WPA3 Encryption and Configuration Guide

Introduction

The original Wi-Fi Protected Access (WPA) standard was released in 2003 to replace the Wired Equivalent Privacy security algorithm (WEP), which was then in turn superseded by WPA2 in 2004. WPA3, announced by the Wi-Fi Alliance in 2018, introduced new features to simplify Wi-Fi security, including enabling better authentication, increased cryptographic strength, and requiring the use of Protected Management Frames (PMFs) to increase network security.

This article provides insight into WPA3 to help users make educated network security decisions.

> WPA3 is enabled by default on wireless networks configured for MR 27.X

Legacy access points (802.11ac Wave-1 or older) will **not** support WPA3/MR 27+, if configured with an SSID that uses WPA3, the APs will encrypt traffic using WPA2. For more information check MR Mixed Firmware Networks

Encryption

Cisco Meraki supports two WPA3 modes:

- WPA3-Personal
- WPA3-Enterprise

WPA3-Personal allows for better password-based authentication even when using non-complex combinations. WPA3 uses Simultaneous Authentication of Equals (SAE) to provide stronger defenses against password guessing. SAE is a secure key establishment protocol.

WPA3-Enterprise provides additional protections for networks transmitting sensitive data by offering the equivalent of 192-bit cryptographic strength. WPA3 networks use a suite of 192-bit cryptographic tools to ensure consistent protection across networks.

WPA3-Personal

WPA3-Personal using Simultaneous Authentication of Equals (SAE) builds upon WPA2 PSK, where users can authenticate using a passphrase only.

SAE adds a layer of security by authenticating both the STA and Meraki AP even before having an Association Request/Response. This provides an advantage when using non-complex passphrases. SAE it is a variant of RFC 7664, the Dragonfly Key Exchange.

WPA3-Personal has two variants:

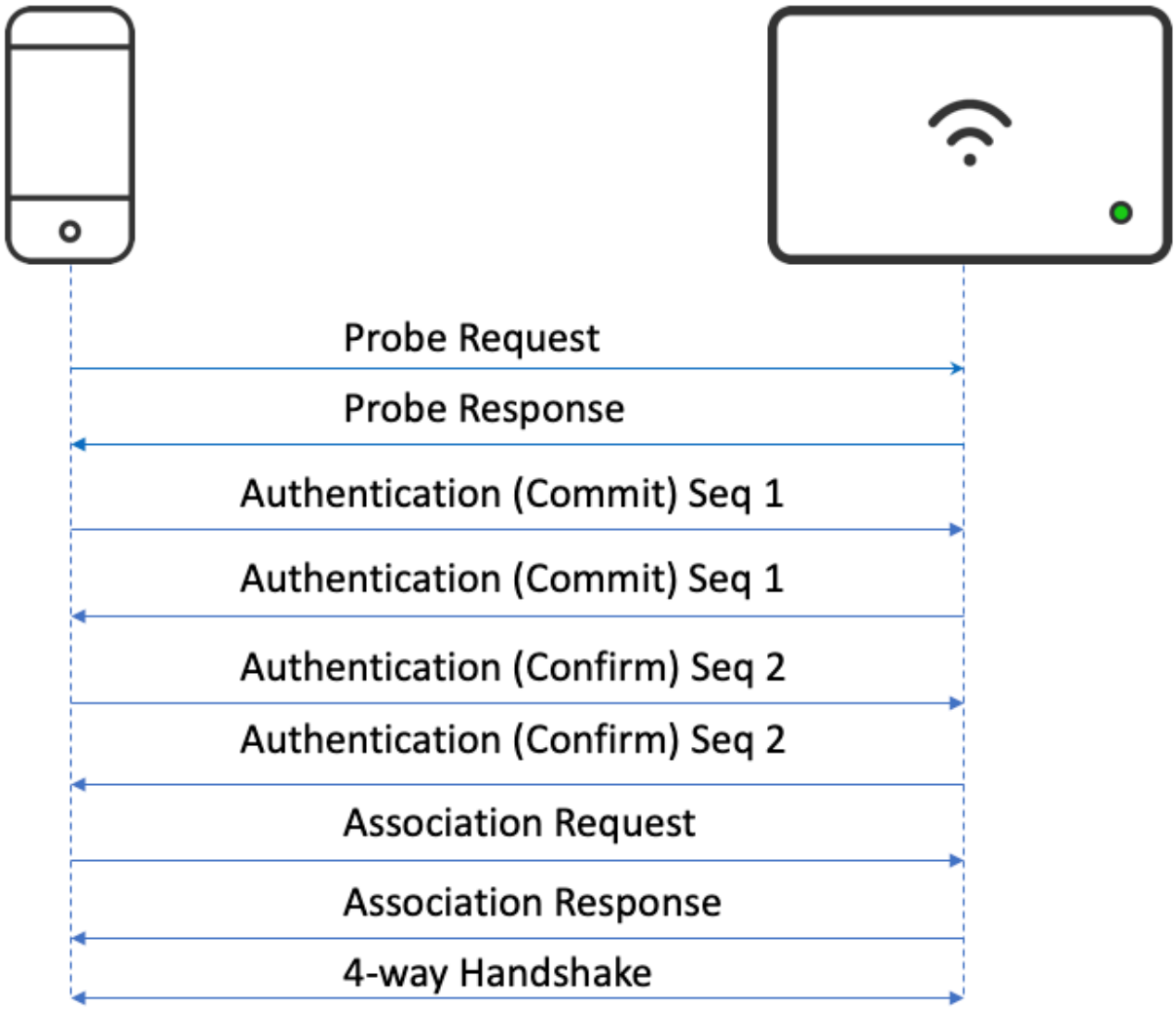
- WPA3 Only
- WPA3 Transition Mode

WPA3 Only

When using WPA3 only, the access point will transmit in the beacon the capability to only accept STA using WPA3 SAE. When using transition mode (in Dashboard presented as "WPA2 + WPA3), the access point will broadcast in the beacon capabilities to accept STA using both WPA2 and WPA3. In this configuration, STA that do not support WPA3 can still connect to the SSID.

> ⓘ WPA2 relies on complexity of the password for dictionary attacks. Consider this while using transition mode for the password.

WPA3 SAE follows the following process:

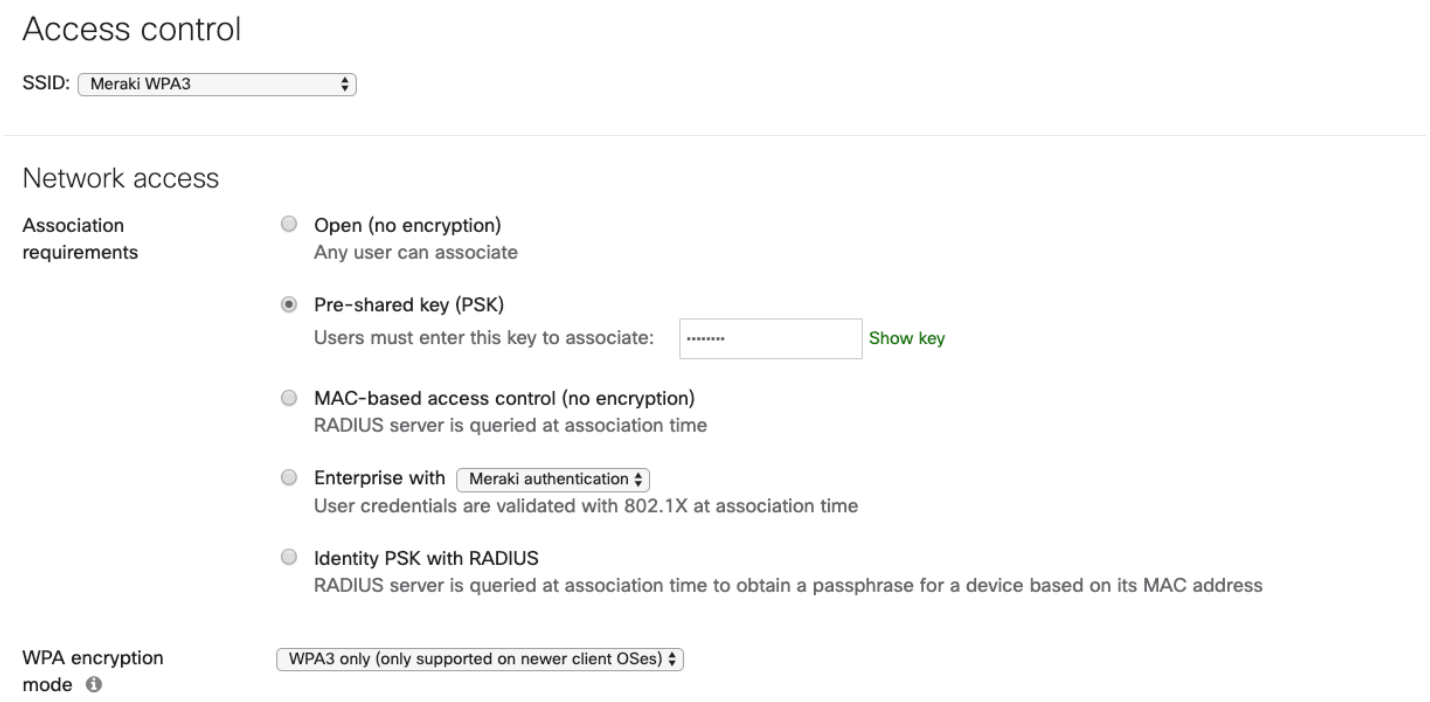


1. Probe Request.
    - Regular request to AP after beacon.
2. Probe Respond
    - Regular response to STA.

3. Authentication (Commit) from STA to AP.
    - This packet is 802.11 authentication.
    - Commit will include SAE authentication Seq Number 1 with a scalar and an element not related to the password to be used.
    - This is used to generate PMK (Pairwise master Key) on STA.
4. Authentication (Commit) from AP to STA.
    - This packet is 802.11 authentication.
    - Commit will include SAE authentication Seq Number 1 with a scalar and an element not related to the password to be used.
    - This is used to generate PMK (Pairwise master Key) on AP.
5. Authentication (Confirm) from STA to AP.
    - This packet is 802.11 authentication.
    - Confirm includes Seq2 with confirm message with key generated for AP to validate.
6. Authentication (Confirm) from AP to STA.
    - This packet is 802.11 authentication.
    - Confirm includes Seq2 with confirm message with key generated letting STA know key is correct or rejecting the authentication.
7. Regular Association Request.
8. Regular Association Response.
9. 4-way handshake utilizing PMK generated with SAE method. After this step regular data can be transmitted.

Configuration

To enable WPA3-SAE, navigate to **Wireless > Access Control** and change the WPA encryption mode to **WPA3 only.**



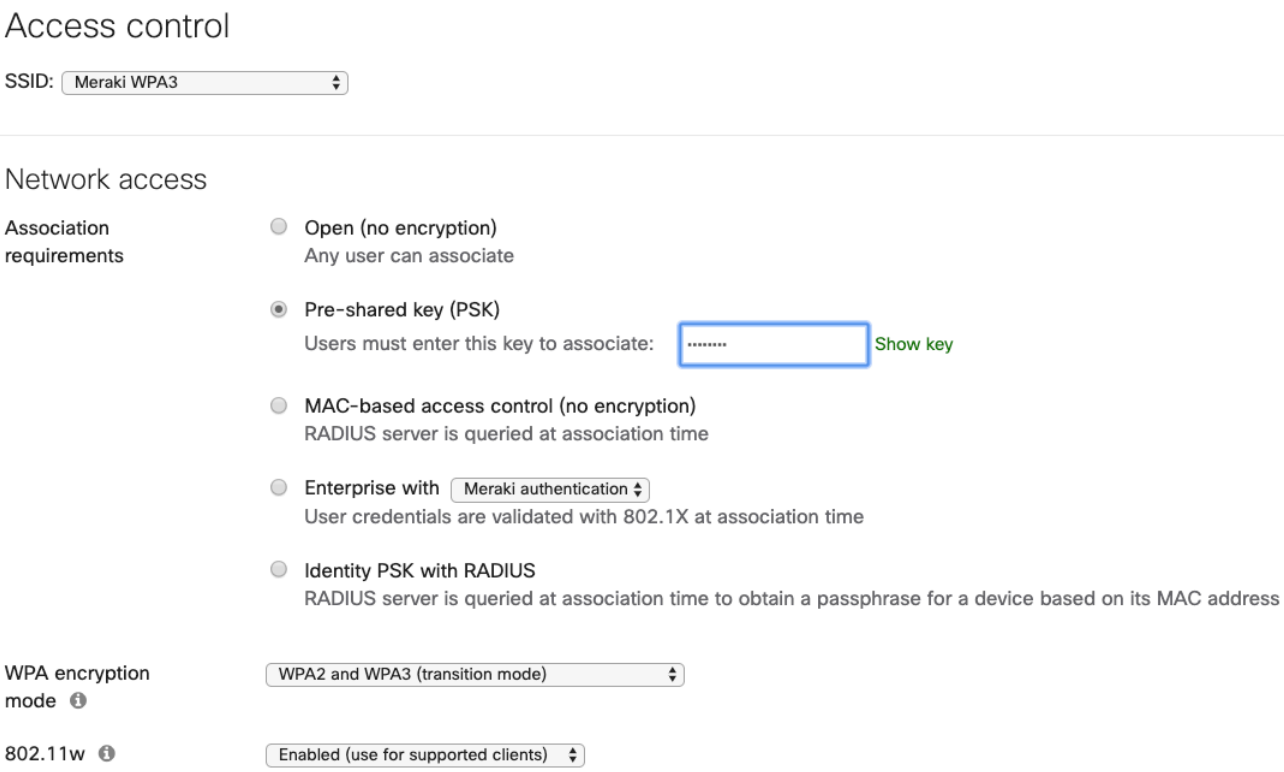
WPA3 Transition Mode

WPA3 SAE has a transition mode (sometimes called mixed mode) created to allow WPA2 clients to co-exist on the same SSID used for WPA3. Although WPA3 needs to have PMF set to **Required**, the STA can also set is as **Enabled**, so that the STA which is not compliant with either WPA3 or PMF can still connect seamlessly.

PMF can be still set as Required, however, when WPA2 clients who need to use this and if STA does not support it, they will **not** be able to associate.

Configuration

To enable WPA3 Transition Mode, navigate to **Wireless > Access Control** and select the WPA encryption mode to **WPA2 and WPA3 (transition mode)**.



Client Behavior Chart for WPA3 Personal

The following chart delineates the different connection behaviors of STA based on the dashboard configuration:

Dashboard Configuration		Client behavior		
WPA3	802.11w PMF	WPA2 STA	WPA2 STA PMF	WPA3 STA
Only	Required	Cannot Connect	Cannot Connect	Connects
Transition	Required	Cannot Connect	Connects	Connects
	Enabled	Connects	Connects	Connects

WPA3-Enterprise

WPA3 Enterprise builds upon WPA2 and it is meant to replace it in the future. It utilizes 192-bit security while still using the 802.1x standard to provide a secure wireless network for enterprise use. This provides a superior encryption method to better protect any kind of data. The security suite is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) suite and commonly placed in high-security Wi-Fi networks such as in government, defense, finance, and other industries.

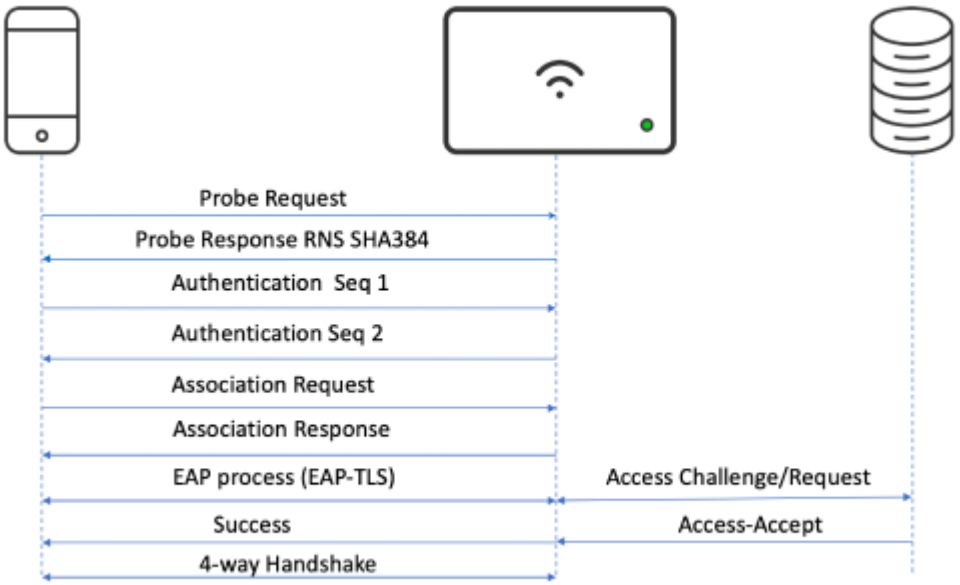
To use WPA3 enterprise, the RADIUS servers **must** use one of the permitted EAP ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

In order to use this authentication, the RADIUS server must support these ciphers. Also, WPA3 192-bit security will be exclusive for EAP-TLS, which will require certificates on both STA and RADIUS server.

WPA3 - Enterprise follows a similar process as the one in WPA2, however, it is enhanced due to the aforementioned ciphers.

The WPA3 - Enterprise process is the following:



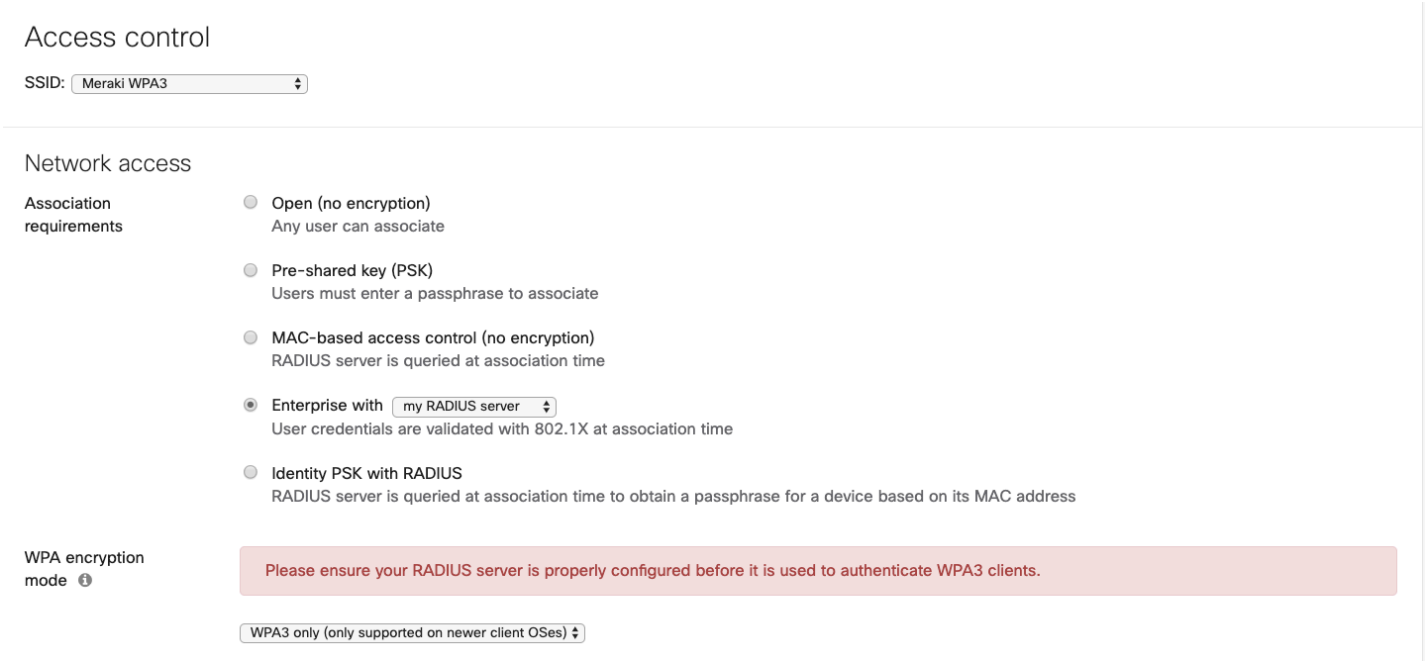
1. Regular Probe Request from STA to AP.
2. Probe response will include RSN SHA384 Suite-b stating this is WPA3 enterprise with 192-bit security.
3. Regular 802.11 Authentication with SEQ 1 from STA to AP.
4. Regular 802.11 Authentication with SEQ 2 from AP to STA.
5. Association Request including RSN capabilities from STA to AP.
6. Association Response from AP to STA.
7. EAP process that will include Identity Request/Response and exchange of credentials with RADIUS server using EAP-TLS protocol.
8. If authentication is complete with RADIUS server it will send an Access-Accept message which will be transmitted to the STA from the AP as a "Success" message.
9. Finally based on EAP process a PMK will be created and 4-way handshake will generate valid keys to ensure encryption. After this step regular data can be transmitted.

Configuration

To enable this on the dashboard, follow these steps:

1. Navigate to **Wireless** > **Access Control**
2. Select **Enterprise with my RADIUS server**

3. Choose WPA encryption mode as **WPA3 only.**
4. Configure the RADIUS server.



WPA3 enterprise is **not** supported with Meraki Auth.

WPA3 and 6Ghz

6Ghz SSIDs only support the use of WPA3, this means that transition mode will not be supported. Therefore, if a configuration that is not supported on the SSID is implemented, 6Ghz will be turned off by default.

It is recommended to use different SSID names if encryptions will be mismatched (WPA2 on 2.4/5Ghz vs WPA3 on 6Ghz).

Compatibility Configuration:

Security Type:	2.4/5Ghz	6Ghz
Open	ON	OFF
OWE*	ON	**ON**
OWE* Transition	ON	OFF

WPA2 Personal	ON	OFF
WPA2 Enterprise	ON	OFF
WPA3 Personal	ON	**ON**
WPA3 Personal Transition	ON	OFF
WPA3 Enterprise	ON	**ON**
WPA3 Enterprise transition	ON	OFF

*OWE support will be added in a future firmware release.

Below are the three most typical types of WLAN and the most popular choice of security protocol for each:

	2.4 & 5 GHz	6 GHz
Corporate Access	WPA2-Enterprise	WPA3-Enterprise
SMB & Home Office	WPA2-PSK	WPA3-SAE-H2E
Wi-Fi HotSpot	Open	OWE

Overtime it is expected for newer client drivers to support WPA3-Enterprise and WPA3-SAE-H2E mode on both the 2.4 & 5GHz bands as well as 6GHz. This will then allow clients to seamlessly roam between 2.4/5GHz and 6GHz bands using WPA3-SAE-H2E.