データ暗号化の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

データ暗号化を設定するための前提条件

- Cisco 1260、3500、3600、801、1140、1310、および 1520 シリーズのアクセス ポイントは、Datagram Transport Layer Security（DTLS）のデータ暗号化をサポートします。
- スイッチを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効化または無効化できます。
- シスコ スイッチを使用するロシア人以外のお客様はデータ DTLS ライセンスは必要ありません。

データ暗号化の設定に関する制限

- 暗号化はスイッチおよびアクセス ポイントの両方においてスループットを制限するため、多くのエンタープライズ ネットワークにおいて最大スループットが必要です。
- スイッチにデータ DTLS のライセンスがなく、スイッチに関連付けられているアクセス ポイントで DTLS が有効になっている場合、データ パスは暗号化されません。
- DTLS ライセンスがないイメージでは DTLS コマンドは使用できません。

データ暗号化について

スイッチにより、DTLS を使用してアクセス ポイントとスイッチの間に送信される Control And Provisioning of Wireless Access Points（CAPWAP）のコントロール パケット（および任意で CAPWAP データ パケット）を暗号化できます。 DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会（IETF）プロトコルです。 CAPWAP コントロール パケットとはスイッチとアクセス ポイントの間で交換される管理パケットであり、CAPWAP データ パケットは転送された無線フレームをカプセル化します。 CAPWAP コントロールおよびデータ パケットはそれぞれ異なる UDP ポートである 5246（コントロール）および 5247（データ）で送信されます。 アクセス ポイントが DTLS データ暗号化をサポートしない場合、DTLS はコントロール プレーンにのみ有効となり、データ プレーンの DTLS セッションは確立されません。

データ暗号化の設定方法

データ暗号化の設定（CLI）

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap link-encryption** 例： `Switch(config)# ap link-encryption`	このコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントのデータ暗号化をイネーブルにします。 デフォルト値はディセーブルです。 データ暗号化モードを変更するには、アクセス ポイントをスイッチに再 join する必要があります。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 4	**show ap link-encryption** 例： `Switch# show ap link-encryption`	すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化の状態を表示します。 このコマンドはまた、整合性チェックの失敗およびリプレイ エラーの数を追跡する認証エラーを表示します。リレー エラーは、アクセス ポイントが同じパケットを受信する回数の追跡に役立ちます。
ステップ 5	**show wireless dtls connections** 例： `Switch# show wireless dtls connections`	すべてのアクティブな DTLS 接続の概要を表示します。 （注） DTLS データ暗号化で問題が発生した場合は、**debug dtls ap** {**all**|**event**|**trace**} コマンドを入力して、すべての DTLS メッセージ、イベントまたはトレースをデバッグします。

データ暗号化の設定（GUI）

ステップ 1 [Configuration] > [Wireless] > [Access Points] > [All APs] と選択します。
[All APs] ページが表示されます。

ステップ 2 暗号化を有効にするアクセス ポイントの名前をクリックします。
[AP > Edit] ページが表示されます。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [Data Encryption] チェックボックスをオンまたはオフにします。
（注） データ暗号化モードを変更するには、アクセス ポイントをスイッチに再アソシエイトする必要があります。

ステップ 5　[Apply] をクリックします。

ステップ 6　[Save Configuration] をクリックします。

データ暗号化の設定の設定例

すべてのアクセス ポイントのデータ暗号化の状態の表示：例

次に、すべてのアクセスポイントまたは特定のアクセスポイントの暗号化の状態を表示する例を示します。このコマンドはまた、整合性チェックの失敗およびリプレイエラーの数を追跡する認証エラーを表示します。 リレー エラーは、アクセス ポイントが同じパケットを受信する回数の追跡に役立ちます。

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

次に、すべてのアクティブな DTLS 接続のサマリーを表示する例を示します。

```
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
```