Configuring Data Encryption

Finding Feature Information

Prerequisites for Configuring Data Encryption

- Cisco 1260, 3500, 3600, 801, 1140, 1310, and 1520 series access points support Datagram Transport Layer Security (DTLS) data encryption.
- You can use the switch to enable or disable DTLS data encryption for a specific access point or for all access points.
- Non-Russian customers who use the Cisco switch do not need a data DTLS license.

Restrictions for Configuring Data Encryption

- Encryption limits throughput at both the switch and the access point, and maximum throughput is desired for most enterprise networks.
- If your switch does not have a data DTLS license and if the access point associated with the switch has DTLS enabled, the data path will be unencrypted.
- In images that do not have a DTLS license, the DTLS commands are not available.

Information About Data Encryption

The switch enables you to encrypt Control and Provisioning of Wireless Access Points (CAPWAP) control packets (and optionally, CAPWAP data packets) that are sent between the access point and the switch using DTLS. DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a switch 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.

How to Configure Data Encryption

Configuring Data Encryption (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap link-encryption**
3. **end**
4. **show ap link-encryption**
5. **show wireless dtls connections**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap link-encryption** **Example:** `Switch(config)# ap link-encryption`	Enables data encryption for all access points or a specific access point by entering this command. The default value is disabled. Changing the data encryption mode requires the access points to rejoin the switch.

Step 3	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Step 4	**show ap link-encryption** **Example:** `Switch# show ap link-encryption`	Displays the encryption state of all access points or a specific access point. This command also shows authentication errors, which track the number of integrity check failures and replay errors. Relay errors help in tracking the number of times the access point receives the same packet.

	Command or Action	Purpose
Step 5	**show wireless dtls connections** **Example:** `Switch# show wireless dtls connections`	Displays a summary of all active DTLS connections. **Note** If you experience any problems with DTLS data encryption, enter the **debug dtls ap** {**all** | **event** | **trace**} command to debug all DTLS messages, events, or traces.

Configuring Data Encryption (GUI)

Step 1 Choose **Configuration** > **Wireless** > **Access Points** > **All APs**.
The All APs page is displayed.

Step 2 Click the name of the access point for which you want to enable data encryption.
The **AP > Edit** page is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Select or unselect the **Data Encryption** check box.

Note Changing the data encryption mode requires the access points to reassociate with the switch.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuration Examples for Configuring Data Encryption

Displaying Data Encryption States for all Access Points: Examples

This example shows how to display the encryption state of all access points or a specific access point. This command also shows authentication errors, which track the number of integrity check failures and replay errors. Relay errors help in tracking the number of times the access point receives the same packet:

```
Switch# show ap link-encryption
                    Encryption  Dnstream  Upstream    Last
AP Name                  State     Count     Count  Update
------------------  ----------  --------  --------  ------
3602a                  Enabled         0         0   Never
```

This example shows how to display a summary of all active DTLS connections:

```
Switch# show wireless dtls connections
AP Name         Local Port   Peer IP       Peer Port  Ciphersuite
--------------- ------------ ------------- ---------- --------------------
3602a           Capwap_Ctrl  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
3602a           Capwap_Data  10.10.21.213  46075      TLS_RSA_WITH_AES_128_CBC_SHA
```