# Data DTLS



# Information About Data Datagram Transport Layer Security

Data Datagram Transport Layer Security (DTLS) enables you to encrypt CAPWAP data packets that are sent between an access point and the controller using DTLS, which is a standards-track IETF protocol that can encrypt both control and data packets based on TLS. CAPWAP control packets are management packets that are exchanged between a controller and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data).

If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

If an access point supports Data DTLS, it enables data DTLS after receiving the new configuration from the controller . The access point performs a DTLS handshake on port 5247 and after successfully establishing the DTLS session. All the data traffic (from the access point to the controller and the controller to the access point) is encrypted.

**Note** The throughput is affected for some APs that have data encryption enabled.

The controller does not perform a DTLS handshake immediately after processing client-hello with a cookie, if the following incorrect settings are configured:

- ECDHE-ECDSA cipher in “ap dtls-cipher <>” and RSA-based certificate in “wireless management trustpoint”.
- RSA cipher in “ap dtls-cipher <>” and EC-based certificate in “wireless management trustpoint”.

**Note** This is applicable when you move from CC -> FIPS -> non-FIPS mode.

**Note** If the AP's DHCP lease time is less and the DHCP pool is small, access point join failure or failure in establishing the Data Datagram Transport Layer Security (DTLS) session may occur. In such scenarios, associate the AP with a named site-tag and increase the DHCP lease time for at least 8 days.

# Configuring Data DTLS (GUI)

Follow the procedure to enable DTLS data encryption for the access points on the controller :

**Procedure**

**Step 1** Click **Configuration** > **Tags and Profile** > **AP Join**.

**Step 2** Click **Add** to create a new **AP Join Profile** or click an existing profile to edit it.

**Step 3** Click **CAPWAP** > **Advanced**.

**Step 4** Check **Enable Data Encryption** check box to enable Datagram Transport Layer Security (DTLS) data encryption.

**Step 5** Click **Update & Apply to Device**.

# Configuring Data DTLS (CLI)

Follow the procedure given below to enable DTLS data encryption for the access points on the controller :

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **ap profile** *ap-profile*<br>**Example:**<br>`Device(config)# ap profile test-ap-profile` | Configures an AP profile and enters AP profile configuration mode.<br>**Note** You can use the default AP profile (default-ap-profile) or create a named AP profile, as shown in the example. |
| **Step 3** | **link-encryption**<br>**Example:**<br>`Device(config-ap-profile)# link-encryption` | Enables link encryption based on the profile. Answer yes, when the system prompts you with this message: |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If you set stats-timer as as zero (0) under the AP profile, then the AP will not send the link encryption statistics.<br>`Enabling link-encryption will reboot the APs with link-encryption.`<br>`Are you sure you want to continue? (y/n)[y]:` |
| **Step 4** | **end**<br>**Example:**<br>`Device(config-ap-profile)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show wireless dtls connections**<br>**Example:**<br>`Device# show wireless dtls connections` | (Optional) Displays the DTLS session established for the AP that has joined this controller. |
| **Step 6** | **show ap link-encryption**<br>**Example:**<br>`Device# show ap link-encryption` | (Optional) Displays the link encryption-related statistics (whether link encryption is enabled or disabled) counter received from the AP. |