire load bar Note the orientation into plug	6	Cable Seal (Cable OD range 5 mm to 7 mm)
3	Gasket It is pre-attached to the Clamp ring.	7	Cable Seal (Cable OD range 7 mm to9 mm)
4	Clamp ring	8	Cable sealing nut

Before you begin

You must supply these tools and materials:

- Shielded outdoor-rated Ethernet (CAT 6 or CAT 6A) cable with a diameter of 0.2 to 0.35 inch (5 to 9 mm)
- CAT 6 RJ45 connector installation tool
- Adjustable wrench or 18–mm box wrench

Note We recommend the application of dielectric grease on the RJ45 connector pins as an additional layer of protection from moisture. The dielectric grease creates a moisture barrier preventing the RJ45 connector pins from corrosion if the gland's weathertight seal fails.

Procedure

Step 1 Disconnect the power to the power injector.

Step 2 Ensure a 6 AWG ground wire is connected to the AP (see Grounding the Access Point, on page 27).

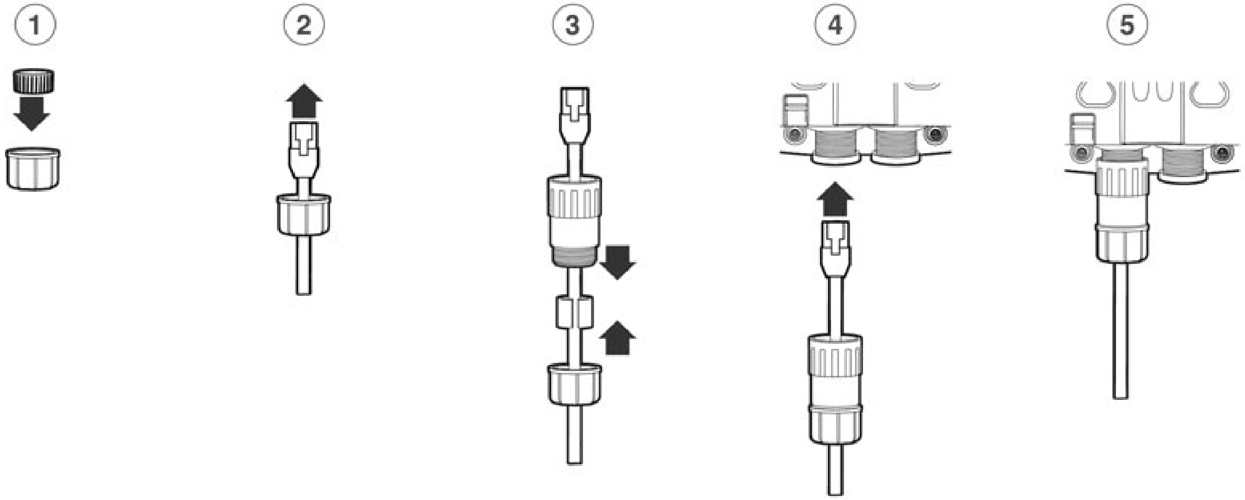
Step 3 Remove the covering cap from the PoE port.

Note Verify that the cable gland has a rubber seal and gasket. Ensure that it is not damaged.

Caution If the cable gland and rubber gasket are not installed correctly, it causes the cable grip to leak.

Step 4 Loosen and remove the cable sealing nut of the cable gland by turning it counterclockwise.

Figure 14: Visual Representation of CAT 6/6A Ethernet Cable Installation Procedure



Step 5 Insert the Ethernet cable's unterminated end through the cable sealing nut.

Pass the Ethernet cable through the appropriate size cable seal, then pull several inches of cable through the gland components.

Note Install the proper cable seal that fits the OD of the Ethernet cable used.

Step 6 Insert the cable seal into the clamp ring, then install the cable seal nut back to the clamp ring.

Do not tighten the clamp ring.

Step 7 Install the CAT 6/6A RJ45 connector on the Ethernet cable's unterminated end using your Ethernet cable installation tool.

Follow the common CAT6/6A Ethernet connector installation procedures. Fold and crimp the connector metal strain lug end over the outer cable jacket, foil and ground wire if equipped.

Caution Ensure the RJ45 connector end where the cable enters is free from cable foil, shielding, and jacket that was peeled back during termination. If any material is left this may cause internal component interference and fail to seal properly to the RJ45 port.

Step 8 Slide the terminated RJ45 connector into the clamp ring till it stops.

Pull the cable to ensure that the connector is seated into the clamp ring.

Step 9 Tighten the cable seal nut around the cable.

Using a 18mm or adjustable wrench, tighten the nut to 7-9 lbf-in (8 – 10 kgf-cm).

Step 10 Install the RJ45 cable gland assembly into the AP port.

Thread the screw nut onto the AP threaded port and tighten by hand to be sure the gland seals to the port. Torque to 15 lbf-in (17 kgf-cm), if possible.

Step 11 Route your Ethernet cable and cut off any excess cable.

Step 12 Install an RJ45 connector on the unterminated cable end and insert it into the power injector or device PoE port.

Note Ensure the individual conductor sequence matches the opposite connection end. The typical sequence follows the T568B pinout standard.

Step 13 Turn on the power to the power injector.

Mounting Antennas

Installing the Omnidirectional Antenna

The CW-ANT-O1-NS-00 is an N-type connector omnidirectional Self-Identifying Antenna (SIA).

Procedure

Step 1 Match the antenna to the corresponding AP port based on the supporting radio band.

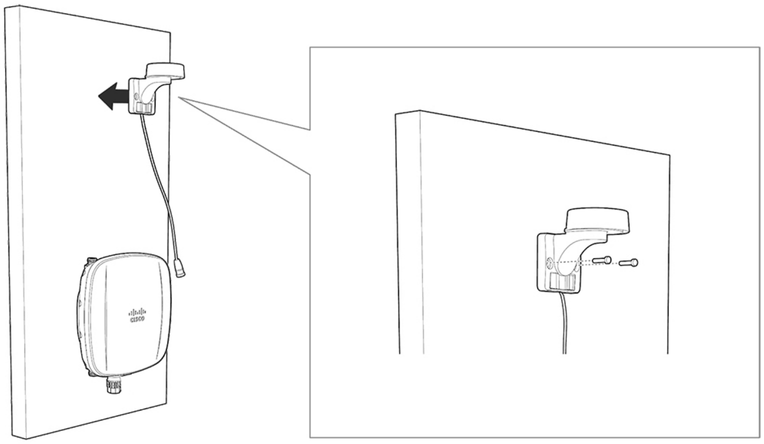
For more information, see Supported External Antennas, on page 7.

Step 2 Connect the antennas to the N-connector on the AP.

Wall Mounting the GNSS Antenna

CW-ANT-GPS2-S-00 is a GNSS antenna with an integrated mounting bracket for mounting to a wall or a pole.

Figure 16: Wall Mounting a GNSS antenna



Before you begin

Ensure that you have the following materials before beginning to mount the GNSS antenna to a wall:

Table 11: Material Required to Mount CW-ANT-GPS2-S-00 to a Wall

Materials Required	Supplied in the Kit?
Wall/pole mount bracket	Yes
Two wall mounting screws	No
Two wall anchors (specified for all material)	No
Drill bit for wall anchors	No
Electric drill and standard screwdriver	No

Procedure

Step 1 Use the GNSS CW-ANT-GPS2-S-00 mounting bracket as a template to mark the two screw hole locations on the mounting wall.

Step 2 Use two screws and, if required, wall anchors to attach the mounting bracket to the mounting surface. These screws and anchors are to be sourced independently.

Note You can use an exterior-grade plywood backboard to mount the GNSS antenna to stucco, cement, or drywall.

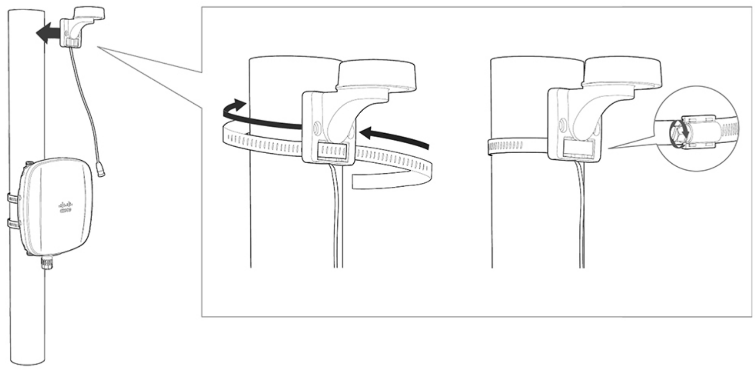
Step 3 Remove the protective cap and connect the antenna to the GNSS port.

The GNSS port is located at the top of the AP. See Connectors and Ports on the AP, on page 5.

Pole Mounting the GNSS Antenna

The CW-ANT-GPS2-S-00 is a mounting bracket with the GNSS antenna for mounting the antenna to a wall or a pole.

Figure 17: Pole mounting a GNSS antenna



Before you begin

Ensure that you have the following materials before beginning to mount the GNSS antenna to a pole:

Table 12: Material Required to Mount CW-ANT-GPS2-S-00 to a Pole

Materials Required	Supplied in the Kit?
Wall/pole mount bracket	Yes
One stainless steel band clamp (adjustable 2.5 to 3.9 inch (63.5 to 99.06 mm)	Yes
A flathead screwdriver	No

Procedure

Step 1 Select a mounting location on the pole to mount the CW-ANT-GPS2-S-00 GNSS antenna bracket.

You can attach the antenna to a pole having a diameter of 2.5 to 3.9 inch (63.5 to 99.06 mm).

Step 2 Hold the bracket up against the pole and slide the band strap through the horizontal slot at the bottom of the mounting bracket.

Step 3 Place the GNSS antenna in its final position.

Tighten the band clamp with the wrench or a screwdriver so that the bracket does not slide on the pole. Ensure that the clamp is tight enough not to let the antenna move.

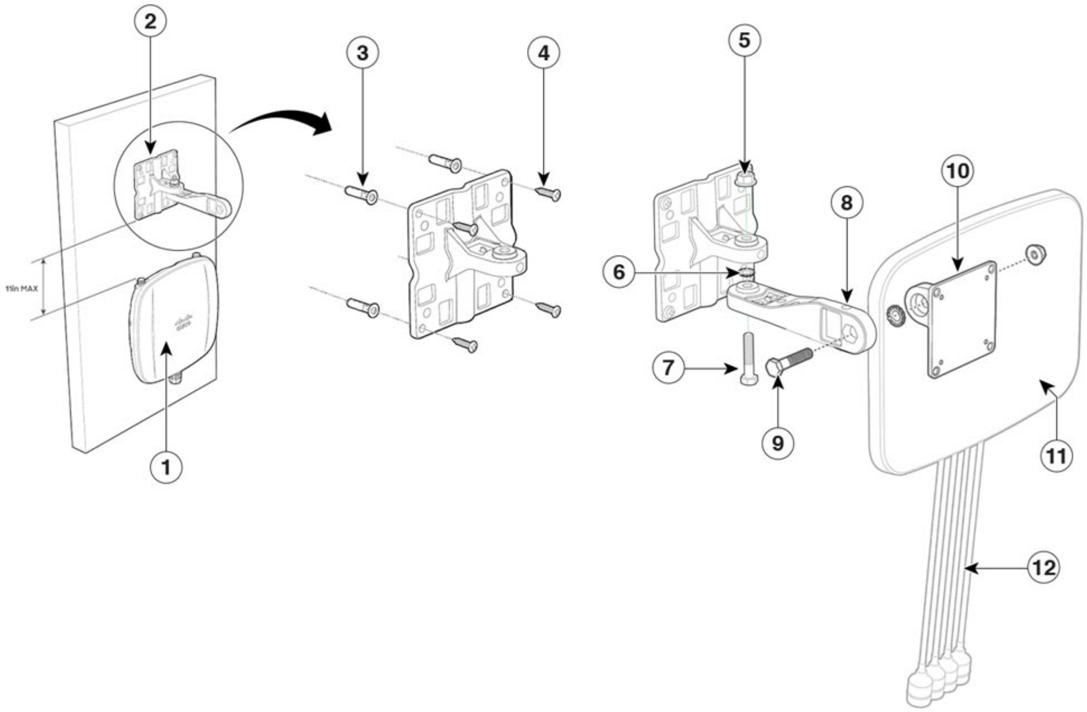
Step 4 Remove the protective cap and connect the antenna to the GNSS port.

The GNSS port is located at the top of the AP. See Connectors and Ports on the AP, on page 5.

Wall Mounting the CW-ANT-D1-NS-00 Antenna

The CW-ANT-D1-NS-00 is a N-type connector directional antenna designed for wall-mounting applications.

Figure 18: Wall Mouting CW-ANT-D1-NS-00 Antenna to AP



1	Access point
2	CW-MNT-ART2-00 articulating mount
3	One of four screw anchors
4	One of four mounting screws
5	Nut
6	Washer
7	Joint bolt
8	Articulating arm
9	Joint bolt

10	Antenna plate
11	CW-ANT-D1-NS-00 antenna
12	N-type connector

Before you begin

Ensure that you have the following materials before beginning to mount the CW-ANT-D1-NS-00 antenna to a wall:

Table 13: Material Required to Mount CW-ANT-D1-NS-00 to a Wall

Materials Required	Supplied in the Kit?
CW-MNT-ART2-00 Articulating mount	Yes
Four M5 x 13 mm screws	Yes
Joint bolts and nuts	Yes
Wall mount screws	No
Drill bit for wall anchors	No
Electric drill and standard screwdriver	No

Procedure

Step 1 Attach the articulating arm segment to the large arm base plate using the provided joint bolt and nut before securing the entire arm assembly to the base plate.

Step 2 Position the antenna at the desired location on the mounting surface.

Step 3 Utilize the large arm base plateas a template to outline the positions for the mounting holes.

Step 4 Use a 0.1360-inch (3.4772 mm) drill bit to create pilot holes at the designated markings for the mounting holes.

Step 5 Identify the pilot holes, insert wall anchors into each one, and secure them firmly in place.

Step 6 Align the large arm base plate with the fastener holes and use screws with a diameter of up to 6 mm and a minimum length of 1-1/4 inches (to be procured separately) to affix the plate against the wall.

Step 7 Fasten the antenna to the small antenna plate and tighten it into place using the screws included in the package.

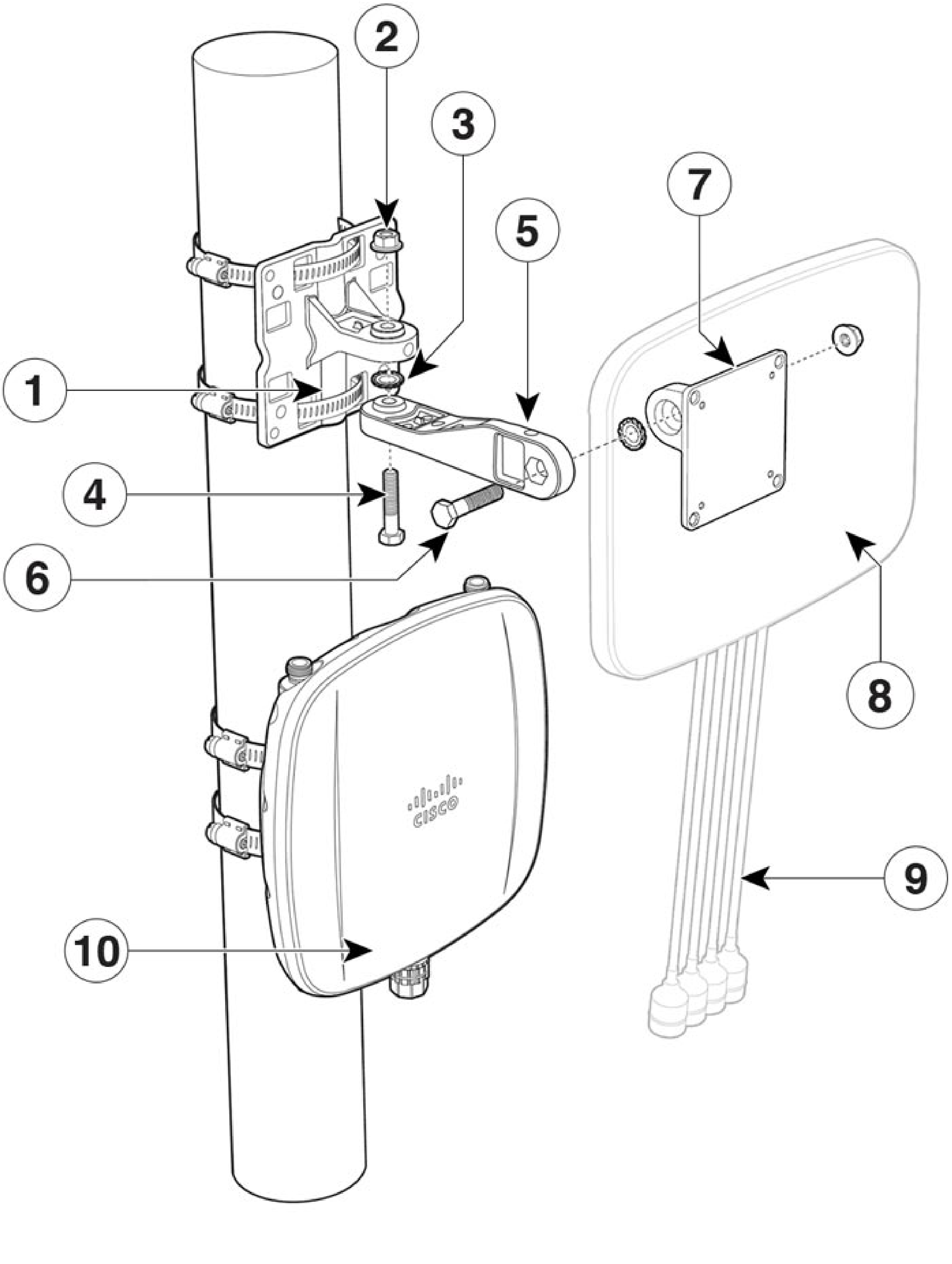
Step 8 Fasten the vertical tilt joint of the small antenna plate to the articulating arm using the bolt and nut provided in the kit.

Step 9 Connect the N-type connectors on the antenna to the antenna ports on the access point. The cables should be connected to the corresponding colors on the AP antenna ports.

Pole Mounting the CW-ANT-D1-NS-00 Antenna

The CW-ANT-D1-NS-00 is a N-type connector directional antenna designed for pole-mounting applications.

Figure 19: Pole Mounting CW-ANT-D1-NS-00 Antenna to AP



1	Articulating arm base plate
2	Nut
3	Washer
4	Joint bolt
5	Articulating arm
6	Joint bolt
7	Antenna plate
8	CW-ANT-D1-NS-00 antenna
9	N-type connector
10	Access point

Before you begin

Ensure that you have the following materials before beginning to mount the CW-ANT-D1-NS-00 antenna to a pole:

Table 14: Material Required to Mount CW-ANT-D1-NS-00 to a Pole

Materials Required	Supplied in the Kit?
CW-MNT-ART2-00 Articulating mount	Yes
Four M5 x13 mm screws	Yes
Joint bolts and nuts	Yes
Two stainless steel band clamps	Yes
Flathead screwdriver	No
Philips PH2 screwdriver	No

Procedure

Step 1 Attach the articulating arm segment to the large arm base plate using the provided joint bolt and nut before securing the entire arm assembly to the base plate.

Step 2 Position and mount the pole mounting flange onto the pole or mast using the hose clamps provided in the kit.

The hose clamps should pass through the slots on the free mounting flange bracket.

Step 3 Tighten the hose clamps and set screws until the flange is fully secure on the mast.

Adjust the flange to its final position. Then, use a slotted screwdriver to tighten the screws on the hose clamps.

Step 4 Fasten the antenna to the small antenna plate and tighten it into place using the screws included in the package.

Step 5 Fasten the vertical tilt joint of the small antenna plate to the articulating arm using the bolt and nut provided in the kit.

Step 6 Connect the N-type connectors on the antenna to the antenna ports on the access point. The cables should be connected to the corresponding colors on the AP antenna ports.

CHAPTER 4

Deploying the Access Point

This section describes how to connect the AP to a controller. For instructions on how to configure the AP, see the relevant release's *Cisco Wireless Controller Configuration Guide.*

Controller Discovery Process

The Cisco AP must join a controller to function as an AP and start serving clients. Cisco uses a process called the controller discovery process to join a controller. The devices use Lightweight Access Point Protocol (LWAPP) to communicate with each other. The AP can be associated to a controller regardless of the physical location or logical location in the network. A new AP, out of the box, can be plugged in anywhere regardless of the subnet. After it is plugged in, it locates the controller, receives the controller version of the software image and configuration. After this is sent to the AP, it can start serving clients.

To support the CW9163E AP, the controller must be running Cisco IOS XE 17.12.3 or a later release. For more information, see the Cisco Catalyst Wireless 9163E Series Outdoor Access Point Data Sheet.

Guidelines and Limitations

- You cannot edit or query any AP using the controller CLI if the AP's name contains a space.
- Make sure that the controller is set to the current time. If the controller is set to a time that has already occurred, the AP might not join the controller because its certificate might not be valid for that time.

The controller must discover the AP before it can become an active part of the network. The AP supports the following controller discovery processes:

- Locally stored controller IP address discovery: If the AP was previously joined to a controller, the primary, secondary, and tertiary controllers' IP addresses are stored in the AP's non-volatile memory. This process of storing controller IP addresses on an AP for later deployment is called priming the AP. For more information about priming, see Performing a Preinstallation Configuration (Optional), on page 16.
- DHCP server discovery: This feature uses DHCP option 43 to provide the controller IP address to the AP. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see Configuring DHCP Option 43, on page 57.

- DNS discovery: The AP can discover controllers through your domain name server (DNS). For the AP to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the AP domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backward compatibility in an existing customer deployment. When an AP receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the AP sends discovery requests to the controllers.

Deploying the Access Point in a Wireless Network

After you have mounted the AP, follow these steps to deploy it in a wireless network:

Procedure

Step 1 Connect the power supply and power up the AP.

Step 2 Observe the AP's LED.

For LED descriptions, see Checking the Access Point LEDs, on page 42.

a) When you power up the AP, it begins a power-up sequence that you can verify by observing the AP's LED. If the power-up sequence is successful, the discovery and join process begins. During this process, the LED blinks sequentially green, red, and off. When the AP has joined a controller, and there are no clients associated, the LED is green or blue when clients are associated with it.

b) If the LED is not on, the AP is most likely not receiving power.

c) If the LED blinks sequentially for more than five minutes, the AP could not find its primary, secondary, and tertiary controller. Check the connection between the AP and the controller, and be sure the AP and the controller are either on the same subnet or that the AP has a route back to its primary, secondary, and tertiary controller. If the AP is not on the same subnet as the controller, be sure that there is a properly configured DHCP server on the same subnet as the AP. See Configuring DHCP Option 43, on page 57 for additional information.

Step 3 Reconfigure the controller so that it is not the primary controller.

Note Use the primary controller to configure the AP only. Avoid using this controller in a working network.

Checking the Access Point LEDs

The location of the AP status LED is shown in Connectors and Ports on the AP, on page 5.

Note About LED status colors, it is expected that there will be small variations in color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect. However, the intensity of the LED can be changed through the controller.

The AP supports dark mode to reduce visibility to the AP. You can enable the dark mode using the GUI or CLI method in the controller. See the Information About LED States for Access Points section in the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

The AP status LED indicates various conditions and is described in the following table:

Table 15: AP LED Signals

LED Message Type	Color	Meaning
Boot loader status sequence	Blinking Green	Boot loader status sequence: • DRAM memory test in progress • DRAM memory test OK • Board initialization in progress • Initializing the Flash file system • Flash memory test OK • Initializing Ethernet • Ethernet OK • Starting AP OS • Initialization successful
Association status	Solid Green	This status indicates a normal operating condition. The unit has joined a controller, but no wireless client is associated with it.
	Solid Blue	Normal operating condition with at least one wireless client associated with the unit
	Cycling through Green, Red, off	Discovery or join process is in progress
	Rapidly cycling through Blue, Green, Red	This status indicates that the AP location command has been invoked.
	Blinking Red	This status indicates that an Ethernet link is not operational
	Solid Red	Ethernet failure
	Blinking Blue	Configuration recovery is in progress (the Reset button has been pushed for 2 to 3 seconds)

LED Message Type	Color	Meaning
Boot loader warnings	Solid Red	Image recovery (the Reset button has been pushed for 20-30 seconds)
Cisco IOS Errors	Cycle through Blue, Green, Red and Off	General warning Insufficient inline power

Management Mode Migration

CW9163E AP supports both Cisco Controller and Meraki cloud architecture. You can switch between on-prem controller and cloud deployments, depending on your requirements.

You can configure the management mode migration with the help of CLI commands in the privileged EXEC mode, at the AP level, and from the controller GUI. The below table provides the links to the respective migration procedures.

Migrating the AP from Cisco controller to Meraki Management mode	Cisco Management Migration Cisco Catalyst Center Management Migration
Migrating the AP from Meraki Management mode to Cisco controller	Meraki Management Migration

CHAPTER 5

Network Deployment

This section provides information about network deployment options, and how to include the 6 GHz access points in the network.

Cisco On-Premises Deployment

You can associate the CW9163E AP to a Cisco On-premises deployed network.

Initializing an Access Point

Perform the following procedure for an out-of-the-box (OOB) AP. This procedure prepares the AP to associate with a network.

Procedure

Step 1 Connect the power supply and power up the AP.

The switch port connected to the access point can be a trunk or access port.

Note The mGig or GE port can be used for the AP's connection.

Step 2 (Optional) Configure the switch port to trunk the VLANs when multiple VLANs are used for client traffic in FlexConnect deployment. Use the access mode in Local Mode/Centralized deployments.

Step 3 Configure the VLAN as a native VLAN.

When the management traffic is untagged, the VLAN is used for management.

Example: Configuring the port on a switch

```
interface GigabitEthernet1/0/37
    switchport trunk native VLAN 122
    switchport trunk allowed VLAN 10,20,122
    switchport mode trunk
```

Example: For Flexconnect/Distributed deployments

```
Switch(config)# interface GigabitEthernet 0/0/10
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 1,2,3,4
```

Example: For Local Mode/Centralized deployments

```
Switch(config)# interface GigabitEthernet 0/0/10
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 10
```

Step 4 VLAN associated with the AP must have DHCP scope enabled.

The DHCP scope can be active in the switch or in an external DHCP server.

Step 5 AP's LED should be solid green and with a valid IP address.

In this state, the AP is ready to join a controller. The process should take about five minutes to complete. For LED descriptions, see Checking the Access Point LEDs, on page 42.

Associating an Access Point with a Controller

The Cisco access points need to associate themselves with a controller in the network. There are multiple methods to complete the association process.

Associate the AP to a controller using one of the following options:

Before you begin

Before associating the AP, ensure that the controller is configured with the correct country code. For more information, see Countries and Regulations chapter in *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

Procedure

- Enable the AP to discover the controller using the L2 discovery process.

Note For the discovery process, both the AP and the controller need to be in the same broadcast domain.

- Configure the AP with the controller name and IP address

  Prime the AP by using the command **capwap ap primary base** *wlc-name wlc-ip*

- Use DHCP Option 43 to initiate the discovery process.
- Use DNS A-record to let the AP discover the controller.
- Add a DNS server entry **pnpserver** in the private DNS server pointing to your Cisco Catalyst Center IP address.
- Use PnP Connect Cloud direction by using a public DNS server.

  The PnP Connect Cloud directs the AP to the Cisco Catalyst Center. From the Catalyst Center, the controller can claim and associate the AP.

Configuring Wireless Controller

Configuring 6-GHz Radio Profile

This procedure enables the 6-GHz radio DCA channels in the controller.

Note The CW9163E AP's 6-GHz radio is enabled for use in AFC approved countries only.

Procedure

Step 1 Log in to the Catalyst 9800 controller.

Step 2 Choose **Configuration** > **Tags & Profiles** > **RF/Radio**.

The **RF/Radio** page is displayed.

Step 3 In the **RF** tab, click **default-rf-profile-6ghz**.

The **Edit RF Profile** window is displayed.

Step 4 Click **RRM** > **DCA** tab.

Step 5 Ensure all the DCA Channels are enabled.

Step 6 Click **Update & Apply to Device**.

Configuring 6-GHz OFDMA

This procedure enables the 6-GHz radio OFDMA in the controller.

Procedure

Step 1 Log in to the Catalyst 9800 controller.

Step 2 Choose **Configuration** > **Radio Configurations** > **High Throughput** > **5 GHz Band** > **11ax**.

Step 3 Check **Enable 11ax** check box.

Step 4 Check the check boxes for the desired MCS/(data rate), or to select all of them, check the **Select All** check box.

Step 5 Choose **Configuration** > **Radio Configurations** > **High Throughput** > **6 GHz Band**.

Step 6 Check the check boxes for the desired MCS/(data rate), or to select all of them, check the **Select All** check box.

Step 7 Click **Update & Apply to Device**.

Configuring WPA3 Security

The Wi-Fi 6E radio protocol requires WPA3 security for the 6-GHz band. WPA3 is not backward compatible, even when the WPA3 Transition mode is enabled.

You have three options when creating a WLAN.

- All-In: You must reconfigure all the WLANs to WPA3 only.
- Multiple SSID: Reconfigure SSIDs by adding SSID/WLAN with specific security settings.

For more information, see *WPA3 Deployment Guide* at the following URL:

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/wpa3-dep-guide-og.html

Procedure

Step 1 Log in to the Cisco Catalyst 9800 Controller.

Step 2 Choose **Configuration** > **Tags & Profiles** > **WLANs**

Perform either of the the following steps as applicable:

- To create a new WLAN for the 6-GHz radio, click **Add** and enter the profile and SSID names.
- You can choose from an existing WLAN.

  The **Edit WLAN** window is displayed

Step 3 Select the type of security protocol for the WLAN.

Enable one of the following security protocol:

- Configuring the WPA3 security protocol.
  a. Choose **Security** > **Layer2** tab.

  b. Select the **WPA3** tab.

  c. Check one of the Auth Key Mgmt check boxes.

    - OWE
    - SAE
    - 802.1X-SHA256

  d. Enable Protected Management Frame (PMF)

  Select the PMF state from **Required** or **Optional** from the drop-down list.

- Configuring WPA2 + WPA3 security protocol.
  a. Choose **Security** > **Layer2** tab.

  b. Select the **WPA2 + WPA3** tab.

  c. Check one of the Auth Key Mgmt check boxes.

- 802.1x
- 802.1x-SHA256

Step 4 In the **Advanced** tab, to enable 802.11ax features, Check all feature check boxes under the **11ax** section.

Step 5 Save the settings.

Configuring Policy Tag

Procedure

Step 1 Log in to the Cisco Catalyst 9800 Controller.

Step 2 Choose **Configuration** > **Tags & Profiles** > **Tags**

Step 3 Click **default-policy-tag**

The **Edit Policy Tag** window is displayed.

Step 4 Select **WLAN-POLICY**, and click **Add**.

Step 5 Choose the **WLAN profile** to map with the appropriate **Policy profile** from the drop-down list and click the tick icon.

Step 6 Click **Update & Apply to Device**.

Step 7 Choose **Monitoring** > **Wireless** > **Radio Statistics** > **6 GHz Radios** *ap-name*

Verify the 6 GHz configurations on the AP after it is associated with the controller.

Configuring Client Band Steering

The client band steering feature nudges the client to join the 6-GHz band if the client supports this band instead of joining the 2.4 or 5-GHz band.

Procedure

Step 1 Log in to the Cisco Catalyst 9800 Controller.

Step 2 Choose **Configuration** > **Tags & Profiles** > **WLANs**

Step 3 Select the WLAN

When selecting an existing WLAN, the **Edit WLAN** window is displayed. Alternatively, you may create a new WLAN if required.

Step 4 Select the **Advanced** tab.

Step 5 Check the **6 GHz Client Steering** check box.

Step 6 Click **Update & Apply to Device**.

Step 7 Choose **Configuration** > **Wireless** > **Advanced** > **6 GHz Client Steering**

Step 8 Configure the threshold values.

You can set the threshold values to meet your requirements.

Step 9 Click **Apply**.

Meraki Cloud Based Deployment

You can associate the CW9163E AP to a Meraki Cloud based deployed network.

Claiming an AP in a Dashboard

In a cloud-based deployment, the access points need to be onboarded from the common pool.

Procedure

Step 1 Initiate adding the APs

You can initiate the AP add process from either of the following ways:

- **Network-wide** > **Configure** > **Add Devices**
- **Organization** > **Configure** > **Inventory**

Step 2 Filter the APs using the **Search Inventory**

You can search for the devices or group of devices with any of the following parameters:

- MAC address
- Serial number (12–digit number)
- Network name
- Model number
- Order number (09-digit Cisco Meraki order number)
- Country code

Step 3 Click **Claim**

The devices are added to the available devices list.

Configuring Firewall for Cloud Management Access

The onboarding APs need to connect with the Cloud management to ensure that the outgoing connections on specific IP addresses and ports are open for this connection to be established.

The outbound ports and IP addresses are listed under the Dashboard's **Help** > **Firewall info** section.

The Wi-Fi 6 APs use an IP address range of 209.206.48.0/20 TCP port 443 to communicate with the Dashboard.

Note Older Wi-Fi APs use TCP port 7734 and UDP port 7351 to communicate with the Dashboard.

Associating AP with Cloud Management

All gateway APs must be assigned with routable IP addresses. The AP can acquire the IP address dynamically, or you can assign a static address.

Dynamic Assignment (Recommended)

The DHCP server should be configured to assign a static IP address for every AP MAC address. Wireless network features, such as 802.1x authentication, may rely on the AP to have a static IP address.

Static Assignment

Static IPs are assigned using the local web server on each AP. Using the following procedure, you can configure the static IP address.

1. Use a PC (laptop) and connect with the AP.

   Connect with the AP over a wired connection or wirelessly on the SSID it is broadcasting.

   When using a wired connection, connect the client machine to the AP through either a PoE switch or an Injector. If using a PoE switch, plug an Ethernet cable into the AP's Ethernet jack and the other end into a PoE switch. Then, connect the client machine over the Ethernet cable to the PoE switch. If using a PoE Injector, connect the AP to the **PoE** port of the Injector and the client machine to the **LAN** port.

Access the AP Local Page

To configure the AP, you need to access and log in to the AP’s local page.

1. Using a web browser on the client machine, access the AP’s built-in web server by browsing to http://my.meraki.com.

   Alternatively, browse to http://10.128.128.128.

2. Click the **Uplink Configuration** tab to Log in.

   The default login is the serial number (for example: Qxxx-xxxx-xxxx), with no password.

3. Configure the static IP address, netmask, gateway IP address, and DNS servers that this AP will use on its wired connection.

   If necessary, reconnect the AP to the LAN.

Firmware Management

We recommend you run the latest stable release on the APs. When there is an upgrade in progress, the LED blinks blue and turn solid blue or green after the upgrade is complete.

License Management

All the devices are required to have a license to associate with the Dashboard.

You can claim an order, license, or device from the Dashboard.

1. Log in to the Dashboard
2. Click **Organization** > **License Info**

   Or **Organization** > **Inventory**
3. Click **Add**
4. Enter the order number, serial number, or license key.

   You can enter multiple items, one per line.
5. Click **Next**

   The list of items added is displayed.
6. You can manually assign the licenses to the devices.

   To auto-assign the licenses, select **Accept and assign**.
7. Click **Select**.

Configuring Cloud Dashboard Deployment

Procedure

Step 1 Enabling SSIDs.

You can update network name, SSID name from the Dashboard's SSID page.

a) **Wireless** > **Configure** > **SSIDs**
b) Select **Enabled** from the drop-down list.
c) Click **Save Changes**

Step 2 Configure the Access Control List.

Navigate to **Wireless** > **Configure** > **Access Control** page.

Configure the per-SSID access control settings including association security, splash page, client addressing option settings.

Step 3 Configure the security protocols.

You can custom configure each SSID security to filter the clients associated with the SSID. You can configure PSK protocols for the SSID.

The Wi-Fi 6E radio protocol requires WPA3 security for the 6-GHz band. WPA3 is not backward compatible, even when the WPA3 Transition mode is enabled.

You have three options when creating a WLAN.

- All-In: You must reconfigure all the WLANs to WPA3 only.

- Multiple SSID: Reconfigure SSIDs by adding SSID/WLAN with specific security settings.

Step 4 Configure RF Profiles

Navigate to **Wireless** > **Radio Settings** > **Overview** tab.

You can create RF profiles to apply specific radio settings that can be applied to a wireless network.

By default, two RF profiles are defined for every network. One is for indoor APs, and one is for outdoor APs. The RF profiles are automatically assigned to an AP. You can verify the RF profile assigned to a particular AP on the **Overview** page.

Step 5 Radio band selection in an RF Profile.

An RF profile can be configured to apply all bands or selective bands to all SSIDs (with or without band steering) or selective SSIDs. In per SSID configuration, 2.4GHz, 5GHz, 6GHz tri-band or tri-band with band steering options are available.

The following are the band selection options available in the Dashboard

- Check the **2.4 GHz**checkbox to set an SSID to 2.4 GHz only.
- Check the **5 GHz** checkbox to set an SSID to 5 GHz only.
- Check the **6 GHz** checkbox to set an SSID to 6 GHz only.
- Select both **2.4 GHz** and **5 GHz** checkboxes to set an SSID to dual-band operation.
- Select all three **2.4 GHz**, **5 GHz**, and **Band steering** checkboxes to set an SSID to dual-band operation with band steering.

Step 6 Band steering configuration for all radio bands.

By default, clients associate with 2.4 GHz and 5 GHz band radio. However, using the client steering feature, the 6 GHz capable clients are nudged to associate with the 6 GHz band, depending on the settings configured.

a) Choose **Wireless** > **Configure** > **Radio Settings** > **RF Profiles**.

b) Choose **Band Selection** > **All SSIDs**.

To enable band steering for all SSIDs on APs assigned to an RF profile.

Note Ensure both **Enable operation on 2.4 GHz band** and **Enable operation on 5 GHz band** check boxes are checked.

c) Check **Enable band steering** check box.

Note **Enable band steering** check box is grayed out if either 2.4 GHz or 5 GHz operation check box is unchecked.

d) Choose **Band Selection** > **Per SSID** .

To enable band steering per SSIDs on APs assigned to an RF profile.

Note The **Band steering** check box is grayed out if either the 2.4 GHz or 5 GHz operation check box is unchecked.

e) Save the settings.

CHAPTER 6

Troubleshooting

Use the Reset button

The **Reset** button (see Connectors and Ports on the Base) is a multi-function button. Using this button, you can reset the AP to factory default or clear the AP's internal storage.

Reset the AP to Factory Default Settings

Connectors and Ports on the Base, on page 6

To reset the AP to the default factory-shipped configuration, perform the following steps:

1. Press and continue to press the **Mode** button on the access point during the AP boot cycle.
2. Press until the AP console shows a seconds counter.

   When the counter indicates the number of seconds for which the **Mode** button is pressed, the AP status LED changes to blinking red.
3. Press the **Mode** button for less than 20 seconds to reset the AP to the default factory-shipped configuration.

Clear the AP Internal Storage

To clear the AP's internal storage, including all the configuration files, perform the following steps:

1. Press and continue to press the **Mode** button on the access point during the AP boot cycle.
2. Press until the AP console shows a seconds counter.

   When the counter indicates the number of seconds for which the **Mode** button is pressed, the AP status LED changes to blinking red.
3. Press the **Mode** button for more than 20 seconds, but less than 60 seconds to clear the AP internal storage, including all the configuration files.

This resets all the configuration settings to factory defaults, including passwords, the IP address, and the SSID.

Note

- If the **Mode** button is pressed for more than 30 seconds, but less than 60 seconds, the FIPS mode flag is also cleared during the full factory reset of the AP. If the FIPS flag is set, the console access is disabled.
- The AP status LED changes from blue to red, and all the files in the AP storage directory are cleared.
- If you keep the **Mode** button pressed for more than 60 seconds, the button is assumed as being faulty and no changes are made.

Troubleshooting the Access Point to Controller Join Process

Note As specified in the Cisco Wireless Solutions Software Compatibility Matrix, ensure that your controller is running Cisco IOS XE Dublin 17.12.3 or a later release to support the Cisco CW9163E AP.

Access points can fail to join a controller for many reasons—a RADIUS authorization is pending, self-signed certificates are not enabled on the controller, the access point and the controller regulatory domains do not match, and so on.

Controller software enables you to configure the access points to send all CAPWAP-related errors to a syslog server. All the CAPWAP error messages can be viewed from the syslog server itself.

When the ordered AP is a CW9163E-MR model, or the AP is in Meraki Management mode, it will not attempt to join the Cisco 9800 Wireless Controller. Contact the Meraki support team to perform the migration procedure on the AP.

The state of the access point is not maintained on the controller. It can be difficult to determine why the discovery request from a certain access point was rejected. In order to troubleshoot such joining problems, we recommend that you run traces commands on the Cisco Catalyst 9800 Wireless Controller.

The controller collects all the join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all the syslog messages to the IP address 255.255.255.255 by default.

You can also configure a DHCP server to return a syslog server IP address to the access point using Option 7 on the server. The access point then starts sending all the syslog messages to this IP address.

When the access point joins a controller for the first time, the controller sends the global syslog server IP address (the default is 255.255.255.255) to the access point.

The access point sends all the syslog messages to this IP address until it is overridden by the following configuration:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the **syslog host** <*ip address*> command. In this case, the controller sends the new global syslog server IP address to the access point.

To configure the global syslog server IP address, run these commands:

1. **configure terminal**
2. **ap profile** *ap-profile-name*
3. **syslog host** *syslog IP address*
4. **exit**

- The access point is disconnected from the controller and joins another controller. In this case, the new controller sends its global syslog server IP address to the access point.
- Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all the syslog messages to the new IP address, provided the access point can reach the syslog server IP address.

Note You can configure the syslog server for access points and view the access point join information only from the controller CLI.

Important Information for Controller-based Deployments

Keep these guidelines in mind when you use the AP:

- The AP can only communicate with Cisco controllers.
- The AP does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the AP joins it.
- CAPWAP does not support Layer 2. The AP must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The AP console port is enabled for monitoring and debugging purposes. All configuration commands are disabled when the AP is connected to a controller.

Configuring DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the AP, enabling it to find and join a controller.

The following is a DHCP Option 43 configuration example on a Microsoft Windows 2003 Enterprise DHCP server for Cisco Catalyst lightweight APs. For other DHCP server implementations, consult the product documentation to configure DHCP Option 43. In Option 43, use the IP address of the controller management interface.

Note DHCP Option 43 is limited to one AP type per DHCP pool. You must configure a separate DHCP pool for each AP type.

The Cisco Catalyst Wireless 9163E Series Outdoor AP uses the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the AP DHCP Vendor Class Identifier (VCI) string (DHCP Option 43). The VCI string for the AP:

Cisco AP CW9163E

The format of the TLV block is listed below:

- Type—0xf1 (decimal 241)
- Length—Number of controller IP addresses * 4
- Value—IP addresses of the controller management interfaces are listed sequentially in hexadecimal format.

Procedure

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

Example:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>
```

Where:

Example:

```
<pool name> is the name of the DHCP pool, such as AP9163E
<IP Network> is the network IP address where the controller resides, such as 10.0.15.1
<Netmask> is the subnet mask, such as 255.255.255.0
<Default router> is the IP address of the default router, such as 10.0.0.1
<DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 43 line using the following syntax:

Example:

```
option 43 hex <hex string>
```

The hex string is assembled by concatenating the TLV values shown below:

Type + Length + Value

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is f1(hex). The length is 2 * 4 = 8 = 08 (hex). The IP addresses translate to 0a7e7e02 and 0a7f7f02. Assembling the string then yields f1080a7e7e020a7f7f02. The resulting Cisco IOS command is added to the DHCP scope is **option 43 hex f1080a7e7e020a7f7f02**.

CHAPTER 7

Safety Guidelines and Warnings

Translated versions of the following safety warnings are provided in the translated safety warnings document shipped with your AP. The translated warnings are also in the Translated Safety Warnings for Cisco Catalyst Access Points, available on Cisco.com.

FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco antennas, Cisco Catalyst products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

For safety and to achieve a good installation, please read and follow these safety precautions:

- Select your installation site with safety as well as performance in mind. Remember: electric power lines and phone lines look alike. For safety, assume that any overhead line can kill.
- Call your electric power company. Tell them your plans, and ask them to come to look at your proposed installation
- Plan your installation carefully and thoroughly before you begin. Successful raising of a mast or tower is mostly a matter of coordination. Each person should be assigned to a specific task and know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
- When installing the AP or its antennas, remember:
  - Do not use a metal ladder.
  - Do not work on a wet or windy day.

- Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.

- Use a rope to lift the AP. If the assembly starts to drop, get away from it and let it fall.
- If any part of the antenna system comes in contact with a power line, do not touch it or remove it yourself. Call your local power company. They will remove it safely.

If an accident should occur, call for qualified emergency help immediately.

Avoiding Damage to Radios in a Testing Environment

The radios on outdoor units (bridges) have higher transmit power levels than radios on indoor units (APs). When you test high-power radios in a link, you must avoid exceeding the receiver's maximum receive input level. At levels above the normal operating range, packet error rate (PER) performance is degraded. At even higher levels, the receiver can be permanently damaged. To avoid receiver damage and PER degradation, you can use one of the following techniques:

- Reduce the configured transmit power to the minimum level.
- Use directional antennas, and keep them away from each other.
- Cable the radios together using a combination of attenuators, combiners, or splitters to achieve a total attenuation of at least 60 dB.

For a radiated testbed, the following equation describes the relationships among transmit power, antenna gain, attenuation, and receiver sensitivity:

```
txpwr + tx gain + rx gain - [attenuation due to antenna spacing] < max rx input level
Where:
txpwr = Radio transmit power level
tx gain = transmitter antenna gain
rx gain = receiver antenna gain
```

For a conducted test bed, the following equation describes the relationships among transmit power, antenna gain, and receiver sensitivity:

```
txpwr - [attenuation due to coaxial components] < max rx input level
```

Caution Under no circumstances should you connect the antenna port from one AP to the antenna port of another AP without using an RF attenuator. If you connect antenna ports, you must not exceed the maximum survivable receive level of 0 dBm. Never exceed 0 dBm, or damage to the AP can occur. Using attenuators, combiners, and splitters having a total of at least 60 dB of attenuation ensures that the receiver is not damaged and that PER performance is not degraded.

Performing Site Surveys

Every network application is a unique installation. Before installing multiple APs, you should perform a site survey to determine the optimum use of networking components and maximize range, coverage, and network performance.

Site surveys reveal problems that can be resolved before the network is operational. Because 802.11a/b/ac/ax radios operate in an unlicensed spectrum, there may be sources of interference from other wireless devices (especially in multi-tenant buildings) that could degrade your 802.11 signals. A site survey can determine if such interference exists at the time of deployment.

Consider the following operating and environmental conditions when performing a site survey:

- Data rates: Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver sensitivity occurs as the radio data increases.
- Antenna type and placement: Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height. However, do not place the antenna higher than necessary because the extra height also increases potential interference from other unlicensed radio systems and decreases the wireless coverage from the ground.
- Physical environment: Clear or open areas provide better radio range than closed or filled areas.
- Obstructions: Physical obstructions such as buildings, trees, or hills can hinder the performance of wireless devices. Avoid locating the devices in a location where there is an obstruction between the sending and receiving antennas.
- How far is your wireless link?
- Has a previous site survey been conducted?
- Do you have a clear Fresnel zone between the APs or radio line of sight?
- What is the minimum acceptable data rate within the link?
- Do you have the correct antenna (if more than one antenna is being offered?)
- Do you have the proper permits, if required?
- Are you following the proper safety procedures and practices?
- Have you configured the APs before you go onsite? It is always easier to resolve configurations or device problems first.
- Do you have the proper tools and equipment to complete your survey?

CHAPTER 8

Declarations of Conformity and Regulatory Information

This section provides declarations of conformity and regulatory information for the Cisco Catalyst Wireless 9163E Series OutdoorAPs. You can find additional information at this URL: http://www.cisco.com/go/aironet/compliance.

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Access Point Models	Certification Number
CW9163E-B CW9163E-MR	UDX-600191010

Manufacturer:

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference,
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B 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 residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

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

⚠

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using the integrated antennas. Any changes or modification to the product not expressly approved by Cisco could void the user’s authority to operate this device.

Operation of Cisco Catalyst Access Points in México

Declaración para México

La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

VCCI Statement for Japan

⚠

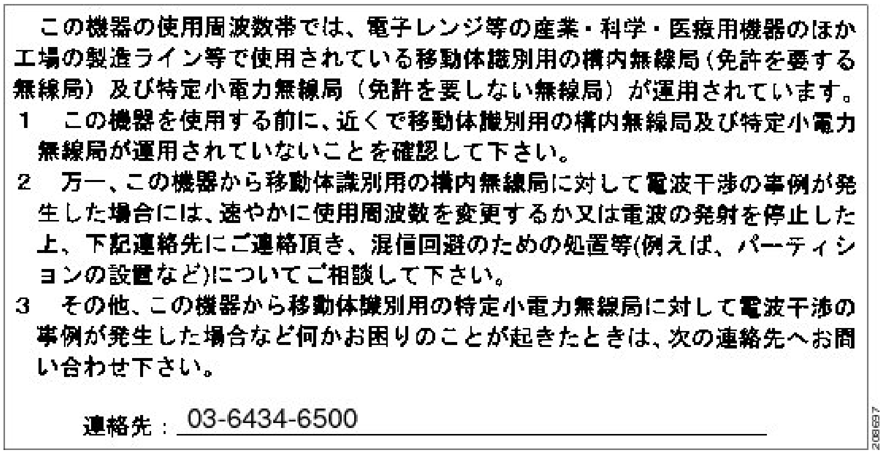
Danger This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

	Danger	This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

警告	**Danger**	この装置は、クラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。 取扱説明書に従って正しい取り扱いをして下さい。 ＶＣＣＩ－Ｂ

Guidelines for Operating Cisco Catalyst Access Points in Japan

This section provides guidelines for avoiding interference when operating Cisco Catalyst access points in Japan. These guidelines are provided in both Japanese and English.



この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

1　この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。

2　万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。

3　その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：03-6434-6500

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

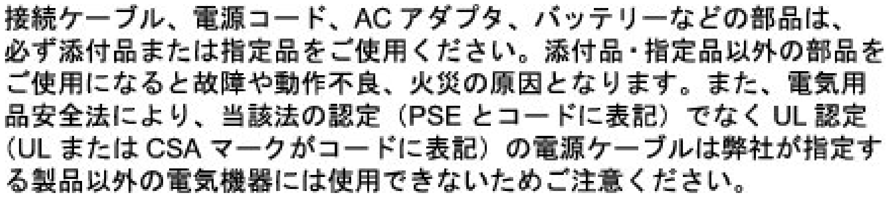
1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.

2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.

3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

Contact Number: **03-6434-6500**

Statement 371—Power Cable and AC Adapter



接続ケーブル、電源コード、AC アダプタ、バッテリーなどの部品は、
必ず添付品または指定品をご使用ください。添付品・指定品以外の部品を
ご使用になると故障や動作不良、火災の原因となります。また、電気用
品安全法により、当該法の認定（PSE とコードに表記）でなく UL 認定
（UL または CSA マークがコードに表記）の電源ケーブルは弊社が指定す
る製品以外の電気機器には使用できないためご注意ください。

English Translation

When installing the product, please use the provided or designated connection cables/power cables/AC adaptors. Using any other cables/adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the “UL” shown on the code) for any other electrical devices than products designated by CISCO. The use of cables that are certified by Electrical Appliance and Material Safety Law (that have “PSE” shown on the code) is not limited to CISCO-designated products.

Compliance Statement for Canada

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.Le présent émetteur radio a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.La bande 5 150-5 250 MHz est réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Users are advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.Les utilisateurs êtes avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Industry Canada

Access Point Models	Certification Number
CW9163E-A CW9163E-MR	6961A-600191010

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Access Point Models:

- CW9163E-E

Note This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Cisco Corporate Compliance.

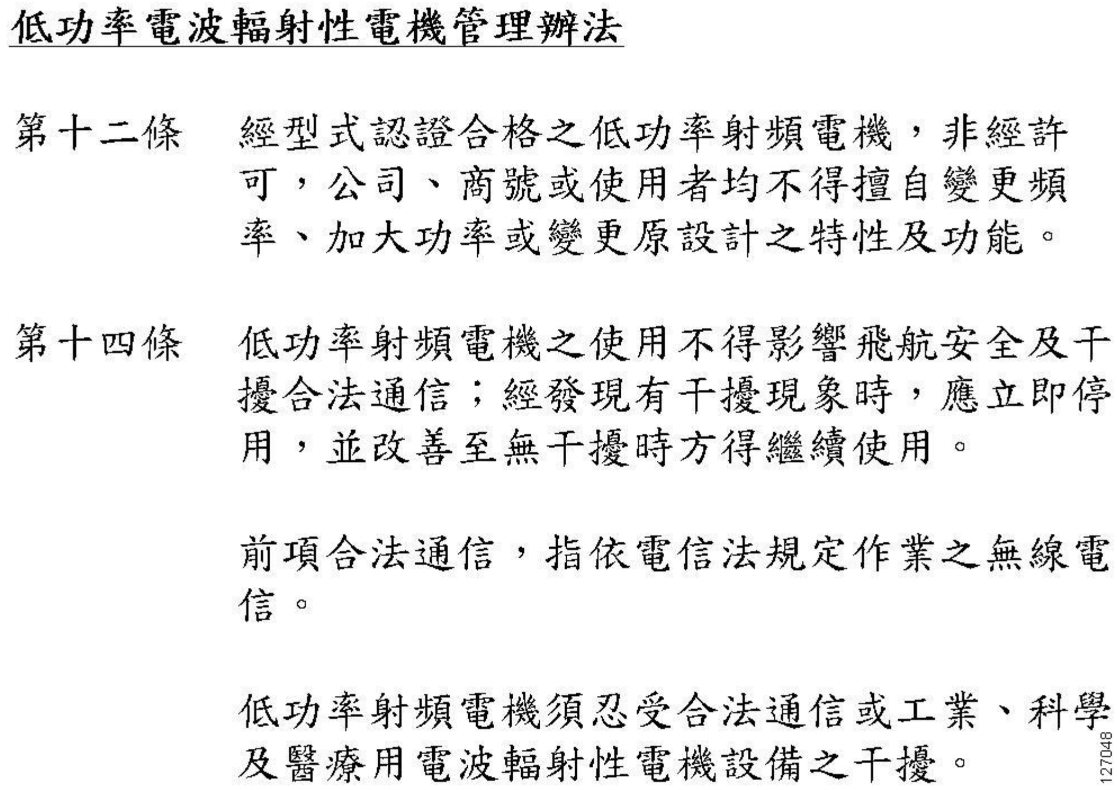
The product carries the CE Mark:

CE

Administrative Rules for Cisco Catalyst Access Points in Taiwan

This section provides administrative rules for operating Cisco Catalyst APs in Taiwan. The rules for all access points are provided in both Chinese and English.

Chinese Translation



低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 12

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

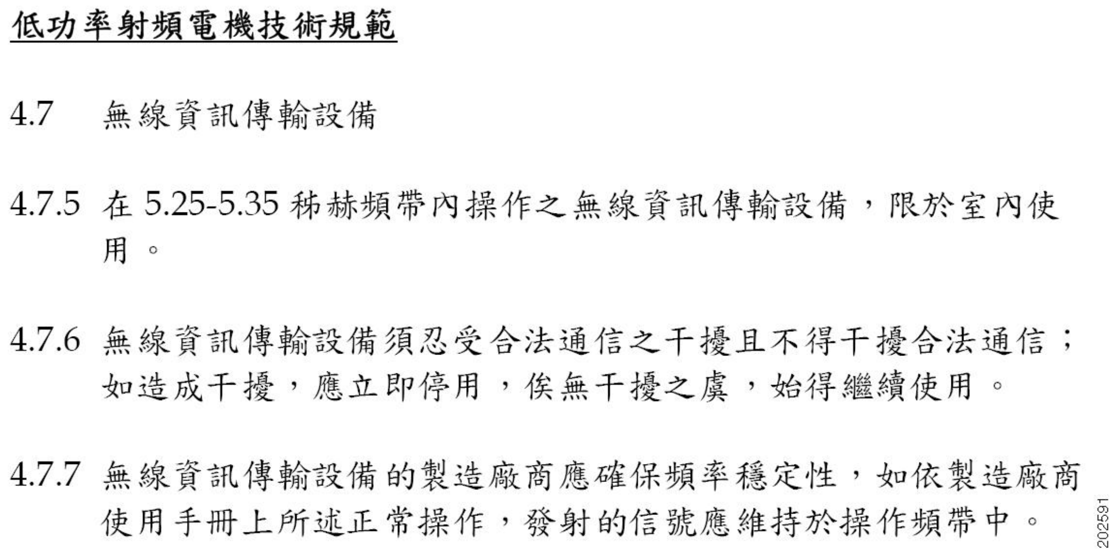
Article 14

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

Chinese Translation



低功率射頻電機技術規範

4.7 無線資訊傳輸設備

4.7.5 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

4.7.6 無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。

4.7.7 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。

English Translation

Low-power Radio-frequency Devices Technical Specifications

4.7	Unlicensed National Information Infrastructure
4.7.5	Within the 5.25-5.35 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.
4.7.6	The U-NII devices shall accept any interference from legal communications and shall not interfere the legal communications. If interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.
4.7.7	Manufacturers of U-NII devices are responsible for ensuring frequency stability such that an emission is maintained within the band of operation under all conditions of normal operation as specified in the user manual.

Operation of Cisco Catalyst Access Points in Brazil

This section contains special information for operation of Cisco Catalyst APs in Brazil.

Access Point Models	Certification Number
CW9163E-ROW	xxxxx-xxxxxxxxx

Figure 20: Brazil Regulatory Information

Portuguese Translation

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

English Translation

This equipment is not entitled to the protection from harmful interference and may not cause interference with duly authorized systems.

Declaration of Conformity for RF Exposure

This section contains information on compliance with guidelines related to RF exposure.

Generic Discussion on RF Exposure

The Cisco products are designed to comply with the following national and international standards on Human Exposure to Radio Frequencies:

- US 47 Code of Federal Regulations Part 2 Subpart J
- American National Standards Institute (ANSI) / Institute of Electrical and Electronic Engineers / IEEE C 95.1 (99)
- International Commission on Non Ionizing Radiation Protection (ICNIRP) 98
- Ministry of Health (Canada) Safety Code 6. Limits on Human Exposure to Radio Frequency Fields in the range from 3kHz to 300 GHz
- Australia Radiation Protection Standard

To ensure compliance with various national and international Electromagnetic Field (EMF) standards, the system should only be operated with Cisco approved antennas and accessories.

This Device Meets International Guidelines for Exposure to Radio Waves

The Cisco Catalyst Wireless 9163E Series Outdoor AP device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) recommended by international guidelines. The guidelines were developed by an independent scientific organization (ICNIRP) and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

The World Health Organization has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices. They recommend that if you are interested in further reducing your exposure then you can easily do so by reorienting antennas away from the user or placing he antennas at a greater separation distance then recommended.

This Device Meets FCC Guidelines for Exposure to Radio Waves

The Cisco Catalyst Wireless 9163E Series Outdoor AP device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in FCC Part 1.1310. The guidelines are based on IEEE ANSI C 95.1 (92) and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

The device has been tested and found compliant with the applicable regulations as part of the radio certification process.

The US Food and Drug Administration has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices. The FCC recommends that if you are interested in further reducing your exposure then you can easily do so by reorienting antennas away from the user or placing the antennas at a greater separation distance then recommended or lowering the transmitter power output.

This Device Meets the Industry Canada Guidelines for Exposure to Radio Waves

The Cisco Catalyst Wireless 9163E Series Outdoor AP device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in Health Canada Safety Code 6. The guidelines include a substantial safety margin designed into the limit to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

Health Canada states that present scientific information does not indicate the need for any special precautions for the use of wireless devices. They recommend that if you are interested in further reducing your exposure you can easily do so by reorienting antennas away from the user, placing the antennas at a greater separation distance than recommended, or lowering the transmitter power output.

Cet appareil est conforme aux directives internationales en matière d'exposition aux fréquences radioélectriques

Cet appareil de la gamme Cisco Catalyst Wireless 9163E Series Outdoor AP comprend un émetteur-récepteur radio. Il a été conçu de manière à respecter les limites en matière d'exposition aux fréquences radioélectriques (champs électromagnétiques de fréquence radio), recommandées dans le code de sécurité 6 de Santé Canada. Ces directives intègrent une marge de sécurité importante destinée à assurer la sécurité de tous, indépendamment de l'âge et de la santé.

Par conséquent, les systèmes sont conçus pour être exploités en évitant que l'utilisateur n'entre en contact avec les antennes. Il est recommandé de poser le système là où les antennes sont à une distance minimale telle que précisée par l'utilisateur conformément aux directives réglementaires qui sont conçues pour réduire l'exposition générale de l'utilisateur ou de l'opérateur.

Santé Canada affirme que la littérature scientifique actuelle n'indique pas qu'il faille prendre des précautions particulières lors de l'utilisation d'un appareil sans fil. Si vous voulez réduire votre exposition encore davantage, selon l'agence, vous pouvez facilement le faire en réorientant les antennes afin qu'elles soient dirigées à l'écart de l'utilisateur, en les plaçant à une distance d'éloignement supérieure à celle recommandée ou en réduisant la puissance de sortie de l'émetteur.

Additional Information on RF Exposure

You can find additional information on the subject at the following links:

- Cisco Systems Spread Spectrum Radios and RF Safety white paper at this URL: http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/rfhr_wi.htm
- FCC Bulletin 56: Questions and Answers about Biological Effects and Potential Hazards of Radio Frequency Electromagnetic Fields
- FCC Bulletin 65: Evaluating Compliance with the FCC guidelines for Human Exposure to Radio Frequency Electromagnetic Fields

You can obtain additional information from the following organizations:

- World Health Organization Internal Commission on Non-Ionizing Radiation Protection at this URL: www.who.int/emf
- United Kingdom, National Radiological Protection Board at this URL: www.nrpb.org.uk
- Cellular Telecommunications Association at this URL: www.wow-com.com
- The Mobile Manufacturers Forum at this URL: www.mmfai.org

Declaration of Conformity Statements

All the Declaration of Conformity statements related to this product can be found at the following location: https://pas.cisco.com/pdtcnc/#/