WPA3 導入ガイド

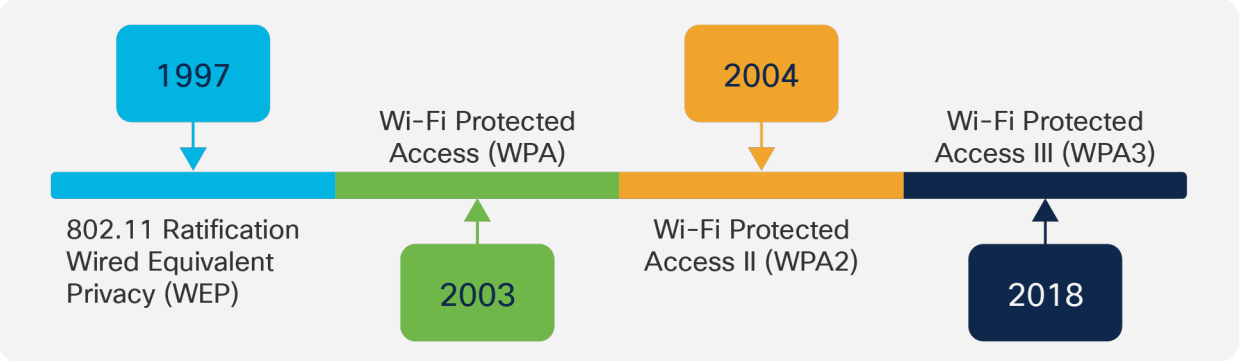
© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3 の概要

WPA3 は、Wi-Fi Alliance によって開発された Wi-Fi Protected Access 標準の最新第 3 版であり、以前の標準である WPA2 と置き換わります。WPA 標準は、ワイヤレスセキュリティを標準化することを目的として、シスコの Stephen Orr が委員長を務める Wi-Fi Alliance セキュリティ技術タスクグループによって作成されました。WPA3 では、暗号強度が向上したことより、企業、個人、およびオープン セキュリティ ネットワークに新機能がもたらされ、WPA3 対応のすべてのエンドポイントでより安全な認証プロセスが可能になりました。WPA3 Enterprise の枠組みでは、保護された管理フレーム（PMF）をすべての接続で使用することを必須にすることで、WPA2 Enterprise によって提供される強固な基盤を拡張します。このセキュリティ機能により、サービス妨害（DoS）、ハニーポット、盗聴などの危険な攻撃から保護されます。

シスコは、今後数年間で、特に政府機関や金融機関での WPA3 の採用が急増すると予想しています。インターネットに接続されたデバイスの数は 4 年以内に 416 億台に達すると予測されており、セキュリティの向上は当然の必要事項となっています。そして、WPA3 がその答えとなります。

図 1.　　Wi-Fi セキュリティ標準のタイムライン



サポートされる WPA3 モード

- WPA3-Enterprise（802.1X セキュリティネットワーク向け）。このモードでは、認証およびキー管理（AKM）として IEEE 802.1X と SHA-256 を活用します。
- WPA3-Personal。パーソナル セキュリティ ネットワークに Simultaneous Authentication of Equals（SAE）方式を使用します。
- WPA3 移行モード（個人および企業用の WPA2 + WPA3 セキュリティベース WLAN）。（17.12.1 以降、これは 1 つの SSID と 1 つのプロファイルで使用でき、6 GHz 帯域をサポートします。）
- オープン セキュリティ ネットワーク向けの Opportunistic Wireless Encryption（OWE）。

ロードマップ上の WPA3 機能

- FlexConnect モードの WPA3-Enterprise SuiteB192-1X
- WPA3-Enterprise SuiteB192-1X Fast Transition

必要なソフトウェア バージョン

1. パスワード要素生成に SAE Hash-to-Element 方式を使用する WPA3-Personal の場合、ソフトウェアバージョン 17.7.1 以降を使用する必要があります。
2. WPA3-Enterprise および WPA3-Personal 移行無効の場合、ソフトウェアバージョン 17.7.1 以降を使用する必要があります。

© 2024 Cisco and/or its affiliates. All rights reserved.

3. AKM としての SAE と Fast Transition（FT）を使用する WPA3-Personal の場合、ソフトウェアバージョン 17.9 以降を使用する必要があります。
4. FlexConnect モードの WPA3-Enterprise 802.1X-256 の場合、推奨ソフトウェアバージョンは 17.12.3 です。

シスコデバイスの互換性

表 1.　Cisco® Catalyst® 9800 シリーズ ワイヤレスコントローラの WPA3 サポートマトリックス

9800-L-F	9800-L-C	9800-L	9800-40	9800-80
対応、次のバージョン以降： 16.12.1s	対応、次のバージョン以降： 16.12.1s	対応、次のバージョン以降： 16.12.1s	対応、次のバージョン以降： 16.12.1s	対応、次のバージョン以降： 16.12.1s

表 2.　Catalyst 9100 アクセスポイントの WPA3 サポートマトリックス

9105AX	9115AX	9117AX	9120AX	9130AX	9124AXE	9136AX	9166/9164/9162
対応*	対応*	対応*	対応*	対応	対応	対応	対応

*SuiteB192-1X はサポートされていません

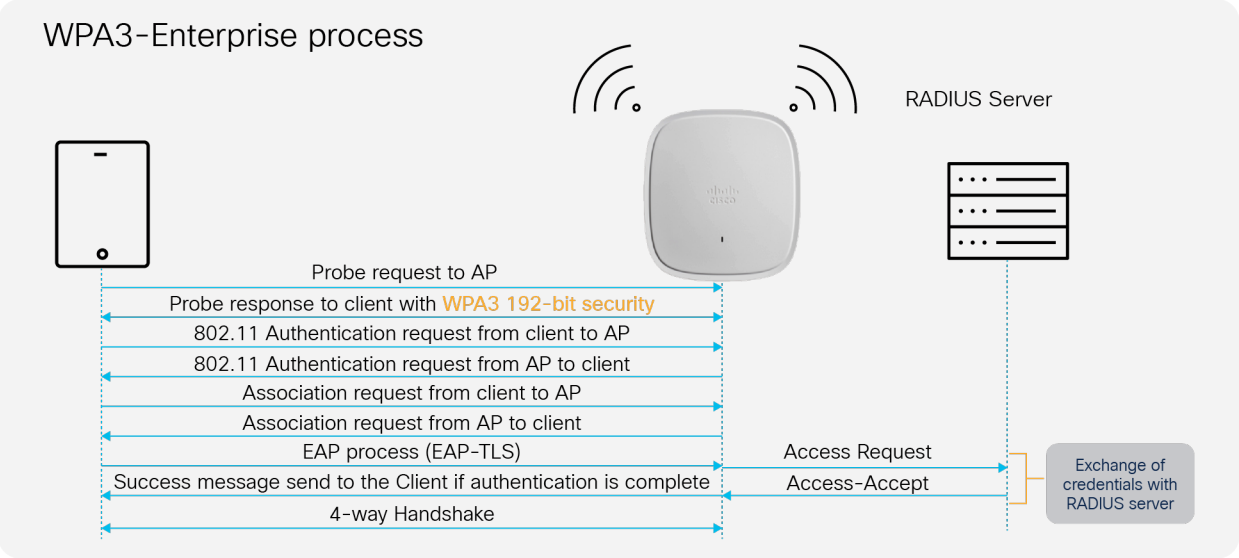
この導入ガイドの目的は、さまざまな WPA3 モードの詳細を説明し、GUI またはコマンドライン インターフェイス（CLI）を使用して Cisco Catalyst 9800 シリーズ コントローラで WPA3 モードを設定する手順を提供することです。

WPA3-Enterprise

WPA3-Enterprise は、WPA2-Enterprise の基盤の上に構築されており、RADIUS サーバーによるユーザー認証のために、保護された管理フレームを 802.1X を使用したすべての WPA3 接続で使用するという追加の要件があります。デフォルトでは、WPA3 は 128 ビット暗号化を使用しますが、オプションで GMCP-256 を使用した設定可能な SuiteB-192 ビット暗号強度の暗号化も導入されています。これにより、機密データを送信するあらゆるネットワークの保護が強化されます。WPA3-Enterprise は、ネットワークセキュリティが最も重要である企業、金融機関、政府機関、およびその他の市場セクターで高く評価され、使用が強く推奨されます。またこのような市場セクターで一般的に使用されています。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 2.　　WPA3-Enterprise エンドポイントとネットワーク ハンドシェイク プロセス



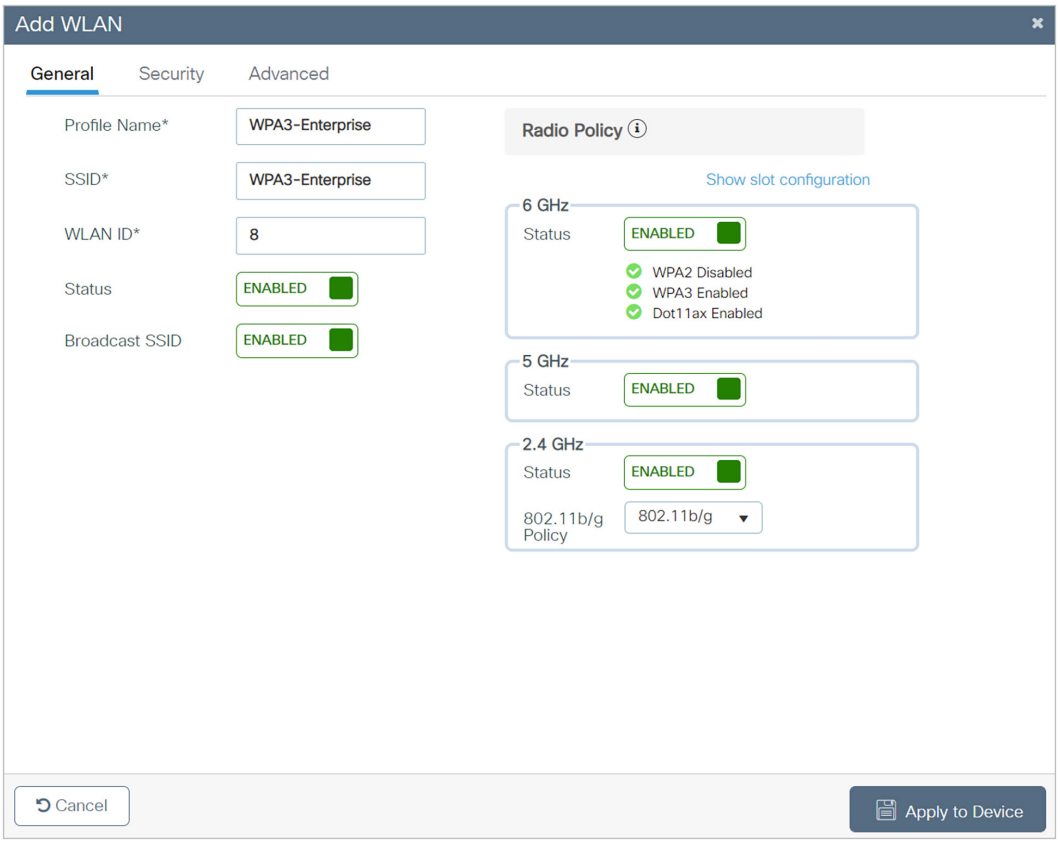
WPA3-Enterprise GUI の設定

次の手順では、WPA3-Enterprise セキュリティを使用した WLAN を作成します。

5. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
6. [Add] をクリックします。
7. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] の両方が自動的に入力されます。
8. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

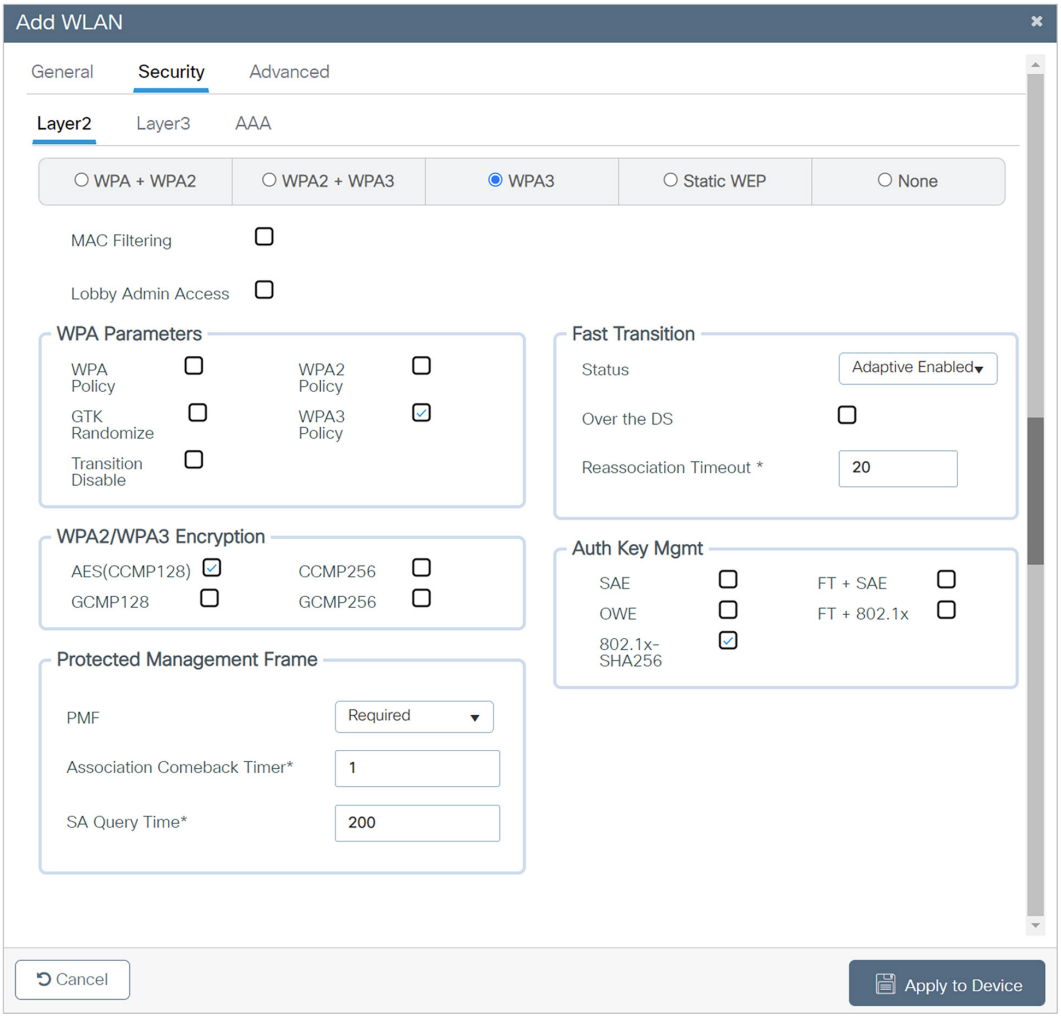
図 3.　　無線/スロットの設定



9. [Security] タブ > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。
10. [PMF] が [Required] に設定されていることを確認します。

© 2024 Cisco and/or its affiliates. All rights reserved.

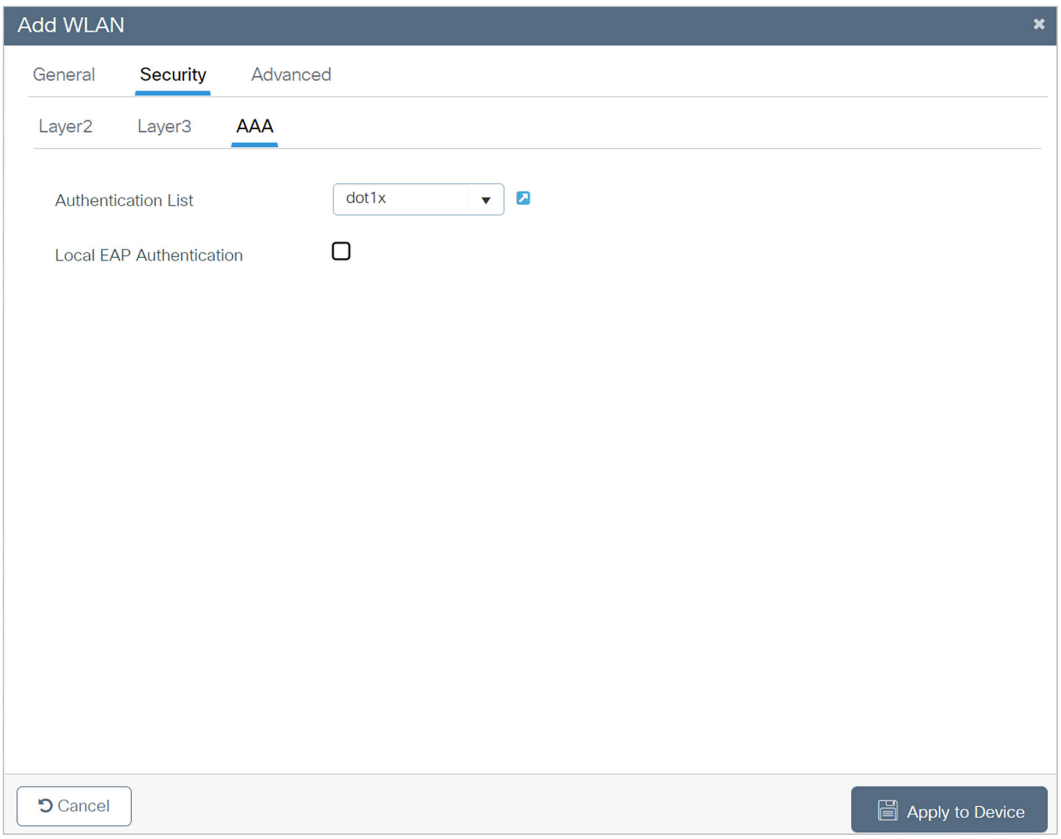
図 4.　　WLAN のセキュリティ設定



11. [WPA3 Policy]、[AES]、および [802.1X-SHA256] チェックボックスをオンにし、選択されている他のパラメータの選択をすべて解除します。
12. [Security] タブをクリックし、[AAA] タブをクリックして [Authentication List] ドロップダウンリストから事前設定済みの RADIUS サーバー認証リストを選択します。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 5.　　WLAN の AAA 設定



13. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

WPA3-Enterprise の CLI 設定

次の手順では、WPA3-Enterprise セキュリティを使用した WLAN を作成します。

表 3.　　WPA3-Enterprise の CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan WPA3-Enterprise 8 WPA3-Enterprise`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`no security wpa akm dot1x`	セキュリティ認証キー管理（AKM）802.1X-SHA1 を無効にします。
ステップ 4	`no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 5	`security wpa akm dot1x-sha256`	セキュリティ認証キー管理（AKM）802.1X-SHA2 を有効にします。
ステップ 6	`security wpa wpa3`	WPA3 のサポートを有効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

	コマンド	目的

ステップ 7	`security dot1x authentication-list list-name`
	例：
	`Device(config-wlan)# security dot1x authentication-list dot1x`
		802.1X セキュリティのセキュリティ認証リストを設定します。

ステップ 8	`no shutdown`	WLAN をイネーブルにします。
ステップ 9	`end`	特権 EXEC モードに戻ります。

WPA3-Enterprise 192 ビットの GUI 設定（オプション）

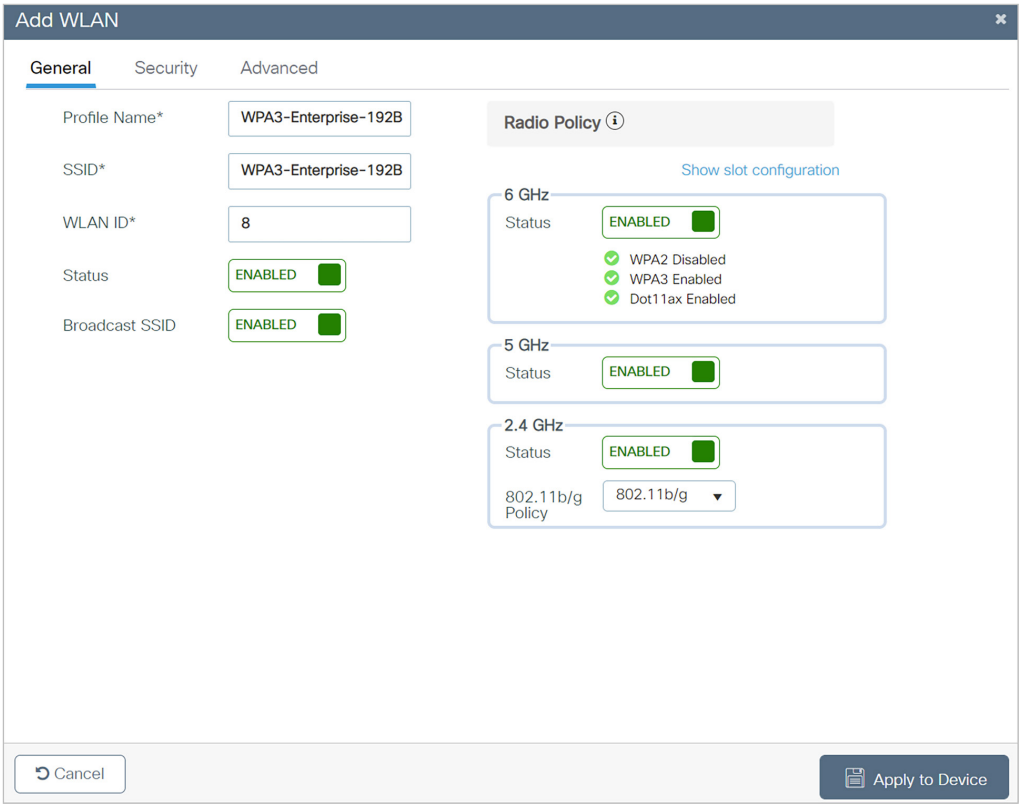
SuiteB192-1X 暗号化をサポートするエンドポイントについては、後述するクライアント相互運用性マトリックスのセクションを参照するか、デバイスのベンダーにお問い合わせください。

次の手順では、192 ビット WPA3-Enterprise セキュリティを使用して WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] の両方が自動的に入力されます。
4. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

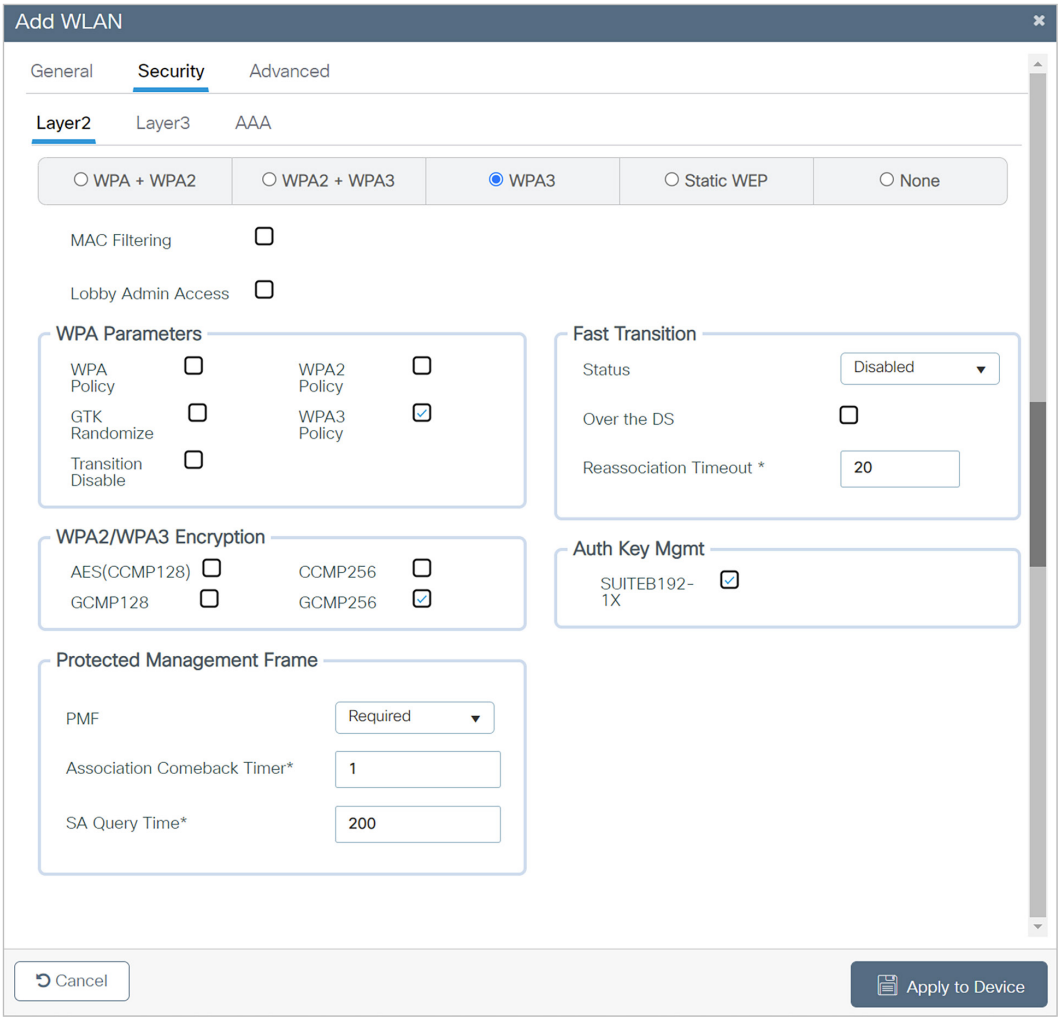
図 6.　　無線/スロットの設定



5. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。
6. [PMF] が [Required] に設定されていることを確認します。
7. Fast Transition を無効にします。
8. [WPA3 Policy]、[GCMP256]、および [SUITEB192-1X] チェックボックスをオンにして、選択されている他のパラメータの選択をすべて解除します。

© 2024 Cisco and/or its affiliates. All rights reserved.

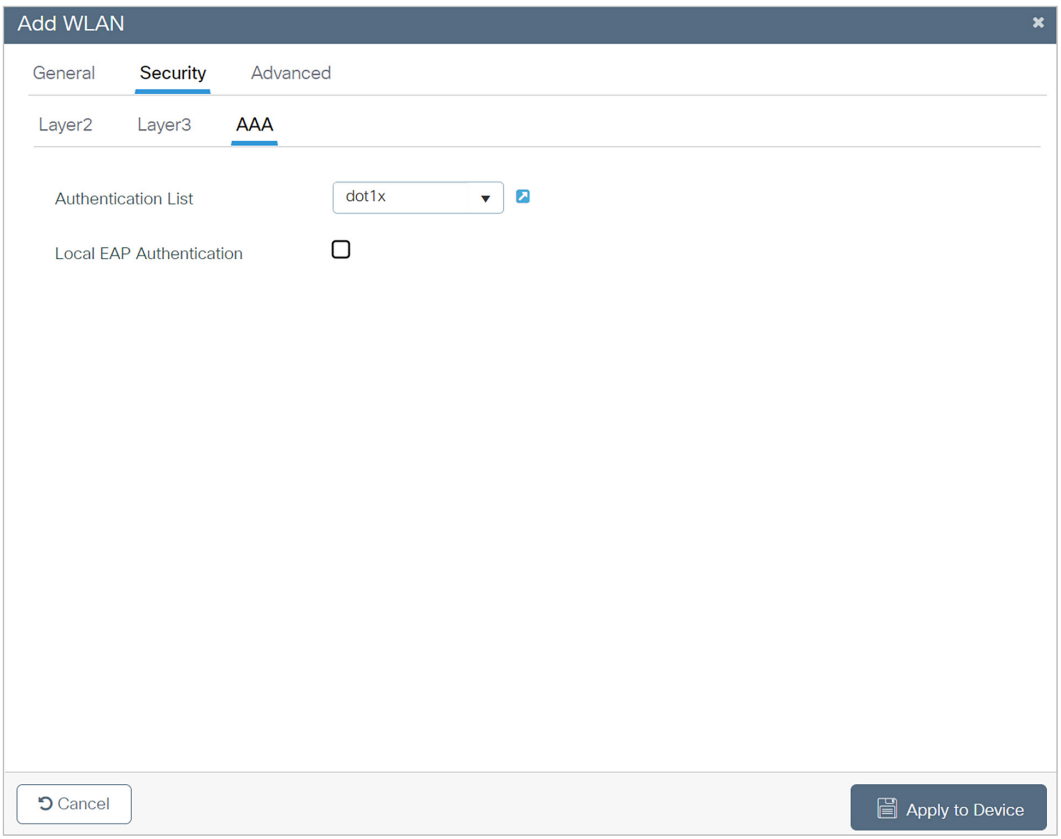
図 7.　　WLAN のセキュリティ、暗号化、および AKM の設定



9. [Security] タブをクリックし、[AAA] タブをクリックして [Authentication List] ドロップダウンリストから事前設定済みの RADIUS サーバー認証リストを選択します。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 8.　　セキュリティ AAA 方式リストの設定



10. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

注：SuiteB192-1X は、C9120/C9105/C9115 AP および FlexConnect モードではサポートされません。

WPA3-Enterprise 192 ビットの CLI 設定（オプション）

次の手順では、192 ビット WPA3-Enterprise セキュリティを使用して WLAN を作成します。

表 4.　　WPA3-Enterprise 192 ビット暗号化のCLI 設定

	コマンドまたはアクション	目的
ステップ 1	`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	`wlan <wlan-name> wlan-id <SSID-name>`
	例：
	`Device(config)# wlan WPA3-Enterprise-192B 8 WPA3-Enterprise-192B`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`no security ft adaptive`	Fast Transition Adaptive サポートを無効にします。
ステップ 4	`no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 5	`no security wpa wpa2 ciphers aes`	WPA2/CCMP128 サポートを無効にします。
ステップ 6	`security wpa wpa2 ciphers gcmp256`	GCMP256 サポートを有効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

	コマンドまたはアクション	目的
ステップ 7	`no security wpa akm dot1x`	セキュリティ AKM 802.1X-SHA1 サポートを無効にします。
ステップ 8	`security wpa wpa3`	WPA3 のサポートを有効にします。

ステップ 9	`security dot1x authentication-list list-name`
	例：
	`Device(config-wlan)# security dot1x authentication-list dot1x`
		802.1X セキュリティのセキュリティ認証リストを設定します。

ステップ 10	`no shutdown`	WLAN をイネーブルにします。
ステップ 11	`end`	特権 EXEC モードに戻ります。

WPA3-Enterprise 移行モード

WPA3-Enterprise 移行モード（WPA3+WPA2-Enterprise 混在モード設定とも呼ばれる）は、一部のクライアントが WPA2 までしかサポートできず、一部のクライアントが WPA3 までサポートできる場合に使用されます。WPA3 対応クライアントは WPA3-Enterprise の 802.1X-SHA256 AKM を使用し、WPA2 対応クライアントは WPA2-Enterprise の 802.1X SHA1 または 802.1X-SHA256 を使用できます。このモードは、2.4 GHz と 5 GHz の両方の帯域に適用されます。

注： このモードは、必要な場合にのみ使用してください。最大限のセキュリティを得るには、WPA3 のみを使用し、WPA3 と WPA2 が混在したモードを使用しないことが推奨されます。

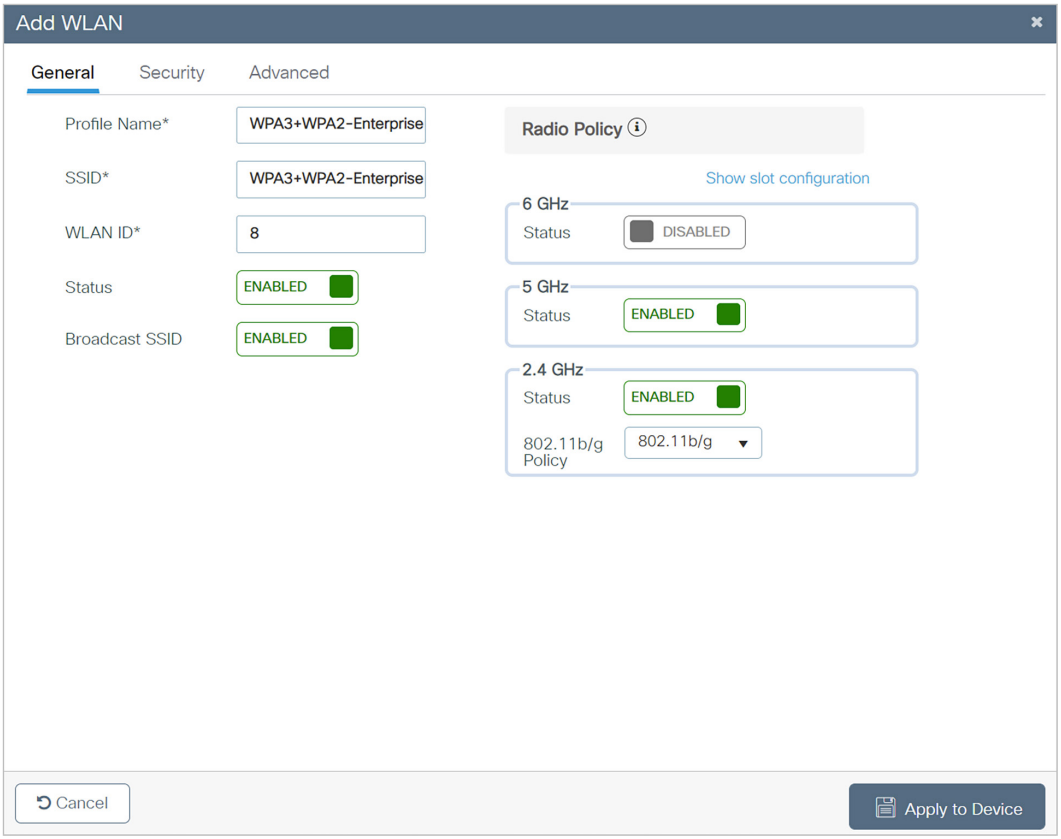
WPA3-Enterprise 移行モードの GUI 設定

次の手順では、WPA3+WPA2-Enterprise 混在モードレベルのセキュリティを備えた WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] が自動的に入力されます。
4. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。
5. [6-GHz] 無線ポリシーはサポートされていないため、無効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

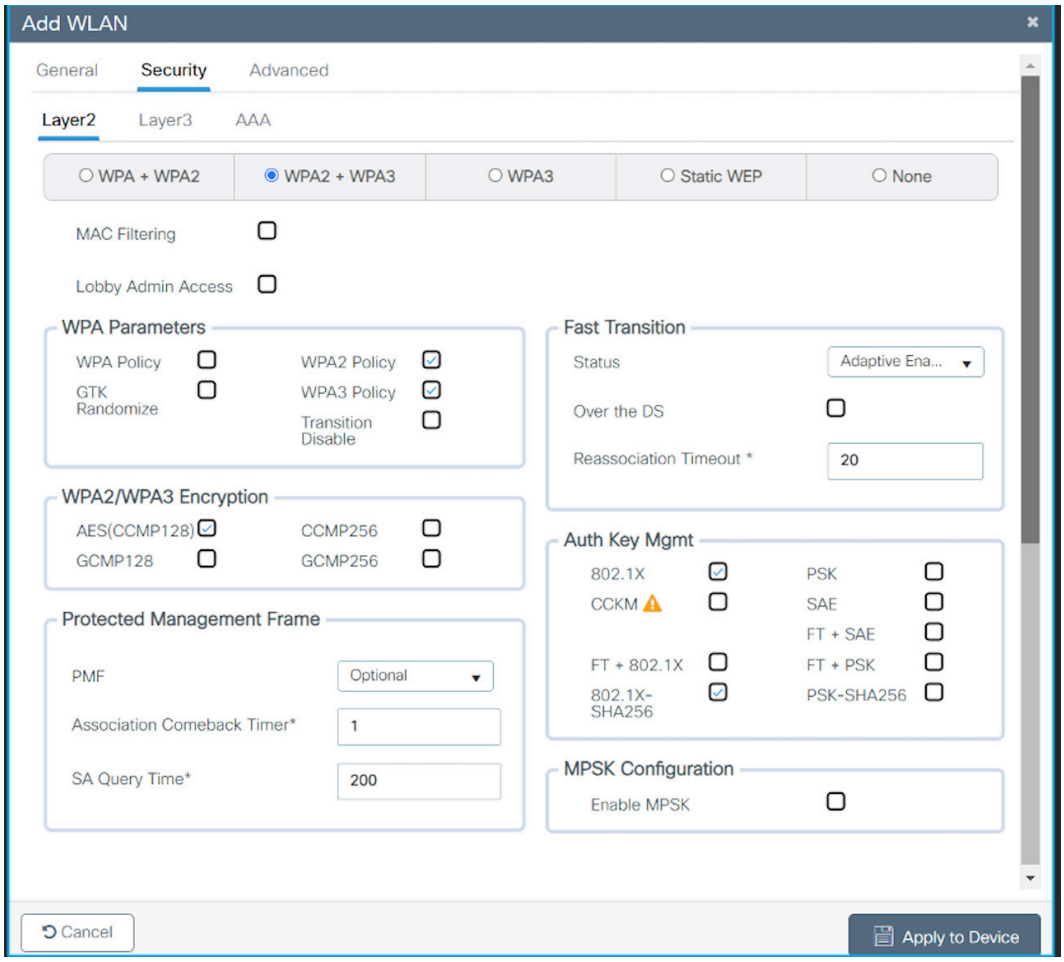
図 9.　　無線/スロットポリシーの設定



6. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。
7. [PMF] が [Optional] に設定されていることを確認します。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 10.　　セキュリティ、暗号化、および AKM の設定



8. [WPA Parameters] まで下にスクロールします。[WPA2 Policy]、[WPA3 Policy]、および [Encryption] の [AES] チェックボックスをオンにし、[802.1X] と [802.1X-SHA256] チェックボックスをオンにします。
9. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Enterprise 移行モードの CLI 設定

次の手順では、WPA3+WPA2-Enterprise 混在モードレベルのセキュリティを備えた WLAN を作成します。

表 5.　　WPA3-Enterprise 移行モードの CLI 設定

	コマンド	目的
ステップ 1	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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device (config)# wlan WPA3+WPA2-Enterprise 8 WPA3+WPA2-Enterprise`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`security wpa wpa3`	WPA3 を有効にします。
ステップ 4	`Security wpa wpa2`	WPA2 を有効にします。
ステップ 5	`security wpa akm dot1x-sha256`	802.1X SHA2 AKM を有効にします。
ステップ 6	`radio policy dot11 24ghz`	2.4 GHz 帯域を有効にします。
ステップ 7	`radio policy dot11 5ghz`	5 GHz 帯域を有効にします。
ステップ 8	`no shutdown`	
ステップ 9	`end`	

注：このセキュリティの組み合わせは、FT 対応モードでも使用できます。

WPA3-Enterprise Transition Disable モード

ネットワークアップグレードの容易さ：WPA2 デバイスが Wi-Fi ネットワークに長年存在しているため、WPA2 デバイスと WPA3 デバイスの両方が共存できる展開モードが重要でした。これは、Wi-Fi ネットワークが WPA2 ベースのネットワークから WPA3 ベースのネットワークに徐々に移行するのに確実に役立ちます。Wi-Fi Alliance は、パーソナルネットワークとエンタープライズ ネットワークの両方に WPA3 移行モードを導入しました。SSID で移行モードを有効にすると、WPA2 をサポートするデバイスと WPA3 をサポートするデバイスを同時に接続できるため、WPA2 から WPA3 へのデバイスエコシステムの段階的な移行への道が開かれます。

Transition Disable：移行モードを使用すると上記のようにネットワークアップグレードが容易になりますが、ダウングレード攻撃を受けている WPA3 STA（ステーション）のセキュリティ上の課題があります。攻撃者は、WPA3 STA を強制的にダウングレードして、WPA2 および従来のセキュリティ脆弱性のあるテクノロジーを使用させることができます。この問題を回避するために、Wi-Fi アライアンスは「Transition Disable」指示を導入しました。これを使用して、AP とネットワークのオペレーターは、WPA3 STA を更新してネットワークを完全にアップグレードし、移行モードで定義された最もセキュアなアルゴリズムをサポートするようにできます。Transition Disable 指示は、STA 上の該当ネットワークの移行モードを無効にするために（アソシエーション中の 4 ウェイ ハンドシェイクで）使用され、ダウングレード攻撃に対する保護を提供します。STA は、この指示を受信すると、後続の接続に対して特定の移行モードを無効にし、PMF のネゴシエーションなしのアソシエーションを拒否します。

© 2024 Cisco and/or its affiliates. All rights reserved.

STA 実装により、ネットワークプロファイルで特定の移行モード（および他のレガシーセキュリティアルゴリズム）が有効になる場合があります。

たとえば、WPA3-Personal STA は、ネットワークプロファイルで、事前共有キー（PSK）アルゴリズムを有効にする WPA3-Personal 移行モードをデフォルトで有効にする場合があります。しかし、ネットワークが移行モードで定義された最もセキュアなアルゴリズムを（完全に）サポートしている場合、STA で Transition Disable 指示を使用して、そのネットワークの移行モードを無効にし、ダウングレード攻撃から保護できます。

これによりすべてのクライアントデバイスは、移行モードの WLAN に参加するときに WPA3 のみに移行するため、セキュリティ面では優れている一方で、ネットワークが複数の物理的な場所で構成されている場合、たとえば、一部が WPA2 に設定され、その他が WPA3/WPA2 移行モードに設定されている場合、移行したクライアントが WPA2 のみを使用する場所に移動すると接続に失敗することになります。

これは、同じ SSID が異なるコントローラ/AP セットアップをカバーし、設定が 100% 一致しない一部の大規模ネットワークで考えられるシナリオです。最も規模が大きな例は、世界中で同じ SSID 名を共有する Edu Roam です。これを設定すると、異なるネットワークプロバイダー間を移動するクライアントに重大な問題が発生する可能性があるため、すべてのネットワークの場所で同じセキュリティ設定が適切に設定されていることを確認できる場合にのみ、慎重に使用してください。

この方法は通常は推奨されません。絶対に必要な場合にのみ有効にする必要があります。

以下のセクションでは、WLAN で Transition Disable を有効にする方法について説明します。

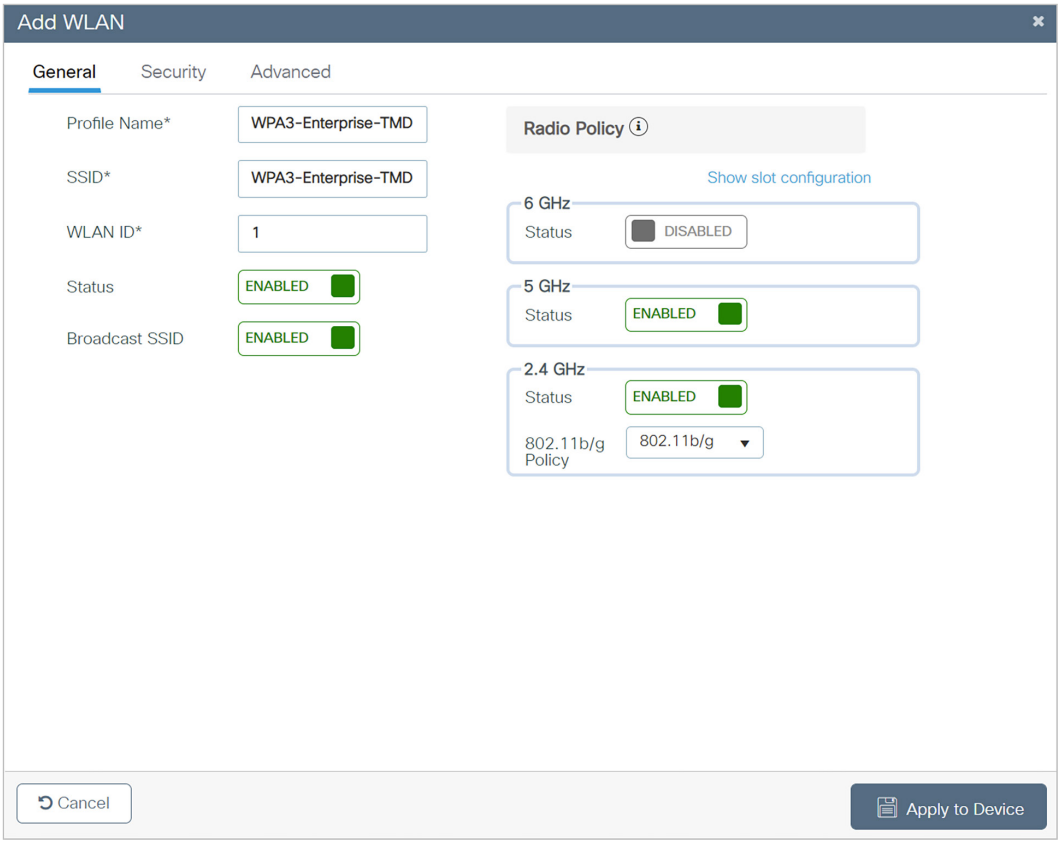
WPA3-Enterprise Transition Disable モードの GUI 設定

次の手順では、Transition Disable を有効にして WPA3-Enterprise セキュリティを備えた WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] が自動的に入力されます。
4. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

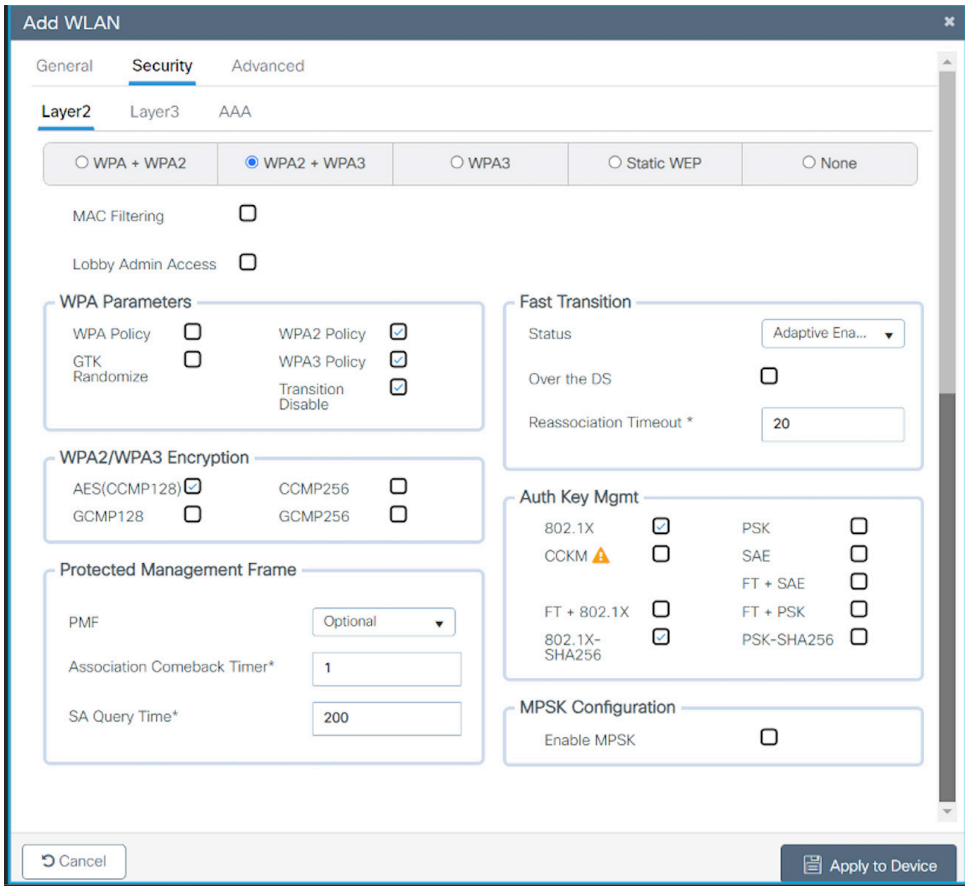
図 11.　　無線ポリシーの設定



5. [6 GHz] ポリシーはサポートされていないため、無効にします。
6. [Security] タブをクリックして、[WPA2 + WPA3] オプションを有効にします。
7. [WPA Parameters] まで下にスクロールします。[WPA2 Policy] と [WPA3 Policy]、[AES]、AKM として [802.1X] と [802.1X-SHA256] チェックボックスをオンにします。
8. [PMF] が [Optional] に設定されていることを確認します。
9. [WPA Parameters] で [Transition Disable] を有効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 12.　　セキュリティ、暗号化、および AKM の設定



WPA3-Enterprise Transition Disable モードの CLI 設定

表 6.　　WPA3-Enterprise Transition Disable モードの CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan WPA3-Enterprise-TMD 1 WPA3-Enterprise-TMD`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`security wpa wpa3`	WPA3 を有効にします。
ステップ 4	`security wpa wpa2`	WPA2 セキュリティを有効にします。PMF はオプションになっています。
ステップ 5	`security wpa wpa2 ciphers aes`	Advanced Encryption Standard（AES）/CCMP128 暗号を有効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

	コマンド	目的
ステップ 6	`security wpa akm dot1x-sha256`	AKM 802.1x-SHA256 を有効にします。
ステップ 7	**`transition-disable`**	Transition Disable を有効にします。
ステップ 8	`radio policy dot11 5ghz`	5 GHz 帯域を有効にします。
ステップ 9	`radio policy dot11 24ghz`	2.4 GHz 帯域を有効にします。
ステップ 10	`no shutdown`	WLAN をイネーブルにします。
ステップ 11	`end`	特権 EXEC モードに戻ります。

注：このセキュリティの組み合わせは、FT 対応モードでも使用できます。

WPA2+WPA3-Enterprise 移行モード（6 GHz）

6 GHz 規格では、WPA2 セキュリティ（WPA2 のみと WPA2+WPA3 WLAN の両方に適用）が設定されている場合、6 GHz 帯域での WLAN のブロードキャストは許可されません。したがって、その本質から、WLAN が WPA2 で設定されている場合は 6 GHz 無線をサポートしないという動作になります。

これは、レガシークライアントが同じ SSID の 5 GHz でオプションの PMF とともに 802.1X-SHA1 をサポートする必要がある特定のユースケースで制限をもたらしますが、一方で 6 GHz クライアントは PMF 必須で 802.1X-SHA256 AKM をサポートします。

これらの展開をサポートするために、17.12.1 より前の SW バージョンでは、レガシーと最新の 6 GHz クライアントの両方をサポートするために、異なるプロファイルを持つ同じ WLAN で WPA2 + WPA3 移行モードを使用することが推奨されていました。この設計の課題はローミングです。この設定での帯域間のローミングはサポートされておらず、これは常にフルローミングであり、推奨されません。

17.12.1 以降、6 GHz 帯域の純粋な WPA3 の移行モードがサポートされています。これにより、ユーザーは 6 GHz の同じ WLAN で WPA2 + WPA3 を有効にできます。このモードでは、レガシーの 6 GHz デバイスと最新の 6 GHz デバイスに対応するために 2 つの異なるプロファイルを作成する必要がなくなります。このモードでは、WPA2+WPA3 移行モードは 2.4 GHz/5 GHz で使用でき、WLAN に WPA2 と WPA3 の両方の設定がある場合、WPA3 関連の設定のみが 6 GHz 帯域にプッシュされます。

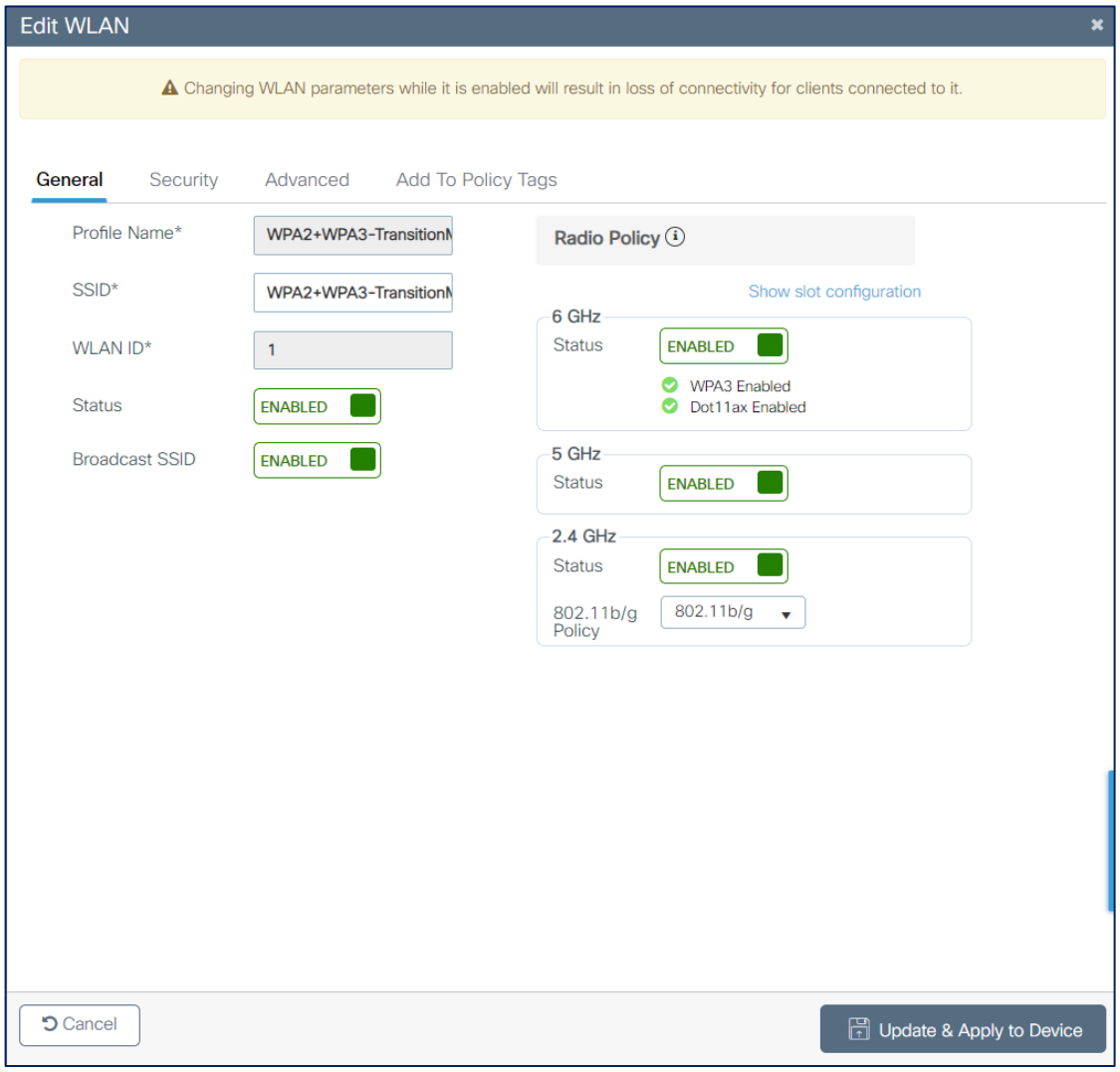
WPA2+WPA3-Enterprise 移行モード（6 GHz）：GUI 設定

次の手順では、WPA2+WPA3-Enterprise 移行モード（6 GHz）の WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] の両方が自動的に入力されます。
4. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 13.　　無線/スロットの設定

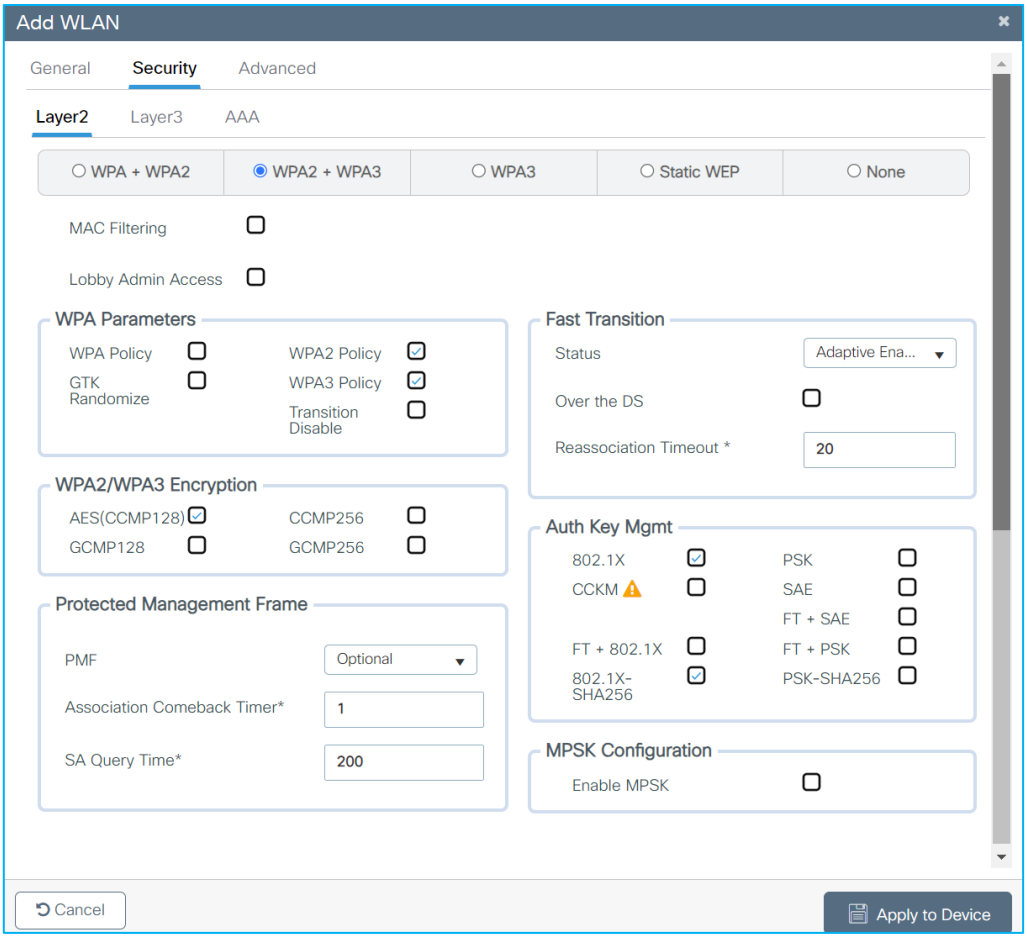


5. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。
6. [PMF] が [Optional] に設定されていることを確認します。

   注：PMF はオプションですが、WPA3 設定では、6 GHz 帯域で必須と見なされます。
7. [WPA Parameters] まで下にスクロールします。[WPA2 Policy] と [WPA3 Policy]、[WPA2/WPA3 Encryption] の [AES(CCMP128)]、および [802.1X] と [802.1X-SHA256] チェックボックスをオンにして、その他の選択されているパラメータをすべてオフにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

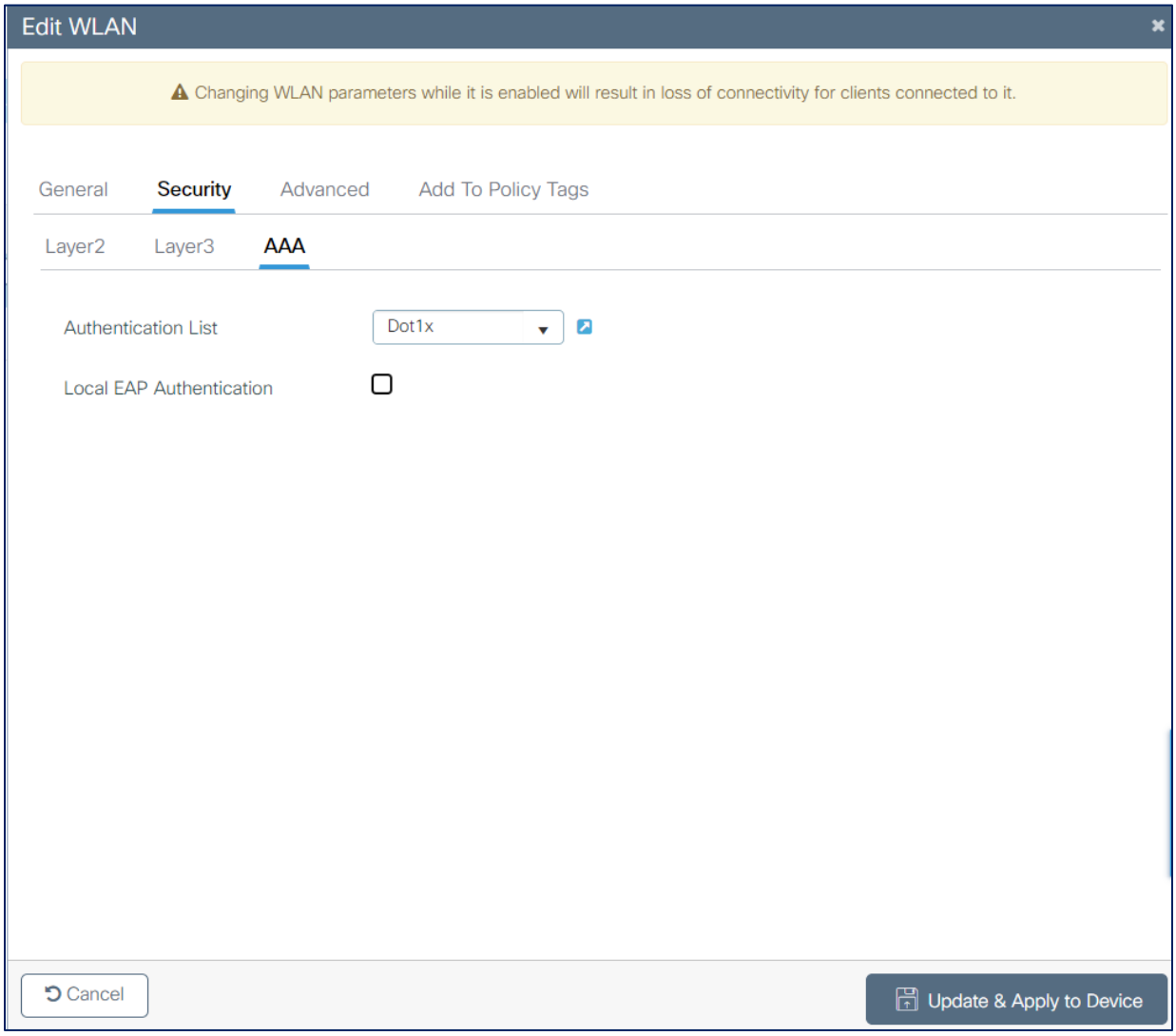
図 14.　　無線/スロットの設定



8. [Security] タブをクリックし、[AAA] タブをクリックして [Authentication List] ドロップダウンリストから事前設定済みの RADIUS サーバー認証リストを選択します。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 15.　　無線/スロットの設定



9. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

WPA2+WPA3-Enterprise 移行モード（6 GHz）の CLI 設定

次の手順では、WPA2+WPA3-Enterprise 移行モード（6 GHz）の WLAN を作成します。

表 7.　　WPA2+WPA3-Enterprise 移行モードの CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	Example:
	`Device (config)# wlan WPA2+WPA3-TransitionMode 1 WPA2+WPA3-TransitionMode`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`security wpa wpa3`	WPA3 を有効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

	コマンド	目的
ステップ 4	security wpa wpa2	WPA2 を有効にします。
ステップ 5	security wpa akm dot1x-sha256	SHA2 AKM を有効にします。
ステップ 6	security wpa akm dot1x	SHA1 AKM を有効にします。
ステップ 7	radio policy dot11 6ghz	6 GHz 帯域を有効にします。
ステップ 8	radio policy dot11 24ghz	2.4 GHz 帯域を有効にします。
ステップ 9	radio policy dot11 5ghz	5 GHz 帯域を有効にします。
ステップ 10	no shutdown	
ステップ 11	end	

WPA2+WPA3-Enterprise 移行モード（6 GHz）の CLI 出力

```
#show wlan summary
           Number of WLANs: 1
           ID    Profile Name                    SSID                            Status
           2.4GHz/5GHz Security
           6GHz Security
           ------------------------------------------------------------------------------------
           ------------------------------------------------------------------------------------
           ------------------------------------------------------------------------------------
           ----------------------------------
           1     WPA2+WPA3-TransitionMode        WPA2+WPA3-TransitionMode        UP
           [WPA2 + WPA3][802.1x][AES][PMF 802.1X]
           [WPA3][AES][PMF 802.1X]
```

注： この設定は、GCM256 暗号化 SuiteB192-1X でもサポートされています。純粋な WPA3 を使用した WPA2+WPA3 移行モードが 192 ビット暗号化とともに有効になっている場合、帯域は次のように動作します。

- 2.4 GHz および 5 GHz：WPA2 + WPA3-SUITEB-192-1X-GCMP256
- 6 GHz：WPA3-SUITEB-192-1X-CCMP256

WPA3-Personal

WPA3-Personal は、ユーザー認証の目的で、SAE によるパスワードベースの認証方式で 128 ビットの暗号強度を使用します。さらに、WPA2-Personal とは異なり、WPA3-Personal は、パスワードの推測を制限して、ユーザーがこれを行う際に毎回ライブネットワークと対話することを要求することで、オフライン辞書攻撃に対するネットワークセキュリティを強化します。この要件により、ネットワークへのハッキングに時間がかかり、ブルートフォース攻撃の試みが抑されます。

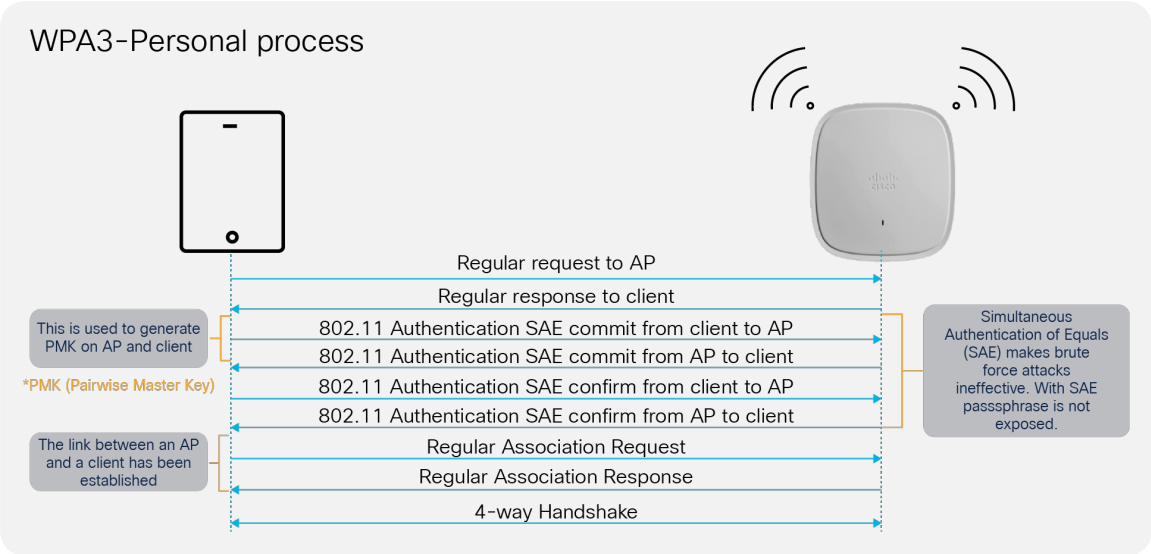
WPA3-Personal には、次の主な利点があります。

- SAE 認証ごとに異なる共有秘密を作成する

© 2024 Cisco and/or its affiliates. All rights reserved.

- ブルートフォース「辞書」攻撃と受動劇攻撃からの保護
- 前方秘匿性を提供

図 16.　　WPA3-Personal のエンドポイントとネットワーク ハンドシェイク プロセス



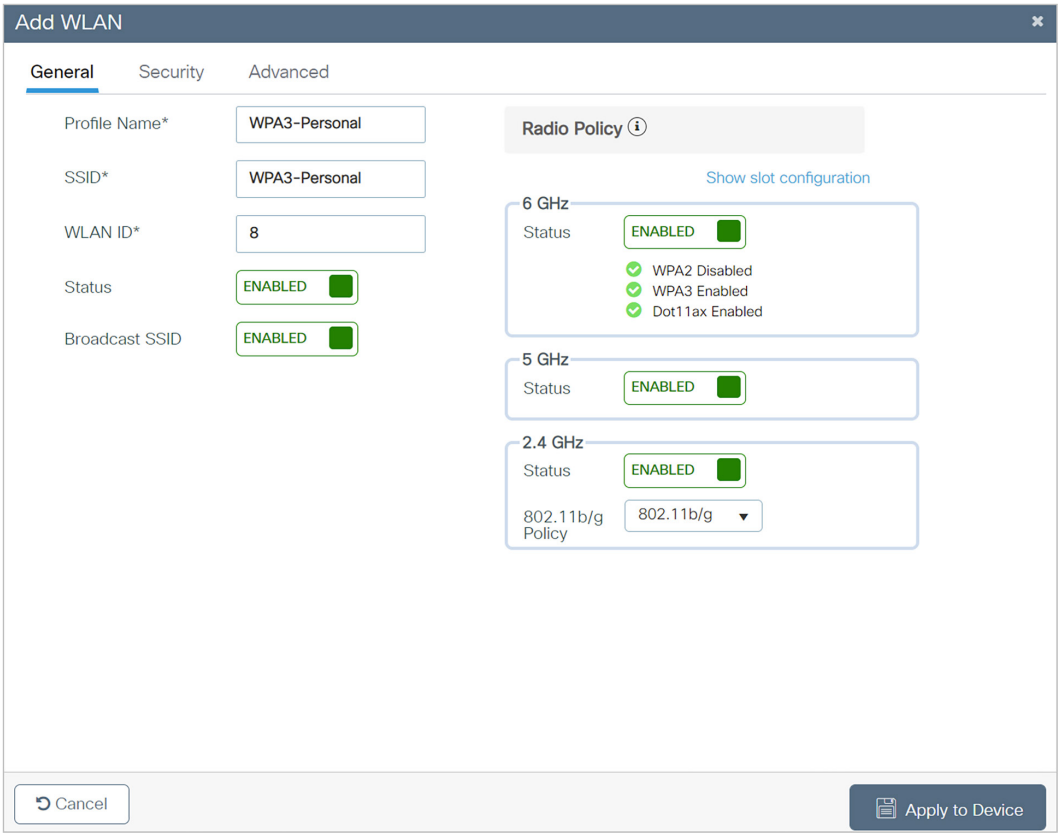
WPA3-Personal の GUI 設定

次の手順では、WPA3-Personal レベルのセキュリティを備えた WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] が自動的に入力されます。
4. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

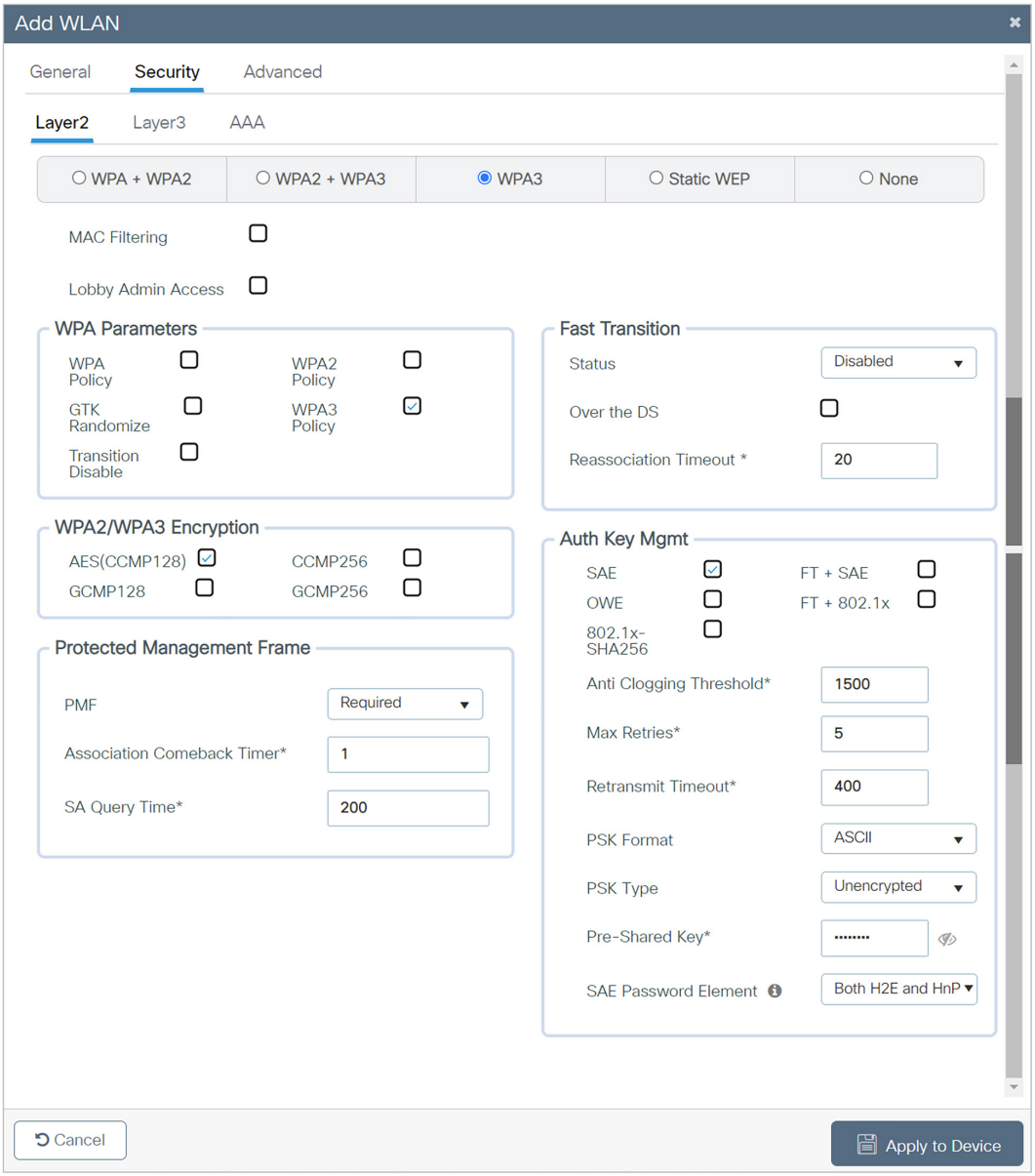
図 17.　　WPA3-Personal 無線/スロットの設定



5. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。
6. [PMF] が [Required] に設定されていることを確認します。
7. Fast Transition を無効にします。
8. [WPA Parameters] まで下にスクロールします。[WPA3 Policy]、[AES]、および [SAE] チェックボックスをオンにします。
9. [Pre-Shared Key] を入力し、[PSK Format] ドロップダウンリストから PSK フォーマットを選択し、[PSK Type] ドロップダウンリストから PSK タイプを選択します。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 18.　　WPA3 SAE AKM の設定



10. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

注：　6 GHz 帯域のみを使用する場合、サポートされる SAE のパスワード要素は Hash to Element（H2E）です。Hunting and Pecking（HnP）は、6 GHz のみのネットワークでは使用できません。5 GHz と 2.4 GHz の両方を使用する場合は、H2E と HnP を SAE のパスワード要素として使用できます。

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Personal の CLI 設定

次の手順では、WPA3-Personal レベルのセキュリティを備えた WLAN を作成します。

表 8.　　WPA3-Personal の CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan WPA3-Personal 8 WPA3-Personal`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`no security wpa akm dot1x`	セキュリティ AKM 802.1X を無効にします。
ステップ 4	`no security ft over-the-ds`	WLAN 上のデータソースを介した Fast Transition を無効にします。
ステップ 5	`no security ft`	WLAN の 802.11r 高速移行をディセーブルにします。
ステップ 6	`no security wpa wpa2`	WPA2 セキュリティを無効にします。これで PMF は無効になります。
ステップ 7	`security wpa wpa2 ciphers aes`	Advanced Encryption Standard（AES）/CCMP128 暗号を有効にします。

ステップ 8	`security wpa psk set-key ascii value preshared-key`
	`Example:`
	`Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`
		事前共有キーを指定します。

ステップ 9	`security wpa wpa3`	WPA3 のサポートを有効にします。 **注：**WPA2 と WPA3 の両方がサポートされている場合（SAE と PSK の組み合わせ）、PMF の設定は任意です。ただし、PMF を無効にすることはできません。WPA3 の場合、PMF は必須です。
ステップ 10	`security wpa akm sae`	AKM SAE のサポートを有効にします。
ステップ 11	`security wpa akm sae pwe h2e/hnp/both`	パスワード要素を選択します。
ステップ 12	`no shutdown`	WLAN をイネーブルにします。
ステップ 13	`End`	特権 EXEC モードに戻ります。

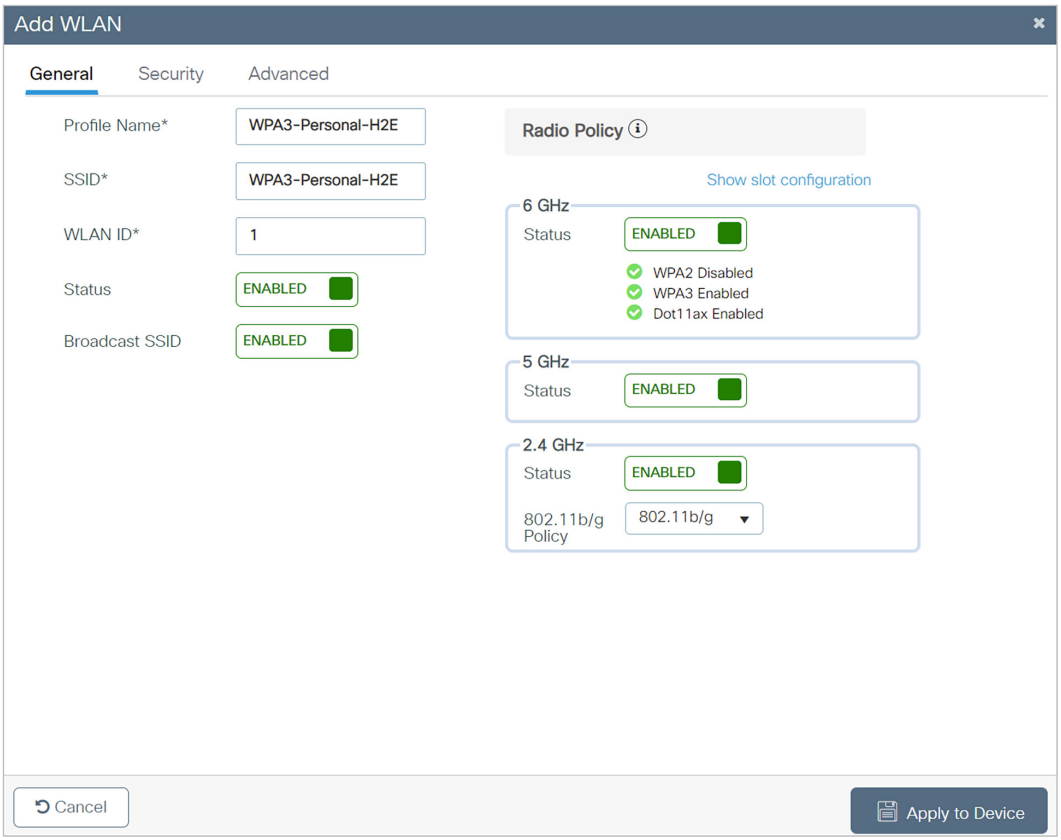
© 2024 Cisco and/or its affiliates. All rights reserved.

パスワード要素を生成するために SAE Hash-to-Element 方式を使用した WPA3-Personal

次の手順では、パスワード要素の生成に H2E を使用した、WPA3 パーソナルレベルのセキュリティを備えた WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] が自動的に入力されます。
4. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。
5. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。

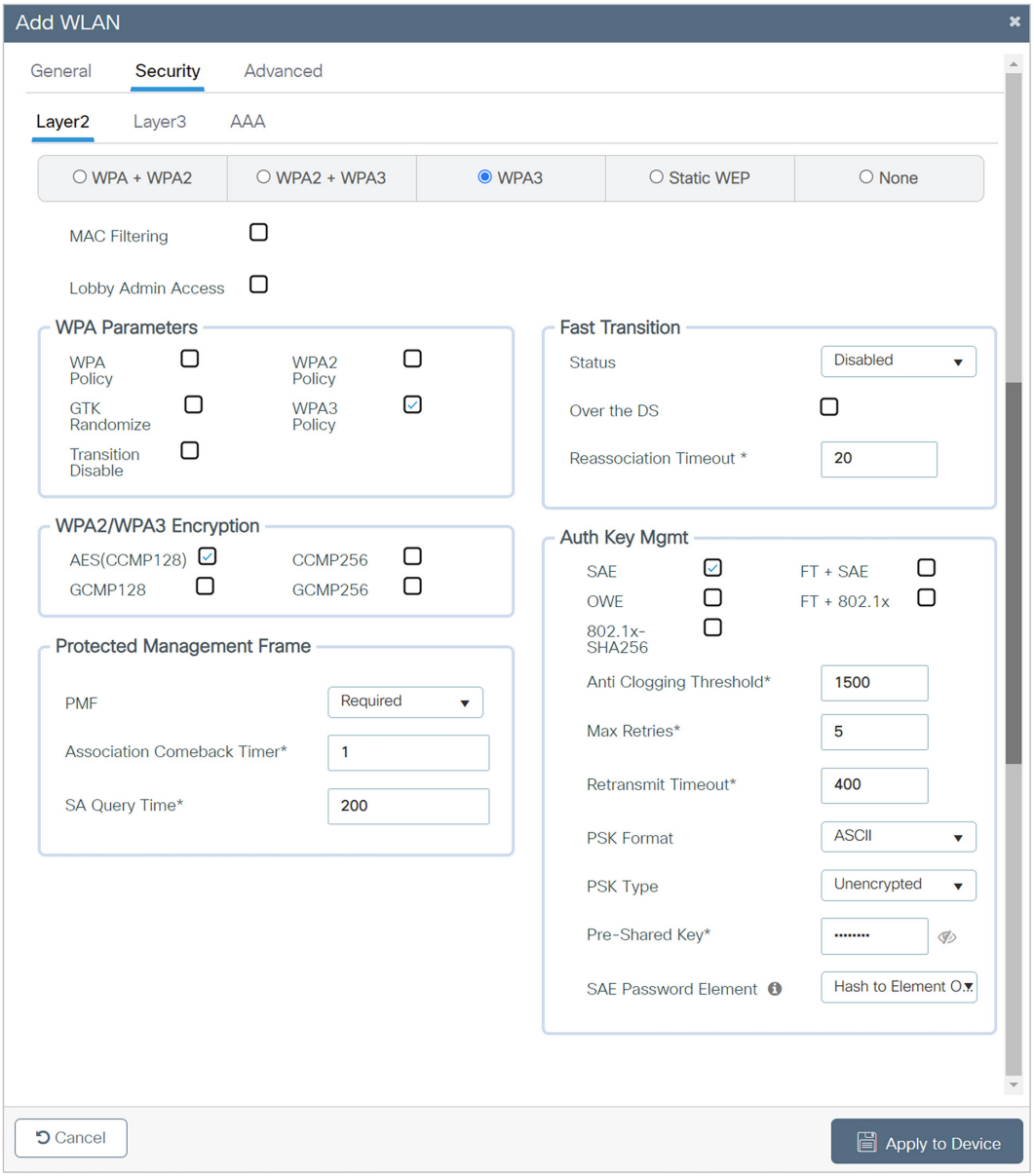
図 19.　　無線/スロットポリシーの設定



6. [PMF] が [Required] に設定されていることを確認します。
7. Fast Transition を無効にします。
8. [WPA Parameters] まで下にスクロールします。[WPA3 Policy]、[AES]、および [SAE] チェックボックスをオンにします。
9. [Pre-Shared Key] を入力し、[PSK Format] ドロップダウンリストから PSK フォーマットを選択し、[PSK Type] ドロップダウンリストから PSK タイプを選択します。
10. [SAE Password Element] ドロップダウンリストから、[Hash to Element Only] を有効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 20.　セキュリティおよび AKM パスワード要素の設定



注：　6 GHz 帯域のみを使用する場合、サポートされる SAE のパスワード要素は H2E です。HnP は、6 GHz のみのネットワークでは使用できません。5 GHz と 2.4 GHz の両方を使用する場合は、H2E と HnP を SAE のパスワード要素として使用できます。

© 2024 Cisco and/or its affiliates. All rights reserved.

パスワード要素を生成するために SAE Hash-to-Element 方式を使用した WPA3-Personal のCLI 設定

次の手順では、パスワード要素の生成に H2E を使用した、WPA3 パーソナルレベルのセキュリティを備えた WLAN を作成します。

表 9.　　WPA3-Personal SAE hash-to-element の CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan WPA3-Personal-H2E 1 WPA3-Personal-H2E`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`no security wpa akm dot1x`	セキュリティ AKM 802.1X を無効にします。
ステップ 4	`security wpa wpa3`	WPA3 を有効にします。
ステップ 5	`no security ft`	WLAN の 802.11r 高速移行をディセーブルにします。
ステップ 6	`no security wpa wpa2`	WPA2 セキュリティを無効にします。これで PMF は無効になります。
ステップ 7	`security wpa wpa2 ciphers aes`	AES/CCMP128 暗号を有効にします。

ステップ 8	`security wpa psk set-key ascii value preshared-key`
	`Example:`
	`Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`
		事前共有キーを指定します。

ステップ 9	`security wpa akm sae`	AKM SAE のサポートを有効にします。
ステップ 10	`security wpa akm sae pwe h2e`	パスワード要素を生成するための H2E を有効にします。
ステップ 11	`no shutdown`	WLAN をイネーブルにします。
ステップ 12	`End`	特権 EXEC モードに戻ります。

© 2024 Cisco and/or its affiliates. All rights reserved.

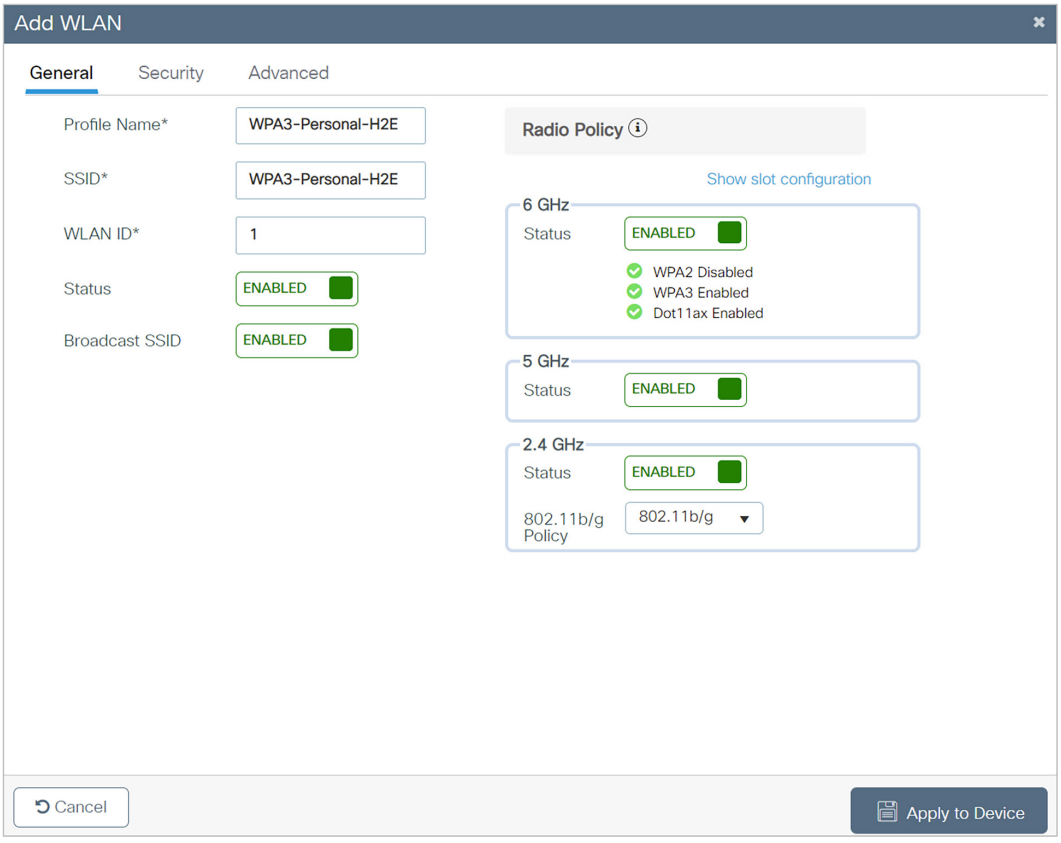
Fast Transition が有効な WPA3-Personal SAE

Cisco IOS® XE バージョン 17.9.1 以降では、Fast Transition が有効な WPA3-Personal SAE （SAE-FT）がサポートされています。WPA3 SAE-FT 用に WLAN を設定するには、次の手順に従います。

次の手順では、Fast Transition を有効にして、WPA3-Personal レベルの SAE セキュリティを備えた WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [追加（Add）] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] が自動的に入力されます。
4. [Status] と [Broadcast SSID] トグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。
5. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。

図 21.　　無線ポリシーの設定

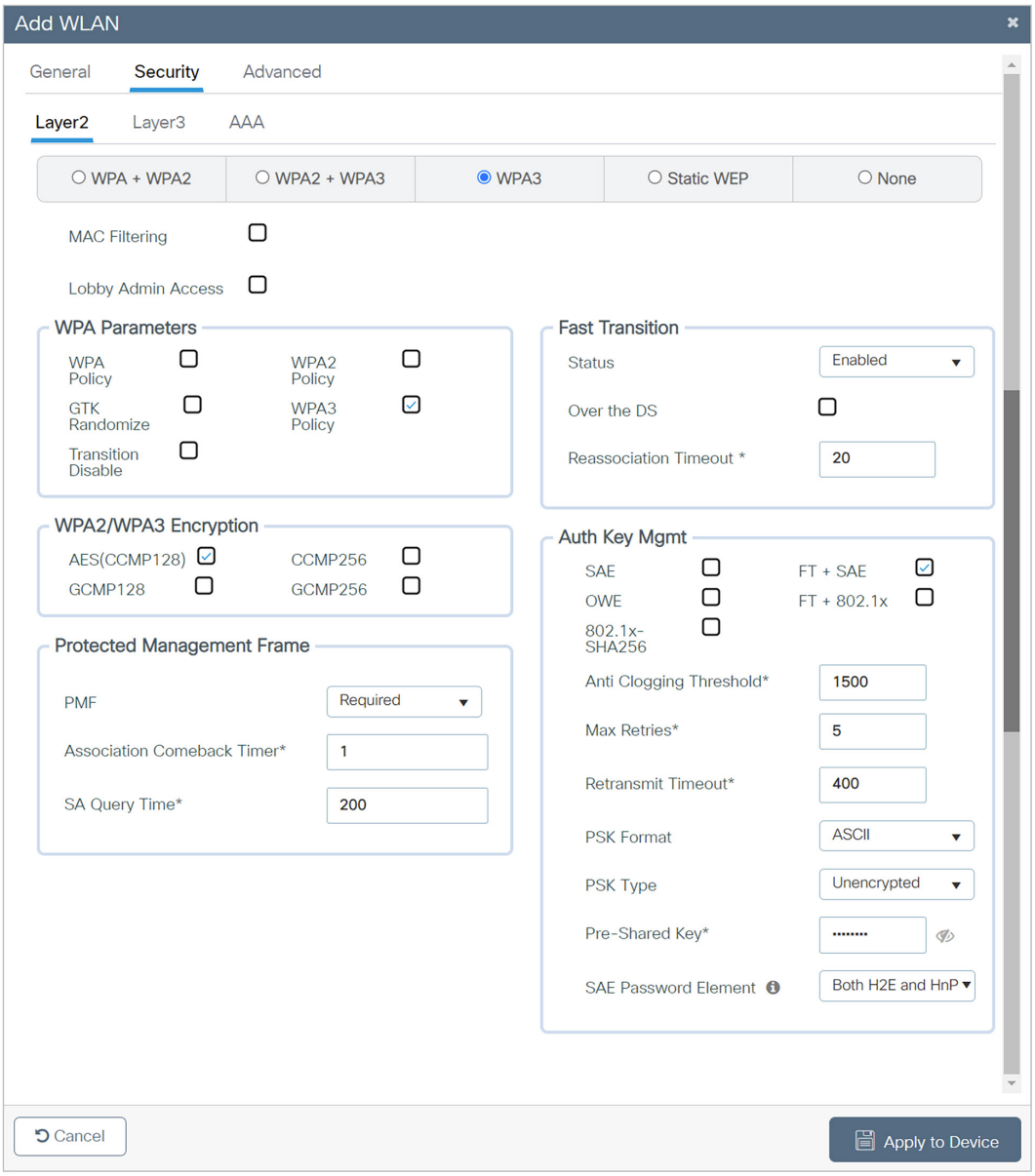


6. [PMF] が [Required] に設定されていることを確認します。
7. Fast Transition を有効にします。
8. [WPA Parameters] まで下にスクロールします。[WPA3 Policy]、[AES]、および [SAE] チェックボックスをオンにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

9. [Pre-Shared Key] を入力し、[PSK Format] ドロップダウンリストから PSK フォーマットを選択し、[PSK Type] ドロップダウンリストから PSK タイプを選択します。
10. [SAE Password Element] ドロップダウンリストから、[Hash to Element Only] または [HnP] または [both]を 有効にします。

図 22.　　FT が有効になっている WPA3 SAE



© 2024 Cisco and/or its affiliates. All rights reserved.

Fast Transition が有効な WPA3-Personal SAE の CLI 設定

次の手順では、Fast Transition を有効にして、WPA3-Personal レベルのセキュリティを備えた WLAN を作成します。

表 10.　　WPA3-Personal SAE FT の CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan WPA3-Personal-H2E 1 WPA3-Personal-H2E`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`no security wpa akm dot1x`	セキュリティ AKM 802.1X を無効にします。
ステップ 4	`security wpa wpa3`	WPA3 を有効にします。
ステップ 5	**`security ft`**	WLAN で 802.11r 高速移行を有効にします。
ステップ 6	`no security wpa wpa2`	WPA2 セキュリティを無効にします。これで PMF は無効になります。
ステップ 7	`security wpa wpa2 ciphers aes`	AES/CCMP128 暗号を有効にします。

ステップ 8	`security wpa psk set-key ascii value preshared-key`
	`Example:`
	`Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`
		事前共有キーを指定します。

ステップ 9	`security wpa akm sae`	AKM SAE のサポートを有効にします。
ステップ 10	`Security wpa akm ft sae`	FT SAE を有効にします。
ステップ 11	**`security wpa akm sae pwe h2e`**	パスワード要素を生成するための H2E を有効にします。
ステップ 12	`no shutdown`	WLAN をイネーブルにします。
ステップ 13	`End`	特権 EXEC モードに戻ります。

WPA3-Personal 移行モード

WPA3-Personal 移行モード（WPA2+WPA3-Personal 混在モード設定とも呼ばれる）は、一部のクライアントが WPA2 のみをサポートし、一部のクライアントが WPA3 までサポートできる場合に使用されます。WPA3 対応クライアントは WPA3-Personal の SAE を使用し、WPA2 対応クライアントは WPA2-Personal の PSK を使用します。このモードは、2.4 GHz と 5 GHz の両方の帯域に適用されます。

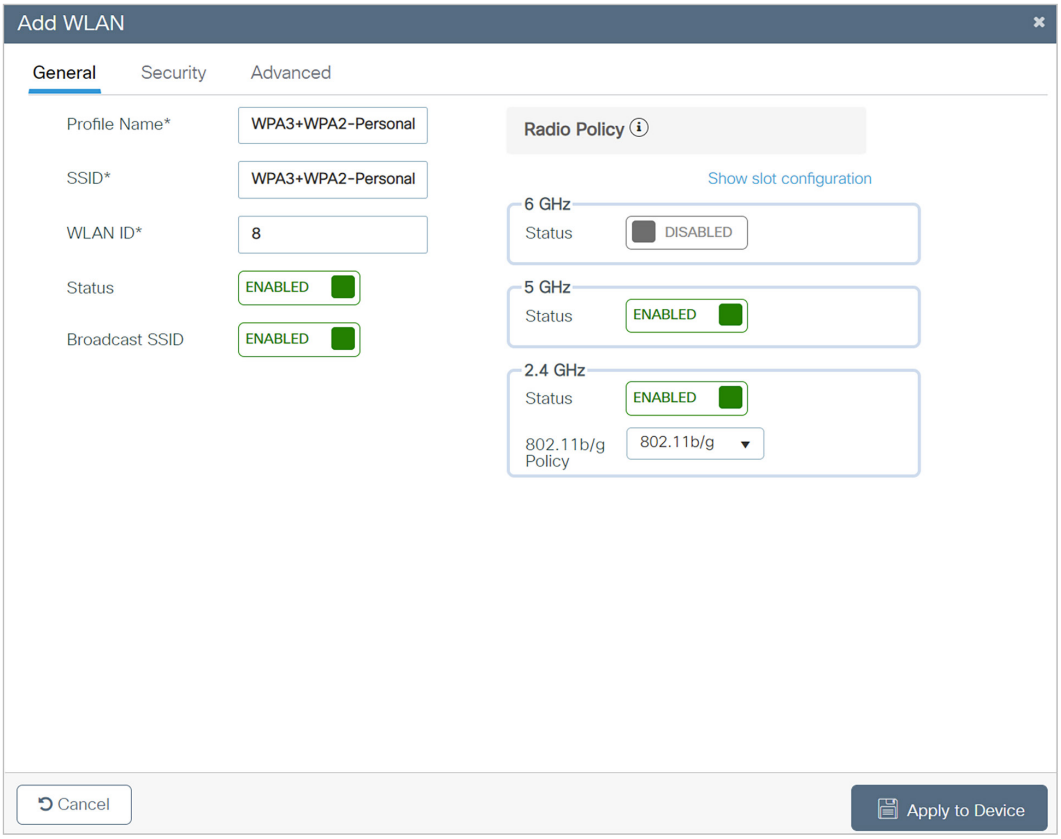
注：　このモードは、必要な場合にのみ使用してください。最大限のセキュリティを得るには、WPA3 のみを使用し、WPA3 と WPA2 が混在したモードを使用しないことが推奨されます。

© 2024 Cisco and/or its affiliates. All rights reserved.

次の手順では、WPA3+WPA2-Personal 混在モードレベルのセキュリティを備えた WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] が自動的に入力されます。
4. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。
5. **6 GHz** 帯域を無効にします。

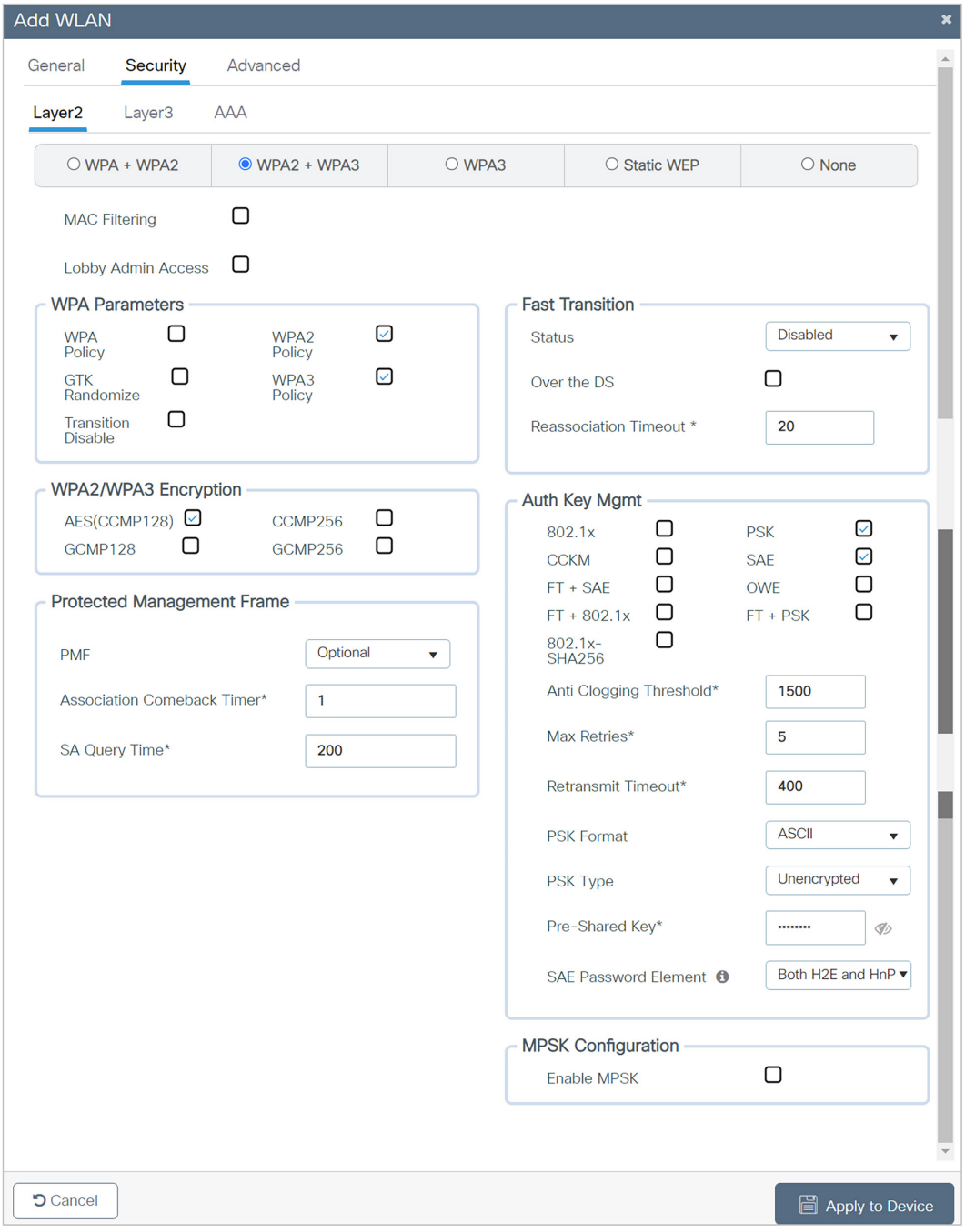
図 23.　　移行モードの無線設定



6. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。
7. [PMF] が [Optional] に設定されていることを確認します。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 24.　セキュリティ、暗号化、および AKM の設定



8. [WPA Parameters] まで下にスクロールします。[WPA2 Policy]、[WPA3 Policy]、[AES]、[PSK]、および [SAE] チェックボックスをオンにします。
9. [Pre-Shared Key] を入力し、[PSK Format] ドロップダウンリストから PSK フォーマットを選択し、[PSK Type] ドロップダウンリストから PSK タイプを選択します。
10. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Personal 移行モードの CLI 設定

次の手順では、WPA3+WPA2-Personal 混在モードレベルのセキュリティを備えた WLAN を作成します。

表 11.　　WPA3-Personal 移行モードの CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan WPA3+WPA2-Personal 1 WPA3+WPA2-Personal`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`no security wpa akm dot1x`	セキュリティ AKM 802.1X を無効にします。
ステップ 4	`no security ft`	WLAN の 802.11r 高速移行をディセーブルにします。
ステップ 5	`security wpa wpa2 ciphers aes`	WPA2 暗号を設定します。 **注：no security wpa wpa2 ciphers aes** コマンド を使用して、暗号が設定されているかどうかを確認できます。暗号がリセットされない場合は、暗号を設定します。
ステップ 6	`security wpa psk set-key ascii 0 Cisco123`	事前共有キーを指定します。
ステップ 7	`security wpa wpa3`	WPA3 のサポートを有効にします。 **注：**WPA2 と WPA3 の両方がサポートされている場合（SAE と PSK の組み合わせ）、PMF の設定は任意です。ただし、PMF を無効にすることはできません。WPA3 の場合、PMF は必須です。
ステップ 8	`security wpa akm sae`	AKM SAE のサポートを有効にします。
ステップ 9	`security wpa akm psk`	AKM PSK のサポートを有効にします。
ステップ 10	`radio policy dot11 24ghz`	2.4 GHz 帯域を有効にします。
ステップ 11	`radio policy dot11 5ghz`	5 GHz 帯域を有効にします。
ステップ 12	`no shutdown`	WLAN をイネーブルにします。
ステップ 13	`end`	特権 EXEC モードに戻ります。

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Personal Transition Disable モード

Transition Disable は、AP から STA への指示であり、STA は AP のネットワークへの後続の接続で特定の移行モードを無効にします。

STA 実装により、ネットワークプロファイルで特定の移行モード（および他のレガシーセキュリティアルゴリズム）が有効になる場合があります。たとえば、WPA3-Personal STA は、ネットワークプロファイルで、PSK アルゴリズムを有効にする WPA3-Personal 移行モードをデフォルトで有効にする場合があります。しかし、ネットワークが移行モードで定義された最もセキュアなアルゴリズムを（完全に）サポートしている場合、STA で Transition Disable 指示を使用して、そのネットワークの移行モードを無効にし、ダウングレード攻撃からの保護が提供されます。

注： Transition Disable 指示を使用する AP は、自身の BSS で対応する移行モードを無効にする必要はありません。たとえば、WPA3-Personal ネットワーク内の AP は、Transition Disable 指示を使用して、WPA3-Personal をサポートするすべての STA がダウングレード攻撃から保護されるようにする一方で、レガシー STA が接続できるように BSS で WPA3-Personal 移行モードを有効にする場合があります。

これによりすべてのクライアントデバイスは、移行モードの WLAN に参加するときに WPA3 のみに移行するため、セキュリティ面では優れている一方で、ネットワークが複数の物理的な場所で構成されている場合、たとえば、一部が WPA2 に設定され、その他が WPA3/WPA2 移行モードに設定されている場合、移行したクライアントが WPA2 のみを使用する場所に移動すると接続に失敗することになります。

これは、同じ SSID が異なるコントローラ/AP セットアップをカバーし、設定が 100% 一致しない一部の大規模ネットワークで考えられるシナリオです。最も規模が大きな例は、世界中で同じ SSID 名を共有する Edu Roam です。これを設定すると、異なるネットワークプロバイダー間を移動するクライアントに重大な問題が発生する可能性があるため、すべてのネットワークの場所で同じセキュリティ設定が適切に設定されていることを確認できる場合にのみ、慎重に使用してください。

注： この方法は通常は推奨されません。絶対に必要な場合にのみ有効にする必要があります。

以下のセクションでは、WLAN で Transition Disable を有効にする方法について説明します。

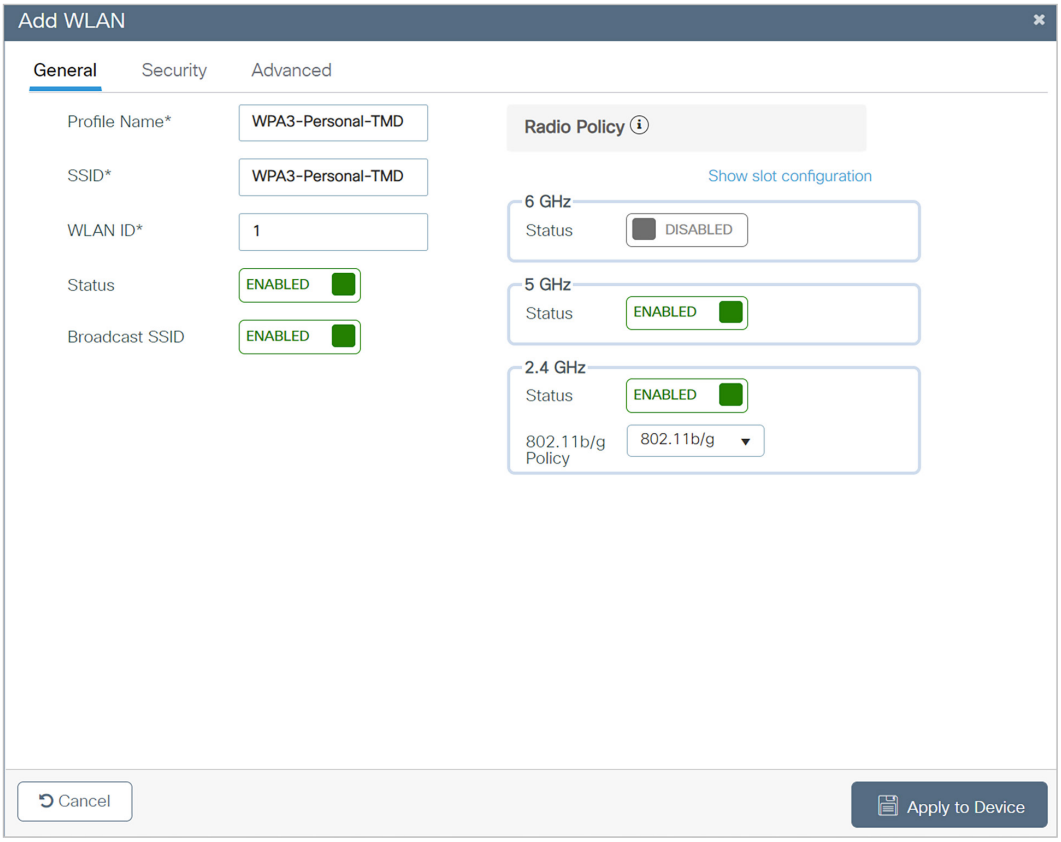
WPA3-Personal Transition Disable モードの GUI 設定

次の手順では、Transition Disable を有効にして、WPA3-Personal レベルのセキュリティを備えた WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] が自動的に入力されます。
4. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられた AP がこの設定済み WLAN のブロードキャストを開始するようにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

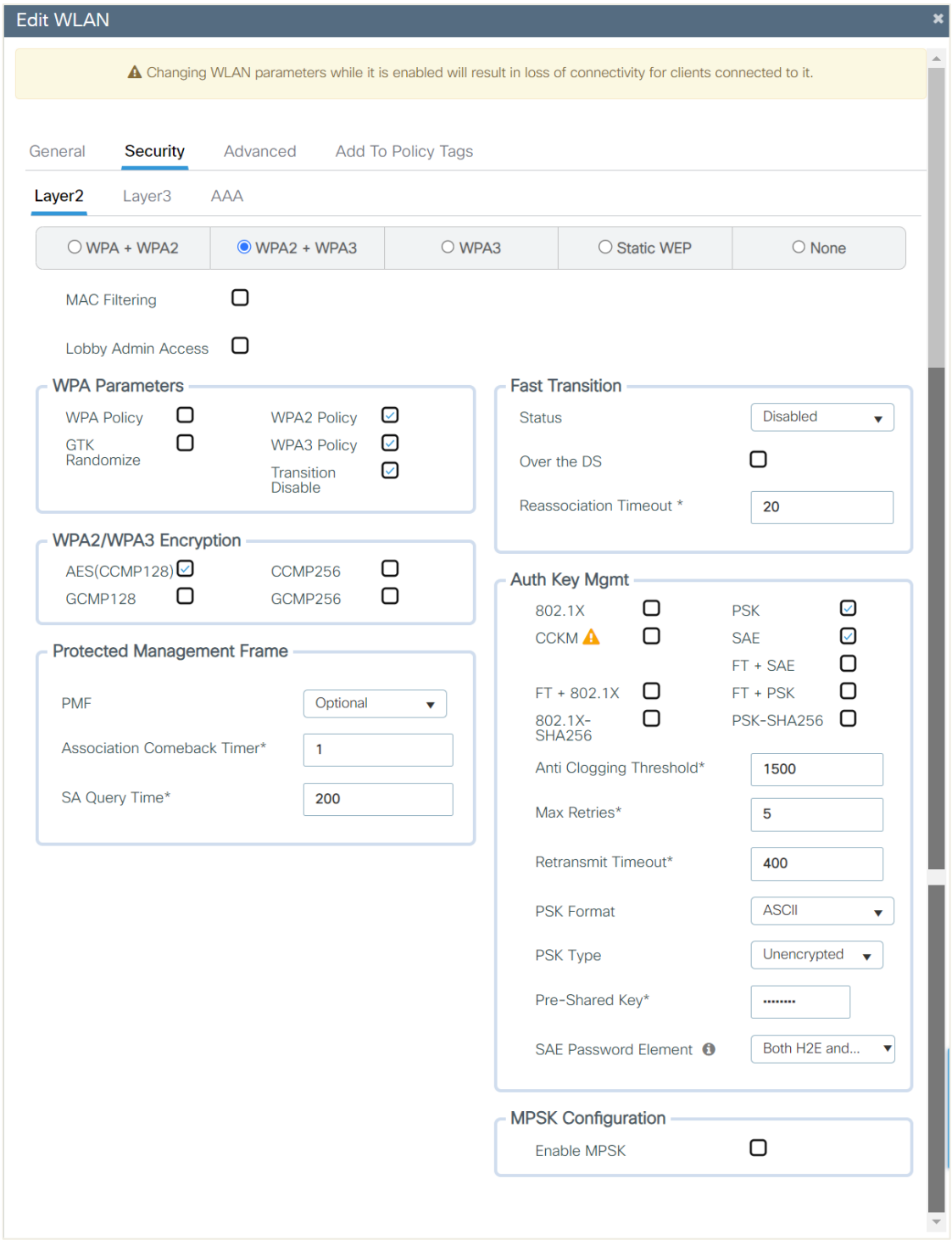
図 25.　　Transition Disable モードの無線/スロット設定



5. **6 GHz** 帯域を無効にします。
6. [Security] タブで、[WPA2 + WPA3] オプションを有効にします。
7. Fast Transition を無効にします。
8. [WPA Parameters] まで下にスクロールします。[WPA2 Policy] と [WPA3 Policy]、[AES]、AKM として [SAE] と [PSK] チェックボックスをオンにします。
9. [Pre-Shared Key] を入力し、[PSK Format] ドロップダウンリストから PSK フォーマットを選択し、[PSK Type] ドロップダウンリストから PSK タイプを選択します。
10. [PMF] が [Optional] であることを確認します。
11. [WPA Parameters] で [Transition Disable] オプションを有効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 26.　Transition Disable モードのセキュリティと AKM の設定



© 2024 Cisco and/or its affiliates. All rights reserved.

WPA3-Personal Transition Disable モードの CLI 設定

表 12.　WPA3-Personal Transition Disable モードの CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan WPA3-Personal-TMD 1 WPA3-Personal-TMD`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`no security wpa akm dot1x`	セキュリティ AKM 802.1X を無効にします。
ステップ 4	`security wpa wpa3`	WPA3 を有効にします。
ステップ 5	`no security ft`	WLAN の 802.11r 高速移行をディセーブルにします。
ステップ 6	`security wpa wpa2`	WPA2 セキュリティを有効にします。PMF はオプションになっています。
ステップ 7	`security wpa wpa2 ciphers aes`	AES/CCMP128 暗号を有効にします。

ステップ 8	`security wpa psk set-key ascii value preshared-key`
	`Example:`
	`Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`
		事前共有キーを指定します。

ステップ 9	`security wpa akm sae`	AKM SAE のサポートを有効にします。
ステップ 10	`security wpa akm psk`	AKM PSK を有効にします。
ステップ 11	**`transition-disable`**	Transition Disable を有効にします。
ステップ 11	`radio policy dot11 24ghz`	2.4 GHz を有効にします。
ステップ 12	`radio policy dot11 5ghz`	5 GHz を有効にします。
ステップ 13	`no shutdown`	WLAN をイネーブルにします。
ステップ 14	`End`	特権 EXEC モードに戻ります。

© 2024 Cisco and/or its affiliates. All rights reserved.

WPA2+WPA3-Personal 移行モード（6 GHz）

6 GHz 規格では、WPA2 セキュリティ（WPA2 のみと WPA2+WPA3 WLAN の両方に適用）が設定されている場合、6 GHz 帯域での WLAN のブロードキャストは許可されません。したがって、その本質から、WLAN が WPA2 で設定されている場合は 6 GHz 無線をサポートしないという動作になります。

PMF がオプションで PSK/SAE AKM を使用した 2.4 GHz/5 GHz と同時に、同じ SSID で WPA3 の SAE AKM を使用する 6 GHz、などのユースケースがあります。これは、17.12.1 より前では有効な設定ではありません。

これらの展開をサポートするために、17.12.1 より前の SW バージョンでは、レガシーと最新の 6 GHz クライアントの両方をサポートするために、異なるプロファイルを持つ同じ WLAN で WPA2 + WPA3 移行モードを使用することが推奨されていました。この設計の課題はローミングです。この設定での帯域間のローミングはサポートされておらず、これは常にフルローミングであり、推奨されません。

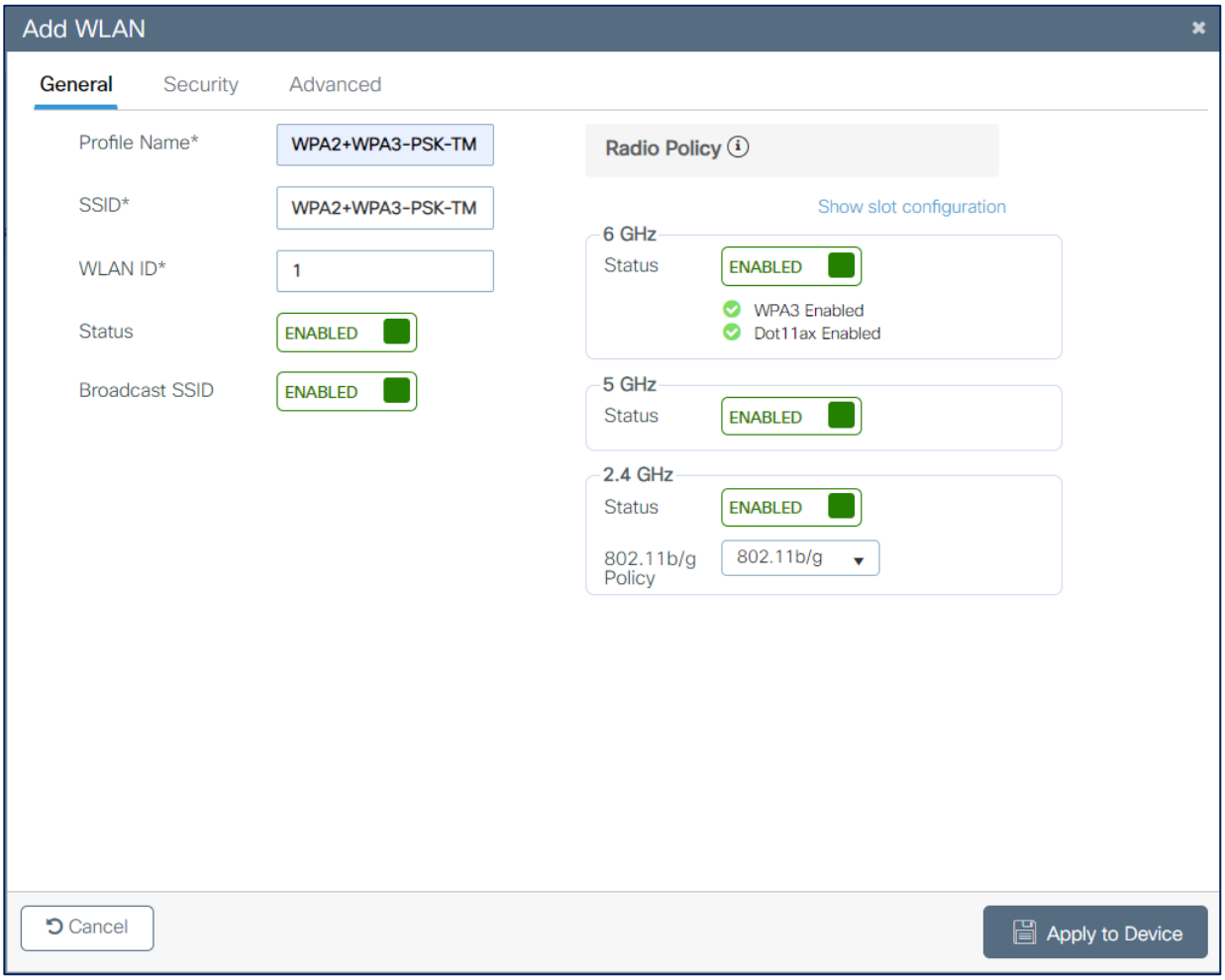
17.12.1 以降、6 GHz 帯域の純粋な WPA3 の移行モードがサポートされています。これにより、ユーザーは 6 GHz の同じ WLAN で WPA2 + WPA3 を有効にできます。このモードでは、レガシーの 6 GHz デバイスと最新の 6 GHz デバイスに対応するために 2 つの異なるプロファイルを作成する必要がなくなります。このモードでは、WPA2+WPA3 移行モードは 2.4 GHz/5 GHz で使用でき、WLAN に WPA2 と WPA3 の両方の設定がある場合、WPA3 関連の設定のみが 6 GHz 帯域にプッシュされます。

WPA2+WPA3-Personal 移行モード（6 GHz）の GUI 設定

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] の両方が自動的に入力されます。
4. [Status] と [Broadcast SSID] のトグルボタンを有効にして、このプロファイルに関連付けられたアクセスポイント（AP）がこの設定済み WLAN のブロードキャストを開始するようにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 27.　　無線/スロットの設定

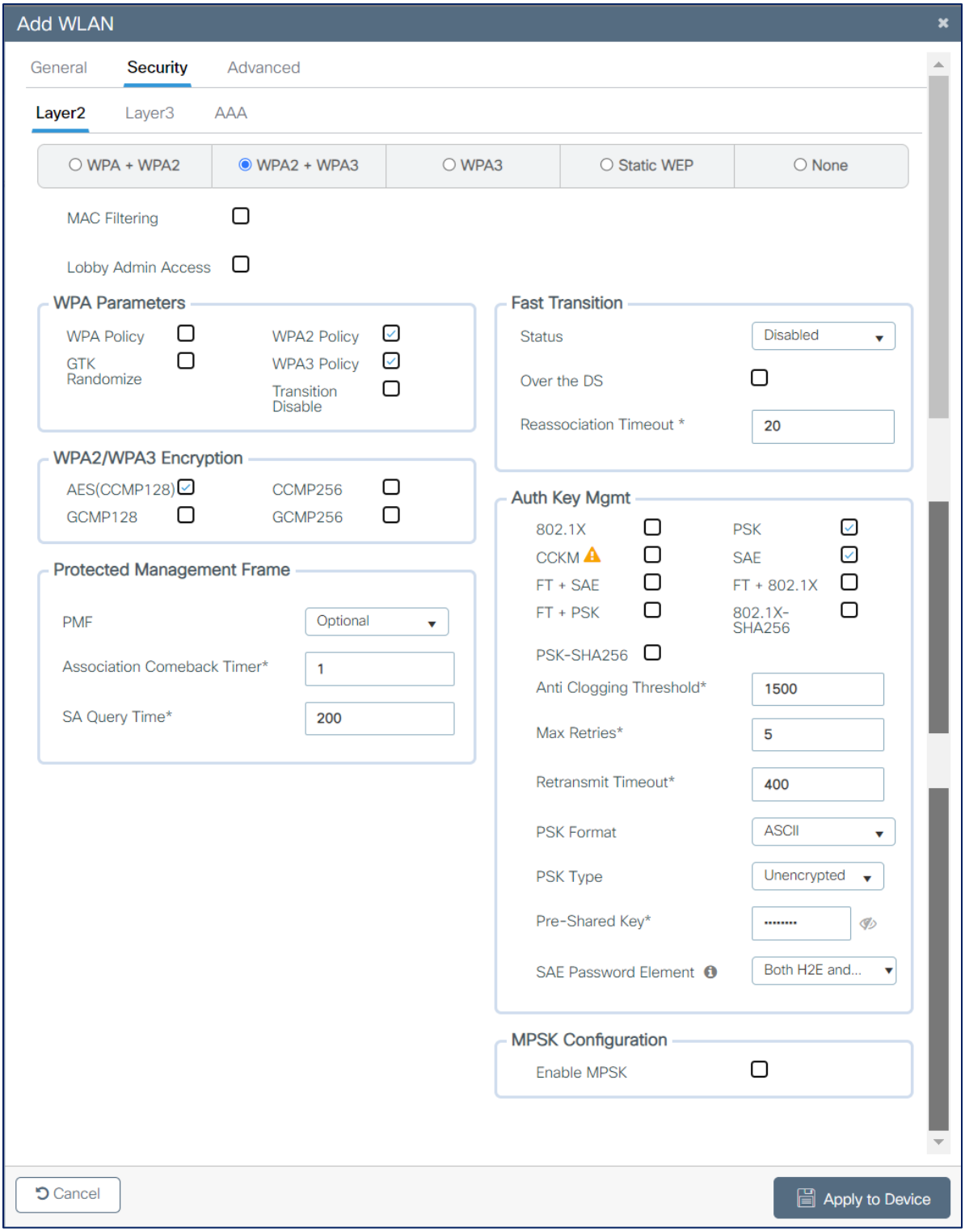


5. [Security] タブ > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。
6. [PMF] が [Optional] に設定されていることを確認します。

   注：PMF はオプションですが、WPA3 設定では、6 GHz 帯域で必須と見なされます。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 28.　　設定



7. [WPA Parameters] で [WPA2 Policy] と [WPA3 Policy] をオンにして、[WPA2/WPA3 Encryption] で [AES(CCMP128)] をオンにします。また、[PSK] と [SAE] チェックボックスをオンにします。その他の選択されているパラメータをすべてオフにします。
8. 共有キーを入力します。

© 2024 Cisco and/or its affiliates. All rights reserved.

9. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

WPA2+WPA3-Personal 移行モード（6 GHz）の CLI 設定

次の手順では、6 GHz が有効な WPA2+WPA3-Personal 移行モードの WLAN を作成します。

表 13. 純粋な 6 GHz の WPA2+WPA3 移行モードの CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan WPA2+WPA3-PTM 1 WPA2+WPA3-PTM`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`no security wpa akm dot1x`	802.1X のセキュリティ AKM を無効にします。
ステップ 4	`no security ft`	WLAN の 802.11r 高速移行をディセーブルにします。
ステップ 5	`security wpa wpa2 ciphers aes`	WPA2 暗号を設定します。 注：`no security wpa wpa2 ciphers aes` コマンド を使用して、暗号が設定されているかどうかを確認できます。暗号がリセットされない場合は、暗号を設定します。
ステップ 6	`security wpa psk set-key ascii 0 Cisco123`	事前共有キーを指定します。
ステップ 7	`security wpa wpa3`	WPA3 のサポートを有効にします。 注：WPA2 と WPA3 の両方がサポートされている場合（SAE と PSK の組み合わせ）、PMF の設定は任意です。ただし、PMF を無効にすることはできません。WPA3 の場合、PMF は必須です。
ステップ 8	`security wpa akm sae`	AKM SAE のサポートを有効にします。
ステップ 9	`security wpa akm psk`	AKM PSK のサポートを有効にします。
ステップ 10	`radio policy dot11 6ghz`	6 GHz 帯域を有効にします。
ステップ 11	`radio policy dot11 24ghz`	2.4 GHz 帯域を有効にします。
ステップ 12	`radio policy dot11 5ghz`	5 GHz 帯域を有効にします。
ステップ 13	`no shutdown`	WLAN をイネーブルにします。
ステップ 14	`end`	特権 EXEC モードに戻ります。

© 2024 Cisco and/or its affiliates. All rights reserved.

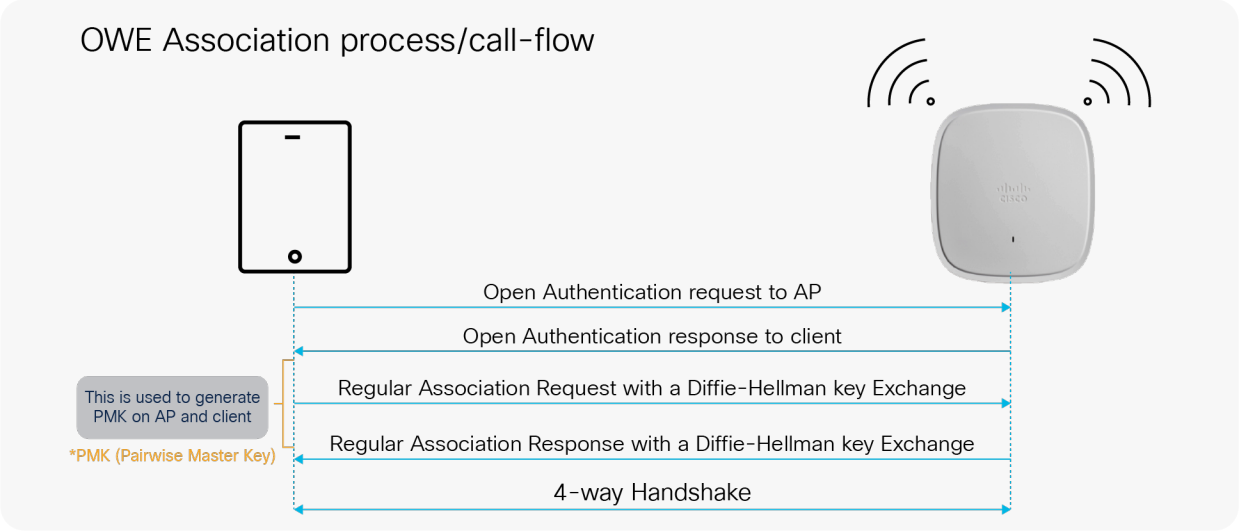
WPA2+WPA3-Personal 移行モード（6 GHz）の CLI 出力

```
#show wlan summary

Number of WLANs: 1

ID    Profile Name                    SSID                            Status 2.4GHz/5GHz
Security
6GHz Security
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
---
1     WPA2+WPA3-PTM                   WPA2+WPA3-PTM                   UP      [WPA2 +
WPA3][PSK][SAE][AES]
[WPA3][SAE][AES]
```

OWE

OWE はオープンセキュリティのワイヤレスネットワークと組み合わせて使用し、盗聴者からネットワークを保護するための暗号化を提供します。OWE では、クライアントと AP がエンドポイント アソシエーション パケットの交換中に Diffie-Hellman キーの交換を実行し、その結果として作成された PMK を 4 ウェイハンドシェイクの実行で使用します。OWE はオープンセキュリティのワイヤレスネットワークに関連付けられているため、通常のオープンネットワークだけでなく、キャプティブポータルに関連付けられたネットワークでも使用できます。

図 29.　　OWE のエンドポイントとネットワークのハンドシェイクプロセス



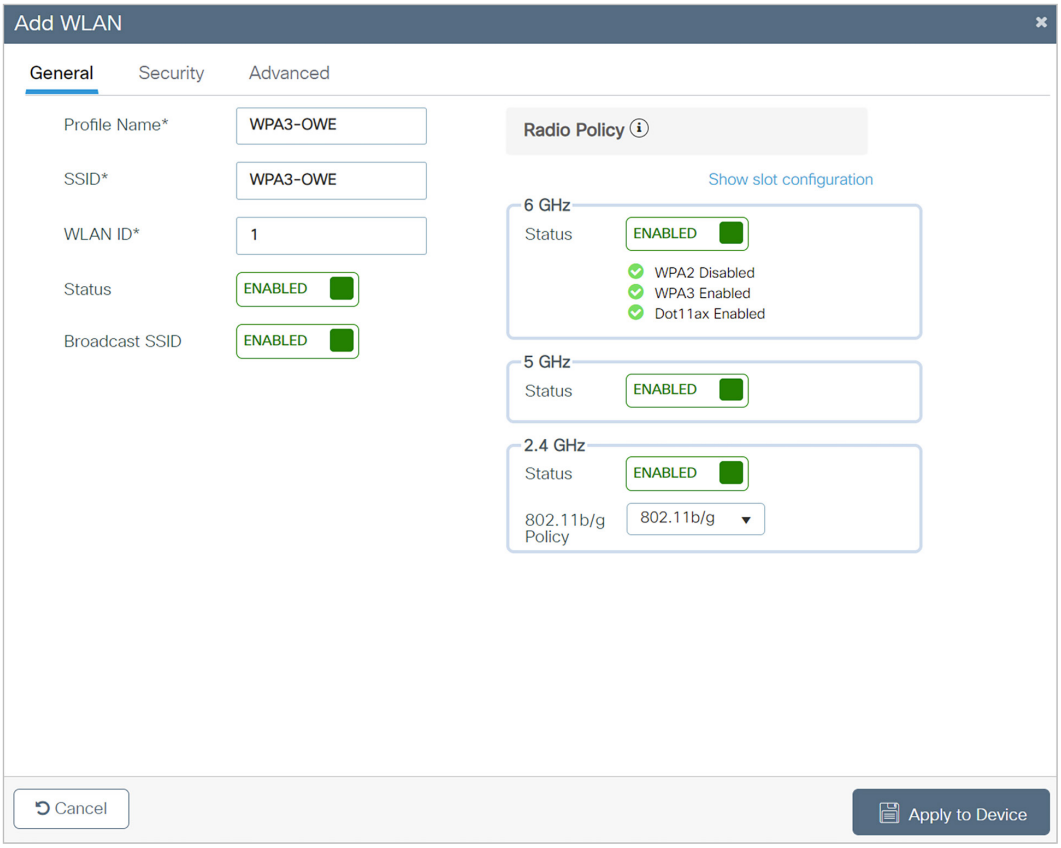
WPA3 OWE の GUI 設定

次の手順では、WPA3 OWE セキュリティを使用して WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] が自動的に入力されます。
4. [Status] および [Broadcast SSID] トグルボタンを有効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

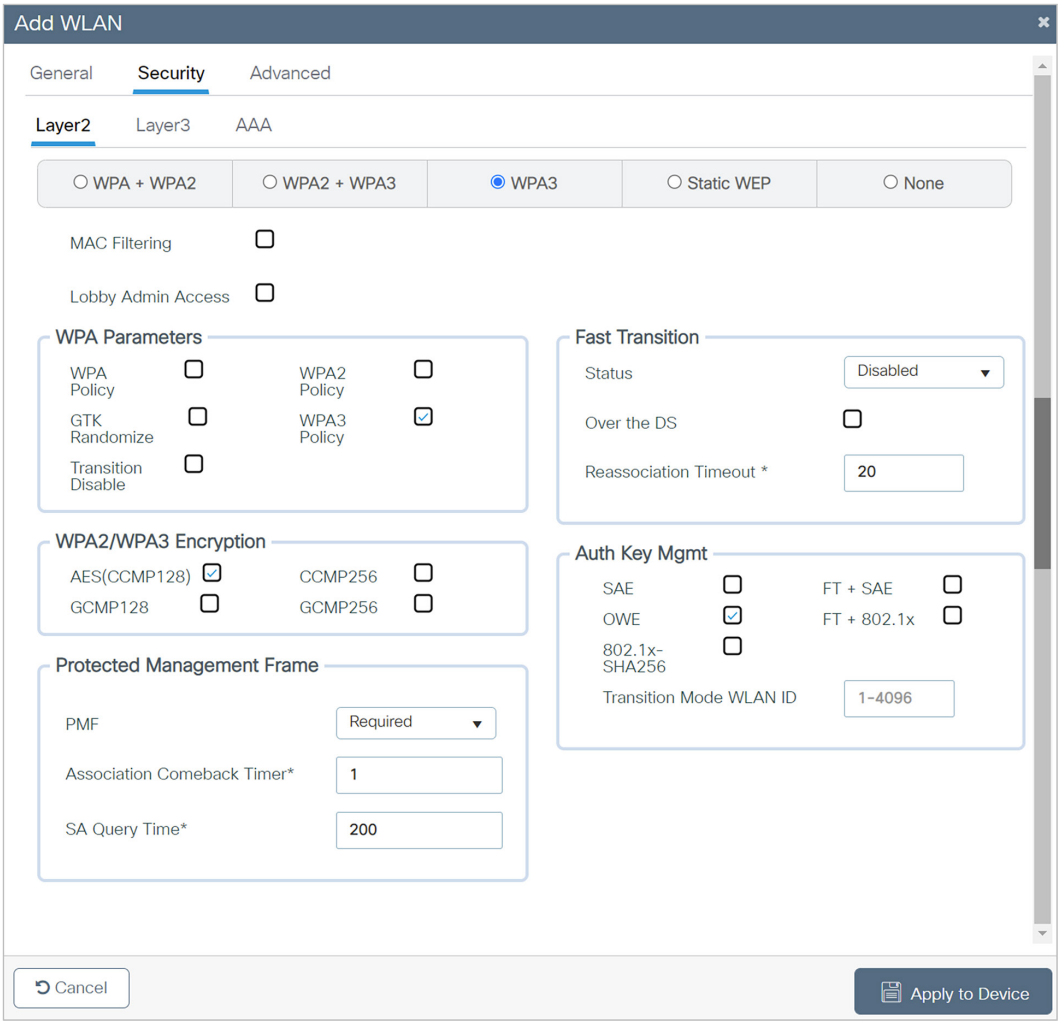
図 30.　　WPA3 OWE 無線/スロット設定



5. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。
6. [Fast Transition] ドロップダウンリストから [Disabled] を選択します。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 31.　　OWE AKM の設定



7. [WPA3 Policy]、[AES (CCMP 128)]、および [OWE] チェックボックスをオンにします。選択されている他のパラメータをオフにします。
8. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

WPA3 OWE の CLI 設定

次の手順では、WPA3 OWE セキュリティを使用して WLAN を作成します。

表 14.　　WPA3 OWE の CLI 設定

	コマンド	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	`wlan wlan-name wlan-id SSID-name` **例：**	WLAN コンフィギュレーション サブモードを開始します。

© 2024 Cisco and/or its affiliates. All rights reserved.

	コマンド	目的
	`Device(config)# wlan WPA3 1 WPA3`	
ステップ 3	`no security ft over-the-ds`	WLAN 上のデータソースを介した Fast Transition を無効にします。
ステップ 4	`no security ft`	WLAN の 802.11r 高速移行をディセーブルにします。
ステップ 5	`no security wpa akm dot1x`	802.1X のセキュリティ AKM を無効にします。
ステップ 6	`no security wpa wpa2`	WPA2 セキュリティを無効にします。これで PMF は無効になります。
ステップ 7	`security wpa wpa2 ciphers aes`	AES の WPA2 暗号化を有効にします。 注：WPA2 と WPA3 の暗号は共通です。
ステップ 8	`security wpa wpa3`	WPA3 のサポートを有効にします。
ステップ 9	`security wpa akm owe`	WPA3 OWE のサポートを有効にします。
ステップ 10	`no shutdown`	WLAN をイネーブルにします。
ステップ 11	`End`	特権 EXEC モードに戻ります。

WPA3 OWE 移行モードの GUI 設定

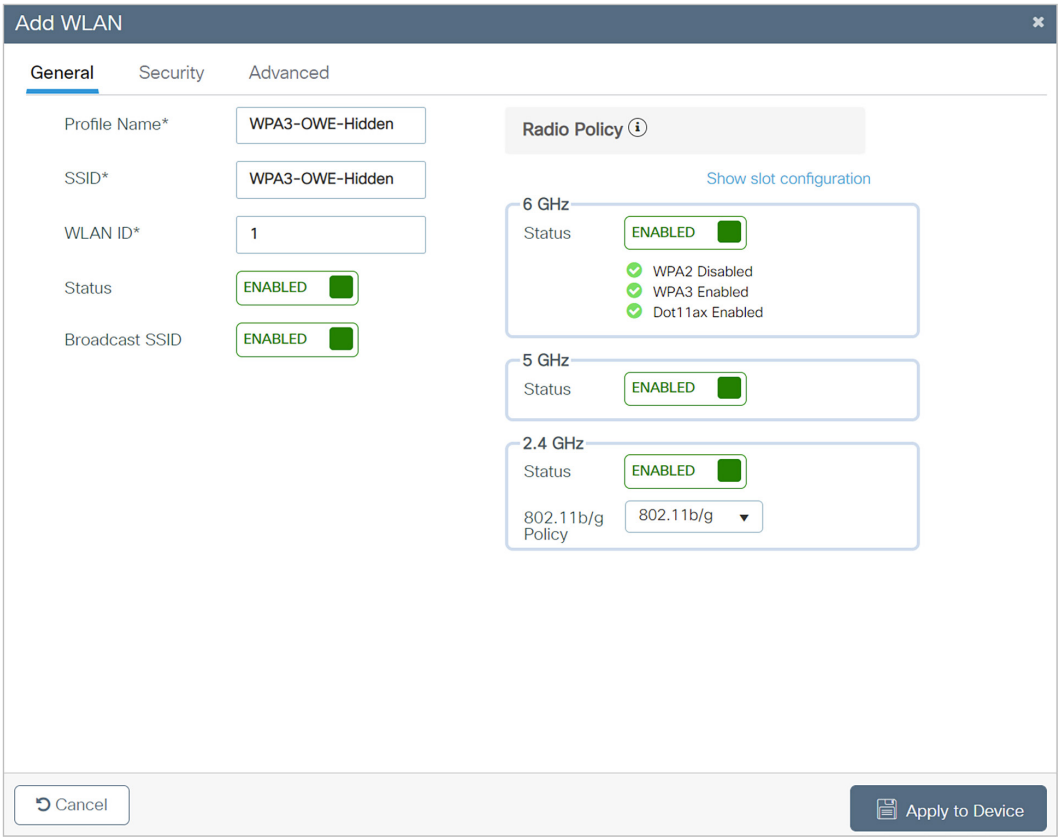
一部のデバイスが拡張オープン機能をサポートしていないため（デバイスの相互運用性マトリックスを参照）、移行モードが公開されました。移行モードは、拡張オープン OWE モードの適応性を高めるために設計されています。Wi-Fi Alliance では、一部のデバイスがこのモードをサポートしていない環境でこの方法を使用して、拡張オープンワイヤレス ネットワークを実装することを推奨しています。OWE 移行モードでは、拡張オープン OWE SSID と同様のプロパティで設定された別のオープン SSID が必要です。OWE とオープン WLAN の両方に、対応する移行モード WLAN ID があります。これは、OWE WLAN には、オープン WLAN ID 対して設定された移行モード ID があり、オープン WLAN には OWE WLAN ID に対して設定された移行モード ID があることを意味します。

パート 1：次の手順では、WPA3 OWE セキュリティを使用して非表示の WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。[SSID] と [WLAN ID] が自動的に入力されます。
4. [Status] および [Broadcast SSID] トグルボタンを無効にします。
5. WLAN の [WLAN ID] をメモします。

© 2024 Cisco and/or its affiliates. All rights reserved.

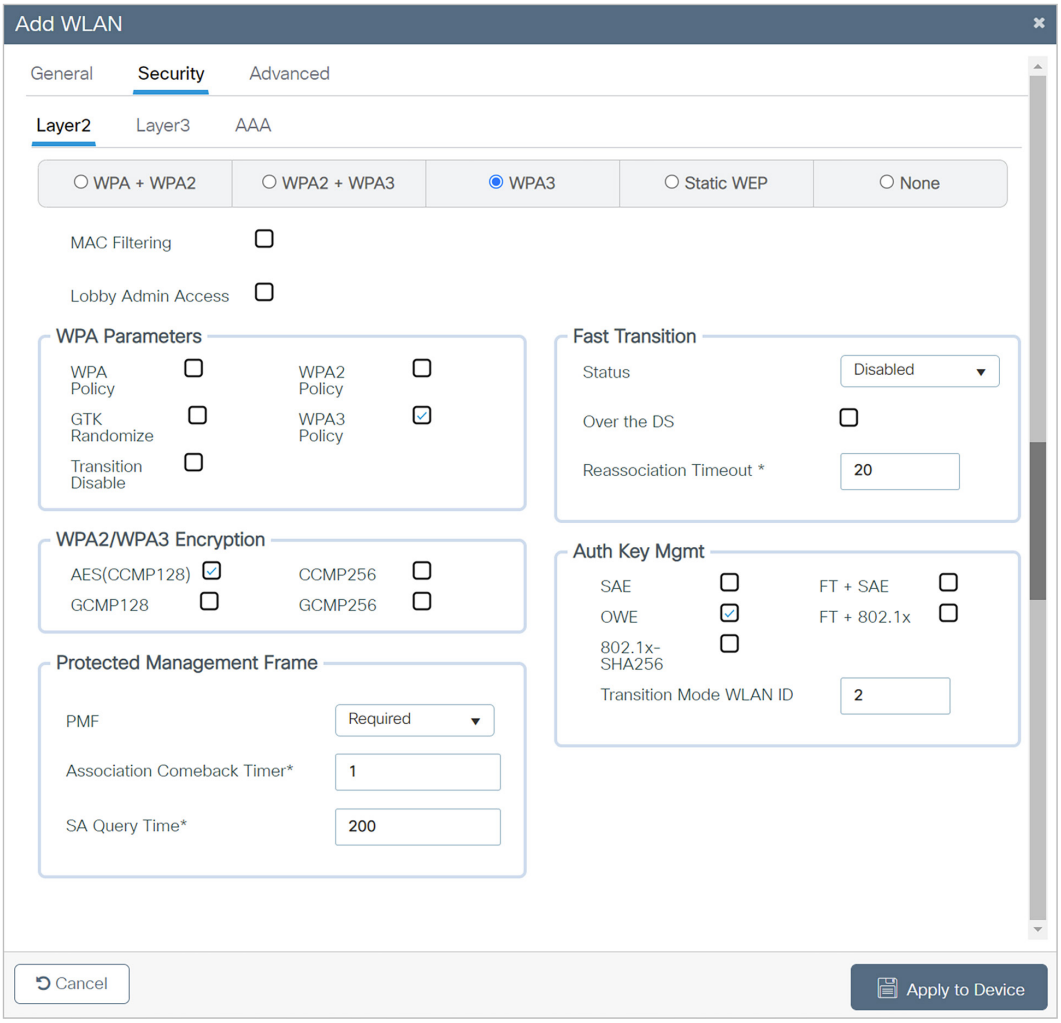
図 32.　　OWE の無線ポリシー



6. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。
7. [PMF] が [Required] に設定されていることを確認します。
8. [Fast Transition] ドロップダウンリストから [Disabled] を選択します。
9. [WPA3 Policy]、[AES (CCMP 128)]、および [OWE] チェックボックスをオンにします。選択されている他のパラメータをオフにします。
10. [Transition mode WLAN ID] を入力します。これは、次に設定される SSID の WLAN ID になります。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 33.　　OWE と移行モード ID の設定



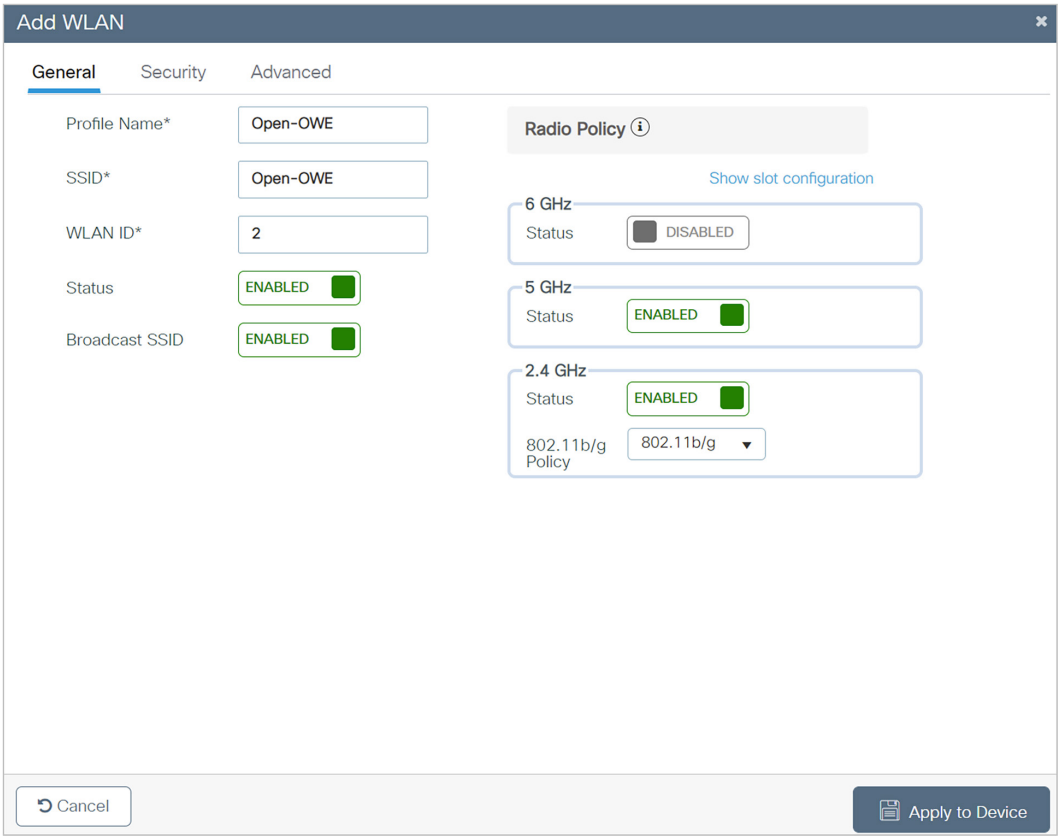
11. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

パート 2 : 次の手順では、オープンセキュリティの WLAN を作成します。

1. [Configuration] > [Tags and Profiles] > [WLANs] を選択します。
2. [Add] をクリックします。
3. [General] タブの [Profile Name] に、わかりやすい識別子を入力します。
4. [SSID] は、拡張オープン SSID と一致する必要があります。[WLAN ID] は自動的に入力されます。
5. [Status] および [Broadcast SSID] トグルボタンを有効にします。

© 2024 Cisco and/or its affiliates. All rights reserved.

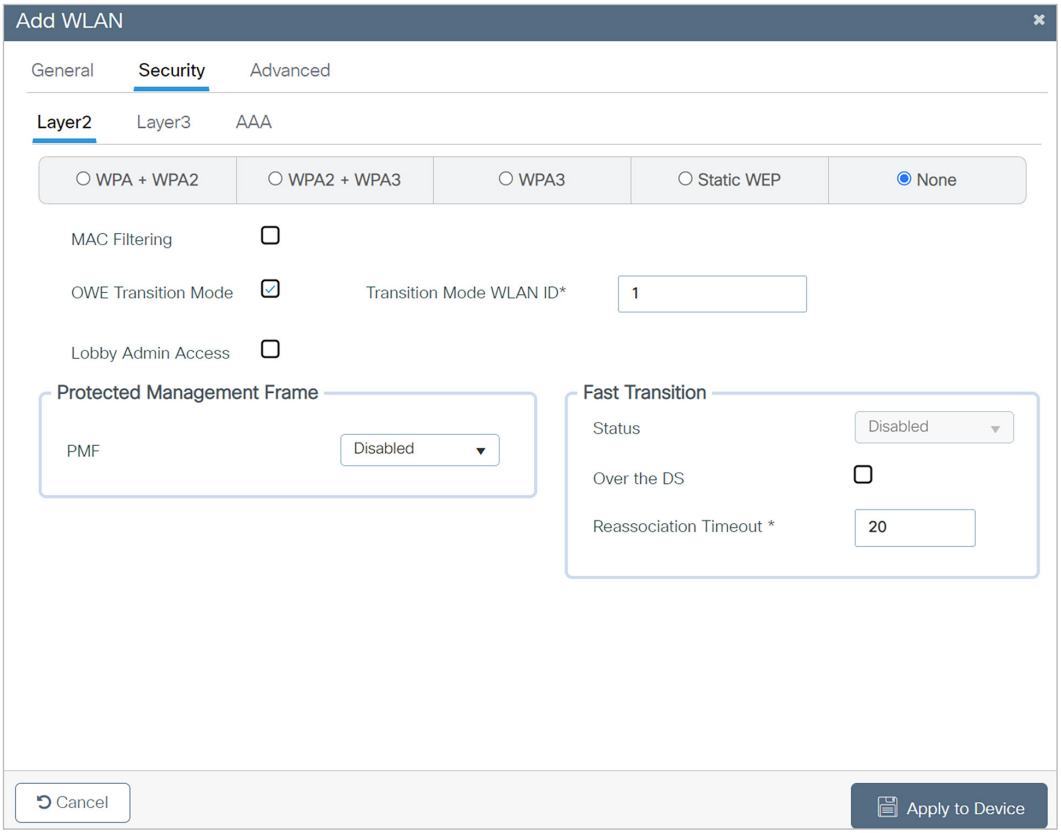
図 34.　　WLAN オープンセキュリティの設定



6. [Security] > [Layer 2] タブをクリックします。[Layer 2 Security Mode] ドロップダウンリストから、[WPA3] を選択します。

© 2024 Cisco and/or its affiliates. All rights reserved.

図 35.　　OWE 移行モードの設定



7. [Transition Mode WLAN ID] には、オープン WLAN にマッピングするためにレイヤ 2 セキュリティが [Enhanced Open] に設定されている **WLAN ID** を入力します。
8. [Apply to Device] をクリックして、WLAN 作成プロセスを保存して終了します。

WPA3 OWE 移行モードの CLI 設定

パート 1：次の手順では、WPA3 OWE セキュリティを使用して非表示の WLAN を作成します。

表 15.　　WPA3 OWE 移行モードの CLI 設定

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan WPA3-OWE-Hidden 1 WPA3-OWE-Hidden`
		WLAN コンフィギュレーション サブモードを開始します。

ステップ 3	`no broadcast-ssid`	SSID ブロードキャストを無効化します。
ステップ 4	`no security ft over-the-ds`	WLAN 上のデータソースを介した Fast Transition を無効にします。
ステップ 5	`no security ft`	WLAN の 802.11r 高速移行をディセーブルにします。

© 2024 Cisco and/or its affiliates. All rights reserved.

	コマンド	目的
ステップ 6	`no security wpa akm dot1x`	802.1X のセキュリティ AKM を無効にします。
ステップ 7	`no security wpa wpa2`	WPA2 セキュリティを無効にします。これで PMF は無効になります。
ステップ 8	`security wpa akm owe`	WPA3 OWE のサポートを有効にします。
ステップ 9	`security wpa transition-mode-wlan-id 2`	移行モードを有効にします。
ステップ 10	`security wpa wpa3`	WPA3 のサポートを有効にします。
ステップ 11	`no shutdown`	WLAN をイネーブルにします。
ステップ 12	`End`	特権 EXEC モードに戻ります。

パート 2：次の手順では、オープン OWE セキュリティの WLAN を作成します。

	コマンド	目的
ステップ 1	`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	`wlan wlan-name wlan-id SSID-name`
	例：
	`Device(config)# wlan Open-OWE 2 Open-OWE`
		WLAN コンフィギュレーション サブモードを開始します。
		注：非表示 WLAN とオープン WLAN の SSID は同じである必要があります。

ステップ 3	`no security ft over-the-ds`	WLAN 上のデータソースを介した Fast Transition を無効にします。
ステップ 4	`no security ft`	WLAN の 802.11r 高速移行をディセーブルにします。
ステップ 5	`no security wpa akm dot1x`	802.1X のセキュリティ AKM を無効にします。
ステップ 6	`no security wpa`	セキュリティを無効にします。
ステップ 7	`no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化を無効にします。
ステップ 8	`security wpa transition-mode-wlan-id 1`	移行モードを有効にします。
ステップ 9	`no shutdown`	WLAN をイネーブルにします。
ステップ 10	`end`	特権 EXEC モードに戻ります。

© 2024 Cisco and/or its affiliates. All rights reserved.

クライアント相互運用性マトリックス

WPA3 でサポートされる AP モードとサポートされるクライアント

表 16.　　WPA3 でサポートされる AP モードとクライアント

	WPA3 サポートマトリックス										
WPA3 プロトコル	**暗号/AKM**	**AP モード ローカル**	**AP モード Flex（中央認証）**	**AP モード Flex（ローカル認証）**	**Apple（11/12/13）**	**Samsung S21/Google Android**	**Intel**	**Apple iPad（iPadOS：16.3）**	**MacOS（M1 以降）**	**Zebra（TCS53/58/73）**	
WPA3-Personal	WPA3-SAE AES CCMP128	サポート対象	サポート対象	サポート対象 FT：サポート対象外	サポートあり FT：サポート対象外	サポートあり FT-SAE：サポート対象 H2E：iOS16 でサポート	サポートあり FT-SAE：S21 Galaxy Ultra/Galaxy Z Fold でのみサポート	サポート対象：H2E のみ FT-SAE：Linux WPA サプリカント（AX210）でサポート	サポートあり FT-SAE：サポート対象	サポートあり FT-SAE：サポート対象 Adaptive FT：サポート対象外	サポートあり
WPA3-Enterprise	WPA3-802.1x-SHA256 AES CCMP 128	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象：SHA256 および FT-OTA サポート対象外：FT-ODS	サポート対象：SHA256、Adaptive および FT-OTA	*サポートあり* Adaptive FT：サポート対象外	サポートあり
	WPA3-Enterprise GCMP128 SuiteB 1x	サポート対象	未サポート	サポート対象外	サポート対象外	サポート対象外	サポート対象外	サポート対象外：GCMP128、FT-OTA、FT-ODS	サポート対象外	サポート対象外	サポート対象外
	WPA3-Enterprise GCMP256 SuiteB 192 ビット	サポート対象	未サポート	サポート対象外	サポート対象外	サポート対象	サポート対象 サポート対象外：FT-ODS	サポート対象：GCMP256 サポート対象外：FT（FT-OTA と FT-ODS の両方）	サポートあり	サポート対象：FT-ODS/ITA	*サポートあり*
OWE	WPA3-OWE AES CCMP128	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象外	対応	サポート対象：OWE 認証	サポート対象：OWE 認証	サポート対象	*サポート対象*

© 2024 Cisco and/or its affiliates. All rights reserved.

便利な Catalyst 9800 コントローラコマンド

SAE 認証の成功、SAE 認証の失敗、SAE の進行中のセッション、または SAE のコミットが発生したクライアントのシステムレベルの統計情報を表示したり、メッセージ交換を確認したりするには、次の show コマンドを使用します。

```
show wireless stats client detail
```

WLAN サマリーの詳細を表示するには、次のコマンドを使用します。

- `show wlan summary`
- `show wlan all`
- `show wlan name <wlan-name>`
- `show wlan id {Starting 17.12.1, the security section on the WLAN is displayed individually for 2.4GHz/5GHz band and 6GHz band as below}`

```
#show wlan id 1
WLAN Profile Name     : WPA2+WPA3-TransitionMode
================================================
Identifier                                      : 1
Description                                     :
Network Name (SSID)                             : WPA2+WPA3-TransitionMode
Status                                          : Enabled
....
    Security-2.4GHz/5GHz
         ....
     Security-6GHz
....
#
```

SAE 認証を済ませたクライアントの正しい AKM を表示するには、次のコマンドを使用します。

```
show wireless client mac-address <xxxx.xxxx.xxxx> detail
```

ローカルに保存されている PMK キャッシュのリストを表示するには、次のコマンドを使用します。

```
show wireless pmk-cache
```

便利な Catalyst AP コマンド

次のコマンドを入力して、クライアント上の WPA3 のデバッグを設定します。

```
debug client client-mac-address
```

次のコマンドを入力して、SAE イベントおよび詳細のデバッグを設定します。

```
debug sae {events | details} {enable | disable}
```

© 2024 Cisco and/or its affiliates. All rights reserved.

参照

- Cisco Catalyst 9800 Series Wireless Controller 17.8.1 Configuration Guide：
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-8/config-guide/b_wl_17_8_cg.html
- Cisco Catalyst 9100 アクセスポイントのドキュメント:
  https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/series.html

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)

Printed in USA

© 2024 Cisco and/or its affiliates. All rights reserved.

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。