Figure 11: CW9162I - Scanning Radio Normalized Radiation Pattern (5-GHz Azimuth)

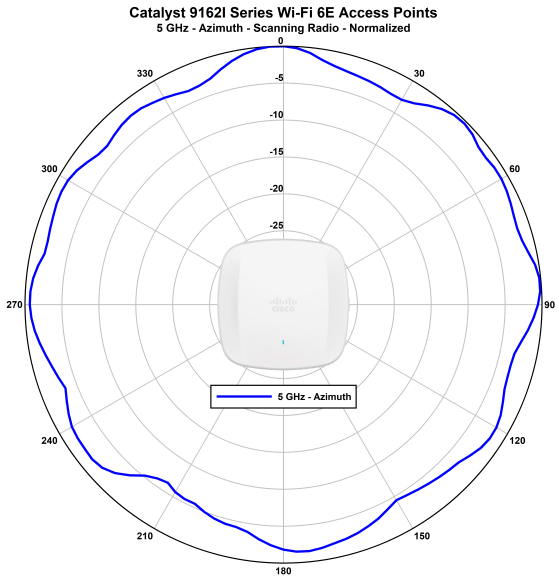


Figure 12: CW9162I - Scanning Radio Normalized Radiation Pattern (5-GHz Elevation)

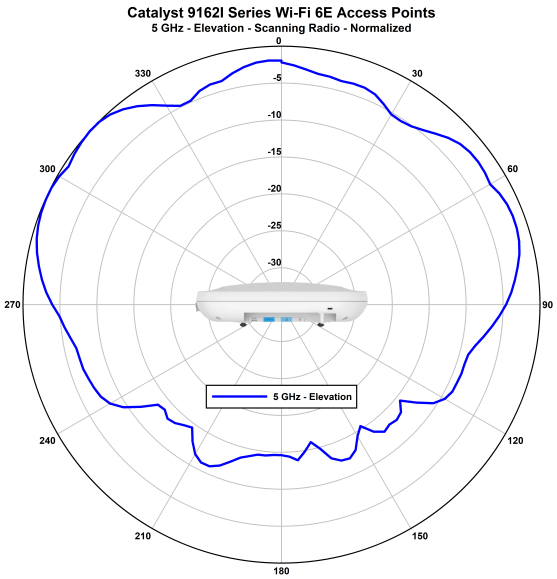


Figure 13: CW9162I - Scanning Radio Normalized Radiation Pattern (6-GHz Azimuth)

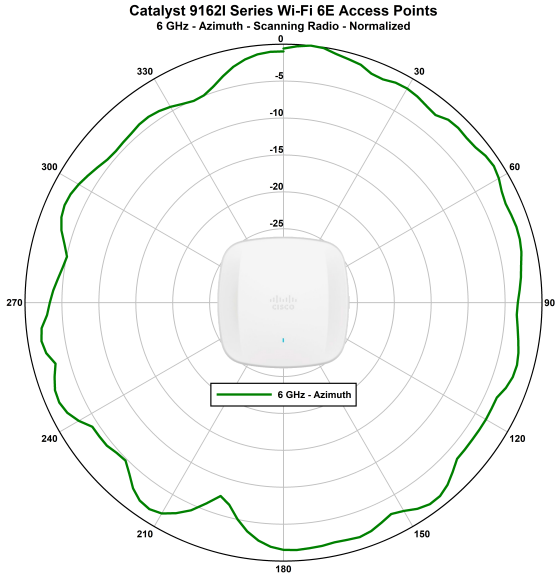


Figure 14: CW9162I - Scanning Radio Normalized Radiation Pattern (6-GHz Elevation)

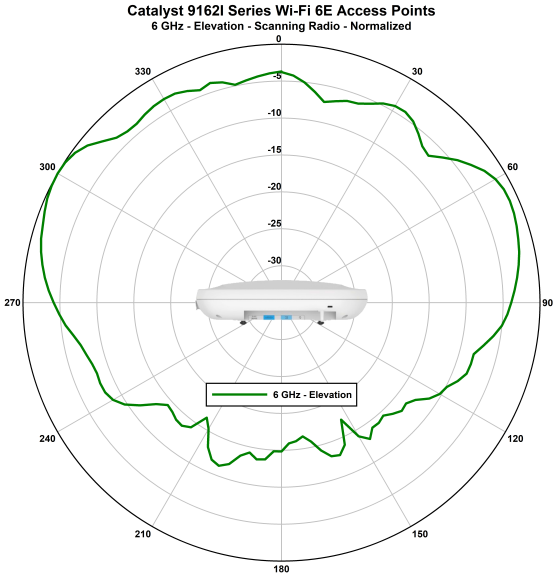


Figure 15: CW9162I - IoT Antenna Normalized Radiation Pattern (2.4-GHz Azimuth)

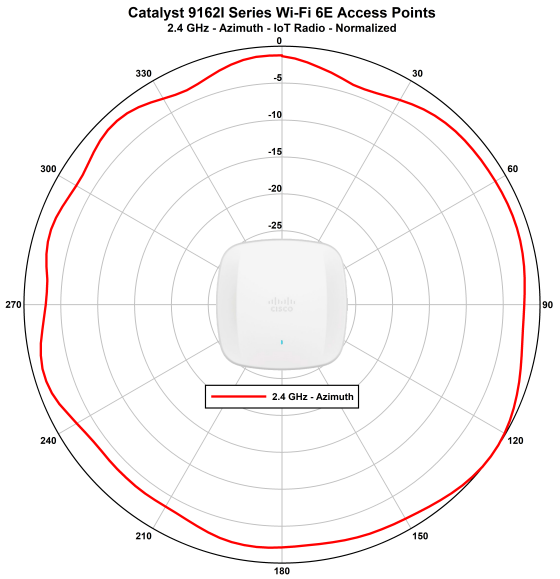
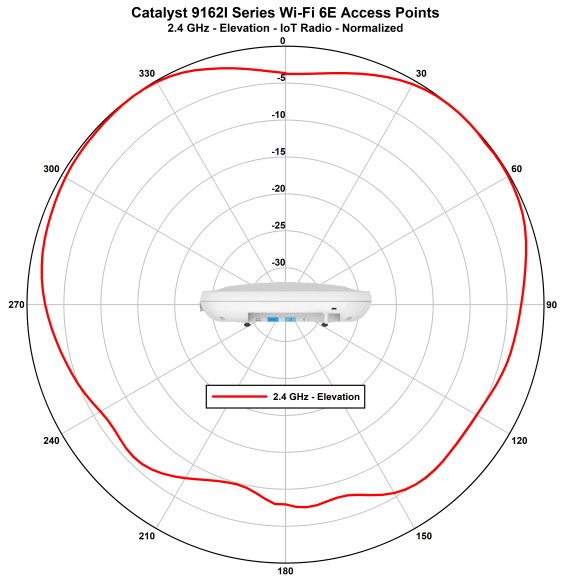
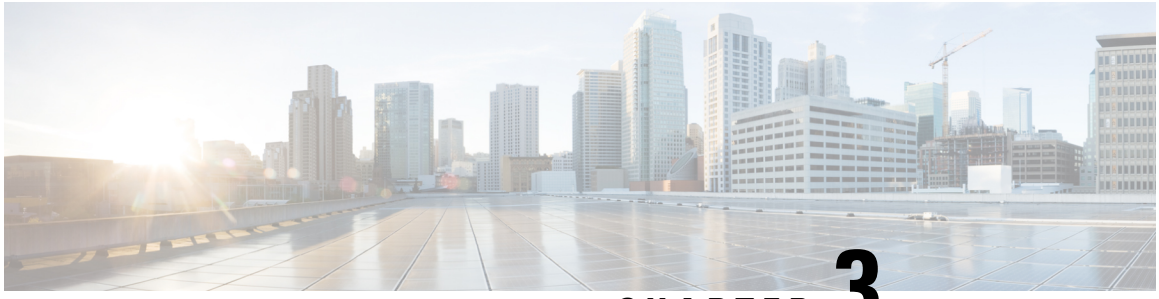


Figure 16: CW9162I - IoT Antenna Normalized Radiation Pattern (2.4-GHz Elevation)





CHAPTER 3

Unpacking Your Access Point

- Package Contents, on page 13
- Unpacking the Access Point, on page 13
- Cisco Orderable Accessories, on page 14

Package Contents

Each AP package contains the following items:

- One CW9162I AP
- Default mounting brackets: Adjustable ceiling-rail clip AIR-AP-T-RAIL-R and AIR-AP-BRACKET-1=
- Orderable optional mounting brackets: AIR-AP-T-RAIL-F, AIR-AP-BRACKET-2=
- Cisco product documentation and pointer card

Note When Cisco CW9162I-MR AP is ordered, mounting bracket AIR-AP-BRACKET-2= is included by default.

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

Cisco Orderable Accessories

Order the following accessories separately from Cisco:

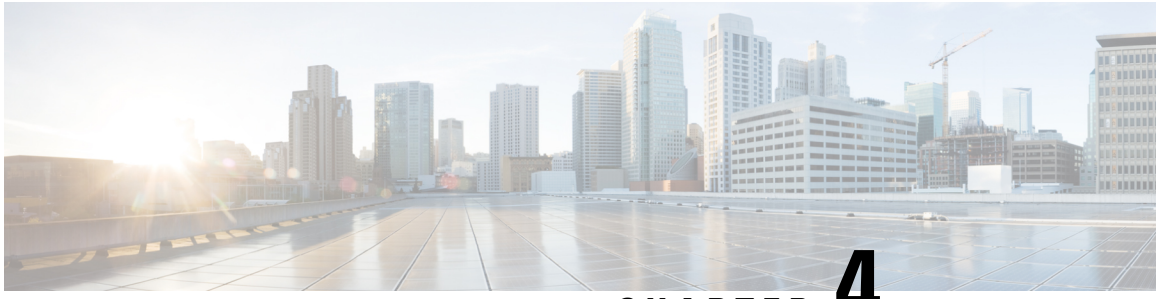
- AP-mounting brackets to mount the AP.

Mounting Brackets	Description
AIR-AP-BRACKET-1=	For low profile installations
AIR-AP-BRACKET-2=	For electrical or network boxes above ceiling mounts
AIR-AP-T-RAIL-F=	Flush ceiling grid clip
AIR-AP-T-RAIL-R=	Recessed ceiling grid clip
AIR-CHNL-ADAPTER=	T-RAIL channel adapter

- Power injectors when PoE is not available.

Power Supply	Description
AIR-PWRINJ7=	Mid-span power injector AIR-PWRINJ7= when Power over Ethernet (PoE) is not available Power specifications: 50W, 56VDC. For more information, see the power injector data sheet.
AIR-PWRINJ5=	A 802.3af power injector Power specifications: 15.4W, 48VDC. For more information, see the power injector data sheet.
AIR-PWRINJ6=	A 802.3at power injector when PoE is not available Power specifications: 30W, 55VDC. For more information, see the power injector data sheet.
MA-INJ-4-US	Meraki 802.3at PoE injector Power specifications: 30W, 55VDC. For more information, see the power injector data sheet.

Power Supply	Description
MA-INJ-6-x	Meraki 802.3bt PoE injector Power specifications: 60W, 55VDC. For more information, see the power injector data sheet.
MA-PWR-30W	DC Power Adapter Power specifications: 30W, 12VDC. For more information, see the power injector data sheet.



CHAPTER 4

Installation Overview

Installing an AP involves the following high-level tasks.

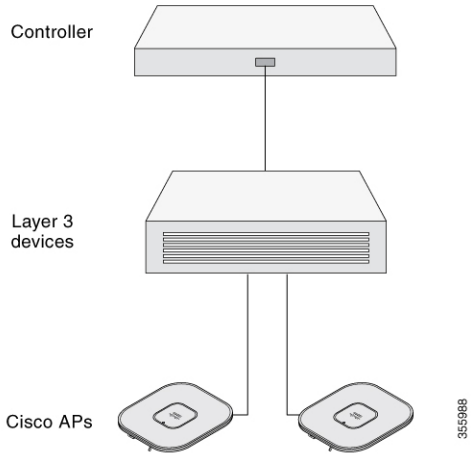
- Performing a Preinstallation Configuration (Optional), on page 17
- Preinstallation Checks and Installation Guidelines, on page 19
- Mounting the Access Point, on page 20
- Powering the Access Point, on page 21

Performing a Preinstallation Configuration (Optional)

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 the Wireless Network, on page 24.

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, Cisco Controller Management, and AP-Manager 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 802.11ax 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 the Configuring DHCP Option 43, on page 29 for more information.

Note The AP requires a multi-gigabit Ethernet (5 Gbps) link to prevent the Ethernet port from becoming a bottleneck for traffic.

Note The Cisco CW9162I-MR AP does not join the Cisco 9800 Wireless Controller. The AP needs to be migrated to join the controller and requires you to contact the Meraki support team.

Procedure

Step 1 Power the AP using supported power source.

See Powering the Access Point, on page 21.

- As the AP attempts to connect to the controller, the LED cycles through a green, red, and off sequence, which can take up to five minutes.

  Note If the AP remains in this mode for more than five minutes, the AP cannot find the primary Cisco 9800 controller. Check the connection between the AP and the Cisco 9800 controller and be sure that they are on the same subnet.

- If the AP shuts down, check the power source.

- After the AP finds the Cisco Catalyst 9800 Series Wireless Controller, it attempts to download the new operating system code if the AP code version differs from the Cisco Catalyst 9800 Series Wireless Controller code version. While this is happening, the Status LED blinks blue.

If the operating system download is successful, the AP reboots.

Step 2 (Optional) Configure the AP. Use the controller CLI, GUI, or Cisco DNA Center to customize the access point-specific 802.11ax network settings.

Step 3 If the preinstallation configuration is successful, the Status LED is green, indicating normal operation. Disconnect the AP and mount it at the location at which you intend to deploy it on the wireless network.

Step 4 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 Cisco 9800 controller, ensure 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, or 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 Mounting the Access Point, on page 20.

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

Note

- The Underwriter Laboratories (UL)-approved Listed Power Adapter must meet the following minimum specifications: Rated output of 54Vdc, min. 0.92A.
- If 802.3af is used, Ethernet gets downgraded to 1 GbE. The USB port is also off.

- Operating temperature:
  - CW9162I: 32°F to 104°F (0°C to 40°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 derates to 1x1 for tri-radio (2.4-GHz, 5-GHz, 6-GHz).

- 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.

Mounting the Access Point

Cisco Catalyst 9162I Series Wi-Fi 6E Access Point can be mounted in the following places:

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

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 is listed in the table below.

Table 4: Brackets and Clips for Mounting the AP

Mounting Type	Part Number	Description
Brackets[1][2][3]	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.
Desk mount		Desk mount rubber feet using screw size 8-32x.28”

1 Mount the AP using no less than four screw holes on a bracket.
2 AIR-AP-BRACKET-3 is not compatible for use with Cisco Catalyst Wireless 9162I access points.
3 You can also use *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

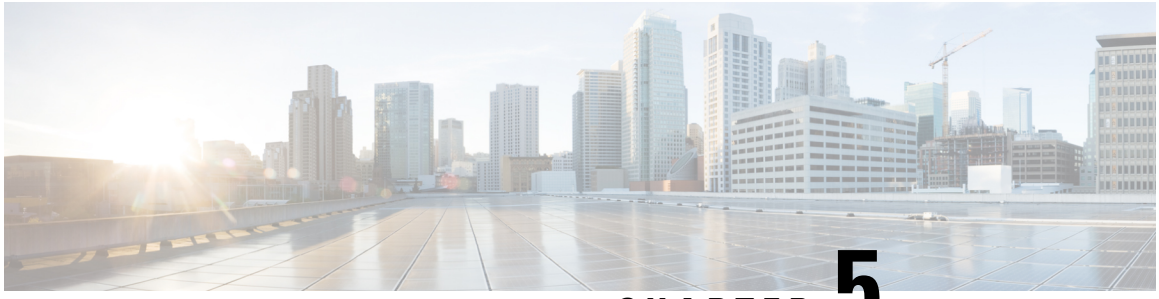
Caution Ensure that the AP is powered using a Underwriters' Laboratories-compliant (UL-compliant) PoE power source. You must connect the unit only to the PoE network, without routing to the outside plant.

The AP can be powered only through Power-over-Ethernet (PoE) using the following:

- 802.3bt: Any 802.3bt-compliant switch port or Cisco Power Injector AIR-PWRINJ7=
- Cisco Universal PoE (Cisco UPoE)
- 802.3at (PoE+): Any 802.3at (30.0 W)-compliant switch port
- 802.3af: Any 802.3af (15.4 W)-compliant switch port

Note If 802.3af power injector is used, 2.4-GHz radio is switched off, and both 5-GHz and 6-GHz radios derate to 1x1 radio. The Ethernet port gets downgraded to 1 GbE, and the USB port is switched off.

- DC power jack



CHAPTER 5

Configuring and Deploying the Access Point

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

- The Controller Discovery Process, on page 23
- Deploying the Access Point on the Wireless Network, on page 24
- Checking the Access Point LEDs, on page 24

The Controller Discovery Process

To support CW9162I AP, the controller must be running Cisco IOS-XE 17.9.1 or a later release. For more information, see the access point data sheet at:

Cisco Catalyst 9164 Series Access Points Data Sheet

Cisco Catalyst 9166 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 the Performing a Preinstallation Configuration (Optional), on page 17.
- 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 the Configuring DHCP Option 43, on page 29.

- 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 the controllers.

Deploying the Access Point on the Wireless Network

After you have mounted the access point, follow these steps to deploy it on the 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 24.

- 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 has 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, the access point is most likely 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.

  For more information, see Configuring DHCP Option 43, on page 29.

Checking the Access Point LEDs

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

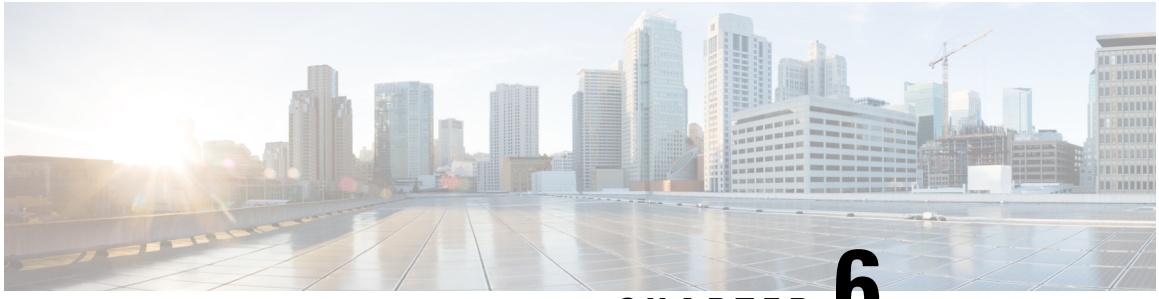
Note

- Regarding LED status colors, it is expected that there will be small variations in color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect. However, the intensity of the LED can be changed through the controller.
- When the AP is under Meraki management mode, the LED status indicators convey status differently than the Cisco APs. For more information, see the *Meraki CW9162 Installation Guide*.

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

Table 5: LED Status Indications

Message Type	LED State	Message Meaning
Association status	Green	Normal operating condition, but no wireless client associated
	Blue	Normal operating condition, at least one wireless client association
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



CHAPTER 6

Troubleshooting

- Using the Mode Button, on page 27
- Troubleshooting the Access Point to Cisco Controller Join Process, on page 28
- Important Information for Controller-Based Deployments, on page 29
- Configuring DHCP Option 43, on page 29

Using the Mode Button

Using the **Mode** button (see Figure 2: CW9162I Top View with Connectors and Ports, on page 7) you can perform the following tasks:

- Reset the AP to the default factory-shipped configuration
- Clear AP's internal storage, including all the configuration files

To use the **Mode** button, press, and continue to press the **Mode** button on the access point during the AP boot cycle. Wait until the AP console shows a seconds counter. When the counter indicates the number of seconds for which the **Mode** button is pressed, the AP status LED changes to blinking red. Then reset the AP to the default factory-shipped configuration, keep the mode button pressed for less than 20 seconds. The AP configuration files are cleared.

Clear the AP internal storage, including all the configuration files, keep the **Mode** button pressed for more than 20 seconds, but less than 60 seconds. This resets all the configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

Note If the **Mode** button is pressed for more than 30 seconds, but less than 60 seconds, the FIPS mode flag is also cleared during the full factory reset of the AP. If the FIPS flag is set, the console access is disabled.

The AP status LED changes from blue to red, and all the files in the AP storage directory are cleared.

If you keep the **Mode** button pressed for more than 60 seconds, the button is assumed as being faulty and no changes are made.

Troubleshooting the Access Point to Cisco Controller Join Process

Note As specified in the Cisco Wireless Solutions Software Compatibility Matrix, ensure that your controller is running controller software Cisco IOS-XE 17.9.1 or a later release to support Cisco CW9162I AP.

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

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

When the ordered AP is a CW9162I-MR model, or the AP is in Meraki Management mode, it will not attempt to join the Cisco 9800 Wireless Controller. You need to contact the Meraki support team to perform the migration procedure on the AP.

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

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

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

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

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

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

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

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

  To configure the global syslog server IP address

  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 CW9162I Series AP:

- The AP can only communicate with Cisco wireless controllers.
- The AP does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the AP joins it.
- CAPWAP does not support Layer 2. The AP must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The AP console port is enabled for monitoring and debug purposes.
- 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 CW9162I Series 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 CW9162I access point is:

Cisco AP CW9162I

The format of the TLV block is listed below:

- 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:

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 AP9136I

<*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

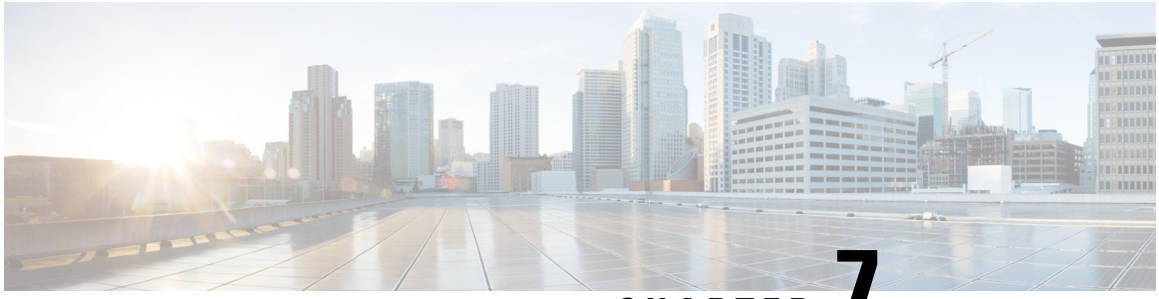
Step 3 Add the Option 43 line using the following syntax:

```
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 7

Safety Guidelines and Warnings

- Safety Instructions, on page 31

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 in the Translated Safety Warnings for Cisco Catalyst Access Points, which is available on Cisco.com.

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

Danger **Read the installation instructions before using, installing or connecting the system to the power source.** Statement 1004

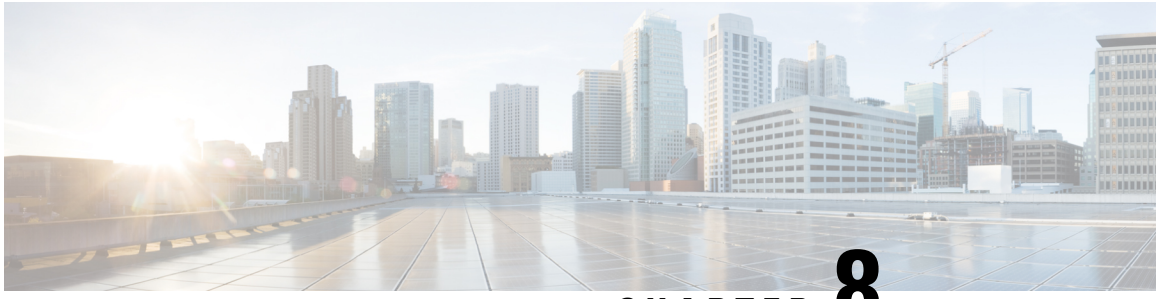
Danger **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 20A.** Statement 1005

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

Danger **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 16.14 inches (41 cm) or more from the body of all persons.** Statement 332

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

Caution **Ensure to connect the power cord of the power adapter to a socket outlet with an earthing connection.**



CHAPTER 8

Declarations of Conformity and Regulatory Information

This section provides declarations of conformity and regulatory information for the Cisco Catalyst 9162I Series Wi-Fi 6E Access Point. You can find additional information at: http://www.cisco.com/go/aironet/compliance.

- Manufacturers Federal Communication Commission Declaration of Conformity Statement, on page 33
- VCCI Statement for Japan, on page 34
- Canadian Compliance Statement, on page 36
- European Community, Switzerland, Norway, Iceland, and Liechtenstein Compliance, on page 37
- United Kingdom Compliance, on page 37
- Administrative Rules for Cisco Catalyst Access Points in Taiwan, on page 38
- Operation of Cisco Catalyst Access Points in Brazil, on page 39
- Declaration of Conformity for RF Exposure, on page 39
- Declaration of Conformity Statements, on page 42

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Access Point Models	Certification Number
Cisco CW9162I-B	UDX-600155010

Manufacturer:

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

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

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radiofrequency energy, and if not installed and used according to the instructions, it may cause harmful interference. Hence, professional installation is recommended. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

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

Caution 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.FCC regulations restrict the operation of this device to indoor use only. The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.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	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 Models:

CW9162I-Q

Guidelines for Operating Cisco Catalyst Access Points in Japan

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

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか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 } I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**

Statement 371—Power Cable and AC Adapter

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

English Translation

When installing the product, please use the provided or designated connection cables/power cables/AC adaptors. Using any other cables/adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the “UL” shown on the code) for any other electrical devices than products designated by CISCO. The use of cables that are certified by Electrical

Appliance and Material Safety Law (that have “PSE” shown on the code) is not limited to CISCO-designated products.

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 6E Device

- Operation shall be limited to indoor use only.
- Operation on oil platforms, cars, trains, boats and aircraft shall be prohibited except for on large aircraft flying above 10,000 ft.

appareil Wi-Fi 6E

- Utilisation limitée à l’intérieur seulement.
- Utilisation interdite à bord de plateformes de forage pétrolier, de voitures, de trains, de bateaux et d’aéronefs, sauf à bord d’un gros aéronef volant à plus de 10 000 pieds d’altitude.

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.

Industry Canada

Access Point Models:

CW9162I-A

Access Point Model	Certification Number
CW9162I-A V01	6961A-600155010

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

The product carries the CE Mark:

The device is restricted to indoor use only when operating between 5150 MHz and 5350 MHz, 5945 MHz and 6425 MHz frequency range.

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 Models:

CW9162I-E

Manufacturer:

Cisco Systems, Inc.125 West Tasman Drive San Jose, CA 95134-1706 USA

United Kingdom Compliance

The device is restricted to indoor use only when operating between 5150 MHz and 5350 MHz, 5925 MHz and 6425 MHz frequency range. This equipment should be installed and operated with minimum distance 20 cm (7.87 inches) between the radiator & your body.

Access Point Models:

CW9162I-ROW

Manufacturer:

Cisco Systems, Inc.125 West Tasman Drive San Jose, CA 95134-1706 USA

Administrative Rules for Cisco Catalyst Access Points in Taiwan

This section provides administrative rules for operating Cisco Catalyst 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。

Note 6E 頻段在台灣尚未開放使用，故本器材在台灣暫不支援6E。

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 characteristic as well as performance to a approved low power radio-frequency devices. The low power radio-frequency devices shall not influence aircraft security and interfere legal communications; If found, the user shall cease operating immediately until no interference is achieved. The said legal communications means radio communications is operated in compliance with the Telecommunications Management Act. The low power radio-frequency devices must be susceptible with the interference from legal communications or ISM radio wave radiated devices.

Note This device does not support Wi-Fi 6E frequency bands in Taiwan.

The operations near the radar system shall not be influenced.

This section contains special information for operation of Cisco Catalyst access points in Taiwan.

Access Point Models	Certification Number
CW9162I-ROW	xxxxx-xx-xxxxx

Operation of Cisco Catalyst Access Points in Brazil

Figure 17: Brazil Regulatory Information

Portuguese Translation

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

English Translation

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

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

Access Point Models	Certification Number
CW9162I-ROW	xxxxx-xx-xxxxx

Declaration of Conformity for RF Exposure

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

Generic Discussion on RF Exposure

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

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

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

This Device Meets International Guidelines for Exposure to Radio Waves

The Cisco CW9162I series device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) recommended by international guidelines. The guidelines were developed by an independent scientific organization (ICNIRP) and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

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

Separation Distance
20 cm (7.87 inches)

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

This Device Meets FCC Guidelines for Exposure to Radio Waves

The Cisco CW9162I series device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in FCC Part 1.1310. The guidelines are based on IEEE ANSI C 95.1 (92) and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

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

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

Separation Distance
41 cm (16.14 inches)

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

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

The Cisco CW9162I series device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in Health Canada

Safety Code 6. The guidelines include a substantial safety margin designed into the limit to ensure the safety of all persons, regardless of age and health.

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

Table 6: Separation Distance

Frequency	Distance
2.4-GHz	24 cm (9.44 inches)
5-GHz	
6-GHz	

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

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

Cet appareil de la gamme Cisco CW9162I comprend un émetteur-récepteur radio. Il a été conçu de manière à respecter les limites en matière d'exposition aux fréquences radioélectriques (champs électromagnétiques de fréquence radio), recommandées dans le code de sécurité 6 de Santé Canada. Ces directives intègrent une marge de sécurité importante destinée à assurer la sécurité de tous, indépendamment de l'âge et de la santé.

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

Table 7: Distance d'éloignement

Fréquence	Distance
2.4-GHz	24 cm (9.44 inches)
5-GHz	
6-GHz	

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

Additional Information on RF Exposure

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

- Cisco Systems Spread Spectrum Radios and RF Safety white paper at this URL:

  http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/rfhr_wi.htm

- FCC Bulletin 56: Questions and Answers about Biological Effects and Potential Hazards of Radio Frequency Electromagnetic Fields
- FCC Bulletin 65: Evaluating Compliance with the FCC guidelines for Human Exposure to Radio Frequency Electromagnetic Fields

You can obtain additional information from the following organizations:

- World Health Organization Internal Commission on Non-Ionizing Radiation Protection
- United Kingdom, National Radiological Protection Board
- 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/#/

APPENDIX A

Transmit Power and Receive Sensitivity Values

Table 8: Transmit Power and Receive Sensitivity Values

			6-GHz Radio		5-GHz Primary Radio		2.4-GHz Radio	
	Spatial Streams	Number of Active Antennas	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)
802.11/11b								
1 Mbps	1	2	–	–	–	–	20	-98
11 Mbps	1	2	–	–	–	–	20	-91
802.11a/g								
6 Mbps	1	2	20	-95	20	-94	20	-95
24 Mbps	1	2	18	-85	19	-86	20	-87
54 Mbps	1	2	17	-78	18	-77	18	-79
802.11n HT20								
MCS0	1	2	–	–	20	-94	20	-94
MCS4	1	2	–	–	19	-84	18	-85
MCS7	1	2	–	–	18	-77	15	-77
MCS8	2	2	–	–	20	-93	20	-93
MCS12	2	2	–	–	19	-82	18	-82
MCS15	2	2	–	–	18	-74	15	-75
802.11n HT40								
MCS0	1	2	–	–	20	-91	–	–
MCS4	1	2	–	–	19	-79	–	–

			6-GHz Radio		5-GHz Primary Radio		2.4-GHz Radio	
	Spatial Streams	Number of Active Antennas	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)
MCS7	1	2	–	–	18	-73	–	–
MCS8	2	2	–	–	20	-90	–	–
MCS12	2	2	–	–	19	-79	–	–
MCS15	2	2	–	–	18	-72	–	–
802.11ac VHT20								
MCS0	1	2	–	–	20	-94	–	–
MCS4	1	2	–	–	19	-85	–	–
MCS7	1	2	–	–	18	-78	–	–
MCS8	1	2	–	–	18	-74	–	–
MCS9	1	2	–	–	–	–	–	–
MCS0	2	2	–	–	20	-92	–	–
MCS4	2	2	–	–	19	-81	–	–
MCS7	2	2	–	–	18	-74	–	–
MCS8	2	2	–	–	18	-70	–	–
MCS9	2	2	–	–	–	–	–	–
802.11ac VHT40								
MCS0	1	2	–	–	20	-92	–	–
MCS4	1	2	–	–	19	-82	–	–
MCS7	1	2	–	–	18	-76	–	–
MCS8	1	2	–	–	18	-72	–	–
MCS9	1	2	–	–	17	-70	–	–
MCS0	2	2	–	–	20	-91	–	–
MCS4	2	2	–	–	19	-79	–	–
MCS7	2	2	–	–	18	-72	–	–
MCS8	2	2	–	–	18	-69	–	–
MCS9	2	2	–	–	17	-67	–	–

			6-GHz Radio		5-GHz Primary Radio		2.4-GHz Radio	
	Spatial Streams	Number of Active Antennas	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)
802.11ac VHT80								
MCS0	1	2	–	–	20	-89	–	–
MCS4	1	2	–	–	19	-79	–	–
MCS7	1	2	–	–	18	-72	–	–
MCS8	1	2	–	–	18	-68	–	–
MCS9	1	2	–	–	17	-66	–	–
MCS0	2	2	–	–	20	-88	–	–
MCS4	2	2	–	–	19	-75	–	–
MCS7	2	2	–	–	18	-68	–	–
MCS8	2	2	–	–	18	-64	–	–
MCS9	2	2	–	–	17	-62	–	–
802.11ax HE20								
MCS0	1	2	20	-94	20	-95	20	-96
MCS4	1	2	18	-85	19	-84	18	-85
MCS7	1	2	17	-78	18	-77	15	-78
MCS8	1	2	16	-74	18	-73	14	-73
MCS9	1	2	16	-72	17	-72	13	-72
MCS10	1	2	15	-68	17	-67	12	-68
MCS11	1	2	15	-67	17	-66	12	-67
MCS0	2	2	20	-93	20	-93	20	-93
MCS4	2	2	18	-82	19	-81	18	-81
MCS7	2	2	17	-75	18	-74	15	-74
MCS8	2	2	16	-72	18	-70	14	-71
MCS9	2	2	16	-70	17	-69	13	-69
MCS10	2	2	15	-67	17	-65	12	-66
MCS11	2	2	15	-64	17	-63	12	-64

			6-GHz Radio		5-GHz Primary Radio		2.4-GHz Radio	
	Spatial Streams	Number of Active Antennas	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)
802.11ax HE40								
MCS0	1	2	20	-91	20	-92	–	–
MCS4	1	2	18	-82	19	-82	–	–
MCS7	1	2	17	-75	18	-75	–	–
MCS8	1	2	16	-71	18	-71	–	–
MCS9	1	2	16	-69	17	-70	–	–
MCS10	1	2	15	-67	17	-66	–	–
MCS11	1	2	15	-64	17	-64	–	–
MCS0	2	2	20	-91	20	-91	–	–
MCS4	2	2	18	-80	19	-79	–	–
MCS7	2	2	17	-73	18	-73	–	–
MCS8	2	2	16	-69	18	-69	–	–
MCS9	2	2	16	-67	17	-67	–	–
MCS10	2	2	15	-64	17	-64	–	–
MCS11	2	2	15	-62	17	-62	–	–
802.11ax HE80								
MCS0	1	2	20	-88	20	-89	–	–
MCS4	1	2	18	-80	19	-80	–	–
MCS7	1	2	17	-72	18	-72	–	–
MCS8	1	2	16	-69	18	-68	–	–
MCS9	1	2	16	-67	17	-66	–	–
MCS10	1	2	15	-64	17	-62	–	–
MCS11	1	2	15	-62	17	-60	–	–
MCS0	2	2	20	-88	20	-88	–	–
MCS4	2	2	18	-77	19	-77	–	–
MCS7	2	2	17	-70	18	-69	–	–

			6-GHz Radio		5-GHz Primary Radio		2.4-GHz Radio	
	Spatial Streams	Number of Active Antennas	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)	Total Tx Power (dBm)	Rx Sensitivity (dBm)
MCS8	2	2	16	-66	18	-65	–	–
MCS9	2	2	16	-65	17	-63	–	–
MCS10	2	2	15	-61	17	-59	–	–
MCS11	2	2	15	-59	17	-57	–	–
802.11ax HE160								
MCS0	1	2	20	-85	–	–	–	–
MCS4	1	2	18	-77	–	–	–	–
MCS7	1	2	17	-69	–	–	–	–
MCS8	1	2	16	-65	–	–	–	–
MCS9	1	2	16	-64	–	–	–	–
MCS10	1	2	15	-60	–	–	–	–
MCS11	1	2	15	-58	–	–	–	–
MCS0	2	2	20	-85	–	–	–	–
MCS4	2	2	18	-74	–	–	–	–
MCS7	2	2	17	-67	–	–	–	–
MCS8	2	2	16	-63	–	–	–	–
MCS9	2	2	16	-61	–	–	–	–
MCS10	2	2	15	-58	–	–	–	–
MCS11	2	2	15	-56	–	–	–	–

Transmit Power and Receive Sensitivity Values