Wi-Fi Protected Access 3

Simultaneous Authentication of Equals

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 Simultaneous Authentication of Equals (SAE) to provide stronger protections for users against password guessing attempts by third parties. SAE employs a discrete logarithm cryptography to perform an efficient exchange in a way that performs mutual authentication using a password that is probably resistant to an offline dictionary attack. An offline dictionary attack is where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

WPA3-Personal brings better protection to individual users by providing more robust password-based authentication making the brute-force dictionary attack much more difficult and time-consuming, while WPA3-Enterprise provides higher grade security protocols for sensitive data networks.

When the client connects to the access point, they perform an SAE exchange. If successful, they will each create a cryptographically strong key, from which the session key will be derived. Basically a client and access point goes into phases of commit and then confirm. Once there is a commitment, the client and access point can then go into the confirm states each time there is a session key to be generated. The method uses forward secrecy, where an intruder could crack a single key, but not all of the other keys.

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

Note Cisco Wave 2 APs do not support SAE. As a result, the AP clients are not able to connect to SAE SSID with these APs, as the clients fail to join back after receiving M3 from the APs.

The following are the Cisco Wave 2 APs that do not support SAE:

- 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 an extension to IEEE 802.11 that provides encryption of the wireless medium. The purpose of OWE based authentication is avoid open unsecured wireless connectivity between the AP's and clients. The OWE uses the Diffie-Hellman algorithms based Cryptography to setup the wireless encryption. With OWE, the client and AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise secret with the 4-way handshake. The use of OWE enhances wireless network security for deployments where Open or shared PSK based networks are deployed.

Hash-to-Element (H2E)

Hash-to-Element (H2E) is a new SAE Password Element (PWE) method. In this method, the secret PWE used in the SAE protocol is generated from a password.

When a STA that supports H2E initiates SAE with an AP, it checks whether AP supports H2E. If yes, the AP uses the H2E to derive the PWE by using a newly defined Status Code value in the SAE Commit message.

If STA uses Hunting-and-Pecking, the entire SAE exchange remains unchanged.

While using the H2E, the PWE derivation is divided into the following components:

- Derivation of a secret intermediary element PT from the password. This can be performed offline when the password is initially configured on the device for each supported group.
- Derivation of the PWE from the stored PT. This depends on the negotiated group and MAC addresses of peers. This is performed in real-time during the SAE exchange.

Note

- 6-GHz supports only Hash-to-Element SAE PWE method.
- The H2E method also incorporates protection against the Group Downgrade man-in-the-middle attacks. During the SAE exchange, the peers exchange lists of rejected groups binded into the PMK derivation. Each peer compares the received list with the list of groups supported, any discrepancy detects a downgrade attack and terminates the authentication.

YANG (RPC model)

To create an RPC for SAE Password Element (PWE) mode, use the following 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 the following 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

Transition Disable is an indication from an AP to an STA. This feature disables few transition modes for subsequent connections to the APs network.

An STA implementation might enable certain transition modes in a network profile. For example, a WPA3-Personal STA might enable the WPA3-Personal transition mode in a network profile by default. This enables a PSK algorithm. However, you can use the Transition Disable indication to disable transition modes for that network on a STA.

Note The Transition Disable indication provides protection against downgrade attacks.

An AP that uses Transition Disable indication does not necessarily disable the corresponding transition modes on its own BSS. For example, 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 RADIUS server and Identity PSK (iPSK) create unique preshared keys for individuals or a group of users present in the same SSID. This kind of setup is useful in networks where end-client devices do not support 802.1X authentication. However, you will need a more secure and granular authentication. From a client perspective, the WLAN looks identical to the traditional PSK network. If one of the PSKs is compromised, only the affected individual or group needs to update their PSK. The rest of the devices connected to the WLAN remain unaffected.

The Simultaneous Authentication of Equals (SAE) H2E authentication mode uses a password token derived from the SAE authentication passphrase. You can configure the passphrase in the WLAN profile for client authentication during commit and confirm message exchanges.

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 replaces the one in the WLAN profile to generate password token. If the iPSK passphrase is not configured in the authorization policy, the SAE H2E falls back to the passphrase in the WLAN profile.

Configuring SAE (WPA3+WPA2 Mixed Mode)

Follow the procedure given below to configure WPA3+WPA2 mixed mode for SAE.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 6	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Configures WPA2 cipher. **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	**security wpa psk set-key ascii** *value preshared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`	Specifies a preshared key.
Step 8	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support. **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.

	Command or Action	Purpose
Step 9	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 10	**security wpa akm psk** **Example:** `Device(config-wlan)# security wpa akm psk`	Enables AKM PSK support.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 12	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 Enterprise (GUI)

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** tab, choose the Authentication List from the **Authentication List** drop-down list.

Step 7 Click **Apply to Device**.

Configuring WPA3 Enterprise

Follow the procedure given below to configure WPA3 enterprise.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wl-dot1x 4 wl-dot1x`	Enters the WLAN configuration sub-mode.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 5	**security wpa akm dot1x-sha256** **Example:** `Device(config-wlan)# security wpa akm dot1x-sha256`	Configures 802.1x support.
Step 6	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 7	**security dot1x authentication-list** *list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list ipv6_ircm_aaa_list`	Configures security authentication list for dot1x security.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode. **Note** A WLAN configured with WPA3 enterprise (SUITEB192-1X) is not supported on C9115/C9120 APs.

Configuring the WPA3 OWE

Follow the procedure given below to configure WPA3 OWE.

Before you begin

Configure PMF internally. The associated ciphers configuration can use the WPA2 ciphers.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 4	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Enables WPA2 ciphers for AES. **Note** The ciphers for WPA2 and WPA3 are common.
Step 8	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.

	Command or Action	Purpose
Step 9	**security wpa akm owe** **Example:** `Device(config-wlan)# security wpa akm owe`	Enables WPA3 OWE support.
Step 10	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 11	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 OWE Transition Mode (GUI)

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**.

Configuring WPA3 OWE Transition Mode

Follow the procedure given below to configure the WPA3 OWE transition mode.

Note Policy validation is not done between open WLAN and OWE WLAN. The operator is expected to configure them appropriately.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Enables WPA2 ciphers for AES.
Step 8	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 9	**security wpa akm owe** **Example:** `Device(config-wlan)# security wpa akm owe`	Enables WPA3 OWE support.
Step 10	**security wpa transition-mode-wlan-id** *wlan-id* **Example:**	Configures the open or OWE transition mode WLAN ID.

	Command or Action	Purpose
	`Device(config-wlan)# security wpa transition-mode-wlan-id 1`	**Note** Validation is not performed on the transition mode WLAN. The operator is expected to configure it correctly with OWE WLAN having open WLAN identifier and the opposite way. You should configure OWE WLAN ID as transition mode WLAN in open WLAN. Similarly, open WLAN should be configured as transition mode WLAN in OWE WLAN configuration.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 12	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 SAE (GUI)

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**check boxes.Check the **WPA3 Policy**, **AES** and **PSK** check boxes. 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**.

Configuring WPA3 SAE

Follow the procedure given below to configure WPA3 SAE.

Before you begin

Configure PMF internally. The associated ciphers configuration can use the WPA2 ciphers.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Configures WPA2 cipher. **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	**security wpa psk set-key ascii** *value preshared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`	Specifies a preshared key.
Step 9	**security wpa wpa3**	Enables WPA3 support.

	Command or Action	Purpose
	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	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 12	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 SAE iPSK (CLI)

Configuring a WPA3 SAE iPSK WLAN Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wl-sae-ipsk 8 wl-sae-ipsk`	Enters the WLAN configuration sub-mode.
Step 3	**mac-filtering** *mac-filter-name* **Example:** `Device(config-wlan)# mac-filtering aaa_list`	Sets MAC filtering support in WLAN.
Step 4	**no security ft adaptive** **Example:**	Disables adaptive 802.11r.

	Command or Action	Purpose
	`Device(config-wlan)# no security ft adaptive`	
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**security wpa psk set-key** [*ascii/hex*] **0** [*key*] **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 123456789`	Configures the preshared key in WLAN. **Note** WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
Step 7	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for 802.1X.
Step 8	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 9	**security wpa akm sae pwe h2e** **Example:** `Device(config-wlan)# security wpa akm sae pwe h2e`	Enables AKM SAE PWE support (hash-to-element). **Note** This step is applicable to Hunting and Pecking (HnP) password element method as well.
Step 10	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 11	**security pmf mandatory** **Example:** `Device(config-wlan)# security pmf mandatory`	Makes clients negotiate Protected Management Frames (PMF) protection in WLAN.
Step 12	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring a Policy Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy po-sae-ipsk`	Configures policy profile.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa-override`	Configures AAA override to apply to the policies coming from the AAA or Cisco Identity Services Engine (ISE) server.
Step 4	**vlan 166** **Example:** `Device(config-wireless-policy)# vlan 166`	Configures VLAN.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.

Configuring a Passphrase in a Client Authorization Policy in the RADIUS Server(GUI)

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 the following one by one and 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**.

Configuring WPA3 SAE H2E (GUI)

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**.

Configuring WPA3 SAE H2E

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.

	Command or Action	Purpose
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:** `Device(config-wlan)# no security ft`	Disables 802.11r fast transition on the WLAN.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Configures WPA2 cipher. **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	**security wpa psk set-key ascii** *value preshared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`	Specifies a preshared key.
Step 9	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 10	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 11	**security wpa akm sae pwe** {**h2e** | **hnp** | **both-h2e-hnp**} **Example:** `Device(config-wlan)# security wpa akm sae pwe`	Enables AKM SAE PWE support. PWE supports the following options: • h2e—Hash-to-Element only; disables HnP.

	Command or Action	Purpose
		• 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	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 13	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring WPA3 WLAN for Transition Disable

Before you begin

You can enable Transition Disable only when the **security wpa wpa3** is enabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**transition-disable** **Example:** `Device(config-wlan)# transition-disable`	Enables Transition Disable support.
Step 4	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Configuring Anti-Clogging and SAE Retransmission (GUI)

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**.

Configuring Anti-Clogging and SAE Retransmission

Follow the procedure given below to configure anti-clogging and SAE retransmission.

Note If the simultaneous SAE ongoing sessions are more than the configured anti-clogging threshold, then anti-clogging mechanism is triggered.

Before you begin

Ensure that SAE WLAN configuration is in place, as the steps given below are incremental in nature, in addition to the SAE WLAN configuration.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**shutdown** **Example:** `Device(config-wlan)# no shutdown`	Disables the WLAN.

	Command or Action	Purpose
Step 4	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables simultaneous authentication of equals as a security protocol.
Step 5	**security wpa akm sae anti-clogging-threshold** *threshold* **Example:** `Device(config-wlan)# security wpa akm sae anti-clogging-threshold 2000`	Configures threshold on the number of open sessions to trigger the anti-clogging procedure for new sessions.
Step 6	**security wpa akm sae max-retries** *retry-limit* **Example:** `Device(config-wlan)# security wpa akm sae max-retries 10`	Configures the maximum number of retransmissions.
Step 7	**security wpa akm sae retransmit-timeout** *retransmit-timeout-limit* **Example:** `Device(config-wlan)# security wpa akm sae retransmit-timeout 500`	Configures SAE message retransmission timeout value.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to the privileged EXEC mode.

Verifying 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 the following 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 the following 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 the following 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                     : Disabled
            SUITEB192-1X                  : Disabled
    CCKM TSF Tolerance                    : 1000
    OSEN                                  : Disabled
    FT Support                            : Adaptive
        FT Reassociation Timeout          : 20
        FT Over-The-DS mode               : Enabled
    PMF Support                           : Required
        PMF Association Comeback Timeout  : 1
        PMF SA Query Time                 : 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
!
!
!
```

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

```
Device# show wireless client mac-address <e0ca.94c9.6be0> detail

Client MAC Address : e0ca.94c9.6be0
!
!
!
Wireless LAN Name: WPA3

!
!
!
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : SAE
!
!
!
```

To view the correct AKM for the client that has undergone OWE authentication, use the following command.

```
Device# show wireless client mac-address <e0ca.94c9.6be0> detail

Client MAC Address : e0ca.94c9.6be0
!
!
!
Wireless LAN Name: WPA3

!
!
!
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : OWE
!
!
!
```

To view the list of PMK cache stored locally, use the following command.

```
Device# show wireless pmk-cache

Number of PMK caches in total : 0

Type      Station             Entry Lifetime  VLAN Override         IP Override
Audit-Session-Id              Username
------------------------------------------------------------------------------
```

Verifying WPA3 SAE H2E Support in WLAN

To view the WLAN properties (PWE method) based on the WLAN ID, use the following 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 the following 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: 000000000000000C76750C17
  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 the following 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
```

Verifying WPA3 Transition Disable in WLAN

To view the WLAN properties (transition disable) based on the WLAN ID, use the following 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 the following 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 : 166.166.1.101
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
```