White Paper

WPA3 Support

Cisco Catalyst 9800 Series Wireless Controllers Cisco IOS XE Release 16.12

Cisco Unified Wireless Network Controllers AireOS Release 8.10

Last updated: July 2019

Contents

WPA3 preface

The Wi-Fi Alliance has recently announced a new certification in wireless, called Wi-Fi CERTIFIED WPA3. WPA3 is designed to succeed the somewhat dated and widely used WPA2 and bring a number of key enhancements to improve security protections and onboarding procedures across personal, public, government, financial, and enterprise networks.

WPA, which stands for Wi-Fi Protected Access, defines the security and authentication methods that wireless access points and Wi-Fi client devices use to perform the “handshake” they need to connect securely and communicate using strong encryption. This encryption ensures that a wireless access point and a Wi-Fi client (such as a laptop, smartphone, or IoT wireless device) can communicate wirelessly without the traffic being snooped on or compromised in any way.

From the beginning, and even before the creation of the Wi-Fi Alliance, Cisco was a front runner in wireless security in all of its wireless controllers and access points. Cisco fully complies with all Wi-Fi Alliance security requirements and certifications and in many cases goes beyond those industry standard requirements. This compliance and other Cisco security innovations have enabled individuals and businesses to increase the protection of information moving across wireless networks through the WPA2 and upcoming WPA3 family. The security features of WPA constantly evolve to include stronger protections and new security practices as the security landscape changes. The original WPA standard was released back in 2003 to replace Wired Equivalent Privacy (WEP), and WPA2 came the following year. WPA3 is a long-awaited and much-welcomed update that will benefit the Wi-Fi industry, businesses, and the millions of average Wi-Fi users around the world.

The WPA2 protocol with the Advanced Encryption Standard (AES) patched some security holes in the original WPA, which used the encryption protocol Temporal Key Integrity Protocol (TKIP). WPA2 was considered much more secure than the long-dead WEP security. However, WPA2 still had significant vulnerabilities that have emerged over the past decade. In October 2017, a researcher published 10 possible “attacks” against WPA2. All of them involve “small prints” in the WPA2 testing method. Patches are available for most platforms, but this research shows that WPA2 is aging and it is time to update.

WPA3 is the next generation of Wi-Fi security and provides cutting-edge security protocols to the market. The WPA security family includes solutions for personal and enterprise networks.

Building on the widespread success and adoption of WPA2, WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain the resiliency of mission-critical networks. All WPA3 networks:

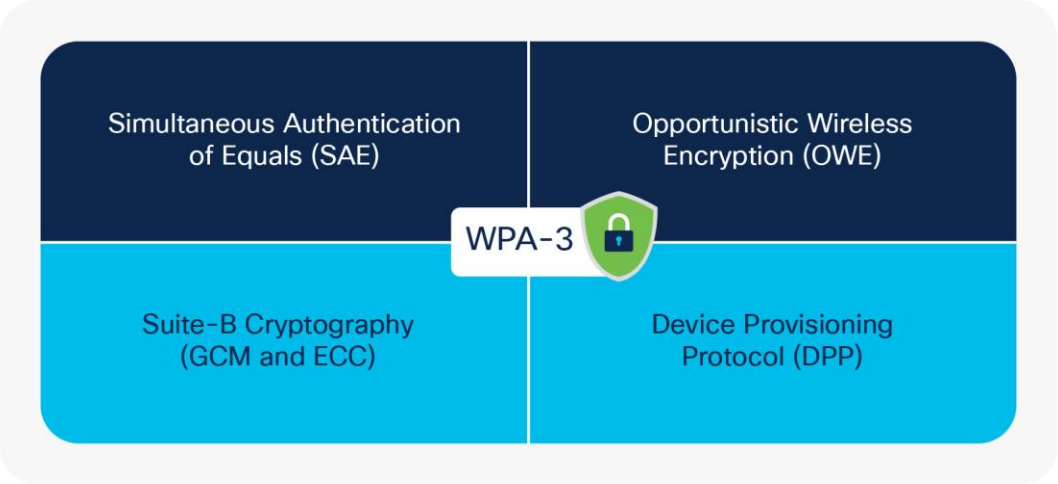
- Use the latest security methods
- Disallow outdated legacy protocols
- Require the use of Protected Management Frames (PMF)

Since Wi-Fi networks differ in their purpose and security needs, WPA3 includes capabilities that are specific to personal networks as well as enterprise networks. Users of WPA3-Personal receive increased protection from password-guessing attempts, while WPA3-Enterprise users can now take advantage of higher-grade security protocols for sensitive data networks. WPA3 retains interoperability with WPA2 devices.

The following are the key WPA3 enhancements in Cisco® AireOS and Cisco IOS® XE based controllers.

- Simultaneous Authentication of Equals (SAE)
- Opportunistic Wireless Encryption (OWE)
- Suite B Cryptography (GCM and ECC)

Note: DPP (also known as Wi-Fi Easy Connect) and Wi-Fi Enhanced Open (based on OWE) are not part of the WPA3 certification process, and support is not mandatory. DPP will not be supported on Cisco controllers.


Simultaneous Authentication of Equals (SAE)
Opportunistic Wireless Encryption (OWE)
WPA-3
Suite-B Cryptography (GCM and ECC)
Device Provisioning Protocol (DPP)

Platform support

Cisco Catalyst® wireless platforms: 9800-40, 9800-80, 9800-L and 9800-CL

Cisco Unified Wireless Network wireless controllers: 3504, 5520 Series, 8540 Series, and Virtual Wireless Controller

802.11ac Wave 1 and Wave 2 access points: Cisco Aironet® 1800 Series, 2802, 3802, 4800, and the 1540, 1560, 1700, 2700, 3700, and 1570 Series

802.11ax access points: Cisco Catalyst 9115AX, 9117AX, and 9120AX Series

Note: It is mandatory for all 802.11ax access points to support WPA3.

Supported releases

Cisco IOS XE Release 16.12 and higher
AireOS Release 8.10 and higher

SAE, aka WPA3-Personal

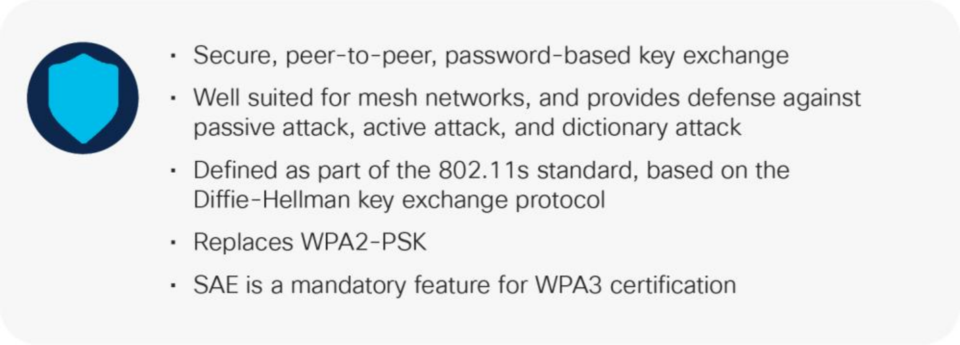
One key concern of personal networks is authentication. These networks typically cannot perform individual user authentication. Therefore, the network is either left open (anyone can join when in range, but anyone can see everyone else’s traffic) or protected with WPA2 PSK (preshared keys), where security is built upon a shared password, or passphrase. One limitation of PSK is that it is susceptible to offline cracking. An attacker can capture a valid association and then use offline tools to find the passphrase.

WPA3-Personal brings better protection to individual users by providing more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE), which improves on the PSK method in WPA2-Personal. The technology is resistant to offline dictionary attacks in which an adversary attempts to determine a network password by trying possible passwords without further network interaction.

The encryption with WPA3-Personal is more individualized. Users on a WPA3-Personal network can't ever snoop on another's WPA3-Personal traffic, even when the user has the Wi-Fi password and is successfully connected. Furthermore, if an outsider determines the password, it is not possible to passively observe an exchange and determine the session keys, providing forward secrecy of network traffic. Plus, they can't decrypt any data captured prior to the cracking.

WPA3 provides improvements to the general Wi-Fi encryption:

- Natural password selection: Allows users to choose passwords that are easier to remember
- Ease of use: Delivers enhanced protection with no change to the way users connect to a network
- Forward secrecy: Protects data trace even if a password is compromised after the data was transmitted
- Well suited for mesh networks and provides defense against passive attacks, active attacks, and dictionary attacks
- Defined as part of the 802.11s standard and then generalized in 802.11-2016, based on the Diffie-Hellman key exchange protocol
- Transition mode: Coexistence of WPA2 and WPA3, easy adoption
- PMF enabled and mandatory



- Secure, peer-to-peer, password-based key exchange
- Well suited for mesh networks, and provides defense against passive attack, active attack, and dictionary attack
- Defined as part of the 802.11s standard, based on the Diffie-Hellman key exchange protocol
- Replaces WPA2-PSK
- SAE is a mandatory feature for WPA3 certification

OWE, aka Wi-Fi Enhanced Open networks

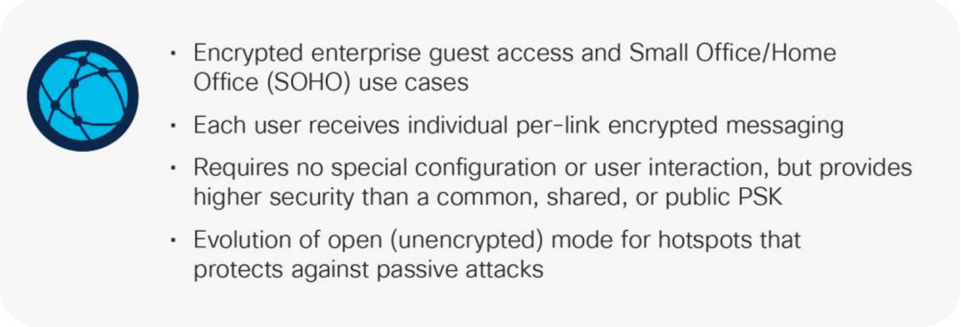
A concerning deficiency of Wi-Fi since its inception is the lack of any built-in security, encryption, or privacy on open public networks. Anyone with the right tools could snoop on users connected to Wi-Fi hotspots in cafes, hotels, and other public areas. This snooping could be passive, as in just monitoring websites visited or capturing unsecured email login credentials, or active, such as hijacking a session to gain access to a user's website login.

Enhanced Open is a Wi-Fi Alliance certification that preserves the convenience of open networks (no need for a shared password) while reducing some of the risks associated with accessing an open, unsecured network. Wi-Fi Enhanced Open networks provide unauthenticated data encryption to users, an improvement over traditional open networks with no protection at all. This protection is transparent to the user.

Based on Opportunistic Wireless Encryption (OWE) defined in the IETF RFC 8110 specification and the Wi-Fi Alliance OWE specification, Wi-Fi Enhanced Open benefits users by providing data encryption that maintains the ease of use of open networks and benefits network providers because there are no public passphrases to maintain, share, or manage.

The advantage of OWE is that passive attacks are prevented. Unfortunately, active attacks still enable an adversary to intercept traffic in some limited cases. Nevertheless, under the proposal of RFC 7435, "Some Protection Most of the Time," it still increases security.

From a technical perspective, the OWE handshake negotiates a new PMK using a Diffie-Hellman key exchange. This handshake is encapsulated in Information Elements (IEs) in the (re)association request and response frames. The resulting PMK is used in a four-way handshake, which negotiates and installs frame encryption keys.



- Encrypted enterprise guest access and Small Office/Home Office (SOHO) use cases
- Each user receives individual per-link encrypted messaging
- Requires no special configuration or user interaction, but provides higher security than a common, shared, or public PSK
- Evolution of open (unencrypted) mode for hotspots that protects against passive attacks

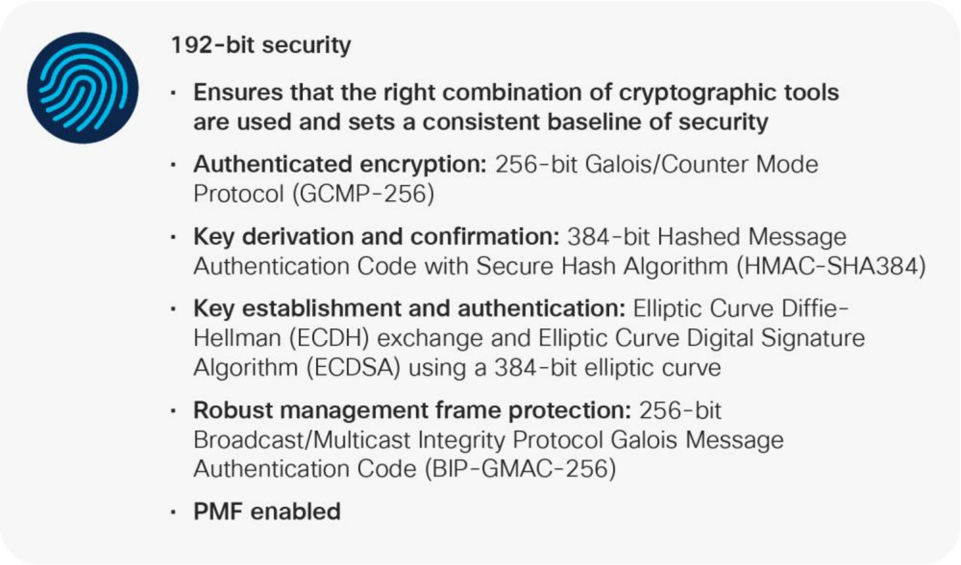
Note: Wi-Fi Enhanced Open was published under the WPA3 general umbrella but is not part of the WPA3 mandatory certification process, and its support is not mandatory.

WPA3-Enterprise

Enterprises, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocols across the network. WPA3-Enterprise offers increased key sizes, specifically referring to the Commercial National Security Algorithms (CNSA) suite. CNSA was defined by the U.S. National Security Agency (NSA) to protect top-secret data on government and military networks. Due to the fact that the CNSA suite mandates consistent security and employs strong cryptographic encryption, it was adopted by organizations that require top security.

This means WPA3 will support AES Galois/Counter Mode (GCM) with 256-bit keys for encryption, and Elliptic Curve Cryptography (ECC) based on 384-bit curves. This method is extremely fast to compute yet provides the same level of security as a 3072-bit Rivest-Shamir-Adleman (RSA) key. Additionally, SHA384 of the Secure Hash Algorithm 2 (SHA2) family will be used, and any employed RSA keys must be at least 3072 bits. All combined, this results in what is called 192-bit security, because that’s roughly the effective strength of 384-bit elliptic curves and SHA384 (the security is half the key length).

WPA3-Enterprise offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data.



192-bit security

- **Ensures that the right combination of cryptographic tools are used and sets a consistent baseline of security**
- **Authenticated encryption:** 256-bit Galois/Counter Mode Protocol (GCMP-256)
- **Key derivation and confirmation:** 384-bit Hashed Message Authentication Code with Secure Hash Algorithm (HMAC-SHA384)
- **Key establishment and authentication:** Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
- **Robust management frame protection:** 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
- **PMF enabled**

WPA3 allows several types of Extensible Authentication Protocol (EAP) methods for authentication. However, WPA3- Enterprise 192-bit mode mandates the use of EAP Transport Layer Security (EAP-TLS) for the EAP method, and the TLS ciphers as required by the CNSA suite.

Permitted EAP cipher suites for use with WPA3-Enterprise 192-bit mode are:

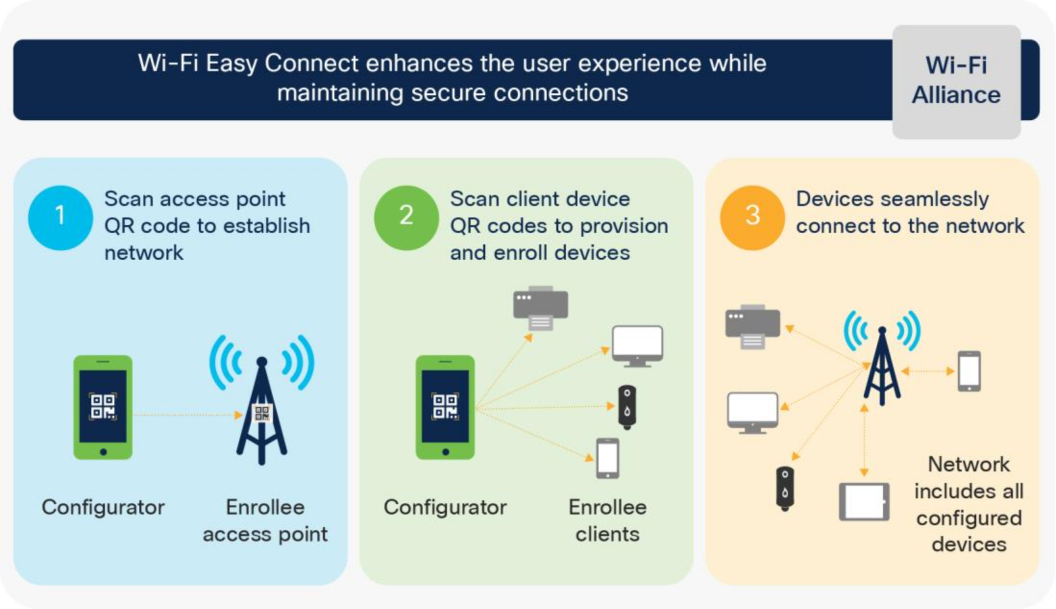
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - ECDHE and ECDSA using the 384-bit prime modulus curve P-384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - ECDHE using the 384-bit prime modulus curve P-384 - RSA ≥ 3072-bit modulus
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - RSA ≥ 3072-bit modulus - DHE ≥ 3072-bit modulus

The 192-bit security mode offered by WPA3-Enterprise ensures that the right combination of cryptographic tools is used and sets a consistent baseline of security within a WPA3 network. This will be a welcome feature for government entities, large corporations, and other highly sensitive environments. Depending on the specific RADIUS server implementation, however, the 192-bit security mode in WPA3-Enterprise may require updates related to the EAP server component of the AAA server.

Wi-Fi Easy Connect

The Wi-Fi Alliance has introduced a feature called Wi-Fi Easy Connect, which essentially allows new devices to connect to the wireless network with minimal user interaction, and is intended for small Internet of Things (IoT) and home networks. For example, you can join a WPA3 network by scanning a QR code. In some non-WPA2 networks in the past, organizations and individuals developed ways to place a QR code in a central location (such as in a coffee shop), allowing users to scan the code and be joined to the wireless environment. This method is similar in spirit to what the Wi-Fi Alliance is looking to accomplish in the Easy Connect feature, but the goal is to use your phone to scan an object's QR code, connect to that object, and provision credentials to get that object onto your network.

Note: **Wi-Fi Easy Connect was released under the WPA3 general umbrella but is not part of the WPA3 mandatory certification process; its support is not mandatory. Wi-Fi Easy Connect will not be supported on Cisco controllers.**


Wi-Fi Easy Connect enhances the user experience while maintaining secure connections
Wi-Fi Alliance
1
Scan access point QR code to establish network
Configurator
Enrollee access point
2
Scan client device QR codes to provision and enroll devices
Configurator
Enrollee clients
3
Devices seamlessly connect to the network
Network includes all configured devices

WPA3 and WPA2 compatibility

WPA2 continues to provide security and privacy for Wi-Fi networks and devices throughout the Wi-Fi ecosystem. WPA2 devices will continue to interoperate and provide recognized security that has been its hallmark for more than a decade.

WPA2 will also continue to evolve to meet standards for interoperability and security in all Wi-Fi certified devices. It will be available in Wi-Fi certified devices for the foreseeable future, and all devices supporting WPA3 will continue to work with WPA2.

Did someone say WPA3 vulnerabilities?

A researcher found five vulnerabilities in the SAE protocol used as part of WPA3-Personal. These vulnerabilities allow an attacker to:

- Perform Denial of Service (DoS) by flooding spoofed authentication frames to an Access Point (AP)
- Switch clients from WPA3-Personal to WPA2-Personal on the WPA3-Transition mode Basic Service Set (BSS)
- Downgrade Diffie-Hellman groups used in SAE
- Perform ECC and modular exponential (MODP) side-channel timing attacks

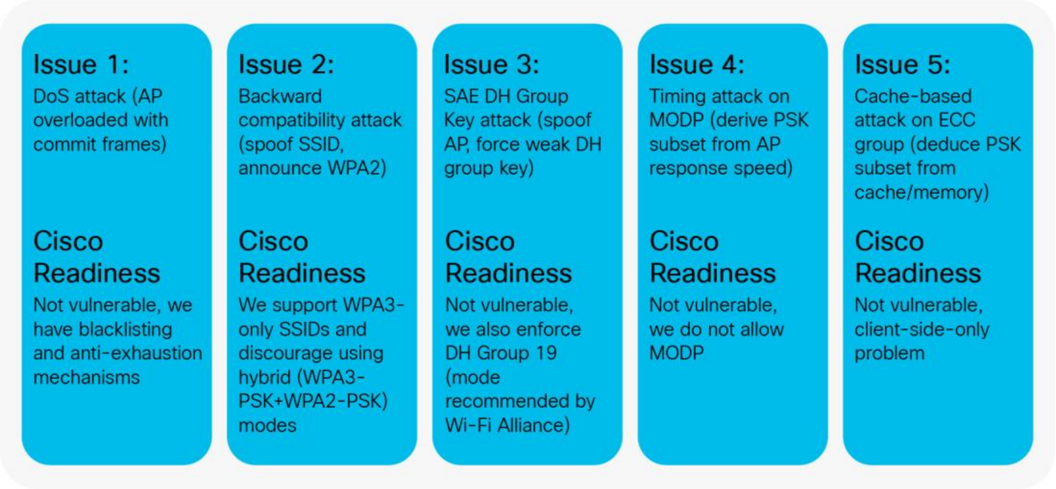
Impacted client devices

On client stations that implement WPA3-Personal,

- ECC and MODP side-channel timing attacks can occur:
    - If the vendor isn’t implementing constant-time calculations
    - If the client has been compromised by malware or malicious application (machine CLI access)
- Diffie-Hellman (DH) group downgrade can occur:
    - Clients that support weak DH groups could be compromised
- WPA3-Transition mode compromise can occur:
    - Clients can be “downgraded” from WPA3-Personal to WPA2-Personal and the passphrase can be recovered through a normal WPA2-PSK cracking technique

Cisco’s response to WPA3 vulnerabilities

- Cisco APs and WLCs are not susceptible to these attacks.
- Cisco WLANs can be configured as WPA3-Personal only, thus disabling WPA3-Transition mode.
- Vulnerabilities do not affect WPA2-Enterprise and WPA3-Enterprise.
- Cisco has implemented protection mechanisms for control plane traffic to protect the CPU from DoS attacks.
- Only the required DH groups are allowed; downgrading is not possible.
- Customers should avoid PSK WLANs in general, and when using PSK, use WPA3-PSK, not WPA2-PSK or hybrid WPA3-PSK+WPA2-PSK.
- Customers should check with their endpoint vendor for WPA3 vulnerability.



Issue 1:	Issue 2:	Issue 3:	Issue 4:	Issue 5:
DoS attack (AP overloaded with commit frames)	Backward compatibility attack (spoof SSID, announce WPA2)	SAE DH Group Key attack (spoof AP, force weak DH group key)	Timing attack on MODP (derive PSK subset from AP response speed)	Cache-based attack on ECC group (deduce PSK subset from cache/memory)
Cisco Readiness	**Cisco Readiness**	**Cisco Readiness**	**Cisco Readiness**	**Cisco Readiness**
Not vulnerable, we have blacklisting and anti-exhaustion mechanisms	We support WPA3-only SSIDs and discourage using hybrid (WPA3-PSK+WPA2-PSK) modes	Not vulnerable, we also enforce DH Group 19 (mode recommended by Wi-Fi Alliance)	Not vulnerable, we do not allow MODP	Not vulnerable, client-side-only problem

Configuring WPA3 on Cisco Catalyst 9800 Series with Cisco IOS XE 16.12.1

Cisco IOS XE on 9800 Series – WPA3 SAE configuration on WLAN

```
C9800(config)#wlan WPA3 1 WPA3
C9800(config-wlan)#no security wpa akm dot1x
C9800(config-wlan)#no security ft over-the-ds
C9800(config-wlan)#no security ft
C9800(config-wlan)#no security wpa wpa2
```

PMF is now disabled.

```
C9800(config-wlan)#security wpa wpa2 ciphers aes
C9800(config-wlan)#security wpa psk set-key ascii 0 Cisco123
C9800(config-wlan)#security wpa wpa3
C9800(config-wlan)#security wpa akm sae
C9800(config-wlan)#no shutdown
C9800 (config-wlan)#end
```

Cisco IOS XE configuration – SAE + PSK for WPA3 + WPA2 on the same WLAN

```
C9800(config)#no wlan tme-sae 2 tme-sae
C9800(config)#wlan tme-sae 2 tme-sae
C9800(config-wlan)#no security wpa akm dot1x
C9800(config-wlan)#no security ft over-the-ds
C9800(config-wlan)#no security ft
C9800(config-wlan)#security wpa wpa2 ciphers aes
C9800(config-wlan)#security wpa psk set-key ascii 0 cisco123
C9800(config-wlan)#security wpa wpa3
C9800(config-wlan)#security wpa akm sae
C9800(config-wlan)#security wpa akm psk
C9800(config-wlan)#no shut
C9800(config-wlan)#no shutdown
C9800(config-wlan)#end
```

Cisco IOS XE configuration – WPA3 OWE

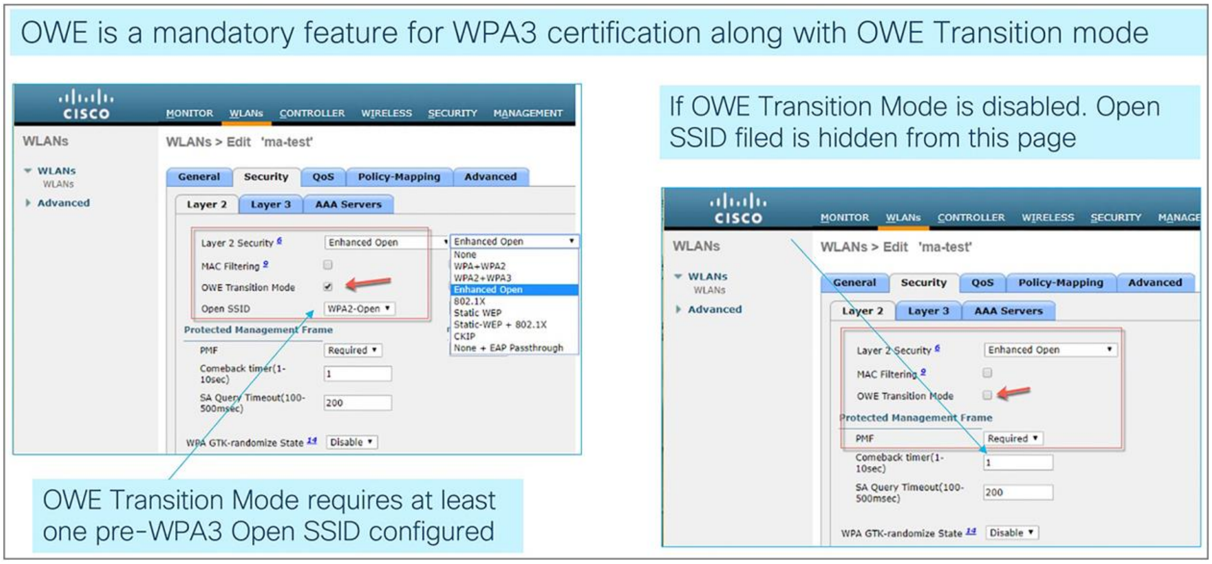
```
C9800(config)#no wlan WPA3 1 WPA3
C9800(config)#wlan WPA3 1 WPA3
C9800(config-wlan)#no security wpa akm dot1x
C9800(config-wlan)#no security ft over-the-ds
C9800(config-wlan)#no security ft
C9800(config-wlan)#no security wpa wpa2
```

PMF is now disabled.

```
C9800(config-wlan)#security wpa wpa2 ciphers aes
C9800(config-wlan)#security wpa wpa3
C9800(config-wlan)#security wpa akm owe
C9800(config-wlan)#no shutdown
C9800(config-wlan)#end
```

Configuring WPA3 on Cisco Unified Wireless Network AireOS 8.10 in WebUI

AireOS – OWE for Wi-Fi Enhanced Open networks



OWE is a mandatory feature for WPA3 certification along with OWE Transition mode

WLANs > Edit 'ma-test'

Layer 2 Security: Enhanced Open
MAC Filtering: □
OWE Transition Mode: ☑
Open SSID: WPA2-Open
Protected Management Frame
PMF: Required
Comeback timer(1-10sec): 1
SA Query Timeout(100-500msec): 200
WPA GTK-randomize State: Disable

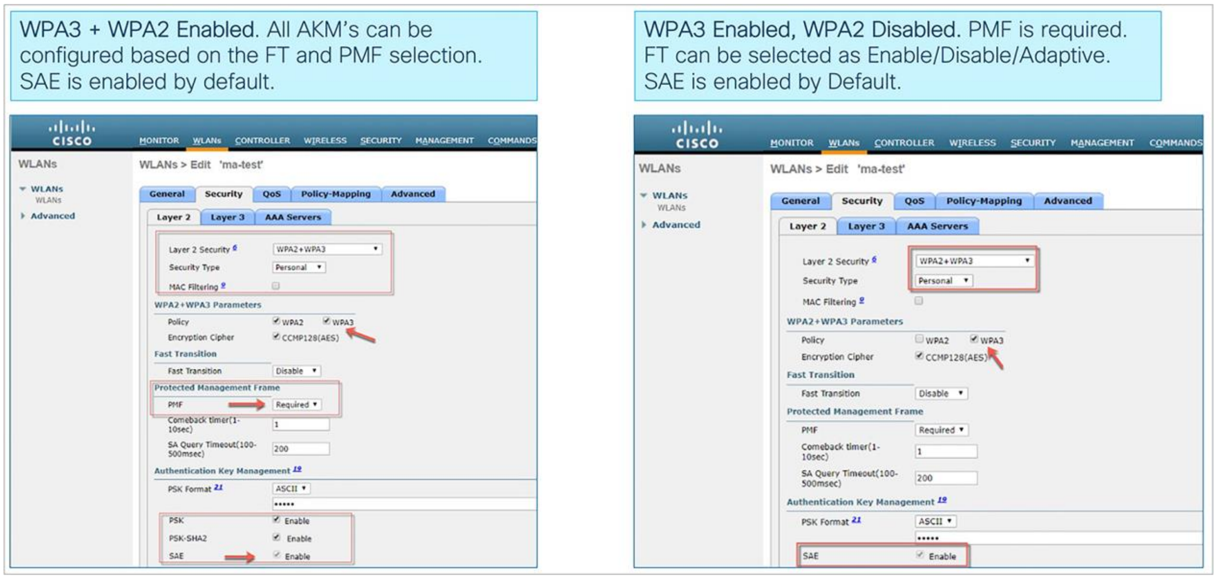
OWE Transition Mode requires at least one pre-WPA3 Open SSID configured

If OWE Transition Mode is disabled. Open SSID filed is hidden from this page

WLANs > Edit 'ma-test'

Layer 2 Security: Enhanced Open
MAC Filtering: □
OWE Transition Mode: □
Protected Management Frame
PMF: Required
Comeback timer(1-10sec): 1
SA Query Timeout(100-500msec): 200
WPA GTK-randomize State: Disable

AireOS – WPA3 SAE configuration



WPA3 + WPA2 Enabled. All AKM's can be configured based on the FT and PMF selection. SAE is enabled by default.

WLANs > Edit 'ma-test'

Layer 2 Security: WPA2+WPA3
Security Type: Personal
MAC Filtering: □
WPA2+WPA3 Parameters
Policy: ☑ WPA2 ☑ WPA3
Encryption Cipher: ☑ CCMP128(AES)
Fast Transition
Fast Transition: Disable
Protected Management Frame
PMF: Required
Comeback timer(1-10sec): 1
SA Query Timeout(100-500msec): 200
Authentication Key Management
PSK Format: ASCII
•••••
PSK: ☑ Enable
PSK-SHA2: ☑ Enable
SAE: ☑ Enable

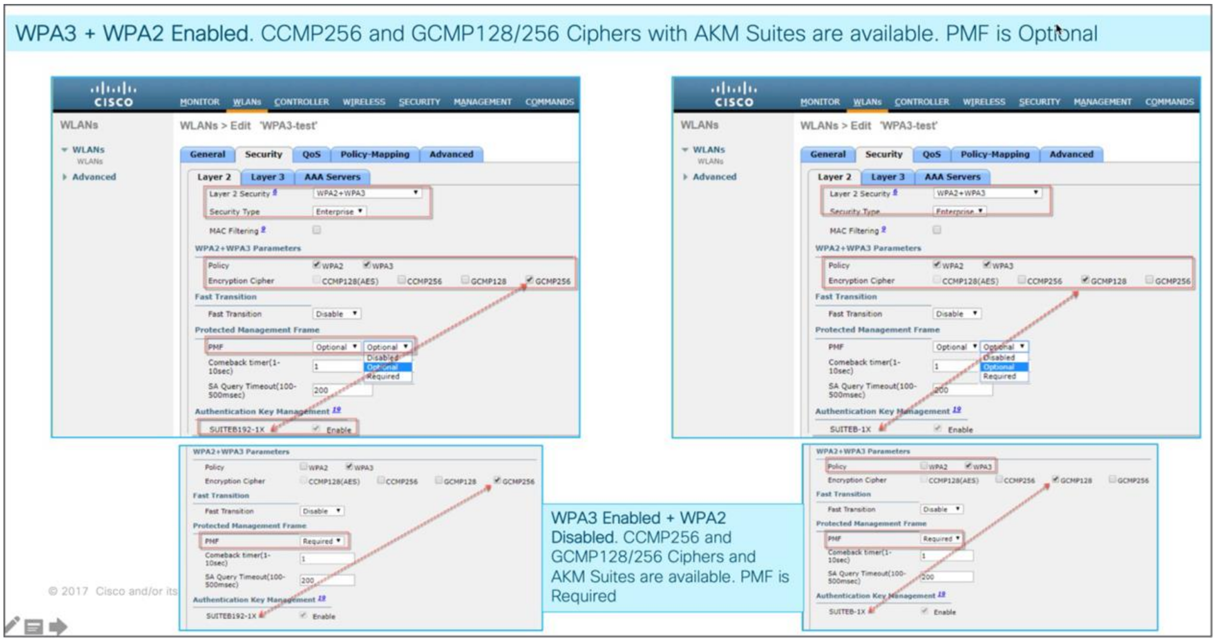
WPA3 Enabled, WPA2 Disabled. PMF is required. FT can be selected as Enable/Disable/Adaptive. SAE is enabled by Default.

WLANs > Edit 'ma-test'

Layer 2 Security: WPA2+WPA3
Security Type: Personal
MAC Filtering: □
WPA2+WPA3 Parameters
Policy: □ WPA2 ☑ WPA3
Encryption Cipher: ☑ CCMP128(AES)
Fast Transition
Fast Transition: Disable
Protected Management Frame
PMF: Required
Comeback timer(1-10sec): 1
SA Query Timeout(100-500msec): 200
Authentication Key Management
PSK Format: ASCII
•••••
SAE: ☑ Enable

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
Layer 2 Layer 3 AAA Servers

AireOS – WPA3 Enterprise mode configuration



WPA3 + WPA2 Enabled. CCMP256 and GCMP128/256 Ciphers with AKM Suites are available. PMF is Optional

WLANs > Edit 'WPA3-test'

- Layer 2 Security: WPA2+WPA3
- Security Type: Enterprise
- MAC Filtering: □
- WPA2+WPA3 Parameters
  - Policy: ☑ WPA2 ☑ WPA3
  - Encryption Cipher: □ CCMP128(AES) □ CCMP256 □ GCMP128 ☑ GCMP256
- Fast Transition
  - Fast Transition: Disable
- Protected Management Frame
  - PMF: Optional
  - Comeback timer(1-10sec): 1
  - SA Query Timeout(100-500msec): 200
- Authentication Key Management
  - SUITEB192-1X ☑ Enable

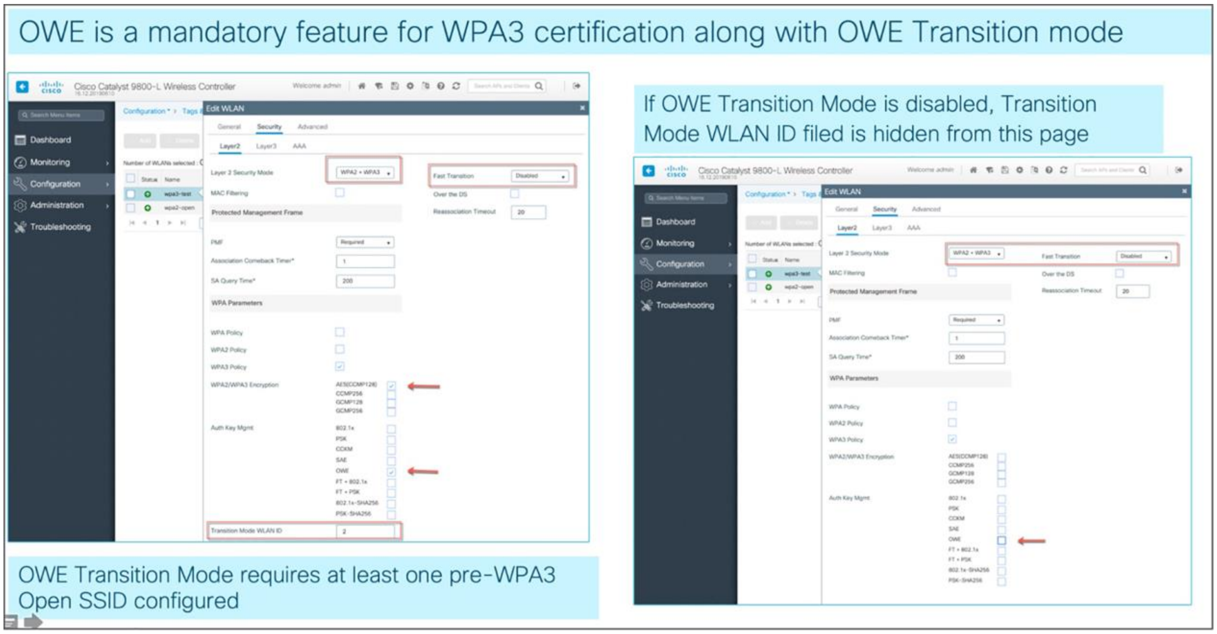
WPA3 Enabled + WPA2 Disabled. CCMP256 and GCMP128/256 Ciphers and AKM Suites are available. PMF is Required

- WPA2+WPA3 Parameters
  - Policy: □ WPA2 ☑ WPA3
  - Encryption Cipher: □ CCMP128(AES) □ CCMP256 □ GCMP128 ☑ GCMP256
- Fast Transition: Disable
- Protected Management Frame
  - PMF: Required
  - Comeback timer(1-10sec): 1
  - SA Query Timeout(100-500msec): 200
- Authentication Key Management
  - SUITEB192-1X ☑ Enable

© 2017 Cisco and/or its

Configuring WPA3 on Cisco IOS XE 16.12 in WebUI

IOS-XE 16.12 – OWE for Wi-Fi Enhanced Open networks



OWE is a mandatory feature for WPA3 certification along with OWE Transition mode

Cisco Catalyst 9800-L Wireless Controller

Edit WLAN

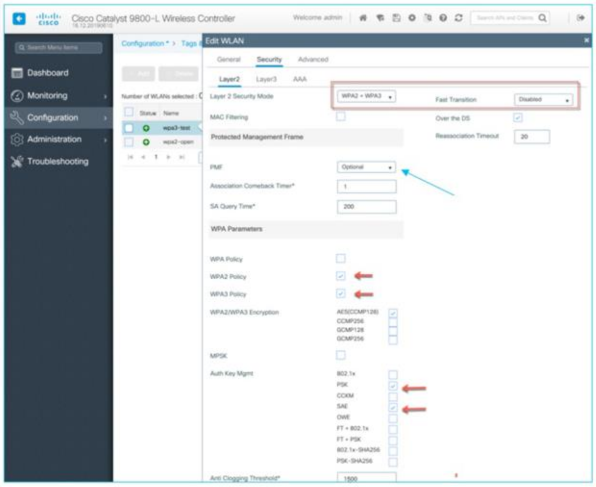
- Layer 2 Security Mode: WPA2 + WPA3
- MAC Filtering: □
- Protected Management Frame
  - PMF: Required
  - Association Comeback Timer*: 1
  - SA Query Time*: 200
- WPA Parameters
  - WPA Policy: □
  - WPA2 Policy: □
  - WPA3 Policy: ☑
  - WPA2/WPA3 Encryption: AES(CCMP128) ☑ CCMP256 □ GCMP128 □ GCMP256 □
  - Auth Key Mgmt: 802.1x □ PSK □ CCKM □ SAE □ OWE ☑ FT + 802.1x □ FT + PSK □ 802.1x-SHA256 □ PSK-SHA256 □
  - Transition Mode WLAN ID: 2
- Fast Transition: Disabled
- Over the DS: □
- Reassociation Timeout: 20

OWE Transition Mode requires at least one pre-WPA3 Open SSID configured

If OWE Transition Mode is disabled, Transition Mode WLAN ID filed is hidden from this page

Cisco IOS XE 16.12 – WPA3 Personal, aka SAE

WPA3 + WPA2 Enabled. All AKM's can be configured based on the FT and PMF selection.
SAE is enabled by default.



Layer 2 Security Mode: WPA2 + WPA3
Fast Transition: Disabled
MAC Filtering: □
Over the DS: ☑
Reassociation Timeout: 20

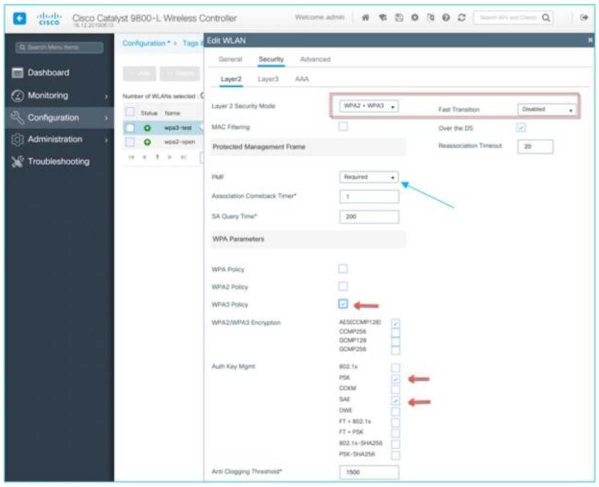
Protected Management Frame

PMF: Optional
Association Comeback Timer*: 1
SA Query Time*: 200

WPA Parameters

WPA Policy: □
WPA2 Policy: ☑
WPA3 Policy: ☑
WPA2/WPA3 Encryption: AES(CCMP128) ☑ CCMP256 □ GCMP128 □ GCMP256 □
MPSK: □
Auth Key Mgmt: 802.1x □ PSK ☑ CCKM □ SAE ☑ OWE □ FT + 802.1x □ FT + PSK □ 802.1x-SHA256 □ PSK-SHA256 □
Anti Clogging Threshold*: 1500

WPA3 Enabled, WPA2 Disabled. PMF is required. FT can be selected as Enable/Disable/Adaptive. SAE is enabled by Default.



Layer 2 Security Mode: WPA2 + WPA3
Fast Transition: Disabled
MAC Filtering: □
Over the DS: ☑
Reassociation Timeout: 20

Protected Management Frame

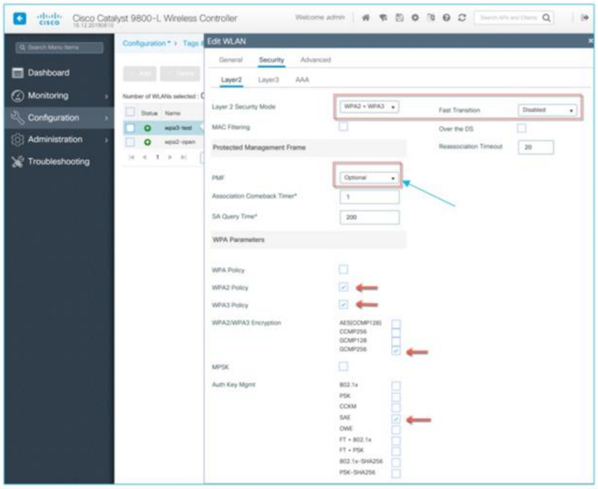
PMF: Required
Association Comeback Timer*: 1
SA Query Time*: 200

WPA Parameters

WPA Policy: □
WPA2 Policy: □
WPA3 Policy: ☑
WPA2/WPA3 Encryption: AES(CCMP128) ☑ CCMP256 □ GCMP128 □ GCMP256 □
Auth Key Mgmt: 802.1x □ PSK ☑ CCKM □ SAE ☑ OWE □ FT + 802.1x □ FT + PSK □ 802.1x-SHA256 □ PSK-SHA256 □
Anti Clogging Threshold*: 1500

Cisco IOS XE 16.12 – WPA3 Enterprise mode

WPA3 + WPA2 Enabled. CCMP256 and GCMP128/256 Ciphers with AKM Suites are available. PMF is Optional



Layer 2 Security Mode: WPA2 + WPA3
Fast Transition: Disabled
MAC Filtering: □
Over the DS: □
Reassociation Timeout: 20

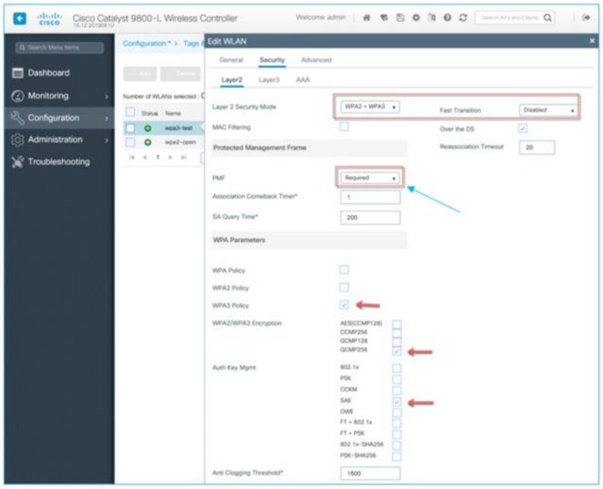
Protected Management Frame

PMF: Optional
Association Comeback Timer*: 1
SA Query Time*: 200

WPA Parameters

WPA Policy: □
WPA2 Policy: ☑
WPA3 Policy: ☑
WPA2/WPA3 Encryption: AES(CCMP128) □ CCMP256 □ GCMP128 □ GCMP256 ☑
MPSK: □
Auth Key Mgmt: 802.1x □ PSK □ CCKM □ SAE ☑ OWE □ FT + 802.1x □ FT + PSK □ 802.1x-SHA256 □ PSK-SHA256 □

WPA3 Enabled + WPA2 Disabled. CCMP256 and GCMP128/256 Ciphers and AKM Suites are available. PMF is Required



Layer 2 Security Mode: WPA2 + WPA3
Fast Transition: Disabled
MAC Filtering: □
Over the DS: ☑
Reassociation Timeout: 20

Protected Management Frame

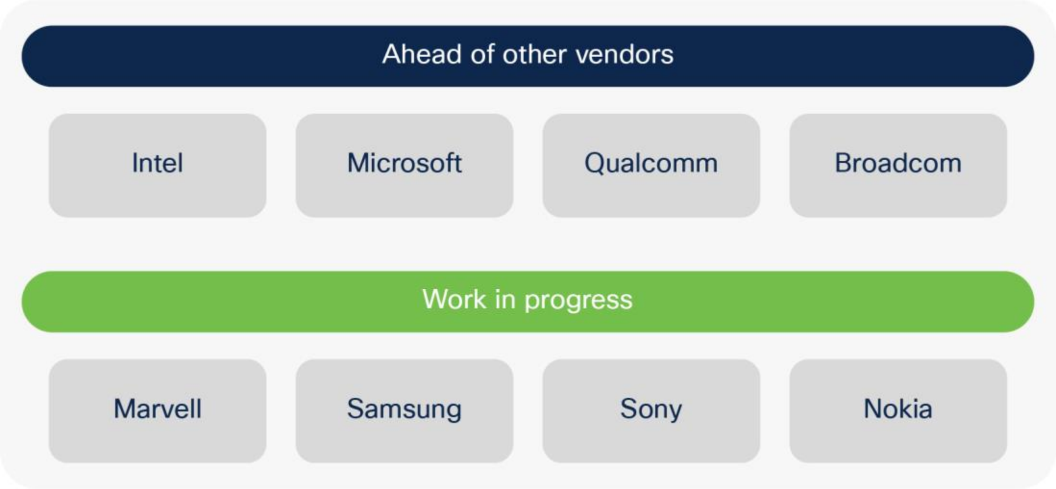
PMF: Required
Association Comeback Timer*: 1
SA Query Time*: 200

WPA Parameters

WPA Policy: □
WPA2 Policy: □
WPA3 Policy: ☑
WPA2/WPA3 Encryption: AES(CCMP128) □ CCMP256 □ GCMP128 □ GCMP256 ☑
Auth Key Mgmt: 802.1x □ PSK □ CCKM □ SAE ☑ OWE □ FT + 802.1x □ FT + PSK □ 802.1x-SHA256 □ PSK-SHA256 □
Anti Clogging Threshold*: 1500

Client WPA3 configuration

The following companies are participating in early development and support of the WPA3 protocols and security enhancements.



Ahead of other vendors

Intel

Microsoft

Qualcomm

Broadcom

Work in progress

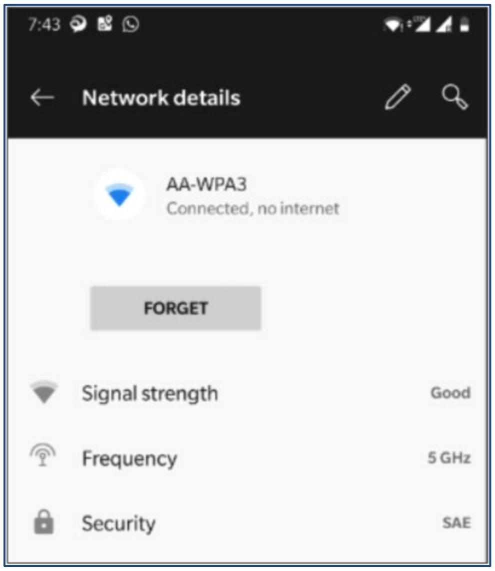
Marvell

Samsung

Sony

Nokia

Qualcomm-based client configuration



7:43

Network details

AA-WPA3
Connected, no internet

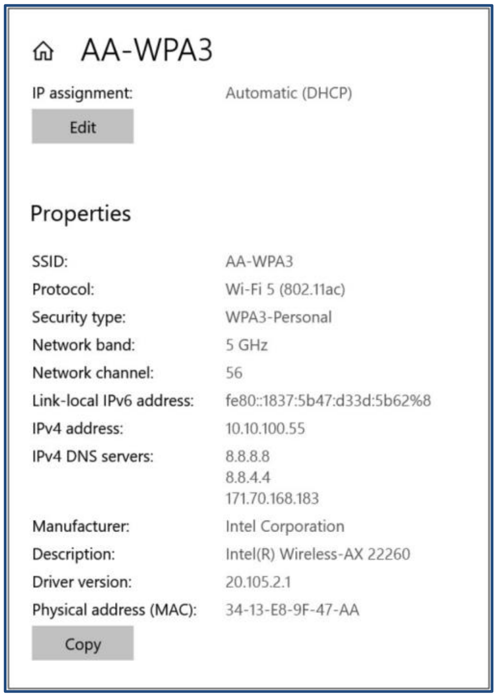
FORGET

Signal strength: Good

Frequency: 5 GHz

Security: SAE

Intel plus MS Windows-based client configuration



AA-WPA3

IP assignment:	Automatic (DHCP)

Properties

SSID:	AA-WPA3
Protocol:	Wi-Fi 5 (802.11ac)
Security type:	WPA3-Personal
Network band:	5 GHz
Network channel:	56
Link-local IPv6 address:	fe80::1837:5b47:d33d:5b62%8
IPv4 address:	10.10.100.55
IPv4 DNS servers:	8.8.8.8 8.8.4.4 171.70.168.183
Manufacturer:	Intel Corporation
Description:	Intel(R) Wireless-AX 22260
Driver version:	20.105.2.1
Physical address (MAC):	34-13-E8-9F-47-AA

Appendix

Web links

Cisco Catalyst 9800 Series Wireless Controllers information:
https://software.cisco.com/download/home/286322524

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices.**

Printed in USA C11-742565-00 07/19