



Cisco Wireless 9171I Series Wi-Fi 7 Access Point Hardware Installation Guide

First Published: 2025-12-19

Americas Headquarters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

About the Access Point 1

- Introduction to Cisco Wireless 9171I Wi-Fi 7 Access Point 1
- Cisco Wireless 9171I Wi-Fi 7 Access Point features 1
- AP model numbers and regulatory domains 4
- Antennas and radios 4
 - Internal antennas 4
 - Operating frequency and effective isotropic radiated power 5

CHAPTER 2

Hardware Features 7

- Access point views, ports, and connectors 7
 - Connectors and ports on the AP 7
- Checking the access point LEDs 9

CHAPTER 3

Installing the Access Point 13

- Package Contents 13
- Unpacking the access point 13
- Cisco orderable accessories 14
- Preinstallation configuration - Cisco Catalyst mode 15
 - Controller Discovery Process 15
 - Performing a preinstallation configuration 15
 - Preinstallation checks and installation guidelines 17
- Preinstallation Configuration - Cisco Meraki Mode 19
 - Perform a preinstallation configuration - Cisco Meraki mode 19
- Mount the access point 19
- Powering the access point 20
- Deploying the access point on a wireless network 21

CHAPTER 4**Troubleshooting 23**

- Using the reset button 23
- Troubleshooting the access point to Cisco controller join process 24
- Important information for controller-based deployments 25
- Configuring DHCP option 43 25

CHAPTER 5**Safety Guidelines and Warnings 27**

- Safety instructions 27

CHAPTER 6**Declarations of Conformity and Regulatory Information 29**

- Manufacturers Federal Communication Commission declaration of conformity statement 29
- VCCI statement for Japan 31
 - Guidelines for operating Cisco Wireless Access Points in Japan 31
- Canadian compliance statement 32
- European community, Switzerland, Norway, Iceland, and Liechtenstein compliance 33
- United Kingdom compliance 34
- Administrative rules for Cisco Wireless Access Points in Taiwan 34
- Operation of Cisco Wireless Access Points in Brazil 35
- Declaration of conformity for RF exposure 36
 - This device meets applicable international guidelines for exposure to radio frequency electromagnetic fields 36
 - RF Exposure Compliance (FCC/ISED/International) 37
 - Additional information on RF exposure 38
- Declaration of conformity statements 38



CHAPTER 1

About the Access Point

- [Introduction to Cisco Wireless 9171I Wi-Fi 7 Access Point, on page 1](#)
- [Cisco Wireless 9171I Wi-Fi 7 Access Point features, on page 1](#)
- [AP model numbers and regulatory domains, on page 4](#)
- [Antennas and radios, on page 4](#)

Introduction to Cisco Wireless 9171I Wi-Fi 7 Access Point

The Cisco Wireless 9171I Wi-Fi 7 Access Point (AP) is an enterprise-class device designed for indoor environments, delivering high-performance wireless solutions that

- Offers a migration path for existing MR36 and Cisco Catalyst 9105 Series Access Point customers.
- Functions as a converged platform, serving both Cisco Catalyst and Meraki customers with a common hardware architecture and industrial design.
- Operates in dual-radio tri-band configuration (Fixed 2.4 GHz and configurable 5 GHz or 6 GHz) with concurrent operation in two bands.

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 9171I Wi-Fi 7 Access Point Data Sheet](#).

Cisco Wireless 9171I Wi-Fi 7 Access Point features

The CW9171I Access Point (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.

Below are the hardware and supporting features:

- **Radios and Wireless Capabilities**

- Wi-Fi 7 radios supporting 2.4 GHz and 5 GHz or 6 GHz frequencies with integrated omnidirectional antennas.
- The AP operates in dual-radio tri-band mode with 4 spatial streams, allowing operation in (2.4 + 5 GHz) or (2.4 + 6 GHz).
- Supports Wi-Fi 7 (802.11be), as well as previous Wi-Fi standards up to, and including Wi-Fi 6 R2 and Wi-Fi 6E.
- Dedicated auxiliary scanning radio for real-time network monitoring and optimization.
- Integrated radio for Bluetooth/BLE 6.0+, Thread, and Matter.



Note Thread and Matter are planned to be supported in a future software release.

- Supports Modulation up to 4096 QAM.
 - Multi-Link Operation (MLO) for Multi-Link Devices (MLDs) to maintain associations and simultaneously transmit data across multiple frequency bands.
 - Orthogonal Frequency Division Multiple Access (OFDMA) for efficient traffic scheduling and resource utilization.
 - Channel Puncturing for efficient spectrum utilization.
 - Supports security features including WPA3 Beacon Protection, WPA3 SAE-PK, WPA3 192-bit, and GCMP for WPA2 and WPA3.
 - USB port for optional CW-ACC-GPS1= GPS module and other accessories.
- **Ports and Connectivity**
- Ethernet Uplink: One 2.5Gbps RJ45 Ethernet port, supporting 10/1000/2500Mbps speeds, VXLAN, CDP, LLDP, and MACSEC.
 - Power over Ethernet (PoE): Supports 802.3af, 802.3at, 802.3bt (PoE, PoE+, PoE++, UPOE). Full feature enablement requires 802.3at.



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

- USB Port: One USB-A connector (USB 2.0 spec) providing 4.5W power output.
- DC Power Jack: Supports external power supply (MA-PWR-50WAC).
- Console Port: One RJ45 Console port.

• **Ethernet Cable Requirements**

- CAT 5E or above required, CAT 6/6A: Required for 2.5 Gbps operation.
- 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.

• System Hardware and Mechanical

- Antennas: Integrated internal omnidirectional antennas.
- Security: Implements Cisco-TPM for secure boot and secure storage of device certificates, and includes a Kensington locking mechanism.
- LED Indicators: Supports multi-color (red, green, blue, white, violet, orange) system LEDs that are dimmable, and LED indicators on the Ethernet port for link/status.
- Form Factor: Indoor ceiling mount AP, with dimensions not exceeding (200mm x 200mm x 43.2mm max) and weight not exceeding 2.15 lbs (0.97 kg).
- Power Management: Includes circuitry to measure power consumption and the ability to control power by enabling/disabling radios, reducing spatial streams, turning USB port on/off, and controlling Ethernet port speed.

• Operating Modes with Controller

- Local Mode: Default mode for client servicing, utilizing CAPWAP tunnels for centralized management and offering central switching capabilities.
- FlexConnect Mode: Allows local data switching and enables continued operation during controller disconnection.
- Monitor Mode: Acts as a dedicated sensor for Intrusion Detection Systems (IDS), rogue AP detection, and Location-based services (LBS).
- Sniffer Mode: Captures and forwards wireless packets for remote analysis using tools like Wireshark or AiroPeek NX, including 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: Enables RF parameter configuration for site survey investigations, simplifying network planning and installation.
- SDA/Fabric Mode: Supports Software-Defined Access (SD-Access) for advanced segmentation and policy enforcement.

• Intelligent Network Capabilities

- CleanAir Pro Technology: Provides advanced spectrum intelligence in (2.4 + 5 GHz) or (2.4 + 6 GHz) bands, supporting high-speed spectrum analysis (20 MHz to 160 MHz) to identify and mitigate interference sources.
- Intelligent Capture: Probes the network to provide deep diagnostic insights, enabling troubleshooting of latency, interference, and other performance issues.

• Software Features

- Cisco Catalyst Center Support: Integrates with Cisco Catalyst Center to enable Cisco Spaces for location services.
- Apple FastLane: For optimized iOS device performance.

- 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	CW9171I	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 9171I Access Point is designed with integrated internal antennas. The antenna configuration includes

- Two Wi-Fi serving antennas, each capable of supporting 2.4 GHz and 5 GHz or 6 GHz, for dual-radio concurrent operation.
- One tri-band antenna for the dedicated 2.4 GHz, 5 GHz, and 6 GHz Auxiliary (scanning) radio.
- One single-band antenna for the dedicated 2.4 GHz IoT radio.



Note All antennas are internal and integrated into the CW9171I unit, not visible from outside the chassis.

Operating frequency and effective isotropic radiated power

Table 1: Cisco CW9171I AP values for the European Union (CE) region

Band	Frequency range	EIRP power limit ¹
	(MHz)	(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	13.98
5GHz SDR	5725-5875	14
EN 300 440		
6GHz WLAN	5945~6425	LPI: 23 ²
EN 303 687		
Bluetooth	2400-2483.5	10
IEEE 802.15.4	2400-2483.5	10

¹ Decimal EIRP values have been rounded to regulatory maxima using $\leq$ notation.

² 6 GHz operation is limited to Low Power Indoor (LPI) use only.



Note Restrictions applicable to one band do not apply to other supported bands.

Table 2: Cisco CW9171I Values for the United Kingdom Region

Band	Frequency Range	EIRP Power Limit
	(MHz)	(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	23
5GHz WLAN B4	5725-5850	23
(IR 2030)		
6G WLAN	5925-6425	LPI: 24
(IR 2030)		
Bluetooth	2400-2483.5	10

Band	Frequency Range	EIRP Power Limit
	(MHz)	(dBm)
IEEE 802.15.4	2400-2483.5	10

**Note**

- UK limits differ from EU due to national regulatory requirements.
- The regulatory domain automatically enforces applicable limits.



CHAPTER 2

Hardware Features

This chapter describes the hardware features of Cisco Wireless 9171I Wi-Fi 7 Access Point and contains the following sections:

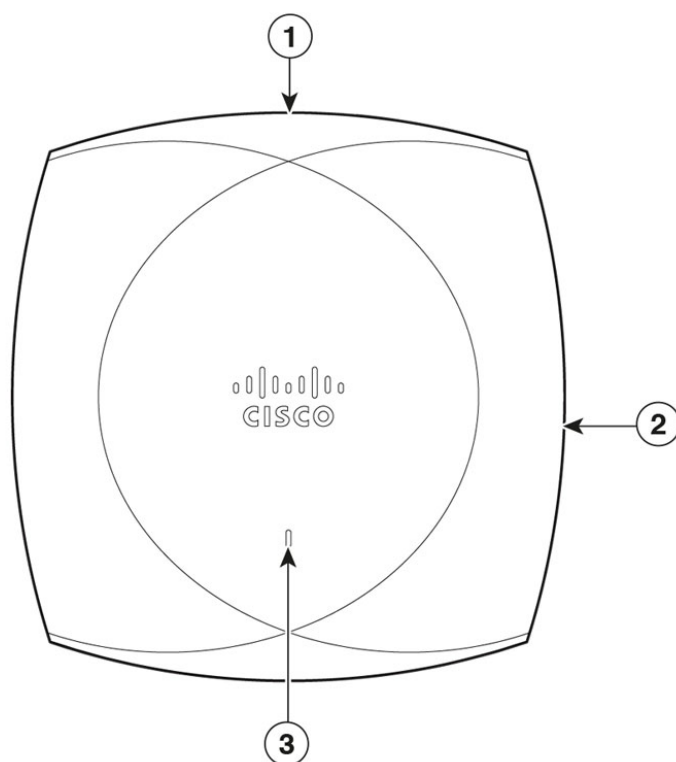
- [Access point views, ports, and connectors, on page 7](#)
- [Checking the access point LEDs, on page 9](#)

Access point views, ports, and connectors

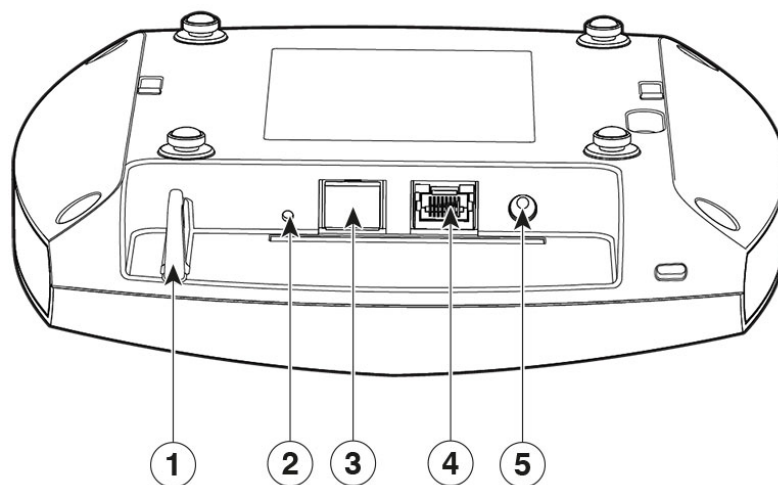
Cisco Wireless 9171I Wi-Fi 7 Access Point has multiple options that you can use to power the AP. For information about connectors and ports for the AP models, see [Connectors and ports on the AP, on page 7](#).

Connectors and ports on the AP

The following figures show the available ports on the AP:

CW9171I face view*Figure 1: CW9171I face view*

1	Kensington lock slot
2	USB 2.0 port
3	Status LED For information on the LEDs status, see Table 3: LED Status indications in controller mode, on page 10 .

CW9171I bottom view*Figure 2: CW9171I bottom 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 Using the reset button, on page 23 .	5	DC power jack
3	RJ-45 console port Default baud rate is 115200.		

Checking the access point LEDs

The location of the access point status LED is shown in [Connectors and ports on the AP, on page 7](#).

**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 in controller mode

Message Type	LED State	Message Meaning
System LED	Blinking Green 	Boot loader status (DRAM test, board initialization, Flash initialization, Ethernet initialization, Starting IOS).
	Green 	Normal operating condition, no wireless client associated.
	Blue 	Normal operating condition, at least one wireless client associated.
	Alternating between Green and Red 	Discovery or join process in progress.
	Blinking Red	AP Location Command.
	Red 	Ethernet failure.
	Blinking Blue 	Configuration recovery in progress (Mode button pressed for 2-3 seconds).
	Red 	Image recovery (Mode button pressed for 20-30 seconds).
	Cycling Blue, Green, Red, and Off 	General warning, insufficient inline power.
Ethernet Port LEDs	Off 	Link speed is 10 Mb, 100 Mb, or disconnected.
	Orange 	Link speed is 1000 Mb.
	Green 	Link speed is 2.5 Gb.
	Blinking Green 	Activity indicator for received 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
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



CHAPTER 3

Installing the Access Point

Installing an AP involves the following high-level tasks.

- [Package Contents, on page 13](#)
- [Unpacking the access point, on page 13](#)
- [Cisco orderable accessories, on page 14](#)
- [Preinstallation configuration - Cisco Catalyst mode, on page 15](#)
- [Preinstallation Configuration - Cisco Meraki Mode, on page 19](#)
- [Mount the access point, on page 19](#)
- [Powering the access point, on page 20](#)
- [Deploying the access point on a wireless network, on page 21](#)

Package Contents

Each Cisco Wireless 9171I Access Point package contains the following items:

- One Cisco Wireless 9171I Access Point
- 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

Unpacking the access point

Procedure

-
- | | |
|---------------|--|
| Step 1 | Unpack and remove the access point and the selected mounting 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 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 for the Cisco Wireless 9171I Access Point:

- AP-mounting brackets to mount the AP

Mounting Brackets	Description
AIR-AP-BRACKET-1=	Low-profile bracket: Used for ceiling-mount installations
AIR-AP-BRACKET-2=	Universal bracket: Used for wall or electrical box installations
AIR-AP-T-RAIL-R=	Ceiling grid clip (recessed mounting)
AIR-AP-T-RAIL-F=	Flush ceiling grid clip
AIR-CHNL-ADAPTER=	T-RAIL channel adapter

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

Power Supply / Injector	Description
MA-PWR-50WAC	External AC power supply.
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. Power Specifications: 50W, 56VDC. For more information, see the Cisco Multigigabit 802.3bt Power Injector .
AIR-PWRINJ6=	802.3at power injector. 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 .

- Other Accessories

Accessory	Description
CW-ACC-GPS1=	USB GPS module

Preinstallation configuration - Cisco Catalyst mode

Controller Discovery Process

To support the CW9171I AP, the controller must be running Cisco IOS XE 17.18.2 or a later release. For more information, see the [Cisco Wireless 9171I Series Access Points Data Sheet](#).

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 15](#).
- 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 25](#).
- 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.

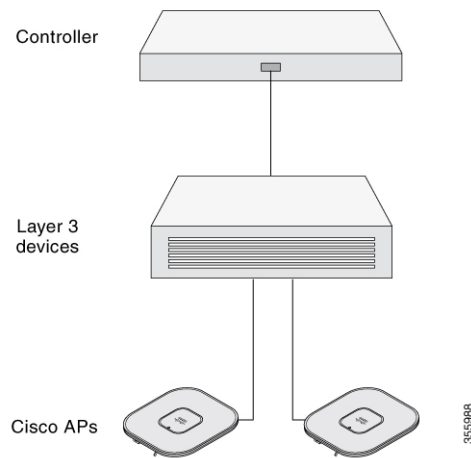
Performing a preinstallation configuration

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 [Deploying the access point on a wireless network, on page 21](#).

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 25](#) for more information.



Note The AP requires an 10G Ethernet link to prevent the Ethernet port from becoming a bottleneck for traffic.

Procedure

Step 1 Power the AP using a supported power source.

See [Powering the access point, on page 20](#).

- 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.

Step 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.

Step 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 19](#).

- Access point power options: Use either of the following options to power the AP:
 - Cisco-approved power injector
 - PoE with a supporting switch
 - MA-PWR-50WAC External power supply



Note • The Underwriter Laboratories (UL)-approved Listed Power Adapter must meet the following minimum specifications: Rated output of 42.5 to 57 Vdc, min. 0.81-1.08A, Tmax of 50°C minimum, altitude of 3048m minimum.

- Operating temperature:
 - CW9171I: 113°F to 122°F (45°C to 50°C)

- 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

-
- | | |
|---------------|--|
| Step 1 | Log in to Cisco Meraki dashboard . If this is your first time, create a new account. |
| Step 2 | Find the network to which you plan to add your APs or create a new network. |
| Step 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. |
| Step 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 9171I Wi-Fi Access Point can be mounted in the following places:

- Suspended ceiling
- Hard ceiling
- 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 ³⁴⁵	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.

³ Mount the AP using no less than four screw holes on a bracket.

⁴ AIR-AP-BRACKET-3 is not compatible for use with Cisco CW9171I access points.

⁵ 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.

Powering the access point



Caution

Ensure that the AP is powered using an 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	2.4-GHz radio	5-GHz or 6-GHz radio	Scan radio	IoT radio	Ethernet	USB	Max POE power consumption	Configuration information
802.3at	2x2	2x2	Enabled	Enabled	2.5G	Enabled (4.5W)	27.9W	
802.3at	2x2	2x2	Enabled	Enabled	2.5G	Disabled	21.9W	4ss, 2G 2x2 + (5G 2x2 or 6G 2x2)
802.3af (PoE)	1x1	1x1	Disabled	Disabled	1.0G	Gypsum only	14.0W	4ss, 2G 2x2 + (5G 2x2 or 6G 2x2)

Deploying the access point on a wireless network

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

Procedure

Step 1 Connect and power up the access point.

Step 2 Observe the access point LED.

For LED status descriptions, see [Checking the access point LEDs, on page 9](#).

- 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.
-



CHAPTER 4

Troubleshooting

- [Using the reset button, on page 23](#)
- [Troubleshooting the access point to Cisco controller join process, on page 24](#)
- [Important information for controller-based deployments, on page 25](#)
- [Configuring DHCP option 43, on page 25](#)

Using the reset button

Using the **Reset** button (see [CW9171I top view with connectors and ports](#)), 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 CW9171I 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 CW9171I 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 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 CW9171I APs:

- 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 Wireless 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 CW9171I 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 CW9171I access point is:

Cisco Wireless AP CW9171I

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 initial discovery process. For more information on day 0 workflow, see [Global Use Access Points](#).

Procedure

Step 1 Enter the configuration mode

Step 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 AP9171I.

<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:

```
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**.



CHAPTER 5

Safety Guidelines and Warnings

- [Safety instructions, on page 27](#)

Safety instructions

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](https://www.cisco.com).



Warning Statement 1071—Warning Definition

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 Statement 1005—Circuit Breaker

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 Statement 1074—Comply with Local and National Electrical Codes

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



CHAPTER 6

Declarations of Conformity 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>.

- [Manufacturers Federal Communication Commission declaration of conformity statement, on page 29](#)
- [VCCI statement for Japan, on page 31](#)
- [Canadian compliance statement, on page 32](#)
- [European community, Switzerland, Norway, Iceland, and Liechtenstein compliance, on page 33](#)
- [United Kingdom compliance, on page 34](#)
- [Administrative rules for Cisco Wireless Access Points in Taiwan, on page 34](#)
- [Operation of Cisco Wireless Access Points in Brazil, on page 35](#)
- [Declaration of conformity for RF exposure, on page 36](#)
- [Declaration of conformity statements, on page 38](#)

Manufacturers Federal Communication Commission declaration of conformity statement



Access Point model	Certification number
CW9171I	UDX-600219010

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 is classified as a Low Power Indoor (LPI) access point and must be operated indoors only. Operation of the 6 GHz band outdoors is prohibited under FCC rules. This restriction applies exclusively to 6 GHz operation and does not affect operation in other supported frequency bands, which remain subject to applicable FCC regulations.

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
- Professional Installation is recommended


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.

Low power indoor access points and subordinate devices

- FCC regulations restrict the operation of this device to indoor use only.
- This device is prohibited from being operated on oil platforms, cars, trains, boats, and aircraft, except it can be operated in large aircraft while 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 access points

- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.

- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

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:

CW9171I

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、ノーク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**

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

For operation in the 5925–6425 MHz band, this device is classified as a Low Power Indoor (LPI) or Very Low Power (VLP) device under Innovation, Science and Economic Development Canada (ISED) RSS-247 and shall be operated in accordance with applicable indoor-use and platform-based restrictions defined by ISED. These restrictions apply exclusively to 6 GHz operation and include limitations related to indoor use and operation on aircraft, vehicles, trains, maritime vessels, oil platforms, and unmanned aircraft systems. Operation in the 2.4 GHz and 5 GHz bands is not subject to these restrictions and remains governed by the applicable ISED regulatory requirements for those bands.

appareil Wi-Fi 7

Pour le fonctionnement dans la bande 5925–6425 MHz, cet appareil est classé comme dispositif de faible puissance intérieur (LPI) ou de très faible puissance (VLP) conformément à la norme CNR-247 d'Innovation, Sciences et Développement économique Canada (ISDE) et doit être utilisé conformément aux restrictions applicables relatives à l'utilisation intérieure et aux plateformes définies par ISDE. Ces restrictions s'appliquent exclusivement au fonctionnement dans la bande de 6 GHz et comprennent des limitations liées à l'utilisation intérieure ainsi qu'à l'exploitation sur les aéronefs, les véhicules, les trains, les navires maritimes, les plateformes pétrolières et les systèmes d'aéronefs sans pilote. Le fonctionnement dans les bandes de 2,4 GHz et de 5 GHz n'est pas soumis à ces restrictions et demeure régi par les exigences réglementaires applicables d'ISDE pour ces bandes.

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
CW9171I	6961A-600219010

European community, Switzerland, Norway, Iceland, and Liechtenstein compliance

The product carries the CE Mark:



When operating in the 5150–5350 MHz band and the 5945–6425 MHz band, this device is restricted to indoor use in accordance with applicable European Union and EFTA regulatory requirements. These restrictions

apply exclusively to operation within the specified frequency bands and do not affect operation in other supported bands, which remain subject to national regulations.

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



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:

CW9171I

Manufacturer:

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

United Kingdom compliance

When operating in the 5150–5350 MHz band and the 5925–6425 MHz band, this device is restricted to indoor use in accordance with applicable United Kingdom regulatory requirements. These restrictions apply exclusively to operation within the specified frequency bands and do not affect operation in other supported bands, which remain subject to applicable UK regulations.

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

Access Point model:

CW9171I

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 for all access points are provided in both Simplified Chinese and English.

Simplified 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 National Communications Commission (NCC), no company, enterprise, or user shall alter the frequency, increase the transmitting power, or modify the original characteristics or performance of approved low-power radio-frequency devices.

Low-power radio-frequency devices shall not affect aviation safety or interfere with lawful communications. If interference is observed, operation shall be ceased immediately and shall not resume until the interference has been resolved. Lawful communications refer to radio communications operated in accordance with the Telecommunications Management Act.

Low-power radio-frequency devices must accept interference from lawful communications and from industrial, scientific, and medical (ISM) radio-frequency equipment. Operation shall avoid interference with nearby radar systems.

This equipment must be installed and configured by qualified professional personnel and is not intended for direct sale to the general public.

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

Access Point model	Certification number
CW9171I	TBD

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 the protection from harmful interference and may not cause interference with duly authorized systems.

equipamento Wi-Fi 7

Para operação na faixa de 5925–6425 MHz, este equipamento é classificado como dispositivo de baixa potência para uso interno, conforme os requisitos regulatórios aplicáveis no Brasil. As restrições relacionadas ao uso interno e à operação em aeronaves, veículos, trens, embarcações e plataformas petrolíferas aplicam-se exclusivamente à operação na banda de 6 GHz e não afetam a operação do equipamento em outras faixas de frequência suportadas, que permanecem sujeitas às regulamentações brasileiras aplicáveis.

Wi-Fi 7 Device

For operation in the 5925–6425 MHz band, this device is classified as a low-power indoor device in accordance with applicable Brazilian regulatory requirements. Restrictions on indoor use and on the operation of aircraft, vehicles, trains, maritime vessels, and oil platforms apply exclusively to 6 GHz operations and do not affect operations in other supported frequency bands, which remain subject to applicable Brazilian regulations.

Access Point model	Certification number
CW9171I	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 CW9171I 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 CW9171I 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 CW9171I 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/environmental-workplace-health/reports-publications/radiation/safety-code-6.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/pdtncc/#/>