

# Migrate to 6 GHz and Wi-Fi 7 with Cisco Wireless

## Contents

---

### [Introduction](#)

[CX Design Guide](#)

### [Why 6 GHz and Wi-Fi 7](#)

### [Base requirements for 6 GHz operations and Wi-Fi 7](#)

[6 GHz band requirements](#)

[Wi-Fi 7 requirements](#)

[IOS XE 17.15.3 and later 17.15.x versions](#)

### [Radio design considerations for 6 GHz coverage](#)

[Roaming behaviors between pre-Wi-Fi 6E/7 and Wi-Fi 6E/7 APs](#)

### [Enabling Wi-Fi 7 globally](#)

[Enabling Wi-Fi 7 globally on IOS XE](#)

[Enabling Wi-Fi 7 globally on Cisco Meraki Dashboard](#)

### [Use cases](#)

[802.1X / WPA3-Enterprise networks](#)

[WPA3-Enterprise configuration on IOS XE](#)

[WPA3-Enterprise configuration on the Cisco Meraki dashboard](#)

[Passphrase / WPA3-Personal / IoT networks](#)

[WPA3-SAE and WPA2-Personal configuration on IOS XE](#)

[WPA3-SAE configuration on the Cisco Meraki dashboard](#)

[Open / Enhanced Open / OWE / Guest networks](#)

[OWE configuration on IOS XE](#)

[OWE configuration on the Cisco Meraki dashboard](#)

### [Additional WPA3 and related options](#)

[Beacon protection](#)

[GCMP256](#)

### [Troubleshoot and verify](#)

### [References](#)

---

## Introduction

This document describes design and configuration guidelines to optimize the performance of Wi-Fi 7 and fully leverage the 6 GHz spectrum.

## CX Design Guide



# Design Guide

CX Design Guides are written by specialists from Cisco CX in collaboration with engineers from other departments and peer-reviewed by experts within Cisco; the guides are based on Cisco leading practices as well as knowledge and experience gained from countless customer implementations over many years. Networks designed and configured in line with the recommendations in this document help avoid common pitfalls and improve network operation.

## Why 6 GHz and Wi-Fi 7

The 6 GHz band became available for WLAN operations in 2020 and was required for Wi-Fi 6E certification. While Wi-Fi 6 operates in the 2.4 GHz and 5 GHz bands, Wi-Fi 6E utilises the same IEEE 802.11ax standard but extends its functionality to the 6 GHz band, provided specific requirements are met. The new Wi-Fi 7 certification is based on the IEEE 802.11be standard and supports operations in the 2.4 GHz, 5 GHz, and 6 GHz bands. Wi-Fi 7 also introduces new features and enhancements compared to previous certifications.

Supporting the 6 GHz band and/or Wi-Fi 7 comes with specific requirements, often necessitating new configurations and RF designs, especially when compared to the established practices for the 2.4 GHz and 5 GHz bands with Wi-Fi 6.

For instance, just as using outdated WEP security prevents the adoption of 802.11 standards beyond 802.11a/b/g, newer standards impose even stricter security prerequisites to encourage the deployment of more secure networks.

Conversely, the introduction of the 6 GHz band offers access to cleaner frequencies, improved performance, and support for new use cases. It also enables a more seamless implementation of existing applications, such as voice and video conferencing.

## Base requirements for 6 GHz operations and Wi-Fi 7

These are the security requirements written in the certifications for 6 GHz and Wi-Fi 7 operations.

### 6 GHz band requirements

The 6 GHz band only allows WPA3 or Enhanced Open WLANs, which means one of these security options:

- WPA3-Enterprise with 802.1X authentication
- WPA3 Simultaneous Authentication of Equals (SAE) (a.k.a. WPA3-Personal) with passphrase. SAE-FT (SAE with Fast Transition) is another possible AKM and is actually recommended for use since the SAE handshake is not trivial, and FT allows skipping that longer exchange.
- Enhanced Open with Opportunistic Wireless Encryption (OWE)

While, as per the [WPA3 v3.4](#) specifications (Section 11.2), Enhanced Open transition mode is not supported

with 6 GHz, a lot of vendors (including Cisco up to IOS® XE 17.18) do not enforce that yet. Therefore, it is technically possible to configure, for example, an Open SSID on 5 GHz, a corresponding Enhanced Open SSID on 5 and 6 GHz, both with Transition Mode enabled, and all of this without complying with the standards specifications. However, in such a scenario, it must be expected that we rather configure an Enhanced Open SSID without transition mode and available on 6 GHz only (clients supporting 6 GHz typically support Enhanced Open too), while keeping our regular Open SSID on 5 GHz, also without transition mode.

There are no new specific ciphers or algorithm requirements for WPA3-Enterprise, apart from 802.11w/Protected Management Frame (PMF) enforcement. Many vendors, including Cisco, consider 802.1X-SHA256 or "FT + 802.1X" (which actually is 802.1X with SHA256 and Fast Transition on top) only to be WPA3 compliant and plain 802.1X (which uses SHA1) is considered part of WPA2, therefore not fit/supported for 6 GHz.

## Wi-Fi 7 requirements

With the Wi-Fi 7 certification of the 802.11be standard, the Wi-Fi Alliance increased the security requirements. Some of them allow to use of the 802.11be data rates and protocol improvements, while some others are specific for supporting Multi-Link Operations (MLO), allowing compatible devices (clients and/or APs) to use multiple frequency bands while maintaining the same association.

In general, Wi-Fi 7 mandates one of these security types:

- WPA3-Enterprise with AES(CCMP128) and 802.1X-SHA256 or FT + 802.1X (which still uses SHA256, even if it is not explicit in its naming). This does not represent a change compared to previously existing WPA3 security prerequisites for the 6 GHz band.
- WPA3-Personal with GCMP256 and SAE-EXT-KEY and/or FT + SAE-EXT-KEY (AKM 24 or 25). Wi-Fi 6E mandates WPA3 SAE and/or FT + SAE with regular AES(CCMP128) and no additional extended key usages; this means that a new cipher was specifically introduced for Wi-Fi 7.
- Enhanced Open / OWE with GCMP256. While AES(CCMP128) can still be configured on the same SSID, clients using AES 128 do not support Wi-Fi 7. Before Wi-Fi 7, most clients supporting Enhanced Open were using AES 128 only, so this is a new, stronger requirement. As for 6 GHz support, no transition mode is allowed.

Regardless of the selected security type, Protected Management Frames (PMF) and Beacon Protection are required to support Wi-Fi 7 on the WLAN.

Because Wi-Fi 7 is still a recent certification at the time of this writing, with an as early as possible release, many vendors did not enforce all these security requirements from the beginning.

More recently, Cisco has been progressively enforcing the configuration options to be compliant with the Wi-Fi 7 certification. Here are the version-specific behaviors:

### IOS XE 17.15.3 and later 17.15.x versions

In this branch, all the WLANs are broadcasted as Wi-Fi 7 SSIDs, provided that Wi-Fi 7 is enabled globally and regardless of the security settings.

A client can associate as Wi-Fi 7 capable and achieve Wi-Fi 7 data rates regardless of the security method it uses, provided it's still supported by the WLAN. However, the client can only associate as MLO capable (on one or more bands) if it respects the strict requirements for Wi-Fi 7 security, or else it is rejected.

This could potentially cause issues when some early Wi-Fi 7 clients unable to support more secure ciphers, like GCMP256, try to associate as Wi-Fi 7 MLO capable to a WLAN, whose security settings do not match

the Wi-Fi 7 requirements. In such a situation, the client is rejected because of the invalid security settings (still allowed to be configured under the WLAN).

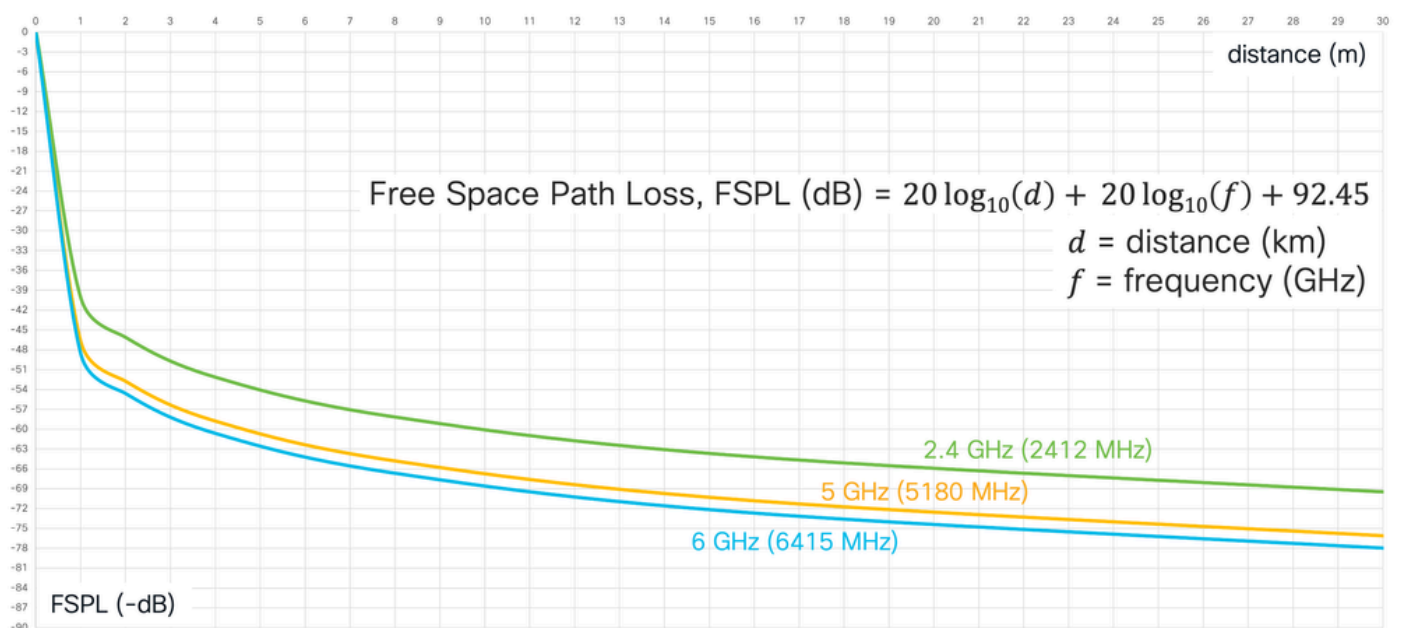
## Radio design considerations for 6 GHz coverage

Without meaning to become a full prescriptive guide on site surveys, this section briefly describes some base considerations when designing for 6 GHz coverage, especially if there is an already existing installation for 2.4/5 GHz that we would like to migrate to Wi-Fi 6E or 7.

As for any new Wi-Fi deployment we were used to on 2.4 and/or 5 GHz, a new wireless project on 6 GHz must include a corresponding dedicated 6 GHz site survey too.

When pre-Wi-Fi 6E/7 APs are already positioned for specific 5 GHz coverage and needs, in some cases, we can expect to be able to replace them with Wi-Fi 6E/7 capable APs and still obtain good coverage on 6 GHz. For this theory to work, our existing APs must already provide correct 5 GHz coverage for the intended needs (data only, voice, specific applications, and so on) while already being at least 3-4 transmit power levels under their maximum limit. APs typically have 7 to 8 power levels, and each power level divides the transmit power by half. This means a comfortable spot to be is when APs are using the medium of their allowed transmit power range.

According to free space loss calculations, 6 GHz signals are attenuated by 2 dB more than 5 GHz ones. On top of that, 6 GHz signals can also be more impacted by obstacles than their 5 GHz equivalents.



When a Cisco AP increases/decreases its transmit power by one level, it does so by a “jump” of 3 dB. An AP going from a power level of 4, with a transmit power of 11 dBm for example, to a power level of 3, increases its transmit power to 14 dBm (11 dBm for power level 4 and 14 dBm for power level 3 are just a generic example, as different models/generations of APs could have slightly different transmit power values in dBm for the same power level number).



Assuming similar antenna gains/patterns and the same transmit power level, the 6 GHz radio is expected to cover slightly less than the 5 GHz radio.

The overall 6 GHz coverage throughout multiple APs could be more comparable, especially if those APs are already dense enough for good 5 GHz coverage.

If a pre-Wi-Fi 6E/7 AP already provides good coverage at 5 GHz on power level 4, for instance, a newer Wi-Fi 6E/7 AP with similar 5 GHz radio patterns could replace that former AP without any significant impact on the existing 5 GHz network.

Also, the 6 GHz radio of the new Wi-Fi 6E/7 AP could provide similar 6 GHz coverage to the 5 GHz one just by being at one transmit power level (so 3 dB) higher.

If 5 GHz is already correctly covered with the AP's 5 GHz radio at 3-4 power levels under its maximum, the corresponding 6 GHz radio could hence be set at 2-3 power levels under its maximum for comparable coverage.

Also, if the 6 GHz radio already provides correct coverage at 2-3 power levels lower than its maximum, it could still exceptionally go even a couple of levels higher, for example to try working around temporary unexpected coverage holes (a neighbor AP's failure, unannounced obstacles, new RF needs and so on).

## Roaming behaviors between pre-Wi-Fi 6E/7 and Wi-Fi 6E/7 APs

Deploying APs supporting different standards and/or frequency bands in the same coverage area has always not been a recommended practice, especially if those different generations of APs are installed in a "salt and pepper" fashion (that is, mixed in the same zone).

While a wireless controller could handle operations (for example, dynamic channel assignment, transmit power control, PMK cache distribution, and so on) from a group of several AP models, clients moving between different standards and even different frequency bands are not always able to handle that properly and they could likely run into roaming issues for example.

On top of that, because of the newer standards, Wi-Fi 6E/7 APs support GCMP256 ciphers for WPA3. The same could however not always be true for some Wi-Fi 6 APs and earlier models. For passphrase/WPA3-Personal and Enhanced Open/OWE SSIDs, requiring the configuration of both AES(CCMP128) and GCMP256 ciphers, certain Wi-Fi 6 (like the 9105, 9115 and 9120 series) do not support GCMP256 and can offer AES(CCMP128) ciphers only to associating clients, including Wi-Fi 6E/7 capable ones. If these Wi-Fi 6E/7 clients needed to roam from/to neighboring Wi-Fi 6E/7 APs supporting GCMP256, they would have to go through a brand-new association, as renegotiating ciphers between AES(CCMP128) and GCMP256 is not supported for transparent roaming. Moreover, in general, it is not optimal to have APs offering different capabilities in the same area: this deployment does not allow clients to use these capabilities reliably while

moving and may lead to stickiness or disconnections.

While this scenario must represent a corner case, we want to still keep in mind that, with GCMP256 ciphers configured under the WLAN, roaming of Wi-Fi 6E/7 clients between 9105/9115/9120 APs and 9130/9124/916x/917x APs can not be possible, as these latter series support GCMP256 and the former does not.

Channel widths of 40 MHz or more on 6 GHz can also cause stickiness for 6 GHz-capable clients, who can refuse to re-associate to other bands. This must be one more reason not to mix 6 GHz-capable APs and non-6 GHz-capable APs in the same roaming area.

## Enabling Wi-Fi 7 globally

### Enabling Wi-Fi 7 globally on IOS XE

When installing or upgrading to an IOS XE version supporting Wi-Fi 7, by default, support for Wi-Fi 7 is globally disabled.

To activate it, we need to navigate under the High Throughput configuration menu of each 2.4/5/6 GHz band and check the box to enable 11be.

Configuration > Radio Configurations > High Throughput

6 GHz Band 5 GHz Band 2.4 GHz Band

⚠ 6 GHz Network is operational. Configuring High Throughput will result in loss of connectivity of clients. [Apply](#)

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

> 11ax

▼ 11be

⚠ 11be check enables Wi-Fi 7 capability in Wi-Fi 7 capable APs. Please ensure the WLANs are compatible with Wi-Fi 7 specific security. [Click here](#) to view the security constraints.

Enable 11be ☒ Select All ☒

SS/MCS	SS/MCS	SS/MCS	SS/MCS
<input checked="" type="checkbox"/> 1/9	<input checked="" type="checkbox"/> 1/11	<input checked="" type="checkbox"/> 1/13	<input checked="" type="checkbox"/> 1/14
<input checked="" type="checkbox"/> 1/15	<input checked="" type="checkbox"/> 2/9	<input checked="" type="checkbox"/> 2/11	<input checked="" type="checkbox"/> 2/13
<input checked="" type="checkbox"/> 3/9	<input checked="" type="checkbox"/> 3/11	<input checked="" type="checkbox"/> 3/13	<input checked="" type="checkbox"/> 4/9
<input checked="" type="checkbox"/> 4/11	<input checked="" type="checkbox"/> 4/13		

Another option could also be to run these three command lines via SSH/console, in terminal configuration mode:

```
ap dot11 24ghz dot11be
ap dot11 5ghz dot11be
ap dot11 6ghz dot11be
```

As mentioned in the warning note, when trying to modify these settings, changing the status of 802.11be support results in a brief loss of connectivity for all clients across radios of Wi-Fi 7 APs. If you want to do MLO, which means clients connecting to several bands at the same time, you need to enable 11be on all the bands you want the client to connect to. It is not necessary to enable all the bands, but recommended simply for performance.

## Enabling Wi-Fi 7 globally on Cisco Meraki Dashboard

When adding Wi-Fi 7-capable APs (for example CW9178I, CW9176I/D1) to a Cisco Meraki Dashboard network for the first time, support for 802.11be operation is on their default RF Profile.

To activate it, we need to navigate under **Wireless > Radio Settings**, click on the **RF Profile** tab and select the profile assigned to the AP (default: 'Basic Indoor Profile' for indoor APs).

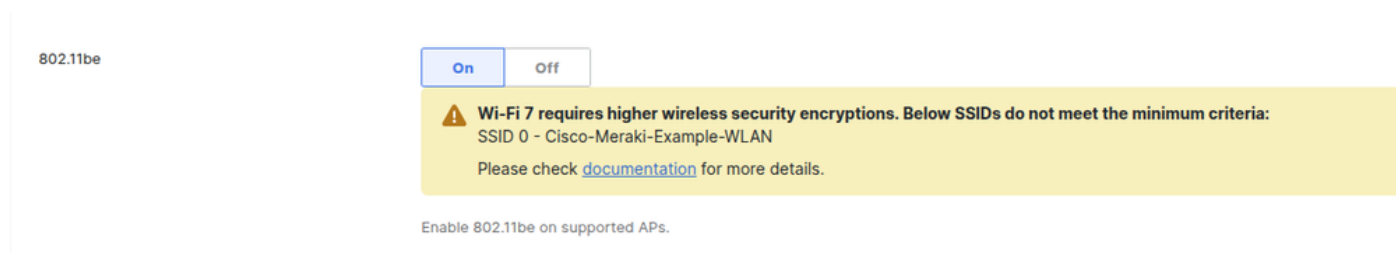
In the **General** section, enable **802.11be** (on) as shown in this screenshot:



If one or more WLANs are configured with security settings weaker than those required by the Wi-Fi 7 specification, the Dashboard displays a banner alerting users as shown hereafter.

While the Dashboard allows the configuration to be saved, Wi-Fi 7 is not enabled on the flagged SSIDs until compliance with the Wi-Fi 7 requirements is ensured.

As of this writing, all WLANs enabled in the network must meet the Wi-Fi 7 specification requirements to be enabled on firmware version MR 31.1.x and later (this behaviour changes in a future version of firmware MR 32.1.x).



Once the configuration of the SSID meets the Wi-Fi 7 minimum criteria, the banner disappears.

In the same RF Profile, make sure to enable 6 GHz operation on the APs.

This can be done either for all the SSIDs in bulk or per individual SSID.

Note that Band Steering is available only between 2.4 and 5 GHz.

Example of 6 GHz enablement for all the SSIDs.



## General

Band selection

All SSIDs

Per SSID

☒ Enable operation on 2.4 GHz band

SSID will be broadcast on 2.4 GHz. This band does not support 802.11a devices.

☒ Enable operation on 5 GHz band

SSID will be broadcast on 5 GHz. This band does not support 802.11b/g devices.

☒ Enable operation on 6 GHz band

SSID will be broadcast on 6 GHz.

☐ Enable band steering

Attempt to steer clients from 2.4 GHz to 5 GHz.

Example of 6 GHz enablement for a single SSID.

## General

Band selection

All SSIDs

Per SSID

Name	2.4 GHz	5 GHz	6 GHz	Band steering ⓘ
meraki-wpa3-ent-transition	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[Show disabled SSIDs](#)

## Use cases

### 802.1X / WPA3-Enterprise networks

#### WPA3-Enterprise configuration on IOS XE

Enterprise WLANs based on WPA2/3 with 802.1X authentication are the easiest to migrate to 6 GHz and/or Wi-Fi 7.

Enabling your 802.1X SSID for 6 GHz only requires enabling PMF support, even as optional, as well as 802.1X-SHA256 and/or FT + 802.1X AKMs, both of which are WPA3 compliant.

We can keep offering WPA2 with standard 802.1X (SHA1) on the same WLAN. Wi-Fi 7 support requires enabling Beacon Protection and setting PMF as required rather than optional; WPA2 802.1X (SHA1) can stay present on the WLAN as a backwards compatibility option. This means you can have all your corporate devices under a single SSID, provided they support 802.11w/PMF, which is quite common on current



wireless NICs for laptops and other mobile endpoints.

From a typical WPA2 SSID with these L2 security settings:

<input type="radio"/> WPA + WPA2		<input checked="" type="radio"/> WPA2 + WPA3	<input type="radio"/> WPA3	<input type="radio"/> Static WEP	<input type="radio"/> None
MAC Filtering <input type="checkbox"/>					
Lobby Admin Access <input type="checkbox"/>					
<b>WPA Parameters</b>					
WPA Policy <input type="checkbox"/>	<input checked="" type="checkbox"/> WPA2 Policy				
GTK Randomize <input type="checkbox"/>	WPA3 Policy <input type="checkbox"/>				
<b>WPA2/WPA3 Encryption</b>					
<input checked="" type="checkbox"/> AES(CCMP128)	CCMP256 <input type="checkbox"/>				
GCMP128 <input type="checkbox"/>	GCMP256 <input type="checkbox"/>				
<b>Protected Management Frame</b>					
PMF	Optional				
Association Comeback Timer*	1				
SA Query Time*	200				
<b>Fast Transition</b>					
Status		Enabled			
Over the DS		<input type="checkbox"/>			
Reassociation Timeout *		20			
<b>Auth Key Mgmt (AKM)</b>					
<input checked="" type="checkbox"/> 802.1X	<input checked="" type="checkbox"/> FT + 802.1X				
802.1X-SHA256 <input type="checkbox"/>	CCKM ⚠ <input type="checkbox"/>				
PSK <input type="checkbox"/>	FT + PSK <input type="checkbox"/>				
PSK-SHA256 <input type="checkbox"/>	Easy-PSK <input type="checkbox"/>				
<b>MPSK Configuration</b>					
Enable MPSK		<input type="checkbox"/>			

We can migrate the configuration for WPA3, 6 GHz and Wi-Fi 7 support as shown here:

☐ 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 <input checked="" type="checkbox"/>	FT + 802.1X <input checked="" type="checkbox"/>
802.1X-SHA256 <input checked="" type="checkbox"/>	CCKM <input type="checkbox"/>
PSK <input type="checkbox"/>	FT + PSK <input type="checkbox"/>
PSK-SHA256 <input type="checkbox"/>	SAE <input type="checkbox"/>
FT + SAE <input type="checkbox"/>	SAE-EXT-KEY <input type="checkbox"/>
FT + SAE-EXT-KEY <input type="checkbox"/>	

## WPA3-Enterprise configuration on the Cisco Meraki dashboard

At the time of this writing, WPA3-Enterprise operation is available only with an external RADIUS server (aka "my RADIUS server").

WPA3-Enterprise is not available with Meraki Cloud Authentication.

## Security WPA3 Enterprise with 1 RADIUS server

☐ Open (no encryption)  
Any user can associate

☐ 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  
my RADIUS server ▾  
User credentials are validated with 802.1X at association time

☐ Identity-based access control with RADIUS

Starting with MR 31.x, the WPA types are:

- 'WPA3 only', which uses the same ciphers as WPA2, but requires 802.11w (PMF).
- 'WPA3 192-bit', which allows only the EAP-TLS method with chipers TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, or TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384. This mode requires configuring the same chipers on the RADIUS server to enable this mode.
- 'WPA3 Transition Mode' (aka mixed mode), which allows the coexistence of WPA2 clients on the same WLAN used for WPA3.

### WPA encryption ⓘ

802.11r ⓘ

802.11w ⓘ

WPA3 only ▾

WPA2 only

WPA1 and WPA2

**WPA3 only**

WPA3 192-bit Security

WPA3 Transition Mode

clients)

1 clients)

When using 'WPA3 only' or 'WPA3 192-bit Security', PMF is mandatory for all clients.

In most applications, FT (802.11r), while not mandatory, must better be enabled to mitigate the impact of roaming and re-authentication latency while using an external RADIUS server.

6 GHz operation requires enabling PMF (802.11w).

WPA encryption ⓘ WPA3 only ▾

802.11r ⓘ ☒ Enabled

☐ Adaptive

☐ Disabled

802.11w ⓘ ☐ Enabled (allow unsupported clients)

☒ Required (reject unsupported clients)

☐ Disabled (never use)

When selecting WPA3 Transition Mode, all the clients capable of using WPA3 default to using PMF. All the clients operating on 6 GHz use WPA3.

In this mode, you can select if the legacy client using WPA2 must use PMF (802.11w *required*) or if that feature is optional (802.11w *enabled*).

WPA encryption ⓘ WPA3 Transition Mode ▾

802.11r ⓘ ☒ Enabled

☐ Adaptive

☐ Disabled

802.11w ⓘ ☒ Enabled (allow unsupported clients)

☐ Required (reject unsupported clients)

☐ Disabled (never use)

Regardless of the WPA3 selection, Cisco Meraki APs require the GCMP 256 cipher suite to be enabled to operate in Wi-Fi 7 mode.

Furthermore, Beacon Protection is enabled by default on 2.4, 5, and 6 GHz when the APs are operating in Wi-Fi 7 mode.

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.

## Passphrase / WPA3-Personal / IoT networks



Enabling a passphrase SSID for 6 GHz, up to Wi-Fi 6E support, is simple and requires SAE and/or FT + SAE, along with other WPA2 PSK AKMs if needed. However, for Wi-Fi 7 support, the certification mandates adding SAE-EXT-KEY and/or FT + SAE-EXT-KEY AKMs, along with GCMP256 cipher. It is therefore not possible to have a passphrase-based WLAN with both maximum compatibility for older clients and Wi-Fi 7 performance.

In such cases, we can configure a dedicated WPA3-only SSID with SAE, FT + SAE, SAE-EXT-KEY and FT + SAE-EXT-KEY, offering both AES(CCMP128) and GCMP256 ciphers, for more recent Wi-Fi 6E and Wi-Fi 7 clients.

It is possible to have a transition mode WLAN that allows for WPA2 PSK, on top of WPA3 SAE and SAE-EXT, but this represents 6 AKMs (If FT is used) and some rigit clients could potentially have a problem with that. We recommend you test this possibility with your clients if you decide to go for transition mode WPA2-PSK+WPA3-SAE+SAE-EXT + FT.

In all these scenarios, we strongly recommend enabling FT when using SAE. The SAE frame exchange is costly in terms of resources and longer than the WPA2 PSK 4-way handshake.

Some device manufacturers like Apple expect to use SAE only when FT is enabled and can refuse to connect if not available.

### WPA3-SAE and WPA2-Personal configuration on IOS XE

<input type="radio"/> WPA + WPA2		<input type="radio"/> WPA2 + WPA3	<input checked="" type="radio"/> WPA3	<input type="radio"/> Static WEP	<input type="radio"/> None
----------------------------------	--	-----------------------------------	---------------------------------------	----------------------------------	----------------------------

MAC Filtering ☐

Lobby Admin Access ☐

WPA Parameters

WPA Policy ☐

WPA2 Policy ☐

GTK Randomize ☐

Transition Disable ☐

WPA3 Policy ☒

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)

FT + 802.1X ☐

802.1X-SHA256 ☐

SUITEB192-1X ☐

OWE ☐

SAE ☒

FT + SAE ☒

SAE-EXT-KEY ☒

FT + SAE-EXT-KEY ☒

Anti Clogging Threshold\*  1500

Max Retries\*  5

Retransmit Timeout\*  400



**Note:** If (FT +) SAE is enabled on the WLAN and a Wi-Fi 7 client tries to associate with it instead of (FT +) SAE-EXT-KEY, it is rejected. As long as (FT +) SAE-EXT-KEY is enabled too, Wi-Fi 7 clients must anyway use this latter AKM, and this issue must not happen.

---

Although using a legacy WLAN with only PSK on top of a WPA-3 only WLAN increases the amount of total SSIDs, it allows to keep maximum compatibility on one SSID, where we can also potentially disable other advanced features that could impact compatibility and which could be helpful for many IoT scenarios, while offering maximum features and performances to more recent devices through the other SSID. This can be a preferred scenario if you have older or more sensitive IoT devices in the picture. If you don't have IoT devices, going for a single transition mode WLAN can be more efficient as you only advertise one SSID.

### **WPA3-SAE configuration on the Cisco Meraki dashboard**

## Security WPA3 SAE configured

☐ Open (no encryption)  
Any user can associate

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

☒ Password  
Users must enter this key to associate: ⓘ

☐ MAC-based access control (no encryption)

Up to firmware MR 30.x, the only supported WPA type is 'WPA3 only', and the dashboard does not let you select a different method.

PMF is mandatory in this configuration, while FT (802.11r) is recommended to be enabled when using SAE.

WPA encryption ⓘ

WPA3 only ▼

802.11r ⓘ

☒ Enabled

☐ Adaptive

☐ Disabled

802.11w ⓘ

☐ Enabled (allow unsupported clients)

☒ Required (reject unsupported clients)

☐ Disabled (never use)

To allow Wi-Fi 7 operation, the GCMP 256 cipher suite and SAE-EXT AKM suite must be enabled upon configuration of the SSID.

They are disabled by default, and can be enabled under 'Advanced WPA3 settings.'

### 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.

As of this writing, all WLANs enabled in the network must meet the Wi-Fi 7 specification requirements to be enabled on firmware version MR 31.1.x and later.

This means that a Wi-Fi 7 SSID configured as described previously cannot coexist with another SSID using WPA2-Personal or WPA3-SAE Transition Mode.



If a WPA2-Personal SSID is configured in the dashboard network, all the Wi-Fi 7 APs would revert to Wi-Fi 6E operation.

This behaviour changes in a future version of firmware MR 32.1.x.

## **Open / Enhanced Open / OWE / Guest networks**

Guest networks come with many flavors. Typically, they require no 802.1X credentials or passphrase to connect, and possibly imply a splash page or portal, which can require credentials or a code. This is traditionally handled with an Open SSID and either local or external guest portal solutions. However, SSIDs with open security (no encryption) are not allowed on 6 GHz or for Wi-Fi 7 support.

A first very conservative approach would be to dedicate guest networks to the 5 GHz band and Wi-Fi 6 at best. This leaves the 6 GHz band reserved for corporate devices, solves the complexity problem and brings maximum compatibility, although not up to Wi-Fi 6E/7 performances.

If, on one side Enhanced Open is a great security method offering privacy while keeping the “open” experience (end users do not need to enter any 802.1X credentials or passphrase), to this day it still has limited support among endpoints. Some clients still do not support it and, even when they do, this technique is not always handled smoothly (the device can show the connection as unsecured, while it actually is secure, or it can display it as passphrase protected, even if no passphrase is needed with OWE). A guest network being expected to work on all guest uncontrolled devices, it can be too early to provide just an Enhanced Open SSID and it is recommended to provide both options through separate SSIDs: an open one on 5 GHz and an OWE enabled one on 5 and 6 GHz, both with the same captive portal behind if this is a requirement too. Transition Mode is not supported on Wi-Fi 6E, 6 GHz (even though it could still be allowed on software) or Wi-Fi 7, so that is not an advised solution. All the portal redirection techniques (web authentication internal or external, Central Web Authentication, ...) are still supported with OWE.

## **OWE configuration on IOS XE**

If we wanted to provide 6 GHz service to guests, the recommendation would be to create a separate SSID with Enhanced Open / OWE (Opportunistic Wireless Encryption). It could offer both AES(CCMP128) cipher, for maximum compatibility up to Wi-Fi 6E clients, as well as GCMP256 bits for Wi-Fi 7 capable clients.

☐ WPA + WPA2
 ☐ WPA2 + WPA3
 ☒ WPA3
 ☐ Static WEP
 ☐ None

MAC Filtering ☐
 Needed if using CWA or other web portal techniques requiring MAC filtering

Lobby Admin Access ☐

**WPA Parameters**

WPA Policy ☐
 WPA2 Policy ☐
 WPA3 Policy ☒
 Beacon Protection ☒

GTK Randomize ☐

Transition Disable ☐

**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 ☐
 OWE ☒

SUITEB192-1X ☐

SAE ☐
 FT + SAE ☐

SAE-EXT-KEY ☐
 FT + SAE-EXT-KEY ☐

Transition Mode WLAN ID  0-4096

## OWE configuration on the Cisco Meraki dashboard

Similar to what was done on IOS XE, the recommendation is to create a separate Guest SSID with Enhanced Open / OWE operating on 6 GHz on the Cisco Meraki dashboard.

This can be configured again in **Wireless > Access Control**, and selecting 'Opportunistic Wireless Encryption (OWE)' as the Security method.

Security *Opportunistic Wireless Encryption*

☐ Open (no encryption)  
Any user can associate

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

☐ Password  
Users must enter a passphrase to associate ⓘ

When running firmware up to MR 31, the only supported WPA type is 'WPA3 only', and the dashboard does not let you select a different method.

PMF is mandatory in this configuration, while FT (802.11r) cannot be enabled.

Note that the labelling 'WPA3 only' is overloaded as OWE is not part of the WPA3 standard; however, this configuration refers to OWE without Transition Mode.

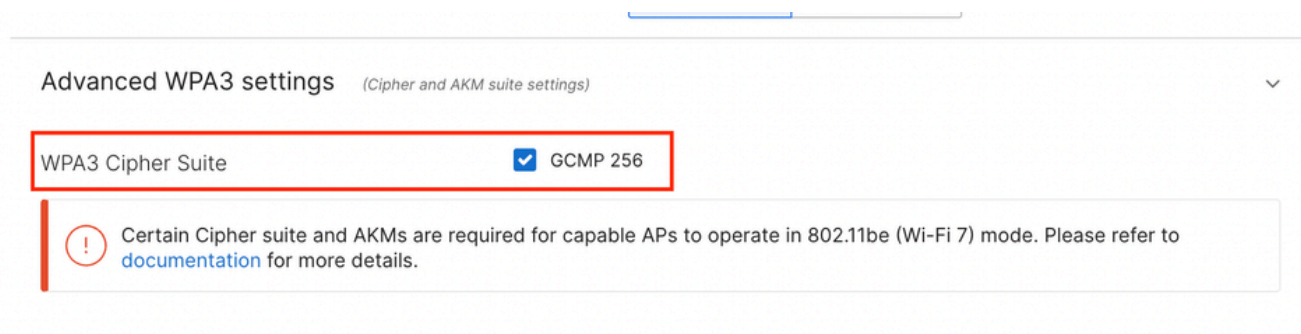
OWE Transition Mode is made available as part of a future release of MR 32.1.x.



A screenshot of a network configuration interface. At the top, a red rectangular box highlights the 'WPA encryption' section, which includes a dropdown menu currently set to 'WPA3 only'. Below this, there are two main sections: '802.11r' and '802.11w'. The '802.11r' section has three radio button options: 'Enabled', 'Adaptive', and 'Disabled', with 'Disabled' being selected. The '802.11w' section has three radio button options: 'Enabled (allow unsupported clients)', 'Required (reject unsupported clients)', and 'Disabled (never use)', with 'Required (reject unsupported clients)' being selected.

The AES(CCMP128) cipher is enabled by default for maximum compatibility up to Wi-Fi 6E clients.

GCMP256 bits can be enabled alongside CCMP128 for compliance with Wi-Fi 7 requirements.



A screenshot of the 'Advanced WPA3 settings' section in a network configuration interface. The section title is 'Advanced WPA3 settings' with a subtitle '(Cipher and AKM suite settings)'. Below the title, there is a red rectangular box highlighting the 'WPA3 Cipher Suite' section, which includes a checkbox labeled 'GCMP 256' that is checked. Below this, there is a warning message with a red exclamation mark icon: '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.'

## Additional WPA3 and related options

While WPA3 options are best described and covered in the WPA3 deployment guide, this section covers some additional recommendations for WPA3 specifically related to 6 GHz and Wi-Fi 7 support.

### Beacon protection

This is a feature that solves the vulnerability, where a malicious attacker can transmit beacons instead of the legitimate access point, while modifying some fields to change security or other settings of already associated clients. Beacon protection is an extra information element (Management MIC) in the beacon acting as a signature for the beacon itself, to prove that it was sent by the legitimate access point and that it has not been tampered with. Only associated clients with a WPA3 encryption key can verify the legitimacy of the beacon; probing clients have no means to verify it. The additional information element in the beacon must simply be ignored by clients not supporting it (this refers to non-Wi-Fi 7 clients), and it does not normally cause compatibility issues (unless with a poorly programmed client driver).

This screenshot shows an example of the content of the Management MIC Information Element:

```
✓ Tag: Management MIC
  Tag Number: Management MIC (76)
  Tag length: 16
  KeyID: 6
  IPN: 350200000000
  MIC: c0105301ca902ff1
```

## GCMP256

Until the Wi-Fi 7 certification, most clients implemented AES(CCMP128) cipher encryption. CCMP256 and GCMP256 are very specific variants related to SUITE-B 802.1X AKM. Although some first generations of Wi-Fi 7 clients on the market claim Wi-Fi 7 support, they sometimes still do not implement GCMP256 encryption, which can become an issue if Wi-Fi 7 APs enforcing the standard as expected prevent these clients from connecting without proper GCMP256 support.

When GCMP256 is enabled, the Robust Security Network Element (RSNE) in the Beacon Frames for the WLAN advertises the capability in the Pairwise Cipher Suite List as shown here.

```
Pairwise Cipher Suite Count: 2
✓ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) GCMP (256) 00:0f:ac (Ieee 802.11) AES (CCM)
  ✓ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
    Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Pairwise Cipher Suite type: GCMP (256) (9)
  ✓ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Pairwise Cipher Suite type: AES (CCM) (4)
```

## Troubleshoot and verify

The Wireless Configuration Analyzer Express latest version (<https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer-express-gui/>) has a Wi-Fi 7 readiness check that evaluates your 9800 configuration for all the Wi-Fi 7 requirements mentioned previously.

If you still have doubts whether your configuration is Wi-Fi 7 ready, the WCAE lets you know what is wrong.

WLANs + Policies In Use									
WLAN Name	SSID	WLAN Status	Policy Name	Policy Status	VLAN	WLAN Active Clients	Radio Policy	Security Policies	WiFi-7
open	open	Disabled	home	Enabled	home	0	Radio Band: All Radio Operation: 2.4GHz 5GHz	6GHz Disabled	Not Compatible
open	open	Disabled	io1	Enabled	io1	0	Radio Band: All Radio Operation: 2.4GHz 5GHz	6GHz Disabled	Not Compatible
owe	owe	Disabled	Not in use on any valid Tag			0	Radio Band: All Radio Operation: All	WPA3 AES Auth: OWE PMF: Required * Security 6GHz * WPA3 aes Auth: OWE PMF: Required	Valid AKM, Missing GCMP256
wep	wep	Disabled	Not in use on any valid Tag			0	Radio Band: All Radio Operation: 2.4GHz 5GHz	Static WEP 6GHz Disabled	Not Compatible
wpa2_ft	wpa2_ft	Disabled	Not in use on any valid Tag			0	Radio Band: All Radio Operation: 2.4GHz 5GHz	WPA2 AES Auth: 802.1x FT-802.1x OKC PMF: Disabled	Not Compatible

## References

1. [Cisco Systems. “WPA3 Encryption and Configuration Guide.”](#)
2. [Meraki WPA3 guide](#)