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.

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.

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.

	Command or Action	Purpose
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.
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.

	Command or Action	Purpose
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**	Enables WPA2 ciphers for AES.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security wpa wpa2 ciphers 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.
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:**	Enables WPA3 OWE support.

	Command or Action	Purpose
	`Device(config-wlan)# security wpa akm owe`	
Step 10	**security wpa transition-mode-wlan-id** *wlan-id* **Example:** `Device(config-wlan)# security wpa transition-mode-wlan-id 1`	Configures the open or OWE transition mode WLAN ID. **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*	Specifies a preshared key.

	Command or Action	Purpose
	Example: `Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`	
Step 9	**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.
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 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.
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.

	Command or Action	Purpose
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
------------------------------------------------------------------------------
```