CW9176D1 Installation Guide

Product Overview

The Cisco Wireless CW9176D1 is a Tri-band, Tri-radio, enterprise-class, Wi-Fi 7, cloud-managed access point supporting 2.4 GHz, 5 GHz, and the newly opened unlicensed 6 GHz frequency bands. Designed for the ultra-high capacity and highest density, CW9176D1 meets the needs of the most demanding and mission-critical environments. The Cisco Wireless CW9176D1 is designed with an integrated directional antenna allowing the coverage pattern to favour the area the AP is facing - ideal for warehouses, auditoriums, etc. The access point also includes a fourth radio dedicated to optimizing the RF environment and securing the airwaves. This model also has an additional Bluetooth Low Energy (BLE) capable radio used for location and other IoT applications. In addition to this CW9176D1 has a USB port to support external devices for IoT applications.

About this Guide

This guide provides instructions on how to install and configure your CW9166D1 access points. This guide also provides mounting instructions and limited troubleshooting procedures. For more wireless installation guides, refer to the wireless installation guides section on our documentation website.

Physical Specifications

CW9176D1

Interfaces

- 1x 100/1000/2.5G/5G/10G BASE-T Ethernet (RJ45)
- USB 2.0 at 9W
- Console Port (default speed of 115200 bps)
- External GPS/GNSS Antenna Port

Power

- Power over Ethernet: 42.5 - 57 V (802.3at/PoE+ and 802.3bt/UPoE compliant)
- Power consumption: 30W to 52W (802.3bt required for full AP operation)
- Power over Ethernet injector **(CW-INJ-8, MA-INJ-6 & AIR-PWRINJ7)**

ⓘ **Note:**

- PoE Injector sold separately
- Actual power consumption may vary depending on the AP usage.

- USB will be disabled when powered by 802.3at (PoE+)
- It is required that you ensure that LLDP is enabled to allow proper power negotiation

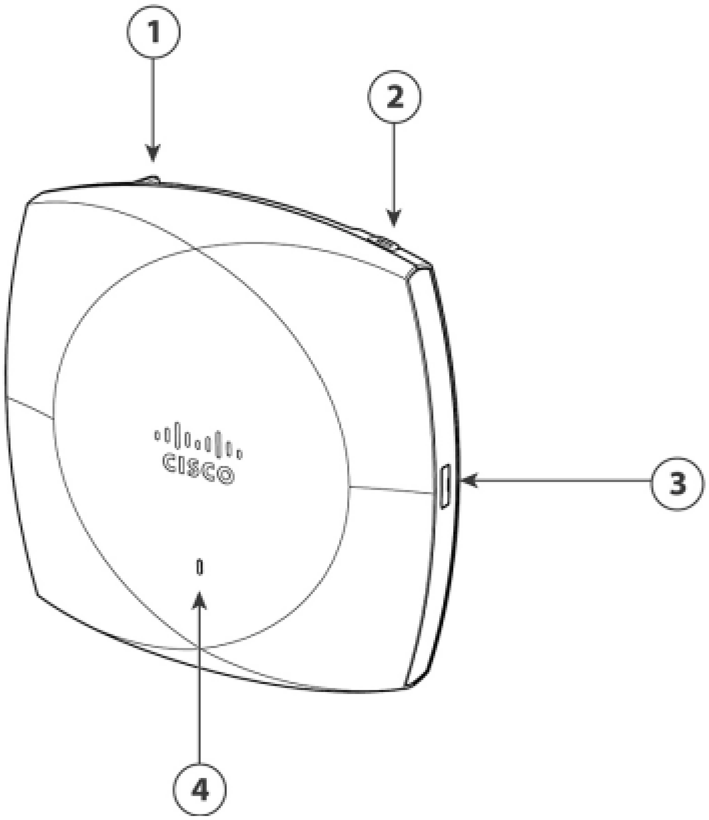
Environment

- Nonoperating (storage) temperature: -22° to 158°F (-30° to 70°C)
- Nonoperating (storage) altitude test: 25°C (77°F) at 15,000 ft (4570 m)
- Operating temperature: 32° to 122°F (0° to 50°C)
- Operating humidity: 10% to 90% (noncondensing)
- Operating altitude test: 40°C (104°F) at 9843 ft (3000 m)
- Humidity:10% to 90% non-condensing

Product View and Physical Features

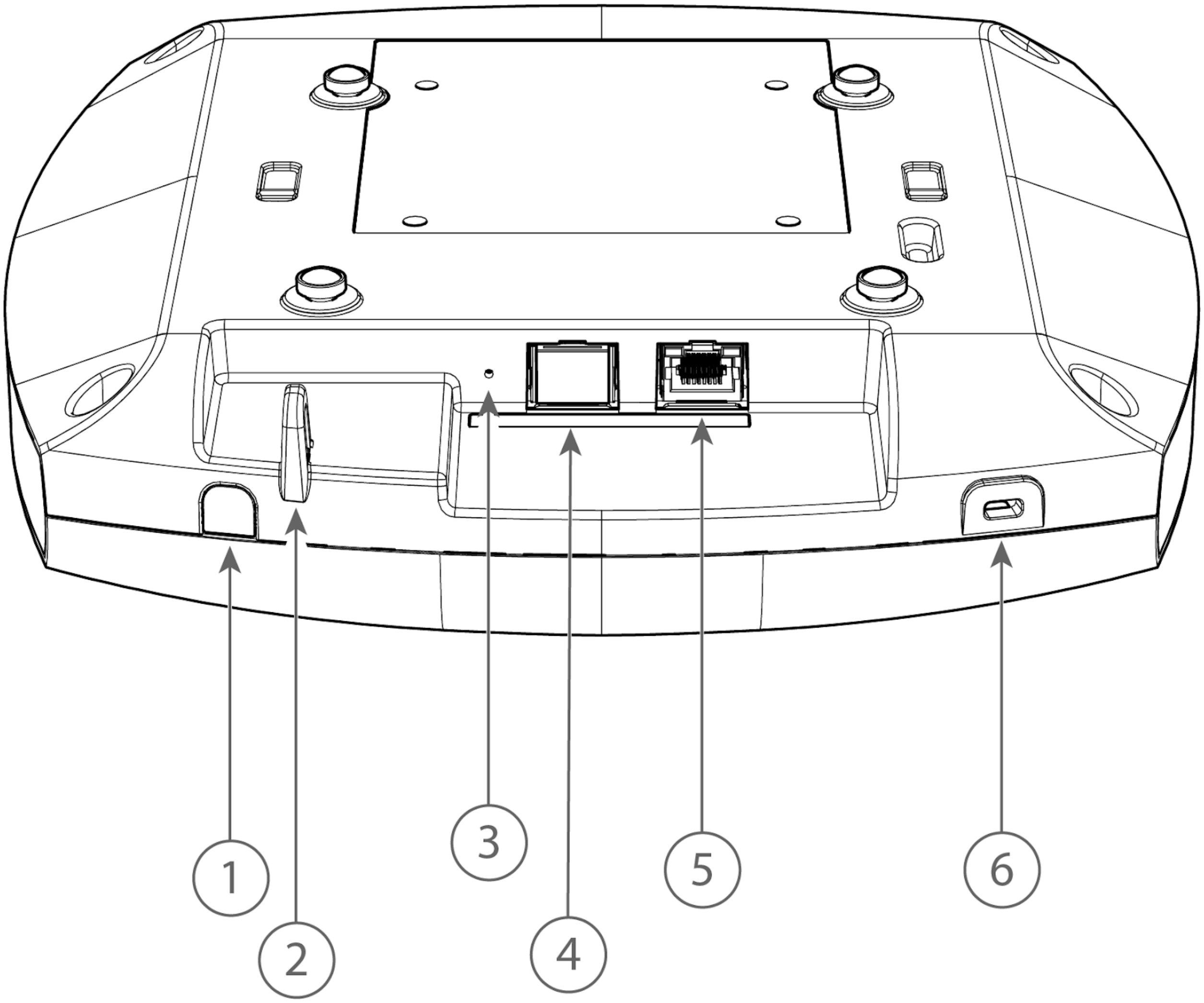
Your CW9176D1 has the following features:

CW9176D1 Face View



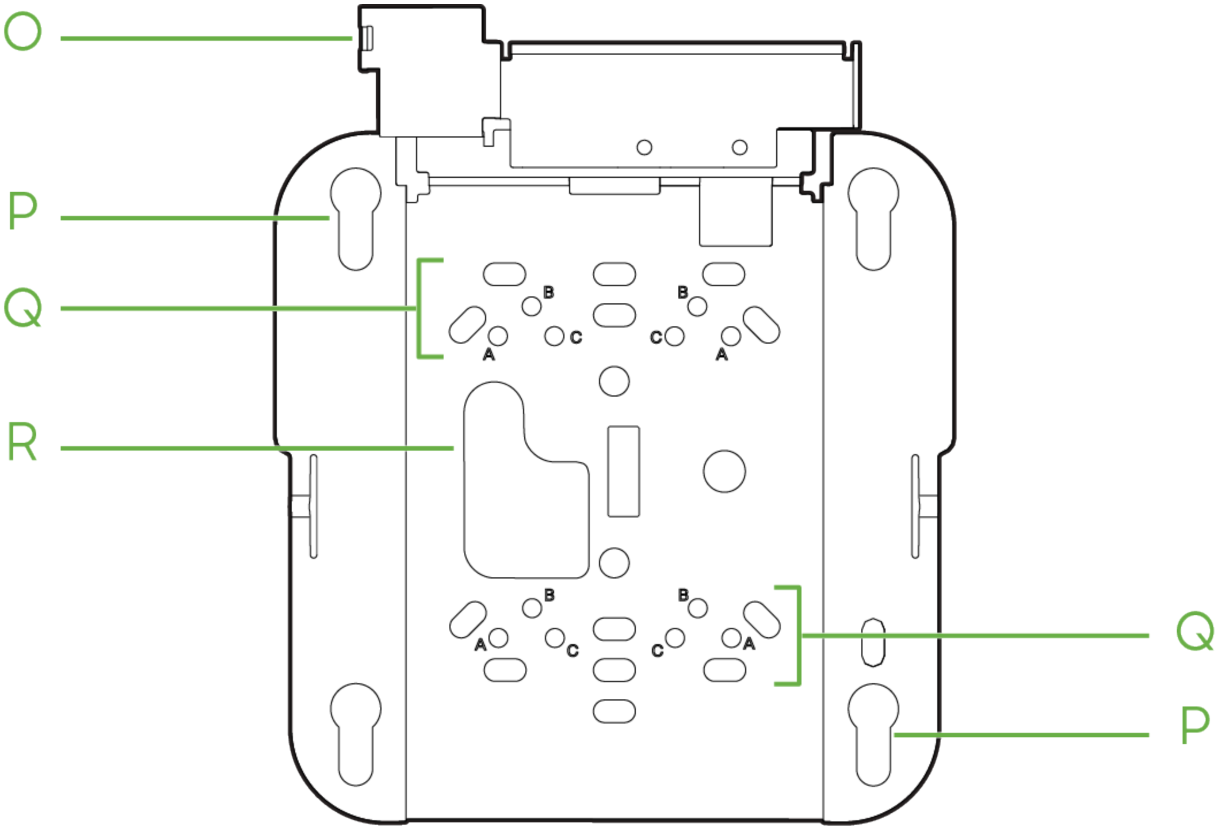
1. Security hasp for padlocking AP to the mounting bracket.
2. Kensington lock socket
3. USB 2.0 Port
4. Status LED

CW9176D1 Top View



1. GPS Antenna Port
2. Security hasp for padlocking AP to the mounting bracket.
3. Mode button
4. RJ-45 Console Port
5. Ethernet Port (Eth1)
6. Kensington Lock slot

The AP ships with Cisco "mounting bracket 2" (AIR-AP-BRACKET-2) that has the following features:



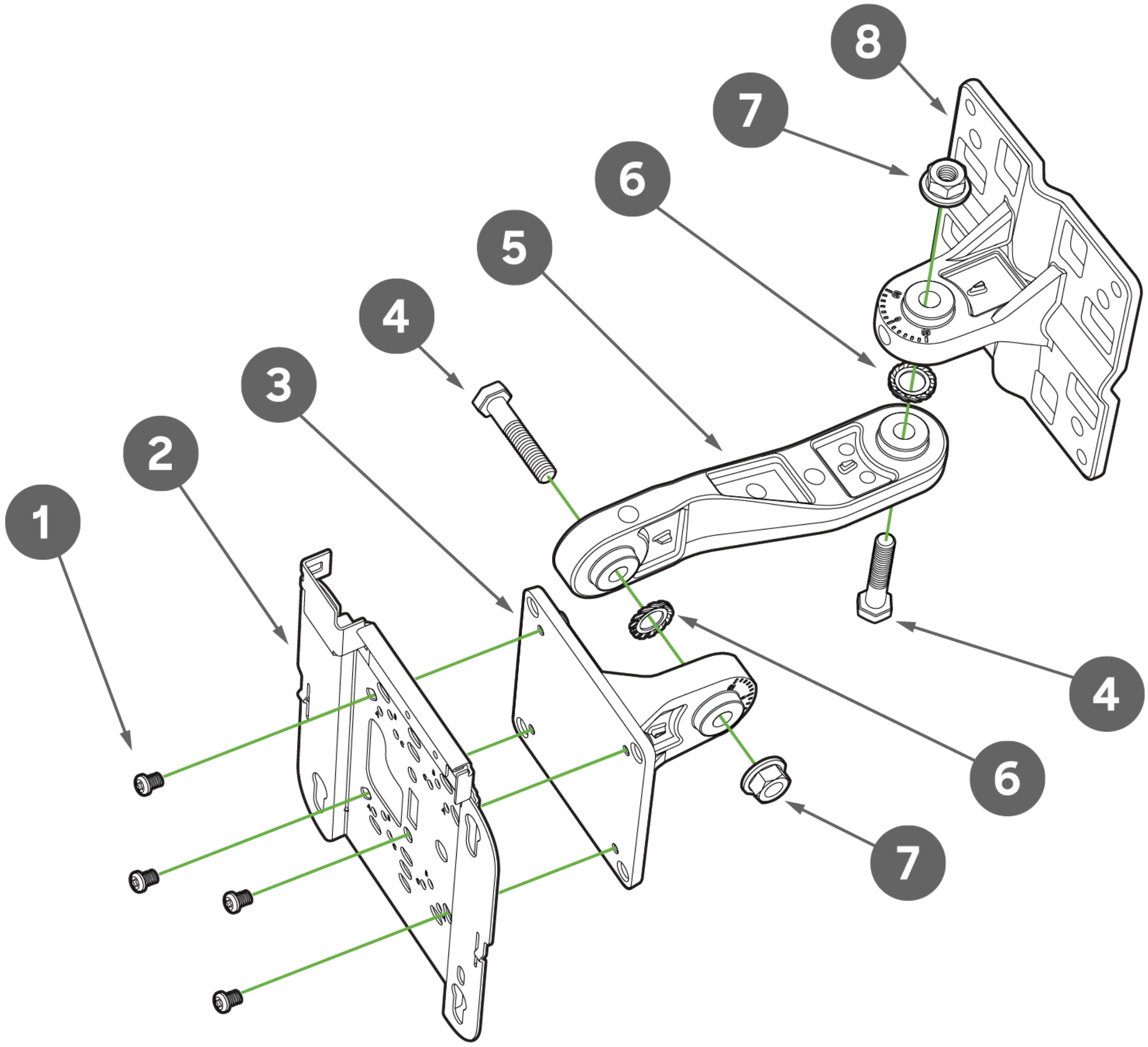
O - Security Hasp

P - Access Point Mounting Keyholes

Q- T-rail attachment points

R - Cable access slot

The AP can also be installed with the optional (purchased separately) articulating arm (CW-MNT-ART2-00), which has the following features:



1 - M4 X 10mm screw with washer

2 - AIR-AP-BRACKET-2 (Not included in this kit., Included with the AP)

3 - Access point bracket plate

4 - M8 x40 Hex bolts

5 - Mounting arm

6 - M8 washer (external-tooth)

7 - M8 flanged lock nut

8 - Pole or wall mounting flange

Security Features

These APs feature multiple options for physically securing the access point after installation:

1. Security hasp – The universal mounting bracket has a security hasp and can be used to secure the access point to the universal mounting bracket. Engaging the security screw prevents accidental dislodging and theft.

2. Kensington lock – The access point contains a hard point that allows it to be secured to any nearby permanent structure using a standard Kensington lock.

Ethernet Ports

The CW9176D1 features one RJ45 Ethernet port capable of operating at 100/1000/2.5G/5G/10G BASE-T Ethernet (RJ45).

<..> 10G **?**

The labeled "<..> 10G **?**" accepts 802.3af , 802.3at and 802.3bt power. This port is typically used as the primary uplink to your LAN/WAN.

Note: The CW9176D1 needs 802.3bt, class 6 (up to 60W) for full operation of AP. They can operate with 802.3at power but with a degraded operation.

Note: When operated with 802.3af, the AP powers up and connects to the Meraki Dashboard, but all the Radios will be operationally down.

Note: Cat 6/6A cabling is recommended for CW9176, as they support speeds up to 10Gig.

Warning: Some of the pre-standard 802.3at/PoE+ switches do not negotiate full 802.3at power output with the CW9176D1 by default. For these switches (Cisco Catalyst 2960,3560, etc) the switch port that is connected to and powering up the CW9176D1 should be manually configured to provide 30 watts of power. This can be done by going into the interface of the switch and setting the inline power to 30 watts using the following command.

power inline consumption 30000

before actually powering up the AP. Failure to do so may result in the CW9176D1 not receiving enough power to operate and can remain at low power which can cause the APs to continuously reboot.

Power Source Options

CW9176D1 can be powered by 802.3bt capable PoE ports. The AP is capable of operating at its full capacity when powered by a single 802.3bt power at full capacity. The AP needs 802.3bt, Class 6 that can supply 60W of power for full operation. The table below indicates the different modes of PoE power input and the expected operation of the AP.

PoE	Ethernet Speed	2.4 XOR 5 GHz	5GHz	6GHz	Scan
AF	1 Gig	OFF	OFF	OFF	ON
AT	1 Gig	2x2	4x4(FB)	4x4	ON
AT	1 Gig	2x2 (5 GHz LB)	4x4 (5 GHz HB)	2x2	ON
BT	10 Gig	4x4	4x4	4x4	ON
BT	10 Gig	4x4 (5 GHz LB)	4x4 (5 GHz HB)	4x4	ON

CW9176D1 APs can be powered by the PoE power in different modes as mentioned above when using a PoE-capable switch. CW9176D1 can also be powered by a single 802.3bt capable PoE injector CW-INJ-8, Cisco Wireless multiGigabit 802.3bt Power over Ethernet Injector.

Factory Reset Button

If the button is pressed and held for at least sixty seconds and then released, the AP will reboot and be restored to its original factory settings by deleting all configuration information stored on the unit.

Below is the sequence of reset:

Approx 5 seconds - Blink Green for Meraki Mode

More than 10 seconds - Clear config

More than 20 seconds - Full reset, maintain management mode

More than 30 seconds - Clear FIPS config (Only for Catalyst Mode)

More than 60 seconds - Factory reset

ⓘ **Note:** For more details on resetting CW Access Points, please see Resetting Cisco Meraki Devices to Factory Defaults.

LED Indicators and Run Dark Mode

Your access point is equipped with a multi-color LED light on the front of the unit to convey information about system functionality and performance:

- Orange - AP is booting (permanent Orange suggests hardware issue)
- Rainbow - AP is initializing/scanning
- Blinking Blue - AP is upgrading
- Green - AP in Gateway mode with no clients

- Blue - AP in Gateway mode with clients
- Blinking Orange - AP can't find uplink

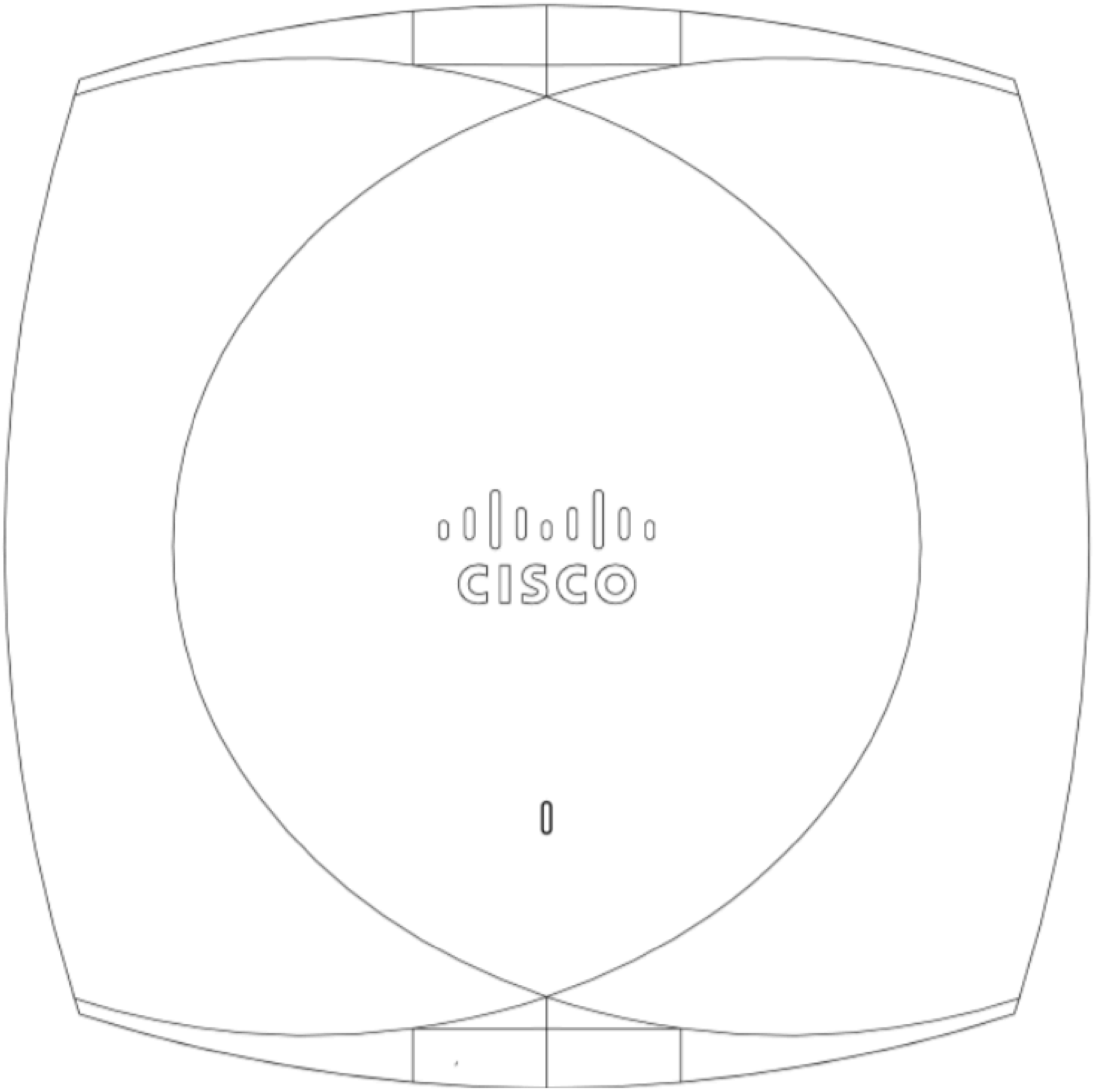
NOTE: A blinking Green LED indicates that the device is in site survey mode. Please see the Conducting Site Surveys with MR Access Points for more details.

The CW9176D1 access point may be operated in the “Run Dark” mode for additional security and to reduce the visibility of the access point. In this mode, the LED will not be illuminated. This mode may be enabled through the Meraki Dashboard.

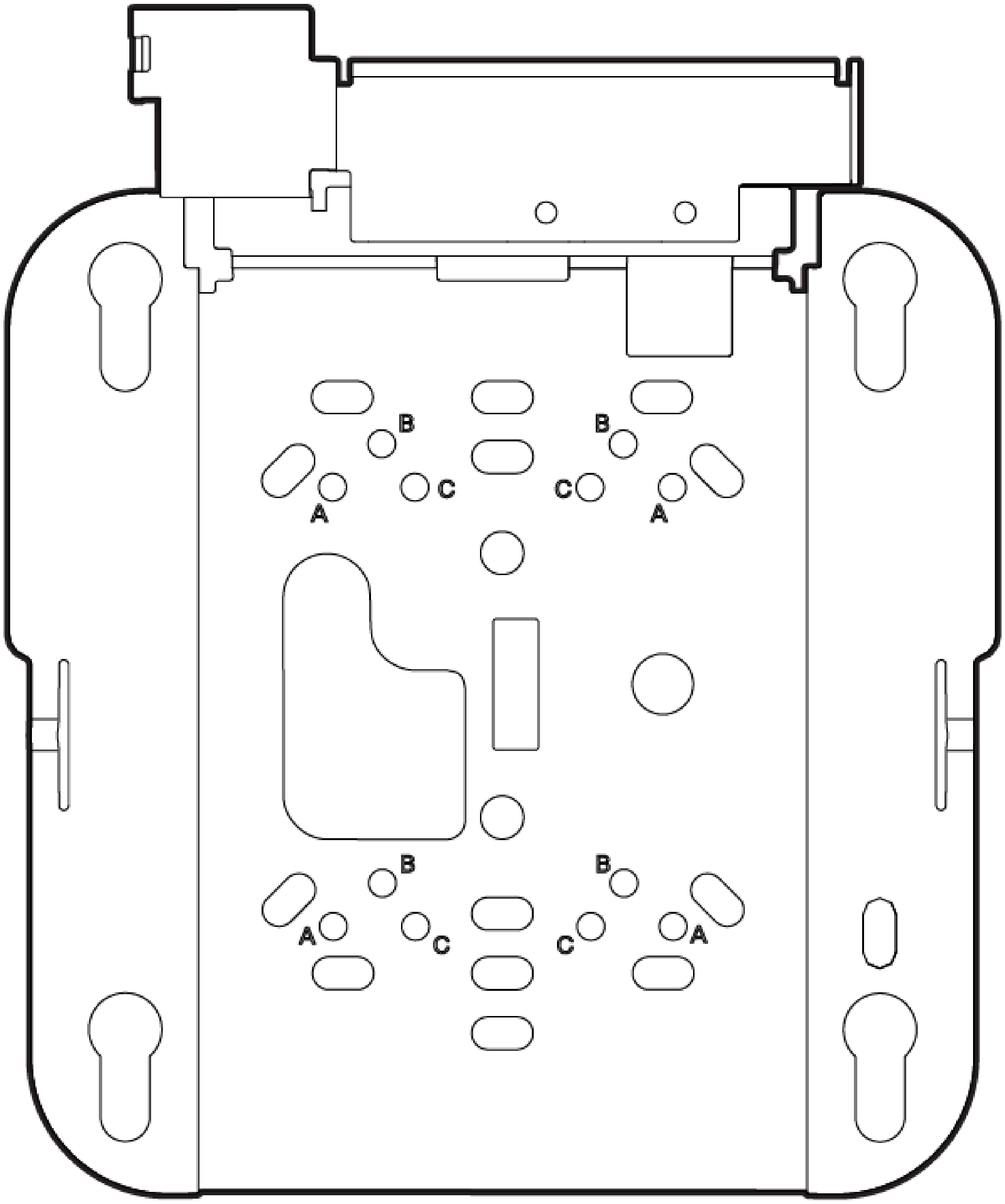
Package Contents

The access point packages contain the following:

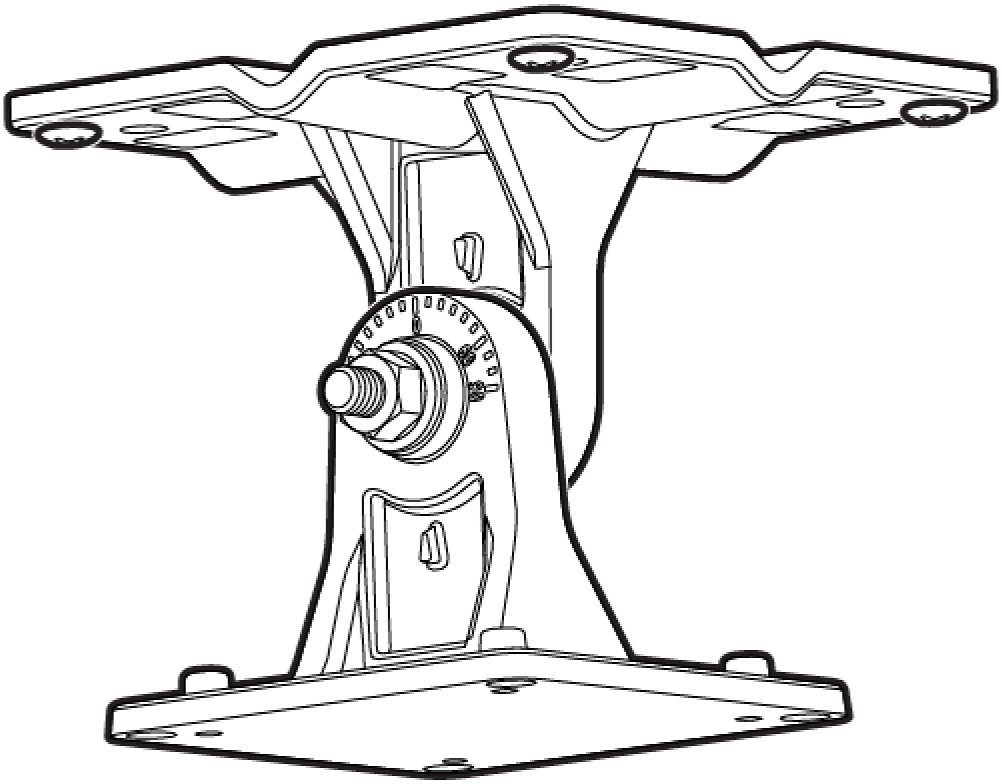
CW9176D1 Cloud-Managed Access Point



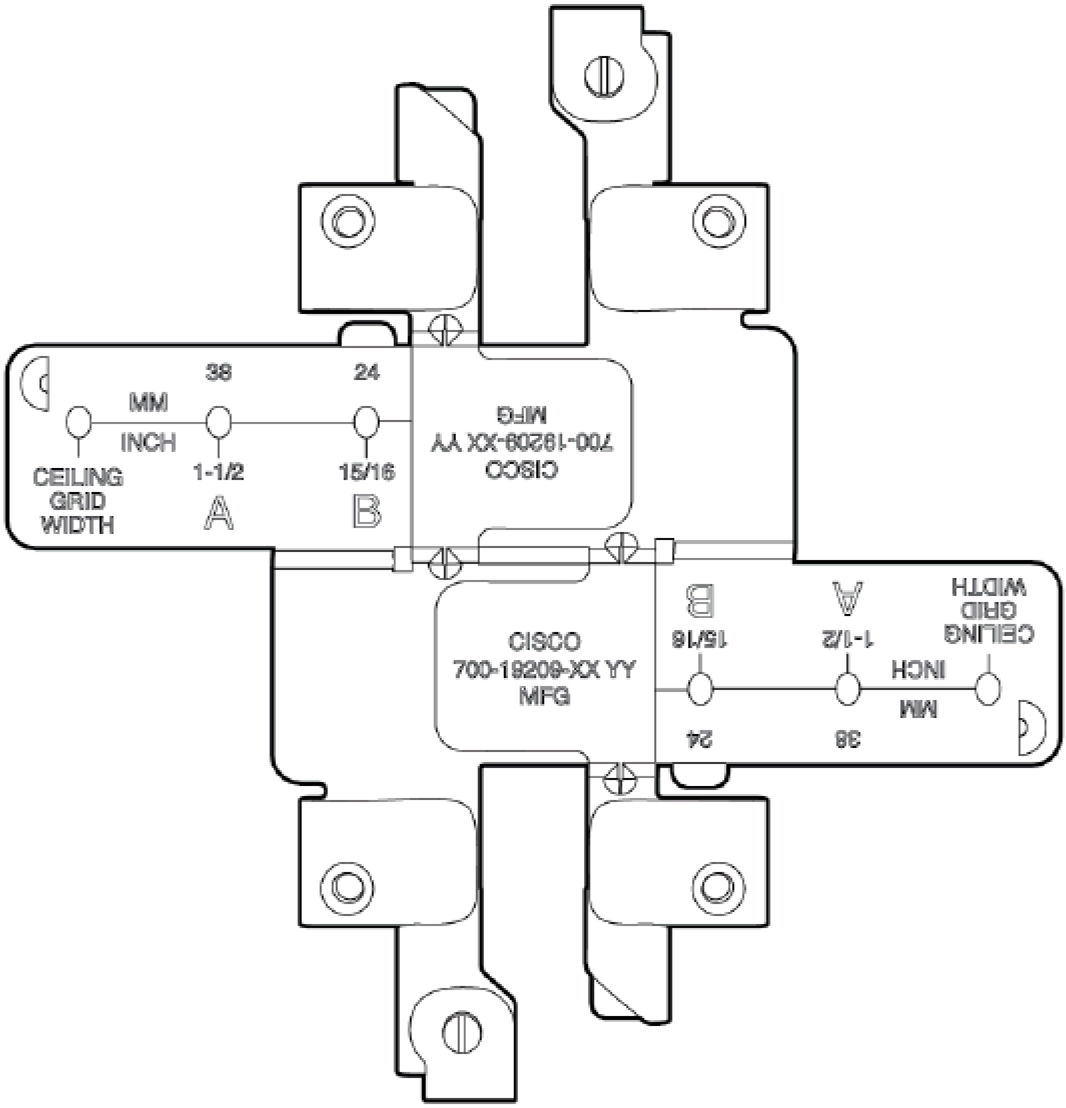
Cisco Universal Mount Bracket - AIR-AP-BRACKET-2

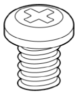


Cisco Articulating Arm - CW-MNT-ART2-00 (Optional)



T-Rail mount attachment (AIR-AP-T-RAIL-R) and screws (5 Nos - 6-32 x 1/4 included) (Optional)




x5

Safety and Warnings

These operations must adhere to full compliance with all applicable local laws. Please consider the following for safe operation:

• Power off the unit before you begin. Read the installation instructions before connecting the system to the power source.

• 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 wall-mounting instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation for people and damage to the system.

• This product relies on the building’s installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 15 A, 125 Vac, or 10A, 240 Vac.

• Please only power the device with the provided power cables or standard PoE to ensure regulatory compliance.

Pre-install Preparation

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

Configure your Dashboard Network

The following is a brief overview only of the steps required to add an access point to your network. For detailed instructions about creating, configuring, and managing Meraki wireless networks, refer to the online documentation (documentation.meraki.com).

1. Log in to http://dashboard.meraki.com. If this is your first time, create a new account.

2. Find the network to which you plan to add your APs or create a new network.

3. Add your APs to your network. You will need your Meraki order number (found on your invoice) or the serial number of each AP, which looks like Qxxx-xxxx-xxxx, and is found on the bottom of the unit. You will also need your license key, which you should have received via email.

4. Go to the map/floor plan view and place each AP on the map by clicking and dragging it to the location where you plan to mount it.

Check and Set the Firmware

To ensure your access point performs optimally immediately following installation, it is recommended that you facilitate a firmware upgrade prior to mounting your AP.

1. Attach your AP to power and a wired Internet connection. See the "Getting Power to the AP" section for details.

2. The AP will turn on and the LED will glow solid orange. If the unit does not require a firmware upgrade, the LED will turn either green (no clients associated) or blue (clients associated) within thirty seconds.

* If the unit requires an upgrade, the LED will begin blinking orange until the upgrade is complete, at which point the LED will turn solid green or blue. You should allow at least a few minutes for the firmware upgrade to complete, depending on the speed of your internet connection.

Check and Configure Upstream Firewall Settings

If a firewall is in place, it must allow outgoing connections on particular ports to particular IP addresses. The most current list of outbound ports and IP addresses for your particular organization can be found on the firewall configuration page in your dashboard.

Assigning an IP Address

All gateway APs (An AP with Ethernet connections to the LAN) must be assigned a routable IP address. These IP addresses can be dynamically assigned via DHCP or statically assigned.

Static Assignment

- Static IPs are assigned using the local web server on each AP. The following procedure describes how to set the static IP:

- Using a client machine (e.g., a laptop), connect to the AP wirelessly (by associating to any SSID broadcast by the AP) or over a wired connection.

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

- Using a web browser on the client machine, access the AP’s built-in web server by browsing http://my.meraki.com. Alternatively, browse to http://10.128.128.128.

- Click on the “Uplink Configuration” tab. Log in. The default login is the serial number (e.g. Qxxx-xxxx-xxxx), with no password (e.g., Q2DD-551C-ZYW3).

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

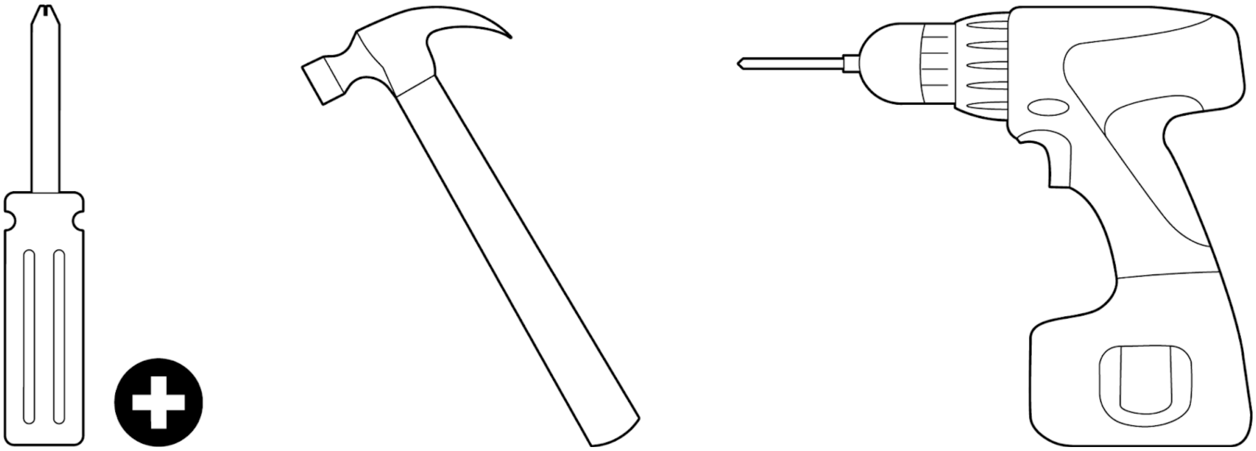
- If necessary, reconnect the AP to the LAN.

Static IP via DHCP Reservations

- Instead of associating to each Meraki AP individually to configure static IP addresses, an administrator can assign static IP addresses on the upstream DHCP server. Through “DHCP reservations,” IP addresses are “reserved” for the MAC addresses of the Meraki APs. Please consult the documentation for the DHCP server to configure DHCP reservations.

Collect Tools

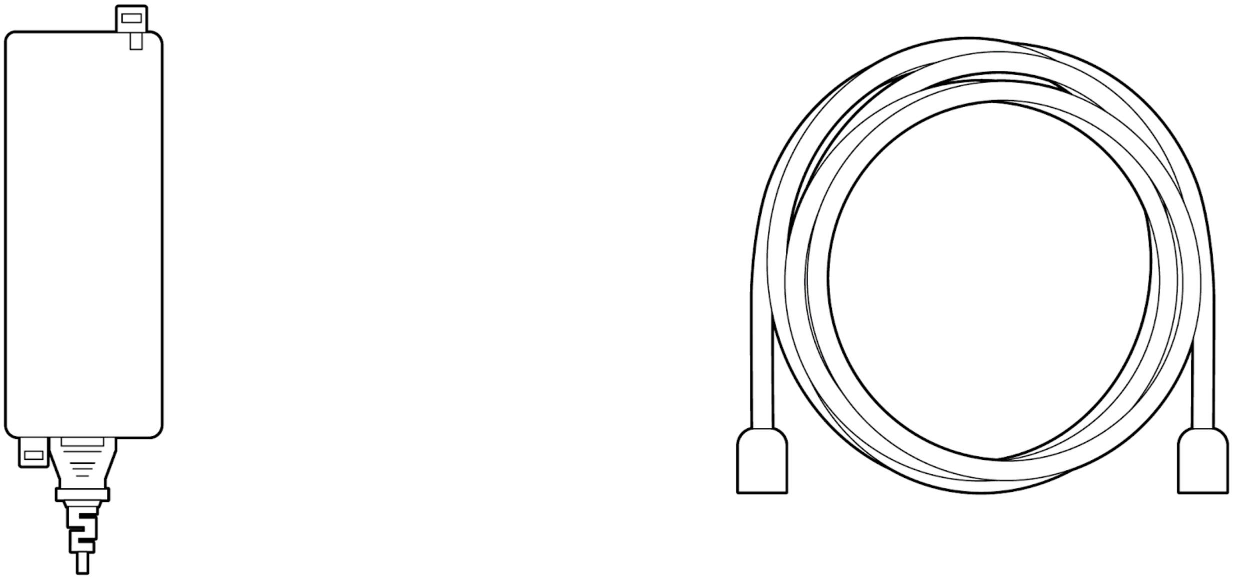
You will need the following tools to perform an installation:



Phillips screwdriver, Hammer (optional), Drill with 1/4" (6.3mm) bits (optional) - depending on install type

Collect Additional Hardware for Installation

You will need the following hardware to perform an installation:



802.3bt/at PoE Power Source (either PoE switch or Meraki 802.3bt/at PoE Injector) and network cables with RJ45 connectors long enough for your particular mounting location

> **Note:** CW9166D1 does not support 802.3af power sources.
>
> **Note:** CW9166D1 can be powered by a PoE Switch, PoE Injector or an AC adaptor. Powering up the AP with an AC adapter while connecting to a PoE source is not recommended. Proper functionality of the AP is not guaranteed and this can potentially cause damage to the AP hardware.

Installation Instructions

Choose Your Mounting Location

The Cisco Catalyst Wireless 9166D1 Series Wi-Fi 6E Access Point can be mounted in the following places:

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

A good mounting location is important to get the best performance out of your access point. Keep the following in mind:

1. The device should have an unobstructed line of sight to most coverage areas. For example, if installing in an office filled with workspaces divided by mid-height cubicle walls, installing on the ceiling or high on a wall would be ideal.

2. Power over Ethernet supports a maximum cable length of 300 ft (100 m).

3. If being used in a mesh deployment, the AP should have a line of sight to at least two other Meraki devices. A Cisco Partner and/or site survey can help

ensure that your AP placement is ideal.

Install the AP

For some mounting scenarios, the access point universal mounting bracket provides a quick, simple, and flexible means of mounting your device. The installation should be done in two steps. First, install the universal mounting bracket to your selected location. Then, attach the AP to the universal mounting bracket.

If you have purchased the separate articulating bracket accessory, you can mount the AP in other configurations and change the direction the AP is facing.

Attaching the Universal Mounting Bracket

The access point universal mounting bracket (AIR-AP-BRACKET-2 - included) can be used to install your access point in a wide range of scenarios including a wall or solid ceiling, below a drop ceiling, or on various electrical junction boxes.

Wall Mount the AP using a Universal Mounting Bracket

To mount the AP on the wall first, identify the location of the wall

1. Use the mounting bracket as a template to mark the locations of the mounting holes on the bracket

2. Use a 0.1360-in. [3.4772 mm] bit to drill a pilot hole at the mounting hole locations you marked.

3. Locate the pilot holes and then insert a fastener(not included) into each mounting hole and tighten.

4. Place the universal mounting bracket over the faster holes and then use screws up to 6 mm in diameter and at least 1 - 1/4 inch in length (not included) to tighten it flush to the wall

The AP is now ready to be mounted on the wall

Electrical Junction Box Mount Using Universal Mounting Bracket

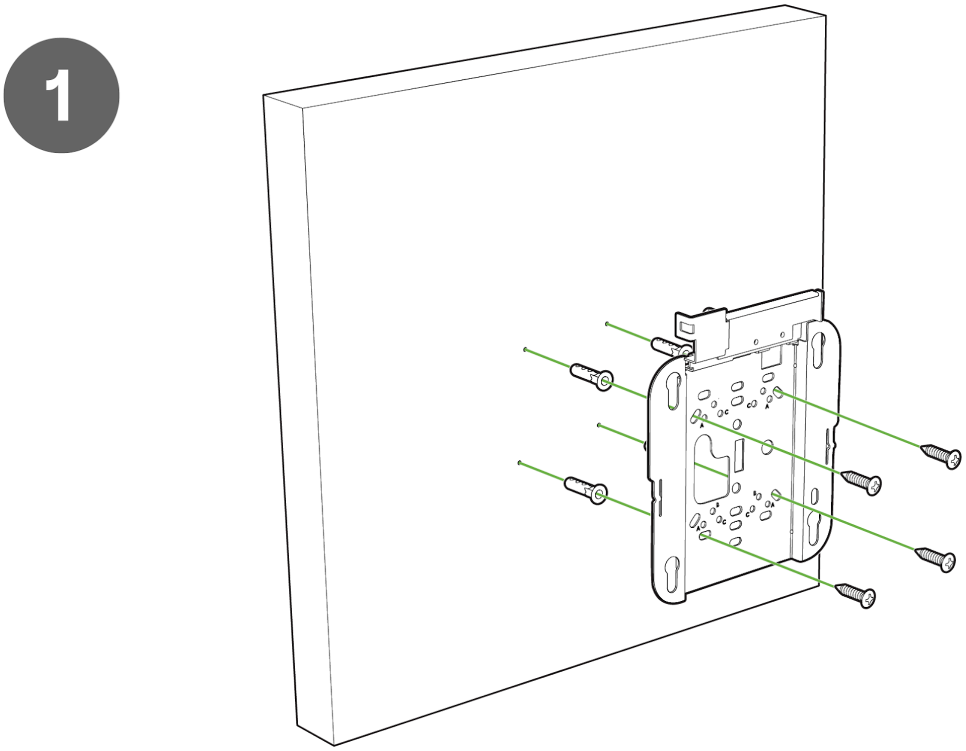
The access point can be mounted to a 4” square cable junction box, a 3.5 or 4” round cable junction box, or various U.S. and European outlet boxes (mounting screws are not included).

Using appropriate mounting hardware for your specific type of junction box, attach the universal mounting bracket to the junction box.

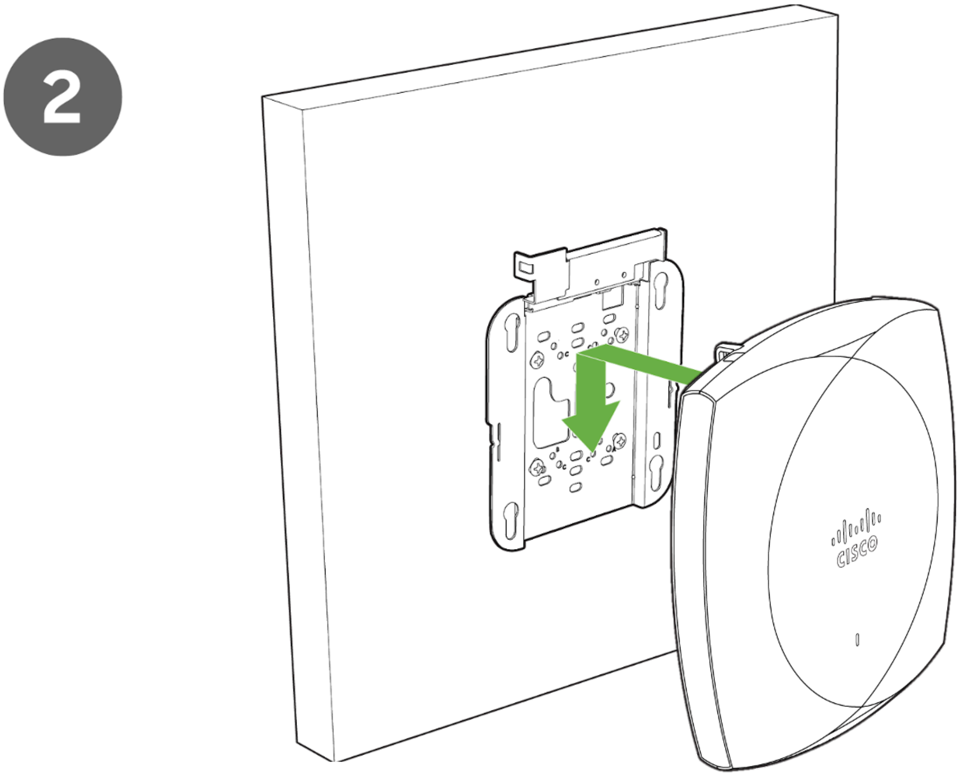
Attach the AP to the Universal Mounting Bracket

The AP has four rubber feet that when gently slid in attach to the universal mounting bracket

1. Install the universal mounting bracket to the wall/ceiling.

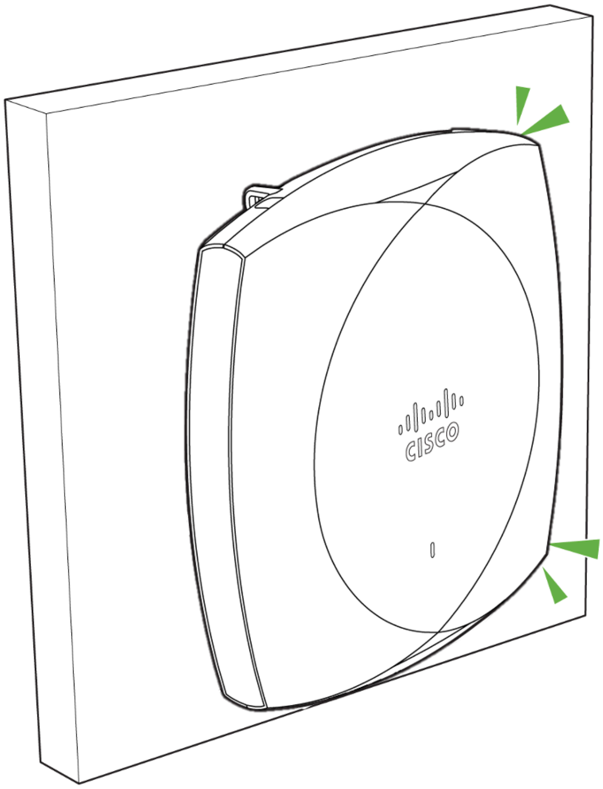


2. To attach the AP to the universal mounting bracket properly, align the access point feet over the keyhole mounting slots on the mounting bracket.



3. Since the cradle is already mounted to the wall/ceiling, gently guide the AP towards the mounting cradle until it clicks into place.

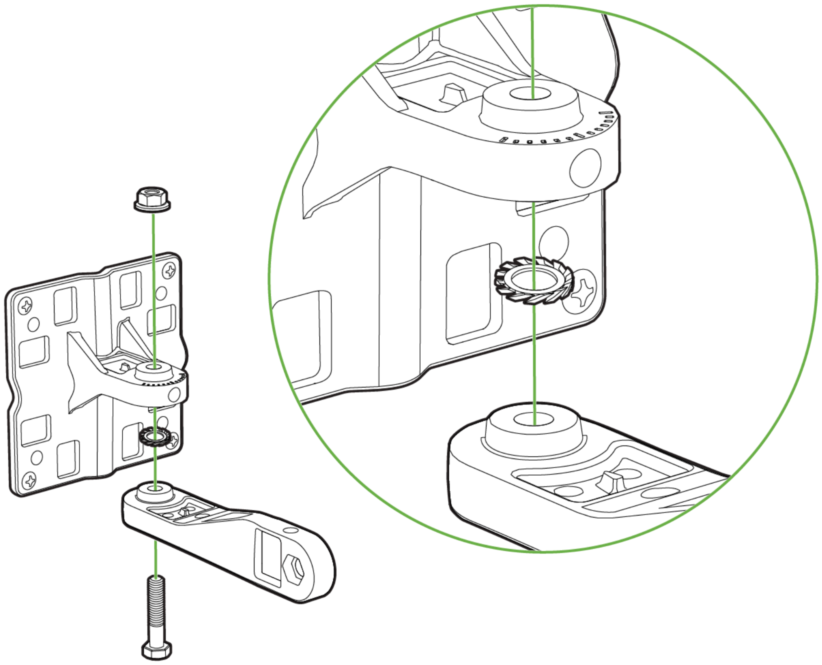
3



Mounting on a Wall or Ceiling Using Articulating Bracket

1. Assemble the mounting arm by connecting the mounting arm and the wall mounting flange. Hand tighten the screw, M8 washer, and screw.

1

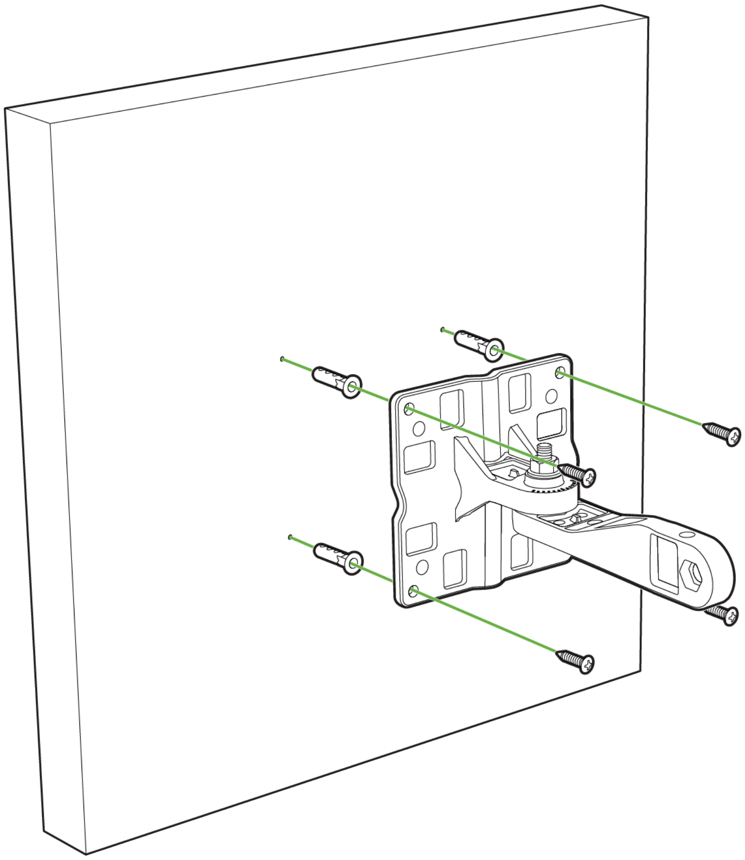


2. Determine the mounting location for the access point and attach the wall mounting flange to the wall or ceiling using four M6 screws through the holes in the bracket.

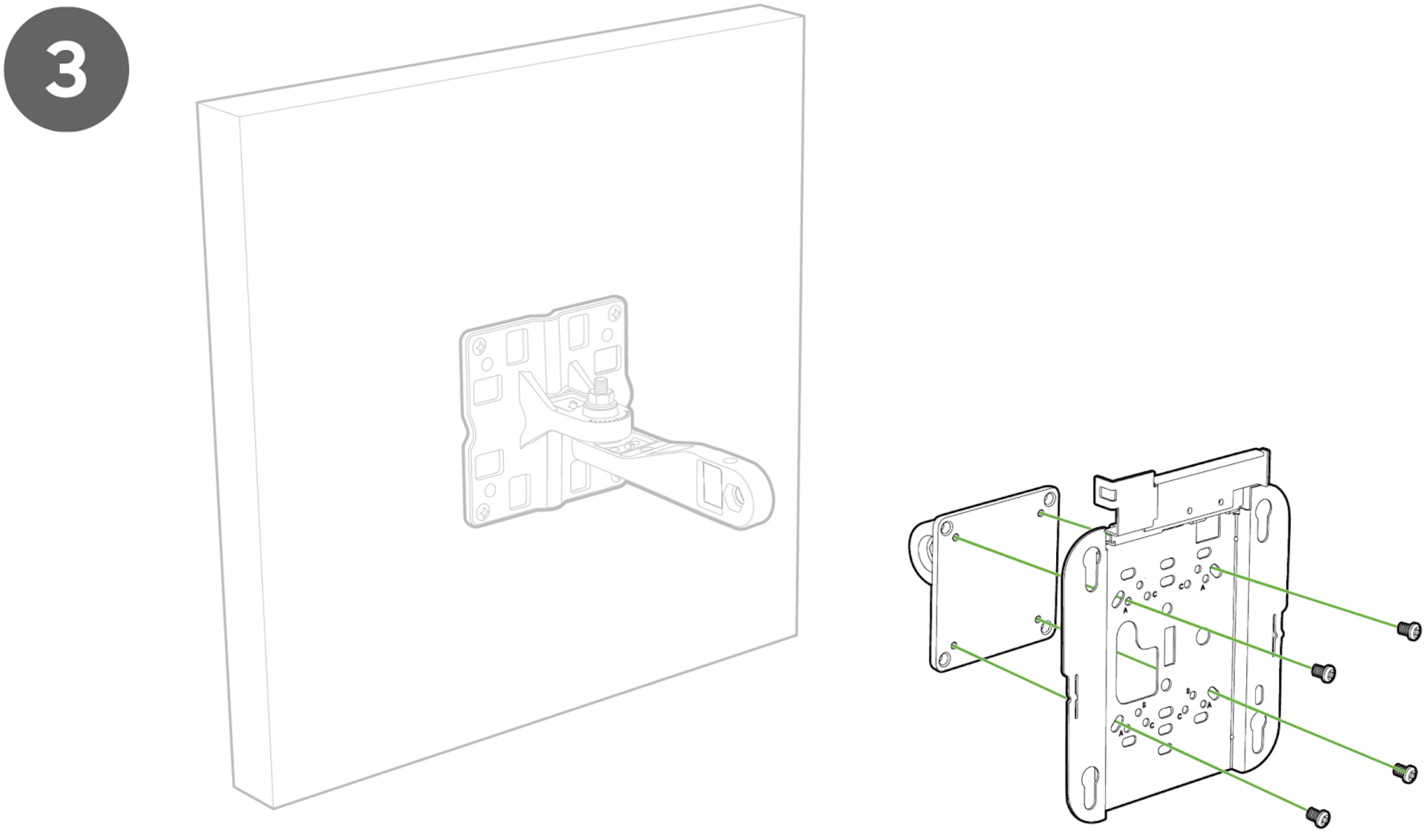
Caution: The mounting wall, attaching screws, and wall anchors must support a 50-lb (22.7–kg) static weight.

Note: The mounting kit does not include the M6 screws for securing the bracket to the mounting surface.

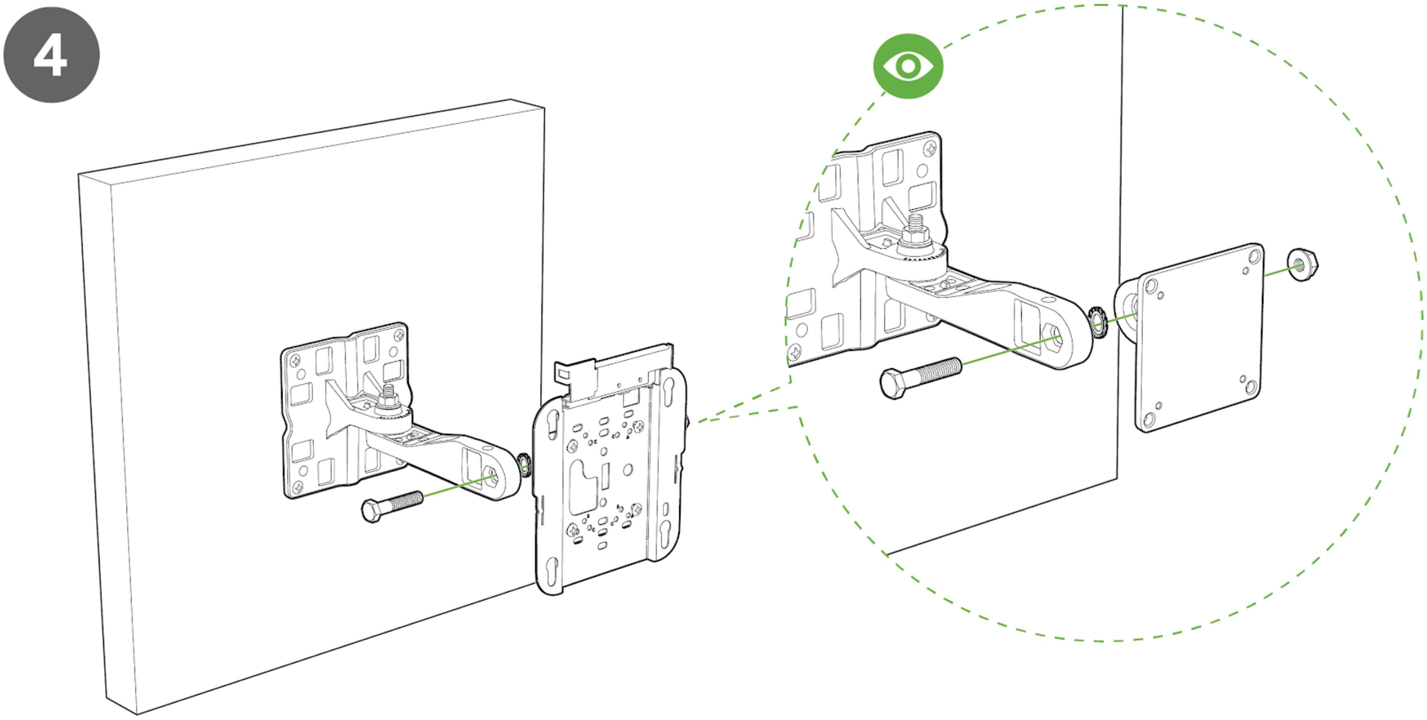
2



3. Attach the AIR-AP-BRACKET-2 to the access point bracket plate by using four M4 screws through the holes in the bracket. Hand tighten the four screws.

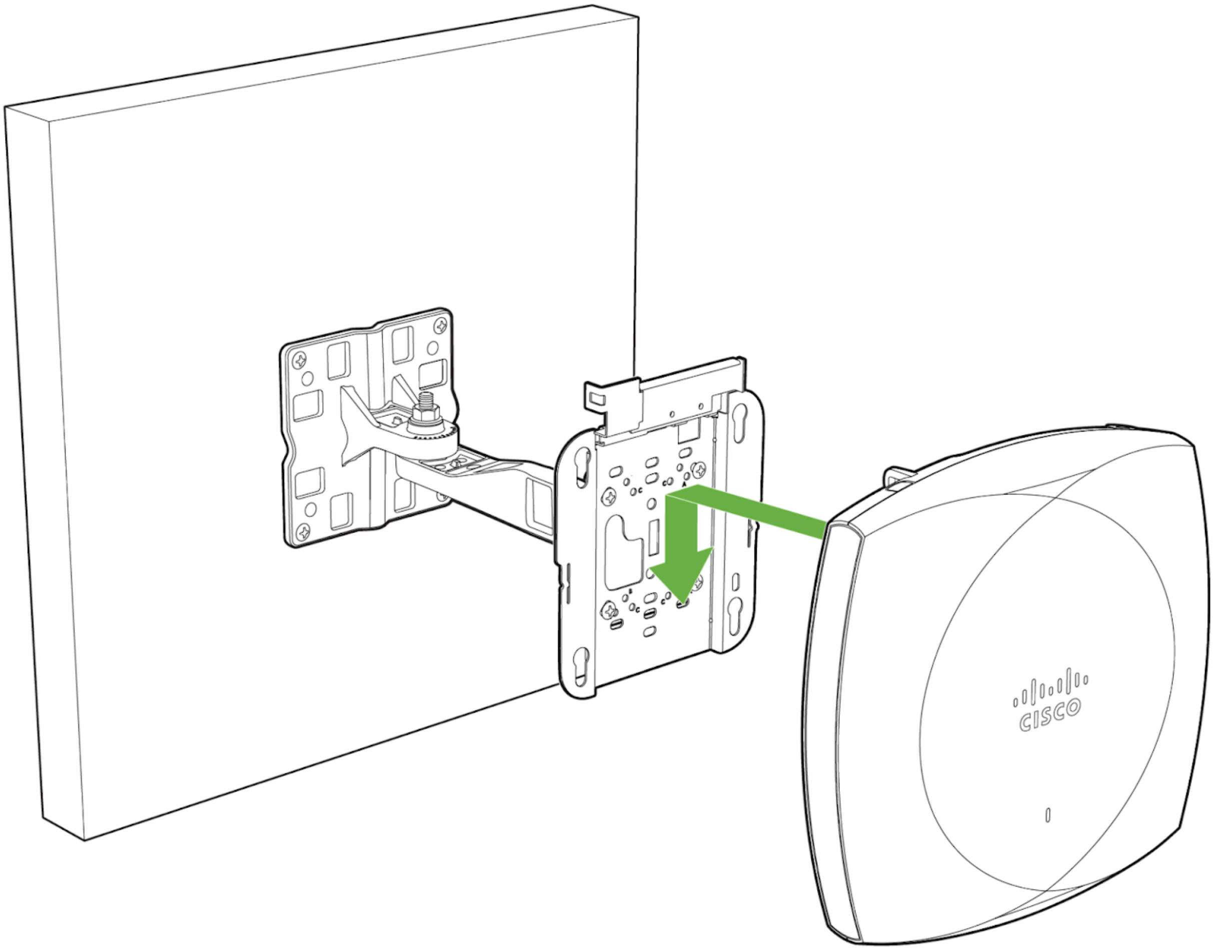


4. Connect the access point bracket plate connected to the AIR-AP-BRACKET-2 with the mounting arm. Hand tighten the screw, M8 washer, and screw.



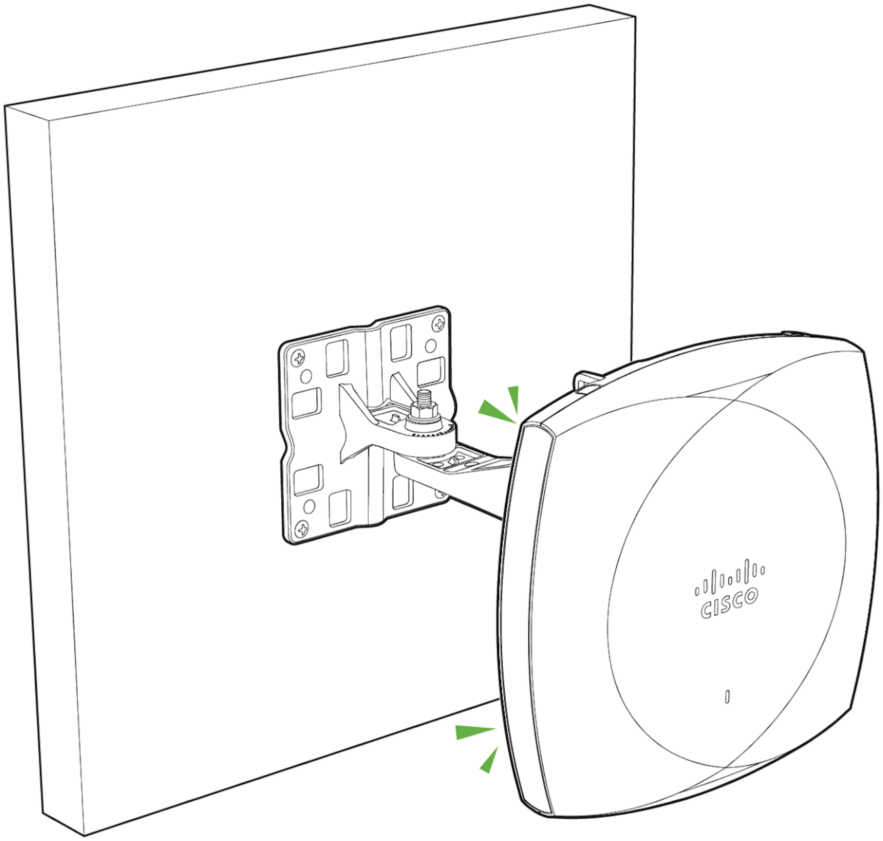
5. Attach the access point to the AIR-AP-BRACKET-2. Use a 13 mm wrench to loosen or tighten the fasteners at the azimuth- and elevation-adjustment pivots.

5



6. Adjust the access point's azimuth (side-to-side position) and elevation (up-and-down position). Loosen the adjustment pivot nuts slightly to allow for adjustment. Use the azimuth and elevation markings on the articulating mounting arm and the flange brackets as a guide. You may adjust the azimuth angle up to ±60 degrees and elevation up to +60 / -90 degrees.

6



7. After adjusting the access point position, tighten the pivot nuts. Tighten all nuts at the pivot points to 5.6 lb-ft to 5.9 lb-ft (7.6 Nm to 8.0 Nm) torque.

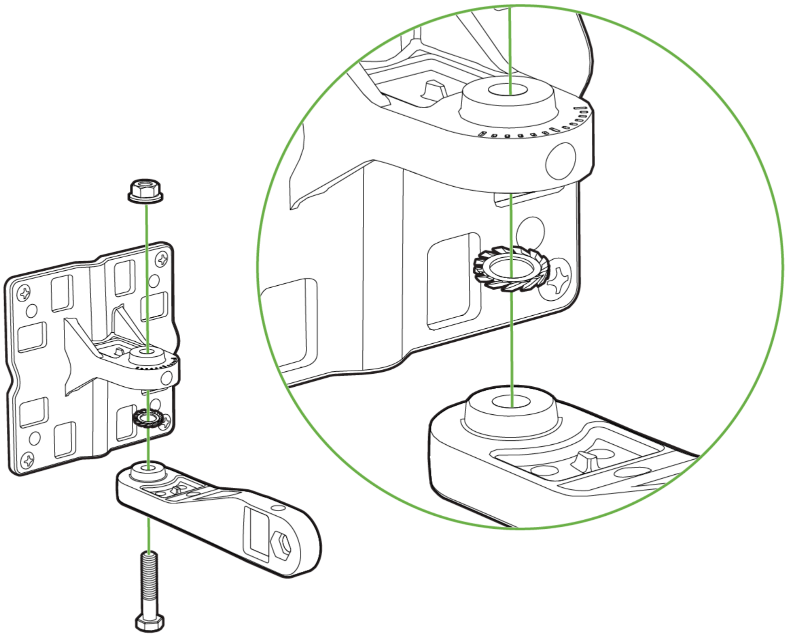
8. Connect the Ethernet cable to the access point using the termination kit.

Mounting on a Pole or Mast Using an Articulating Bracket

> ***Note:*** *The pole or mast must be rigid enough to hold the weight of an access point along with the associated forces produced by wind loads. In addition, the mast must be structurally strong enough to withstand the clamping force of the hose clamps.*

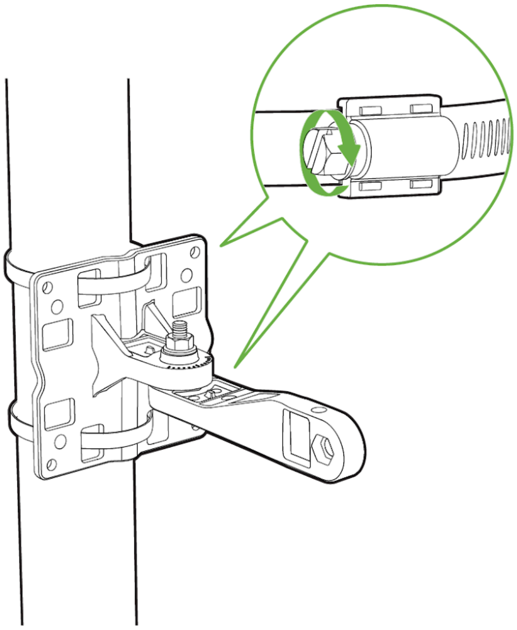
1. Assemble the mounting arm by connecting the mounting arm and the wall mounting flange. Hand tighten the screw, M8 washer, and screw.

1



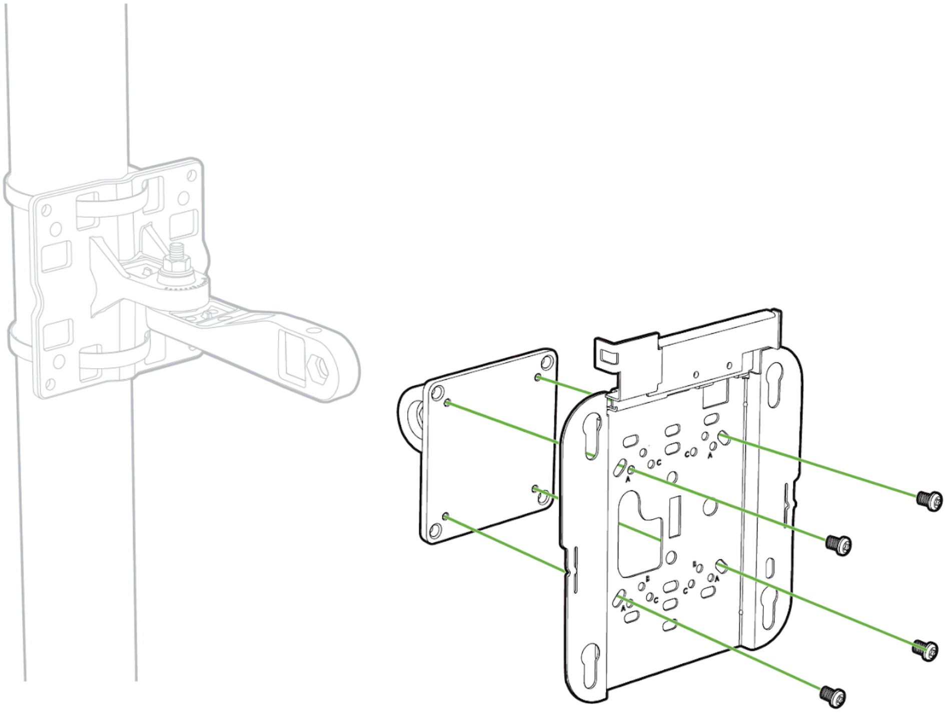
2. Determine the mounting location for the access point on the pole or mast. Position and mount the pole mounting flange onto the pole or mast using the hose clamps provided in the kit. The hose clamps should pass through the slots on the free-mounting flange bracket. Tighten the hose clamps and set screws until the flange is fully secure on the mast. Adjust the flange to its final position. Then, use a slotted screwdriver to tighten the screws on the hose clamps.

2



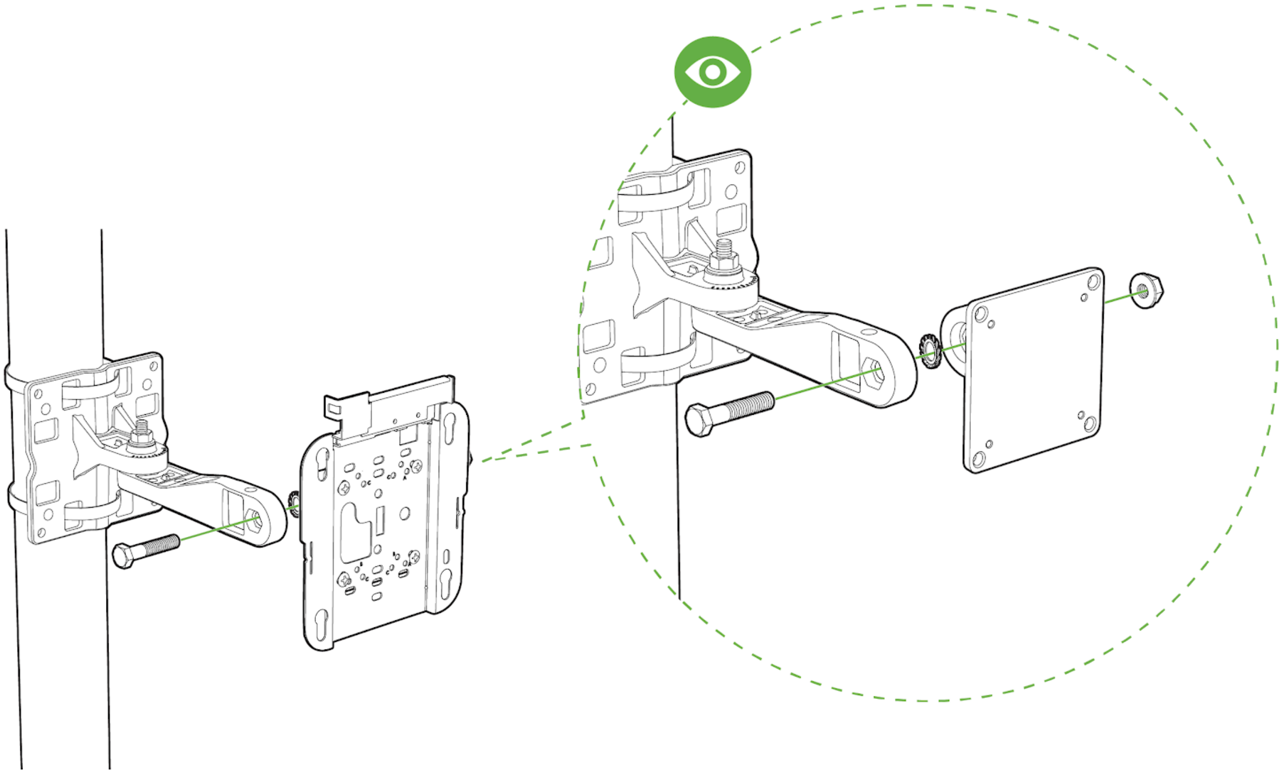
3. Attach the AIR-AP-BRACKET-2 to the access point bracket using four M4 screws through the holes in the bracket. Snugly hand tighten the M4 four screws included in the mounting kit.

3



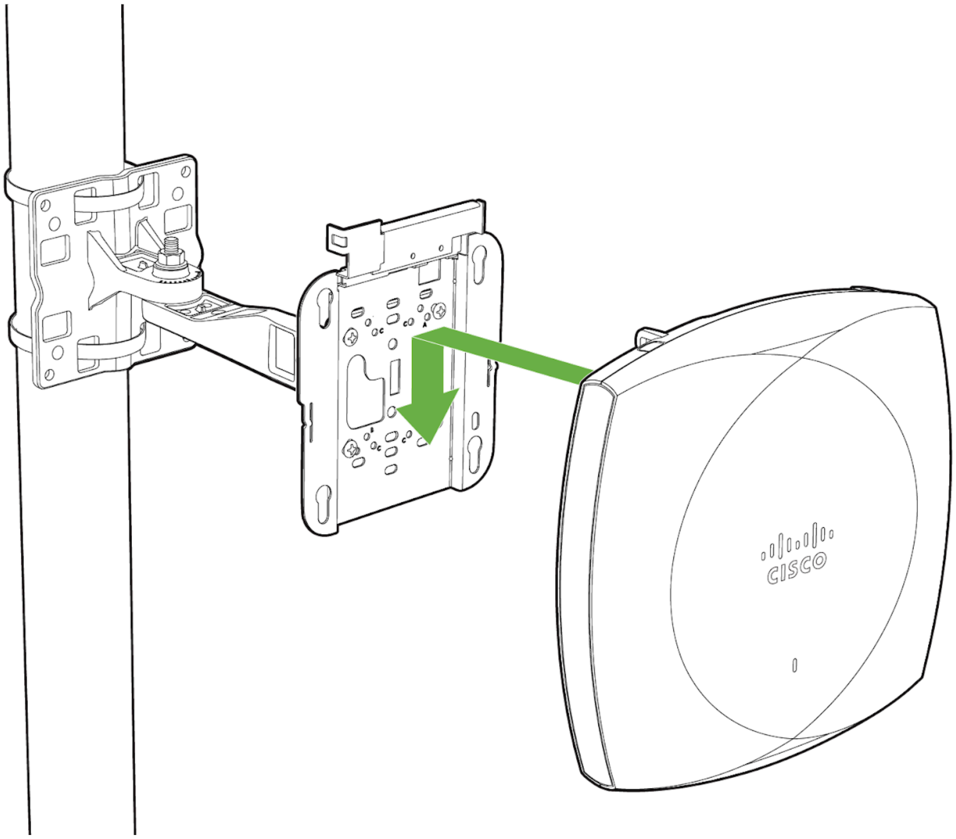
4. Connect the access point bracket plate connected to the AIR-AP-BRACKET-2 with the mounting arm. Hand tighten the screw, M8 washer, and screw.

4



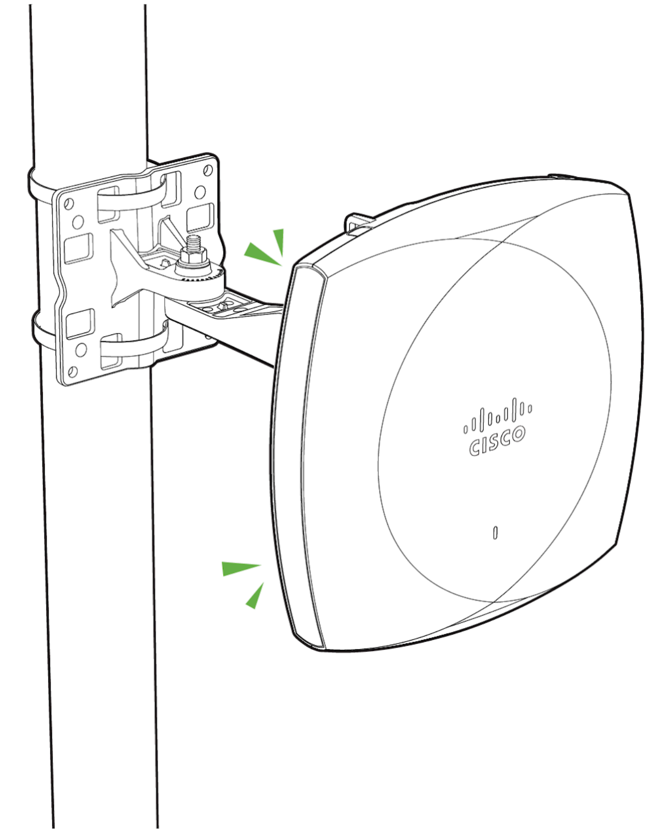
5. Attach the access point to the AIR-AP-BRACKET-2.

5



6. Adjust the access point's azimuth (side-to-side position) and elevation (up-and-down position). Loosen the adjustment pivot nuts slightly to allow for adjustment. Use the azimuth and elevation markings on the articulating mounting arm and the flange brackets as a guide. You may adjust the azimuth angle up to ±60 degrees and elevation up to +60 / -90 degrees.

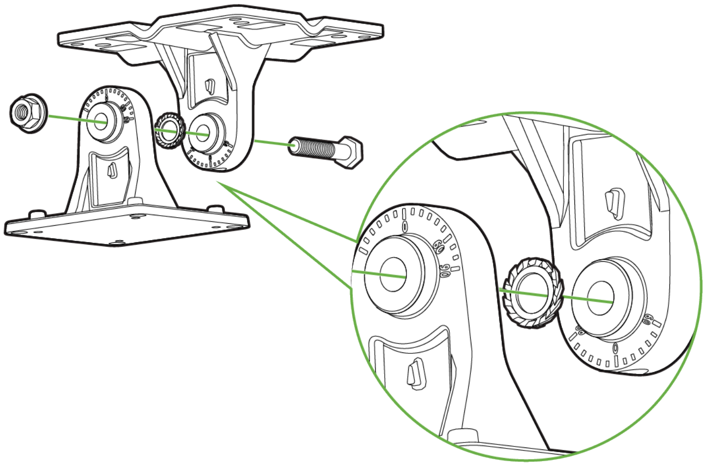
6



Mounting the Access Point Using Single Axis Articulating Bracket

1. Assemble the mounting arm by connecting the mounting arm and the wall mounting flange. Hand tighten the screw, M8 washer, and screw.

1

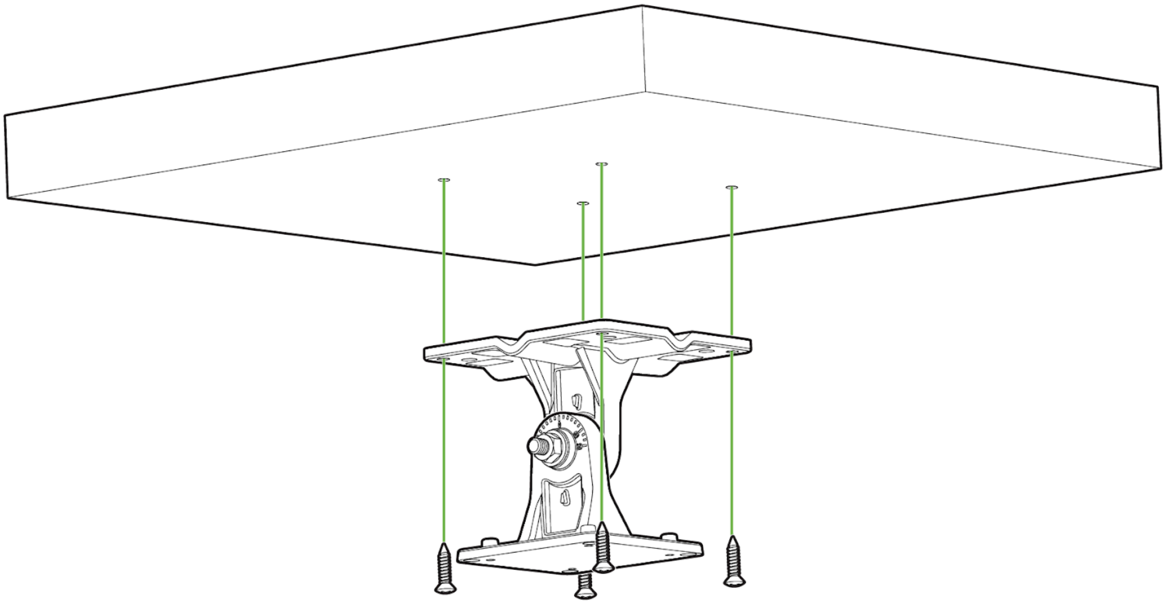


2. Determine the mounting location for the access point and attach the wall mounting flange to the wall or ceiling using four M6 screws through the holes in the bracket.

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

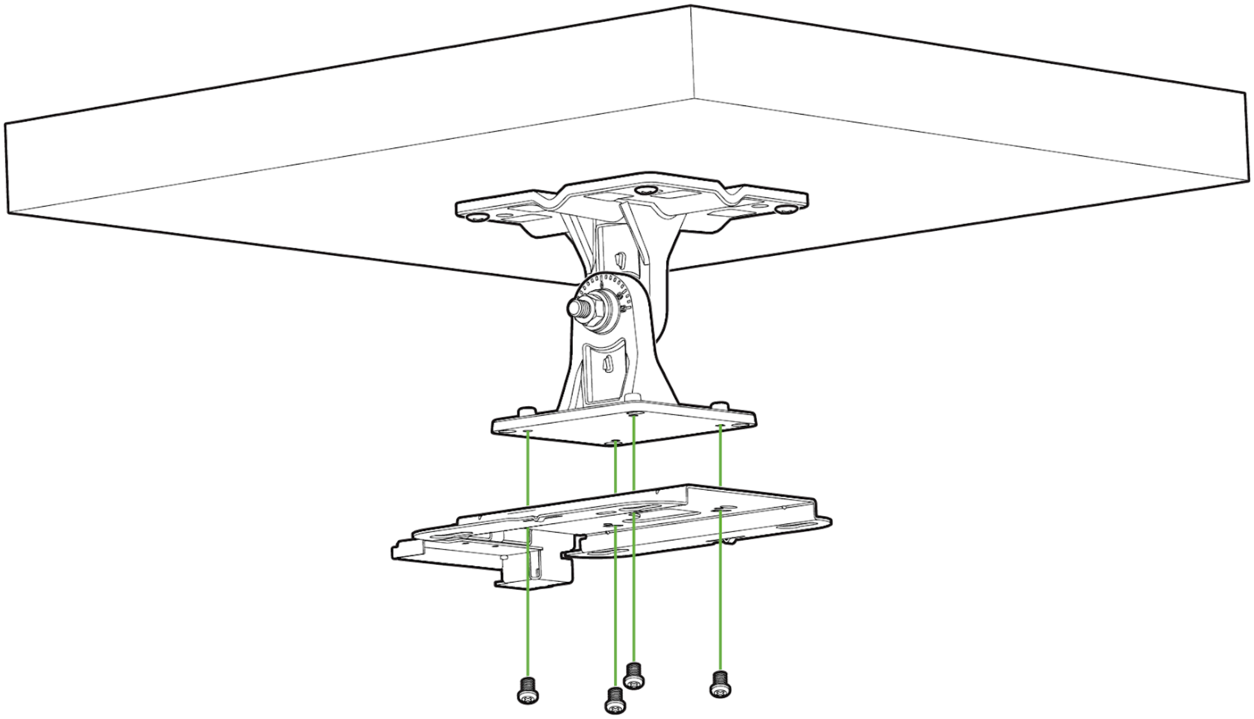
> ⓘ **Note:** The mounting kit does not include the M6 screws for securing the bracket to the mounting surface.

2



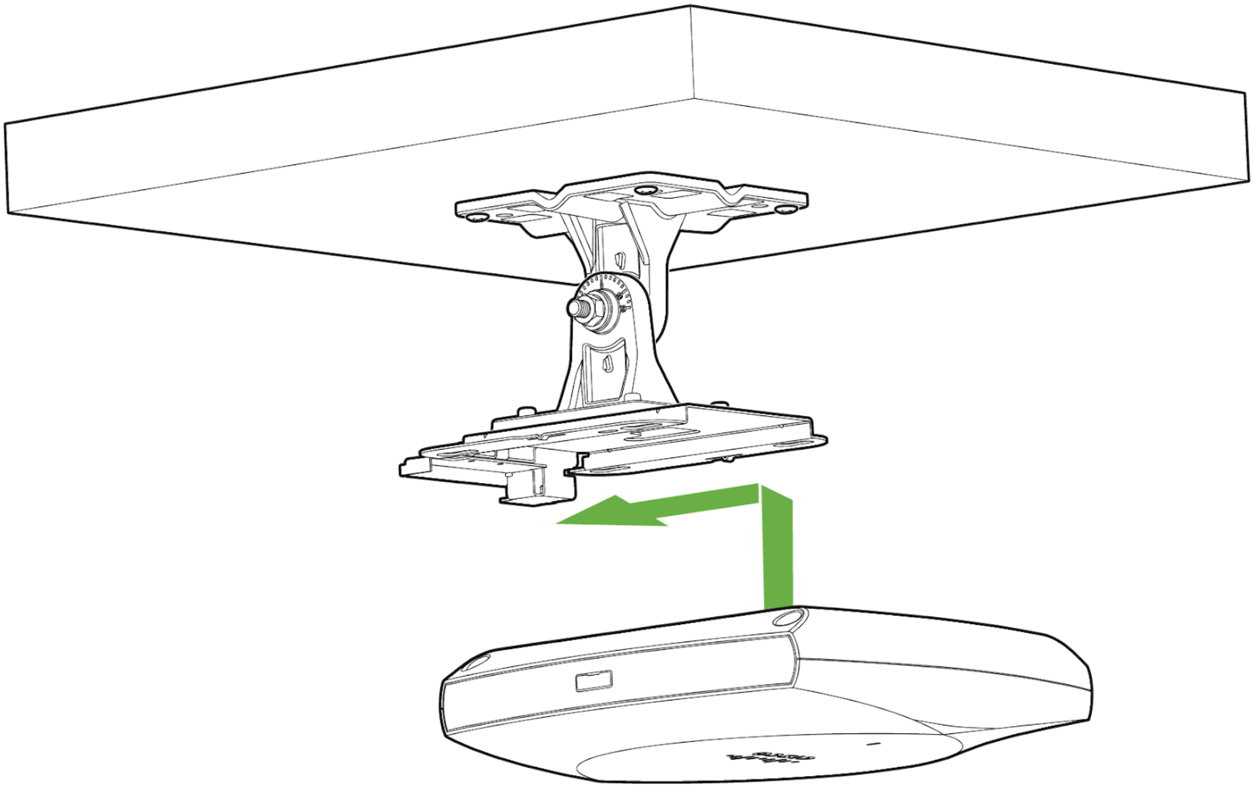
3. Attach the AIR-AP-BRACKET-2 to the access point bracket using four M4 screws through the holes in the bracket. Hand tighten snug the four screws.

3



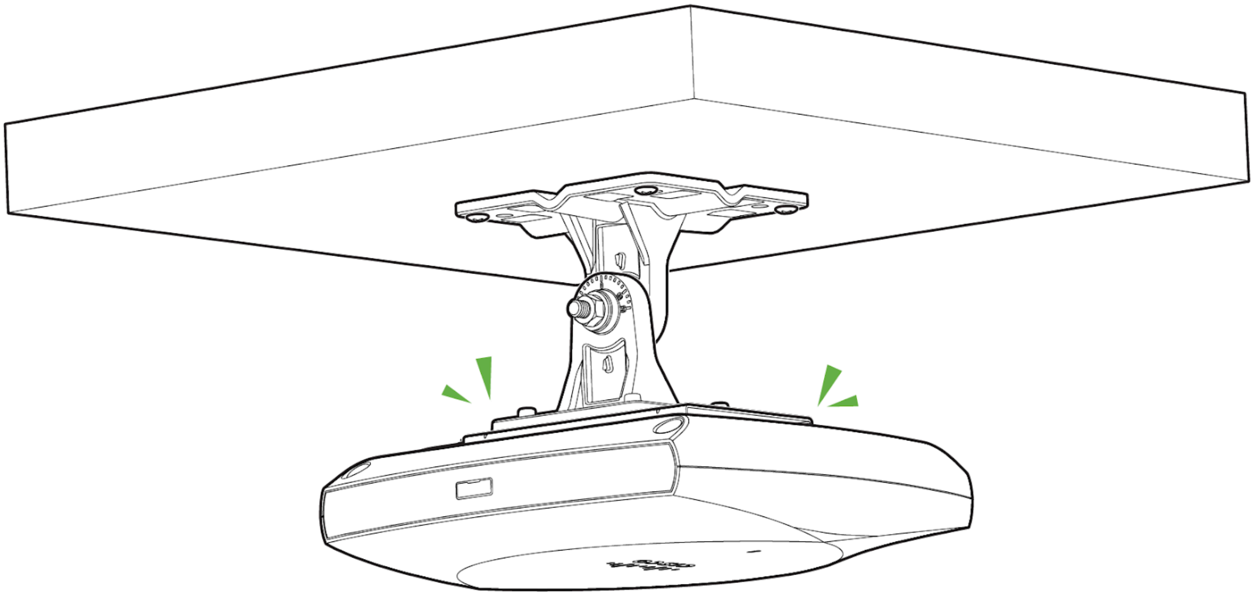
4. Attach the access point to the AIR-AP-BRACKET-2. Use a 13-mm wrench to loosen or tighten the fasteners.

4



5. Adjust the access point's position.Loosen the adjustment pivot nut slightly to allow for adjustment. Use the markings on the flange bracket as a guide. You may adjust the angle ±50 degrees.

5



6. After adjusting the access point position, tighten the pivot nut. Tighten the nut at the pivot point to 5.6 to 5.9 lb-ft (7.6 to 8.0 Nm) torque.

7. Connect the Ethernet cable to the access point using the termination kit.

Drop Ceiling Mount using T-Rail Mount attachment

To mount your AP on a drop ceiling T-rail (AIR-AP-T-RAIL-R - included), use the included T-Rail mount attachment. The T-Rail mount attachment can be used to mount to most 9/16”, 15/16” or 1 ½” T-rails.

1. Place the ceiling grid clip over the T-rail and close it to the appropriate detent (A, B, or C).

2. Use a screwdriver to tighten the two ceiling grid clip locking screws to prevent the clip from sliding along the T-rail.

3. Observe the ceiling grid clip width detent letter (A, B, or C) that corresponds to the T-rail width.

4. Align the corresponding holes (A, B, or C) on the mounting bracket over the mounting holes on the ceiling grid clip.

5. Hold the mounting bracket and insert a 6-32 x 1/4 in. screw into each of the four corresponding holes (A, B, or C) and tighten.

Getting Power to the AP

If mounting to an electrical junction box, feed the Ethernet cable through the cable access hole in the universal mounting bracket. If mounting to a wall or ceiling, the Ethernet cable will feed from behind the AP. The "Power Source Options" section of this document lists the different powering options and their unique characteristics.

Physical Security

Depending on your mounting environment, you may want to secure the AP to its mount location. The access point can be secured in several ways. If the AP has been installed using the universal mounting bracket, it should be secured via a security screw and/or Kensington lock. If the universal mounting bracket was not used, the AP can still be secured using a Kensington lock.

Kensington Lock

The access point contains a hard point that allows it to be secured to any nearby permanent structure using a standard Kensington lock. Attach a Kensington lock cable to the access point at the hard point on the side of the device. Attach the other end of the cable to a secure location, such as a pipe or building fixture.

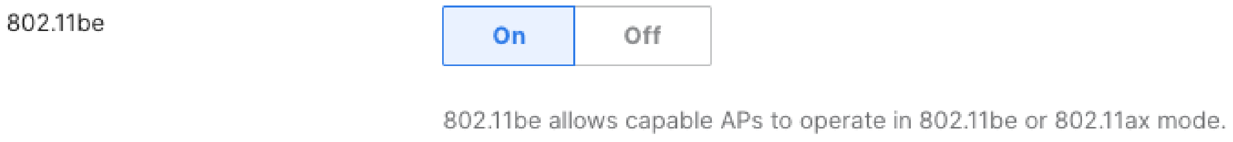
Verify Device Functionality and Test Network Coverage

- Check LED
  - The Power LED should be solid green (or blue, if clients are connected).
  - If it is flashing blue, the firmware is automatically upgrading and the LED should turn green when the upgrade is completed (normally within a few minutes). See the "LED Indicators" section for more details.
- Your AP must have an active route to the Internet to check and upgrade its firmware.
  - Use any 802.11 client device to connect to the AP and verify proper connectivity using the client’s web browser.
- Check network coverage
  - Confirm that you have good signal strength throughout your coverage area. You can use the signal strength meter on a laptop, smartphone, or another wireless device.

Enable 802.11be

To have the Wi-Fi 7 clients connect with 11be rates or do MLO (Multi-Link operation), 802.11be has to be explicitly enabled in the Meraki Dashboard.

802.11be can be enabled from **Wireless > Configure > Radio Settings>RF Profiles**



802.11be: On

802.11be allows capable APs to operate in 802.11be or 802.11ax mode.

320 MHz Channel Width

Wi-Fi 7 allows a channel width of up to 320 MHz for the 6 GHz Frequency band. This higher channel width helps to increase the overall throughput. In countries with support of 1200 MHz of 6 GHz Frequency spectrum, a total of 3 non-overlapping 320 MHz channels can be achieved, when the AP is operating in Low Power (LPi) Indoor Mode. When the AP is operating in Standard Power, only one 320 MHz channel can be achieved in the UNII-5 band. In countries with support of 500 MHz of 6 GHz Frequency spectrum, only one 320 MHz channel can be achieved.

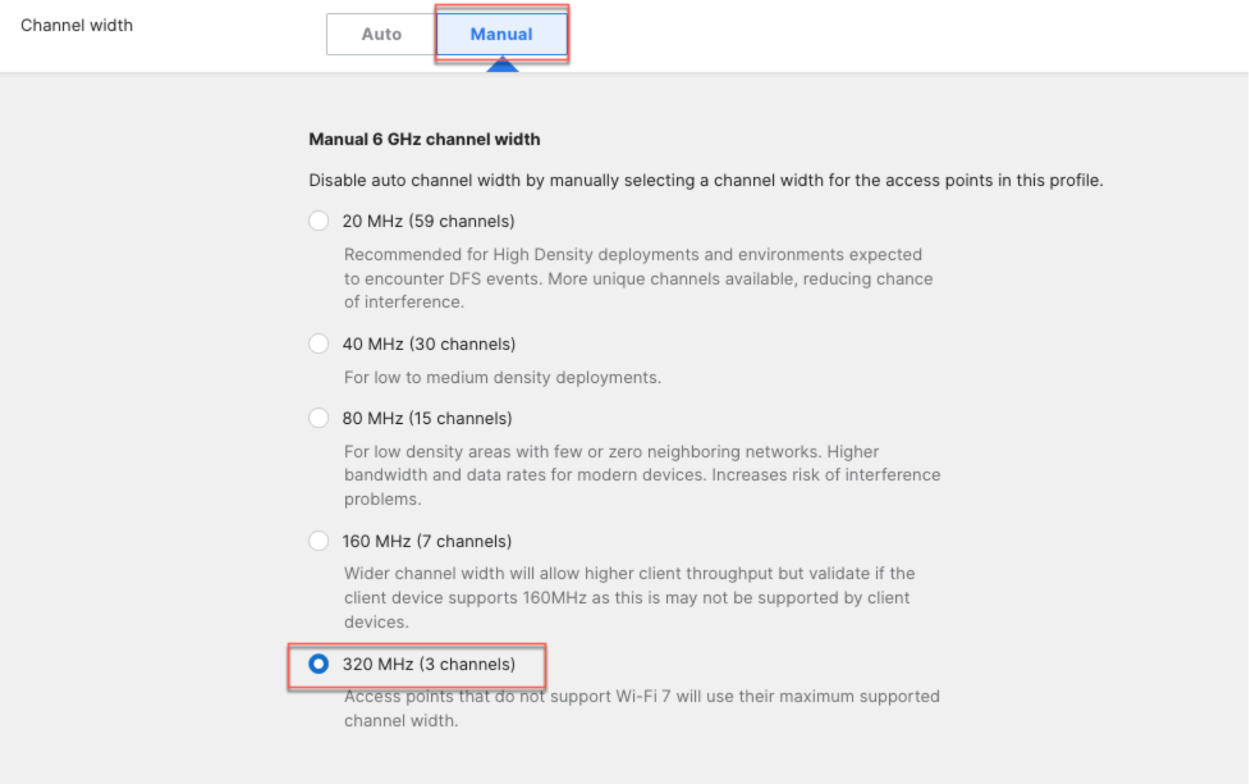
Meraki Dashboard allows manual configuration of 320 MHz Channel Width

Internal Note: Auto-RF does not support 320 MHz Channel Width in R31. This can be only manually assigned.

320 MHz channel width can be enabled from

Wireless → Configure → Radio Settings → RF Profile → 6 GHz.

Change the Channel width setting to Manual to enable 320 MHz.


Channel width

Manual 6 GHz channel width

Disable auto channel width by manually selecting a channel width for the access points in this profile.

○ 20 MHz (59 channels)

Recommended for High Density deployments and environments expected to encounter DFS events. More unique channels available, reducing chance of interference.

○ 40 MHz (30 channels)

For low to medium density deployments.

○ 80 MHz (15 channels)

For low density areas with few or zero neighboring networks. Higher bandwidth and data rates for modern devices. Increases risk of interference problems.

○ 160 MHz (7 channels)

Wider channel width will allow higher client throughput but validate if the client device supports 160MHz as this is may not be supported by client devices.

● 320 MHz (3 channels)

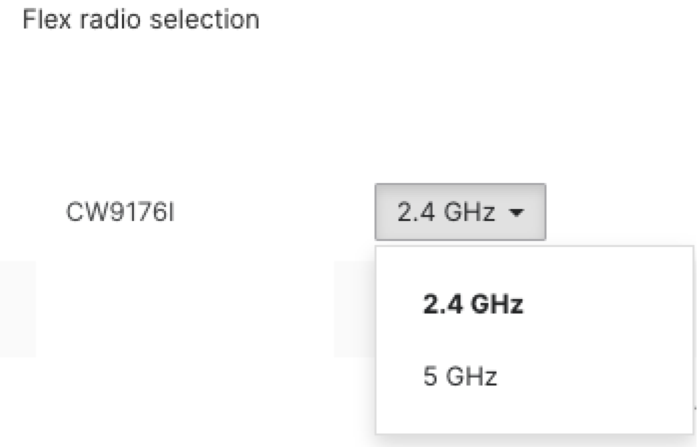
Access points that do not support Wi-Fi 7 will use their maximum supported channel width.

Dual 5 GHz Mode

The CW9176D1 has three client-serving Wi-Fi Radios capable of operating in the 2.4, 5 and 6 GHz Frequencies. On the CW9176D1 the first radio can be configured to operate in the 2.4 Frequency GHz band or 5 GHz Frequency band,

The out-of-the-box setting of the CW9176D1 will have the radios operate in 2.4, 5 and 6 GHz Frequency bands.

The AP can be made to operate in Dual 5 GHz mode by changing the Flex Radio Selection in RF Profile settings (Wireless → Configure → Radio Settings → RF Profiles)


Flex radio selection

CW9176I: 2.4 GHz

ⓘ **Note:** When the CW9176D1 is operating in Dual 5 GHz mode, the operating channels are restricted to UNII-1 and UNII-2a for the first 5 GHz radio and UNII-2c and UNII-3 for the second 5 GHz radio.

WPA3 Support

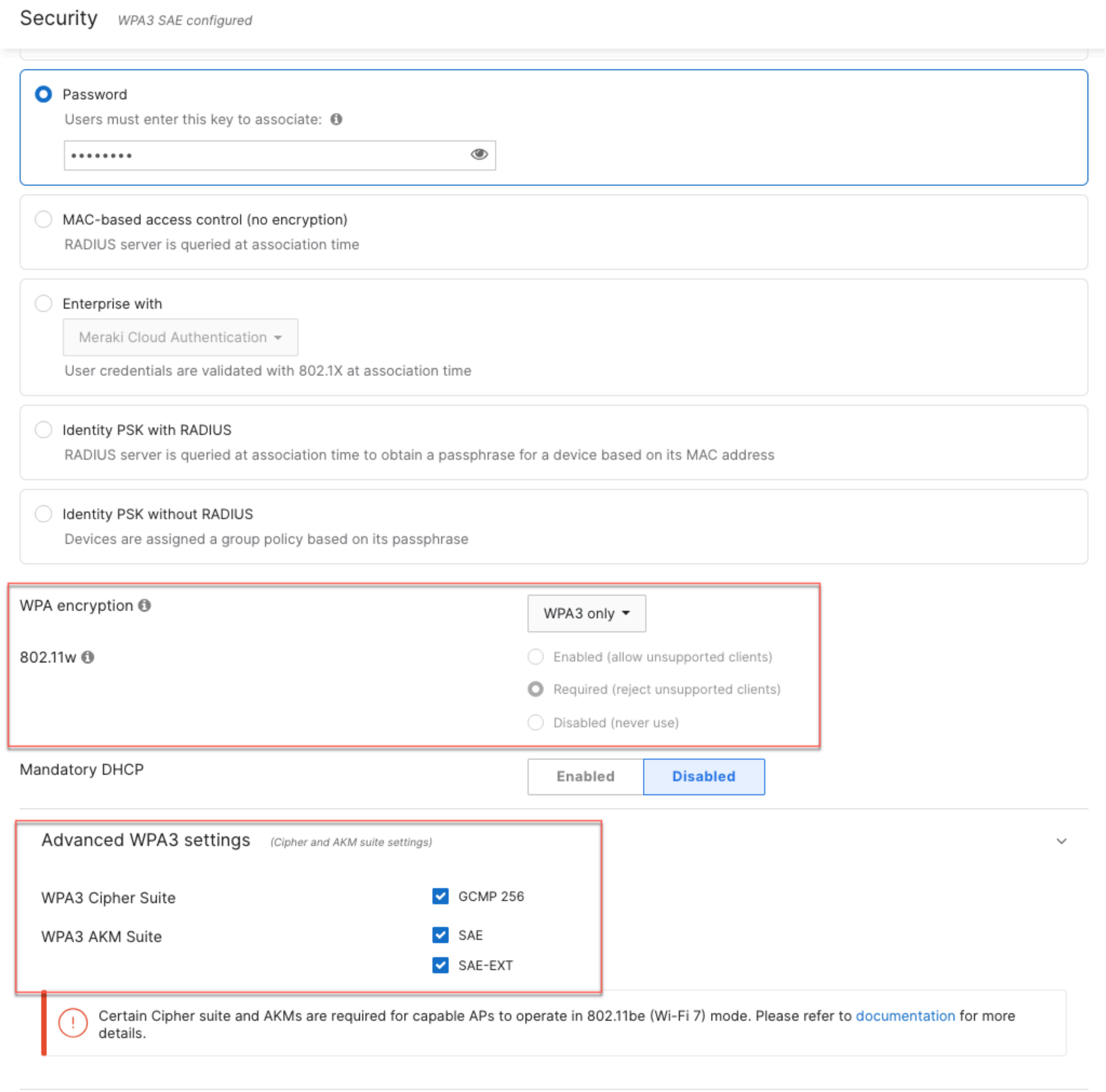
Wi-Fi 7 requires the client to support WPA3 or OWE with Protected Management Frame (PMF) as a mandatory mode of operation for Wi-Fi 7, i.e. for 11be rates and MLO. The Wi-Fi 7 Access Point is backwards compatible with the earlier security mechanisms like WPA2, but when a Wi-Fi 7 client connects with a lower security type, it cannot achieve the Wi-Fi 7 functionality.

Wi-Fi 7 brings new AKM support for WPA3-SAE and new increased cyphers for Enhanced Open (OWE) and WPA3-SAE. The new AKM is SAE-EXT (AKM 24). The cipher needed for OWE and WPA3-SAE in Wi-Fi 7 is GCMP256

WPA3-SAE Configuration:

From the **Wireless > Configure > Access Control > Security**,

1. enter the password for WPA3-Personal,
2. select WPA3 as the Encryption,
3. 802.11w as Required.
4. From Advanced WPA3 settings (Cipher and AKM suite settings), select SAE-EXT and GCMP 256.



Security *WPA3 SAE configured*

● Password

Users must enter this key to associate:

••••••••

○ MAC-based access control (no encryption)

RADIUS server is queried at association time

○ Enterprise with

Meraki Cloud Authentication ▾

User credentials are validated with 802.1X at association time

○ Identity PSK with RADIUS

RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

○ Identity PSK without RADIUS

Devices are assigned a group policy based on its passphrase

WPA encryption: WPA3 only ▾

802.11w:
○ Enabled (allow unsupported clients)
● Required (reject unsupported clients)
○ Disabled (never use)

Mandatory DHCP: Enabled [✓ Disabled]

Advanced WPA3 settings *(Cipher and AKM suite settings)*

WPA3 Cipher Suite: ☑ GCMP 256

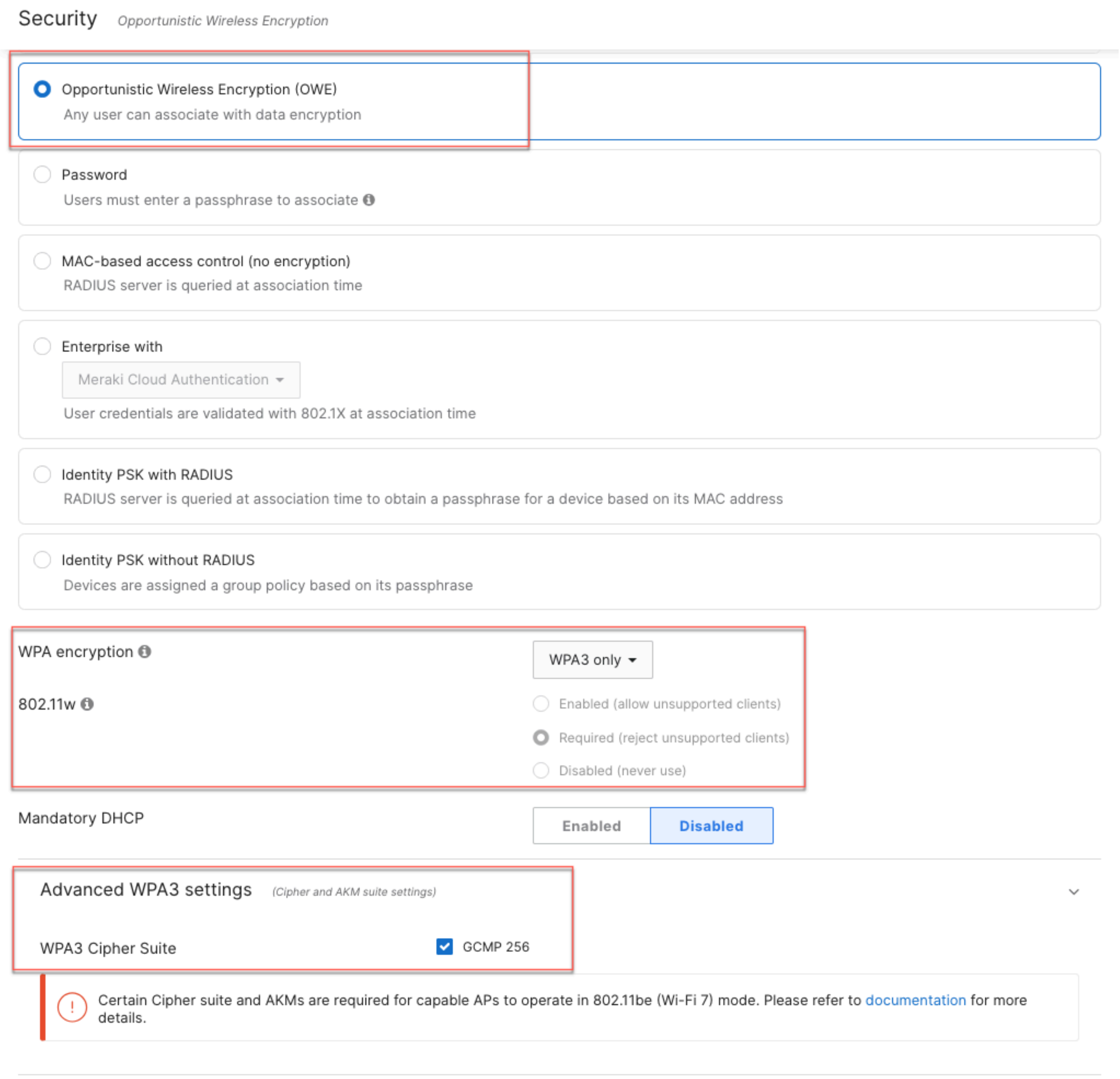
WPA3 AKM Suite: ☑ SAE ☑ SAE-EXT

Certain Cipher suite and AKMs are required for capable APs to operate in 802.11be (Wi-Fi 7) mode. Please refer to documentation for more details.

OWE Configuration:

From **Wireless** → **Configure** → **Access Control** → **Security**

1. Select Opportunistic Wireless Encryption (OWE)
2. select WPA3 as the Encryption,
3. 802.11w as Required.
4. From Advanced WPA3 settings (Cipher and AKM suite settings), select the cipher as GCMP 256.



Security *Opportunistic Wireless Encryption*

● Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

○ Password
Users must enter a passphrase to associate

○ MAC-based access control (no encryption)
RADIUS server is queried at association time

○ Enterprise with Meraki Cloud Authentication
User credentials are validated with 802.1X at association time

○ Identity PSK with RADIUS
RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

○ Identity PSK without RADIUS
Devices are assigned a group policy based on its passphrase

WPA encryption: WPA3 only

802.11w:
○ Enabled (allow unsupported clients)
● Required (reject unsupported clients)
○ Disabled (never use)

Mandatory DHCP: Enabled [✓ Disabled]

Advanced WPA3 settings *(Cipher and AKM suite settings)*

WPA3 Cipher Suite: ☑ GCMP 256

Certain Cipher suite and AKMs are required for capable APs to operate in 802.11be (Wi-Fi 7) mode. Please refer to documentation for more details.

Note: If an SSID is configured to support WPA3 transition mode for Personal across all three frequency bands, then the 2.4 GHz and the 5 GHz frequency will broadcast the SSID with transition mode support. The SSID will not be broadcasted in the 6 GHz mode.

Note: Starting with the MR 31 software release, if an SSID is configured to support WPA3 transition mode for Enterprise across all three frequency bands, then the 2.4 GHz and the 5 GHz frequency will broadcast the SSID with transition mode support and the SSID will be broadcasted as WPA3 in the 6 GHz band.

Note: If the AP is broadcasting at least one of the SSIDs with a lower security type, then the AP will not broadcast 11be information in the Beacon and Probe Response and will function as 11ax.This behaviour is due to change in a future firmware upgrade.

Basic Troubleshooting

The following steps can be used for troubleshooting basic connectivity issues with your access point.

- Reboot the access point
- Factory reset the access point by holding the factory reset button for 60 seconds
- Try switching cables, or testing your cable on another device

If your access point still does not connect, the following instructions may be useful, depending on your issue.

Check Radio Functionality by Making the AP a Repeater

1. If your AP is acting as a gateway, disconnect the Ethernet cable from the LAN (while keeping the AP powered on). This will switch your AP into repeater mode. If no other gateways are within range, the AP will begin broadcasting an SSID appended with "-scanning". If you can connect to this SSID and go to my.meraki.com from your web browser, then your radio is working.
2. Physically place the repeater AP (AP with disconnected LAN) next to a working gateway AP.
3. Connect the power adapter or PoE. The radio and signal strength LEDs on the AP will turn solid green or blue once the access point boots up and detects the gateway.
4. The access point is now a repeater and will check into the Dashboard.
5. On the Wireless > Access Points page in the Dashboard, you will see the connectivity bar for the specific Repeater AP reflecting a light green color, which means the AP is a repeater. Gateway APs will reflect a dark green color in the connectivity bar and also will have the letter G (Gateway) on top of the AP symbol.

Check Ethernet Port Functionality by Connecting to the AP

1. Disable the Wireless adapter on your computer.
2. Make sure the Ethernet adapter on your device is set to obtain an IP address automatically via DHCP.
3. Connect your computer to the Ethernet port on the AP with an Ethernet cable.
4. The Ethernet LED on the AP should turn solid green or blue.
5. If the Ethernet LED does not turn solid green or blue, try swapping the cable. If the Ethernet port still does not turn green or blue, try the second Ethernet port, if the AP has one.
6. If the Ethernet LED does not turn solid green or blue, you may have a bad port on the AP. If this is the case, the AP signal LEDs will continue to scan.
7. Once the Ethernet LED turns solid green or blue, your computer should obtain an IP address from the AP via DHCP.

Check Static IP Address Configuration

1. If the AP has a static IP address, the green signal LEDs will begin to flash on and off and you will not receive an IP address via DHCP.
2. Disconnect the Ethernet cable from the AP.
3. Associate to the SSID being broadcasted by the AP. If there are no other APs in the network within range the SSID may be appended with "-scanning".
4. Go to my.meraki.com in your web browser.

5. The MAC address on the back of the access point should match the physical address value on the my.meraki.com Overview page.
6. Once you have verified that the MAC address is correct on the overview tab, click the tab Static IP configuration.
7. Enter the username (serial number on the back of the AP) which is case sensitive and must include the dashes. (There is no password).
8. Make sure your AP is set to obtain a correct DHCP or static IP address configuration from your network.

Reference https://documentation.meraki.com/MR for additional information and troubleshooting tips.

If you are still experiencing hardware issues, please contact Cisco Meraki support by logging in to the Dashboard and using the **Help** option near the top of the page, then opening and email case or calling using the contact information on that page.

Warranty

Additional warranty information can be found on the CW9176 Datasheet or on the Warranty Returns (RMA) page of the Cisco Product Warranties website

If your Cisco Meraki device fails and the problem cannot be resolved by troubleshooting, contact support to address the issue. Once support determines that the device is in a failed state, they can process an RMA and send out a replacement device free of charge. In most circumstances, the RMA will include a pre-paid shipping label so the faulty equipment can be returned.

To initiate a hardware replacement for non-functioning hardware that is under warranty, you must have access to the original packaging the hardware was shipped in. The original hardware packaging includes the device serial number and order information and may be required for return shipping.

Meraki CW9176D1 devices have been tested and found to comply with the limits for a Class B digital device, under 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.

Support and Additional Information

If issues are encountered with device installation or additional help is required, **contact Meraki Support** by logging in to **dashboard.meraki.com** and opening a case by visiting the **Get Help** section.

- The equipment is intended for industrial or other commercial activities.
- The equipment is used in areas without exposure to harmful and dangerous production factors unless otherwise specified in the operational documentation and/or on the equipment labeling.
- The equipment is not for domestic use. The equipment is intended for operation without the constant presence of maintenance personnel.
- The equipment is subject to installation and maintenance by specialists with the appropriate qualifications, sufficient specialized knowledge, and skills.
- Rules and conditions for the sale of equipment are determined by the terms of contracts concluded by Cisco or authorized Cisco partners with equipment buyers.
- Disposal of a technical device at the end of its service life should be carried out in accordance with the requirements of all state regulations and laws.
- Do not throw in the device with household waste. The technical equipment is subject to storage and disposal in accordance with the organization's disposal procedure.
- The equipment should be stored in its original packaging in a room protected from atmospheric precipitation. The permissible temperature and humidity ranges during storage are specified in the Operation (Installation) Manual.
- Transportation of equipment should be carried out in the original packaging in covered vehicles by any means of transport. The temperature and humidity during transportation must comply with the permissible established ranges of temperature and humidity during storage (in the off state) specified in the Operation Manual (Installation)

For additional information on Meraki hardware and for other installation guides, please refer to **documentation.meraki.com.**