Cisco Wireless 9174I Series Wi-Fi 7 Access Point Hardware Installation Guide

Cisco Wireless 9174 Series Access Points
Updated December 19, 2025

© 2025 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Hardware License

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

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

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

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

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

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

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

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

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

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

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

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

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

Topics included

1 About the Access Point....6

Introduction to Cisco Wireless 9174I Wi-Fi 7 Access Point....7

Cisco Wireless 9174I Wi-Fi 7 Access Point features....7

AP model numbers and regulatory domains....9

Antennas and radios....9

2 Hardware Features....12

Access point views, ports, and connectors....13

Connectors and ports on the AP....13

Checking the access point LEDs....14

3 Installing the Access Point....18

Access point mounting and installation....19

Package contents....19

Unpack the access point....19

Cisco orderable accessories....19

Configure - On-premises (Cisco Catalyst Wireless Controllers) 20

Preinstallation configuration - Cisco Meraki mode....24

Mount the access point....25

Power the access point....26

Deploy the access point on a wireless network....26

4 Troubleshooting....28

Troubleshooting and diagnostics....29

Using the reset button....29

Troubleshooting the access point to Cisco controller join process....29

Important information for controller-based deployments....30

Configuring DHCP option 43....31

5 Safety Guidelines and Warnings....34

Safety instructions....35

6 Declarations of Conformity and Regulatory Information....36

Compliance and regulatory information....37

Manufacturers Federal Communication Commission Declaration of Conformity Statement....37

VCCI Statement for Japan....38

Canadian Compliance Statement....39

European Community, Switzerland, Norway, Iceland, and Liechtenstein Compliance.....41
United Kingdom Compliance.....41
Administrative Rules for Cisco Wireless Access Points in Taiwan.....42
Operation of Cisco Wireless Access Points in Brazil.....42
Declaration of conformity for RF exposure.....43
Declaration of Conformity Statements.....45

1 About the Access Point

Topics:

- Introduction to Cisco Wireless 9174I Wi-Fi 7 Access Point

Introduction to Cisco Wireless 9174I Wi-Fi 7 Access Point

Introduces the access point by describing its key wireless features, available model numbers, associated regulatory domains, and hardware details such as antennas and radios, including specifics on internal antennas and supported operating frequencies.

The Cisco Wireless 9174I Wi-Fi 7 Access Point is an enterprise-class device that supports tri-band (2.4 GHz, 5 GHz, 6 GHz) and dual-band radio, where the combination serves as a eight or ten spatial-stream wireless 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 known as Cisco DNA Center) on-premises
- Cisco Wireless Controllers
- Meraki cloud-based stack

A full listing of the AP's features and specifications is provided in the *Cisco Wireless 9174I Wi-Fi 7 Access Points Data Sheet*.

Cisco Wireless 9174I Wi-Fi 7 Access Point features

The CW9174I AP is a tri-band Wi-Fi 7 enterprise indoor access point. It is designed for seamless integration with the Cisco Catalyst 9800 Series Wireless Controller and Meraki dashboard. This AP delivers superior connectivity, expanded coverage, and support for advanced IoT applications. The AP includes the following hardware and supporting features:

- **Radio and Wireless Capabilities**
  - Wi-Fi 7 radios supporting 2.4 GHz, 5 GHz, and 6 GHz frequencies with integrated omnidirectional antennas.
  - The AP operates in tri-band mode with 10 spatial stream with 2.4 GHz (2x2:2), 5 GHz (4x4:4), 6 GHz (4x4:4), or in dual-band mode with 8 spatial stream as 2.4 GHz (4x4:4), and 5 GHz (4x4:4).
  - Dedicated scanning/AUX radio for real-time network monitoring and optimization.
  - Integrated Bluetooth Low Energy (BLE): Enables IoT applications, such as location tracking and wayfinding.
  - USB port for optional CW-ACC-GPS1= GPS module and other accessories
  - Multiuser Multiple-Input, Multiple-Output (MU-MIMO) for simultaneous uplink and downlink connections.
  - Orthogonal Frequency Division Multiple Access (OFDMA) for efficient traffic scheduling and resource utilization.
  - Spatial Reuse (BSS Coloring), enabling differentiation between multiple basic service sets for increased transmission efficiency.
  - Target Wake Time (TWT): An energy-saving mode that allows battery-powered devices to stay asleep and wake only at predefined intervals for data exchange, optimizing energy efficiency.
  - Multi-Link Operation (MLO): Multi-Link Operation (MLO) allows Multi-Link Devices (MLDs) to maintain associations and simultaneously transmit data across multiple frequency bands, including 2.4-GHz, 5-GHz, and 6-GHz band.
  - Preamble Puncturing: Preamble puncturing allows Extremely High Throughput (EHT) stations to transmit and receive Physical Layer Protocol Data Units (PPDUs) efficiently by omitting signals in unused 20-MHz subchannels, even with bandwidth interference like rogue APs.
- **Power and Connectivity**
  - Ethernet Port: Supports the following speeds: 100 Mbps, 1 Gbps, 2.5 Gbps, and 5 Gbps.

- Power over Ethernet (PoE): Full radio functionality, 2.5Gbps uplink and 2.5W of USB with 802.3at PoE. Full 5Gbps uplink and 9W USB available when used with 802.3bt class 5 PoE.

  > **Note**
  >
  > Before deployment, verify that all PoE injectors and switches provide the necessary power budget to enable all access point features.

- DC power jack

- **Ethernet Cable Requirements**
  - CAT 5E or above required, CAT 6/6A (recommended): Recommended for distances up to 100m.
  - Environmental Considerations: Avoid routing cables near high-interference sources such as electrical panels or motors. Ensure cable installations comply with local building and fire safety codes.

- **Intelligent Network Capabilities**
  - CleanAir Pro Technology: Provides advanced spectrum intelligence for 2.4 GHz, 5 GHz, and 6 GHz bands. Supports high-speed spectrum analysis across channel widths from 20 MHz to 160 MHz. The technology identifies and mitigates interference sources, optimizing network performance in real-time.

- **Operating Modes**
  - Local Mode: It is the default mode for client servicing, which utilizes CAPWAP tunnels for centralized management. This mode offers central switching capabilities, which handles management and data traffic.
  - FlexConnect Mode: FlexConnect mode allows local data switching, and enables continued operation during controller disconnection.
  - Monitor Mode: The mode acts as a dedicated sensor for Intrusion Detection Systems (IDS), rogue AP detection, and Location-based services (LBS).
  - Sniffer Mode: Sniffer mode captures and forwards wireless packets for remote analysis using tools like Wireshark or AiroPeek NX. It also includes metadata like timestamps, signal strength, and packet size.

    > **Note**
    >
    > Requires the receiving server to be on the same VLAN as the controller management VLAN.

  - Site Survey Mode: This mode enables RF parameter configuration for site survey investigations, and simplifies network planning and installation.
  - SDA/Fabric Mode: The SDA mode supports Software-Defined Access (SD-Access) for advanced segmentation and policy enforcement.

- **External Interfaces**
  - USB Port: USB ports supports additional device connectivity for enhanced flexibility.
  - Uplink Ethernet (100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps)

- **Software Features**
  - Intelligent Capture: It probes the network to provide deep diagnostic insights, enabling troubleshooting latency, interference, and other performance issues.
  - Cisco Catalyst Center Support: The support integrates with CCS Catalyst Center to enable CCS Spaces for location services.
  - Cisco Identity Services Engine (ISE) support: Integration with ISE for advanced security and network access control.

AP model numbers and regulatory domains

AP Type	Product ID	Details
Access Point for indoor environments, with internal antennas and external antenna connector.	CW9174I	Wi-Fi 7 AP, tri-band, 802.11be with internal antennas

With the new Wi-Fi 7 APs, Cisco now has one AP portfolio that can be used either with the Meraki cloud native network or Catalyst on-premise controller-based deployments. With the introduction of the one AP portfolio, it is essential to have a single product ID (PID) at manufacturing, to simplify logistics or operations. This AP model is designed for global use under a single PID. To verify approval and to identify the regulatory domain that corresponds to a particular country, see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html. Regulatory approvals are continually updated as they are obtained.

Antennas and radios

The following sections provide detailed information about the AP's antennas and radios.

Internal antennas

The Cisco Wireless 9174I AP (CW9174I) has the following list of internal antennas:

- Four Wi-Fi serving antennas with a dedicated 2.4-GHz radio and a 5-GHz radio
- Four Wi-Fi serving antennas with a dedicated 6-GHz radio
- One internal single-band antenna with a dedicated 2.4-GHz IoT radio
- Two tri-band antennas with a dedicated 2.4 GHz, 5-GHz, and 6-GHz Aux radio

Operating frequency and effective isotropic radiated power

Table 1: Cisco CW9174I AP values for European Union (CE) region

Evaluation mode	Frequency range (MHz)	EIRP power limit (dBm)
2.4GHz WLAN	2400-2483.5	20 in 2x2 or 23 in 4x4 mode
5GHz WLAN B1	5150-5250	23
5GHz WLAN B2	5250-5350	23
5GHz WLAN B3	5470-5725	28
5GHz WLAN B4	5725-5875	14
(EN 300 440 V2.2.1)		

Evaluation mode	Frequency range (MHz)	EIRP power limit (dBm)
6GHz WLAN (Draft EN 303 687)	5945-6425	Indoor use only per EN 303 687, max 23 dBm EIRP
Bluetooth	2400-2483.5	10
IEEE 802.15.4 (Zigbee)	2400-2483.5	9

Table 2: Cisco CW9174I values for United Kingdom region

Evaluation mode	Frequency range (MHz)	EIRP power limit (dBm)
2.4GHz WLAN	2400-2483.5	20
5GHz WLAN B1	5150-5250	23
5GHz WLAN B2	5250-5350	23
5GHz WLAN B3	5470-5725	28
5GHz WLAN B4 (IR 2030)	5725-5850	23
6G WLAN (IR 2030)	5945-6425	Indoor use only per IR 2030, maximum 24 dBm EIRP
Bluetooth	2400-2483.5	10
IEEE 802.15.4 (Zigbee)	2400-2483.5	9

Note

6 GHz operation is restricted to indoor use per IR 2030.

2 Hardware Features

Topics:

- Access point views, ports, and connectors

This chapter describes the hardware features of Cisco Wireless 9174I Wi-Fi 7 Access Point and contains the following sections:

Access point views, ports, and connectors

Describes the physical layout of access points, detailing the locations and functions of connectors and ports, and explains procedures for checking LED indicators to assist with hardware identification and status verification.

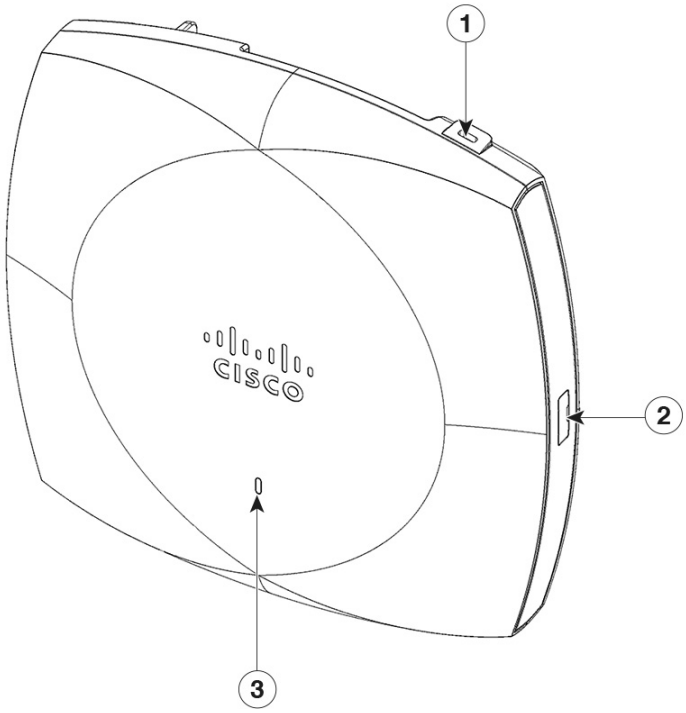
Cisco Wireless 9174I Wi-Fi 7 Access Point has multiple options that you can use to power the AP. For information about connectors and ports for the AP models, see Connectors and ports on the AP on page 13.

Connectors and ports on the AP

The following figures show the available ports on the AP:

CW9174I face view

Figure 1: CW9174I face view



1 Kensington lock slot

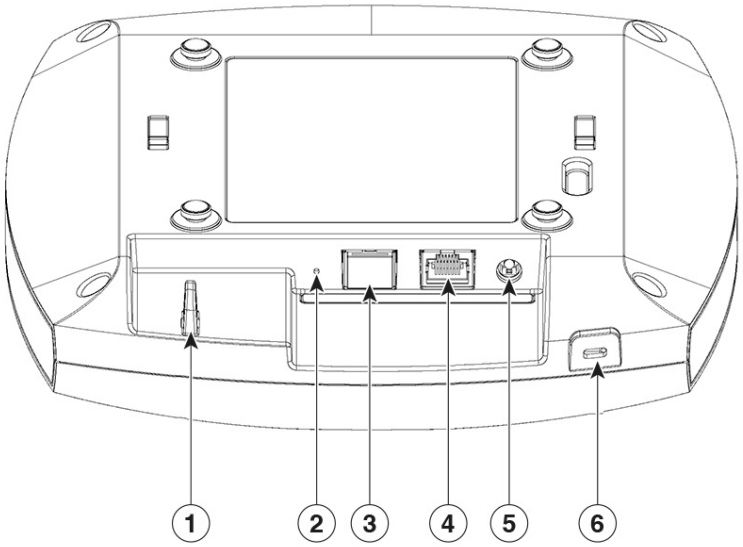
2 USB 2.0 port

3 Status LED

For information on the LED status, see Checking the access point LEDs on page 14.

CW9174I top view

Figure 2: CW9174I top view with connectors and ports



1	Security hasp for padlocking AP to mounting bracket	4	Ethernet port 0
2	Reset button For information about how to use the Reset button, see the Using the reset button on page 29 section	5	DC jack
3	RJ-45 console port Default baud rate is 115200.	6	Kensington lock slot

Checking the access point LEDs

The location of the access point status LED is shown in Connectors and ports on the AP on page 13.

Note

- Regarding LED status colors, it is expected that there might 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.
- When the AP is in Meraki management mode, the LED status indicators convey the status differently from the Cisco APs.

The access point status LED indicates various conditions, which are described in the following table.

Table 3: LED status indications

Message Type	LED State	Message Meaning
Association status	Green 	Normal operating condition, but no wireless client is associated
	Blue 	Normal operating condition, at least one wireless client is associated
Boot loader status	Green 	Executing boot loader
Boot loader error	Blinking Green 	Boot loader signing verification failure
Operating status	Blinking Blue 	Software upgrade in progress
	Alternating between Green and Red 	Discovery or join process in progress
Access point operating system errors	Cycling through Red-Off-Green-Off-Blue-Off 	General warning; insufficient inline power
Top right ethernet LED	Off	Link speed is 10Mbps or disconnected
	Orange 	Link speed is 100, or 1000 Mbps
	Green 	Link speed is 2.5 Gb, 5 Gb, or 10 Gb
Top left ethernet LED	Blinking Green 	Activity indicator for received signal or transmitted signal

Table 4: LED status indications for Meraki

Message type	LED state	Message meaning
Boot status	Orange 	AP is booting (permanent Orange suggests hardware issue)
Initialization status	Rainbow	AP is initializing/scanning
Upgrade status	Blinking Blue	AP is upgrading

Message type	LED state	Message meaning
Gateway mode (no clients)	Green 	AP in Gateway mode with no clients
Gateway mode (with clients)	Blue 	AP in Gateway mode with clients
Uplink status	Blinking Orange	AP can't find uplink

3 Installing the Access Point

Topics:

- Access point mounting and installation

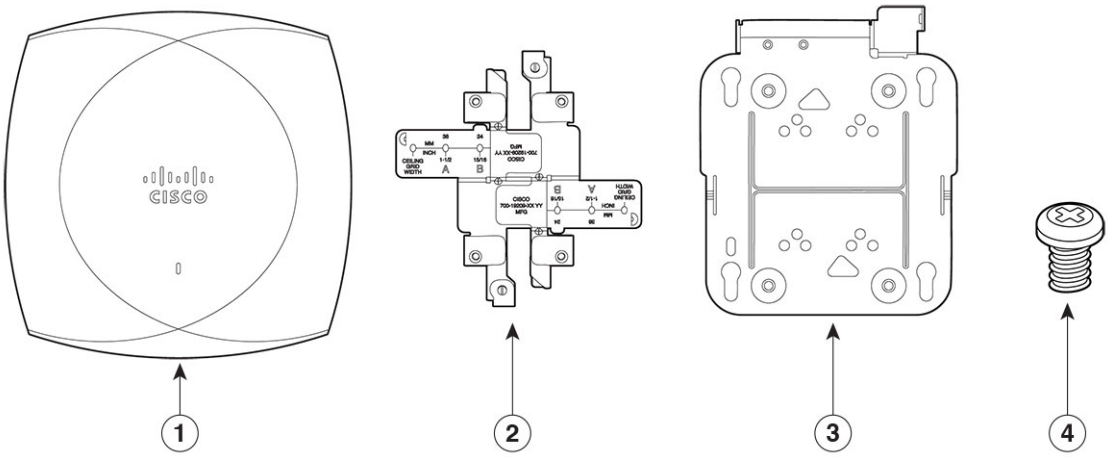
Installing an AP involves the following high-level tasks.

Access point mounting and installation

Details access point mounting and installation, covering package contents, unpacking procedures, available Cisco accessories, preinstallation configuration for both Catalyst and Meraki modes, mounting options, powering instructions, and guided deployment on a wireless network.

Package contents

Each AP package contains the following items:



1	CW9174I access point
2	AIR-AP-T-RAIL-R
3	AIR-AP-BRACKET-1
4	Screws

- One CW9174I AP
- Default mounting brackets: Adjustable ceiling-rail clips AIR-AP-T-RAIL-R= and AIR-AP-BRACKET-1=
- Orderable optional mounting brackets: AIR-AP-T-RAIL-F=, and AIR-AP-BRACKET-2=
- Cisco product documentation and pointer card

Unpack the access point

Procedure

1. Unpack and remove the access point and the selected mounting accessory kit from the shipping box.
2. Return the packing material to the shipping container and save it for future use.
3. Verify that you have received all the items you ordered. If any item is missing or is damaged, contact your Cisco representative or reseller for instructions.

Cisco orderable accessories

You can order the following accessories separately, from Cisco:

- MA-PWR-50WAC
  - Description: Cisco 50W AC Power Supply
  - Power Specifications: 50W, 54VDC
- AP-mounting brackets to mount the AP

Mounting brackets	Description
AIR-AP-BRACKET-2=	For electrical or network boxes above ceiling mounts
AIR-AP-T-RAIL-F=	Flush ceiling grid clip
AIR-CHNL-ADAPTER=	T-RAIL channel adapter

- Power injectors when Power over Ethernet (PoE) is not available

Power supply	Description
CW-INJ-8	Meraki 802.3bt PoE injector Power Specifications: 60W, 10 Gbps Ethernet For more information, see *Cisco Power Injector CW-INJ-8 Quick Start Guide*.
AIR-PWRINJ7=	Mid-span power injector AIR-PWRINJ7= when (PoE) is not available Power specifications: 50W, 56VDC For more information, see the *Cisco Multigigabit 802.3bt Power Injector*.
AIR-PWRINJ6=	[1] Power Specifications: 30W, 55VDC For more information, see the *Cisco Aironet Power Injector AIR-PWRINJ6= Installation Guide*.
MA-INJ-6-x	Meraki 802.3bt PoE injector Power Specifications: 60W, 55VDC For more information, see the *MA-INJ-6 Meraki Multigigabit 802.3bt Power over Ethernet Injector*.

Configure - On-premises (Cisco Catalyst Wireless Controllers)

Configuration - Cisco Catalyst Mode

Controller discovery process

To support the CW9174I AP, the controller must be running Cisco IOS XE 17.18.2 or a later release. For more information, see the *Cisco Catalyst 9174I Series Access Points Data Sheet*.

[1] If 802.3af is used, the system function will be disabled.

A 802.3at power injector when PoE is not available

Guidelines and limitations

- It is not possible to edit or query an access point using the controller CLI if the name of the access point 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 access point might not join the controller because its certificate may not be valid for that time.

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

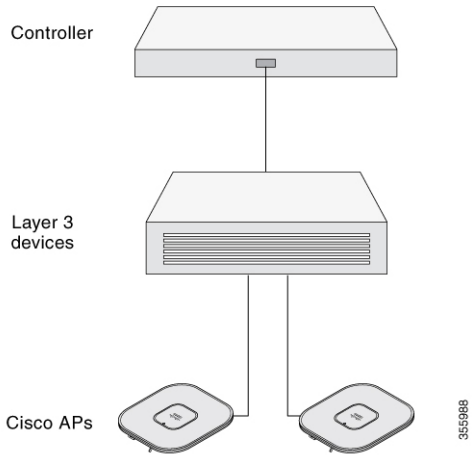
- Locally stored controller IP address discovery: If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point. For more information about priming, see Performing a preinstallation configuration on page 21.
- DHCP server discovery: This feature uses DHCP Option 43 to provide controller IP addresses to the access points. 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 31.
- DNS discovery: The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point 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 access point sends discovery requests to these controllers.

Performing a preinstallation configuration

The following procedures describe the processes to ensure that your AP installation and initial operation go as expected.

> **Note**
>
> Performing a preinstallation configuration is an optional procedure. If your network controller is properly configured, you can install your AP in its final location and connect it to the network from there. For more information, see Deploy the access point on a wireless network on page 26.

The following illustration shows the preinstallation configuration setup:



Perform the following steps:

Before you begin

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

- Enable Layer 3 connectivity between APs and wireless controller's wireless management interface.
- Configure the switch to which your AP has to attach. See the *Cisco Wireless Controller Configuration Guide* for the release you are using, for additional information.
- Ensure that the DHCP is enabled on the network. The AP must receive its IP address through DHCP.

> **Note**
>
> An AP is assigned an IP address from the DHCP server 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.

- CAPWAP UDP ports must not be blocked in the network.
- 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, see the product documentation. See also Configuring DHCP option 43 on page 31 for more information.

> **Note**
>
> The AP requires an 5G Ethernet link to prevent the Ethernet port from becoming a bottleneck for traffic.

Procedure

1. Power the AP using a supported power source.

   See Power the access point on page 26.

   - The AP checks for cloud connectivity and attempts to connect to the Meraki dashboard.
   - If the AP is unable to find cloud connectivity, it uses fast offline migration to look for a Cisco Catalyst 9800 Controller. The AP uses DHCP, DNS, and L2 discovery mechanisms for the migration. For more information, see *Global Use Access Points*.

     > **Note**
     >
     > The AP should not have cloud connectivity from its subnet if it intends to connect to a controller. If the AP joins a Meraki Dashboard, it can be later migrated to a controller.

   Once the AP discovers the controller, it performs a firmware image download and reboots.
2. If the preinstallation configuration is successful, the Status LED is green, indicating normal operation. Disconnect the AP and mount it on the location at which you intend to deploy it on the wireless network.
3. If your AP does not indicate normal operation, turn it off and repeat the preinstallation configuration.

Note

When you are installing a Layer 3 access point on a subnet that is different from the Catalyst 9800 controller, ensure that the following setup is configured:

- A DHCP server is reachable from the subnet on which you plan to install the AP.
- The subnet has a route back to the controller.
- This route has destination UDP ports 5246 and 5247 open for CAPWAP communications.
- The route back to the primary, secondary, and tertiary controller allows IP packet fragments.
- If address translation is used, the access point and the controller have a static 1-to-1 NAT to an outside address. Port Address Translation is not supported.

Preinstallation checks and installation guidelines

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

You should have the following information about your wireless network available:

- Access point locations
- Access point mounting options:
  - Below a suspended ceiling
  - on a flat horizontal surface
  - on top of a desk

Note

You can mount the access point above a suspended ceiling, but you must purchase additional mounting hardware. For more information, see Mount the access point on page 25.

- Access point power options: Use either of the following options to power the AP:
  - Cisco-approved power injector
  - PoE with a supporting switch
  - DC power jack

Note

- The power adapter must be certified to IEC/EN 62368-1 (or equivalent IT/telecom safety standard) by a Nationally Recognized Testing Laboratory (NRTL) or other authority accepted in the country of use (UL, CSA, ETL, TUV, CE,CCC, PSE, BIS, INMETRO). The adapter must meet the following minimum specifications: Rated output of 42.5 to 57VDC, min 0.701A-0.941A, Tmax of 50C minimum, altitude of 3048m minimum.
- If 802.3af is used, all the radios get switched off. Ethernet gets downgraded to 1 GbE. The Wi-Fi client serving radios and IoT radio are switched off.

- Operating temperature:
  - CW9174I: 32° F to 122° F (0° C to 50° C)

Note

When installing the AP in an environment where the ambient temperature is in the range of 104° and 122° F (>40° and 50° C), the access point configuration changes.

- 10SS mode: 5G and 6G radios scale to 2x2, Ethernet remains at 5G, and the USB remains enabled.
- 8SS mode: 2G and 5G radios scale to 2x2, Ethernet remains at 5G, and the USB remains enabled.

- 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 make a site map showing access point 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.

Preinstallation configuration - Cisco Meraki mode

Perform a preinstallation configuration - Cisco Meraki mode

This is a brief overview of the steps required to add the access point to your network. For more information about creating, configuring and managing Meraki wireless networks, see the Cisco Meraki documentation.

Before you begin

You should complete these steps before going on-site to perform an installation.

Follow these steps to configure dashboard network.

Procedure

1. Log in to Cisco Meraki dashboard. If this is your first time, create a new account.
2. Find the network to which you plan to add your APs or create a new network.
3. Add your APs to your network. You will need your Meraki order number (found on your invoice) or the Cloud ID of each AP, which looks like Qxxx-xxxx-xxxx, and is found on the bottom of the unit. You will also need your license key, which you should have received via email.
4. Go to the map or floor plan view and place each AP on the map by clicking and dragging it to the location where you plan to mount it.

What to do next

For more information about onboarding access points, see *Wireless Access Points Quick Start Guide*.

Mount the access point

Cisco Wireless 9174I Wi-Fi Access Point can be mounted in the following places:

- Suspended ceiling
- Hard ceiling
- Wall
- Electrical or network box
- Above a suspended ceiling

For detailed instructions on mounting the AP, see the *Access Point Mounting Instructions* document at:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mounting/guide/apmount.html.

The standard mounting hardware supported by the AP are listed in the following table.

Table 5: Brackets and clips to mount the AP

Mounting type	Part number	Description
Brackets[2][3][4]	AIR-AP-BRACKET-1	Low-profile bracket: Used for ceiling-mount installations. (This is the default option.)
	AIR-AP-BRACKET-2	Universal bracket: Used for wall or electrical box installations.
Clips	AIR-AP-T-RAIL-R	Ceiling grid clip (recessed mounting). (This is the default option.)
	AIR-AP-T-RAIL-F	Ceiling grid clip (flush mounting).
	AIR-CHNL-ADAPTER	Optional adapter for channel-rail ceiling grid profile.

[2] Mount the AP using no less than four screw holes on a bracket.
[3] AIR-AP-BRACKET-3 is not compatible for use with Cisco CW9174I access points.
[4] You can also use the *in-tile* mounting options available from third parties. For more information, see the access point data sheet.

When mounting the AP in areas where there is a possibility of the AP being knocked off the mounting bracket, use the lock hasp at the back of the AP to lock it to the bracket.

Power the access point

Caution

Ensure that the AP is powered using a Underwriters' Laboratories-compliant (UL-compliant) PoE power source. You must connect the unit only to the PoE network, without routing to the outside plant.

Note

Actual power consumption may vary depending on access point usage. It is recommended that you ensure that Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol is enabled to allow proper power negotiation.

Power source	2GHz Radio	5GHz Radio	6G Radio	Link Speed	USB	Max power consumption	Configuration
802.3bt/Class 5/UPOE, DC Jack	2x2	4x4	4x4	5G	Y (9W)	37.3W	10SS, Tri-band
802.3bt/Class 5/UPOE, DC Jack	4x4	4x4	-	5G	Y (9W)	32.1W	8SS, Dual-band
802.3at/POE+	2x2	4x4	4x4	2.5G	Y (2.5W)	25.5W	10SS, Tri-band
802.3at/POE+	4x4	4x4	-	2.5G	Y (2.5W)	25.5W	8SS, Dual-band
802.3af/POE	-	-	-	1G	N	13.9W	All radios off

Deploy the access point on a wireless network

After you mount the access point, follow these steps to deploy it on a wireless network:

Procedure

1. Connect and power up the access point.
2. Observe the access point LED.

   For LED status descriptions, see Checking the access point LEDs on page 14.

   - When you power up the access point, it begins a power-up sequence that you can verify by observing the access point LED. If the power-up sequence is successful, the discovery and join process begins. During this process, the LED blinks green, red, and off sequentially. When the access point joins a controller, the LED is green if no clients are associated, or blue if one or more clients are associated.
   - If the LED is not on, it is most likely that the access point is not receiving power.
   - If the LED blinks sequentially for more than five minutes, the access point is unable to find its primary, secondary, and tertiary controller. Check the connection between the access point and the Cisco Wireless Controller, and

be sure that the access point and the Cisco Wireless Controller are either on the same subnet or that the access point has a route back to its primary, secondary, and tertiary Cisco Wireless Controller. Also, if the access point is not on the same subnet as the Cisco Wireless Controller, ensure that there is a properly configured DHCP server on the same subnet as the access point.

4 Troubleshooting

Topics:

- Troubleshooting and diagnostics

Troubleshooting information.

Troubleshooting and diagnostics

Introduces troubleshooting and diagnostics techniques for access points, highlighting how to use the mode button, address controller join processes, understand vital controller-based deployment details, and configure DHCP Option 43 for seamless network integration.

Using the reset button

Using the **Reset** button (see Figure 2: CW9174I top view with connectors and ports on page 13), you can reset the AP to factory default.

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

1. Unplug the AP from the power source.
2. Hold the **Reset** button.
3. Power on the AP.

   Press, and continue to press the **Reset** button for the duration corresponding to your requirements listed in the table below:

0-5 seconds	Blinks green for Meraki mode, and blue for Catalyst mode.
> 10 seconds	The AP undergoes configuration wipe.
> 20 seconds	Ap resets completely and enters maintain management mode.
> 30 seconds	Configures FIPS in Catalyst mode.
> 60 seconds	The LED light turns solid pink, which indicates a factory reset.
> 90 seconds	LED turns off.

Troubleshooting the access point to Cisco controller join process

Note

As specified in the *Cisco Wireless Solutions Software Compatibility Matrix*, ensure that your controller is running Cisco IOS XE 17.18.2 or a later release to support the Cisco CW9174I 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.

If the CW9174I is in Meraki Management mode, it does not attempt to join the Cisco Catalyst 9800 Series Wireless Controller. For more information, see *Cisco Wireless Global Use Access Points Deployment Guide*.

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 trace commands on the Cisco Catalyst 9800 Series 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 AP 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** *syslog-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 Cisco CW9174I APs:

- 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 debug purposes.

> **Note**
>
> The default band rate is 115200.

- All the 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 access points, enabling them to find and join a controller.

The following is a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with Cisco Catalyst lightweight access points. For other DHCP server implementations, see the product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.

> **Note**
>
> DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

The Cisco CW9174I access point uses the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point DHCP Vendor Class Identifier (VCI) string (DHCP Option 43). The VCI string for the Cisco CW9174I access point is:

Cisco Wireless AP CW9174I

The following is the format of the TLV block:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses x 4
- Value: IP addresses of the wireless controller management interfaces listed sequentially in Hex code.

To configure DHCP Option 43 in the embedded Cisco IOS DHCP server, follow these steps:

> **Note**
>
> The procedure describes configuration process for an AP that has completed the intial discovery process. For more information on day 0 workflow, see Global Use Access Points.

Procedure

1. Enter the configuration mode

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

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

Here:

<*pool name*> is the name of the DHCP pool, such as AP9174I.

<*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.

3. Add the Option 43 line using the following syntax:

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

The hex string is assembled by concatenating the following TLV values:

Type + Length + Value

For example, if 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), and the IP addresses translate to 0a7e7e02 and 0a7f7f02. Assembling the string then yields f1080a7e7e020a7f7f02. The resulting Cisco IOS command added to the DHCP scope is **option 43 hex f1080a7e7e020a7f7f02**.

5 Safety Guidelines and Warnings

Topics:

- Safety instructions

Safety instructions

Introduces key safety instructions for equipment handling, operation, and maintenance, focusing on important precautions and warnings to prevent hazards and ensure user safety.

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

Warning

IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number at the beginning of each warning statement to locate its translation in the translated safety warnings for this device.

SAVE THESE INSTRUCTIONS



Warning

This product relies on the building's installation for short-circuit (overcurrent) protection. To reduce risk of electric shock or fire, ensure that the protective device is rated not greater than: **20 A**

Warning

To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

DANGER

In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.87 inches (20 cm) or more from the body of all persons. Statement 332

6 Declarations of Conformity and Regulatory Information

Topics:

- Compliance and regulatory information

This section provides declarations of conformity and regulatory information for the . You can find additional information at: https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.

Compliance and regulatory information

Details global compliance and regulatory requirements, providing manufacturers' conformity statements, country-specific certifications for Japan, Canada, the European Community, the UK, Taiwan, and Brazil, as well as comprehensive RF exposure guidelines, operational procedures, and additional declaration resources.

Manufacturers Federal Communication Commission Declaration of Conformity Statement



Access Point model	Certification number
CW9174I	UDX-600218010

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 conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.
3. For 6 GHz operation, this device includes authorization for both Low Power Indoor (LPI) operation and Standard Power (SP) operation, as permitted by the applicable FCC regulatory grant. LPI operation is restricted to indoor use only. Standard Power operation is permitted only when operating under Automated Frequency Coordination (AFC) and in accordance with applicable regulatory grant and deployment requirements.

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 this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try 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
- This device is intended for professional installation and must be installed and configured in accordance with Cisco instructions and applicable regulatory requirements

Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

6 GHz operating class restrictions

These restrictions apply to 6 GHz operation based on the operating class (LPI or SP):

Low Power Indoor (LPI) Access Points

- FCC regulations restrict Low Power Indoor (LPI) operation to indoor use only.
- LPI operation is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation is permitted in large aircraft flying above 10,000 feet in the 5.925-6.425 GHz band.
- Transmitters in the 5.925-7.125 GHz band are prohibited from operating to control or communicate with unmanned aircraft systems.

Standard Power (SP) Access Points

- Operation is prohibited on oil platforms, cars, trains, boats, and aircraft.
- Standard Power operation is permitted only under Automated Frequency Coordination (AFC) and in accordance with applicable regulatory grant and deployment requirements.

VCCI Statement for Japan

Warning

Warning

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

Warning

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

Access Point model:

CW9174I

Guidelines for Operating Cisco Wireless Access Points in Japan

This section provides guidelines for avoiding interference when operating Cisco Wireless 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・医療用機器のほかエ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、近くで移動体臓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（例えぱ、ノく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撒別用の特定，ト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**

Canadian Compliance Statement

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes:

- L'appareil ne doit pas produire de brouillage.
- L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Wi-Fi 7 Device (6 GHz Band)

Operation in the 6 GHz band is subject to the following restrictions:

- Operation shall be limited to indoor use only.

- Devices shall not be used for control of or communications with unmanned aircraft systems.
- Devices shall not be used on oil platforms.
- Devices shall not be used on automobiles.
- Devices shall not be used on trains.
- Devices shall not be used on maritime vessels.
- Devices shall not be used on aircraft, except for low-power indoor access points and indoor subordinate devices operating in the 5925-6425 MHz band, which may be used on large aircraft as defined in the Canadian Aviation Regulations, while flying above 3,048 metres (10,000 feet).

Appareil Wi-Fi 7 (bande de 6 GHz)

Le fonctionnement dans la bande de 6 GHz est soumis aux restrictions suivantes:

- Utilisation limitée à l'intérieur seulement.
- Les dispositifs ne doivent pas être utilisés pour commander des systèmes d'aéronef sans pilote ni pour communiquer avec de tels systèmes.
- Les dispositifs ne doivent pas être utilisés sur les plateformes de forage pétrolier.
- Les dispositifs ne doivent pas être utilisés dans les automobiles.
- Les dispositifs ne doivent pas être utilisés dans les trains.
- Les dispositifs ne doivent pas être utilisés sur les navires maritimes.
- Les dispositifs ne doivent pas être utilisés dans les aéronefs, à l'exception des points d'accès intérieurs de faible puissance et des dispositifs subordonnés intérieurs fonctionnant dans la bande de 5925 à 6425 MHz, qui peuvent être utilisés dans les gros aéronefs tel que défini dans le Règlement de l'aviation canadien, lorsqu'ils volent à une altitude supérieure à 3,048 mètres (10,000 pieds).

The device for 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.

Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont 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.

The transmitter module may not be co-located with any other transmitter or antenna.

Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

Low power indoor access points and indoor subordinate devices

- Operation shall be limited to indoor use only.
- Le fonctionnement doit être limitée à une utilisation à l'intérieur seulement.

Standard client devices

- The antenna height shall be determined by the installer or operator of the standard-power access point or fixed client device, or by automatic means. This information shall be stored internally in the device. Provision of accurate device information is mandatory. Information for antenna type(s), antenna models(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 4.5.4 (c) shall be clearly indicated.

- La hauteur de l'antenne doit être déterminée par l'installateur ou l'opérateur du point d'accès de puissance normale ou du dispositif client fixe, ou par des dispositifs automatiques. Cette information doit être enregistrée dans le dispositif. La fourniture d'information précise sur le dispositif est obligatoire. le ou les types d'antennes, le ou les modèles d'antennes et le ou les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la section 4.5.4 c. s'appliquant au masque de p.i.r.e. doivent être clairement indiqués.

Industry Canada

Access Point model	Certification number
CW9174I	6961A-600218010

European Community, Switzerland, Norway, Iceland, and Liechtenstein Compliance

The product carries the CE Mark:



This device is restricted to indoor use only when operating in the following frequency ranges:

- 5150-5350 MHz
- 5945-6425 MHz

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm (7.87 inches) between the radiator and your body.

This equipment is intended for use 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.

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.

Access Point model:

CW9174I

Manufacturer:

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA

United Kingdom Compliance

This device is restricted to indoor use only when operating in the following frequency ranges:

- 5150-5350 MHz
- 5945-6425 MHz

This equipment should be installed and operated with a minimum distance of 20 cm (7.87 inches) between the radiator and your body.

Access Point Model:

CW9174I

Manufacturer:

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA

Administrative Rules for Cisco Wireless Access Points in Taiwan

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

Traditional Chinese Translation

【低功率射頻器材技術規範】取得審驗證明之低功率射頻器材，非經核准，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。低功率射頻器材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。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材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。應避免影響附近雷達系統之操作。

【本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者】

English Translation

Without permission granted by the NCC, any company, enterprise, or user is not allowed to change frequency, enhance transmitting power, or alter original characteristics or performance of approved low power radio-frequency devices.

Low power radio-frequency devices shall not affect aircraft safety or interfere with legal communications. If interference is observed, operation shall be immediately discontinued until the condition is resolved.

Legal communications refer to radio communications operated in accordance with the Telecommunications Management Act. Low power radio-frequency devices must accept interference from legal communications or ISM radio wave radiated devices.

Operation should avoid affecting nearby radar syste

Access Point model	Certification number
CW9174I	TBD

Professional installation requirement

This device must be installed and configured by professional personnel.

This device is not intended for direct sale to the general public.

Operation of Cisco Wireless Access Points in Brazil

Figure 3: Brazil Regulatory Information



This section contains special information for operation of Cisco Wireless Access Points in Brazil.

Portuguese

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

English

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

equipamento Wi-Fi 7

O uso deste equipamento é restrito a ambientes fechados.

A operação é proibida em plataformas petrolíferas, automóveis, trens, embarcações e aeronaves, exceto em aeronaves de grande porte voando acima de 3.048 metros (10.000 pés).

Wi-Fi 7 Device

Operation of this device is restricted to indoor use only.

Operation is prohibited on oil platforms, automobiles, trains, maritime vessels, and aircraft, except on large aircraft operating above 3,048 meters (10,000 feet).

Access Point model	Certification number
CW9174I	TBD

Declaration of conformity for RF exposure

This section provides information on compliance with applicable regulatory requirements and international guidelines related to human exposure to radio frequency (RF) electromagnetic fields.

The Cisco CW9174I access point is designed to comply with applicable RF exposure requirements established by regulatory authorities and recognized international standards, including but not limited to:

- **United States**: 47 CFR Part 2, Subpart J
- **Canada**: Innovation, Science and Economic Development Canada (ISED) Safety Code 6
- **European Union**: Council Recommendation 1999/519/EC and applicable EN standards based on ICNIRP guidelines
- **International**: International Commission on Non-Ionizing Radiation Protection (ICNIRP) guidelines
- **Australia**: Applicable Australian Radiation Protection standards

To ensure compliance with these requirements, the Cisco CW9174I shall be installed and operated using **Cisco-approved antennas and accessories only**. The device is intended to be installed in a manner that maintains a minimum separation distance of **20 cm (7.87 inches)** between the radiating elements and all persons during normal operation, unless otherwise specified by applicable regional regulations.

The CW9174I includes radio transmitters and receivers and is designed to operate within established RF exposure limits, which incorporate substantial safety margins to ensure protection for all persons, regardless of age or health condition.

This device meets applicable international guidelines for exposure to radio frequency electromagnetic fields

The Cisco CW9171I device contains radio transmitters and receivers and is designed to operate within the limits for human exposure to radio waves established by applicable regulatory authorities and recognized international guidelines, which incorporate substantial safety margins to ensure the safety of all persons, regardless of age or health condition.

To maintain compliance with these requirements, the device shall be installed and operated in a manner that prevents direct contact with the antennas by the end user and maintains a minimum separation distance of **20 cm (7.87 inches)**

between the radiating elements and all persons during normal operation, unless otherwise specified by applicable regional regulations.

Separation Distance
20 cm (7.87 inches)

RF Exposure Compliance (FCC/ISED/International)

This device meets applicable regulatory requirements and international guidelines for human exposure to radio frequency electromagnetic fields.

The Cisco CW9171I access point contains radio transmitters and receivers and is designed to operate within the limits for RF exposure established by the Federal Communications Commission (FCC), Innovation, Science and Economic Development Canada (ISED), and other applicable regulatory authorities. These limits incorporate substantial safety margins to ensure the safety of all persons, regardless of age or health condition.

To maintain compliance with these requirements, the device shall be installed and operated in a manner that prevents direct contact with the antennas by the end user and maintains a minimum separation distance of **20 cm (7.87 inches)** between the radiating elements and all persons during normal operation, unless otherwise specified by applicable regional regulations.

The device has been evaluated and found compliant with the applicable RF exposure requirements as part of the radio certification process.

Table 6: Minimum Separation Distance

Frequency Band	Minimum Separation distance
2.4 GHz / 5 GHz / 6 GHz	20 cm (7.87 inches)

Conformité à l’exposition aux radiofréquences – Canada

Cet appareil est conforme aux exigences réglementaires applicables et aux directives internationales en matière d’exposition humaine aux champs électromagnétiques de radiofréquence.

L’appareil Cisco CW9171I comprend des émetteurs et récepteurs radio et a été conçu pour fonctionner dans les limites d’exposition aux radiofréquences établies par Innovation, Sciences et Développement économique Canada (ISDE), notamment le Code de sécurité 6 de Santé Canada, ainsi que par d’autres autorités réglementaires applicables. Ces limites intègrent des marges de sécurité importantes afin d’assurer la protection de toutes les personnes, indépendamment de l’âge ou de l’état de santé.

Afin de maintenir la conformité à ces exigences, l’appareil doit être installé et utilisé de manière à empêcher tout contact direct entre les antennes et l’utilisateur final, et à maintenir la distance minimale d’éloignement indiquée ci-dessous entre les éléments rayonnants et toute personne durant le fonctionnement normal, sauf indication contraire prévue par les réglementations régionales applicables.

Table 7: Distance minimale d’éloignement

Bande de fréquences	Distance minimale d’éloignement
2.4 GHz / 5 GHz / 6 GHz	20 cm (7.87 inches)

Note

Remarque : La distance minimale d'éloignement s'applique à toutes les bandes de fréquences prises en charge durant le fonctionnement normal, sauf indication contraire prévue par les réglementations régionales applicables.

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

- **Federal Communications Commission (FCC)**
  - **FCC Bulletin 56**: Questions and Answers about Biological Effects and Potential Hazards of Radio Frequency Electromagnetic Fields
  - **FCC Bulletin 65**: *Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields*

    https://www.fcc.gov/general/radio-frequency-safety-0

You can obtain additional information from the following organizations:

- Federal Communications Commission (FCC) – Radio Frequency Safety

  https://www.fcc.gov/general/radio-frequency-safety

- Innovation, Science and Economic Development Canada (ISED) – Safety Code 6

  https://www.canada.ca/en/health-canada/services/health-risks-safety/radiation/occupational-exposure-regulations/safety-code-6-radiofrequency-exposure-guidelines.html

- European Union – Council Recommendation 1999/519/EC on exposure to electromagnetic fields

  https://eur-lex.europa.eu/eli/reco/1999/519/oj

- Cellular Telecommunications Association at this URL:

  https://www.ctia.org

- The Mobile & Wireless Forum at this URL:

  https://www.mwfai.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/#/