

# WPA3 Deployment Guide

---

# Contents

Introduction to WPA3	4
Supported WPA3 modes	4
Road-mapped WPA3 features	5
Cisco device compatibility	5
WPA3-Enterprise	5
WPA3-Enterprise GUI configuration	6
WPA3-Enterprise CLI configuration	10
WPA3-Enterprise 192-bit GUI configuration (optional)	10
WPA3-Enterprise 192-bit CLI configuration (optional)	13
WPA3-Enterprise transition mode	14
WPA3-Enterprise transition mode GUI configuration	15
WPA3-Enterprise transition mode CLI configuration	17
WPA3-Enterprise transition disable mode	17
WPA3-Enterprise transition mode disable GUI configuration	18
WPA3-Enterprise transition mode disable CLI configuration	20
WPA2+WPA3-Enterprise transition mode with 6GHz	21
WPA2+WPA3-Enterprise transition mode with 6GHz – GUI Configuration	21
WPA2+WPA3-Enterprise transition mode with 6GHz CLI configuration	24
WPA2+WPA3-Enterprise transition mode with 6GHz CLI Output	25
WPA3-Personal	25
WPA3-Personal GUI configuration	26
WPA3-Personal CLI configuration	29
WPA3-Personal SAE hash-to-element method for password element generation	30
WPA3-Personal SAE hash-to-element method for password element generation CLI configuration	32
WPA3-Personal SAE with fast transition enabled	33
WPA3-Personal SAE with fast transition enabled CLI configuration	35
WPA3-Personal transition mode	36
WPA3 Personal transition mode CLI configuration	38
WPA3-Personal transition mode disable	39
WPA3-Personal transition mode disable GUI configuration	39
WPA3-Personal transition mode disable CLI configuration	42
WPA2+WPA3-Personal transition mode with 6GHz	43
WPA2+WPA3-Personal transition mode with 6GHz GUI configuration	43
WPA2+WPA3-Personal transition mode with 6GHz CLI configuration	46
WPA2+WPA3-Personal transition mode with 6GHz CLI Output	47

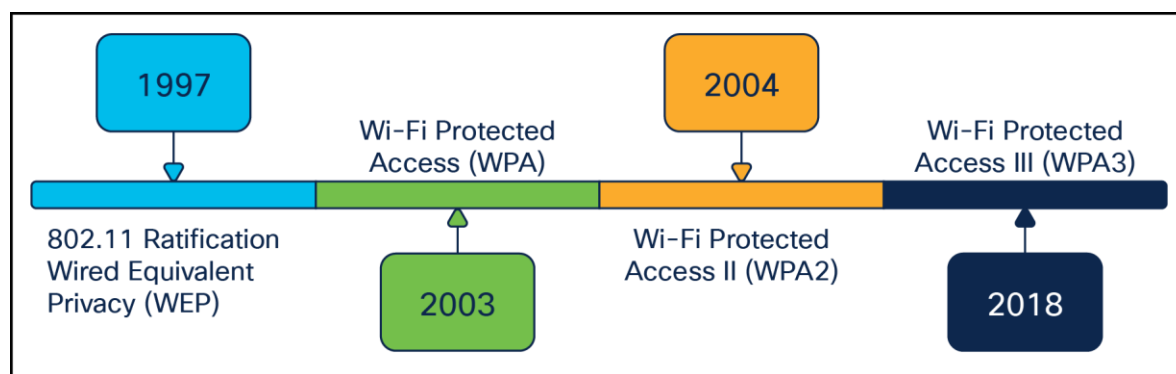
---

OWE	47
<b>WPA3 OWE GUI configuration</b>	<b>48</b>
<b>WPA3 OWE CLI configuration</b>	<b>50</b>
<b>WPA3 OWE transition mode GUI configuration</b>	<b>50</b>
<b>WPA3 OWE Transition mode CLI configuration</b>	<b>54</b>
Client interoperability matrix	56
Useful Catalyst WLC CLI commands	57
Useful Catalyst AP CLI commands	58
References	58

## Introduction to WPA3

WPA3 is the third and latest iteration of the Wi-Fi Protected Access standard developed by the Wi-Fi Alliance and replaces the previous standard, WPA2. The WPA standard was created by the Wi-Fi Alliance security technical task group, chaired by Cisco's Stephen Orr, with the purpose of standardizing wireless security. WPA3 introduces new features on enterprise, personal, and open security networks through an increase in cryptographic strength, allowing for a more secure authentication process for all WPA3-supported endpoints. The WPA3 Enterprise form extends the solid foundation provided by WPA2 Enterprise by making it mandatory to use Protected Management Frames (PMF) on all connections. This security feature protects against such dangerous attacks as Denial of Service, honeypots and eavesdropping.

Over the next few years, Cisco expects the industry to see an exponential increase in WPA3 adoption, especially in government and financial institutions. With the number of internet-connected devices forecasted to reach 41.6 billion in four years, there is an implicit need for better security, and WPA3 is the answer.



**Figure 1.**  
Wi-Fi security standards timeline

### Supported WPA3 modes

- WPA3-Enterprise, for 802.1X security networks. This leverages IEEE 802.1X with SHA-256 as the Authentication and Key Management (AKM).
- WPA3-Personal, which uses the Simultaneous Authentication of Equals (SAE) method for personal security networks.
- WPA3 Transition Mode (WPA2+WPA3 security-based WLANs for both personal and enterprise). {Starting 17.12.1, this can be used with 1 SSID and 1 Profile and support 6GHz band}.
- Opportunistic Wireless Encryption (OWE) for open security networks.

## Road-mapped WPA3 features

- WPA3-Enterprise 802.1x-256 in Flexconnect Mode
- WPA3-Enterprise SuiteB192-1X in Flexconnect Mode
- WPA3-Enterprise SuiteB192-1X Fast Transition

### Note:

1. For WPA3-Personal SAE hash-to-element method for password element generation - min. software version 17.7.1 should be used
2. For WPA3-Enterprise and WPA3-Personal Transition disabled - min. software version 17.7.1 should be used
3. For WPA3-Personal with SAE as AKM + Fast Transition (FT) - min. software version 17.9 should be used

## Cisco device compatibility

**Table 1.** Cisco® Catalyst® 9800 Series Wireless Controller WPA3 support matrix

9800-L-F	9800-L-C	9800-L	9800-40	9800-80
Yes, starting with 16.12.1s	Yes, starting with 16.12.1s	Yes, starting with 16.12.1s	Yes, starting with 16.12.1s	Yes, starting with 16.12.1s

**Table 2.** Catalyst 9100 Access Points WPA3 support matrix

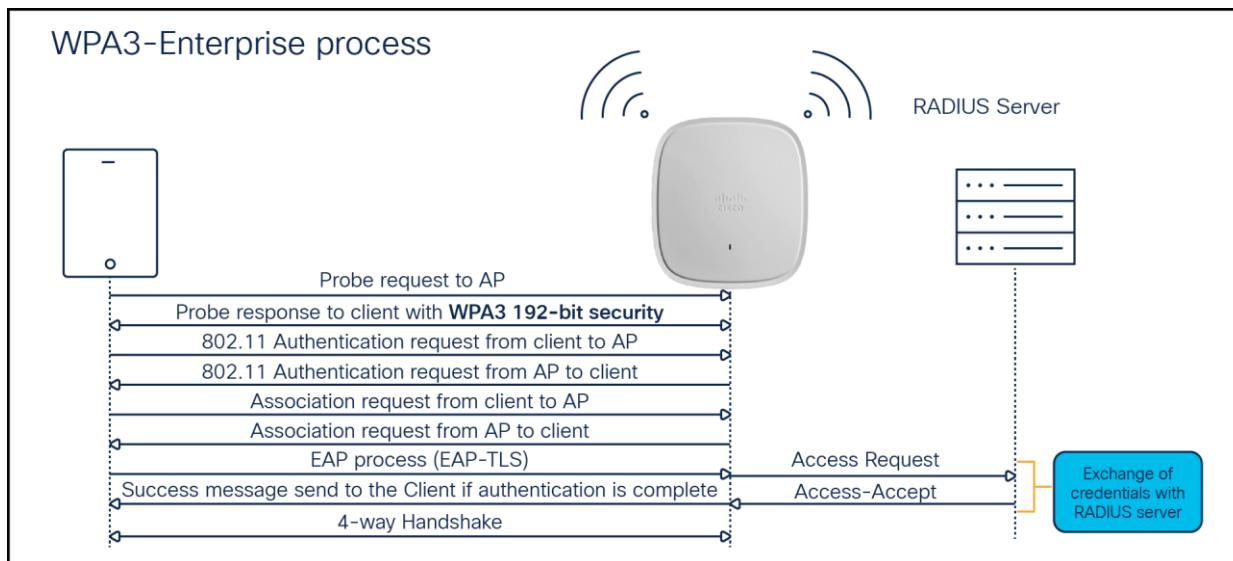
9105AX	9115AX	9117AX	9120AX	9130AX	9124AXE	9136AX	9166/9164/9162
Yes*	Yes*	Yes*	Yes*	Yes	Yes	Yes	Yes

\*SuiteB192-1X is not supported

The purpose of this deployment guide is to provide details of the different WPA3 modes and steps to configure them on the Catalyst 9800 Series controller, using either the GUI or the Command-Line Interface (CLI).

## WPA3-Enterprise

WPA3-Enterprise builds upon the foundation of WPA2-Enterprise with the additional requirement of using Protected Management Frames on all WPA3 connections with 802.1X for user authentication with a RADIUS server. By default, WPA3 uses 128-bit encryption, but it also introduces an optionally configurable SuiteB-192 bit cryptographic strength encryption using GMCP-256, which gives additional protection to any network transmitting sensitive data. The WPA3-Enterprise is highly preferred and recommended to be used and commonly seen in enterprises, financial institutions, government, and other market sectors where network security is most critical.



**Figure 2.**  
WPA3-Enterprise endpoint and network handshake process

## WPA3-Enterprise GUI configuration

The following steps will create a WLAN with WPA3-Enterprise security:

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the General tab, enter the **Profile Name** (friendly identifier). Both the SSID and WLAN ID will be populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have Access Points (APs) associated with this profile begin broadcasting this configured WLAN.

Add WLAN

General

Security

Advanced

Profile Name\*

WPA3-Enterprise

SSID\*

WPA3-Enterprise

WLAN ID\*

8

Status

ENABLED

Broadcast SSID

ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status

ENABLED

WPA2 Disabled

WPA3 Enabled

Dot11ax Enabled

5 GHz

Status

ENABLED

2.4 GHz

Status

ENABLED

802.11b/g Policy

802.11b/g

Cancel

Apply to Device

**Figure 3.**  
Radio/Slot configuration

- Click the **Security** tab > **Layer 2** tab. Choose **WPA3** in the **Layer 2 Security Mode** drop-down list.
- Ensure that **PMF** is set to **Required**.

Add WLAN

General
Security
Advanced

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
☐

Fast Transition

Status
Adaptive Enabled

Over the DS
☐

Reassociation Timeout \*
20

WPA2/WPA3 Encryption

AES(CCMP128)
☒

CCMP256
☐

GCMP128
☐

GCMP256
☐

Protected Management Frame

PMF
Required

Association Comeback Timer\*
1

SA Query Time\*
200

Auth Key Mgmt

SAE
☐

FT + SAE
☐

OWE
☐

FT + 802.1x
☐

802.1x-SHA256
☒

Cancel
Apply to Device

**Figure 4.**  
WLAN Security configurations

7. Select the **WPA3 Policy**, **AES**, and **802.1x-SHA256** checkboxes, then unselect any other selected parameters.
8. Navigate to the **Security** tab > **AAA** tab and choose the preconfigured RADIUS Server Authentication List from the Authentication List drop-down list.



Add WLAN

General

Security

Advanced

Layer2

Layer3

AAA

Authentication List

dot1x

Local EAP Authentication

☐

Cancel

Apply to Device

**Figure 5.**  
WLAN AAA configuration

9. Click **Apply to Device** to save and finish the WLAN creation process.

## WPA3-Enterprise CLI configuration

The following steps will create a WLAN with WPA3-Enterprise security:

Table 3. WPA3-Enterprise CLI configuration

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>wlan wlan-name wlan-id SSID-name</code> <b>Example:</b> <code>Device(config)# wlan WPA3-Enterprise 8 WPA3-Enterprise</code>	Enters the WLAN configuration sub-mode.
Step 3	<code>no security wpa akm dot1x</code>	Disables Security Auth Key Management (AKM) 802.1X-SHA1
Step 4	<code>no security wpa wpa2</code>	Disables WPA2 security.
Step 5	<code>security wpa akm dot1x-sha256</code>	Enables Security Auth Key Management (AKM) 802.1X-SHA2
Step 6	<code>security wpa wpa3</code>	Enables WPA3 support.
Step 7	<code>security dot1x authentication-list list-name</code> <b>Example:</b> <code>Device(config-wlan)# security dot1x authentication-list dot1x</code>	Configures security authentication list for 802.1X security.
Step 8	<code>no shutdown</code>	Enables the WLAN.
Step 9	<code>end</code>	Returns to the privileged EXEC mode.

## WPA3-Enterprise 192-bit GUI configuration (optional)

For endpoints that support SuiteB192-1X encryption, refer to the client interoperability matrix section below, or reach out to the device vendor.

The following steps will create a WLAN with 192-bit WPA3-Enterprise security:

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the General tab, enter the **Profile Name** (friendly identifier). Both the SSID and WLAN ID will be populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

Add WLAN

General
Security
Advanced

Profile Name\*
WPA3-Enterprise-192B

SSID\*
WPA3-Enterprise-192B

WLAN ID\*
8

Status
ENABLED

Broadcast SSID
ENABLED

Radio Policy ⓘ

Show slot configuration

6 GHz

Status
ENABLED

WPA2 Disabled
WPA3 Enabled
Dot11ax Enabled

5 GHz

Status
ENABLED

2.4 GHz

Status
ENABLED

802.11b/g Policy
802.11b/g

Cancel
Apply to Device

**Figure 6.**  
Radio/Slot configuration

- Choose the **Security > Layer 2** tab. Choose **WPA3** in the **Layer 2 Security Mode** drop-down list.
- Ensure that **PMF** is set to **Required**.
- Disable the Fast Transition.
- Check the **WPA3 Policy**, **GCMP256**, and **SUITEB192-1X** checkboxes then unselect any other selected parameters.

Add WLAN

General
Security
Advanced

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
☐

Fast Transition

Status
Disabled

Over the DS
☐

Reassociation Timeout \*
20

WPA2/WPA3 Encryption

AES(CCMP128)
☐

CCMP256
☐

GCMP128
☐

GCMP256
☒

Auth Key Mgmt

SUITEB192-1X
☒

Protected Management Frame

PMF
Required

Association Comeback Timer\*
1

SA Query Time\*
200

Cancel
Apply to Device

**Figure 7.**  
WLAN Security, Encryption and AKM configuration

- Choose the **Security > AAA** tab, and choose the preconfigured RADIUS Server Authentication List from the **Authentication List** drop-down list.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. Under the 'AAA' sub-tab, the 'Authentication List' is set to 'dot1x' and 'Local EAP Authentication' is unchecked. The 'Apply to Device' button is highlighted.

**Figure 8.**  
Security AAA Method list configuration

10. Click **Apply to Device** to save and finish the WLAN creation process.

**Note:** SuiteB192-1X is not supported in C9120/C9105/C9115 APs and in Flexconnect Mode.

## WPA3-Enterprise 192-bit CLI configuration (optional)

The following steps will create a WLAN with 192-bit WPA3-Enterprise security:

**Table 4.** WPA3-Enterprise 192-bit encryption CLI configuration

	Command or action	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan &lt;wlan-name&gt; wlan-id &lt;SSID-name&gt;</code> <b>Example:</b> <code>Device(config)# wlan WPA3-Enterprise-192B 8 WPA3-Enterprise-192B</code>	Enters the WLAN configuration sub-mode.
<b>Step 3</b>	<code>no security ft adaptive</code>	Disables Fast Transition Adaptive support.
<b>Step 4</b>	<code>no security wpa wpa2</code>	Disables WPA2 security.

	Command or action	Purpose
<b>Step 5</b>	<code>no security wpa wpa2 ciphers aes</code>	Disables WPA2/CCMP128 support.
<b>Step 6</b>	<code>security wpa wpa2 ciphers gcmp256</code>	Enables GCMP256 support
<b>Step 7</b>	<code>no security wpa akm dot1x</code>	Disables security AKM 802.1X-SHA1 support.
<b>Step 8</b>	<code>security wpa wpa3</code>	Enables WPA3 support.
<b>Step 9</b>	<code>security dot1x authentication-list list-name</code>  <b>Example:</b>  <code>Device(config-wlan)# security dot1x authentication-list dot1x</code>	Configures security authentication list for 802.1X security.
<b>Step 10</b>	<code>no shutdown</code>	Enables the WLAN.
<b>Step 11</b>	<code>end</code>	Returns to the privileged EXEC mode.

## WPA3-Enterprise transition mode

The WPA3-Enterprise Transition Mode, aka WPA3+WPA2-Enterprise mixed-mode configuration, is used when some clients are capable of supporting only up to WPA2 and some clients are capable of supporting up to WPA3. The WPA3-capable clients will use WPA3-Enterprise's 802.1X-SHA256 AKM, while the WPA2-capable clients can use WPA2-Enterprise's 802.1X SHA1 or 802.1X-SHA256. This mode applies to both the bands 2.4GHz and 5GHz.

**Note:** This mode should be used only when necessary. For maximum security, the recommended mode is to use only WPA3 and not a mix of WPA3 and WPA2.

## WPA3-Enterprise transition mode GUI configuration

The following steps will create a WLAN with WPA3+WPA2-Enterprise mixed-mode-level security:

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the General tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID will be populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.
5. Disable the **6 GHz Radio Policy**, as it is not supported.

The screenshot shows the 'Add WLAN' configuration window with the 'General' tab selected. The 'Profile Name\*' field contains 'WPA3+WPA2-Enterprise', which has been populated to the 'SSID\*' and 'WLAN ID\*' fields. The 'Status' and 'Broadcast SSID' fields are both set to 'ENABLED' with green toggle switches. On the right, the 'Radio Policy' section is expanded, showing three frequency bands: '6 GHz' with a 'Status' of 'DISABLED', '5 GHz' with a 'Status' of 'ENABLED', and '2.4 GHz' with a 'Status' of 'ENABLED'. Below these, the '802.11b/g Policy' is set to '802.11b/g'. At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

**Figure 9.**  
Radio/Slot Policy configuration

6. Choose the **Security > Layer 2** tab. Choose **WPA2 + WPA3** in the Layer 2 Security Mode drop-down list.
7. Ensure that **PMF** is set to **Optional**.

**Add WLAN**

General **Security** Advanced

Layer2 Layer3 AAA

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

MAC Filtering ☐

Lobby Admin Access ☐

**WPA Parameters**

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input checked="" type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
		Transition Disable	<input type="checkbox"/>

**WPA2/WPA3 Encryption**

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>

**Protected Management Frame**

PMF Optional ▾

Association Comeback Timer\* 1

SA Query Time\* 200

**Fast Transition**

Status Adaptive Ena... ▾

Over the DS ☐

Reassociation Timeout \* 20

**Auth Key Mgmt**

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

**MPSK Configuration**

Enable MPSK ☐

↶ Cancel
Apply to Device

**Figure 10.**  
Security, encryption and AKM configuration

8. Scroll down to the WPA Parameters. Check the **WPA2 Policy**, **WPA3 Policy**, and Encryption **AES**, and enable the **802.1x** and **802.1x-SHA256** checkboxes.
9. Click **Apply to Device** to save and finish the WLAN creation process.



## WPA3-Enterprise transition mode CLI configuration

The following steps will create a WLAN with WPA3+WPA2-Enterprise mixed-mode-level security:

**Table 5.** WPA3-Enterprise transition mode CLI configuration

	Command	Purpose
<b>Step 1</b>	configure terminal	Enters global configuration mode.
<b>Step 2</b>	wlan wlan-name wlan-id SSID-name <b>Example:</b> Device (config)# wlan WPA3+WPA2-Enterprise 8 WPA3+WPA2-Enterprise	Enters the WLAN configuration submode.
<b>Step 3</b>	security wpa wpa3	Enables WPA3.
<b>Step 4</b>	Security wpa wpa2	Enables WPA2.
<b>Step 5</b>	security wpa akm dot1x-sha256	Enables the 802.1x SHA2 AKM.
<b>Step 6</b>	radio policy dot11 24ghz	Enables the 2.4-GHz band.
<b>Step 7</b>	radio policy dot11 5ghz	Enables the 5-GHz band
<b>Step 8</b>	no shutdown	
<b>Step 9</b>	end	

**Note:** This security combination can be used with FT enabled mode as well.

## WPA3-Enterprise transition disable mode

Ease of network upgrade – WPA2 devices has been there for many years in Wi-Fi networks and therefore it was important to have mode of deployment where both WPA2 and WPA3 devices can co-exist. This certainly helps in Wi-Fi networks to migrate gradually from WPA2 towards WPA3 based networks. Wi-Fi alliance has introduced the WPA3 Transition modes for both personal and enterprise networks. With transition mode enabled on SSID both WPA2 and WPA3 supporting devices can connect simultaneously thus paving path for gradual migration of device eco-system from WPA2 to WPA3.

Transition Disable – With above ease of network upgrade using transition mode comes the security challenge of WPA3 STAs (stations) undergoing downgrade attacks. The attackers can force WPA3 STAs downgrade to use the WPA2 and legacy security vulnerable technologies. To circumvent this problem Wi-Fi alliance has introduced “Transition Disable” indication using which AP and network operator can update WPA3 STAs that the network is fully upgraded to support the most secured algorithm defined in a transition mode. Transition Disable indication is used (in 4-way handshake during association) to disable transition modes for that network on a STA, and therefore provide protection against downgrade attacks. STAs on receiving this indication shall disable certain transition mode for subsequent connections and will disallow association without negotiation of PMF.

---

A STA implementation might enable certain transition modes (and possibly other legacy security algorithms) in a network profile.

For example, a WPA3-Personal STA might by default enable WPA3-Personal transition mode in a network profile, which enables a PSK algorithm. However, when a network (fully) supports the most secure algorithm defined in a transition mode, it can use the Transition Disable indication to disable transition modes for that network on a STA, and therefore provide protection against downgrade attacks.

On one side, this is good for security, as it will migrate all client devices to WPA3 only, as they join the transition mode WLAN, but if the network is composed of multiple physical locations, for example, some are set to WPA2, others to WPA3/WPA2 transition mode, this will cause the migrated clients to fail when moved to a location with WPA2 only.

This is a possible scenario for some large networks, with the same SSID covering different controllers/AP setups and with configurations not matching 100%. The largest example would be Edu roam, which shares the same SSID name worldwide. Setting this could have serious issues for clients moving across different network providers, so please use this with care, and only if you can ensure the same security setting is set properly across all network locations

This method is not generally recommended and should be enabled only when it is absolutely necessary.

The below section explains how to enable Transition Disable in the WLAN.

## **WPA3-Enterprise transition mode disable GUI configuration**

**The following steps will create a WLAN with WPA3-Enterprise security with Transition Disable:**

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID will be populated automatically.
4. Enable the Status and Broadcast SSID toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

Add WLAN

General
Security
Advanced

Profile Name\*
WPA3-Enterprise-TMD

SSID\*
WPA3-Enterprise-TMD

WLAN ID\*
1

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

Cancel
Apply to Device

**Figure 11.**  
Radio Policy Configuration

5. Disable the 6 GHz policy, as it is not supported.
6. Enable the **WPA2 + WPA3** option under the Security tab.
7. Scroll down to the WPA Parameters. Check the **WPA2** and **WPA3 Policy**, **AES**, and **802.1x** and **802.1x-SHA256** checkboxes as AKM.
8. Let the PMF be **Optional**.
9. Enable **Transition Disable** under WPA Parameters.

**Add WLAN**

General **Security** Advanced

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 ☒

**WPA2/WPA3 Encryption**

AES(CCMP128) ☒ CCMP256 ☐  
 GCMP128 ☐ GCMP256 ☐

**Protected Management Frame**

PMF   
 Association Comeback Timer\*   
 SA Query Time\*

**Fast Transition**

Status   
 Over the DS ☐  
 Reassociation Timeout \*

**Auth Key Mgmt**

802.1X ☒ PSK ☐  
 CCKM ☐ SAE ☐  
 FT + SAE ☐  
 FT + 802.1X ☐ FT + PSK ☐  
 802.1X-SHA256 ☒ PSK-SHA256 ☐

**MPSK Configuration**

Enable MPSK ☐

**Figure 12.**  
Security, encryption and AKM configurations

## WPA3-Enterprise transition mode disable CLI configuration

**Table 6.** WPA3-Enterprise transition mode disable CLI configuration

	Command	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan wlan-name wlan-id</code> <code>SSID-name</code> <b>Example:</b> <code>Device(config)# wlan WPA3-</code> <code>Enterprise-TMD 1 WPA3-</code> <code>Enterprise-TMD</code>	Enters the WLAN configuration submenu.
<b>Step 3</b>	<code>security wpa wpa3</code>	Enables WPA3.
<b>Step 4</b>	<code>security wpa wpa2</code>	Enables WPA2 security. PMF is optional now.

	Command	Purpose
<b>Step 5</b>	<code>security wpa wpa2 ciphers aes</code>	Enables Advanced Encryption Standard (AES)/CCMP128 ciphers.
<b>Step 6</b>	<code>security wpa akm dot1x-sha256</code>	Enables AKM 802.1x-SHA256.
<b>Step 7</b>	<code>transition-disable</code>	Enables Transition Disable.
<b>Step 8</b>	<code>radio policy dot11 5ghz</code>	Enables the 5-GHz band.
<b>Step 9</b>	<code>radio policy dot11 24ghz</code>	Enables the 2.4-GHz band.
<b>Step 10</b>	<code>no shutdown</code>	Enables the WLAN.
<b>Step 11</b>	<code>end</code>	Returns to the privileged EXEC mode.

**Note:** This security combination can be used with FT enabled mode as well.

## WPA2+WPA3-Enterprise transition mode with 6GHz

Per 6GHz standard, broadcasting a WLAN in 6GHz band is not allowed when configured with WPA2 security (applies to both WPA2 only and WPA2+WPA3 WLAN) so this essentially leads to behavior that we don't support 6GHz radio when WLAN is configured with WPA2.

This poses limitations in certain use-case when legacy clients want to support dot1x-SHA1 along with PMF optional in 5GHz on same SSID where 6GHz clients support dot1x-SHA256 AKM with PMF mandatory.

To support these deployments, the recommendation in pre-17.12.1 SW versions were to use WPA2+WPA3 transition mode with same WLAN with different profiles to support both legacy and latest 6GHz clients. The challenge with this design is roaming. The roaming between bands in this configuration is not supported and it is full roam always which is not preferred.

Starting from 17.12.1, we are supporting transition mode with pure WPA3 for 6GHz band, which allows users to enable WPA2+WPA3 in the same WLAN with 6GHz. This mode eliminates the need to create two different profiles to accommodate legacy and latest 6GHz devices. In this mode, WPA2+WPA3 transition mode can be used in 2.4GHz/5GHz and only WPA3 relevant configs will be pushed on the 6GHz band when wlan has both WPA2 and WPA3 configs.

## WPA2+WPA3-Enterprise transition mode with 6GHz – GUI Configuration

The following steps will create a WLAN with WPA2+WPA3-Enterprise transition mode with 6GHz,

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). Both the SSID and WLAN ID will be populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have Access Points (APs) associated with this profile begin broadcasting this configured WLAN.



Add WLAN

General
Security
Advanced

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
☐

Fast Transition

Status
Adaptive Ena...

Over the DS
☐

Reassociation Timeout \*
20

WPA2/WPA3 Encryption

AES(CCMP128)
☒
CCMP256
☐

GCMP128
☐
GCMP256
☐

Protected Management Frame

PMF
Optional

Association Comeback Timer\*
1

SA Query Time\*
200

Auth Key Mgmt

802.1X
☒
PSK
☐

CCKM
☐
SAE
☐

FT + SAE
☐

FT + 802.1X
☐
FT + PSK
☐

802.1X-SHA256
☒
PSK-SHA256
☐

MPSK Configuration

Enable MPSK
☐

Cancel
Apply to Device

**Figure 14.**  
Radio/Slot Configuration

8. Navigate to the Security tab > AAA tab and choose the preconfigured RADIUS Server Authentication List from the Authentication List drop-down list.
9. Click Apply to Device to save and finish the WLAN creation process.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

**Security**

Advanced

Add To Policy Tags

Layer2

Layer3

**AAA**

Authentication List

Dot1x

⌵

🔗

Local EAP Authentication

☐

⏮ Cancel

🔄

Update & Apply to Device

**Figure 15.**  
Radio/Slot Configuration

## WPA2+WPA3-Enterprise transition mode with 6GHz CLI configuration

**The following steps will create a WLAN with WPA2+WPA3-Enterprise transition mode with 6GHz,**

**Table 7.** WPA2+WPA3-Enterprise Transition Mode CLI configuration

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>wlan wlan-name wlan-id SSID-name</code> <b>Example:</b> <code>Device (config)# wlan WPA2+WPA3-TransitionMode 1 WPA2+WPA3-TransitionMode</code>	Enters the WLAN configuration submode.
Step 3	<code>security wpa wpa3</code>	Enables WPA3.
Step 4	<code>security wpa wpa2</code>	Enables WPA2.



	Command	Purpose
<b>Step 5</b>	security wpa akm dot1x-sha256	Enables the SHA2 AKM.
<b>Step 6</b>	security wpa akm dot1x	Enables the SHA1 AKM.
<b>Step 7</b>	radio policy dot11 6ghz	Enables the 6-GHz band
<b>Step 8</b>	radio policy dot11 24ghz	Enables the 2.4-GHz band.
<b>Step 9</b>	radio policy dot11 5ghz	Enables the 5-GHz band
<b>Step 10</b>	no shutdown	
<b>Step 11</b>	end	

## WPA2+WPA3-Enterprise transition mode with 6GHz CLI Output

```
#show wlan summary
Number of WLANs: 1
ID Profile Name          SSID   Status 2.4GHz/5GHz Security          6GHz Security
-----
1 WPA2+WPA3-TransitionMode UP    [WPA2 + WPA3] [802.1x] [AES] [PMF 802.1X] [WPA3] [AES] [PMF 802.1X]
```

**Note:** This configuration is supported in GCM256 encryption SuiteB192-1x too. When WPA2+WPA3 transition mode with pure WPA3 is enabled along with 192-bit encryption, the bands operate as below,

2.4GHz and 5GHz: WPA2 + WPA3-SUITEB-192-1X-GCMP256

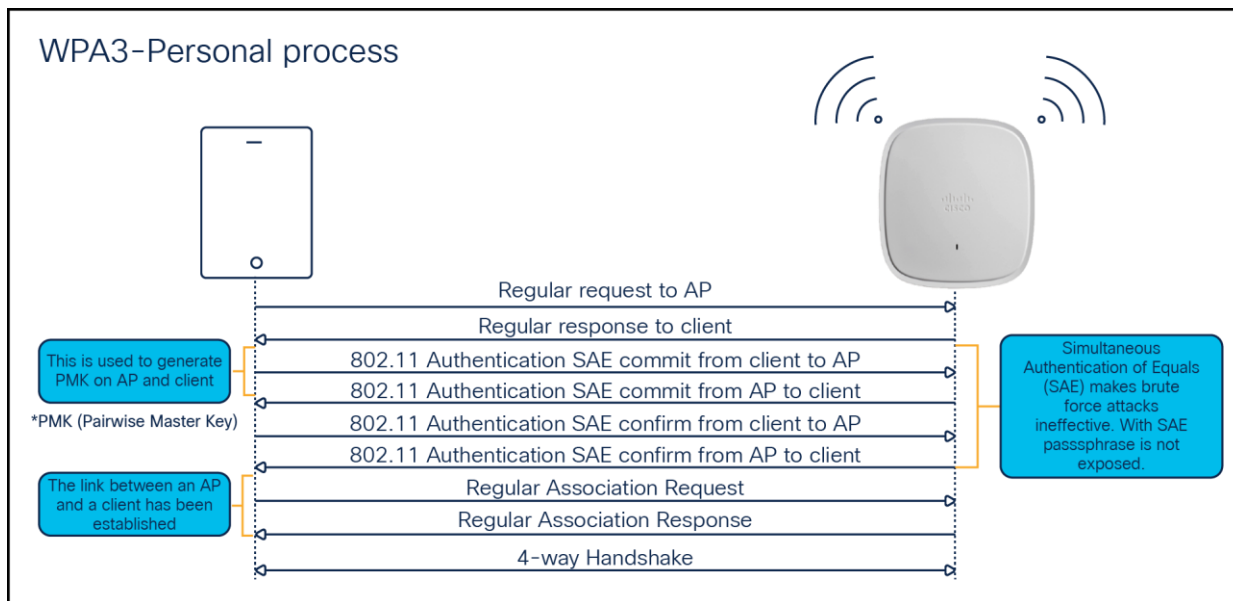
6GHz: WPA3-SUITEB-192-1X-GCMP256

## WPA3-Personal

WPA3-Personal uses 128-bit cryptographic-strength encryption with a password-based authentication method through SAE for user authentication purposes. In addition, unlike WPA2-Personal, WPA3-Personal heightens network security against offline dictionary attacks by limiting password guesses and requiring users to interact with a live network every time they do so. This requirement makes hacking into a network much more time-consuming and dissuades attempts at a brute force attack.

WPA3-Personal provides the following key advantages:

- Creates a shared secret that is different for each SAE authentication.
- Protects against brute force “dictionary” attacks and passive attacks.
- Provides forward secrecy.



**Figure 16.**  
WPA3-Personal endpoint and network handshake process

## WPA3-Personal GUI configuration

The following steps will create a WLAN with WPA3-Personal-level security:

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID will be populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

**Add WLAN**

**General**   Security   Advanced

Profile Name\*

SSID\*

WLAN ID\*

Status ENABLED ☒

Broadcast SSID ENABLED ☒

**Radio Policy** ⓘ

[Show slot configuration](#)

**6 GHz**

Status ENABLED ☒

- ✓ WPA2 Disabled
- ✓ WPA3 Enabled
- ✓ Dot11ax Enabled

**5 GHz**

Status ENABLED ☒

**2.4 GHz**

Status ENABLED ☒

802.11b/g Policy

**Figure 17.**  
WPA3 Personal Radio/Slot configuration

5. Choose the **Security > Layer 2** tab. Choose **WPA3** in the **Layer 2 Security Mode** drop-down list.
6. Ensure that **PMF** is set to **Required**.
7. Disable Fast Transition.
8. Scroll down to the WPA Parameters. Check the **WPA3 Policy**, **AES**, and **SAE** checkboxes.
9. Enter the **Pre-Shared Key** and choose the **PSK format** from the PSK Format drop-down list and the PSK type from the **PSK Type** drop-down list.

Add WLAN

General
Security
Advanced

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 ☐

Fast Transition

Status 

Disabled

Over the DS ☐

Reassociation Timeout \* 

20

WPA2/WPA3 Encryption

AES(CCMP128) ☒
CCMP256 ☐

GCMP128 ☐
GCMP256 ☐

Protected Management Frame

PMF 

Required

Association Comeback Timer\* 

1

SA Query Time\* 

200

Auth Key Mgmt

SAE ☒
FT + SAE ☐

OWE ☐
FT + 802.1x ☐

802.1x-SHA256 ☐

Anti Clogging Threshold\* 

1500

Max Retries\* 

5

Retransmit Timeout\* 

400

PSK Format 

ASCII

PSK Type 

Unencrypted

Pre-Shared Key\* 

.....

SAE Password Element 

Both H2E and HnP

Cancel
Apply to Device

**Figure 18.**  
WPA3 SAE AKM configuration

- Click **Apply to Device** to save and finish the WLAN creation process.

**Note:** If only the 6-GHz band is used, the SAE Password Element supported is Hash to Element (H2E). Hunting and Pecking (HnP) cannot be used in a 6-GHz-only network. If both 5 GHz and 2.4 GHz are used, H2E and HnP can be used as the SAE Password Element.

## WPA3-Personal CLI configuration

The following steps will create a WLAN with WPA3-Personal-level security:

**Table 8.** WPA3-Personal CLI configuration

	Command	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan wlan-name wlan-id SSID-name</code>  <b>Example:</b> <code>Device(config)# wlan WPA3- Personal 8 WPA3-Personal</code>	Enters the WLAN configuration sub-mode.
<b>Step 3</b>	<code>no security wpa akm dot1x</code>	Disables security AKM 802.1x.
<b>Step 4</b>	<code>no security ft over-the-ds</code>	Disables Fast Transition over the data source on the WLAN.
<b>Step 5</b>	<code>no security ft</code>	Disables 802.11r Fast Transition on the WLAN.
<b>Step 6</b>	<code>no security wpa wpa2</code>	Disables WPA2 security. PMF is disabled now.
<b>Step 7</b>	<code>security wpa wpa2 ciphers aes</code>	Enables Advanced Encryption Standard (AES)/CCMP128 ciphers.
<b>Step 8</b>	<code>security wpa psk set-key ascii value preshared-key</code>  <b>Example:</b> <code>Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123</code>	Specifies a preshared key.
<b>Step 9</b>	<code>security wpa wpa3</code>	Enables WPA3 support.  <b>Note:</b> If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.
<b>Step 10</b>	<code>security wpa akm sae</code>	Enables AKM SAE support.
<b>Step 11</b>	<code>security wpa akm sae pwe h2e/hnp/both</code>	Chooses the Password Element.
<b>Step 12</b>	<code>no shutdown</code>	Enables the WLAN.
<b>Step 13</b>	<code>End</code>	Returns to the privileged EXEC mode.

## WPA3-Personal SAE hash-to-element method for password element generation

The following steps will create a WLAN with WPA3-Personal-level security with H2E for password element generation:

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID will be populated automatically.
4. Enable the Status and Broadcast SSID toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.
5. Choose the **Security > Layer 2** tab. Choose **WPA3** in the **Layer 2 Security Mode** drop-down list.

The screenshot shows the 'Add WLAN' configuration window with the 'General' tab selected. The 'Profile Name\*' is 'WPA3-Personal-H2E', 'SSID\*' is 'WPA3-Personal-H2E', and 'WLAN ID\*' is '1'. The 'Status' and 'Broadcast SSID' are both enabled. The 'Radio Policy' section shows three frequency bands: 6 GHz, 5 GHz, and 2.4 GHz. The 6 GHz band is enabled and shows 'WPA2 Disabled', 'WPA3 Enabled', and 'Dot11ax Enabled'. The 5 GHz and 2.4 GHz bands are also enabled. The 2.4 GHz band has a 'Policy' dropdown set to '802.11b/g'. At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

Field	Value
Profile Name*	WPA3-Personal-H2E
SSID*	WPA3-Personal-H2E
WLAN ID*	1
Status	ENABLED
Broadcast SSID	ENABLED

Frequency	Status	Details
6 GHz	ENABLED	WPA2 Disabled, WPA3 Enabled, Dot11ax Enabled
5 GHz	ENABLED	
2.4 GHz	ENABLED	Policy: 802.11b/g

**Figure 19.**  
Radio/Slot Policy configuration

6. Ensure that **PMF** is set to **Required**.
7. Disable Fast Transition.
8. Scroll down to the WPA Parameters. Check the **WPA3 Policy**, **AES**, and **SAE** checkboxes.
9. Enter the **Pre-Shared Key** and choose the PSK format from the **PSK Format** drop-down list and the PSK type from the **PSK Type** drop-down list.

10. Enable **Hash to Element Only** from the SAE Password Element drop-down.

The screenshot shows the 'Add WLAN' configuration window with the 'Security' tab selected. Under the 'Layer2' sub-tab, the 'WPA3' radio button is selected. The 'SAE Password Element' dropdown is set to 'Hash to Element Only'. Other visible settings include 'WPA Parameters' (WPA3 Policy checked), 'WPA2/WPA3 Encryption' (AES/CCMP128 checked), 'Protected Management Frame' (PMF Required), 'Fast Transition' (Status Disabled), and 'Auth Key Mgmt' (SAE checked).

Section	Option	Status
Security Mode	WPA + WPA2	Unselected
	WPA2 + WPA3	Unselected
	WPA3	Selected
	Static WEP	Unselected
	None	Unselected
MAC Filtering	MAC Filtering	Unselected
	Lobby Admin Access	Unselected
WPA Parameters	WPA Policy	Unselected
	WPA2 Policy	Unselected
	WPA3 Policy	Selected
	Transition Disable	Unselected
WPA2/WPA3 Encryption	AES(CCMP128)	Selected
	CCMP256	Unselected
	GCMP128	Unselected
	GCMP256	Unselected
Protected Management Frame	PMF	Required
	Association Comeback Timer*	1
	SA Query Time*	200
	Fast Transition	Status
Auth Key Mgmt	SAE	Selected
	OWE	Unselected
	802.1x-SHA256	Unselected
	FT + SAE	Unselected
	FT + 802.1x	Unselected
	Anti Clogging Threshold*	1500
	Max Retries*	5
	Retransmit Timeout*	400
	PSK Format	ASCII
	PSK Type	Unencrypted
SAE Password Element	Hash to Element Only	

**Figure 20.**  
Security and AKM Password Element configuration

**Note:** If only the 6-GHz band is used, the SAE Password Element supported is H2E. HnP cannot be used in a 6-GHz-only network. If both 5 GHz and 2.4 GHz are used, H2E and HnP can be used as the SAE Password Element.

## WPA3-Personal SAE hash-to-element method for password element generation CLI configuration

The following steps will create a WLAN with WPA3-Personal-level security with H2E for password element generation:

**Table 9.** WPA3-Personal SAE hash-to-element CLI configuration

	Command	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan wlan-name wlan-id SSID-name</code>  <b>Example:</b>  <code>Device(config)# wlan WPA3- Personal-H2E 1 WPA3- Personal-H2E</code>	Enters the WLAN configuration submode.
<b>Step 3</b>	<code>no security wpa akm dot1x</code>	Disables security AKM 802.1X.
<b>Step 4</b>	<code>security wpa wpa3</code>	Enables WPA3.
<b>Step 5</b>	<code>no security ft</code>	Disables 802.11r Fast Transition on the WLAN.
<b>Step 6</b>	<code>no security wpa wpa2</code>	Disables WPA2 security. PMF is disabled now.
<b>Step 7</b>	<code>security wpa wpa2 ciphers aes</code>	Enables AES/CCMP128 ciphers.
<b>Step 8</b>	<code>security wpa psk set-key ascii value preshared-key</code>  <b>Example:</b>  <code>Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123</code>	Specifies a preshared key.
<b>Step 9</b>	<code>security wpa akm sae</code>	Enables AKM SAE support.
<b>Step 10</b>	<code>security wpa akm sae pwe h2e</code>	Enables H2E for password element generation.
<b>Step 11</b>	<code>no shutdown</code>	Enables the WLAN.
<b>Step 12</b>	<code>End</code>	Returns to the privileged EXEC mode.



## WPA3-Personal SAE with fast transition enabled

Starting from Cisco IOS® XE version 17.9.1, WPA3-Personal SAE with Fast Transition (SAE-FT) is supported. Follow the instructions below to configure the WLAN for WPA3 SAE-FT.

**The following steps will create a WLAN with WPA3-Personal-level SAE security with Fast Transition enabled:**

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the General tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID will be populated automatically.
4. Enable the Status and Broadcast SSID toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.
5. Choose the **Security > Layer 2** tab. Choose **WPA3** in the **Layer 2 Security Mode** drop-down list.

The screenshot shows the 'Add WLAN' configuration window with the following details:

- General Tab:**
  - Profile Name\*: WPA3-Personal-H2E
  - SSID\*: WPA3-Personal-H2E
  - WLAN ID\*: 1
  - Status: ENABLED (toggle)
  - Broadcast SSID: ENABLED (toggle)
- Radio Policy:**
  - 6 GHz: Status ENABLED (toggle). Details: WPA2 Disabled, WPA3 Enabled, Dot11ax Enabled.
  - 5 GHz: Status ENABLED (toggle).
  - 2.4 GHz: Status ENABLED (toggle).
  - 802.11b/g Policy: 802.11b/g (dropdown).

Buttons at the bottom: Cancel, Apply to Device.

**Figure 21.**  
Radio Policy configuration

6. Ensure that **PMF** is set to **Required**.
7. Enable Fast Transition.
8. Scroll down to the WPA Parameters. Check the **WPA3 Policy**, **AES**, and **FT + SAE** checkbox.
9. Enter the **Pre-Shared Key** and choose the PSK format from the **PSK Format** drop-down list and the PSK type from the **PSK Type** drop-down list.
10. Enable **Hash to Element Only** or **HnP** or **both** from the SAE Password Element drop-down.

**Add WLAN**

General **Security** Advanced

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 ☐

**WPA2/WPA3 Encryption**

AES(CCMP128) ☒ CCMP256 ☐

GCMP128 ☐ GCMP256 ☐

**Protected Management Frame**

PMF

Association Comeback Timer\*

SA Query Time\*

**Fast Transition**

Status

Over the DS ☐

Reassociation Timeout\*

**Auth Key Mgmt**

SAE ☐ FT + SAE ☒

OWE ☐ FT + 802.1x ☐

802.1x-SHA256 ☐

Anti Clogging Threshold\*

Max Retries\*

Retransmit Timeout\*

PSK Format

PSK Type

Pre-Shared Key\*

SAE Password Element ⓘ

**Figure 22.**  
WPA3 SAE with FT Enabled

## WPA3-Personal SAE with fast transition enabled CLI configuration

The following steps will create a WLAN with WPA3-Personal-level security with Fast Transition enabled:

**Table 10.** WPA3-Personal SAE FT CLI configuration

	Command	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan wlan-name wlan-id SSID-name</code> <b>Example:</b> <code>Device(config)# wlan WPA3-Personal-H2E 1 WPA3-Personal-H2E</code>	Enters the WLAN configuration sub-mode.
<b>Step 3</b>	<code>no security wpa akm dot1x</code>	Disables security AKM 802.1X.
<b>Step 4</b>	<code>security wpa wpa3</code>	Enables WPA3.
<b>Step 5</b>	<b><code>security ft</code></b>	Enables 802.11r Fast Transition on the WLAN.
<b>Step 6</b>	<code>no security wpa wpa2</code>	Disables WPA2 security. PMF is disabled now.
<b>Step 7</b>	<code>security wpa wpa2 ciphers aes</code>	Enables AES/CCMP128 ciphers.
<b>Step 8</b>	<code>security wpa psk set-key ascii value preshared-key</code> <b>Example:</b> <code>Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123</code>	Specifies a preshared key.
<b>Step 9</b>	<code>security wpa akm sae</code>	Enables AKM SAE support.
<b>Step 10</b>	<code>Security wpa akm ft sae</code>	Enables FT SAE
<b>Step 11</b>	<b><code>security wpa akm sae pwe h2e</code></b>	Enables H2E for password element generation.
<b>Step 12</b>	<code>no shutdown</code>	Enables the WLAN.
<b>Step 13</b>	<code>End</code>	Returns to the privileged EXEC mode.

## WPA3-Personal transition mode

The WPA3-Personal Transition Mode, aka WPA2+WPA3-Personal mixed-mode configuration, is used when some clients are capable of supporting only WPA2 and some clients are capable of supporting up to WPA3. The WPA3-capable clients will use WPA3-Personal's SAE, while the WPA2-capable clients will use WPA2-Personal's PSK. This mode applies to both the bands 2.4GHz and 5GHz.

**Note:** This mode should be used only when necessary. For maximum security, the recommended mode is to use only WPA3 and not a mix of WPA3 and WPA2.

**The following steps will create a WLAN with WPA3+WPA2-Personal mixed-mode-level security:**

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the General tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID will be populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons to have Aps associated with this profile begin broadcasting this configured WLAN.
5. Disable the **6 GHz** band.

The screenshot shows the 'Add WLAN' configuration window with the 'General' tab selected. The 'Profile Name' is 'WPA3+WPA2-Personal', the 'SSID' is 'WPA3+WPA2-Personal', and the 'WLAN ID' is '8'. The 'Status' and 'Broadcast SSID' toggles are both enabled. The 'Radio Policy' section shows the 6 GHz band disabled, 5 GHz band enabled, and 2.4 GHz band enabled. The 802.11b/g Policy is set to 802.11b/g. The 'Apply to Device' button is visible at the bottom right.

**Figure 23.**  
Radio configuration for Transition Mode

6. Choose the Security > Layer 2 tab. Choose WPA2 + WPA3 in the Layer 2 Security Mode drop-down list.
7. Ensure that **PMF** is set to **Optional**.

Add WLAN

General
Security
Advanced

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
☐

Fast Transition

Status
Disabled

Over the DS
☐

Reassociation Timeout \*
20

WPA2/WPA3 Encryption

AES(CCMP128)
☒
CCMP256
☐

GCMP128
☐
GCMP256
☐

Protected Management Frame

PMF
Optional

Association Comeback Timer\*
1

SA Query Time\*
200

Auth Key Mgmt

802.1x
☐
PSK
☒

CCKM
☐
SAE
☒

FT + SAE
☐
OWE
☐

FT + 802.1x
☐
FT + PSK
☐

802.1x-SHA256
☐

Anti Clogging Threshold\*
1500

Max Retries\*
5

Retransmit Timeout\*
400

PSK Format
ASCII

PSK Type
Unencrypted

Pre-Shared Key\*
.....

SAE Password Element ⓘ
Both H2E and HnP

MPSK Configuration

Enable MPSK
☐

Cancel
Apply to Device

**Figure 24.**  
Security, Encryption and AKM configuration

8. Scroll down to the WPA Parameters. Check the **WPA2 Policy, WPA3 Policy, AES, PSK, and SAE** checkboxes.
9. Enter the Pre-Shared Key and choose the PSK format from the PSK Format drop-down list and the PSK type from the PSK Type drop-down list.
10. Click **Apply to Device** to save and finish the WLAN creation process.

## WPA3 Personal transition mode CLI configuration

The following steps will create a WLAN with WPA3+WPA2-Personal mixed-mode-level security:

**Table 11.** WPA3 Personal transition mode CLI configuration

	Command	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan wlan-name wlan-id SSID-name</code>  <b>Example:</b> <code>Device(config)# wlan WPA3+WPA2-Personal 1 WPA3+WPA2-Personal</code>	Enters the WLAN configuration submode.
<b>Step 3</b>	<code>no security wpa akm dot1x</code>	Disables security AKM 802.1X.
<b>Step 4</b>	<code>no security ft</code>	Disables 802.11r Fast Transition on the WLAN.
<b>Step 5</b>	<code>security wpa wpa2 ciphers aes</code>	Configures the WPA2 cipher.  <b>Note:</b> You can check whether the cipher is configured by using the <b>no security wpa wpa2 ciphers aes</b> command. If the cipher is not reset, configure the cipher.
<b>Step 6</b>	<code>security wpa psk set-key ascii 0 Cisco123</code>	Specifies a preshared key.
<b>Step 7</b>	<code>security wpa wpa3</code>	Enables WPA3 support.  <b>Note:</b> If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.
<b>Step 8</b>	<code>security wpa akm sae</code>	Enables AKM SAE support.
<b>Step 9</b>	<code>security wpa akm psk</code>	Enables AKM PSK support.
<b>Step 10</b>	<code>radio policy dot11 24ghz</code>	Enables the 2.4-GHz band
<b>Step 11</b>	<code>radio policy dot11 5ghz</code>	Enables the 5-GHz band
<b>Step 12</b>	<code>no shutdown</code>	Enables the WLAN.
<b>Step 13</b>	<code>end</code>	Returns to the privileged EXEC mode.

---

## WPA3-Personal transition mode disable

Transition Disable is an indication from an AP to a STA, that the STA is to disable certain transition modes for subsequent connections to the AP's network.

A STA implementation might enable certain transition modes (and possibly other legacy security algorithms) in a network profile. For example, a WPA3-Personal STA might by default enable WPA3-Personal transition mode in a network profile, which enables a PSK algorithm. However, when a network (fully) supports the most secure algorithm defined in a transition mode, it can use the Transition Disable indication to disable transition modes for that network on a STA, and therefore provide protection against downgrade attacks.

**Note:** An AP that uses Transition Disable indication is not required to disable the corresponding transition mode(s) on its own BSS. For example, the APs in a WPA3-Personal network might use Transition Disable indication to ensure that all STAs that support WPA3-Personal are protected against downgrade attack, but while still enabling WPA3-Personal transition mode on its BSS so that legacy STAs can connect.

On one side, this is good for security, as it will migrate all client devices to WPA3 only, as they join the transition mode WLAN, but if the network is composed of multiple physical locations, for example, some are set to WPA2, others to WPA3/WPA2 transition mode, this will cause the migrated clients to fail when moved to a location with WPA2 only.

This is a possible scenario for some large networks, with the same SSID covering different controllers/AP setups and with configurations not matching 100%. The largest example would be Edu roam, which shares the same SSID name worldwide. Setting this could have serious issues for clients moving across different network providers, so please use this with care, and only if you can ensure the same security setting is set properly across all network locations.

**Note:** This method is not generally recommended and should be enabled only when it is absolutely necessary.

The below section explains how to enable Transition Disable in the WLAN.

## WPA3-Personal transition mode disable GUI configuration

The following steps will create a WLAN with WPA3-Personal-level security with Transition Disable:

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID will be populated automatically.
4. Enable the Status and Broadcast SSID toggle buttons to have APs associated with this profile begin broadcasting this configured WLAN.

**Add WLAN**

**General**   Security   Advanced

Profile Name\*

SSID\*

WLAN ID\*

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

**Figure 25.**  
Radio/Slot configuration for Transition disable mode

5. Disable the **6-GHz** band.
6. Enable the **WPA2+WPA3** option under the Security tab.
7. Disable Fast Transition.
8. Scroll down to the WPA Parameters. Check the **WPA2** and **WPA3 Policy**, **AES**, and **SAE** and **PSK** checkboxes as AKM.
9. Enter the **Pre-Shared Key** and choose the PSK format from the PSK Format drop-down list and the PSK type from the **PSK Type** drop-down list.
10. Let the **PMF** be Optional.
11. Enable the **Transition Disable** option in WPA Parameters.



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

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	<input type="checkbox"/>	WPA2 Policy	<input checked="" type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
		Transition Disable	<input checked="" type="checkbox"/>

- WPA2/WPA3 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>


## Protected Management Frame

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

- Fast Transition

Status	Disabled
Over the DS	<input type="checkbox"/>
Reassociation Timeout *	20

- Auth Key Mgmt

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

Anti Clogging Threshold\*

1500

Max Retries\*

5

Retransmit Timeout\*

400

PSK Format


ASCII ▼

PSK Type

Unencrypted ▼

Pre-Shared Key\*

\*\*\*\*\*

SAE Password Element 

Both H2E and... ▼

- MPSK Configuration

Enable MPSK ☐

**Figure 26.**

### Security and AKM configuration for Transition Disable mode

## WPA3-Personal transition mode disable CLI configuration

**Table 12.** WPA3-Personal transition mode disable CLI configuration

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>wlan wlan-name wlan-id SSID-name</code>  <b>Example:</b>  <code>Device(config)# wlan WPA3- Personal-TMD 1 WPA3- Personal-TMD</code>	Enters the WLAN configuration sub-mode.
Step 3	<code>no security wpa akm dot1x</code>	Disables security AKM 802.1X.
Step 4	<code>security wpa wpa3</code>	Enables WPA3.
Step 5	<code>no security ft</code>	Disables 802.11r Fast Transition on the WLAN.
Step 6	<code>security wpa wpa2</code>	Enables WPA2 security. PMF is optional now.
Step 7	<code>security wpa wpa2 ciphers aes</code>	Enables AES/CCMP128 ciphers.
Step 8	<code>security wpa psk set-key ascii value preshared-key</code>  <b>Example:</b>  <code>Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123</code>	Specifies a preshared key.
Step 9	<code>security wpa akm sae</code>	Enables AKM SAE support.
Step 10	<code>security wpa akm psk</code>	Enables AKM PSK.
Step 11	<b>transition-disable</b>	Enables Transition Disable.
Step 11	<code>radio policy dot11 24ghz</code>	Enables 2.4-GHz.
Step 12	<code>radio policy dot11 5ghz</code>	Enables 5 GHz
Step 13	<code>no shutdown</code>	Enables the WLAN.
Step 14	<code>End</code>	Returns to the privileged EXEC mode.

---

## WPA2+WPA3-Personal transition mode with 6GHz

Per 6GHz standard, broadcasting a WLAN in 6GHz band is not allowed when configured with WPA2 security (applies to both WPA2 only and WPA2+WPA3 WLAN) so this essentially leads to behavior that we don't support 6GHz radio when WLAN is configured with WPA2.

We do have use case like 2.4GHz/5 GHz can be on PSK/SAE AKM with PMF optional and 6GHz with SAE AKM for WPA3 on same SSID, which is not a valid configuration pre-17.12.1.

To support these deployments, the recommendation in pre-17.12.1 SW versions were to use WPA2+WPA3 transition mode with same WLAN with different profiles to support both legacy and latest 6GHz clients. The challenge with this design is roaming. The roaming b/w bands in this configuration is not supported and it is full roam always which is not preferred.

Starting from 17.12.1, we are supporting transition mode with pure WPA3 for 6GHz band, which allows users to enable WPA2+WPA3 in the same WLAN with 6GHz. This mode eliminates the need to create two different profiles to accommodate legacy and latest 6GHz devices. In this mode, WPA2+WPA3 transition mode can be used in 2.4GHz/5GHz and only WPA3 relevant configs will be pushed on the 6GHz band when wlan has both WPA2 and WPA3 configs.

## WPA2+WPA3-Personal transition mode with 6GHz GUI configuration

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). Both the SSID and WLAN ID will be populated automatically.
4. Enable the Status and Broadcast SSID toggle buttons to have Access Points (APs) associated with this profile begin broadcasting this configured WLAN.

Add WLAN

General

Security

Advanced

Profile Name\*

WPA2+WPA3-PSK-TM

SSID\*

WPA2+WPA3-PSK-TM

WLAN ID\*

1

Status

ENABLED

Broadcast SSID

ENABLED

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

Cancel

Apply to Device

**Figure 27.**  
Radio/Slot Configuration

- Click the Security tab > Layer 2 tab. Choose WPA2+WPA3 in the Layer 2 Security Mode drop-down list.
- Ensure that PMF is set to Optional. {Though PMF is optional, with WPA3 configuration, it will be considered required for the 6GHz band}

Add WLAN

General
Security
Advanced

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
☐

Fast Transition

Status
Disabled

Over the DS
☐

Reassociation Timeout \*
20

WPA2/WPA3 Encryption

AES(CCMP128)
☒
CCMP256
☐

GCMP128
☐
GCMP256
☐

Protected Management Frame

PMF
Optional

Association Comeback Timer\*
1

SA Query Time\*
200

Auth Key Mgmt

802.1X
☐
PSK
☒

CCKM
☐
SAE
☒

FT + SAE
☐
FT + 802.1X
☐

FT + PSK
☐
802.1X-SHA256
☐

PSK-SHA256
☐

Anti Clogging Threshold\*
1500

Max Retries\*
5

Retransmit Timeout\*
400

PSK Format
ASCII

PSK Type
Unencrypted

Pre-Shared Key\*
.....

SAE Password Element ⓘ
Both H2E and...

MPSK Configuration

Enable MPSK
☐

Cancel
Apply to Device

**Figure 28.**  
Configuration

7. Select the WPA2 and WPA3 Policy in WPA Parameters, AES(CCMP128) in WPA2/WPA3 encryption, and enable PSK and SAE checkboxes, then unselect any other selected parameters.
8. Input the Shared key.
9. Click Apply to Device to save and finish the WLAN creation process.

## WPA2+WPA3-Personal transition mode with 6GHz CLI configuration

The following steps will create a WLAN with WPA3+WPA2-Personal transition mode with 6GHz enabled.

**Table 13.** WPA2+WPA3 Transition mode with pure 6GHz CLI configuration

	Command	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan wlan-name wlan-id SSID-name</code>  <b>Example:</b> <code>Device(config)# wlan WPA2+WPA3-PTM 1 WPA2+WPA3-PTM</code>	Enters the WLAN configuration submenu.
<b>Step 3</b>	<code>no security wpa akm dot1x</code>	Disables security AKM for 802.1X.
<b>Step 4</b>	<code>no security ft</code>	Disables 802.11r Fast Transition on the WLAN.
<b>Step 5</b>	<code>security wpa wpa2 ciphers aes</code>	Configures the WPA2 cipher.  <b>Note:</b> You can check whether the cipher is configured by using the <code>no security wpa wpa2 ciphers aes</code> command. If the cipher is not reset, configure the cipher.
<b>Step 6</b>	<code>security wpa psk set-key ascii 0 Cisco123</code>	Specifies a preshared key.
<b>Step 7</b>	<code>security wpa wpa3</code>	Enables WPA3 support.  <b>Note:</b> If both WPA2 and WPA3 are supported (SAE and PSK together), it is optional to configure PMF. However, you cannot disable PMF. For WPA3, PMF is mandatory.
<b>Step 8</b>	<code>security wpa akm sae</code>	Enables AKM SAE support.
<b>Step 9</b>	<code>security wpa akm psk</code>	Enables AKM PSK support.
<b>Step 10</b>	<code>radio policy dot11 6ghz</code>	Enables the 6-GHz band
<b>Step 11</b>	<code>radio policy dot11 24ghz</code>	Enables the 2.4-GHz band
<b>Step 12</b>	<code>radio policy dot11 5ghz</code>	Enables the 5-GHz band
<b>Step 13</b>	<code>no shutdown</code>	Enables the WLAN.
<b>Step 14</b>	<code>end</code>	Returns to the privileged EXEC mode.

### WPA2+WPA3-Personal transition mode with 6GHz CLI Output

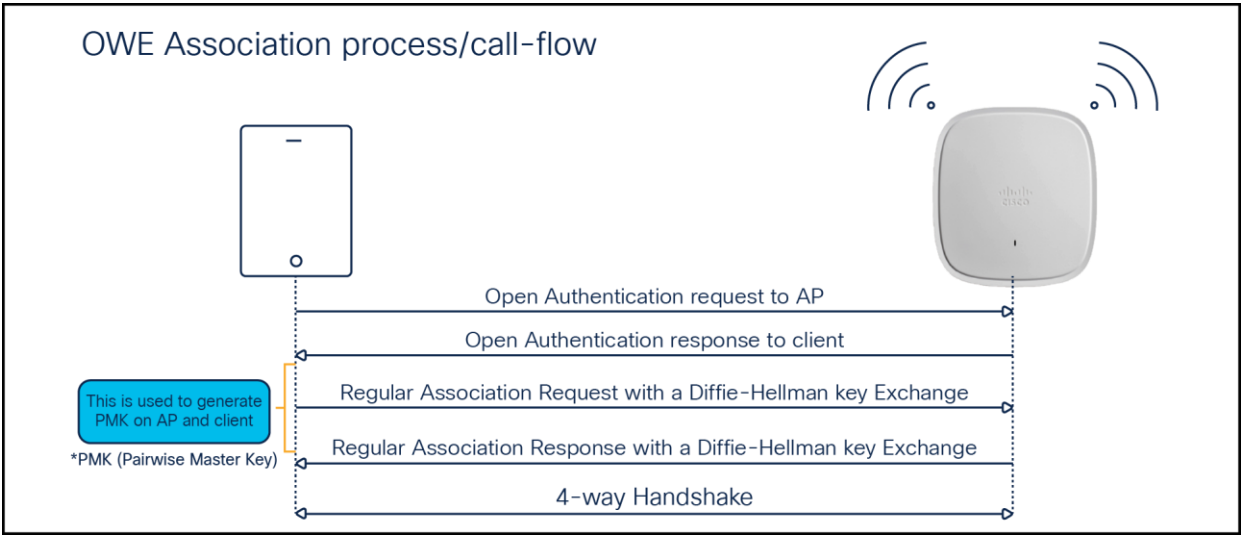
```
#show wlan summary
```

Number of WLANs: 1

ID	Profile Name	SSID	Status	2.4GHz/5GHz Security	6GHz Security
1	WPA2+WPA3-PTM	UP	[WPA2 + WPA3] [PSK] [SAE] [AES]	[WPA3] [SAE] [AES]	

### OWE

OWE is a security method paired with an open-security wireless network to provide it with encryption to protect the network from eavesdroppers. With OWE, the client and AP perform a Diffie-Hellman key exchange during the endpoint association packet exchange and use the resulting PMK to conduct the 4-way handshake. Being associated with open-security wireless networks, OWE can be used with regular open networks as well as those associated with captive portals.



**Figure 29.**  
OWE endpoint and network handshake process

## WPA3 OWE GUI configuration

The following steps will create a WLAN with WPA3 OWE security:

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and the WLAN ID will be populated automatically.
4. Enable the **Status** and **Broadcast SSID** toggle buttons.

The screenshot shows the 'Add WLAN' configuration window with the 'General' tab selected. The 'Profile Name\*' field is 'WPA3-OWE', 'SSID\*' is 'WPA3-OWE', and 'WLAN ID\*' is '1'. The 'Status' and 'Broadcast SSID' toggles are both 'ENABLED'. The 'Radio Policy' section shows three frequency bands: 6 GHz, 5 GHz, and 2.4 GHz. Each band has a 'Status' toggle set to 'ENABLED'. The 6 GHz band also shows a list of features: WPA2 Disabled, WPA3 Enabled, and Dot11ax Enabled. The '802.11b/g Policy' is set to '802.11b/g'. At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

**Figure 30.**  
WPA3 OWE Radio/Slot configuration

5. Choose the **Security > Layer 2** tab. Choose **WPA3** in the **Layer 2 Security Mode** drop-down list.
6. Select **Disabled** from the **Fast Transition** drop-down list.



Add WLAN

General
Security
Advanced

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
☐

Fast Transition

Status
Disabled

Over the DS
☐

Reassociation Timeout \*
20

WPA2/WPA3 Encryption

AES(CCMP128)
☒

CCMP256
☐

GCMP128
☐

GCMP256
☐

Protected Management Frame

PMF
Required

Association Comeback Timer\*
1

SA Query Time\*
200

Auth Key Mgmt

SAE
☐

FT + SAE
☐

OWE
☒

FT + 802.1x
☐

802.1x-SHA256
☐

Transition Mode WLAN ID
1-4096

Cancel
Apply to Device

**Figure 31.**  
OWE AKM configuration

- Check the **WPA3 Policy**, **AES (CCMP 128)**, and **OWE** checkboxes. Uncheck any other selected parameters.
- Click **Apply to Device** to save and finish the WLAN creation process.

## WPA3 OWE CLI configuration

The following steps will create a WLAN with WPA3 OWE security:

Table 14. WPA3 OWE CLI configuration

	Command	Purpose
<b>Step 1</b>	<code>configure terminal</code> <b>Example:</b> <code>Device# configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan wlan-name wlan-id SSID-name</code> <b>Example:</b> <code>Device(config)# wlan WPA3 1 WPA3</code>	Enters the WLAN configuration sub-mode.
<b>Step 3</b>	<code>no security ft over-the-ds</code>	Disables Fast Transition over the data source on the WLAN.
<b>Step 4</b>	<code>no security ft</code>	Disables 802.11r Fast Transition on the WLAN.
<b>Step 5</b>	<code>no security wpa akm dot1x</code>	Disables security AKM for 802.1X.
<b>Step 6</b>	<code>no security wpa wpa2</code>	Disables WPA2 security. PMF is disabled now.
<b>Step 7</b>	<code>security wpa wpa2 ciphers aes</code>	Enables WPA2 ciphers for AES. <b>Note:</b> The ciphers for WPA2 and WPA3 are common.
<b>Step 8</b>	<code>security wpa wpa3</code>	Enables WPA3 support.
<b>Step 9</b>	<code>security wpa akm owe</code>	Enables WPA3 OWE support.
<b>Step 10</b>	<code>no shutdown</code>	Enables the WLAN.
<b>Step 11</b>	<code>End</code>	Returns to the privileged EXEC mode.

## WPA3 OWE transition mode GUI configuration

The Transition mode was introduced to the public since not all devices support enhanced open capability (refer to the device interoperability matrix). Transition mode is designed to make the enhanced open OWE mode more adaptable. The Wi-Fi Alliance recommends using this strategy to implement an enhanced open wireless network in an environment where not all devices support this mode. The OWE Transition mode requires a separate open SSID configured with properties similar to those of the enhanced open OWE SSID. Both OWE and open WLAN have a corresponding Transition mode WLAN ID, which means that the OWE WLAN has a Transition mode ID set to the open WLAN ID, and the open WLAN has a Transition mode ID set to the OWE WLAN ID.

**Part 1 - The following steps will create a hidden WLAN with WPA3 OWE security:**

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier). The SSID and WLAN ID will be populated automatically.
4. Disable the **Status** and **Broadcast SSID** toggle buttons.
5. Note the WLAN ID of the WLAN.

The screenshot displays the 'Add WLAN' configuration interface. The 'General' tab is active, showing the following settings:

- Profile Name\***: WPA3-OWE-Hidden
- SSID\***: WPA3-OWE-Hidden
- WLAN ID\***: 1
- Status**: ENABLED (toggle)
- Broadcast SSID**: ENABLED (toggle)

The **Radio Policy** section is expanded, showing the following configurations:

- 6 GHz**: Status is ENABLED. Security settings: WPA2 Disabled (checked), WPA3 Enabled (checked), Dot11ax Enabled (checked).
- 5 GHz**: Status is ENABLED.
- 2.4 GHz**: Status is ENABLED. 802.11b/g Policy is set to 802.11b/g.

At the bottom of the window, there are 'Cancel' and 'Apply to Device' buttons.

**Figure 32.**  
Radio policy for OWE

6. Choose the **Security > Layer 2** tab. Choose **WPA3** in the **Layer 2 Security Mode** drop-down list.
7. Ensure that **PMF** is set to **Required**.
8. Select **Disabled** from the **Fast Transition** drop-down list.
9. Check the **WPA3 Policy**, **AES (CCMP 128)**, and **OWE** checkboxes. Uncheck any other selected parameters.
10. Enter the **Transition mode WLAN ID**, which will be the WLAN ID of the SSID that will be configured next.

Add WLAN

General
Security
Advanced

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 ☐

Fast Transition

Status 

Disabled

Over the DS ☐

Reassociation Timeout \* 

20

WPA2/WPA3 Encryption

AES(CCMP128) ☒

CCMP256 ☐

GCMP128 ☐

GCMP256 ☐

Protected Management Frame

PMF 

Required

Association Comeback Timer\* 

1

SA Query Time\* 

200

Auth Key Mgmt

SAE ☐

OWE ☒

802.1x-SHA256 ☐

FT + SAE ☐

FT + 802.1x ☐

Transition Mode WLAN ID 

2

Cancel

Apply to Device

**Figure 33.**  
OWE with Transition Mode ID configuration

- Click **Apply to Device** to save and finish the WLAN creation process.

## Part 2 - The following steps will create a WLAN with open security:

1. Navigate to Configuration > Tags and Profiles > WLANs.
2. Click **Add**.
3. In the **General** tab, enter the **Profile Name** (friendly identifier).
4. The SSID must match the enhanced open SSID. The WLAN ID will be populated automatically.
5. Enable the **Status** and **Broadcast SSID** toggle buttons.

The screenshot shows the 'Add WLAN' configuration window with the 'General' tab selected. The window has three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab contains the following fields and controls:

- Profile Name\***: Text input field with the value 'Open-OWE'.
- SSID\***: Text input field with the value 'Open-OWE'.
- WLAN ID\***: Text input field with the value '2'.
- Status**: Toggle switch labeled 'ENABLED' with a green indicator.
- Broadcast SSID**: Toggle switch labeled 'ENABLED' with a green indicator.
- Radio Policy**: Section header with an information icon.
- 6 GHz**: Section header.
- Status**: Toggle switch labeled 'DISABLED' with a grey indicator.
- 5 GHz**: Section header.
- Status**: Toggle switch labeled 'ENABLED' with a green indicator.
- 2.4 GHz**: Section header.
- Status**: Toggle switch labeled 'ENABLED' with a green indicator.
- 802.11b/g Policy**: Dropdown menu with the value '802.11b/g'.

At the bottom of the window, there are two buttons: 'Cancel' and 'Apply to Device'.

**Figure 34.**  
WLAN Open Security configuration

6. Choose the **Security > Layer 2** tab. Choose None in the Layer 2 Security Mode drop-down list.

Add WLAN

General

Security

Advanced

Layer2

Layer3

AAA

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

MAC Filtering

☐

OWE Transition Mode

☒

Transition Mode WLAN ID\*

1

Lobby Admin Access

☐

Protected Management Frame

PMF

Disabled

Fast Transition

Status

Disabled

Over the DS

☐

Reassociation Timeout \*

20

Cancel

Apply to Device

**Figure 35.**  
OWE Transition Mode configuration

- For the Transition Mode WLAN ID, enter the WLAN ID that has Layer 2 security set to Enhanced Open to be mapped to the open WLAN.
- Click **Apply to Device** to save and finish the WLAN creation process.

## WPA3 OWE Transition mode CLI configuration

The following steps will create a hidden WLAN with WPA3 OWE security:

**Table 15.** WPA3 OWE transition mode CLI configuration

	Command	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<code>wlan wlan-name wlan-id SSID-name</code> <b>Example:</b> <code>Device(config)# wlan WPA3-OWE- Hidden 1 WPA3-OWE-Hidden</code>	Enters the WLAN configuration sub-mode.
<b>Step 3</b>	<code>no broadcast-ssid</code>	Disables SSID broadcast.

	Command	Purpose
<b>Step 4</b>	no security ft over-the-ds	Disables Fast Transition over the data source on the WLAN.
<b>Step 5</b>	no security ft	Disables 802.11r Fast Transition on the WLAN.
<b>Step 6</b>	no security wpa akm dot1x	Disables security AKM for 802.1X.
<b>Step 7</b>	no security wpa wpa2	Disables WPA2 security. PMF is disabled now.
<b>Step 8</b>	security wpa akm owe	Enables WPA3 OWE support.
<b>Step 9</b>	security wpa transition-mode-wlan-id 2	Enables Transition mode.
<b>Step 10</b>	security wpa wpa3	Enables WPA3 support.
<b>Step 11</b>	no shutdown	Enables the WLAN.
<b>Step 12</b>	End	Returns to the privileged EXEC mode.

**Part 2 - The following steps will create a WLAN with open OWE security:**

	Command	Purpose
<b>Step 13</b>	configure terminal	Enters global configuration mode.
<b>Step 14</b>	wlan wlan-name wlan-id SSID-name  <b>Example:</b> Device(config)# wlan Open-OWE 2 Open-OWE	Enters the WLAN configuration sub-mode.  <b>Note:</b> The SSID of the hidden WLAN and the open WLAN must be the same.
<b>Step 15</b>	no security ft over-the-ds	Disables Fast Transition over the data source on the WLAN.
<b>Step 16</b>	no security ft	Disables 802.11r Fast Transition on the WLAN.
<b>Step 17</b>	no security wpa akm dot1x	Disables security AKM for 802.1X.
<b>Step 18</b>	no security wpa	Disables security.
<b>Step 19</b>	no security wpa wpa2 ciphers aes	Disables WPA2 ciphers for AES.
<b>Step 20</b>	security wpa transition-mode-wlan-id 1	Enables Transition mode.
<b>Step 21</b>	no shutdown	Enables the WLAN.
<b>Step 22</b>	end	Returns to the privileged EXEC mode.

## Client interoperability matrix

### WPA3 supported AP modes and supported clients

**Table 16.** WPA3 supported AP modes and Clients

WPA3 support matrix									
WPA3 protocol	AP mode Local	AP mode Flex (Central Auth)	AP mode Flex (Local Auth)	Apple (11/12/13)	Samsung S21/Google Android	Intel	Apple iPad (iPadOS: 16.3)	MacOS (M1 or above)	Zebra (TCS53/58/73)
<b>WPA3-Personal</b>	WPA3-SAE AES CCMP128	Supported	Supported  FT: Not supported	Supported  FT-SAE: Supported  H2E: Supported in iOS16	Supported  FT-SAE: Supported only in S21 Galaxy Ultra/Galaxy Z Fold	Supported: H2E only  FT-SAE: Supported in Linux WPA Supplicant (AX210)	Supported  FT-SAE: Supported	Supported  FT-SAE: Supported  Adaptive FT: Not supported	Supported
<b>WPA3-Enterprise</b>	WPA3-802.1x-SHA256 AES CCMP 128	Supported	Supported	Supported	Supported	Supported: SHA256 and FT-OTA  Not supported: FT-ODS	Supported: SHA256, Adaptive and FT-OTA	Supported  Adaptive FT: Not supported	Supported
	WPA3-Enterprise GCMP128 SuiteB 1x	Supported	Not supported	Not supported	Not supported	Not supported: GCMP128, FT-OTA, and FT-ODS	Not supported	Not supported	Not supported
	WPA3-Enterprise GCMP256 SuiteB 192 bit	Supported	Not supported	Supported	Supported  Not supported: FT-ODS	Supported: GCMP256  Not supported: FT (both FT-OTA and FT-ODS)	Supported	Supported: FT-ODS/ITA	Supported
<b>OWE</b>	WPA3-OWE AES CCMP128	Supported	Supported	Not supported	Supported	Supported: OWE Auth	Supported: OWE Auth	Supported	Supported



---

## Useful Catalyst WLC CLI commands

To view the system-level statistics for a client that has undergone successful SAE authentication, SAE authentication failures, SAE ongoing sessions, or SAE commits, and to confirm message exchanges, use the following show command:

- `show wireless stats client detail`

To view the WLAN summary details, use the following command:

- `show wlan summary`
- `show wlan all`
- `show wlan name <wlan-name>`
- `show wlan id {Starting 17.12.1, the security section on the WLAN is displayed individually for 2.4GHz/5GHz band and 6GHz band as below}`

```
#show wlan id 1
WLAN Profile Name           : WPA2+WPA3-TransitionMode
=====
Identifier                  : 1
Description                 :
Network Name (SSID)         : WPA2+WPA3-TransitionMode
Status                      : Enabled
....
    Security-2.4GHz/5GHz
        ....
        Security-6GHz
....
#
```

To view the correct AKM for a client that has undergone SAE authentication, use the following command:

- `show wireless client mac-address <xxxx.xxxx.xxxx> detail`

To view a list of the PMK cache stored locally:

- `show wireless pmk-cache`

---

## Useful Catalyst AP CLI commands

Configure debugging of WPA3 on a client by entering this command:

- `debug client client-mac-address`

Configure debugging of SAE events and details by entering this command:

- `debug sae {events | details} {enable | disable}`

## References

- Cisco Catalyst 9800 Series Wireless Controller 17.8.1 Configuration Guide  
[https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/config-guide/b\\_wl\\_17\\_8\\_cg.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/config-guide/b_wl_17_8_cg.html)
- Cisco Catalyst 9100 Access Points documentation  
<https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/series.html>

**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>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)