WPA3 Security Enhancements for Access Points

Information about WPA3 Security Enhancements for Access Points

Cipher Suites

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LANs. You must use a cipher suite when using Wi-Fi Protected Access (WPA), WPA2, WPA3, or Cisco Centralized Key Management (CCKM). Wired Equivalent Privacy, or WEP, is a form of wireless authentication used for associating to 802.11 wireless networks.

Wireless Encryption Methods for Data Protection

Encryption is used to protect data by using methods to obfuscate data to prevent unauthorized people from accessing it. The following encryption protocols are used in wireless authentication:

- **Temporal Key Integrity Protocol (TKIP)**: TKIP is the encryption method used by WPA and supports legacy WLAN equipment. TKIP addresses the original flaws associated with the 802.11 WEP encryption method. It makes use of WEP but encrypts the Layer 2 payload using TKIP and carries out a message integrity check (MIC) in encrypted packets to ensure that messages have not been altered.
- **Advanced Encryption Standard (AES)**: AES is a preferred method because of its strong encryption. AES uses Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP), which allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered.

  CCMP is the standard encryption protocol for use with Wi-Fi Protected Access 2 (WPA2) and is much more secure than the WEP protocol, and TKIP of WPA.

- **Galois/Counter Mode Protocol (GCMP):** GCMP is more secure and efficient than CCMP.

Benefits of Using GCMP-Based Ciphers

- Provides secure communication and data transmission.
- Provides confidentiality and integrity protection.
- Provides parallel processing and fast encryption.

CCMP-Based and GCMP-Based Ciphers in Cisco IOS XE 17.15.1

To improve the speed and security for extremely high throughput (EHT) devices, the CCMP-based ciphers and GCMP-based ciphers are enhanced, from Cisco IOS XE 17.15.1.

Security Enhancements in Cisco IOS XE 17.15.1

The following are the security enhancements developed in Cisco IOS XE 17.15.1:

- GCMP-256 Cipher and SuiteB-192-1X AKM
- SAE-EXT-KEY Support
- AP Beacon Protection
- Multiple Cipher Support per WLAN
- Opportunistic Wireless Encryption (OWE) Support with GCMP-256 Cipher

Supported Platforms

- Cisco Catalyst 9800-CL Wireless Controller for Cloud
- Cisco Catalyst 9800-L Wireless Controller
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9300 Series Switches
- Cisco Embedded Wireless Controller on Catalyst Access Points

Supported Access Points

- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst 9117 Series Access Points
- Cisco Catalyst 9124AX Series Access Points
- Cisco Catalyst 9130AX Series Access Points

- Cisco Catalyst 9136 Series Access Points
- Cisco Catalyst 9162 Series Access Points
- Cisco Catalyst 9164 Series Access Points
- Cisco Catalyst 9166 Series Access Points
- Cisco Aironet 1560 Series Outdoor Access Points

Guidelines and Limitations

- WPA3 is not supported on Cisco Wave 1 APs.
- GCMP-256 is not supported on Cisco Catalyst 9105, 9110, 9115, 9120 APs and 802.11ac Wave2 QCA APs such as 1852.
- Beacon Protection is only supported on QCA-based APs such as 9130, 9136, 9162, 9164, and 9166.

GCMP-256 Cipher and SuiteB-192-1X AKM

There is a strong dependency between the GCMP-256 cipher with Suite-B-192-1X AKM. Therefore, until Cisco IOS XE 17.14.1, if you configure the GCMP-256 cipher, the Suite-B-192-1X AKM automatically gets enabled, as Suite-B-192-1X AKM cannot be enabled separately using commands.

However, in the Cisco IOS XE 17.15.1 release, the dependency between Suite-B-192-1X AKM and the GCMP-256 cipher is eliminated with the use of certain commands, and the GCMP-256 cipher can be configured with other supported AKMs

SuiteB-192-1X AKM is useful for enterprise networks such as, federal government and health care deployments which require highest level of security. Until Cisco IOS XE 17.14.1, the SuiteB-192-1X AKM had been tied with GCMP-256, and was enabled implicitly when GCMP-256 was enabled at the WLAN level. From Cisco IOS XE 17.15.1 onwards, a new AKM configuration is introduced to enable SuiteB-192-1X AKM separately and the GCMP-256 cipher configuration will configure only the cipher.

Configuring SuiteB-192-1X AKM (GUI)

Procedure

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

Step 2 Click **Add**.

The **Add WLAN** window is displayed.

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

Step 4 Choose **Security** > **Layer2**, select one of the following options:

- **WPA + WPA2**
- **WPA2 + WPA3**

- **WPA3**

The **Auth Key Mgmt (AKM)** section will be populated with the possible AKMs that are supported by cipher selected in the **WPA2/WPA3 Encryption** section. Valid cipher and AKM combinations are displayed in the **Auth Key Mgmt (AKM)** section.

For example, to enable SuiteB-192-1x AKM,

- The valid security encryption and AKM combination for **WPA + WPA2** and **WPA2 + WPA3** is **CCMP256** and/or **GCMP256** cipher + **SuiteB-192-1X** AKM.

  Note CCMP256 cipher is not valid without the GCMP256 cipher for SuiteB-192-1X AKM.

- The valid security encryption and AKM combination for **WPA3** is **GCMP256** cipher + **SUITEB-192-1X** or **OWE** or **SAE-EXT-KEY** or **FT + SAE-EXT-KEY** AKM.

  Note At least one AKM should be enabled. To enable SuiteB-192-1X, check the SUITEB 192-1X check box.

Step 5 In the **WPA2 Encryption** section, check the **GCMP256** check box.

Valid cipher and AKM combinations are displayed in the **Auth Key Mgmt (AKM)** section.

Step 6 In the **Fast Transition** section, in the **Status** drop-down list, select **Disabled**.

Note Disable **Fast Transition** when Suite-B cipher (GCMP256/CCMP256/GCMP128) is configured.

Step 7 In the **Auth Key Mgmt (AKM)** section, check the **SUITEB192-1X** check box.

Step 8 Click **Apply to Device**.

Configuring SuiteB-192-1X AKM (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan suiteb192-akm-profile 17 suiteb192-akm-ssid01`	Configures the WLAN profile and SSID. Enters the WLAN configuration mode.
Step 3	**no security ft adaptive** **Example:** `Device(config-wlan)# no security ft adaptive`	Disables adaptive 802.11r.

	Command or Action	Purpose
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for 802.1X.
Step 5	**security wpa akm suiteb-192** **Example:** `Device(config-wlan)# security wpa akm suiteb-192`	Configures the SuiteB-192-1X support.

Step 6	**security wpa wpa2 ciphers** {**aes** | **ccmp256** | **gcmp128** | **gcmp256**}
	Example:
	`Device(config-wlan)# security wpa wpa2 ciphers gcmp256`
		Configures the GCMP256 support.

SAE-EXT-KEY Support

New SAE AKMs, namely SAE-EXT-KEY (24) and FT-SAE-EXT-KEY (25) are introduced in the Cisco IOS XE 17.15.1 release. Devices can connect using the new SAE AKMs (24/25) and negotiate with the GCMP-256 cipher, or the CCMP-128 cipher, or a combination or both ciphers, for encryption.

Note Ensure that the WPA3 policy is enabled for the new AKMs to be displayed.

Configuring SAE-EXT-KEY AKMs (GUI)

Procedure

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

Step 2 Click **Add**.

The **Add WLAN** window is displayed.

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

Step 4 Choose **Security** > **Layer2** and select one of the following options:

- **WPA2 + WPA3**
- **WPA3**

The **Auth Key Mgmt (AKM)** section will be populated with the possible AKMs that are supported by the cipher that is selected in the **WPA2/WPA3 Encryption** section. Valid AKMs are displayed in the **Auth Key Mgmt (AKM)** section.

Note Ensure that the WPA3 policy is enabled for the new AKMs to be displayed.

Step 5 In the **WPA2/WPA3 Encryption** section, check the **GCMP256** check box, or the **AES(CCMP128)** check box, or a combination of both these check boxes.

Note The AES(CCMP128) cipher check box is selected by default.

The AKMs are displayed in the **Auth Key Mgmt (AKM)** section.

Step 6 In the **Auth Key Mgmt (AKM)** section, check either the **SAE-EXT-KEY** check box or the **FT + SAE-EXT-KEY** check box, or select both the AKMs.

Complete the following steps:

a) Enter the **Anti Clogging Threshold** value. Valid range is 0 to 3000; default value is 1500.
b) Enter the number of allowed **Max Retries**. Valid range is 1 to 10; default value is 5.
c) Enter the **Retransmit Timeout** value in seconds. Valid range is 1 to 10000; default value is 400.
d) From the drop-down lists, select the **PSK Format** and the **PSK Type**.
e) Enter the **Pre-Shared Key**.
f) From the **SAE Password Element** drop-down list, select one of the following methods to generate the SAE password element:

    - **Both H2E and HnP**: The password element is generated from both Hash-to Element (H2E) and Hunting and Pecking methods (HnP). This is the default option.
    - **Hash to Element only**: In this method, the secret password element used in the SAE protocol is generated from a password. H2E is based on an non iterative algorithm that is more computationally efficient and provides robust resistance to side channel attack. If selected, HnP is disabled.
    - **Hunting and Pecking only**: This method uses the iterative looping algorithm to generate the password element. As this method is prone to attacks, we recommend that you use the other two methods. If you select the Hunting and Pecking only option, H2E is disabled..

Note SAE-EXT-KEY and FT + SAE-EXT-KEY requires the password element mode to be **Both H2E and HnP** or **Hash to Element only**.

Note If you select an option with WPA2, configure MPSK by completing the following steps:

a. In the **MPSK Configuration** section, check the **Enable MPSK** check box.

b. In the **Auth Key Mgmt** section, choose the **PSK Format** (default is ASCII), PSK Type (default is unencrypted), and enter the **Pre-Shared Key**.

c. In the **MPSK Configuration** section, click **Add**.

Ensure that there are no warnings or error messages in the **Auth Key Mgmt** section, related to encryption and cipher combination.

d. Click **Apply**, and then click **Apply to Device**.

Step 7 Click **Apply to Device**.

Configuring SAE-EXT-KEY AKMs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan wlan-profile 17 wlan-ssid01`	Configures the WLAN profile and SSID. Enters the WLAN configuration mode.
Step 3	**no security ft adaptive** **Example:** `Device(config-wlan)# no security ft adaptive`	Disables adaptive 802.11r.
Step 4	**security wpa psk set-key** {**ascii** | **hex**} {**0** | **8**} *pre-shared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 123456789`	Configures the pre-shared key (PSK) either in the ASCII format or the HEX format.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security Auth Key Management (AKM) for 802.1X.
Step 6	**security wpa akm sae ext-key** **Example:** `Device(config-wlan)# security wpa akm sae ext-key`	Configures the SAE-EXT-KEY AKM support.
Step 7	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Configures WPA3 support.
Step 8	**security wpa wpa2 ciphers** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers gcmp256`	Configures WPA2 and GCMP-256 cipher support.

Configuring FT-SAE-EXT-KEY AKMs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan wlan-profile 17 wlan-ssid01`	Configures the WLAN profile and SSID. Enters the WLAN configuration mode.
Step 3	**security ft** **Example:** `Device(config-wlan)# security ft adaptive`	Configures fast transition
Step 4	**security wpa psk set-key** {**ascii** | **hex**} {**0** | **8**} *pre-shared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 123456789`	Configures the pre-shared key (PSK) either in the ASCII format or the HEX format.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security Auth Key Management (AKM) for 802.1X.
Step 6	**security wpa akm ft sae ext-key** **Example:** `Device(config-wlan)# security wpa akm ft sae ext-key`	Configures the FT-SAE-EXT-KEY AKM support.
Step 7	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Configures WPA3 support.
Step 8	**security wpa wpa2 ciphers** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers gcmp256`	Configures WPA2 and GCMP-256 cipher support.

AP Beacon Protection

The AP Beacon Protection feature helps to avoid attackers modifying the AP beacons and corresponding AP capabilities.

The following are the features of AP beacon protection:

- Avoids active attack and beacon modification by attackers.
- Genuine APs send a Beacon Integrity Key during the 4-way handshake.
- Genuine APs use the Beacon Integrity Key to generate MIC sent through beacons.
- Clients reject an attacker AP beacons based on the MIC validation.

Configuring AP Beacon Protection (GUI)

Procedure

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

Step 2 Click **Add**.

The **Add WLAN** window is displayed.

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

Step 4 Choose **Security** > **Layer 2**, select either the **WPA2 + WPA3** option or the **WPA3** option.

The **Beacon Protection** check box appears in the WPA parameters section when you enable the WPA3 policy.

Step 5 Check the **Beacon Protection** check box.

Note Protected Management Frame (PMF) is required for Beacon Protection to be enabled.

Step 6 Click **Apply to Device**.

Configuring AP Beacon Protection (CLI)

Beacon protection can be enabled for any WPA3 AKM (SAE, FT-SAE, SAE-EXT-KEY, FT-SAE-EXT-KEY, OWE, DOT1X-SHA256, and FT-DOT1X). The SAE AKM configured in the example can be replaced with any WPA3 AKM.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wlan** *wlan-profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan ap-beacon-profile 17 ap-beacon-ssid01`	Configures the WLAN profile and SSID. Enters the WLAN configuration mode.
Step 3	**no security ft adaptive** **Example:** `Device(config-wlan)# no security ft adaptive`	Disables adaptive 802.11r.
Step 4	**security wpa psk set-key** {**ascii** | **hex**} {**0** | **8**} *pre-shared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 123456789`	Configures the pre-shared key (PSK) either in the ASCII format or the HEX format.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security Auth Key Management (AKM) for 802.1X.
Step 6	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Configures SAE support.
Step 7	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Configures WPA3 support.
Step 8	**security wpa wpa3 beacon-protection** **Example:** `Device(config-wlan)# security wpa wpa3 beacon-protection`	Configures AP beacon protection.
Step 9	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 10	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Multiple Cipher Support per WLAN

Until Cisco IOS XE 17.14.1, only single ciphers were allowed in a WLAN, thereby enabling only a limited number of AKMs at the WLAN level. Only CCMP-128 cipher was used with multiple AKMs, while GCMP-128 was tightly coupled with the Suite-B-1x AKM and CCMP-256 / GCMP-256 were tightly coupled with the Suite-B-192-1x AKM.

As there are new AKMs for certain devices, these devices require GCMP-256 support. However, one WLAN serves both devices with GCMP-256, and devices with CCMP-128. Therefore, from Cisco IOS XE 17.15.1 onwards, there is support for multiple AKMs and multiple cipher combinations on the same WLAN.

Pairwise Cipher Suite, Group Cipher Suite, and Management Cipher Suite Mapping

The configured cipher suite(s) for a WLAN is mapped to the Pairwise Cipher Suite, Group Cipher Suite, and Management Cipher Suite broadcasted in the Beacons or Probe Responses.

Configured Cipher Suite	Pairwise Cipher Suite	Group Cipher Suite	Management Cipher Suite
CCMP-128 only	CCMP-128	CCMP-128	BIP-CMAC-128
GCMP-256 only	GCMP-256	GCMP-256 Management	BIP-GMAC-256
CCMP-128 + GCMP-256	CCMP-128 or GCMP-256 (client chooses)	CCMP-128	BIP-CMAC-128

Configuring Multiple Ciphers (GUI)

Procedure

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

Step 2 Click **Add**.

The **Add WLAN** window is displayed.

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

Step 4 Choose **Security** > **Layer2**, select one of the following options:

- **WPA + WPA2**
- **WPA2 + WPA3**
- **WPA3**

The **AES(CCMP128)** cipher is selected by default.

The **Auth Key Mgmt (AKM)** section will be populated with the possible AKMs that are supported by the cipher that is selected in the **WPA2/WPA3 Encryption** section. Valid cipher and AKM combinations are displayed in the **Auth Key Mgmt (AKM)** section.

Step 5 In the **WPA2/WPA3 Encryption** check the **GCMP256** check box, or the **AES(CCMP128)** check box, or a combination of both these check boxes, to display the AKMs in the same WLAN.

Step 6 In the **Auth Key Mgmt (AKM)** section, check the AKM check boxes to enable the required AKMs. At least one AKM should be enabled.

Step 7 Click **Apply to Device**.

Configuring Multiple Ciphers (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan wlan-profile 17 wlan-ssid01`	Configures the WLAN profile and SSID. Enters the WLAN configuration mode.
Step 3	**no security ft adaptive** **Example:** `Device(config-wlan)# no security ft adaptive`	Disables adaptive 802.11r.
Step 4	**security wpa psk set-key** {**ascii** | **hex**} {**0** | **8**} *pre-shared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 123456789`	Configures the pre-shared key (PSK) either in the ASCII format or the HEX format.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for 802.1X.
Step 6	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Configures the SAE support.
Step 7	**security wpa akm sae ext-key** **Example:** `Device(config-wlan)# security wpa akm sae ext-key`	Configures the SAE-EXT-KEY AKM support.

	Command or Action	Purpose
Step 8	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Configures WPA3 support.

Step 9	**security wpa wpa2 ciphers** {**aes** | **ccmp256** | **gcmp128** | **gcmp256**}
	Example:
	`Device(config-wlan)# security wpa wpa2 ciphers aes`
		Configures WPA2 cipher support. In this example, CCMP-128 cipher is configured.

Step 10	**security wpa wpa2 ciphers** {**aes** | **ccmp256** | **gcmp128** | **gcmp256**}
	Example:
	`Device(config-wlan)# security wpa wpa2 ciphers gcmp256`
		Configures another WPA2 cipher support (multiple cipher support). In this example, GCMP-256 cipher is configured.

Opportunistic Wireless Encryption (OWE) Support with GCMP-256 Cipher

Until Cisco IOS XE 17.14.1, OWE was supported with the CCMP-128 cipher. From Cisco IOS XE 17.15.1 onwards, OWE association is supported on both CCMP-128 and GCMP-256 ciphers. If you configure both ciphers, a client will select its desired cipher suite while connecting in the association request.

Configuring Opportunistic Wireless Encryption AKM (GUI)

Procedure

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

Step 2 Click **Add**.

The **Add WLAN** window is displayed.

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

Step 4 Choose **Security** > **Layer 2** and click the **WPA3** option.

Step 5 In the **WPA2/WPA3 Encryption** section, check the **GCMP256** check box, or the **AES(CCMP128)** check box, or a combination of both these check boxes. The **AES(CCMP128)** check box is selected by default.

Step 6 In the **Fast Transition** section, from the **Status** drop-down list, select **Disabled**

Step 7 In the **Auth Key Mgmt (AKM)** section, check the **OWE** check box.

The **Transition Mode WLAN ID** field is displayed.

Step 8 Enter the **Transition Mode WLAN ID**. The transition-mode WLAN ID ranges are the same as the WLAN ID ranges, that is, the valid range is between 0 and 4096.

Step 9 Click **Apply to Device**.

Configuring Opportunistic Wireless Encryption AKM (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-profile-name wlan-id ssid-name* **Example:** `Device(config)# wlan wlan-profile 17 wlan-ssid01`	Configures the WLAN profile and SSID. Enters the WLAN configuration mode.
Step 3	**no security ft adaptive** **Example:** `Device(config-wlan)# no security ft adaptive`	Disables adaptive 802.11r.
Step 4	**security wpa akm owe** **Example:** `Device(config-wlan)# security wpa akm owe`	Configures the OWE AKM.

Verifying the SAE-EXT-KEY AKM Support

Summary of SAE-EXT-KEY AKMs

To view the summary of the SAE-EXT-KEY AKMs, use the following command:

```
Device# show wlan summary
Number of WLANs: 5

ID   Profile Name                     SSID                             Status 2.4GHz/5GHz
Security                            6GHz Security
------------------------------------------------------------------------------------------

1    wpa3-sae_profile               wpa3-sae                       UP     [WPA3][SAE][AES]
                                [WPA3][SAE][AES]
2    wpa3-sae-ext_profile             wpa3-sae-ext                     UP
[WPA3][SAE-EXT-KEY][GCMP256]                    [WPA3][SAE-EXT-KEY][GCMP256]
3    wpa3-sae-ext-mab_profile         wpa3-sae-ext-mab                 UP
[WPA3][MAB][SAE-EXT-KEY][GCMP256]               [WPA3][MAB][SAE-EXT-KEY][GCMP256]
4    wpa3-sae-ext-webauth_profile     wpa3-sae-ext-webauth_profile     UP
[WPA3][SAE-EXT-KEY][Webauth][GCMP256]           [WPA3][SAE-EXT-KEY][Webauth][GCMP256]
5    wpa3-sae-ext-mab-webauth_profile wpa3-sae-ext-mab-webauth_profile UP
[WPA3][MAB][SAE-EXT-KEY][Webauth][GCMP256]      [WPA3][MAB][SAE-EXT-KEY][Webauth][GCMP256]
```

```
6    wpa3-ft-sae_profile             wpa3-ft-sae                      UP      [WPA3][FT +
SAE][AES]                           [WPA3][FT + SAE][AES]
7    wpa3-ft-sae-ext_profile         wpa3-ft-sae-ext                  UP      [WPA3][FT +
SAE-EXT-KEY][GCMP256]               [WPA3][FT + SAE-EXT-KEY][GCMP256]
8    wpa3-ft-sae-ext-mab_profile     wpa3-ft-sae-ext-mab              UP      [WPA3][MAB][FT
 + SAE-EXT-KEY][GCMP256]           [WPA3][MAB][FT + SAE-EXT-KEY][GCMP256]
9    wpa3-ft-sae-ext-webauth_profile  wpa3-ft-sae-ext-webauth          UP      [WPA3][FT +
SAE-EXT-KEY][Webauth][GCMP256]      [WPA3][FT + SAE-EXT-KEY][Webauth][GCMP256]
10   wpa3-ft-sae-ext-mab-webauth_pro  wpa3-ft-sae-ext-mab-webauth      UP      [WPA3][MAB][FT
 + SAE-EXT-KEY][Webauth][GCMP256]  [WPA3][MAB][FT + SAE-EXT-KEY][Webauth][GCMP256]
```

SAE-EXT-KEY and FT-SAE-EXT-KEY AKM in WLAN Profiles

To view the details of the SAE-EXT-KEY and FT-SAE-EXT-KEY AKMs, use the following commands:

```
Device# show wlan name wpa3-sae-ext-key-profile
WLAN Profile Name     : wpa3-sae-ext-key-profile
================================================
Identifier                                       : 2
Description                                      :
Network Name (SSID)                              : wpa3-sae-ext-key
<...>
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                           : Disabled
            CCMP256 Cipher                       : Disabled
            GCMP128 Cipher                       : Disabled
            GCMP-256 Cipher                       : Enabled
        Auth Key Management
            802.1x                               : Disabled
            PSK                                  : Disabled
            CCKM                                 : Disabled
            FT dot1x                             : Disabled
            FT PSK                               : Disabled
            FT SAE                               : Disabled
            FT SAE-EXT-KEY                       : Disabled
            Dot1x-SHA256                         : Disabled
            PSK-SHA256                           : Disabled
            SAE                                  : Disabled
            SAE-EXT-KEY                          : Enabled
            OWE                                  : Disabled
            SUITEB-1X                            : Disabled
            SUITEB192-1X                         : Disabled
    SAE PWE Method                            : Hash to Element, Hunting and Pecking(H2E-HNP)
.
.
.


Device# show wlan name wpa3-ft-sae-ext-key-profile
WLAN Profile Name     : wpa3-ft-sae-ext-key-profile
================================================
Identifier                                       : 7
Description                                      :
Network Name (SSID)                              : wpa3-ft-sae-ext-key
<...>
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                         : Disabled
            CCMP256 Cipher                     : Disabled
            GCMP128 Cipher                     : Disabled
            GCMP-256 Cipher                     : Enabled
        Auth Key Management
            802.1x                             : Disabled
            PSK                                : Disabled
            CCKM                               : Disabled
            FT dot1x                           : Disabled
            FT PSK                             : Disabled
            FT SAE                             : Disabled
            FT SAE-EXT-KEY                     : Enabled
            Dot1x-SHA256                       : Disabled
            PSK-SHA256                         : Disabled
            SAE                                : Disabled
            SAE-EXT-KEY                        : Disabled
            OWE                                : Disabled
            SUITEB-1X                          : Disabled
            SUITEB192-1X                       : Disabled
    SAE PWE Method                          : Hash to Element, Hunting and Pecking(H2E-HNP)
.
.
.
```

Cipher and AKMs based on Client MAC Address

To view the details of the cipher and AKMs based on the client MAC address, use the following command:

```
Device# show wireless client mac-address 3089.4aXX.f0XX detail
Client MAC Address : 3089.4aXX.f0XX
.
.
.
Policy Type : WPA3
Encryption Cipher : GCMP-256
Authentication Key Management : SAE-EXT-KEY
.
.
.
Client MAC Address : 3089.4aXX.f0XX
.
.
.
Policy Type : WPA3
Encryption Cipher : GCMP-256
Authentication Key Management : FT-SAE-EXT-KEY
.
.
.
```

AKM Support Statistics Report

To view the AKM support statistics report, use the following command:

```
Device# show wireless stats client detail
Total WPA3 SAE attempts                          :71
Total WPA3 SAE successful authentications        : 9
  Total SAE-EXT-KEY successful authentications   : 3
Total WPA3 SAE authentication failures           : 22
  Total incomplete protocol failures             : 0
Total WPA3 SAE commit messages received          : 126
Total WPA3 SAE commit messages rejected                                 : 58
  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              : 175
Total WPA3 SAE confirm messages received         : 13
Total WPA3 SAE confirm messages rejected         : 4
  Total WPA3 SAE message confirm field mismatch  : 4
  Total WPA3 SAE confirm message invalid length  : 0
Total WPA3 SAE confirm messages sent             : 13
Total WPA3 SAE Open Sessions                     : 0
Total SAE Message drops due to throttling        : 0
Total WPA3 SAE Hash to Element commit received   : 111
Total WPA3 SAE Hunting and Pecking commit received : 15
```

Verifying AP Beacon Protection

To verify the AP beacon protection details, use the following command:

```
Device# show wlan name wl-sae
WLAN Profile Name     : wl-sae
================================================
Identifier                                     : 7
Description                                    :
Network Name (SSID)                            : wl-sae
<...>
Security
    Security-2.4GHz/5GHz
        <...>
        Beacon Protection                      : Enabled
    Security-6GHz
        <...>
        Beacon Protection                      : Enabled
<...>
```