Multiple Cipher Support

Default Ciphersuites Supported for CAPWAP-DTLS

From Cisco IOS XE Bengaluru 17.5.1, Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)/Galois Counter Mode (GCM) ciphersuite with perfect forward secrecy (PFS) capability is added in the default list along with the existing AES128-SHA ciphersuite. All Cisco access point (AP) models, except the Cisco IOS APs, will prioritize this PFS ciphersuite for CAPWAP-DTLS under default configuration.

Note If link encryption is enabled to secure data channel traffic, then the AP (DTLS client) will prioritize AES128-SHA over ECDHE/GCM ciphersuite.

During DTLS handshake, the preference order of the ciphersuites are important. This feature allows you to set the order of priority while configuring cipher suites.

When explicit ciphersuites are not configured, default ciphersuites that are listed in the table below are applied.

Table 1: Default Ciphersuites

Security Mode	Ciphersuite
FIPS and non-FIPS	• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA

Security Mode	Ciphersuite
WLANCC	• TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

This feature is supported on all variants of the Cisco Catalyst 9800 Series Wireless Controllers and APs, except Cisco Industrial Wireless 3702 Access Point.

For a list of controllers and APs supported in a particular release, see the release notes available at: https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html

Configuring Multiple Ciphersuites

Note

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dtls-ciphersuite priority** *priority-num ciphersuite* **Example:** `Device(config)# ap dtls-ciphersuite priority 2 TLS_DHE_RSA_WITH_AES_128_CBC_SHA`	Sets priority for a particular cipher suite. Use zero (0) to set the highest priority. **Note** Configuration changes, if any, will automatically disconnect the existing APs.
Step 3	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Setting Server Preference

Ciphersuite configuration enforces the priority order in a DTLS handshake. To give equal priority for all the configured ciphersuites, then use **no ciphersuite server-preference** command in the corresponding AP join profile. By default, server preference is enabled.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile xxy`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**[no] ciphersuite server-preference** **Example:** `Device(config-ap-profile)# [no] ciphersuite server-preference`	Sets the cipher suite server preference. Use the **no** form of this command to disable server preference. By default, server preference is enabled.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to global configuration mode.

Verifying Operational Ciphersuites and Priority

To view the operational ciphersuites and their priority, use the following command:

```
Device# show wireless certification config

WLANCC                          : Not Configured
AP DTLS Version                 : DTLS v1.0 - v1.2

AP DTLS Cipher Suite List:

  Priority                Ciphersuite
------------------------------------------------------------------------------
   0                      AES128-SHA
   1                      DHE-RSA-AES256-SHA256
```