Wi-Fi Protected Access 3

Simultaneous Authentication of Equals

A simultaneous authentication of equals (SAE) is a protocol used in WPA3 that

- provides stronger password protection from guessing attacks by third parties
- employs discrete logarithm cryptography to perform an efficient exchange that enables mutual authentication using a password, and
- resists offline dictionary attacks.

An offline dictionary attack is where an adversary attempts to determine a network password by trying possible passwords without further network interaction

Feature History

Feature Name	Release	Description
WPA3 — SAE H2E with Identity PSK	Cisco IOS XE 17.9.2	Added support for Identity PSK (iPSK) passphrase for SAE H2E authentication in local mode. iPSK replaces WLAN passphrase during SAE H2E authentication when configured.
Wi-Fi Protected Access 3 Hash-to-Element (H2E) Support for SAE Authentication	Cisco IOS XE 17.7.1	Introduced Hash-to-Element (H2E) support for SAE authentication. WLAN command options added: **h2e**, **hnp**, **both-h2e-hnp** (default).
Wi-Fi Protected Access3	Cisco IOS XE 16.12.1	WPA3 is the latest version of Wi-Fi ProtectedAccess (WPA), which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks.

WPA3 and SAE in Wi-Fi Security

WPA3 is the latest version of Wi-Fi Protected Access (WPA), which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks.

WPA3 leverages SAE to provide stronger protections for users against password guessing attempts by third parties.

- WPA3-Personal protects users through robust password-based authentication, making brute-force dictionary attacks more difficult.
- WPA3-Enterprise provides higher-grade security protocols for sensitive data networks.

When the client connects to the AP, they perform an SAE exchange. If the exchange is successful, both parties create a cryptographically strong key, which is used to derive the session key. The client and AP complete commit and confirm phases. After commitment, the devices transition to confirm states whenever a new session key is generated. This method uses forward secrecy so that if an intruder cracks one key, the other session keys remain secure.

Note Home SSIDs configured using the OEAP GUI do not support WPA3 security in Cisco IOS-XE 17.6 and 17.7 releases.

Unsupported APs

Cisco Wave 2 APs do not support SAE. If you attempt to connect an AP client to an SAE SSID using these APs, the client will not be able to join after receiving M3 from the AP.

Cisco Wave 2 APs that do not support SAE include:

- Cisco Aironet 1815 Series APs (AP1815W, AP1815T, AP1815I, AP1815M)

- Cisco Aironet 1815T OfficeExtend APs
- Cisco Aironet 1800 Series APs (AP1800I, AP1800S)
- Cisco Aironet 1542 Series Outdoor APs (AP1542D, AP1542I)
- Cisco Aironet 1840 Series APs (AP1840I)

Opportunistic Wireless Encryption

Opportunistic Wireless Encryption (OWE) is a wireless security protocol that

- serves as an extension to IEEE 802.11 standards
- provides encryption of the wireless medium without requiring user credentials, and
- enables secure wireless communication between APs and clients, even in networks traditionally considered open.

Expanded explanation

OWE authenticates devices using Diffie-Hellman algorithm-based cryptography to set up wireless encryption. During network access, the client and AP perform a Diffie-Hellman key exchange. This process establishes a unique pairwise secret. The secret is then used with the standard 4-way handshake to secure the session. This method reduces the risks of open wireless networks by encrypting data traffic and increases security for deployments that otherwise use unsecured or pre-shared key(PSK) configurations.

An airport Wi-Fi network that previously offered open access (no password required) can implement OWE to encrypt wireless communications, protecting user data from eavesdropping while still avoiding the need for users to enter a password.

A traditional open wireless network (without OWE) allows any nearby device to connect and intercept wireless transmissions, leaving users vulnerable to data theft.

Hash-to-Element (H2E)

An SAE password element method is a cryptographic procedure that

- Derives the secret password element (PWE) in the Simultaneous Authentication of Equals (SAE) protocol
- Transforms a password into a secure intermediary element for authentication, and
- Provides protection against security threats such as group downgrade attacks.

Hash-to-Element is a new SAE Password Element (PWE) calculation method for wireless security protocols.

- **Hash-to-Element (H2E)**: Hash-to-Element is a SAE password element method that derives the PWE directly from a password using a hashing process. When a station (STA) supporting H2E initiates SAE with an AP, it checks if the AP supports H2E. If supported, the AP uses the H2E method to generate the PWE, as indicated by a new Status Code in the SAE Commit message.

PWE derivation steps in H2E

When using the H2E method, PWE derivation consists of two steps:

1. Creation of secret intermediary element (PT): The secret intermediary element (PT) is derived offline from the password when it is initially configured for each supported group.
2. Derivation of the PWE: The PWE is generated in real-time from the stored PT during the SAE exchange, using the negotiated group and the Media Access Control (MAC) addresses of both peers.

Additional reference information

- If a device uses the older Hunting-and-Pecking method, the overall SAE exchange remains unchanged.
- The H2E method protects against man-in-the-middle attacks, including Group Downgrade attacks. During authentication, peers exchange lists of rejected groups as part of PMK derivation. If there is a mismatch, the system terminates authentication to prevent a downgrade attack.
- The 6-GHz band supports only H2E SAE PWE method.

- In a typical SAE exchange on a 6 GHz network, only the H2E method is used for password element generation.
- A station using H2E checks AP support, and if supported, uses H2E for secure and efficient authentication.

YANG (RPC model)

To create an RPC for SAE Password Element (PWE) mode, use this RPC model:

```
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:0a77124f-c563-469d-bd21-cc625a9691cc">
<nc:edit-config>
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
<wlan-cfg-entries>
<wlan-cfg-entry>
<profile-name>test</profile-name>
<wlan-id>2</wlan-id>
<sae-pwe-mode>both-h2e-hnp</sae-pwe-mode>
</wlan-cfg-entry>
</wlan-cfg-entries>
</wlan-cfg-data>
</nc:config>
</nc:edit-config>
</nc:rpc>
```

To delete a 6-GHz radio policy and modify the SAE Password Element (PWE) mode, use this RPC model:

```
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:2b8c4be6-492e-4488-b2cf-1f2a1e39fa8c"><nc:edit-config>
```

```
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
<wlan-cfg-entries>
<wlan-cfg-entry>
<profile-name>test</profile-name>
<wlan-id>2</wlan-id>
<wlan-radio-policies>
<wlan-radio-policy nc:operation="delete">
<band>dot11-6-ghz-band</band>
</wlan-radio-policy>
</wlan-radio-policies>
</wlan-cfg-entry>
</wlan-cfg-entries>
</wlan-cfg-data>
</nc:config>
</nc:edit-config>
</nc:rpc>

##
Received message from host
<?xml version="1.0" ?>
<rpc-reply message-id="urn:uuid:2b8c4be6-492e-4488-b2cf-1f2a1e39fa8c"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>
NETCONF rpc COMPLETE
NETCONF SEND rpc
Requesting 'Dispatch'
Sending:

#1268
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:e19a3309-2509-446f-9dbe-c46a6de433db"><nc:edit-config>
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
<wlan-cfg-entries>
<wlan-cfg-entry>
<profile-name>test</profile-name>
<wlan-id>2</wlan-id>
<wlan-radio-policies>
<wlan-radio-policy nc:operation="merge">
<band>dot11-5-ghz-band</band>
</wlan-radio-policy>
</wlan-radio-policies>
<sae-pwe-mode>hunting-and-pecking-only</sae-pwe-mode>
</wlan-cfg-entry>
</wlan-cfg-entries>
</wlan-cfg-data>
</nc:config>
</nc:edit-config>
</nc:rpc>

##
Received message from host
<?xml version="1.0" ?>
<rpc-reply message-id="urn:uuid:e19a3309-2509-446f-9dbe-c46a6de433db"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
```

```
xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
<ok/>
</rpc-reply>
NETCONF rpc COMPLETE
```

Note The **delete** operation performs one action at a time due to the current infra limitation. That is, in YANG module, the **delete** operation on multiple nodes are not supported.

Transition Disable

A Transition Disable indication is a wireless security feature that

- allows an AP to signal a client device (STA) to disable certain transition modes for future connections
- helps prevent downgrade attacks by restricting less secure connection options, and
- is used to strengthen network security without affecting legacy device connectivity.

Disabling transition modes to enforce WPA3 Security.

A client device (STA) may enable transition modes—such as WPA3-Personal transition mode—by default in its network profile, sometimes allowing fallback to less secure methods like PSK.

The Transition Disable indication lets the AP instruct supported STAs to disable these fallback modes, ensuring only secure connection methods are used when possible.

The Transition Disable indication thus provides protection against downgrade attacks.

Note An AP that uses Transition Disable indication does not necessarily disable the corresponding transition modes on its own BSS.

The APs in WPA3-Personal network might use the Transition Disable indication to ensure that all STAs supporting WPA3-Personal are protected against the downgrade attack. However, the WPA3-Personal transition mode is enabled on the BSS for the legacy STAs to connect.

WPA3 SAE iPSK

A WPA3 SAE iPSK is a Wi-Fi authentication method that:

- uses RADIUS server integration to generate unique pre-shared keys for individual users or groups,
- allows more secure and granular authentication in networks where devices do not support 802.1X, and
- limits breach impact so only compromised keys require updating, not all devices on the SSID.
- **SAE (Simultaneous Authentication of Equals)**: A protocol for mutual secure authentication between client and access point.

- **H2E (Hash-to-Element)**: An SAE mode using a password token derived from the authentication passphrase.

iPSK passphrase handling

In networks using WPA3 SAE iPSKs, the WLAN appears like a traditional PSK network from the client's perspective.

From Cisco IOS-XE 17.9.2, the iPSK passphrase is supported for SAE H2E authentication in Local mode. The iPSK passphrase is configured in the client authorization policy in the RADIUS server. The passphrase pushes the policy to the controller during client MAB authentication.

Note The iPSK passphrase in the RADIUS policy replaces the WLAN profile passphrase when generating the password token.

If only one group's PSK is compromised, that group must update their key; the rest of the WLAN remains secure.

WPA3 SAE iPSK

A WPA3 SAE iPSK is a Wi-Fi authentication method that:

- uses RADIUS server integration to generate unique pre-shared keys for individual users or groups,
- allows more secure and granular authentication in networks where devices do not support 802.1X, and
- limits breach impact so only compromised keys require updating, not all devices on the SSID.

- **SAE (Simultaneous Authentication of Equals)**: A protocol for mutual secure authentication between client and access point.
- **H2E (Hash-to-Element)**: An SAE mode using a password token derived from the authentication passphrase.

iPSK passphrase handling

In networks using WPA3 SAE iPSKs, the WLAN appears like a traditional PSK network from the client's perspective.

From Cisco IOS-XE 17.9.2, the iPSK passphrase is supported for SAE H2E authentication in Local mode. The iPSK passphrase is configured in the client authorization policy in the RADIUS server. The passphrase pushes the policy to the controller during client MAB authentication.

Note The iPSK passphrase in the RADIUS policy replaces the WLAN profile passphrase when generating the password token.

If only one group's PSK is compromised, that group must update their key; the rest of the WLAN remains secure.

Configure SAE (WPA3+WPA2 mixed mode)

Enable secure Wi-Fi connectivity using both WPA3 and WPA2 protocols in a mixed mode for SAE on the device.

Performing this task configures a WLAN to support both legacy WPA2 and newer WPA3 authentication using SAE, enhancing security and compatibility for a range of client devices.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter the WLAN configuration sub-mode.

Example:

```
Device(config)# wlan wlan-name wlan-id SSID-name
```

Example:

```
Device(config)# wlan WPA3 1 WPA3
```

Step 3 Disable security AKM for 802.1X.

Example:

```
Device(config-wlan)# no security wpa akm dot1x
```

Step 4 Disable fast transition over the data source on the WLAN.

Example:

```
Device(config-wlan)# no security ft over-the-ds
```

Step 5 Disable 802.11r fast transition on the WLAN.

Example:

```
Device(config-wlan)# no security ft
```

Step 6 Configure WPA2 cipher.

Example:

```
Device(config-wlan)# security wpa wpa2 ciphers aes
```

Note
You can check whether cipher is configured using **no security wpa wpa2 ciphers aes**command. If cipher is not reset, configure the cipher.

Step 7 Specify a preshared key.

Example:

```
Device(config-wlan)# security wpa psk set-key ascii value preshared-key
```

Example:

```
Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123
```

Step 8 Enable WPA3 support.

Example:

```
Device(config-wlan)# security wpa wpa3
```

Note
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.

Step 9 Enable AKM SAE support.

Example:

```
Device(config-wlan)# security wpa akm sae
```

Step 10 Enable AKM PSK support.

Example:

```
Device(config-wlan)# security wpa akm psk
```

Step 11 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 12 Return to the privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

The WLAN is configured to support both WPA3 (with SAE) and WPA2 authentication modes for client connectivity.

Configure WPA3 enterprise (GUI)

Enable WPA3 enterprise authentication on your WLAN to secure wireless communications.

Use this task when you need to enable WPA3 enterprise security for a WLAN profile on your wireless controller using the GUI.

Before you begin

Ensure necessary RADIUS or AAA servers and authentication lists are configured.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. Choose **WPA2+WPA3** in **Layer 2 Security Mode** drop-down list.

Step 5 Uncheck the **WPA2 Policy** and **802.1x** check boxes. Check the **WPA3 Policy** and **802.1x-SHA256** check boxes.

Step 6 Choose **Security** > **AAA**, and then choose the Authentication List from the **Authentication List** drop-down list.

Step 7 Click **Apply to Device**.

Your newly created WLAN uses WPA3 enterprise security for client authentication.

Configure WPA3 enterprise

Set up a secure wireless LAN (WLAN) that uses WPA3 Enterprise authentication to enhance network security for enterprise environments.

WPA3 Enterprise provides stronger data protection and improved security features compared to earlier WLAN authentication methods. You can enable WPA3 Enterprise on supported APs and controllers with this configuration.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter the WLAN configuration sub-mode.

Example:

```
Device(config)# wlan wlan-name wlan-id SSID-name
```

Step 3 Disable security AKM for 802.1X.

Example:

```
Device(config-wlan)# no security wpa akm dot1x
```

Step 4 Disables WPA2 security.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

Step 5 Configures 802.1x support.

Example:

```
Device(config-wlan)# security wpa akm dot1x-sha256
```

Step 6 Enables WPA3 support.

Example:

```
Device(config-wlan)# security wpa wpa3
```

Step 7 Configure security authentication list for dot1x security.

Example:

```
Device(config-wlan)# security dot1x authentication-list list-name
```

Step 8 **no shutdown**

Example:

```
Device(config-wlan)# no shutdown
```

Enables the WLAN.

Step 9 **end**

Example:

```
Device(config-wlan)# end
```

Return to the privileged EXEC mode.

Note
C9115 and C9120 access points do not support WLANs configured with WPA3 Enterprise (SUITEB192-1X).

The WPA3 enterprise WLAN is configured and enabled. Devices can now securely connect using WPA3 Enterprise authentication.

Configure WPA3 OWE

Enable WPA3 Opportunistic Wireless Encryption (OWE) on a WLAN to provide enhanced security for wireless clients.

Use this task when you need to configure a WLAN with WPA3 OWE mode using CLI.

Before you begin

- Ensure Protected Management Frames (PMF) are configured internally.
- WPA2 ciphers are valid for the cipher configuration.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter the WLAN configuration sub-mode.

Example:

```
Device(config)# wlan wlan-name wlan-id SSID-name
```

Step 3 Disable fast transition over the data source on the WLAN.

Example:

```
Device(config-wlan)# no security ft over-the-ds
```

Step 4 Disable 802.11r fast transition on the WLAN.

Example:

```
Device(config-wlan)# no security ft
```

Step 5 Disable security AKM for dot1x.

Example:

```
Device(config-wlan)# no security wpa akm dot1x
```

Step 6 Disable WPA2 security.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

This action also disables PMF.

Step 7 Enable WPA2 ciphers for AES.

Example:

```
Device(config-wlan)# security wpa wpa2 ciphers aes
```

Note
WPA2 and WPA3 use common ciphers.

Step 8 Enable WPA3 support.

Example:

```
Device(config-wlan)# security wpa wpa3
```

Step 9 Enable WPA3 OWE support.

Example:

```
Device(config-wlan)# security wpa akm owe
```

Step 10 Enable the WLAN to allow client devices to connect.

Example:

```
Device(config-wlan)# no shutdown
```

Step 11 Return to the privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

You have enabled WPA3 OWE on your WLAN, enhancing security for your devices when they connect to the SSID.

Configure WPA3 OWE transition mode (GUI)

Configure WPA3 OWE Transition Mode using the GUI to enable secure wireless connectivity with Opportunistic Wireless Encryption (OWE) in transition mode.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. Choose **WPA2+WPA3** in **Layer 2 Security Mode** drop-down list.

Step 5 Uncheck the **WPA2 Policy**, **802.1x**, **Over the DS**, **FT + 802.1x** and **FT + PSK**check boxes.Check the **WPA3 Policy**, **AES** and **OWE** check boxes.

Step 6 Enter the **Transition Mode WLAN ID**.

Step 7 Click **Apply to Device**.

The WLAN is configured with WPA3 OWE Transition Mode, enabling secure connections for compatible devices.

Configure WPA3 OWE transition mode

Configure a WLAN to support WPA3 OWE transition mode for secure wireless connectivity.

WPA3 Opportunistic Wireless Encryption (OWE) transition mode allows clients to connect using either open or secured (WPA3 OWE) methods during transition deployments.

Policy validation does not take place between the open WLAN and the OWE WLAN. You must configure both WLANs correctly.

Before you begin

Identify the WLAN ID and names for the open and OWE WLANs you will configure.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter the WLAN configuration sub-mode.

Example:

```
Device(config)# wlan wlan-name wlan-id SSID-name
```

Step 3 Disable security AKM for 802.1X.

Example:

```
Device(config-wlan)# no security wpa akm dot1x
```

Step 4 Disable fast transition over the data source on the WLAN.

Example:

```
Device(config-wlan)# no security ft over-the-ds
```

Step 5 Disable 802.11r fast transition on the WLAN.

Example:

```
Device(config-wlan)# no security ft
```

Step 6 Disable WPA2 security. PMF is disabled now.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

Step 7 Enable WPA2 ciphers for AES.

Example:

```
Device(config-wlan)# security wpa wpa2 ciphers aes
```

Step 8 Enable WPA3 support.

Example:

```
Device(config-wlan)# security wpa wpa3
```

Step 9 Enable WPA3 OWE support.

Example:

```
Device(config-wlan)# security wpa akm owe
```

Step 10 Configure the open or OWE transition mode WLAN ID.

Example:

```
Device(config-wlan)# security wpa transition-mode-wlan-id wlan-id
```

Note
Validation is not performed on the transition mode WLAN. You must configure it correctly by assigning the open WLAN identifier to the OWE WLAN, and the OWE WLAN identifier to the open WLAN configuration.

Assign the OWE WLAN ID as the transition mode WLAN ID in the open WLAN configuration. Similarly, assign the open WLAN ID as the transition mode WLAN ID in the OWE WLAN configuration.

Step 11 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 12 Return to the privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

The WLAN is configured in WPA3 OWE transition mode and is ready for client connections using the specified security settings.

Configure WPA3 SAE (GUI)

Set up a wireless LAN (WLAN) that uses WPA3 Simultaneous Authentication of Equals (SAE) security using GUI.

Perform this task to enable enhanced security for your WLAN with WPA3 SAE. Use this configuration to support WPA3 for client authentication and ensure optimal wireless security.

Before you begin

Ensure Protected Management Frames (PMF) are configured internally.

- WPA2 ciphers can be used as associated ciphers.
- Fast Transition Adaptive is not supported for WPA3 SAE.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. Choose **WPA2+WPA3** in **Layer 2 Security Mode** drop-down list.

Step 5 Uncheck the **WPAPolicy**, **802.1x**, **Over the DS**, **FT + 802.1x**, and **FT + PSK** checkboxes. Check the **WPA3 Policy**, **AES**, and **PSK** checkboxes. 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.

Step 6 Click **Apply to Device**.

Your WLAN profile is now configured with WPA3 SAE security, and clients can connect using WPA3 authentication.

Configure WPA3 SAE

Enable WPA3 SAE authentication on a WLAN for enhanced Wi-Fi security.

Use this task to configure WPA3 SAE (Simultaneous Authentication of Equals) on a Cisco device. WPA3 SAE offers stronger security for wireless networks and is required for environments that need improved protection against offline dictionary attacks.

Before you begin

Configure PMF (Protected Management Frames) internally.

- You can use WPA2 ciphers with this configuration.
- Fast Transition Adaptive is not supported for WPA3 SAE.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter the WLAN configuration sub-mode.

Example:

```
Device(config)# wlan wlan-name wlan-id SSID-name
```

Example:

```
Device(config)# wlan WPA3 1 WPA3
```

Step 3 Disable security AKM for dot1x.

Example:

```
Device(config-wlan)# no security wpa akm dot1x
```

Step 4 Disable fast transition over the data source on the WLAN.

Example:

```
Device(config-wlan)# no security ft over-the-ds
```

Step 5 Disable 802.11r fast transition on the WLAN.

Example:

```
Device(config-wlan)# no security ft
```

Step 6 Disable WPA2 security. PMF is disabled now.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

Step 7 Configure WPA2 cipher.

Example:

```
Device(config-wlan)# security wpa wpa2 ciphers aes
```

Note
You can check whether cipher is configured using **no security wpa wpa2 ciphers aes**command. If cipher is not reset, configure the cipher.

Step 8 Specify a preshared key

Example:

```
Device(config-wlan)# security wpa psk set-key ascii value preshared-key
```

Example:

```
Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123
```

Step 9 Enable WPA3 support.

Example:

```
Device(config-wlan)# security wpa wpa3
```

Note
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.

Step 10 Enable AKM SAE support.

Example:

```
Device(config-wlan)# security wpa akm sae
```

Step 11 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 12 Return to the privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

The WLAN is configured using WPA3 SAE authentication, providing enhanced wireless security.

Configuring WPA3 SAE iPSK (CLI)

Configure a WPA3 SAE iPSK WLAN profile (CLI)

Configure a WLAN profile with WPA3 SAE individual pre-shared key (iPSK) security on a Cisco device by using CLI.

Use this procedure to set up a WLAN profile with enhanced authentication and security standards (WPA3 SAE iPSK). Only authorized devices can connect using individual preshared keys

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN.

Example:

```
Device(config)# wlanwlan-name wland-id SSID-name
```

- **wlan-name** is the name of the configured WLAN.

- **wlan-id** is the WLAN identifier. The range is one to 512.
- **SSID-name** is the SSID name which can have up to 32 alphanumeric characters.

If you have already created and configured the WLAN, use the **wlan** *wlan-name* command.

Step 3 Set MAC filtering support in WLAN.

Example:

```
Device(config-wlan)# mac-filtering mac-filter-name
```

Step 4 Disable adaptive 802.11r.

Example:

```
Device(config-wlan)# no security ft adaptive
```

Step 5 Disable WPA2 security.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

Step 6 Configures the preshared key in WLAN using the **security wpa psk set-key** [*ascii/hex*] **0** [*key*] command.

Example:

```
Device(config-wlan)# security wpa psk set-key ascii 0 key
```

Note
WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

Step 7 Disable security AKM for 802.1X.

Example:

```
Device(config-wlan)# no security wpa akm dot1x
```

Step 8 Enable AKM SAE support.

Example:

```
Device(config-wlan)# security wpa akm sae
```

Step 9 Enable AKM SAE PWE support (hash-to-element).

Example:

```
Device(config-wlan)# security wpa akm sae pwe h2e
```

Note
This step applies to the Hunting and Pecking (HnP) password element method as well.

Step 10 Enable WPA3 support.

Example:

```
Device(config-wlan)# security wpa wpa3
```

Step 11 Require clients to negotiate Protected Management Frames (PMF) protection in the WLAN.

Example:

```
Device(config-wlan)# security pmf mandatory
```

Step 12 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Clients can now connect to this WLAN using the specified individual pre-shared keys and WPA3 security protocols after the WPA3 SAE iPSK WLAN profile is configured and enabled.

Configure a policy profile with AAA override and VLAN assignment (CLI)

Create and activate a wireless policy profile using the CLI.

Use this procedure to define a policy profile that controls AAA override, VLAN assignment, and other interface features on a Cisco device.

Before you begin

Verify that necessary VLANs exist on the device.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure policy profile.

Example:

```
Device(config)# wireless profile policy policy-profile-name
```

Step 3 Configure AAA override to apply to the policies coming from the AAA or Cisco Identity Services Engine (ISE) server.

Example:

```
Device(config-wireless-policy)# aaa-override
```

Step 4 Configure VLAN.

Example:

```
Device(config-wireless-policy)# vlan 166
```

Step 5 Enable policy profile.

Example:

```
Device(config-wireless-policy)# no shutdown
```

The policy profile is configured and enabled for wireless operations on the device.

Configure a passphrase in a client authorization policy in the RADIUS server(GUI)

Set up a passphrase in a client authorization policy on the RADIUS server to support secure client authentication.

Configure a passphrase in Cisco Identity Services Engine (ISE). To do this, create a client authorization profile and include the required advanced attributes.

Procedure

Step 1 Log in to the Cisco Identity Services Engine (ISE).

Step 2 Click **Policy** and then click **Policy Elements**.

Step 3 Click **Results**.

Step 4 Expand **Authorization** and click **Authorization Profiles**.

Step 5 Click **Add** to create a new authorization profile for the URL filter.

Step 6 In the **Name** field, enter a name for the profile, for example, *po-sae-ipsk*.

Step 7 From the **Access Type** drop-down list, choose **ACCESS_ACCEPT**.

Step 8 From the **Termination-Action** drop-down list, choose **RADIUS-Request**.

Step 9 In the **Advanced Attributes Setting** section, from the drop-down list, choose **Cisco:cisco-av-pair**.

Step 10 Enter each value separately. After adding a value, click (+) icon after each of them:

- `cisco-av-pair = psk-mode=ascii`
- `cisco-av-pair = psk=123123123`

Step 11 Verify the contents in the **Attributes Details** section and click **Save**.

You created a new client authorization profile in Cisco ISE with a custom passphrase. This enables secure client authentication through RADIUS.

Configure WPA3 SAE H2E (GUI)

Use WPA3 SAE H2E to secure your WLAN through a streamlined GUI-based configuration.

Use this procedure to strengthen Wi-Fi security by configuring WPA3 SAE H2E, which enhances protection against offline dictionary attacks.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab. From the **Layer 2 Security Mode** drop-down list, choose **WPA2+WPA3** or **WPA3**.

Step 5 Uncheck the **WPAPolicy**, **802.1x**, **Over the DS**, **FT + 802.1x**, and **FT + PSK** check boxes. Check the **WPA3 Policy**, **AES** and **PSK** check boxes. Enter the **Pre-Shared Key**, and from the **PSK Format** drop-down list, choose the PSK Format, and from the **PSK Type** drop-down list, choose the PSK Type.

Step 6 Check the **SAE** check box.

Note
SAE is enabled only if the Fast Transition is disabled.

Step 7 From the **SAE Password Element** drop-down list, choose **Hash to Element Only** to configure the WPA3 SAE H2E.

Step 8 Click **Apply to Device**.

Your WLAN is now secured with WPA3 SAE H2E, based on your configuration.

Configure WPA3 SAE H2E (CLI)

Enable WPA3 SAE Hash-to-Element (H2E) for secure WLAN connectivity.

Use this task to configure WPA3 SAE H2E for a WLAN on a device running Cisco IOS-XE.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter the WLAN configuration sub-mode.

Example:

```
Device(config)# wlan wlan-name wlan-id SSID-name
```

Example:

```
Device(config)# wlan WPA3 1 WPA3
```

Step 3 Disable security AKM for 802/1X.

Example:

```
Device(config-wlan)# no security wpa akm dot1x
```

Step 4 Disable fast transition over the data source on the WLAN.

Example:

```
Device(config-wlan)# no security ft over-the-ds
```

Step 5 Disable 802.11r fast transition on the WLAN.

Example:

```
Device(config-wlan)# no security ft
```

Step 6 Disable WPA2 security. PMF is disabled now.

Example:

```
Device(config-wlan)# no security wpa wpa2
```

Step 7 Configure WPA2 cipher.

Example:

```
Device(config-wlan)# security wpa wpa2 ciphers aes
```

Note
You can check whether cipher is configured using **no security wpa wpa2 ciphers aes** command. If cipher is not reset, configure the cipher.

Step 8 Specify a preshared key

Example:

```
Device(config-wlan)# security wpa psk set-key ascii value preshared-key
```

Example:

```
Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123
```

Step 9 Enable WPA3 support.

Example:

```
Device(config-wlan)# security wpa wpa3
```

Step 10 Enable AKM SAE support.

Example:

```
Device(config-wlan)# security wpa akm sae
```

Step 11 Enable AKM SAE PWE support using the **security wpa akm sae pwe** {**h2e** | **hnp** | **both-h2e-hnp**} command.

Example:

```
Device(config-wlan)# security wpa akm sae pwe
```

PWE supports these options:

- h2e: Hash-to-Element only; disables HnP.
- hnp: Hunting and Pecking only; disables H2E.
- Both-h2e-hnp: Both Hash-to-Element and Hunting and Pecking support (Is the default option).

Step 12 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 13 Return to the privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

WPA3 SAE H2E is enabled for the specified WLAN. Wireless clients can now connect securely using WPA3 SAE H2E.

Configure WPA3 WLAN for Transition Disable

Enable the transition-disable feature for a WPA3 Wi-Fi network. This improves wireless security and prevents fallback to less secure protocols.

Use this task to ensure clients connect only with WPA3 security. The configuration prevents fallback to WPA2 in transition mode.

Before you begin

Make sure the **security wpa wpa3** command is enabled on your device, as transition disable is available only when WPA3 is enabled.

Procedure

	Command or Action	Purpose
Step 1	Enter global configuration mode. **Example:** `Device# configure terminal`	
Step 2	Enter the WLAN configuration sub-mode. **Example:** `Device(config)# wlan wlan-name wlan-id SSID-name`	
Step 3	Enable Transition Disable support. **Example:** `Device(config-wlan)# transition-disable`	
Step 4	Return to privileged EXEC mode. **Example:** `Device(config-wlan)# end`	

After completing these steps, clients can connect to your WPA3 WLAN only using WPA3 security.

Configure anti-clogging and SAE retransmission (GUI)

Set up Anti-Clogging and SAE retransmission parameters for a WLAN profile using the graphical user interface.

Perform this task to enable stronger wireless security features. This task also optimizes retransmission settings for your SSID.

Before you begin

Gather necessary values for Profile Name, SSID, WLAN ID, anti-clogging threshold, maximum retries, and retransmit timeout.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID** and the **WLAN ID**.

Step 4 Enable or disable **Status** and **Broadcast SSID** toggle buttons.

Step 5 From the **Radio Policy** drop-down list, choose a policy.

Step 6 Choose **Security** > **Layer2** tab. Check the **SAE** check box.

Step 7 Enter the **Anti Clogging Threshold**, **Max Retries** and **Retransmit Timeout**.

Step 8 Click **Apply to Device**.

Anti-clogging and SAE retransmission settings are applied to the selected WLAN profile. Devices connecting to this SSID will now use the updated security and retransmission settings.

Configure anti-clogging and SAE retransmission (CLI)

Configure anti-clogging thresholds and SAE retransmission settings on a WLAN using CLI commands.

Anti-clogging and Secure Authentication of Equals (SAE) retransmission settings help prevent authentication floods and improve handshake reliability for your WLAN. Perform these steps after you configure the basic SAE WLAN settings.

Before you begin

Complete the SAE WLAN configuration

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter the WLAN configuration sub-mode.

Example:

```
Device(config)# wlan wlan-name wlan-id SSID-name
```

Step 3 Disable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 4 Enable simultaneous authentication of equals as a security protocol.

Example:

```
Device(config-wlan)# security wpa akm sae
```

Step 5 Configure threshold on the number of open sessions to trigger the anti-clogging procedure for new sessions.

Example:

```
Device(config-wlan)# security wpa akm sae anti-clogging-threshold 2000
```

Step 6 Configure the maximum number of retransmissions.

Example:

```
Device(config-wlan)# security wpa akm sae max-retries retry-limit
```

Step 7 Configure SAE message retransmission timeout value.

Example:

```
Device(config-wlan)# security wpa akm sae retransmit-timeout retransmit-timeout-limit
```

Step 8 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

Step 9 Return to the privileged EXEC mode.

Example:

```
Device(config-wlan)# end
```

Anti-clogging and SAE retransmission settings are applied to the WLAN.

Verify WPA3 SAE and OWE

Verify WPA3 SAE and OWE.

To view the system level statistics for the client that has undergone successful SAE authentication, SAE authentication failures, SAE ongoing sessions, SAE commit and confirm message exchanges, use this show command:

```
Device# show wireless stats client detail

        Total Number of Clients : 0

        client global statistics:
        ---------------------------------------------------------------------------------
        Total association requests received             : 0
        Total association attempts                      : 0
        Total FT/LocalAuth requests                     : 0
        Total association failures                      : 0
        Total association response accepts              : 0
        Total association response rejects              : 0
        Total association response errors               : 0
        Total association failures due to blacklist     : 0
        Total association drops due to multicast mac    : 0
        Total association drops due to throttling       : 0
        Total association drops due to unknown bssid    : 0
        Total association drops due to parse failure    : 0
        Total association drops due to other reasons    : 0
        Total association requests wired clients        : 0
        Total association drops wired clients           : 0
        Total association success wired clients         : 0
```

```
        Total peer association requests wired clients    : 0
        Total peer association drops wired clients       : 0
        Total peer association success wired clients     : 0
        Total 11r ft authentication requests received    : 0
        Total 11r ft authentication response success     : 0
        Total 11r ft authentication response failure     : 0
        Total 11r ft action requests received            : 0
        Total 11r ft action response success             : 0
        Total 11r ft action response failure             : 0
        Total AID allocation failures                    : 0
        Total AID free failures                          : 0
        Total roam attempts                              : 0
        Total CCKM roam attempts                       : 0
        Total 11r roam attempts                        : 0
        Total 11i fast roam attempts                   : 0
        Total 11i slow roam attempts                   : 0
        Total other roam type attempts                 : 0
        Total roam failures in dot11                     : 0

        Total WPA3 SAE attempts                          : 0
        Total WPA3 SAE successful authentications        : 0
        Total WPA3 SAE authentication failures           : 0
        Total incomplete protocol failures             : 0
        Total WPA3 SAE commit messages received          : 0
        Total WPA3 SAE commit messages rejected          : 0
        Total unsupported group rejections             : 0
        Total WPA3 SAE commit messages sent              : 0
        Total WPA3 SAE confirm messages received         : 0
        Total WPA3 SAE confirm messages rejected         : 0
        Total WPA3 SAE confirm messgae field mismatch  : 0
        Total WPA3 SAE confirm message invalid length  : 0
        Total WPA3 SAE confirm messages sent             : 0
        Total WPA3 SAE Open Sessions                     : 0
        Total SAE Message drops due to throttling        : 0

        Total Flexconnect local-auth roam attempts       : 0
        Total AP 11i fast roam attempts                : 0
        Total 11i slow roam attempts                   : 0

        Total client state starts                        : 0
        Total client state associated                    : 0
        Total client state l2auth success                : 0
        Total client state l2auth failures               : 0
        Total blacklisted clients on dot1xauth failure   : 0
        Total client state mab attempts                  : 0
        Total client state mab failed                    : 0
        Total client state ip learn attempts             : 0
        Total client state ip learn failed               : 0
        Total client state l3 auth attempts              : 0
        Total client state l3 auth failed                : 0
        Total client state session push attempts         : 0
        Total client state session push failed           : 0
        Total client state run                           : 0
        Total client deleted                             : 0
```

To view the WLAN summary details, use this command.

```
Device# show wlan summary

        Number of WLANs: 3

        ID   Profile Name                    SSID                                Status
```

```
Security

--------------------------------------------------------------------------------------------------------------------------------

        1    wlan-demo                          ssid-demo                          DOWN
[WPA3][SAE][AES]

        3    CR1_SSID_mab-ext-radius            CR1_SSID_mab-ext-radius            DOWN
[WPA2][802.1x][AES]

        109  guest-wlan1                        docssid                            DOWN
[WPA2][802.1x][AES],[Web Auth]
```

To view the WLAN properties (WPA2 and WPA3 mode) based on the WLAN ID, use this command.

```
Device# show wlan id 1

        WLAN Profile Name     : wlan-demo
        ================================================
        Identifier                                    : 1

        !
        !
        !
        Security
        802.11 Authentication                       : Open System
        Static WEP Keys                             : Disabled
        Wi-Fi Protected Access (WPA/WPA2/WPA3)      : Enabled
        WPA (SSN IE)                              : Disabled
        WPA2 (RSN IE)                             : Disabled
        WPA3 (WPA3 IE)                            : Enabled
        AES Cipher                              : Enabled
        CCMP256 Cipher                          : Disabled
        GCMP128 Cipher                          : Disabled
        GCMP256 Cipher                          : Disabled
        Auth Key Management
        802.1x                                  : Disabled
        PSK                                     : Disabled
        CCKM                                    : Disabled
        FT dot1x                                : Disabled
        FT PSK                                  : Disabled
        Dot1x-SHA256                            : Disabled
        PSK-SHA256                              : Disabled
        SAE                                     : Enabled
        OWE                                     : Disabled
        SUITEB-1X
```

Verify WPA3 SAE H2E support in WLAN

To view the WLAN properties (PWE method) based on the WLAN ID, use this command:

```
Device# show wlan id 1
WLAN Profile Name     : wpa3
================================================
Identifier                                    : 1
Description                                   :
Network Name (SSID)                           : wpa3
Status                                        : Enabled
```

```
Broadcast SSID                                  : Enabled
Advertise-Apname                                : Disabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
OKC                                             : Enabled
Number of Active Clients                        : 0
CHD per WLAN                                    : Enabled
WMM                                             : Allowed
WiFi Direct Policy                              : Disabled
Channel Scan Defer Priority:
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Disabled
Peer-to-Peer Blocking Action                    : Disabled
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Mac Filter Override Authorization list name     : Disabled
Accounting list name                            :
802.1x authentication list name                 : Disabled
802.1x authorization list name                  : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)      : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Disabled
        WPA3 (WPA3 IE)                          : Enabled
            AES Cipher                          : Enabled
            CCMP256 Cipher                      : Disabled
            GCMP128 Cipher                      : Disabled
            GCMP256 Cipher                      : Disabled
        Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Disabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            Dot1x-SHA256                        : Disabled
            PSK-SHA256                          : Disabled
            SAE                                 : Enabled
            OWE                                 : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Disabled
    SAE PWE Method                              : Hash to Element(H2E)
    Transition Disable                          : Disabled
    CCKM TSF Tolerance (msecs)                  : 1000
    OWE Transition Mode                         : Disabled
    OSEN                                        : Disabled
    FT Support                                  : Disabled
        FT Reassociation Timeout (secs)         : 20
        FT Over-The-DS mode                     : Disabled
    PMF Support                                 : Required
        PMF Association Comeback Timeout (secs): 1
        PMF SA Query Time (msecs)               : 200
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Webauth On-mac-filter Failure               : Disabled
```

```
    Webauth Authentication List Name           : Disabled
    Webauth Authorization List Name            : Disabled
    Webauth Parameter Map                      : Disabled
Band Select                                    : Disabled
Load Balancing                                 : Disabled
Multicast Buffer                               : Disabled
Multicast Buffers (frames)                     : 0
IP Source Guard                                : Disabled
Assisted-Roaming
    Neighbor List                              : Enabled
    Prediction List                            : Disabled
    Dual Band Support                          : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                 : Enabled
    BSS Max Idle                               : Enabled
        Protected Mode                         : Disabled
    Traffic Filtering Service                  : Disabled
    BSS Transition                             : Enabled
        Disassociation Imminent                : Disabled
            Optimised Roaming Timer (TBTTS)    : 40
            Timer (TBTTS)                      : 200
        Dual Neighbor List                     : Disabled
    WNM Sleep Mode                             : Disabled
802.11ac MU-MIMO                               : Enabled
802.11ax parameters
    802.11ax Operation Status                  : Enabled
    OFDMA Downlink                             : Enabled
    OFDMA Uplink                               : Enabled
    MU-MIMO Downlink                           : Enabled
    MU-MIMO Uplink                             : Enabled
    BSS Target Wake Up Time                    : Enabled
    BSS Target Wake Up Time Broadcast Support  : Enabled
802.11 protocols in 2.4ghz band
    Protocol                                   : dot11bg
Advanced Scheduling Requests Handling          : Enabled
mDNS Gateway Status                            : Bridge
WIFI Alliance Agile Multiband                  : Disabled
Device Analytics
    Advertise Support                          : Enabled
    Advertise Support for PC analytics         : Enabled
    Share Data with Client                     : Disabled
Client Scan Report (11k Beacon Radio Measurement)
    Request on Association                     : Disabled
    Request on Roam                            : Disabled
WiFi to Cellular Steering                      : Disabled
Advanced Scheduling Requests Handling          : Enabled
Locally Administered Address Configuration
    Deny LAA clients                           : Disabled
```

To verify the client association who have used the PWE method as H2E or HnP, use this command:

```
Device# show wireless client mac-address e884.a52c.47a5 detail
Client MAC Address : e884.a52c.47a5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 11.11.0.65
Client IPv6 Addresses : fe80::c80f:bb8c:86f6:f71f
Client Username: N/A
AP MAC Address : d4ad.bda2.e9e0
AP Name: APA453.0E7B.E73C
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : N/A
Wireless LAN Id: 1
```

```
WLAN Profile Name: wpa3
Wireless LAN Network Name (SSID): wpa3
BSSID : d4ad.bda2.e9ef
Connected For : 72 seconds
Protocol : 802.11ax - 5 GHz
Channel : 36
Client IIF-ID : 0xa0000001
Association Id : 2
Authentication Algorithm : Simultaneous Authentication of Equals (SAE)
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1728 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m6 ss2
Supported Rates : 6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 0 (kbps)
  QoS Realtime Average Data Rate Upstream    : 0 (kbps)
  QoS Burst Data Rate Upstream               : 0 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 0 (kbps)
  QoS Average Data Rate Downstream           : 0 (kbps)
  QoS Realtime Average Data Rate Downstream  : 0 (kbps)
  QoS Burst Data Rate Downstream             : 0 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 08/24/2021 04:39:47 Pacific
Client Join Time:
  Join Time Of Client : 08/24/2021 04:39:47 Pacific
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 72 seconds
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : SAE
AAA override passphrase : No
SAE PWE Method : Hash to Element(H2E)
Transition Disable Bitmap : None
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : Yes
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : VLAN0011
Multicast VLAN : 0
WiFi Direct Capabilities:
  WiFi Direct Capable          : No
Central NAT : DISABLED
Session Manager:
```

```
  Point of Attachment : capwap_90000006
  IIF ID              : 0x90000006
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 0000000000000000C76750C17
  Acct Session ID  : 0x00000000
  Auth Method Status List
   Method : SAE
  Local Policies:
   Service Template : wlan_svc_default-policy-profile_local (priority 254)
    VLAN             : VLAN0011
    Absolute-Timer   : 1800
  Server Policies:
  Resultant Policies:
                VLAN Name        : VLAN0011
    VLAN             : 11
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Implemented
11v DMS Capable : No
QoS Map Capable : Yes
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
Client Statistics:
  Number of Bytes Received from Client : 21757
  Number of Bytes Sent to Client : 4963
  Number of Packets Received from Client : 196
  Number of Packets Sent to Client : 37
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -72 dBm
  Signal to Noise Ratio : 20 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: Neighbor Report, Passive Beacon Measurement, Active Beacon Measurement,
Table Beacon Measurement
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
```

To view the number of SAE authentications using the H2E and HnP, use this command:

```
Device# show wireless stats client detail
Total Number of Clients : 0

Protocol Statistics

---------------------------------------------------------------------------
Protcol            Client Count
 802.11b              : 0
 802.11g              : 0
 802.11a              : 0
 802.11n-2.4GHz       : 0
 802.11n-5 GHz        : 0
```

```
 802.11ac             : 0
 802.11ax-5 GHz       : 0
 802.11ax-2.4 GHz     : 0
  802.11ax-6 GHz      : 0


Current client state statistics:
---------------------------------------------------------------------------------
  Authenticating         : 0
  Mobility               : 0
  IP Learn               : 0
  Webauth Pending        : 0
  Run                    : 0
  Delete-in-Progress     : 0


Client Summary
-----------------------------
Current Clients : 0
Excluded Clients: 0
Disabled Clients: 0
Foreign Clients : 0
Anchor Clients  : 0
Local Clients   : 0
Idle Clients    : 0
Locally Administered MAC Clients: 0

client global statistics:
---------------------------------------------------------------------------------
Total association requests received              : 0
Total association attempts                       : 0
Total FT/LocalAuth requests                      : 0
Total association failures                       : 0
Total association response accepts               : 0
Total association response rejects               : 0
Total association response errors                : 0
Total association failures due to exclusion list      : 0
Total association drops due to multicast mac     : 0
Total association drops due to random mac        : 0
Total association drops due to throttling        : 0
Total association drops due to unknown bssid     : 0
Total association drops due to parse failure     : 0
Total association drops due to other reasons     : 0
Total association requests wired clients         : 0
Total association drops wired clients            : 0
Total association success wired clients          : 0
Total peer association requests wired clients    : 0
Total peer association drops wired clients       : 0
Total peer association success wired clients     : 0
Total association success wifi direct clients    : 0
Total association rejects wifi direct clients    : 0
Total association response errors                : 0
Total 11r ft authentication requests received    : 0
Total 11r ft authentication response success     : 0
Total 11r ft authentication response failure     : 0
Total 11r ft action requests received            : 0
Total 11r ft action response success             : 0
Total 11r ft action response failure             : 0
Total 11r PMKR0-Name mismatch                    : 0
Total 11r PMKR1-Name mismatch                    : 0
Total 11r MDID mismatch                          : 0
Total AID allocation failures                    : 0
Total AID free failures                          : 0
```

```
Total Roam Across Policy Profiles               : 0
Total roam attempts                             : 0
  Total CCKM roam attempts                      : 0
  Total 11r roam attempts                       : 0
  Total 11r slow roam attempts                  : 0
  Total 11i fast roam attempts                  : 0
  Total 11i slow roam attempts                  : 0
  Total other roam type attempts                : 0
Total roam failures in dot11                    : 0

Total WPA3 SAE attempts                         : 0
Total WPA3 SAE successful authentications       : 0
Total WPA3 SAE authentication failures          : 0
  Total incomplete protocol failures            : 0
Total WPA3 SAE commit messages received         : 0
Total WPA3 SAE commit messages rejected                                  : 0
  Total unsupported group rejections                                     : 0
  Total PWE method mismatch for SAE Hash to Element commit received      : 0
  Total PWE method mismatch for SAE Hunting And Pecking commit received : 0
Total WPA3 SAE commit messages sent             : 0
Total WPA3 SAE confirm messages received        : 0
Total WPA3 SAE confirm messages rejected        : 0
  Total WPA3 SAE message confirm field mismatch : 0
  Total WPA3 SAE confirm message invalid length : 0
Total WPA3 SAE confirm messages sent            : 0
Total WPA3 SAE Open Sessions                    : 0
Total SAE Message drops due to throttling       : 0
Total WPA3 SAE Hash to Element commit received  : 0
Total WPA3 SAE Hunting and Pecking commit received : 0

Total Flexconnect local-auth roam attempts      : 0
  Total AP 11i fast roam attempts               : 0
  Total AP 11i slow roam attempts               : 0
  Total 11r flex roam attempts                  : 0
```

Verify WPA3 transition disable in WLAN

To view the WLAN properties (transition disable) based on the WLAN ID, use this command:

```
Device# show wlan id 7

WLAN Profile Name     : wl-sae
================================================
Identifier                                    : 7
Description                                   :
Network Name (SSID)                           : wl-sae
Status                                        : Enabled
Broadcast SSID                                : Enabled
Advertise-Apname                              : Disabled
Universal AP Admin                            : Disabled
Max Associated Clients per WLAN               : 0
Max Associated Clients per AP per WLAN        : 0
Max Associated Clients per AP Radio per WLAN  : 200
OKC                                           : Enabled
Number of Active Clients                      : 0
CHD per WLAN                                  : Enabled
WMM                                           : Allowed
WiFi Direct Policy                            : Disabled
Channel Scan Defer Priority:
  Priority (default)                          : 5
  Priority (default)                          : 6
Scan Defer Time (msecs)                       : 100
```

```
Media Stream Multicast-direct                 : Disabled
CCX - AironetIe Support                       : Disabled
Peer-to-Peer Blocking Action                  : Disabled
Configured Radio Bands                        : All
Operational State of Radio Bands
    2.4ghz                                    : UP
    5ghz                                      : UP
DTIM period for 802.11a radio                 :
DTIM period for 802.11b radio                 :
Local EAP Authentication                      : Disabled
Mac Filter Authorization list name            : Disabled
Mac Filter Override Authorization list name   : Disabled
Accounting list name                          :
802.1x authentication list name               : Disabled
802.1x authorization list name                : Disabled
Security
    802.11 Authentication                     : Open System
    Static WEP Keys                           : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)    : Enabled
        WPA (SSN IE)                          : Disabled
        WPA2 (RSN IE)                         : Enabled
            MPSK                              : Disabled
            EasyPSK                           : Disabled
            AES Cipher                        : Enabled
            CCMP256 Cipher                    : Disabled
            GCMP128 Cipher                    : Disabled
            GCMP256 Cipher                    : Disabled
            Randomized GTK                    : Disabled
        WPA3 (WPA3 IE)                        : Enabled
            AES Cipher                        : Enabled
            CCMP256 Cipher                    : Disabled
            GCMP128 Cipher                    : Disabled
            GCMP256 Cipher                    : Disabled
        Auth Key Management
            802.1x                            : Disabled
            PSK                               : Enabled
            CCKM                              : Disabled
            FT dot1x                          : Disabled
            FT PSK                            : Disabled
            Dot1x-SHA256                      : Disabled
            PSK-SHA256                        : Disabled
            SAE                               : Enabled
            OWE                               : Disabled
            SUITEB-1X                         : Disabled
            SUITEB192-1X                      : Disabled
    Transition Disable                        : Enabled
    CCKM TSF Tolerance (msecs)                : 1000
```

To verify the client association who have used the transition disable, use this command:

```
Device# show wireless client mac-address 2c33.7a5b.8fc5 detail
Client MAC Address : 2c33.7a5b.8fc5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 10.166.1.101
Client Username: N/A
AP MAC Address : 7c21.0d48.ed00
AP Name: APF4BD.9EBD.A66C
AP slot : 0
Client State : Associated
Policy Profile : po-sae
Flex Profile : N/A
Wireless LAN Id: 7
WLAN Profile Name: wl-sae
```

```
Wireless LAN Network Name (SSID): wl-sae
BSSID : 7c21.0d48.ed02
Connected For : 15 seconds
Protocol : 802.11n - 2.4 GHz
Channel : 11
Client IIF-ID : 0xa0000002
Association Id : 1
Authentication Algorithm : Simultaneous Authentication of Equals (SAE)
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1787 sec)
Session Warning Time : Timer not running
Input Policy Name : None
Input Policy State : None
Input Policy Source : None
Output Policy Name : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : In-Active
Power Save : OFF
Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
QoS Average Data Rate Upstream : 0 (kbps)
QoS Realtime Average Data Rate Upstream : 0 (kbps)
QoS Burst Data Rate Upstream : 0 (kbps)
QoS Realtime Burst Data Rate Upstream : 0 (kbps)
QoS Average Data Rate Downstream : 0 (kbps)
QoS Realtime Average Data Rate Downstream : 0 (kbps)
QoS Burst Data Rate Downstream : 0 (kbps)
QoS Realtime Burst Data Rate Downstream : 0 (kbps)
Mobility:
Move Count : 0
Mobility Role : Local
Mobility Roam Type : None
Mobility Complete Timestamp : 05/16/2021 11:18:14 UTC
Client Join Time:
Join Time Of Client : 05/16/2021 11:18:14 UTC
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 15 seconds
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : SAE
AAA override passphrase : No
Transition Disable Bitmap : 0x01
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : Yes
```