# SuiteB-1X and SuiteB-192-1X Support in FlexConnect Mode for WPA2 and WPA3



# Information about SuiteB-1X and SuiteB-192-1X Support in FlexConnect Mode for WPA2 and WPA3

### Support for SuiteB-192-1X and SuiteB-1X Ciphers in FlexConnect Mode

From Cisco IOS XE 17.15.1 onwards, Cisco WLAN FlexConnect mode supports enterprise authentication key management (AKM) — SuiteB-192-1X (AKM 12) and SuiteB-1X (AKM 11). These AKMs are already supported in the Local mode. This section describes the configuration for SuiteB-192-1X and SuiteB-1X in FlexConnect mode, and also the requirements to support Galois Counter Mode Protocol 128 (GCMP-128), GCMP-256, and Counter Cipher Mode with Block Chaining Message Authentication Code Protocol 256 (CCMP-256) ciphers for pairwise transport keys (PTK) and group temporal key (GTK) derivation in FlexConnect Local Authentication mode and FlexConnect Central Authentication mode.

### Authentication Types and Ciphers in FlexConnect Mode During PTK and GTK Derivation

- In WPA2 FlexConnect mode:
  - SUITEB192-1X ciphers are CCMP-256 and GCMP-256.
  - SUITEB-1X cipher is GCMP-128.
- In WPA3 FlexConnect mode:
  - SUITEB192-1X cipher is GCMP-256.
  - SUITEB-1X cipher is GCMP-128.

# Configuring SuiteB 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 **Auth Key Mgmt (AKM)** section will be populated with the possible AKMs 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 Encryption** section, select one of the following ciphers:

- **CCMP256**
- **GCMP128**
- **GCMP256**

**Note** The **AES(CCMP128)** cipher is selected by default. Multiple ciphers are not currently supported. Clear the **AES(CCMP128)** cipher check box and then select the desired cipher.

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

**Step 6** In the **Fast Transition** section and 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 **SUITEB-1X** check box.

**Step 8** Click **Apply to Device**.

# Configuring Suite-B Ciphers (CLI)

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **wlan** *wlan-profile-name wlan-id ssid-name*<br>**Example:**<br>`Device(config)# wlan suiteb-profile 17 suiteb-ssid01` | Configures the WLAN profile and SSID. Enters the WLAN configuration mode. |
| **Step 3** | **security wpa wpa2 ciphers** {**aes** \| **ccmp256** \| **gcmp128** \| **gcmp256**}<br>**Example:**<br>`Device(config-wlan)# security wpa wpa2 ciphers aes` | Configures the CCMP-128 support by default. |

# Configuring GCMP-128, GCMP-256, or CCMP-256 (CLI)

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **security wpa wpa2**<br>**Example:**<br>`Device(config-wlan)# security wpa wpa2` | Configures the WPA2 support for a WLAN profile. |
| **Step 2** | **no security wpa akm dot1x**<br>**Example:**<br>`Device(config-wlan)# no security wpa akm dot1x` | Disables security AKM for 802.1X. |
| **Step 3** | **no security wpa wpa2 ciphers ccmp128**<br>**Example:**<br>`Device(config-wlan)# no security wpa wpa2 ciphers ccmp128` | Disables the SuiteB CCMP-128 cipher. |
| **Step 4** | **security wpa wpa2 ciphers** {**aes** \| **ccmp256** \| **gcmp128** \| **gcmp256**}<br>**Example:**<br>`Device(config-wlan)# security wpa wpa2 ciphers gcmp256` | Configures either the CCMP-256 cipher, the GCMP-128 cipher, or the GCMP-256 cipher. |
| **Step 5** | **security dot1x authentication-list** *authlist-name*<br>**Example:**<br>`Device(config-wlan)# security dot1x authentication-list suiteb-authlist` | Sets the authentication list for IEEE 802.1X. |

# Verifying SuiteB Cipher Status

### Verifying SuiteB Cipher in a WLAN Profile

To verify the SuiteB cipher status in a WLAN profile, use the following command:

```
Device# show wlan id 3
saurabh-vwlc#show wlan id 3
WLAN Profile Name     : FIPS
================================================
Identifier                                      : 3
Network Name (SSID)                             : FIPS
Status                                          : Enabled
.
.
.
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            AES Cipher                          : Enabled
            CCMP256 Cipher                      : Enabled
            GCMP128 Cipher                      : Disabled
            GCMP256 Cipher                      : Disabled
        Auth Key Management
            802.1x                              : Enabled
            PSK                                 : Disabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            PMF dot1x                           : Disabled
            PMF PSK                             : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Enabled
.
.
.
```

### Verifying SuiteB Cipher Status using MAC Address

To verify the SuiteB cipher status using a MAC address, use the following command:

```
Device# show wireless client mac-address H.H.H detail
Client MAC Address : a8XX.ddXX.05XX
Client IPv4 Address : 169.254.175.214
……..
……..
Policy Type : WPA2
Encryption Cipher : CCMP256
Authentication Key Management : SUITEB192-1X
```