Guide

Cisco public

The bridge to possible

Cisco Wireless CW9178I Deployment Guide

Cisco Wireless CW9178I Overview

The Cisco Wireless CW9178I is Cisco's high end Wi-Fi 7 Access Point Platform with an hexa radio architecture providing the full capability of Wi-Fi 7 Features based on 802.11be amendment such as 4K Modulation, Multi Link Operation (MLO), 320 MHz channel width, Pre-amble puncturing, Multi Resource Units, compressed block ack enhacements of upto 512 MPDUs and Wi-Fi Protected Access 3 (WPA3) security, all while being able to leverage advanced RF visibility with Cisco CleanAir® Pro together with an artificial intelligence and machine learning (AI/ML)-driven scanning radio.

The Cisco Wireless CW9178I is a Unified Product with one SKU, that can be deployed with a Cisco Catalyst Wireless LAN Controller or Meraki Cloud based deployments. The CW9178I access can be deployed anywhere in the world just with the single SKU and avoids the need to buy a region or country specific SKU based on regulatory domain.

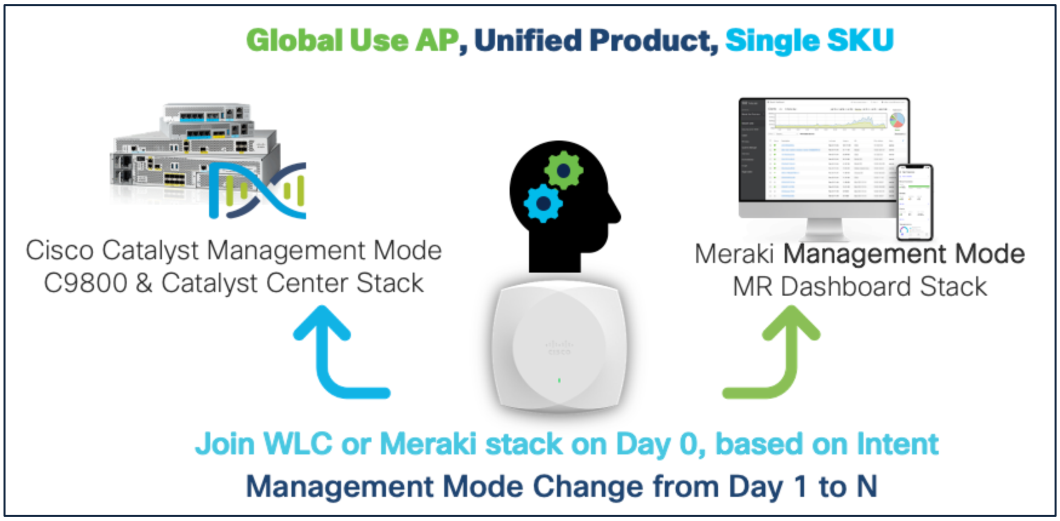
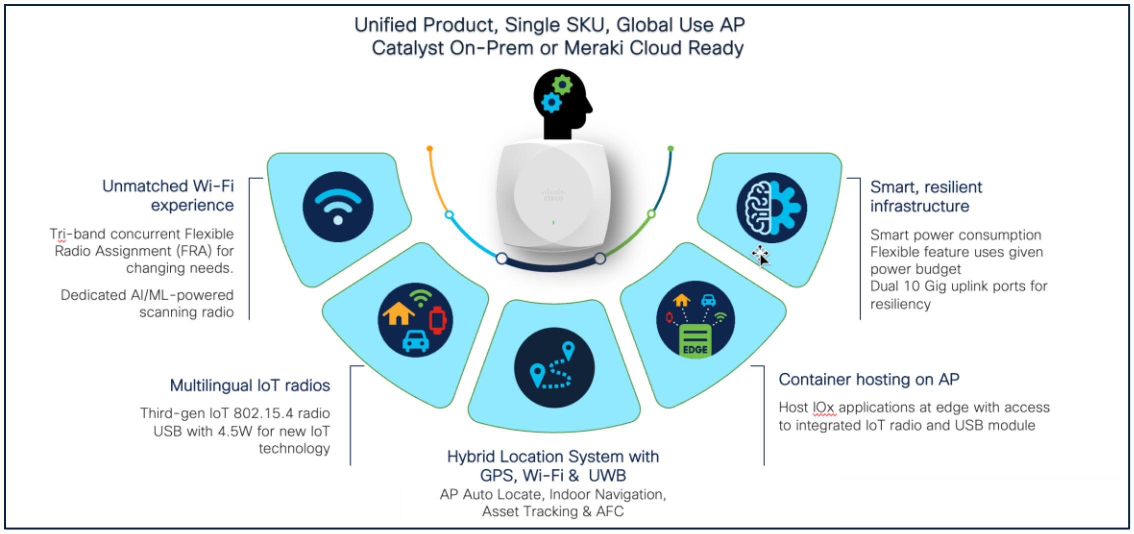

Global Use AP, Unified Product, Single SKU
Cisco Catalyst Management Mode
C9800 & Catalyst Center Stack
Meraki Management Mode
MR Dashboard Stack
Join WLC or Meraki stack on Day 0, based on Intent
Management Mode Change from Day 1 to N

Figure 1. **Global Use AP - Management Mode**

The Cisco Wireless CW9178I supports the entire Cisco Catalyst wireless stack functionality with Cisco Catalyst Center (Automation and Assurance), Cisco Spaces (Location and IoT), Identity Services Engine (security), and more. Throughout this guide, you will learn how the CW9178I is a wireless powerhouse that can take your network to the next level.



Unified Product, Single SKU, Global Use AP
Catalyst On-Prem or Meraki Cloud Ready

Unmatched Wi-Fi experience

Tri-band concurrent Flexible Radio Assignment (FRA) for changing needs.

Dedicated AI/ML-powered scanning radio

Multilingual IoT radios

Third-gen IoT 802.15.4 radio USB with 4.5W for new IoT technology

Hybrid Location System with GPS, Wi-Fi & UWB

AP Auto Locate, Indoor Navigation, Asset Tracking & AFC

Container hosting on AP

Host IOx applications at edge with access to integrated IoT radio and USB module

Smart, resilient infrastructure

Smart power consumption
Flexible feature uses given power budget
Dual 10 Gig uplink ports for resiliency

Figure 2. Global Use AP - Controller Stack Agnostic

Table 1. Cisco® Catalyst® Wireless 9800 Series controller software support matrix

Supported IOS XE releases
Cisco IOS XE 17.15.2 and later

Supported Controller platforms

CW9178I APs are supported with the following Catalyst 9800 Series Controllers:

- 9800-H1
- 9800-H2
- 9800-M
- 9800-80
- 9800-40
- 9800-L
- 9800-CL

Note: Embedded wireless controller on AP (EWC) functionality is not supported on the CW9178I, both as an active EWC or a subordinate AP.

Technical Specifications

Table 2. CW9178I At a Glance

Capability	Details
Product ID	CW9178I
Scale	1600 Clients (400 clients per radio)

Capability	Details
Serving Radio	• 2.4 GHz (Slot 0), 4x4:4 spatial streams • 5 GHz (Slot 1), 4x4:4 spatial streams • 5 GHz (Slot 2), 4x4:4 spatial streams • 6 GHz (Slot 3), 4x4:4 spatial streams **Note:** CW9178I can operate as Tri-radio or Quad-radio, with Tri-radio as the default mode.
IoT Capabilities	• Dedicated 2.4 GHz IoT Radio • Application Hosting Capabilities
Scanning Radio	Yes
Wi-Fi 7 Features	• 4K QAM • 320 MHz Channel Width • Multi-Link Operation • Preamble Puncturing • Multi Resource Units • Compressed Block Ack with 512 MPDUs • UL Triggered OFDMA
Wi-Fi 6 Features	• MU-MIMO • OFDMA • BSS Coloring • TWT
LAN Port	2xPOE-IN 10Gig mGig Ports
Ports	mGig0, mGig1, Console
Antenna	Integrated, Omnidirectional
Dimensions	9.9x9.9x2.0 inches 25x25x5.1 cm
Weight	4.1 lb (1.87 kg)
USB	9W Output
SSIDs	• 2.4 GHz: 16 • 5 GHz: 16 • 6 GHz: 16
MTBF	• 25° C: 942,282 hrs • 50° C: 332,257 hrs
Environment	• Non-operating (storage) temperature: -22° to 158° F (-30° to 70° C) • Non-operating (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)

Capability	Details
Antenna Gain	- 2.4 GHz: 4dBi - 5 GHz: 5 dBi - 6 GHz: 6dBi
Geo Location	Inbuilt GPS/GNSS Module; provision to connect an external GPS/GNSS Antenna.

Table 3. Serving Radio Specifications

Mode	2.4 GHz Slot 0	Primary 5 GHz (Slot 1)	Secondary 5 GHz (Slot 2)	6 GHz (Slot 3)
Tri-radio 12SS	- 4x4:4SS - (20 MHz)	- 4x4:4SS - (20/40/80/160 MHz)	NA	- 4x4:4SS - (20/40/80/160/320 MHz)
Quad-radio 12SS	- 4x4:4SS - (20 MHz)	- 4x4:4SS - (20/40/80/160 MHz)	- 4x4:4SS - (20/40/80/160 MHz)	- 4x4:4SS - (20/40/80/160/320 MHz)

The Cisco Wireless 9178I is interoperable with the following network management and security solutions.

Table 4. Software Interoperability

Catalyst 9800	Cisco Catalyst Center	Cisco Spaces	ISE
17.15.2	TBD	TBD	TBD

Mechanical Design

The CW9178I has an altogether new design which is aesthetically appealing allowing you to identify it among other APs instantly.

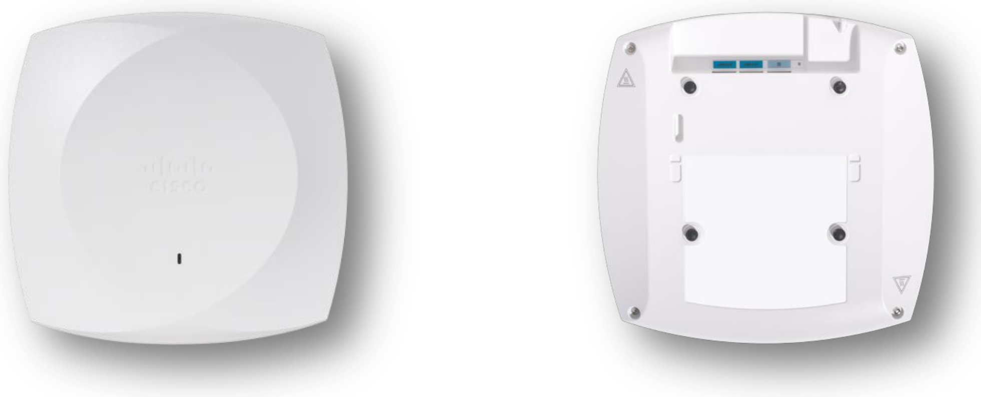


Figure 3. CW9178I - Front and back views

Physical Dimensions

The CW9178I Wi-Fi 7 AP is similar in size and weight to the mid-range and high-end Catalyst Wi-Fi 6 and Wi-Fi 6E APs and smaller and lighter **than** many of the Cisco Catalyst APs prior to Wi-Fi 6. However, it boasts a much more robust hexa-radio architecture, a dedicated scanning radio, a dedicated IoT radio, an inbuilt GPS and GNSS module, Ultra Wide Band Radio, two 10 Gig Multigigabit ports, and supports Wi-Fi 7.

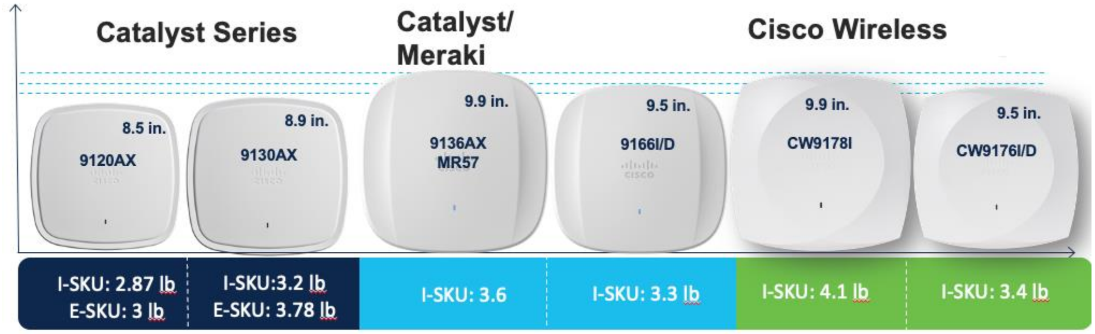


Figure 4. CW9178I showing physical comparison with existing Catalyst APs

Physical Ports

The following figures depict the ports and reset button on the CW9178I:

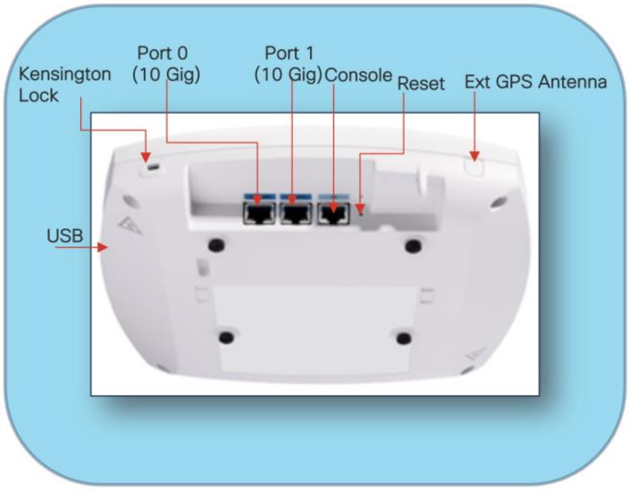


Figure 5. CW9178I Top View with Connectors and Ports

Brackets & Mounting

The CW9178I is compatible with the Cisco Low Profile Mounting Bracket AIR-AP-BRACKET-1 (default option) and Cisco Universal Mounting Bracket AIR-AP-BRACKET-2 mounting brackets. This AP is also compatible with the AIR-AP-T-RAIL-R and AIR-AP-T-RAIL-F for T-rail drop ceiling. These brackets are the same AP brackets provided for all Tier 2 and 3 enterprise-class APs for the last 15+ years. This backward compatibility streamlines the day-0 process for brownfield deployments, allowing the CW9178I to be mounted on existing brackets. In addition, the CW9178I can be mounted using the AIR-CHNL-ADAPTER clip for channel-rail ceiling grid profiles.

For more details on mounting the access point, refer the following documents:

- Cisco Wireless 9178I Hardware Installation Guide

- Access Point Mounting Instructions

The following figures provide details about the AIR-AP-Bracket-1 and AIR-AP-Bracket-2 for reference:

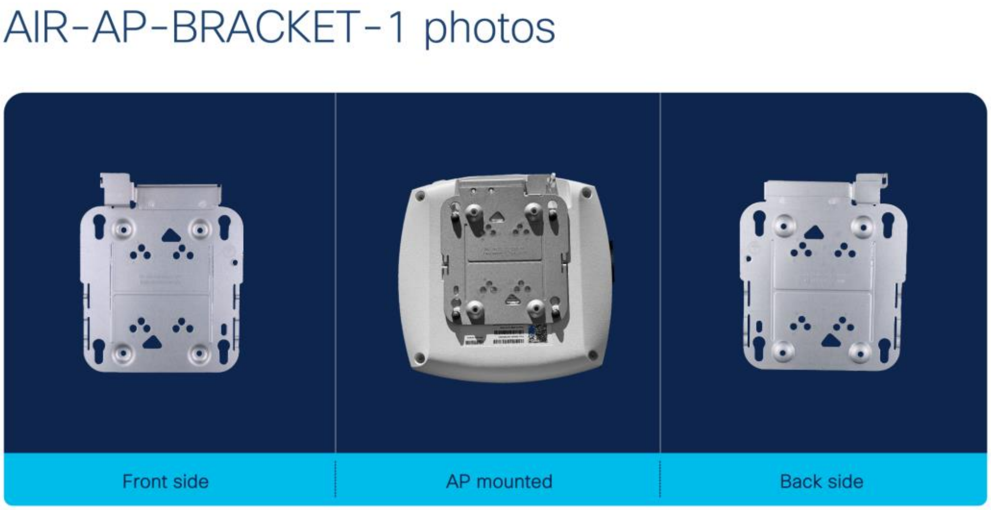
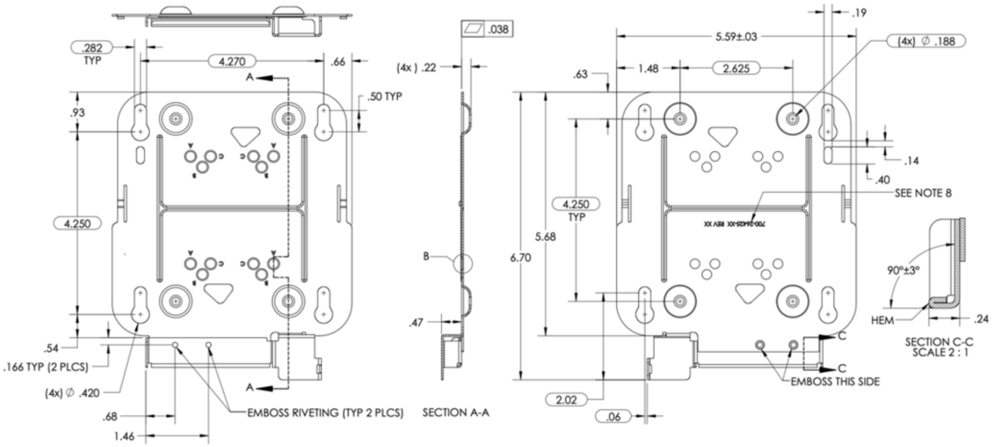


Figure 6. **Mounting brackets (AIR-AP-BRACKET-1) - front & back views**



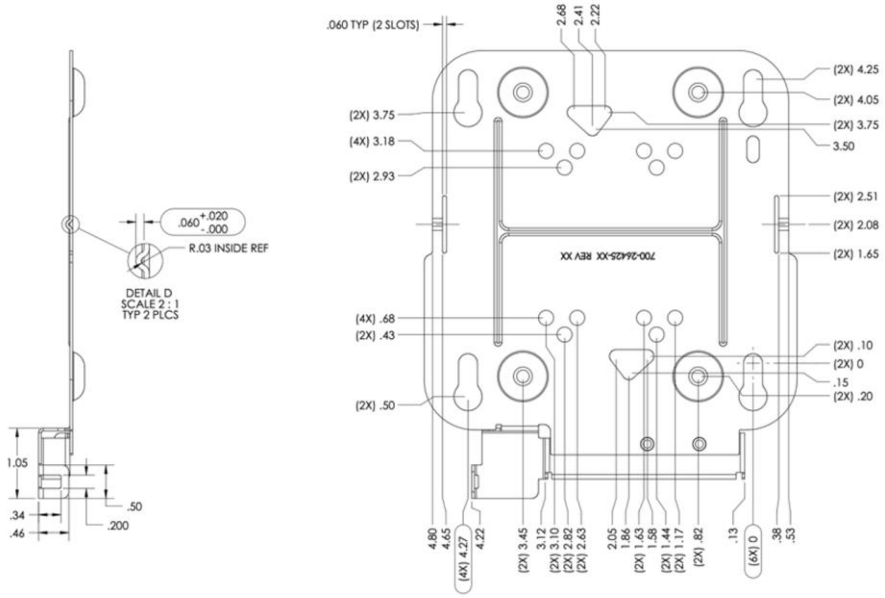


Figure 7. **AIR-AP-BRACKET-1 Schematics**

AIR-AP-BRACKET-2 photos

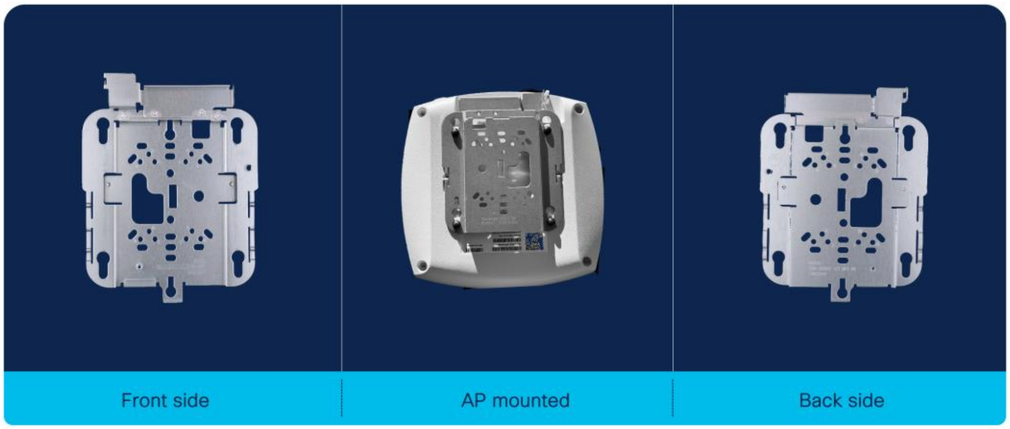


Figure 8. **Mounting brackets (AIR-AP-BRACKET-2) - front & back views**

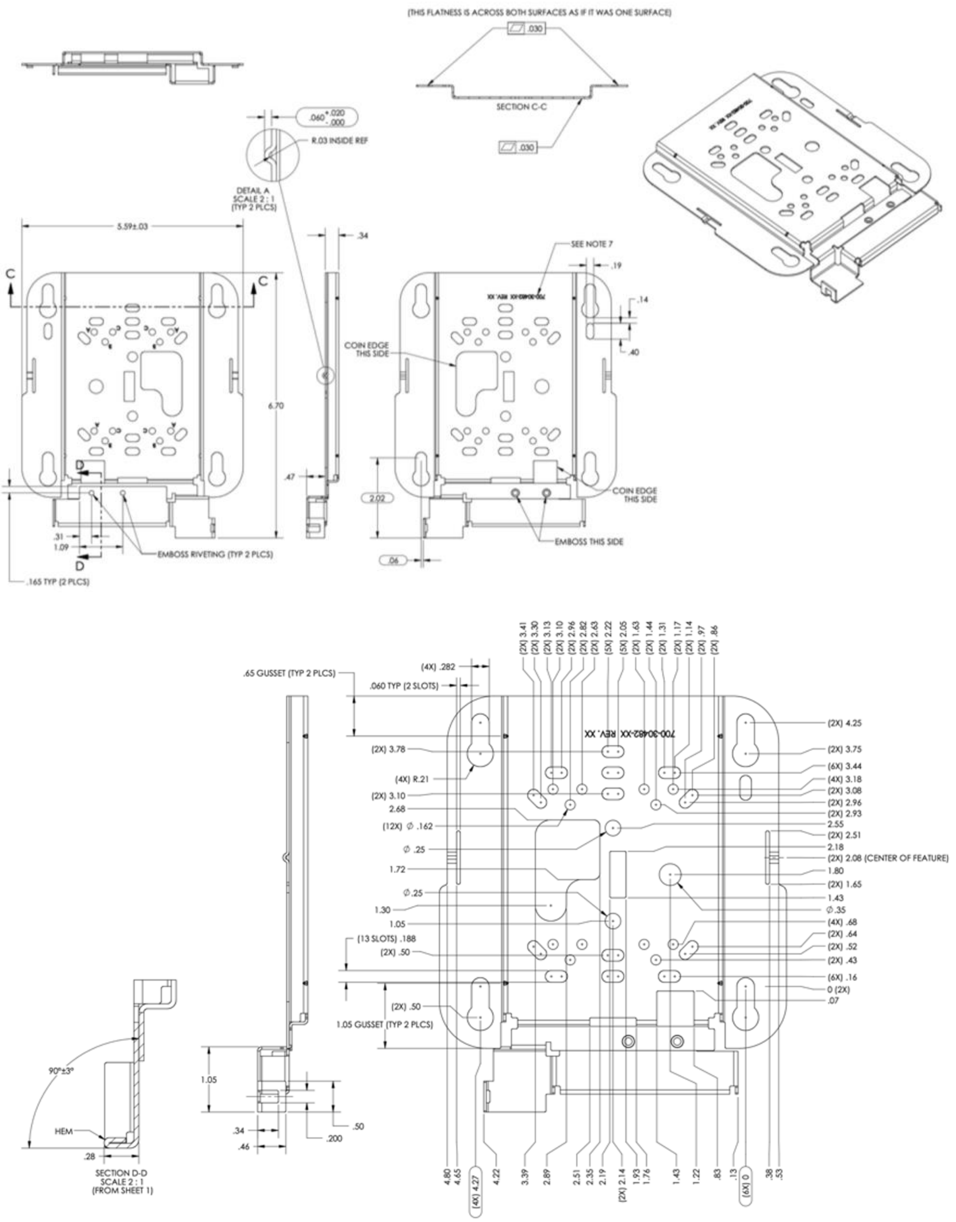


Figure 9. AIR-AP-BRACKET-2 Schematics

Cabling

The use of proper cable types will enhances the performance of the CW9178I. Since this AP has 5-Gbps ports, it is recommended to use either CAT6 or CAT 6a cable which support speeds of up to 10 Gbps. CAT 5e cables can still be used; however, the AP's performance may get degraded.

The table below lists the various cable types that can be used with the CW9178I.

Table 5. Cable Types Supported

Cable Type	Speeds	Maximum Length
CAT 5e	5 Gigabit	328 feet (100 meters)

CAT 6	1/2.5/5 Gigabit	330 feet (100 meters)
	10 Gigabit	164 feet (50 meters)
CAT 6a	10 Gigabit	330 feet (100 meters)

Power Over Ethernet

The following table depicts the radio, port, USB performance, and maximum power draw based on the AP's input power. For optimal performance, 803.2bt is required.

Note: It's recommended to use Cat 6 or Cat 6A cables for the best performance.

Table 6. PoE specifications for CW9178I on Cisco IOS XE 17.15.2

Power Source	Number of Spatial Streams	2.4 GHz Radio (Slot 0)	5 GHz Radio (Slot 1)	5 GHz Radio (Slot 2)	6 GHz Radio (Slot 3)	10 Gig Port 0	10 Gig Port 1	USB	IoT/GPS/UWB/Scan Radio
802.3af (PoE)	NA	Disabled	Disabled	Disabled	Disabled	1G	Disabled	Disabled	Y
802.3at (PoE+) (Quad Radio)	8**	2x2	2x2(HB)	2x2(LB)	2x2	2.5G	2.5G	Disabled	Y
802.3at (PoE+) (Tri Radio)	8**	2x2	4x4(FB)	Disabled	2x2	1G	1G	Disabled	Y
802.3 bt (PoE++ /UPOE) (Class 6)	16	4x4	4x4(LB)	4x4(HB)	4x4	10G	10G	Yes/9W	Y
802.3af (PoE)	NA	Disabled	Disabled	Disabled	Disabled	1G	Disabled	Disabled	Y

Note: ** Starting IOS-XE ver 17.15.3. Till then the number of spatial streams will be limited to 6.

Dual Ethernet Port

The CW9178I comes with dual 10 Gig multigigabit (mGig) ports. These two 10-Gbps uplink ports can be used together to support a link aggregation configuration and provide uplink high availability and port PoE redundancy.

Port PoE redundancy

This feature allows you to plug a PoE source into both uplink ports for high availability and prevent the AP from restarting if power from a single source is lost. When both ports are plugged in, the AP will assume port 0 (left port) as primary (active) and port 1 (middle port) as secondary (standby). The AP will negotiate power in both the ports.

Non-LAG Deployment

In Non LAG Deployment, AP will draw power only from the primary source; however, if the primary source goes down, the secondary source will immediately become the primary. Traffic is exchanged only on the Active Port using its Mac address. Standby port only exchanges CDP/LLDP messages with its own Mac address. In case of active port failure, standby becomes active and exchanges traffic using the Mac address of the initial active port with very minimal traffic loss.

The CW9178I supports both single-homed and dual-homed deployment scenarios. In a dual-homed scenario, where the ethernet ports connect to two different switches, it is recommended to connect to switches in different Intermediate Distribution Frame (IDF), wherever possible. In a single-homed scenario, where the ethernet ports connect to the same logical switch (Stack Wise, Multi Layer switch), it is recommended to connect to two different stack members of the stack or to two different line cards. In both deployment scenarios, the switchports must be configured in the same VLAN.

Note: If the switchports are connected to switch ports belonging to different VLANs, then the switchover will not be seamless.

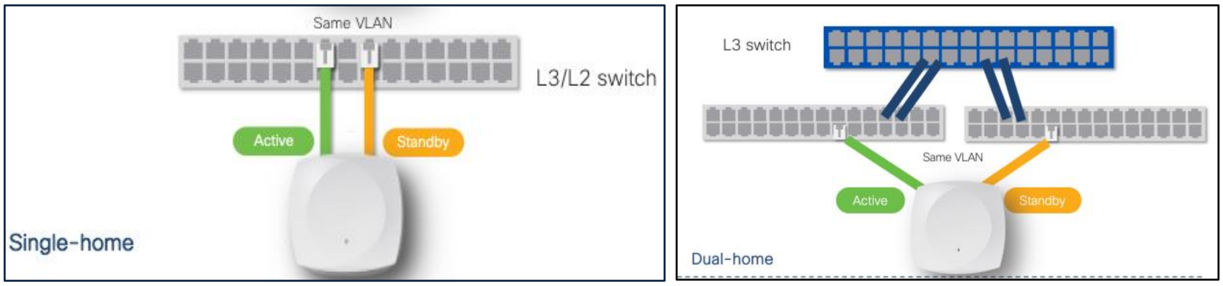


Figure 10. Single-home and dual-home deployments

LAG Deployment

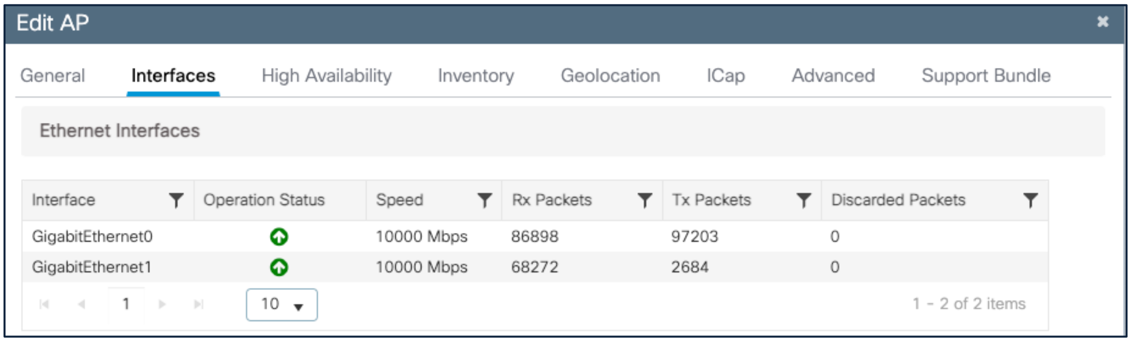
In LAG Deployment, AP will draw power on both the ports. Traffic is load-balanced on both the ports. The AP supports static LAG (mode on) or dynamic with LACP. The CW9178I supports deployment with one single physical or logical switch.

Note:

1. The default mode of operation of the CW9178I is non-LAG mode.
2. When the AP is configured in LAG mode, dual-home deployment is not supported.
3. The maximum aggregated throughput is 10 Gbps. So, even if the speed from both ports totals more than 10 Gbps, the performance will not be higher than 10 Gbps.

View Interface Status

To view the status of the AP's ports on the Catalyst 9800 UI, navigate to **Configuration > Wireless > Access Points > [select the CW9178I AP] > Interfaces > Ethernet Interfaces.** This table allows you to view the port speeds connected to the AP for both Ethernet0 and Ethernet1.



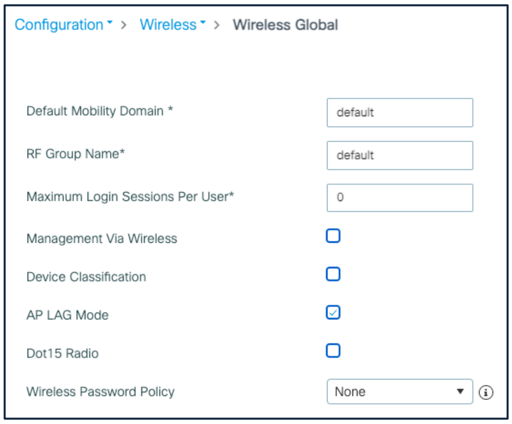
Interface	Operation Status	Speed	Rx Packets	Tx Packets	Discarded Packets
GigabitEthernet0	⬆	10000 Mbps	86898	97203	0
GigabitEthernet1	⬆	10000 Mbps	68272	2684	0

Figure 11. AP Port Status in the Cisco Catalyst 9800 controller GUI

LAG Configuration Steps:

To configure LAG support for the AP, enable it on the Cisco Catalyst 9800 controller and the individual switches.

To configure LAG at the global level in the Cisco Catalyst 9800 controller GUI, navigate to **Configuration > Wireless > Wireless Global** and select **AP LAG mode**.

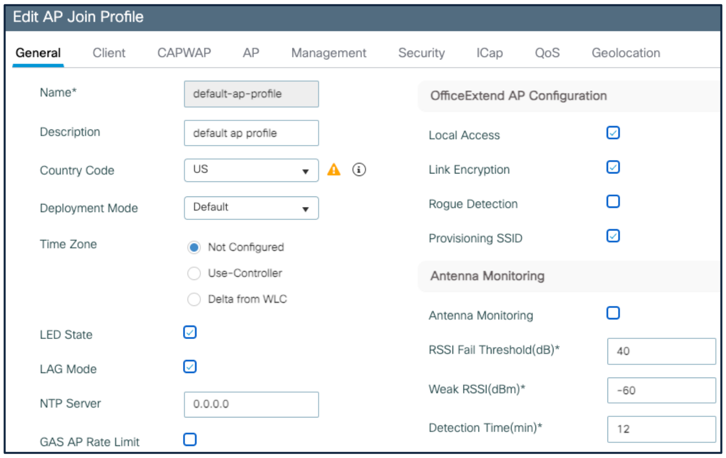


Default Mobility Domain *	default
RF Group Name*	default
Maximum Login Sessions Per User*	0
Management Via Wireless	□
Device Classification	□
AP LAG Mode	☑
Dot15 Radio	□
Wireless Password Policy	None

Figure 12. Enable LAG Globally in the Cisco Catalyst 9800 controller GUI

To configure LAG for an AP join profile, navigate to **Configuration > Tags and Profiles > AP Join >** *[Select the AP Join Profile that CW9178I is associated with]* **> General** and enable **LAG Mode**.

Note: By default, **LAG mode** is disabled on an AP join profile.



Name*	default-ap-profile
Description	default ap profile
Country Code	US
Deployment Mode	Default
Time Zone	● Not Configured ○ Use-Controller ○ Delta from WLC
LED State	☑
LAG Mode	☑
NTP Server	0.0.0.0
GAS AP Rate Limit	□

OfficeExtend AP Configuration

Local Access	☑
Link Encryption	☑
Rogue Detection	□
Provisioning SSID	☑

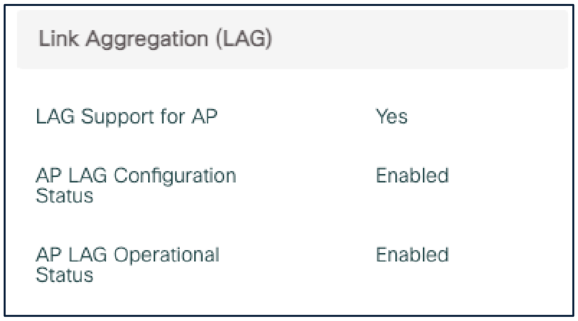
Antenna Monitoring

Antenna Monitoring	□
RSSI Fail Threshold(dB)*	40
Weak RSSI(dBm)*	-60
Detection Time(min)*	12

Figure 13. **Enable LAG for an AP Join Profile in the Cisco Catalyst 9800 controller GUI**

AP LAG verification

To verify that link aggregation is now enabled, navigate to **Configuration > Wireless > Access Points > [select the Catalyst 9178I AP] > Interfaces > Link Aggregation (LAG)**. Both the **AP LAG Configuration Status** and **AP LAG Operational Status** should be **Enabled**.



Link Aggregation (LAG)

LAG Support for AP	Yes
AP LAG Configuration Status	Enabled
AP LAG Operational Status	Enabled

Figure 14. **Verify LAG is enabled in the Cisco Catalyst 9800 controller GUI**

Switch LAG verification

To complete the LAG configuration, configure LAG on the switch too. This can be done either via static LAG configuration or via Link Aggregation Control Protocol (LACP). For more information on configuring LAG on a Cisco Catalyst switch, go to https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-15/configuration_guide/lyr2/b_1715_lyr2_9300_cg/configuring_etherchannels.html.

Note:

1. CW9178I does not support PAgP.
2. LAG can be configured only between two ports of the same speed. If the ports have differing speeds, it will not work, and the AP will default to the primary port (port0).

Recommendations and Limitations for Dual Ethernet Deployment

- The default mode of operation is non-LAG. In a non-LAG deployment, the two ethernet ports can be connected to the same switch (single-homed) or to two different switches (dual-homed). In the single-homed deployment, it is recommended to connect to

- the same switch
- two different members of a stack in a stack deployment, or
- two different line cards of a modular switch.

The switch ports in both single-homed or dual-homed deployments have to be in the same VLAN. If not, then link redundancy will not work and this will result in AP rejoining but with traffic loss.

- In LAG mode, dual-homed deployment is not supported. The 9178I AP has to be connected to the same physical or logical switch.
- AP port authentication with 802.1X or MAB is currently not supported for link redundancy in both non-LAG and LAG deployments. PoE redundancy will work with AP port authentication.
- Dual Ethernet deployment is not supported in SDA deployments for link redundancy with single or dual homed deploments. PoE redundancy will work in SDA deployments.

Table 7. AP Features Supported in Non-LAG and LAG modes

Feature	Non LAG (Single Homed)	Non LAG (Dual Homed)	Non LAG (Mode On)	LAG (Mode Active)
PoE Redundancy	Yes	Yes	Yes	Yes
Link Redundancy	Yes	Yes	Yes	Yes
CAPWAP Control Connection to WLC	Yes	Yes	Yes	Yes
Datapath - Local Mode	Yes	Yes	Yes	Yes
Datapath - Flex Mode	Yes	Yes	Yes	Yes
Datapath - Fabric Mode	Not supported*	Not supported*	Not supported	Not supported
802.1x Port Control	Not supported*	Not supported*	Not supported at the switch	Not supported at the switch
MAB Authentication	Not supported*	Not supported*	Not supported at the switch	Not supported at the switch
IP connectivity (ssh, syslog)	Yes	Yes	Yes	Yes
Connectivity to Catalyst Cetner	Yes	Yes	Yes	Yes
Connectivity to Cisco Spaces	Yes	Yes	Yes	Yes

Note: Not supported* - Current limitation in the software. Limitation will be removed in the future.

Global Use AP

The CW9178I is a unified product, global use access point, that can be deployed with Cisco Catalyst 9800 Wireless LAN Controller (a.k.a Catalyst Management Mode) or cloud-based deployment with Meraki Wireless Stack (a.k.a Meraki Management Mode) anywhere in the world, where it's certified to use without the need for a regulatory domain specific SKU. This gives customers the flexibility and investment protection, when they decide to deploy the Access Point in any of the deployment model.

The CW9178I can discover the management mode based on the customer's intent by the presence of cloud connectivity and discovery options based on DHCP and DNS. Once the Access Point discovers the controller, it can obtain its country specific regulation through 1) GPS/GNSS based geo-location, 2) proximity based discovery or 3) through a regulatory activation file for air-gapped deployments.

Please refer to the Wi-Fi 7 Global Use AP deployment guide for a detailed explanation and configuration options to achieve the desired management mode discovery. <Link TBD >

Quad-Radio Mode

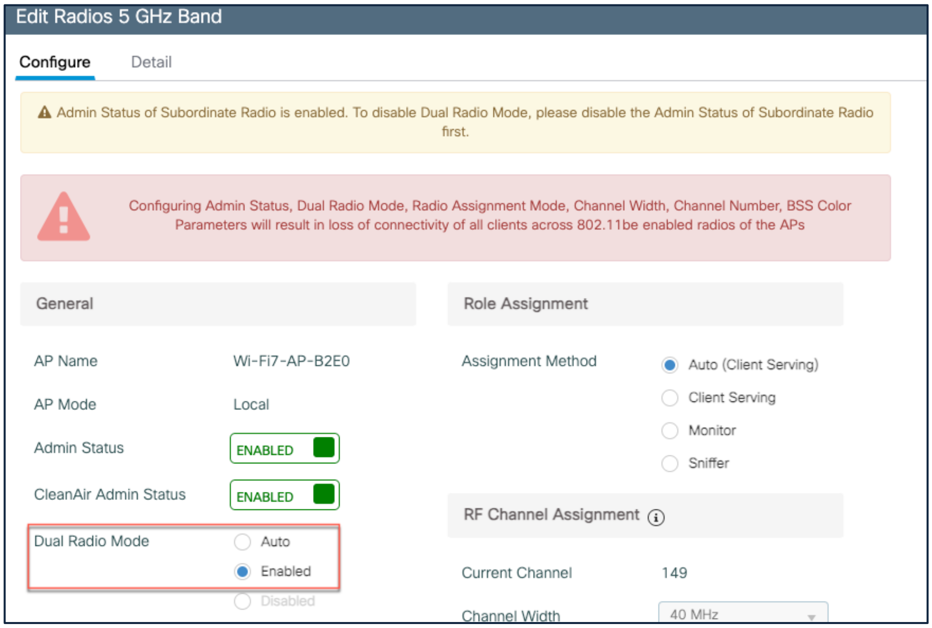
The CW9178I has four client serving radios. It can operate in a Tri-band Tri-Radio mode (2.4/5/6 GHz) or in Tri-band Quad-Radio mode (2.4/5/5/6 GHz) with two 5 GHz radio. When in Tri-Radio mode, the 5 GHz radio serves full band, covering all the allowed 5 GHz channels. When in Quad-Radio mode, the 5 GHz radio in Slot 1, serve UNII 1 &2 (Channels 36 to 64) and the 5 GHz radio in Slot 2, serves UNII 2E & 3 (Channels 100 to 165) in a **Macro-Macro** architecture.

By default, out-of-box, the AP operates in Tri-Radio mode.

All the CW9178I Aps can be converted to a Quad-Radio mode in one shot using the CLI

```
C9800#ap dot11 5ghz dual-radio mode enable
```

To individually convert the APs to Quad-Radio mode, navigate to **Configuration > Wireless > Access Points > 5 GHz Radios**, select Slot 1 of the CW9178, that needs to be converted to a Dual 5 GHz. Set **Dual Radio Mode** to Enabled.



Edit Radios 5 GHz Band

⚠ Admin Status of Subordinate Radio is enabled. To disable Dual Radio Mode, please disable the Admin Status of Subordinate Radio first.

Configuring Admin Status, Dual Radio Mode, Radio Assignment Mode, Channel Width, Channel Number, BSS Color Parameters will result in loss of connectivity of all clients across 802.11be enabled radios of the APs

General

AP Name: Wi-Fi7-AP-B2E0

AP Mode: Local

Admin Status: ENABLED

CleanAir Admin Status: ENABLED

Dual Radio Mode: ○ Auto ● Enabled ○ Disabled

Role Assignment

Assignment Method: ● Auto (Client Serving) ○ Client Serving ○ Monitor ○ Sniffer

RF Channel Assignment

Current Channel: 149

Channel Width: 40 MHz

Figure 15. Convert AP to Quad Radio Mode in the Cisco Catalyst 9800 controller GUI

To convert back to Single 5 GHz Radio, make the Admin Status of the subordinate Radio (Slot 2) to disabled. Then change the setting of Dual Radio Mode in Slot 1 to Disabled.

Getting started with Wi-FI 7

The IEEE developed the 802.11be amendment (a.k.a "Extremely High Throughput") to the 802.11 standard, which the Wi-Fi alliance adopted the draft v3.0, as the basis for Wi-Fi 7 certification. The Wi-Fi 7 alliance planned to adopt a subset of features from the 802.11be amendment as part of their Release 1 certification, that was made available in January 2024. A second release with support for an incremental set of features is planned for Release 2 certification, slated for December of 2025.

Wi-Fi 7 offers many enhancements that will benefit enterprises, as well as end users by increasing speeds up to four times compared to Wi-Fi 6. In addition, it offers super low latency, more robust connection, higher spectral efficiency, better interference mitigation, more power-saving techniques, better roaming experience, and increased security.

Wi-Fi 7 in essence, brings in the following features.

- 4096 QAM (a.k.a 4K-QAM) – encodes the number of bits in a sub-carrier to 12 bits, in contrast to 10 bits encoded in a sub-carrier for 1024 QAM in Wi-Fi 6. This introduces two new MCS rates MCS 12 and 13. 4K QAM helps upto 20% higher data transmission rates. This is an ***optional*** feature for Wi-Fi 7 certification.
- 320 MHz Channel Width (at 6 GHz) - The max channel width is doubled to 320 MHz when compared to 160 MHz in Wi-Fi 6. With 1200 MHz spectrum space available in the 6 GHz band, it's possible to achieve 3x 320 MHz wide channels. This is an ***optional*** feature for Wi-Fi 7 certification.
- Multi-link operation (a.k.a MLO) – enables aggregation of multiple bands or channels. With MLO, the Wi-Fi 7 Access Point and Client devices can can associate and simultaneously exchange traffic on multiple bands (or multiple channels in the same band if the access point has a dual 5 GHz radio). The distribution of traffic on different bands, help achieve higher throughput, reduced latency and improves reliability. This is a ***mandatory*** feature for Wi-Fi 7 certification.
- Preamble Puncturing - allows access points to 'carve out' or 'puncture' a portion of channel width that is affected by interference, resulting in the remaining channel being used for data transmission. This ensures optimal Wi-Fi performance especially when there is interference.This is a ***mandatory*** feature for Wi-Fi 7 certification.
- Multiple Resource Unit (a.k.a MRU) – improves the OFDMA technology (that was introduced in 802.11ax amendment/Wi-Fi 6). OFDMA allows sub-carriers in a channel bandwidth to be grouped into smaller portions called "Resource Units," (RUs). These individual RUs are assigned to different stations, which allows access points to serve them simultaneously during uplink and downlink transmissions. In Wi-Fi 6, access points assign only a single RU to each wireless client. Wi-Fi 7 allows multiple resource units (MRUs) to be assigned to each wireless client. MRUs enhance spectral efficiency and interference mitigation. This is a ***mandatory*** feature for Wi-Fi 7 certification.

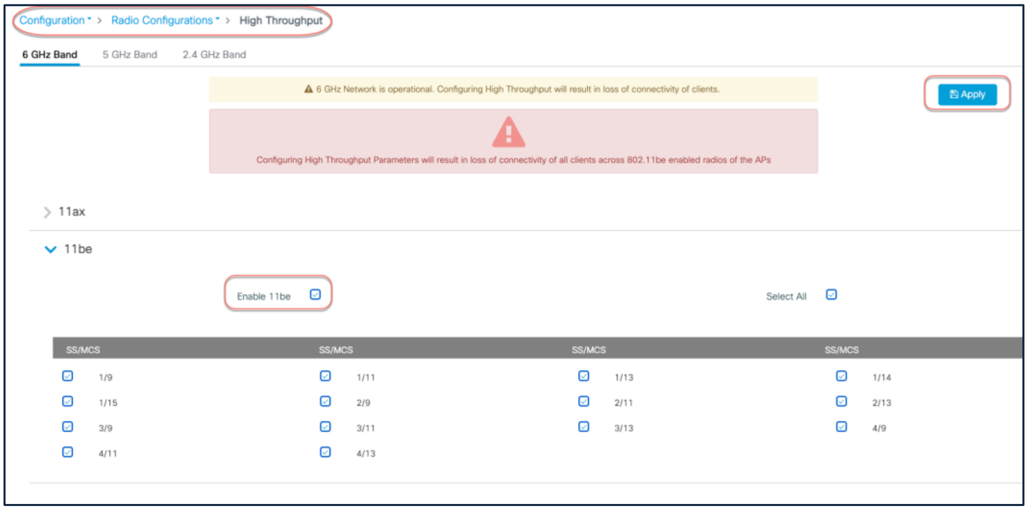
The next sections details the configuration steps needed to enable 802.11be and the other features.

Enable 11be

In the Cisco Catalyst 9800 controller GUI, navigate to **Configurations > Radio Configurations > High Throughput**, and choose **Enable 11be** for the bands where 802.11be is needed, and click **Apply**.

Note:

1. It is recommended to enable this for all the bands.
2. If 802.11be is enabled, MLO gets enabled too. This MLO setting is not independent and of the 802.11be configuration..



⚠ 6 GHz Network is operational. Configuring High Throughput will result in loss of connectivity of clients.

Configuring High Throughput Parameters will result in loss of connectivity of all clients across 802.11be enabled radios of the APs

Enable 11be ☑

Select All ☑

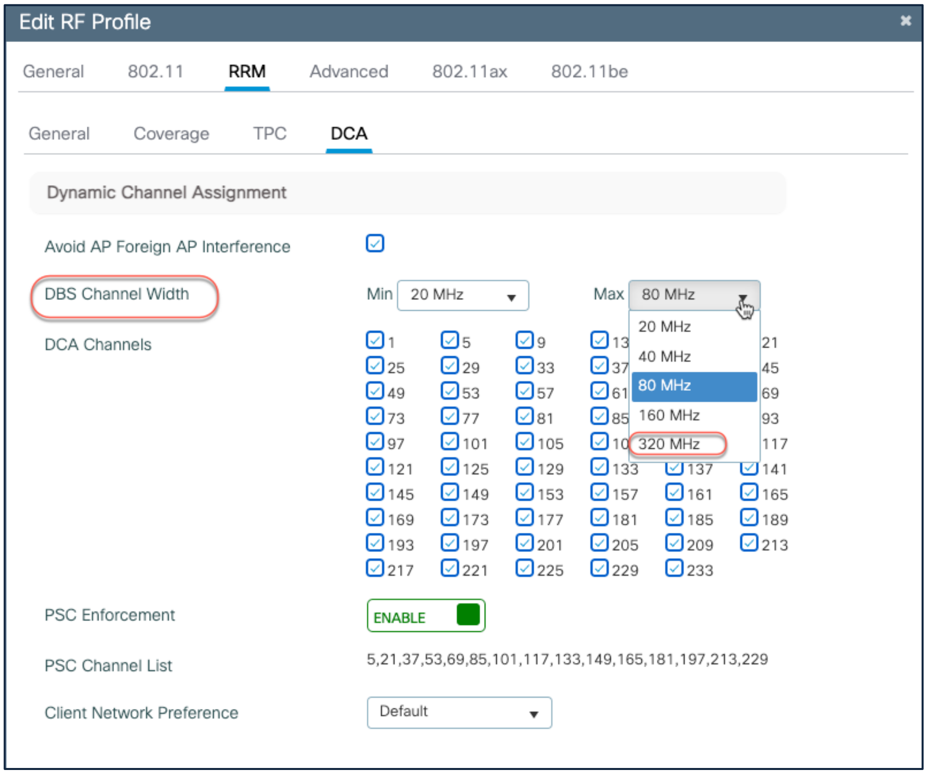
SS/MCS	SS/MCS	SS/MCS	SS/MCS
☑ 1/9	☑ 1/11	☑ 1/13	☑ 1/14
☑ 1/15	☑ 2/9	☑ 2/11	☑ 2/13
☑ 3/9	☑ 3/11	☑ 3/13	☑ 4/9
☑ 4/11	☑ 4/13		

Figure 16. Enable 11be for different bands in the Cisco Catalyst 9800 controller GUI

320 MHz

The channel width for the 6 GHz band, could be set to a maximum of 320 MHz in DBS channel width, for RRM to issue out a 320 MHz channel width, when its algorithm finds it conducive to issue a larger channel width.

From **Configuration > Tags & Profiles > RF/Radio**, edit the 6 GHz RF Profile to include 320 MHz as the max channel width.



Dynamic Channel Assignment

Avoid AP Foreign AP Interference ☑

DBS Channel Width Min 20 MHz Max 80 MHz

DCA Channels

☑ 1	☑ 5	☑ 9	☑ 13		21
☑ 25	☑ 29	☑ 33	☑ 37		45
☑ 49	☑ 53	☑ 57	☑ 61		69
☑ 73	☑ 77	☑ 81	☑ 85		93
☑ 97	☑ 101	☑ 105	☑ 10		117
☑ 121	☑ 125	☑ 129	☑ 133	☑ 137	☑ 141
☑ 145	☑ 149	☑ 153	☑ 157	☑ 161	☑ 165
☑ 169	☑ 173	☑ 177	☑ 181	☑ 185	☑ 189
☑ 193	☑ 197	☑ 201	☑ 205	☑ 209	☑ 213
☑ 217	☑ 221	☑ 225	☑ 229	☑ 233	

PSC Enforcement ENABLE

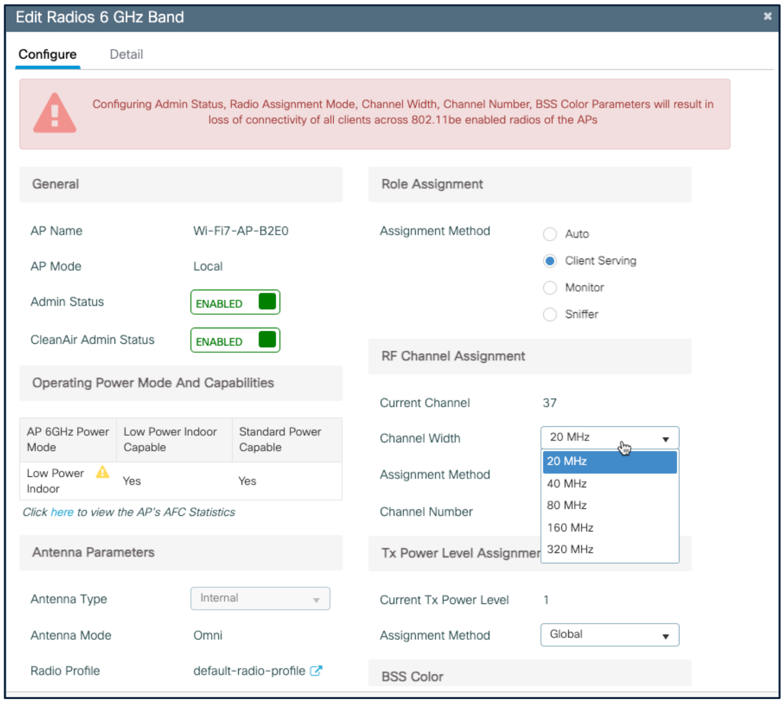
PSC Channel List 5,21,37,53,69,85,101,117,133,149,165,181,197,213,229

Client Network Preference Default

Figure 17. Update RF Profile to Set DBS Channel Width in the Cisco Catalyst 9800 controller GUI

A specific AP could be statically configured for 320 MHz on the access point configuration page.

Navigate to **Configuration > Wireless > Access Points > 6 GHz Radios**, select the AP, change the RF channel assignment to Custom and select 320 MHz as the channel width.



Configuring Admin Status, Radio Assignment Mode, Channel Width, Channel Number, BSS Color Parameters will result in loss of connectivity of all clients across 802.11be enabled radios of the APs

General

AP Name Wi-Fi7-AP-B2E0

AP Mode Local

Admin Status ENABLED

CleanAir Admin Status ENABLED

Operating Power Mode And Capabilities

AP 6GHz Power Mode	Low Power Indoor Capable	Standard Power Capable
Low Power Indoor ⚠	Yes	Yes

Click here to view the AP's AFC Statistics

Antenna Parameters

Antenna Type Internal

Antenna Mode Omni

Radio Profile default-radio-profile

Role Assignment

Assignment Method ○ Auto ● Client Serving ○ Monitor ○ Sniffer

RF Channel Assignment

Current Channel 37

Channel Width 20 MHz

Assignment Method

Channel Number

Tx Power Level Assignmen

Current Tx Power Level 1

Assignment Method Global

BSS Color

Figure 18. Set RF Channel Width in the Cisco Catalyst 9800 controller GUI

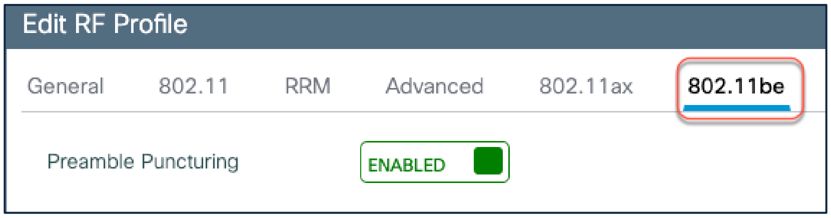
Preamble Puncturing

Preamble puncturing is supported for 80 MHz or higher channel widths. For an 80 MHz, only 20 MHz is allowed to the punctured. The following table lists the allowed preamble puncturing options.

Table 8. Software Interoperability

Channel Width	Allowed Puncturing
20 and 40 MHz	Puncturing not allowed
80 MHz	20 MHz
160 MHz	20 or 40 MHz
320 MHz	40, 80 or 40 + 80 MHz

To enable Preamble Puncturing, navigate to **Configuration > Tags & Profiles > RF/Radio** > edit the **RF Profile** of the 5 GHz and 6 GHz bands and enable **Preamble Puncturing** under the 802.11be tab.



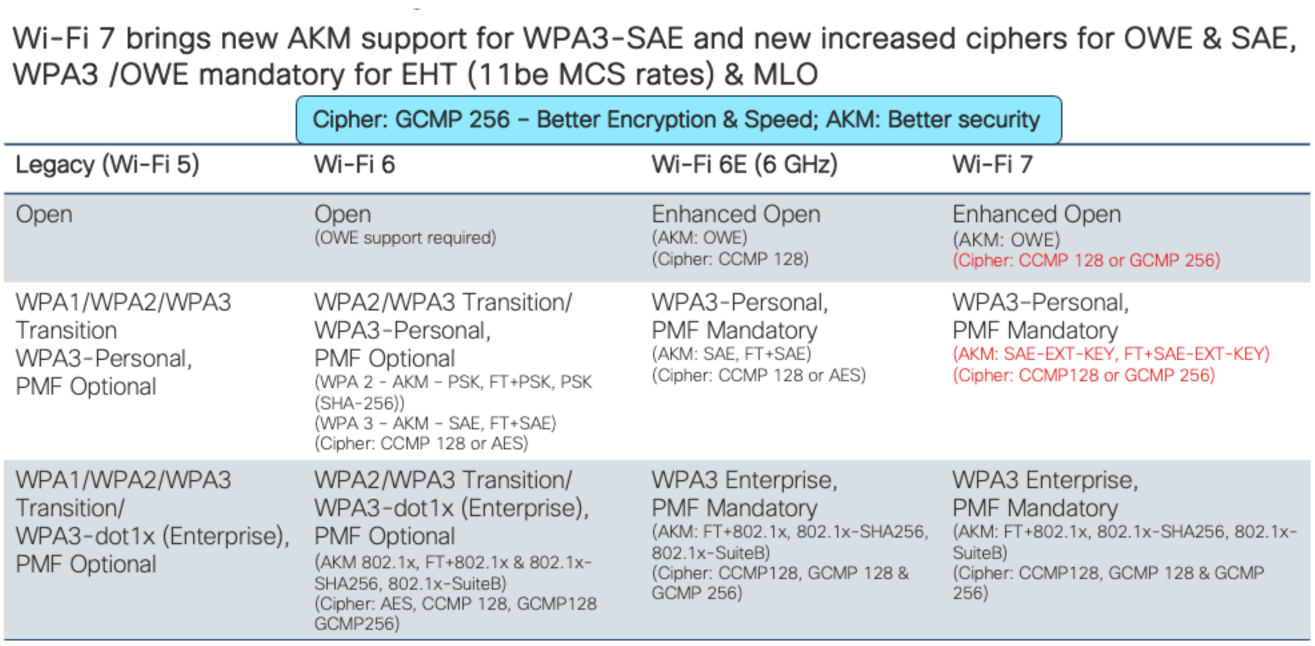
Preamble Puncturing ENABLED

Figure 19. Edit RF Profile to Enable Preamble Puncturing in the Cisco Catalyst 9800 controller GUI

Security

Wi-Fi 7 mandates the support for WPA3 and Enhanced Open (based on OWE) along with Protected Management Frame (PMF) for the clients to operate in 802.11be data rates and features like MLO. There are new AKMs (AKM 24 and 25) added for WPA3-Personal. Additionally, Wi-Fi 7 requires beacon protection for both the AP and the Wireless Clients. With MLO, security needs to be established across all the links of a multi-link association. The security requirements is to mainly make the Wi-Fi networks more secure and protect against cyberattacks.

The following table lists the security requirements for Wi-Fi 7 and comparison with previous Wi-Fi generations.



Wi-Fi 7 brings new AKM support for WPA3-SAE and new increased ciphers for OWE & SAE, WPA3 /OWE mandatory for EHT (11be MCS rates) & MLO

Cipher: GCMP 256 – Better Encryption & Speed; AKM: Better security

Legacy (Wi-Fi 5)	Wi-Fi 6	Wi-Fi 6E (6 GHz)	Wi-Fi 7
Open	Open (OWE support required)	Enhanced Open (AKM: OWE) (Cipher: CCMP 128)	Enhanced Open (AKM: OWE) (Cipher: CCMP 128 or GCMP 256)
WPA1/WPA2/WPA3 Transition WPA3-Personal, PMF Optional	WPA2/WPA3 Transition/ WPA3-Personal, PMF Optional (WPA 2 - AKM – PSK, FT+PSK, PSK (SHA-256)) (WPA 3 – AKM – SAE, FT+SAE) (Cipher: CCMP 128 or AES)	WPA3-Personal, PMF Mandatory (AKM: SAE, FT+SAE) (Cipher: CCMP 128 or AES)	WPA3-Personal, PMF Mandatory (AKM: SAE-EXT-KEY, FT+SAE-EXT-KEY) (Cipher: CCMP128 or GCMP 256)
WPA1/WPA2/WPA3 Transition/ WPA3-dot1x (Enterprise), PMF Optional	WPA2/WPA3 Transition/ WPA3-dot1x (Enterprise), PMF Optional (AKM 802.1x, FT+802.1x & 802.1x-SHA256, 802.1x-SuiteB) (Cipher: AES, CCMP 128, GCMP128 GCMP256)	WPA3 Enterprise, PMF Mandatory (AKM: FT+802.1x, 802.1x-SHA256, 802.1x-SuiteB) (Cipher: CCMP128, GCMP 128 & GCMP 256)	WPA3 Enterprise, PMF Mandatory (AKM: FT+802.1x, 802.1x-SHA256, 802.1x-SuiteB) (Cipher: CCMP128, GCMP 128 & GCMP 256)

WLAN Design Considerations

The security requirements for Wi-Fi 7 may necessitate a design change of the WLANs in the current deployment. There are a few options that the customer can consider, while implementing Wi-Fi 7.

Option 1 – Reconfigure the existing WLANs to WPA3/Enhanced Open, along with the required AKMs and Ciphers – i.e. one SSID for all radio policies. While this makes the WLAN most secure, there are practical difficulties in implementation, as many existing clients may not support WPA3 and PMF.

Option 2 – Add new SSIDs with the new security requirement for Wi-Fi 7 and have the newer clients associate to this SSID. This is an easy and flexible approach. The downside to this is maintaining additional SSIDs.

Option 3 – Migrate the SSIDs to Transition Mode – OWE Transition and WPA3 Transition. This is a conservative approach, taking one step to make the WLANs more secure and allowing newer clients with WPA3 security and older clients with WPA2 security to co-exist.

In the below section, you can find the configuration details for Option 3.

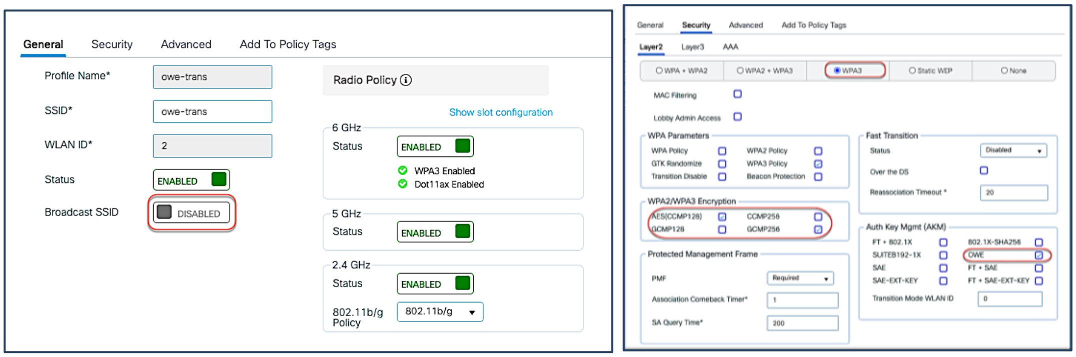
Open Security

Requirements for Wi-Fi 7: OWE, AKM 18, Cipher CCMP128 or GCMP 256.

Recommendation: Configure OWE Transition.

Configure two SSIDs.

SSID #1 with OWE, Broadcast disabled. Select WPA3 as the security, with AKM as OWE and Cipher as CCMP128 and GCMP256. Attach to all radio policies.



General | Security | Advanced | Add To Policy Tags

Profile Name*: owe-trans
SSID*: owe-trans
WLAN ID*: 2
Status: ENABLED
Broadcast SSID: DISABLED

Radio Policy ⓘ
Show slot configuration
6 GHz — Status: ENABLED
✓ WPA3 Enabled
✓ Dot11ax Enabled
5 GHz — Status: ENABLED
2.4 GHz — Status: ENABLED
802.11b/g Policy: 802.11b/g

General | Security | Advanced | Add To Policy Tags
Layer2 | Layer3 | AAA

○ WPA + WPA2 | ○ WPA2 + WPA3 | ● WPA3 | ○ Static WEP | ○ None

MAC Filtering □
Lobby Admin Access □

WPA Parameters
WPA Policy □ | WPA2 Policy □
GTK Randomize □ | WPA3 Policy ☑
Transition Disable □ | Beacon Protection □

WPA2/WPA3 Encryption
AES(CCMP128) ☑ | CCMP256 □
GCMP128 □ | GCMP256 ☑

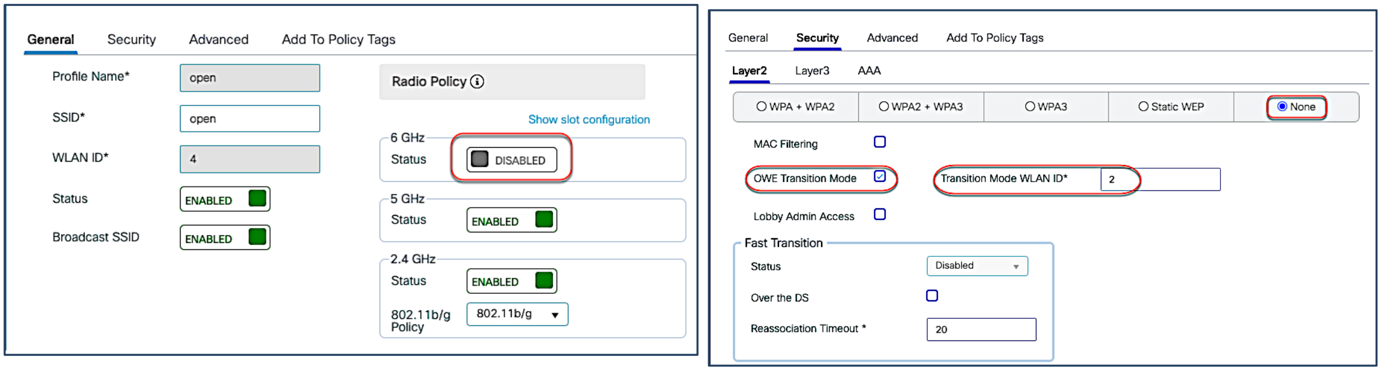
Protected Management Frame
PMF: Required
Association Comeback Timer*: 1
SA Query Time*: 200

Fast Transition
Status: Disabled
Over the DS □
Reassociation Timeout *: 20

Auth Key Mgmt (AKM)
FT + 802.1X □ | 802.1X-SHA256 □
SUITEB192-1X □ | OWE ☑
SAE □ | FT + SAE □
SAE-EXT-KEY □ | FT + SAE-EXT-KEY □
Transition Mode WLAN ID: 0

Figure 20. Configure OWE SSID with Broadcast Disabled and WPA3 security in the Cisco Catalyst 9800 controller GUI

SSID #2 with Open, Broadcast enabled. Select Open as the security and map this WLAN to the OWE WLAN created above (SSID #1). Attach the radio policy to 2.4 and 5 GHz.



General | Security | Advanced | Add To Policy Tags

Profile Name*: open
SSID*: open
WLAN ID*: 4
Status: ENABLED
Broadcast SSID: ENABLED

Radio Policy ⓘ
Show slot configuration
6 GHz — Status: DISABLED
5 GHz — Status: ENABLED
2.4 GHz — Status: ENABLED
802.11b/g Policy: 802.11b/g

General | Security | Advanced | Add To Policy Tags
Layer2 | Layer3 | AAA

○ WPA + WPA2 | ○ WPA2 + WPA3 | ○ WPA3 | ○ Static WEP | ● None

MAC Filtering □
OWE Transition Mode ☑
Transition Mode WLAN ID*: 2
Lobby Admin Access □

Fast Transition
Status: Disabled
Over the DS □
Reassociation Timeout *: 20

Figure 21. Configure Open SSID and Broadcast Enabled in the Cisco Catalyst 9800 controller GUI

Older clients connect with “open” security on 2.4 or 5 GHz bands. Newer Wi-Fi 7 clients connect with “OWE” security on 2.4/5/6 GHz and can perform Multi-link operation (MLO).

Note: Very old clients with outdated drivers may have difficulty in associating to OWE Transition Mode. It’s highly recommended to update the drivers and test the clients in the environment.

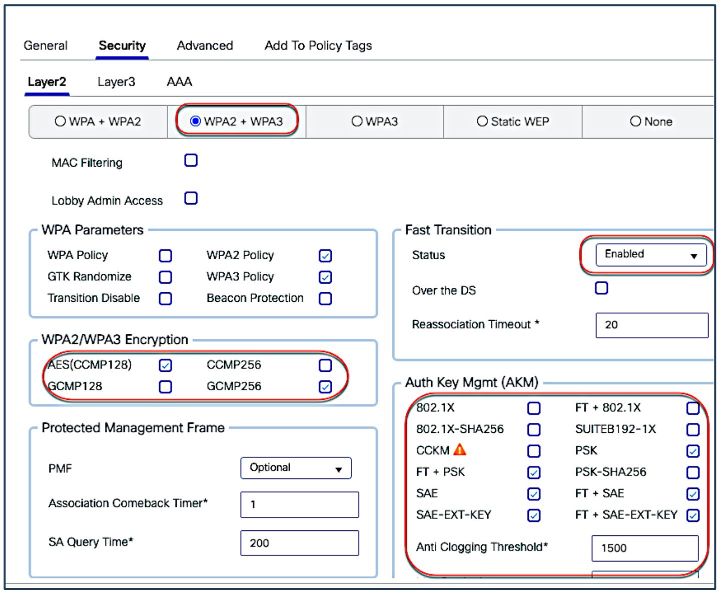
WPA2/WPA3 Personal Security

Requirements for Wi-Fi 7: AKM 24 or 25, Cipher CCMP128 or GCMP 256.

Recommendation: Configure WPA3 Transition (WPA2 + WPA3 Mixed Mode).

Configure the SSID to be WPA2 + WPA3 security type. Select AKM as PSK, SAE and SAE-EXT-KEY. Cipher as CCM128 and GCMP256. PMF as Optional. Use the same password.

Note: If FT is enabled, select FT+PSK, FT+SAE and FT+SAE-EXT-KEY.



General | **Security** | Advanced | Add To Policy Tags

Layer2 | Layer3 | AAA

○ WPA + WPA2 | ● WPA2 + WPA3 | ○ WPA3 | ○ Static WEP | ○ None

MAC Filtering □

Lobby Admin Access □

WPA Parameters

WPA Policy	□	WPA2 Policy	☑
GTK Randomize	□	WPA3 Policy	☑
Transition Disable	□	Beacon Protection	□

WPA2/WPA3 Encryption

AES(CCMP128)	☑	CCMP256	□
GCMP128	□	GCMP256	☑

Protected Management Frame

PMF: Optional

Association Comeback Timer*: 1

SA Query Time*: 200

Fast Transition

Status: Enabled

Over the DS □

Reassociation Timeout *: 20

Auth Key Mgmt (AKM)

802.1X	□	FT + 802.1X	□
802.1X-SHA256	□	SUITEB192-1X	□
CCKM ⚠	□	PSK	☑
FT + PSK	☑	PSK-SHA256	□
SAE	☑	FT + SAE	☑
SAE-EXT-KEY	☑	FT + SAE-EXT-KEY	☑

Anti Clogging Threshold*: 1500

Figure 22. **Configure WPA3 Transition (WPA2+WPA3 mixed mode) in the Cisco Catalyst 9800 controller GUI**

Wi-Fi 7 clients connect with WPA3/SAE-EXT-KEY or WPA3/FT-SAE-EXT-KEY with PMF

Wi-Fi 6E clients connect with WPA3/SAE or WPA3/FT-SAE with PMF

Wi-Fi 6 clients that support WPA3 connect with WPA3/SAE or WPA3/FT-SAE with PMF in 2.4 /5 GHz bands.

Note:

1. Wi-Fi 7 needs AKM 24 or 25 as per specification. The initial clients in the market seem to negotiate 11be rates/MLO even with AKM 8 & 9. This may change in the future, when client driver implementation gets stricter.
2. If very old clients that still use WPA1 are present in the network, then the recommendation is to have those clients in a separate SSID.

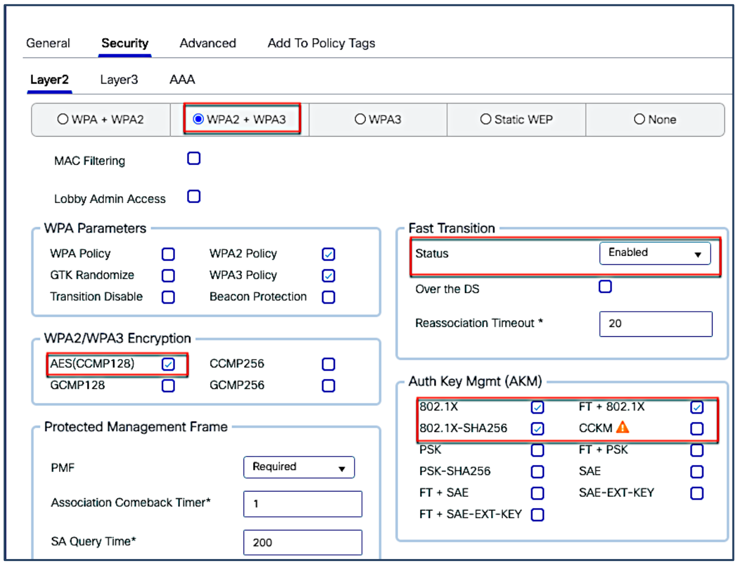
WPA2/WPA3 Enterprise Security

Requirements for Wi-Fi 7 : AKM 3 or 5, Cipher CCMP128 (For most common deployments)

Recommendation : Configure WPA3 Transition (WPA2 + WPA3 Mixed Mode).

Configure the SSID to be WPA2 + WPA3 security type. Select AKM as 802.1x-SHA256 and 802.1x.

Note: If FT is enabled, select AKM as FT+802.1x.



General | **Security** | Advanced | Add To Policy Tags

Layer2 | Layer3 | AAA

○ WPA + WPA2 | ● WPA2 + WPA3 | ○ WPA3 | ○ Static WEP | ○ None

MAC Filtering □

Lobby Admin Access □

WPA Parameters

WPA Policy	□	WPA2 Policy	☑
GTK Randomize	□	WPA3 Policy	☑
Transition Disable	□	Beacon Protection	□

WPA2/WPA3 Encryption

AES(CCMP128)	☑	CCMP256	□
GCMP128	□	GCMP256	□

Protected Management Frame

PMF: Required

Association Comeback Timer*: 1

SA Query Time*: 200

Fast Transition

Status: Enabled

Over the DS □

Reassociation Timeout *: 20

Auth Key Mgmt (AKM)

802.1X	☑	FT + 802.1X	☑
802.1X-SHA256	☑	CCKM ⚠	□
PSK	□	FT + PSK	□
PSK-SHA256	□	SAE	□
FT + SAE	□	SAE-EXT-KEY	□
FT + SAE-EXT-KEY	□		

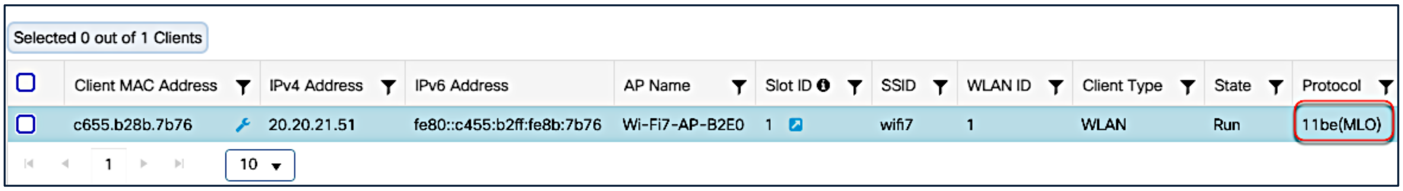
Figure 23. Configure WPA3 Transition (WPA2+WPA3 mixed mode) in the Cisco Catalyst 9800 controller GUI

On the client side that support WPA3, configure WPA3 Enterprise. Wi-Fi 7 clients will use the settings to connect to any band with MLO. For Wi-Fi 6E clients, they will prefer connecting to 6 GHz band and Wi-Fi 6 clients will connect to 5 or 2.4 GHz band. For clients that don't support WPA3, configure a WPA2 profile.

Note: Very old clients with outdated drivers may have difficulty in associating to WPA3 Transition Mode. It's highly recommended to update the drivers and test the clients in the environment.

Viewing Clients

The Cisco Catalyst 9800 GUI now displays the MLO capability and client statistics. From the main dashboard or **Monitoring > Clients**, select a client listed in the Protocol column as "11be (MLO)".



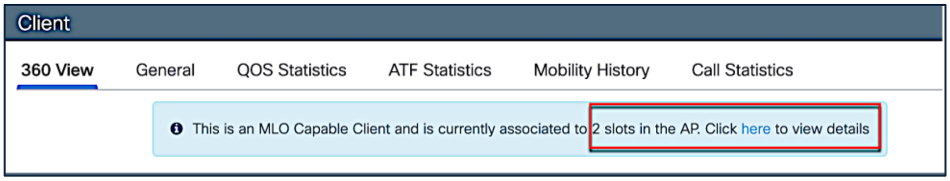
Selected 0 out of 1 Clients

□	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol
□	c655.b28b.7b76	20.20.21.51	fe80::c455:b2ff:fe8b:7b76	Wi-Fi7-AP-B2E0	1	wifi7	1	WLAN	Run	11be(MLO)

1 | 10

Figure 24. View Client Statistics in the Cisco Catalyst 9800 controller GUI

In the 360 View, the client's MLO capability is indicated along with the number of radio slots it is associated to. In the example below, the client is associated to 2 radio slots.



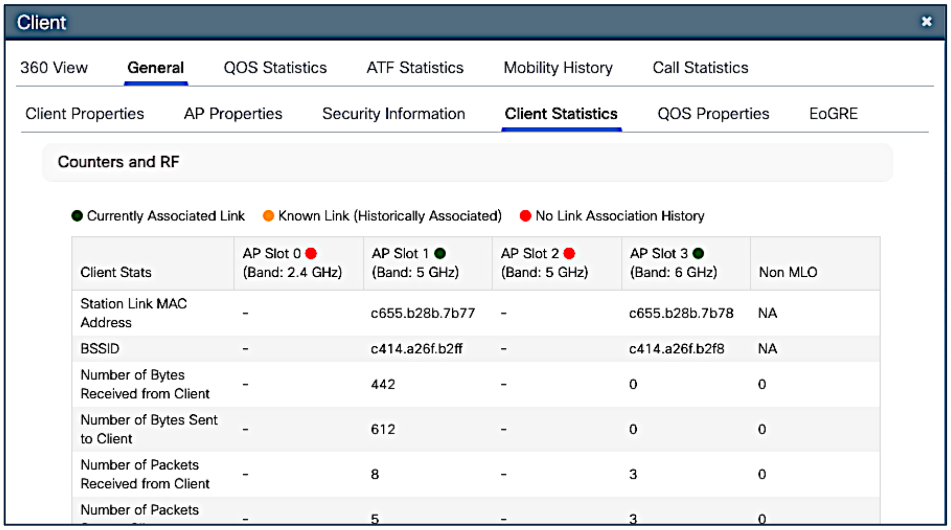
Client

360 View | General | QOS Statistics | ATF Statistics | Mobility History | Call Statistics

This is an MLO Capable Client and is currently associated to 2 slots in the AP. Click here to view details

Figure 25. View Client's MLO Capability and Associated Radio Slots in the Cisco Catalyst 9800 controller GUI

Click on the link to view the details, client propertis, security information and client statistics.



● Currently Associated Link 🟠 Known Link (Historically Associated) 🔴 No Link Association History

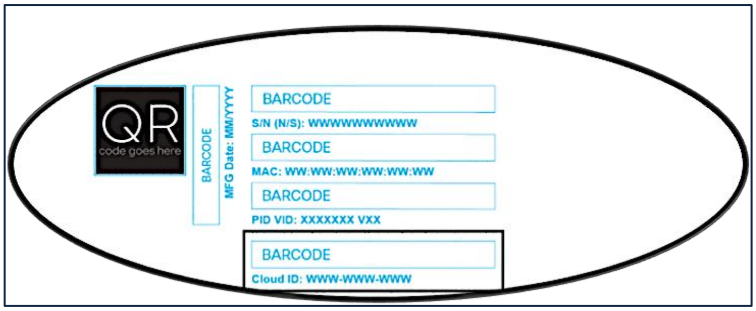
Client Stats	AP Slot 0 🔴 (Band: 2.4 GHz)	AP Slot 1 ● (Band: 5 GHz)	AP Slot 2 🔴 (Band: 5 GHz)	AP Slot 3 ● (Band: 6 GHz)	Non MLO
Station Link MAC Address	-	c655.b28b.7b77	-	c655.b28b.7b78	NA
BSSID	-	c414.a26f.b2ff	-	c414.a26f.b2f8	NA
Number of Bytes Received from Client	-	442	-	0	0
Number of Bytes Sent to Client	-	612	-	0	0
Number of Packets Received from Client	-	8	-	3	0
Number of Packets	-	5	-	3	0

Figure 26. View Client Statistics in the Cisco Catalyst 9800 controller GUI

Migration between Management Modes

The Cisco Wireless CW9178I is a Global Use, Unified Product and can convert from the Cisco Catalyst management mode to the Meraki management mode and vice versa. This Unified Product gives you the flexibility of being deployed in a Catalyst 9800 WLC based deployment or cloud based Meraki deployment. It also provides investment protection for the future in case you want to switch between the two management options anytime from Day 1 to Day N.

Starting with Wi-Fi 7 Access Points, the Meraki Serial Number has been renamed to "Cloud ID". There is no functional change to how this was used in the previous generation product.

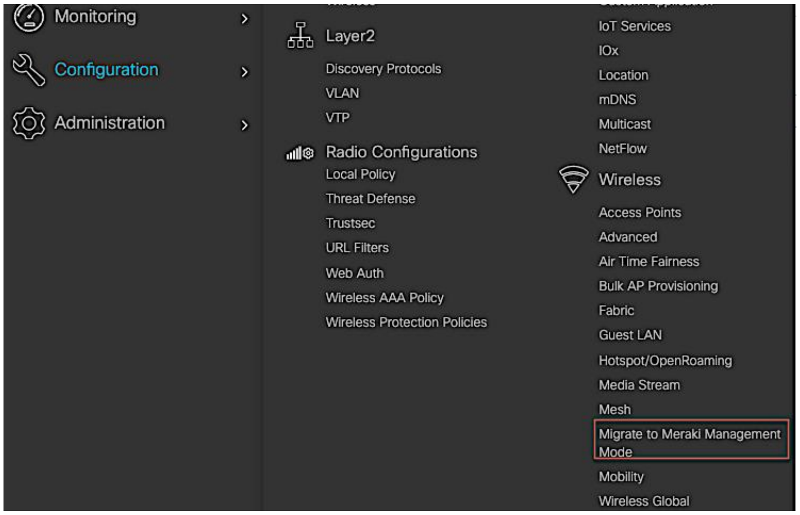


Conversion Process

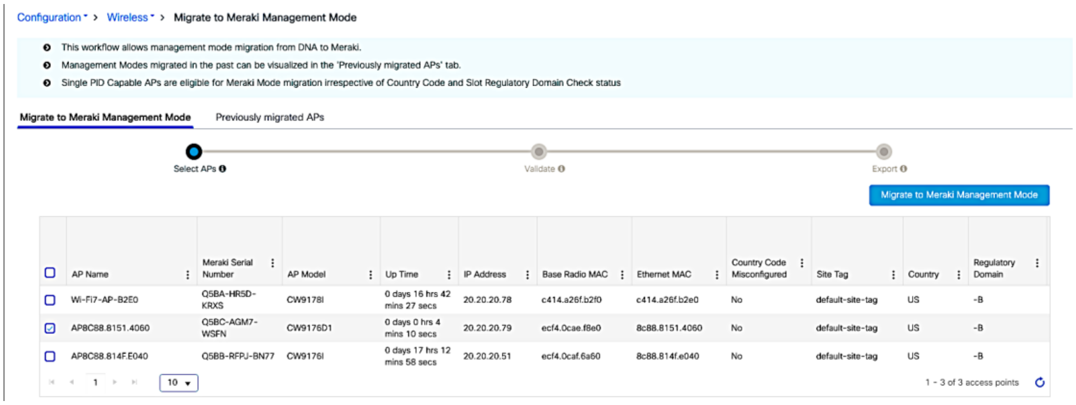
The CW9178I can be converted from Catalyst Management Mode to Meraki Management Mode through a simple work flow in C9800 WLC UI.

The following are the step to perform the conversion process.

1. Start the conversion workflow from Configuration → Wireless → Migrate to Meraki Management Mode.



2. Select the APs you want to convert and click Migrate to Meraki Management Mode.

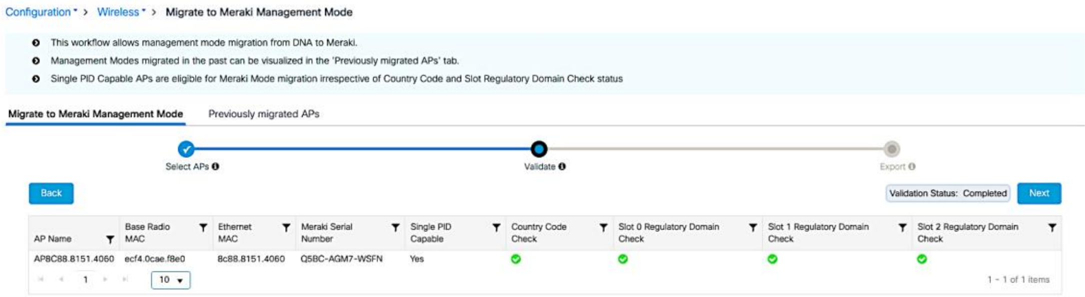

Configuration > Wireless > Migrate to Meraki Management Mode

- This workflow allows management mode migration from DNA to Meraki.
- Management Modes migrated in the past can be visualized in the 'Previously migrated APs' tab.
- Single PID Capable APs are eligible for Meraki Mode migration irrespective of Country Code and Slot Regulatory Domain Check status

Migrate to Meraki Management Mode
Previously migrated APs
Select APs
Validate
Export
Migrate to Meraki Management Mode

□	AP Name	Meraki Serial Number	AP Model	Up Time	IP Address	Base Radio MAC	Ethernet MAC	Country Code Misconfigured	Site Tag	Country	Regulatory Domain
□	Wi-Fi7-AP-B2E0	Q5BA-HR5D-KRXS	CW9178I	0 days 16 hrs 42 mins 27 secs	20.20.20.78	c414.a26f.b2f0	c414.a26f.b2e0	No	default-site-tag	US	-B
☑	AP8C88.8151.4060	Q5BC-AGM7-WSFN	CW9176D1	0 days 0 hrs 4 mins 10 secs	20.20.20.79	ecf4.0cae.f8e0	8c88.8151.4060	No	default-site-tag	US	-B
□	AP8C88.814F.E040	Q5BB-RFPJ-BN77	CW9176I	0 days 17 hrs 12 mins 58 secs	20.20.20.51	ecf4.0caf.6a60	8c88.814f.e040	No	default-site-tag	US	-B

3. The controller will then validate the APs. Select Next.

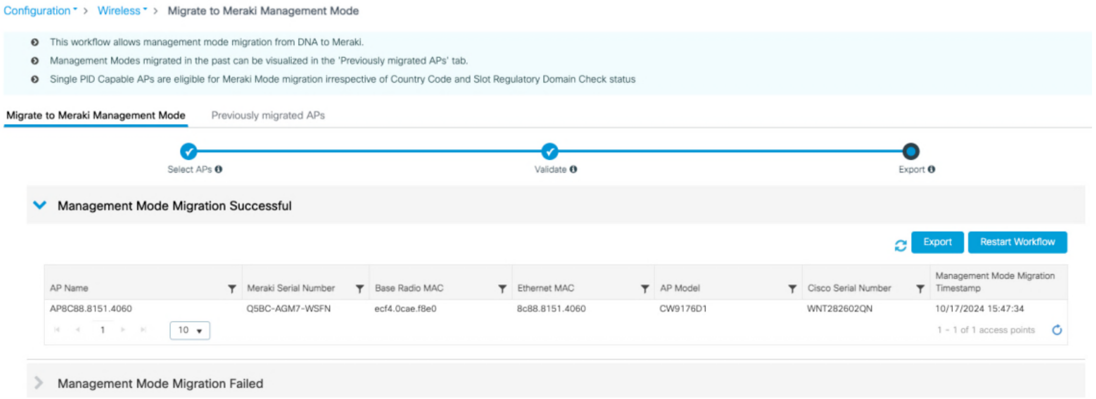

Configuration > Wireless > Migrate to Meraki Management Mode

- This workflow allows management mode migration from DNA to Meraki.
- Management Modes migrated in the past can be visualized in the 'Previously migrated APs' tab.
- Single PID Capable APs are eligible for Meraki Mode migration irrespective of Country Code and Slot Regulatory Domain Check status

Migrate to Meraki Management Mode
Previously migrated APs
Select APs
Validate
Export
Back
Validation Status: Completed
Next

AP Name	Base Radio MAC	Ethernet MAC	Meraki Serial Number	Single PID Capable	Country Code Check	Slot 0 Regulatory Domain Check	Slot 1 Regulatory Domain Check	Slot 2 Regulatory Domain Check
AP8C88.8151.4060	ecf4.0cae.f8e0	8c88.8151.4060	Q5BC-AGM7-WSFN	Yes	✓	✓	✓	✓

4. Confirm the change on the selected Access Points.



Configuration > Wireless > Migrate to Meraki Management Mode

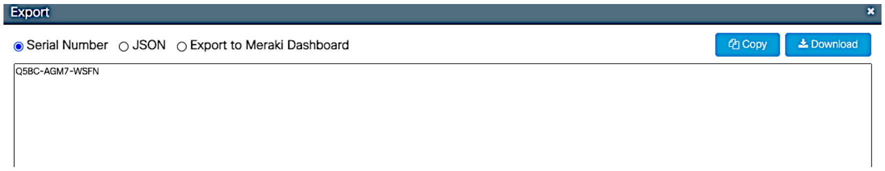
- This workflow allows management mode migration from DNA to Meraki.
- Management Modes migrated in the past can be visualized in the 'Previously migrated APs' tab.
- Single PID Capable APs are eligible for Meraki Mode migration irrespective of Country Code and Slot Regulatory Domain Check status

Management Mode Migration Successful

AP Name	Meraki Serial Number	Base Radio MAC	Ethernet MAC	AP Model	Cisco Serial Number	Management Mode Migration Timestamp
AP8C88.8151.4060	Q5BC-AGM7-WSFN	ecf4.0cae.f8e0	8c88.8151.4060	CW9176D1	WNT282602QN	10/17/2024 15:47:34

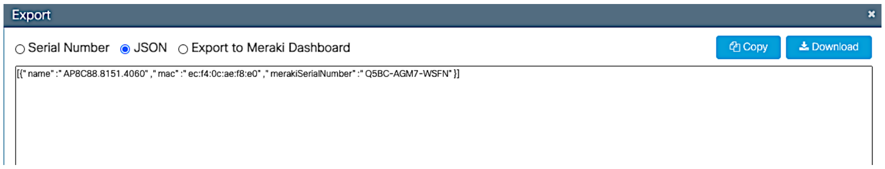
Management Mode Migration Failed

5. Export or download the data to be copied to Meraki Dashboard. The data can be exported in multiple formats – Serial Number, JSON or Export to Meraki Dashboard.



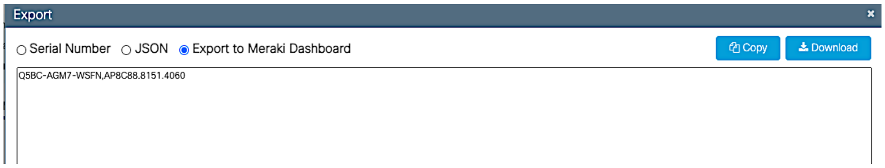
● Serial Number ○ JSON ○ Export to Meraki Dashboard

```
Q5BC-AGM7-WSFN
```



○ Serial Number ● JSON ○ Export to Meraki Dashboard

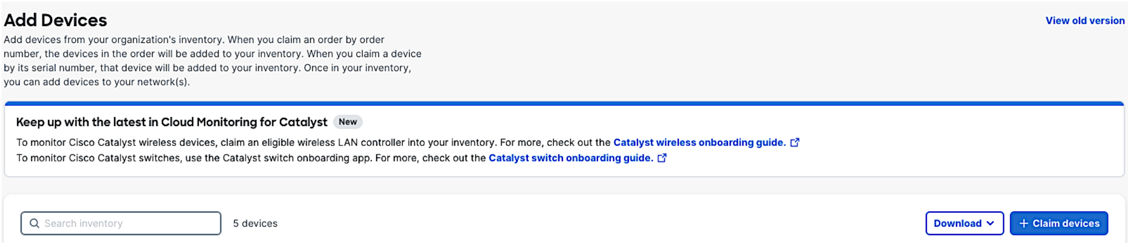
```
[{" name" :" AP8C88.8151.4060" ," mac" :" ec:f4:0c:ae:f8:e0" ," merakiSerialNumber" :" Q5BC-AGM7-WSFN" }]
```



○ Serial Number ○ JSON ● Export to Meraki Dashboard

```
Q5BC-AGM7-WSFN,AP8C88.8151.4060
```

6. Add devices in Meraki Dashboard. Follow the Meraki Claim process.



Add Devices

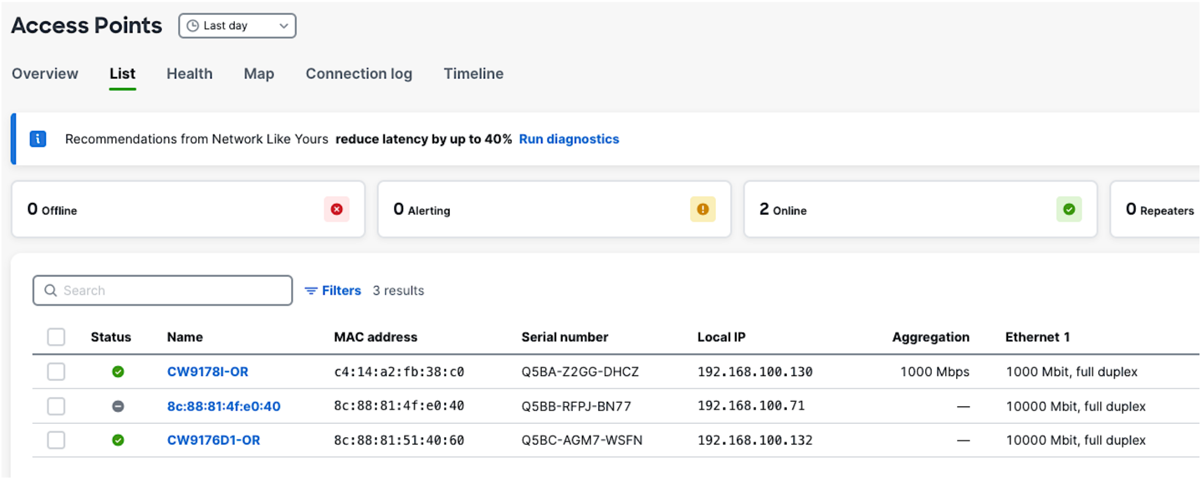
Add devices from your organization's inventory. When you claim an order by order number, the devices in the order will be added to your inventory. When you claim a device by its serial number, that device will be added to your inventory. Once in your inventory, you can add devices to your network(s).

Keep up with the latest in Cloud Monitoring for Catalyst New

To monitor Cisco Catalyst wireless devices, claim an eligible wireless LAN controller into your inventory. For more, check out the **Catalyst wireless onboarding guide.**

To monitor Cisco Catalyst switches, use the Catalyst switch onboarding app. For more, check out the **Catalyst switch onboarding guide.**

7. Once devices and claimed, the AP will appear in the dashboard in few minutes.



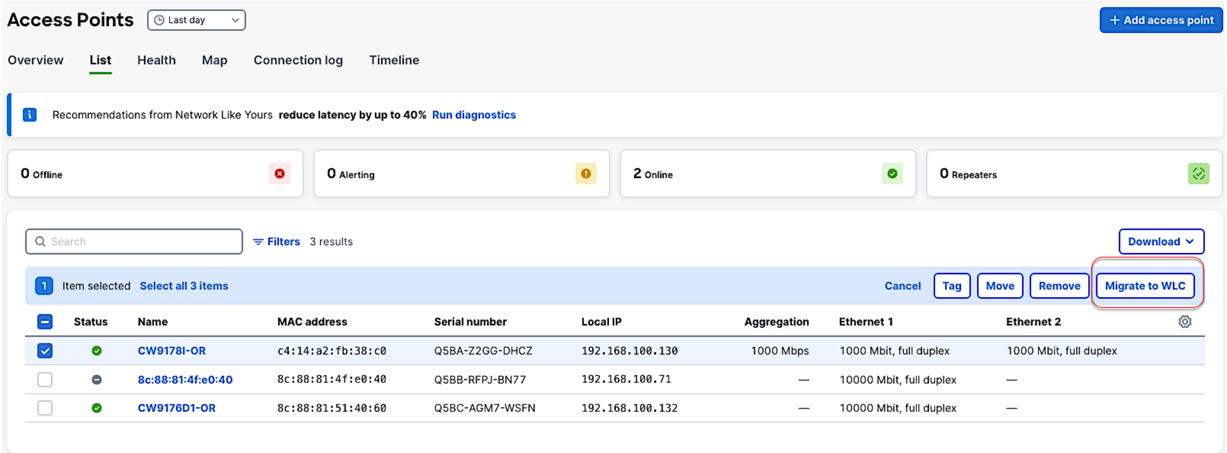
Recommendations from Network Like Yours **reduce latency by up to 40%** Run diagnostics

0 Offline | 0 Alerting | 2 Online | 0 Repeaters

3 results

	Status	Name	MAC address	Serial number	Local IP	Aggregation	Ethernet 1
□	●	CW9178I-OR	c4:14:a2:fb:38:c0	Q5BA-Z2GG-DHCZ	192.168.100.130	1000 Mbps	1000 Mbit, full duplex
□	●	8c:88:81:4f:e0:40	8c:88:81:4f:e0:40	Q5BB-RFPJ-BN77	192.168.100.71	—	10000 Mbit, full duplex
□	●	CW9176D1-OR	8c:88:81:51:40:60	Q5BC-AGM7-WSFN	192.168.100.132	—	10000 Mbit, full duplex

8. To convert an AP from Meraki Management Mode to Catalyst Management Mode, select the AP that you want to migrate and click on “Migrate to WLC”.



Recommendations from Network Like Yours **reduce latency by up to 40%** Run diagnostics

0 Offline | 0 Alerting | 2 Online | 0 Repeaters

3 results

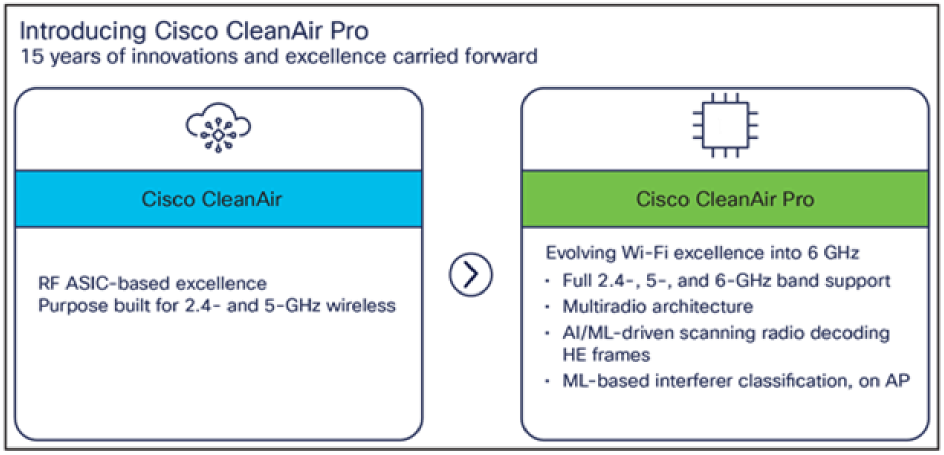
1 Item selected Select all 3 items

	Status	Name	MAC address	Serial number	Local IP	Aggregation	Ethernet 1	Ethernet 2
☑	●	CW9178I-OR	c4:14:a2:fb:38:c0	Q5BA-Z2GG-DHCZ	192.168.100.130	1000 Mbps	1000 Mbit, full duplex	1000 Mbit, full duplex
□	●	8c:88:81:4f:e0:40	8c:88:81:4f:e0:40	Q5BB-RFPJ-BN77	192.168.100.71	—	10000 Mbit, full duplex	—
□	●	CW9176D1-OR	8c:88:81:51:40:60	Q5BC-AGM7-WSFN	192.168.100.132	—	10000 Mbit, full duplex	—

Cisco CleanAir Pro

Wi-Fi 6E added 6 GHz spectrum for unlicensed use of Wi-Fi, and with it came new challenges for RF visibility and much more spectrum to monitor. In the past, the Catalyst 9100 APs relied on Cisco CleanAir® (software) and the RF-ASIC (hardware) for features such as packet capture, spectrum analysis, interference detection, and rogue and wireless intrusion prevention system (WIPS) detection. CleanAir and the RF-ASIC were great for RF visibility for the 2.4- and 5-GHz bands; however, with 6 GHz, Cisco CleanAir Pro and the AI/ML-driven scanning radio are being introduced to increase the performance and granularity required to manage this new spectrum (all 1200 MHz of it).

CleanAir Pro is software designed specifically for 6 GHz and the all-new challenges that have come with the introduction of 1200 MHz of spectrum. While many features work in conjunction with the AI/ML-driven scanning radio, CleanAir Pro also works with the Catalyst 9178I APs’ serving radios. Unlike previous generations of APs, CleanAir Pro can even decode extremely high throughput (EHT, 802.11be) frames, which is crucial since Wi-Fi 7 EHT frames. In the future, there will even be an ML-based interferer classification built directly into the AP software for more efficient interferer analysis, rather than loading the WLC or Cisco Catalyst Center.



Introducing Cisco CleanAir Pro

15 years of innovations and excellence carried forward

Cisco CleanAir

RF ASIC-based excellence
Purpose built for 2.4- and 5-GHz wireless

Cisco CleanAir Pro

Evolving Wi-Fi excellence into 6 GHz

- Full 2.4-, 5-, and 6-GHz band support
- Multiradio architecture
- AI/ML-driven scanning radio decoding HE frames
- ML-based interferer classification, on AP

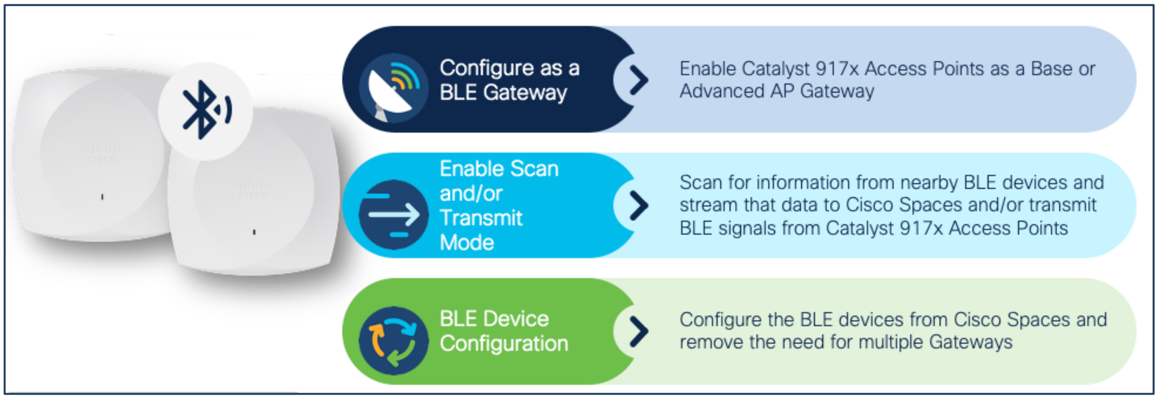
Internet of Things Integration

IoT Services with Cisco Spaces

The Catalyst CW9178I have a built-in IoT radio that can be used in conjunction with the IoT Services platform service in Cisco Spaces. IoT Services is designed to enable management of Internet of Things (IoT) devices across vendors, form factors, and technology protocols.

Within IoT Services, you can enable a CW9178I to be in Scan mode or Transmit mode. In Transmit mode, the AP can broadcast iBeacon, Eddystone URL, and Eddystone UID profiles. While in Scan mode, the AP can scan the vicinity for other BLE devices and receive telemetry data from floor beacons, which can be decoded in Cisco Spaces.

The CW9178I can manage and configure wireless IoT devices if you enable the Advanced AP Gateway feature, which installs a Cisco IOx application on the access point. This saves the user the trouble of having several gateways across different vendors.



Configure as a BLE Gateway

Enable Catalyst 917x Access Points as a Base or Advanced AP Gateway

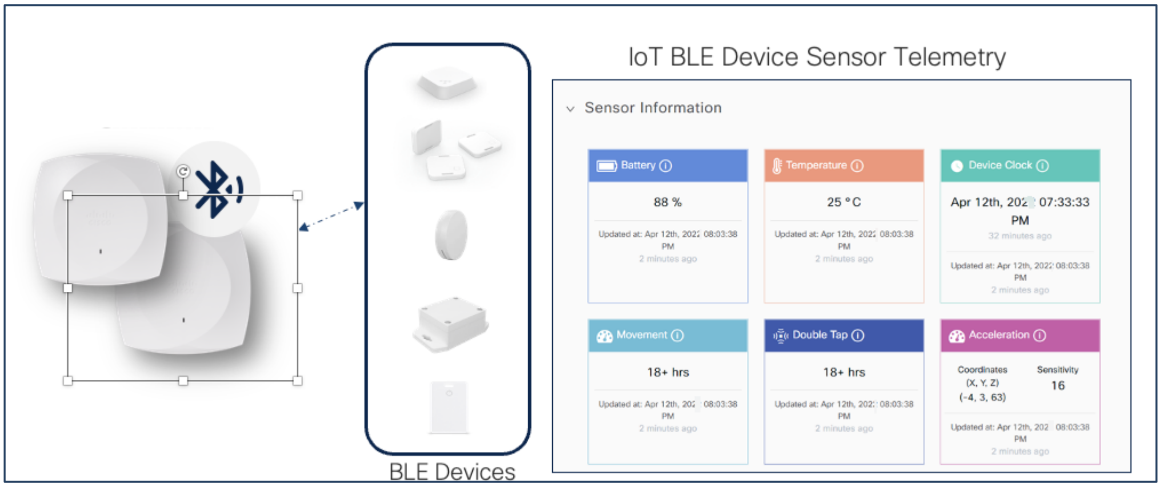
Enable Scan and/or Transmit Mode

Scan for information from nearby BLE devices and stream that data to Cisco Spaces and/or transmit BLE signals from Catalyst 917x Access Points

BLE Device Configuration

Configure the BLE devices from Cisco Spaces and remove the need for multiple Gateways

The figure below depicts the telemetry data received from a BLE device that is decoded in Cisco Spaces.



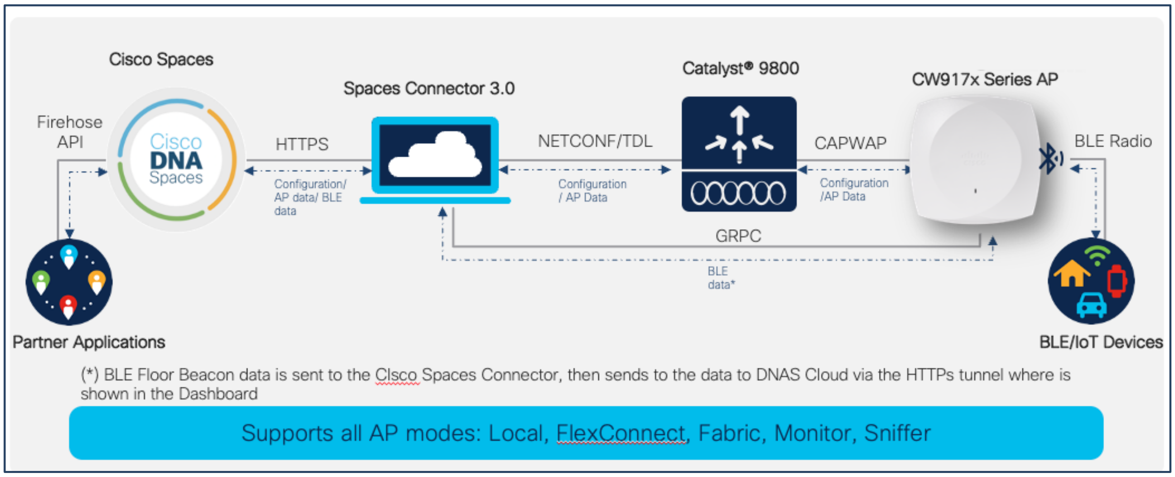
IoT BLE Device Sensor Telemetry

Sensor Information

Battery	Temperature	Device Clock
88 % Updated at: Apr 12th, 202 08:03:38 PM 2 minutes ago	25 °C Updated at: Apr 12th, 202 08:03:38 PM 2 minutes ago	Apr 12th, 202 07:33:33 PM 32 minutes ago Updated at: Apr 12th, 202 08:03:38 PM 2 minutes ago

Movement	Double Tap	Acceleration
18+ hrs Updated at: Apr 12th, 202 08:03:38 PM 2 minutes ago	18+ hrs Updated at: Apr 12th, 202 08:03:38 PM 2 minutes ago	Coordinates (X, Y, Z) (-4, 3, 63) Sensitivity 16 Updated at: Apr 12th, 202 08:03:38 PM 2 minutes ago

The figure below depicts how BLE data is sent from the Cisco Wireless CW9178I to Cisco Spaces.



(*) BLE Floor Beacon data is sent to the Clsco Spaces Connector, then sends to the data to DNAS Cloud via the HTTPs tunnel where is shown in the Dashboard

Supports all AP modes: Local, FlexConnect, Fabric, Monitor, Sniffer

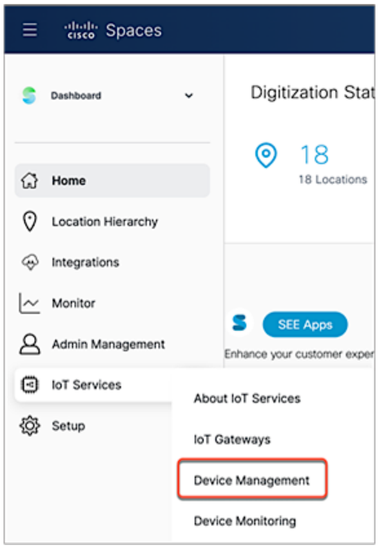
The built-in IoT radio require Cisco Spaces and IoT Services to be configured. Please use the following guides for configuring Cisco Spaces and IoT Services.

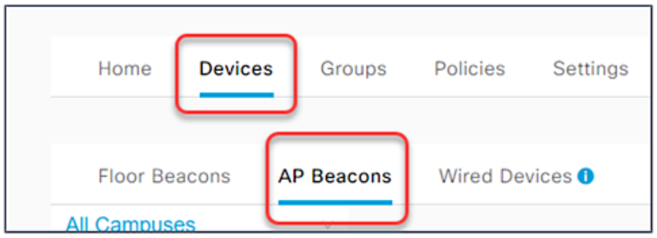
https://www.cisco.com/c/en/us/td/docs/wireless/spaces/config-guide/ciscospaces-configuration-guide.html

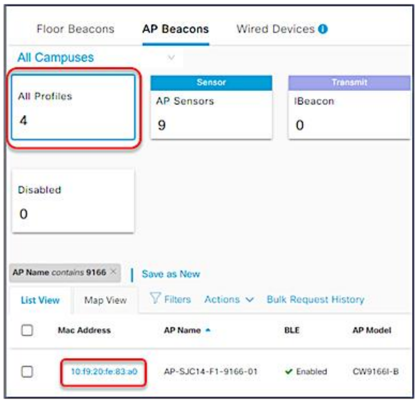
https://www.cisco.com/c/en/us/td/docs/wireless/cisco-dna-spaces/iot-services/b_iot_services.html

To enable the IoT radio or environmental sensors in Cisco Spaces, go to the specific access point in IoT Services in Cisco Spaces and select the feature to turn on or bulk-enable each feature in the AP Beacons page.

The figures below depict how to enable or disable the IoT radio or environmental sensors on Cisco Spaces through a specific access point.







All Profiles 4

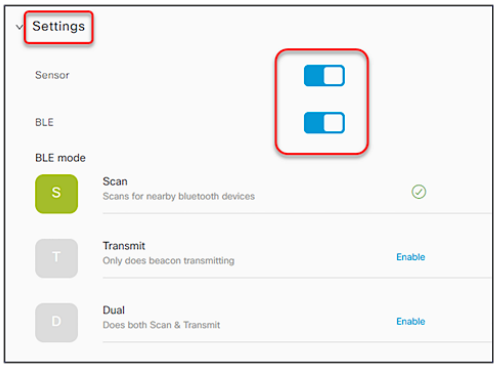
AP Sensors 9

IBeacon 0

Disabled 0

AP Name contains 9166

□	Mac Address	AP Name	BLE	AP Model
□	10:f9:20:fe:83:a0	AP-SJC14-F1-9166-01	✓ Enabled	CW9166I-B



Settings

Sensor

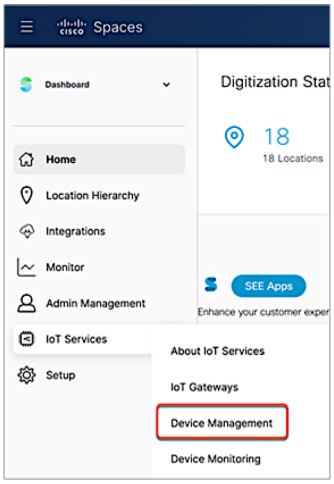
BLE

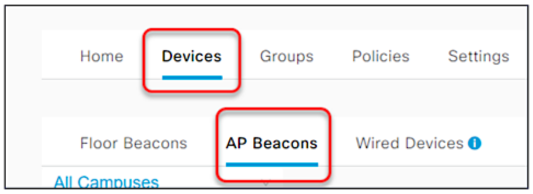
BLE mode

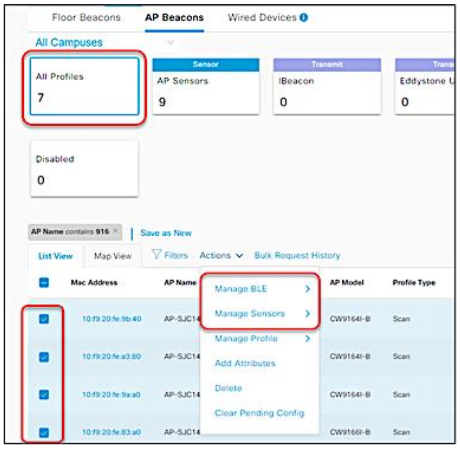
Scan
Scans for nearby bluetooth devices ✓

Transmit
Only does beacon transmitting

Dual
Does both Scan & Transmit







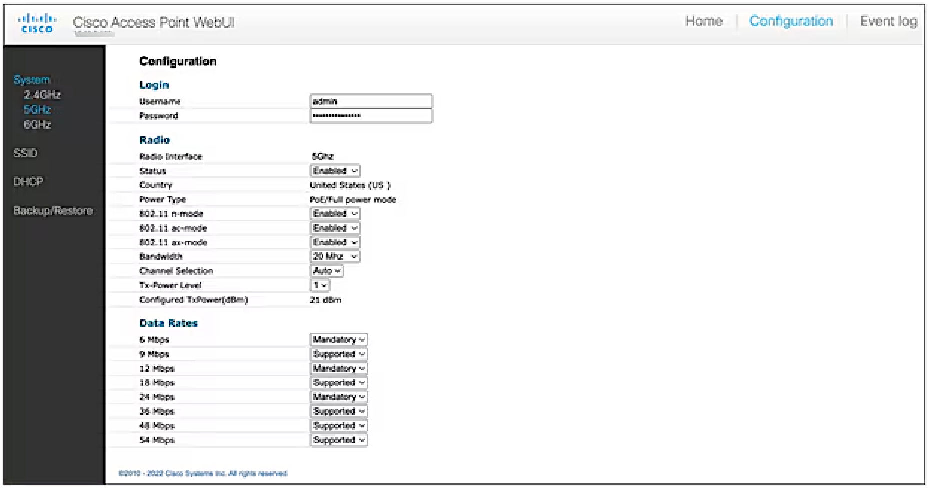
☐	Mac Address	AP Name	AP Model	Profile Type
☑	10:f9:20:fe:9b:40	AP-SJC14	CW9164I-B	Scan
☑	10:f9:20:fe:a3:80	AP-SJC14	CW9164I-B	Scan
☑	10:f9:20:fe:9a:a0	AP-SJC14	CW9164I-B	Scan
☑	10:f9:20:fe:83:a0	AP-SJC14	CW9166I-B	Scan

To learn more about Smart Workspaces or to request a demo, visit https://dnaspaces.cisco.com/smart-workspaces/

Site Survey Mode

The Cisco Wireless CW9178I supports Site Survey mode. The purpose of this mode is to allow users to conduct wireless site survey testing using a single access point, including understanding RF propagation, client join metrics, and so on, without the need for a controller. This mode converts the AP into a limited standalone mode, enabling it to broadcast 2.4-, 5-, and 6-GHz SSIDs and allowing wireless clients to join via an internal Dynamic Host Configuration Protocol (DHCP) pool. Site Survey mode provides all the control needed to configure and conduct a site survey. It lets users bring the AP into any environment with either a power source or battery backup and conduct a site survey test.

When the CW9178I is in Site Survey mode, you will be able to access the AP's WebUI for each configuration and view various RF metrics for RF coverage and planning. These configurations include channel number, channel width, Tx power, SSID, and data rates.



Configuration

Login

Username	admin
Password	•••••••••••••••

Radio

Radio Interface	5Ghz
Status	Enabled
Country	United States (US)
Power Type	PoE/Full power mode
802.11 n-mode	Enabled
802.11 ac-mode	Enabled
802.11 ax-mode	Enabled
Bandwidth	20 Mhz
Channel Selection	Auto
Tx-Power Level	1
Configured TxPower(dBm)	21 dBm

Data Rates

6 Mbps	Mandatory
9 Mbps	Supported
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

Figure 27. View RF Metrics for AP in Site Survey Mode

The steps below describe how to convert a CW9178I AP into Site Survey mode:

1. Change the AP to Site Survey mode. Enter command “ap site-survey”
2. After booting up, the AP is automatically assigned a static IP of 10.0.23.1.
3. The AP will start broadcasting the C9178_site_survey SSID with open/OWE security.
4. Connect your wireless client with the C9178_site_survey SSID and it will receive an IP from 10.0.23.0/24.
5. Access the AP’s Site Survey WebUI via 10.0.23.1.
6. The first time, the default username and password are admin/admin. You will be directed to reset that insecure password on the first login.
7. When done, convert your AP back to CAPWAP mode to join the controller again. Enter command “ap capwap”

Note:

1. If an AP is converted to Site Survey mode while connected to a WLC, it will disjoin and go into standalone mode.
2. For the above mentioned Site Survey functionality, the AP should have joined a Catalyst 9800 WLC atleast once. When the AP is in Day 0 mode, the CLI to convert the AP to Site Survey mode is not present.
3. The AP carries over the country code configured, while it was connected to the Catalyst 9800 WLC.

Antenna Patterns

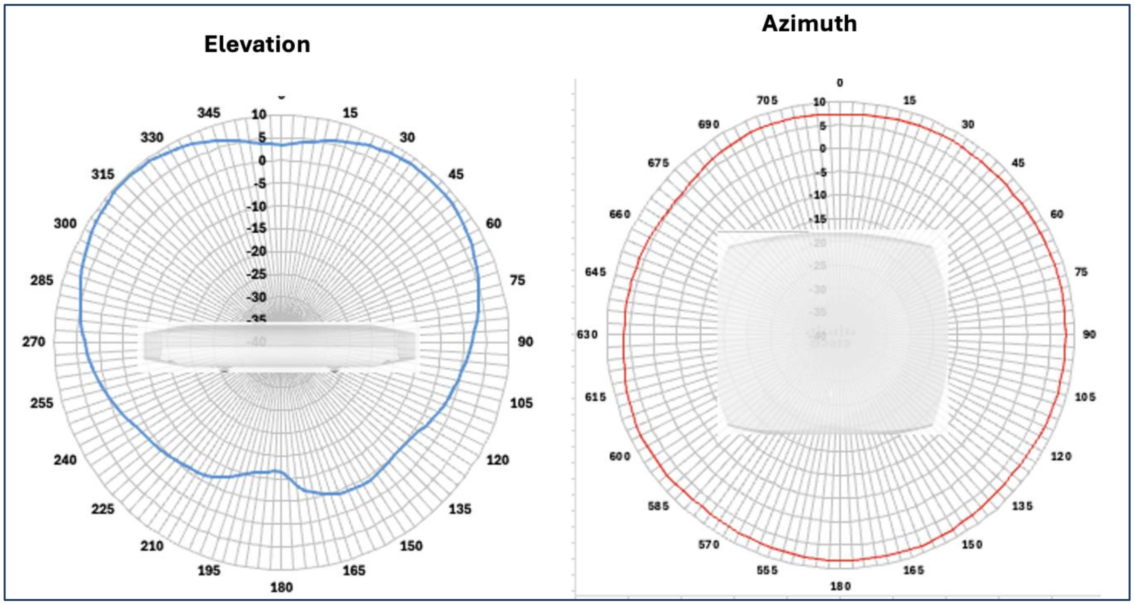


Figure 28. **Dual Band Radio (2.4 GHz) Antenna Patterns**

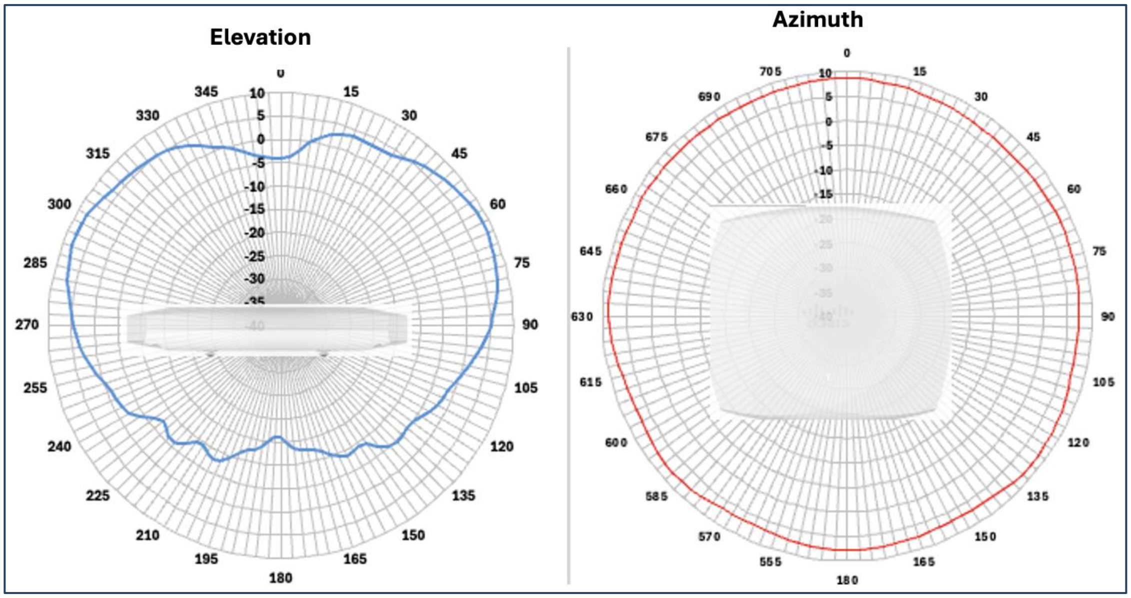


Figure 29. **Dual Band Radio (5 GHz) Antenna Patterns**

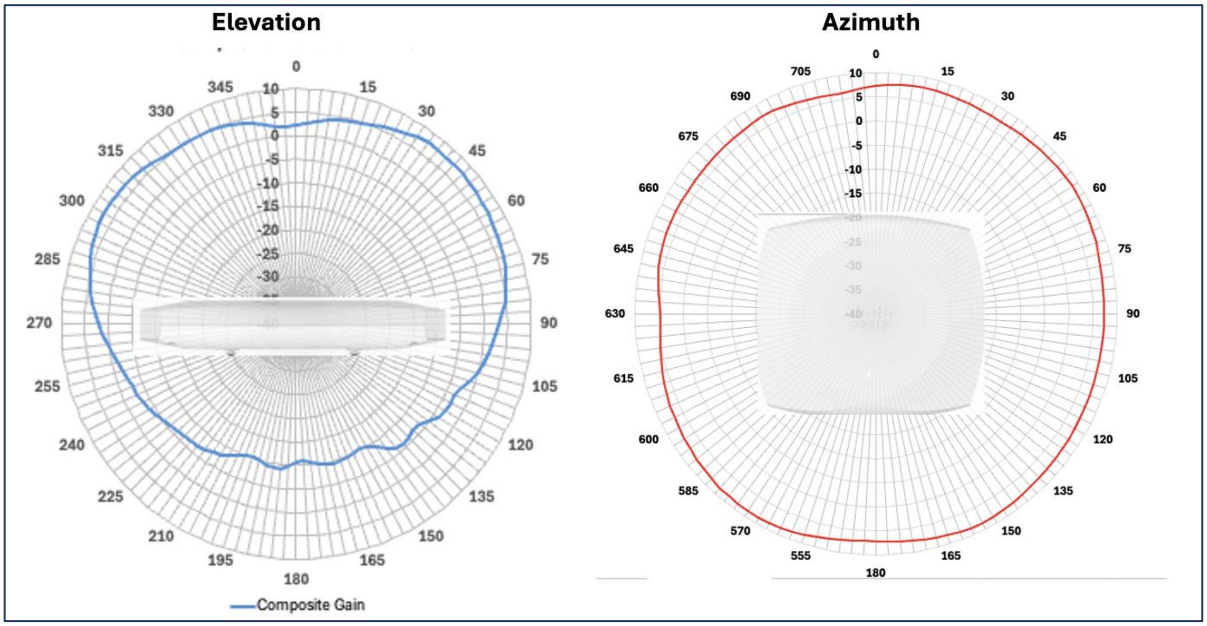


Figure 30. 5GHz Radio (Slot 2) Antenna Patterns

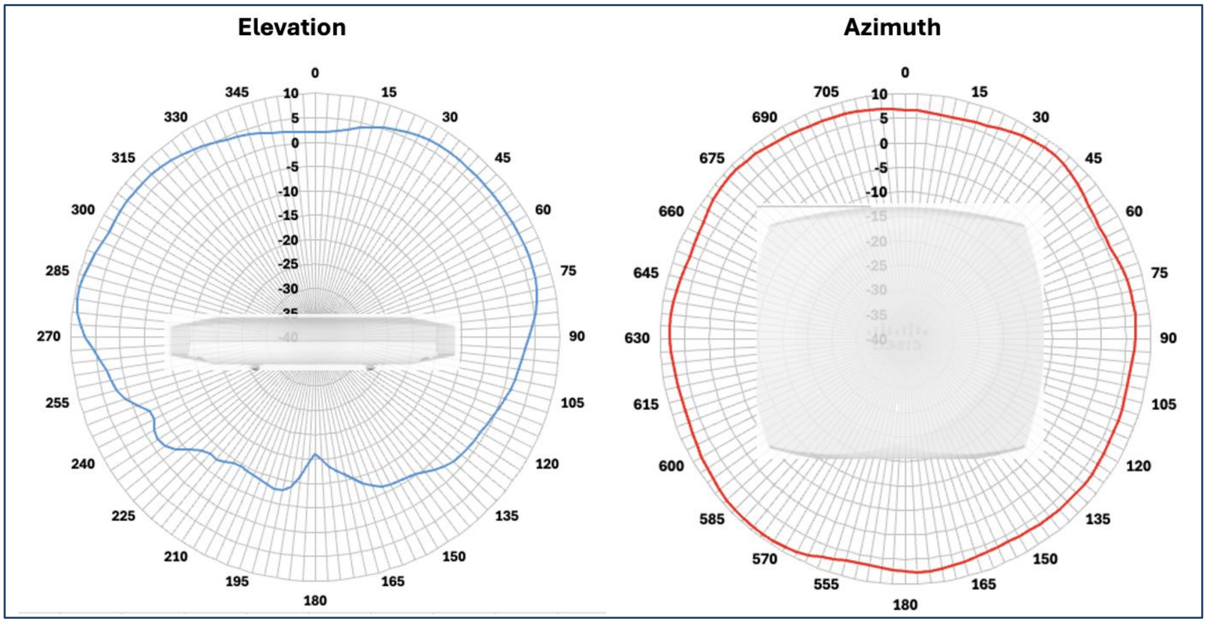


Figure 31. 6GHz Radio Antenna Patterns

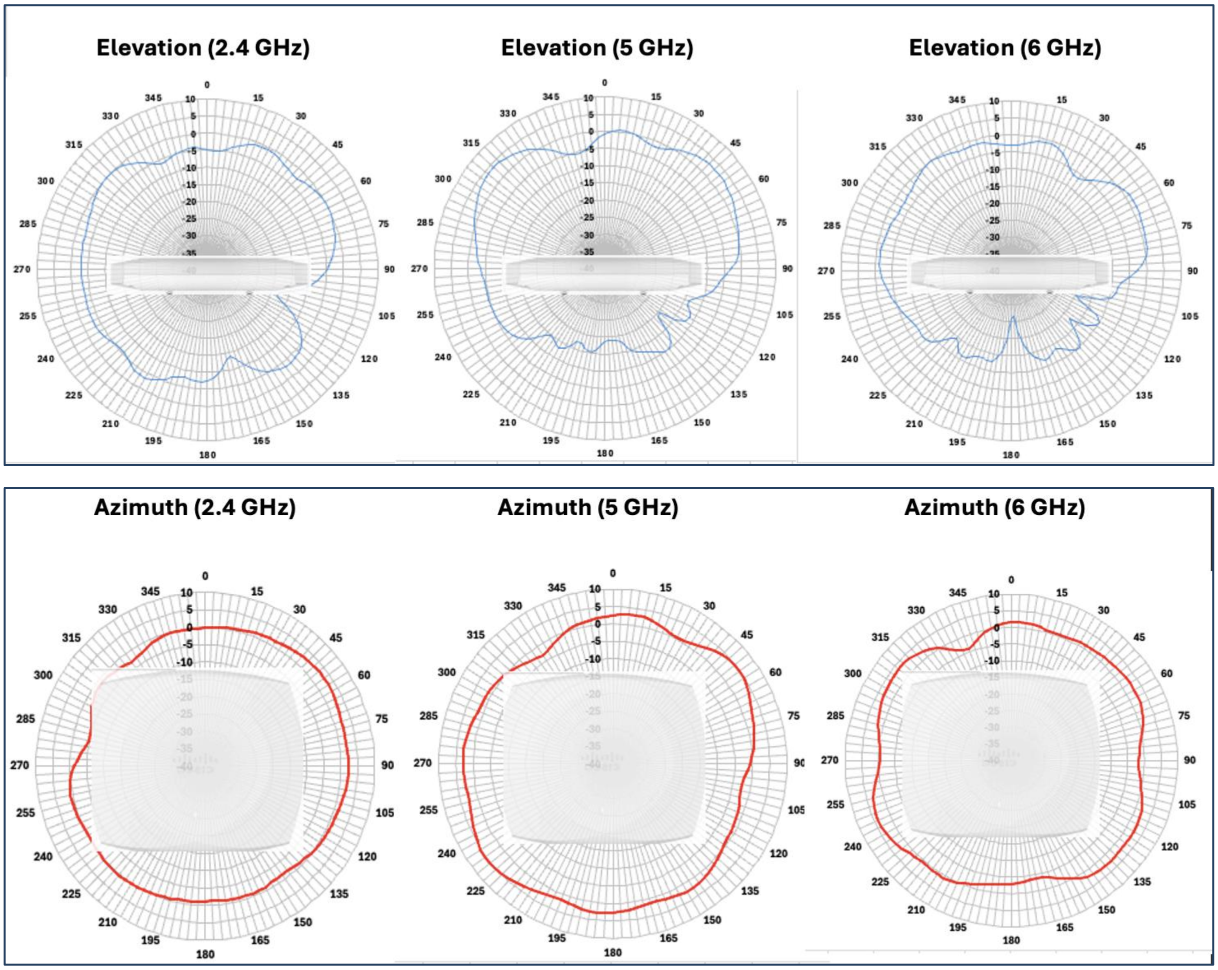


Figure 32. AI/ML-Driven Scanning Radio Antenna Patterns

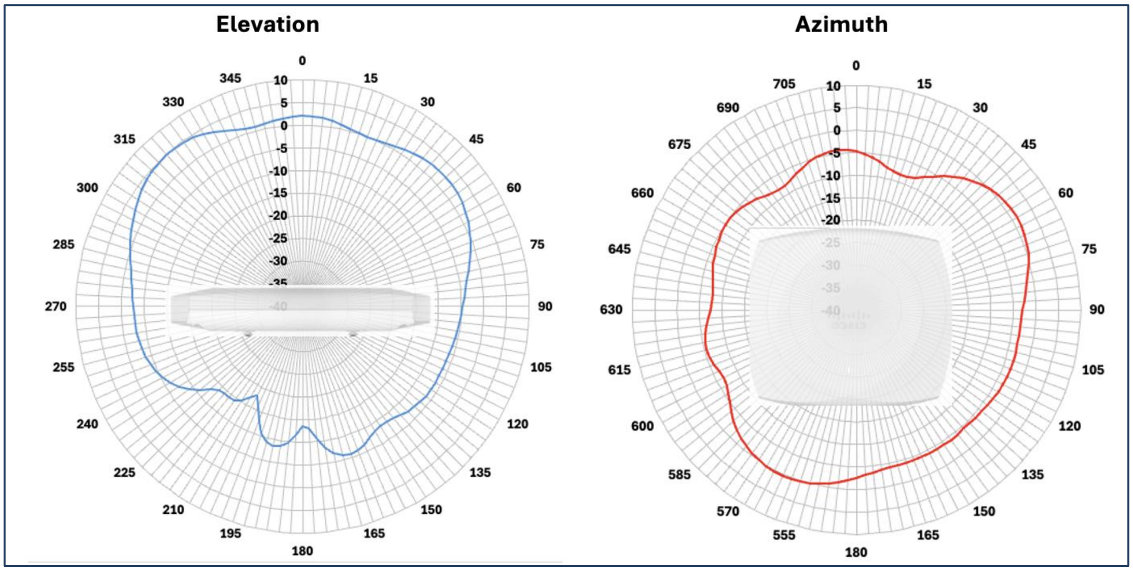


Figure 33. IoT Radio Antenna Patterns

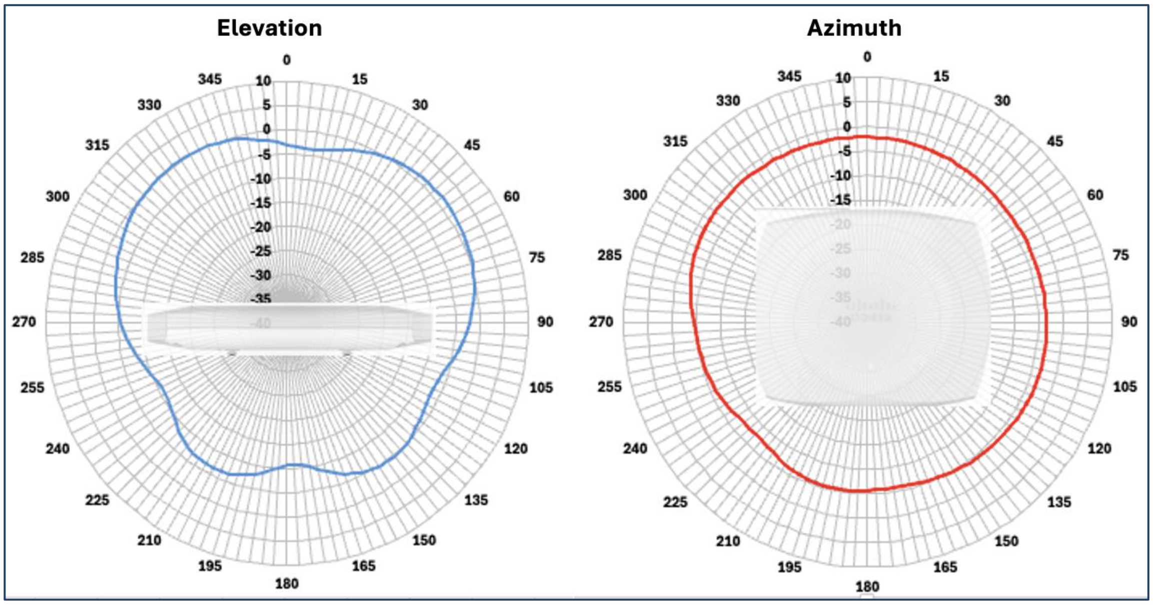


Figure 34. GNSS Antenna Patterns