



データ暗号化の設定

- 機能情報の確認, 1 ページ
- データ暗号化を設定するための前提条件, 1 ページ
- データ暗号化の設定に関する制約事項, 2 ページ
- データの暗号化について, 2 ページ
- データ暗号化の設定方法, 2 ページ
- データ暗号化の設定例, 4 ページ

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約事項

- 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。

データの暗号化について

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 CAPWAP コントロールパケット（および、オプションとして CAPWAP データパケット）の暗号化が可能です。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、スイッチとコントローラ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

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# 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： Device(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 [disabled] です。 データ暗号化モードに変更するには、アクセスポイントスイッチに再 join する必要があります。

	コマンドまたはアクション	目的
ステップ 3	end 例： Device(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： Device# 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： Device# 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 データの暗号化に問題が生じた場合は、 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）

手順

- ステップ 1 [Configuration] > [Wireless] > [Access Points] > [All Aps] の順に選択します。
[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。

```
Device# show ap link-encryption
```

AP Name	Encryption State	Dnstream Count	Upstream Count	Last 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。

```
Device# 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