Aruba ClearPassによる9800 WLC統合の設定 – Dot1x&FlexConnect for Branchesの導入

内容

概要

このドキュメントでは、Catalyst 9800 Wireless Controller(WLC)をAruba ClearPass Policy Manager(CPPM)およびMicrosoft Active Directory(AD)と統合して、Flexconnectの展開でワイヤレスクライアントにdot1x認証を提供する方法について説明します。

前提条件

要件

次の項目に関する知識があり、設定および確認が完了していることを推奨します。

- Catalyst 9800ワイヤレスコントローラ
- Aruba ClearPass Server（プラットフォームライセンス、アクセスライセンス、オンボードライセンスが必要）
- 運用Windows AD
- オプションの認証局(CA)
- DHCPサーバの動作
- 動作可能なDNSサーバ（証明書CRL検証に必要）
- ESXi
- 関連するすべてのコンポーネントがNTPに同期され、正しい時刻であることが確認されます（証明書の検証に必要）
- トピックに関する知識： C9800の導入と新しい設定モデルC9800でのFlexConnectの動作 Dot1x認証

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

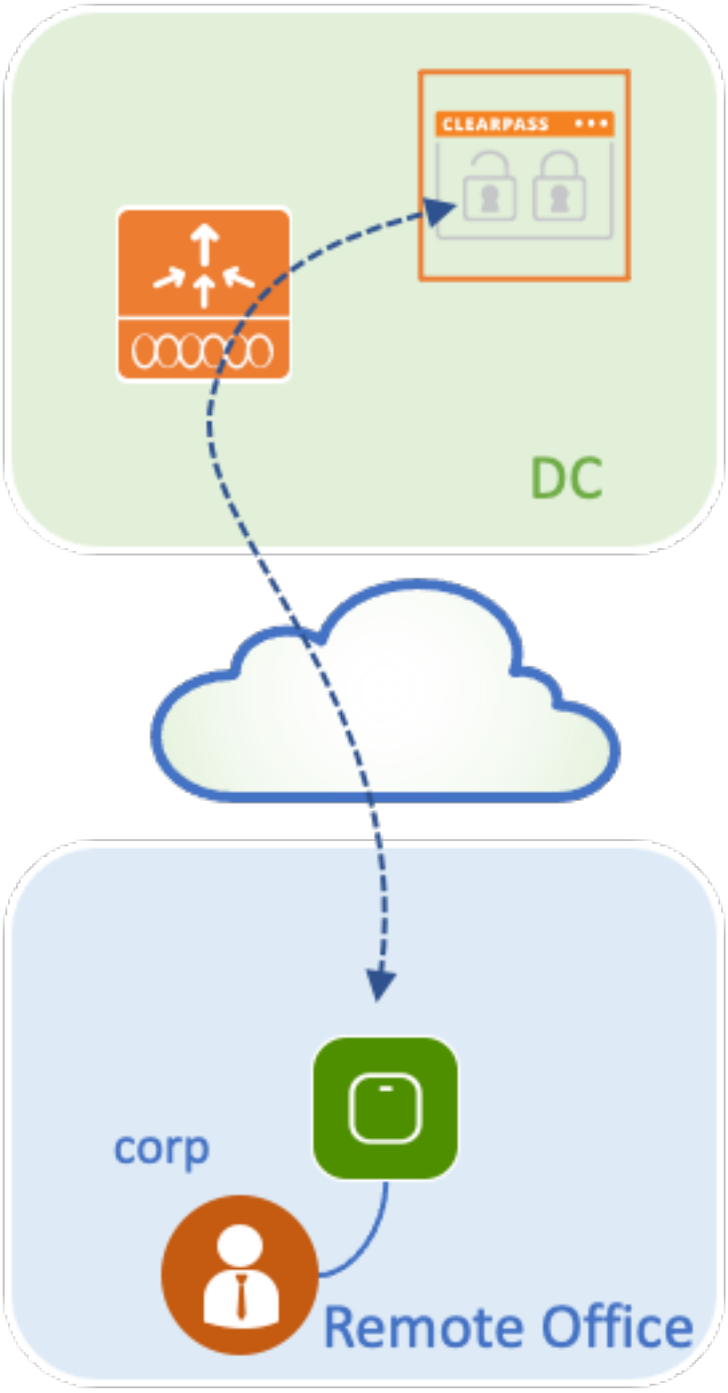
- C9800-L-C Cisco IOS-XE 17.3.3
- C9130AX、4800 AP
- Aruba ClearPass、6-8-0-109592および6.8-3パッチ
- MS Windowsサーバ Active Directory（管理対象エンドポイントへのマシンベースの証明書自動発行用に設定されたGP）オプション43およびオプション60のDHCPサーバDNS サーバすべてのコンポーネントを時刻同期するNTPサーバCA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

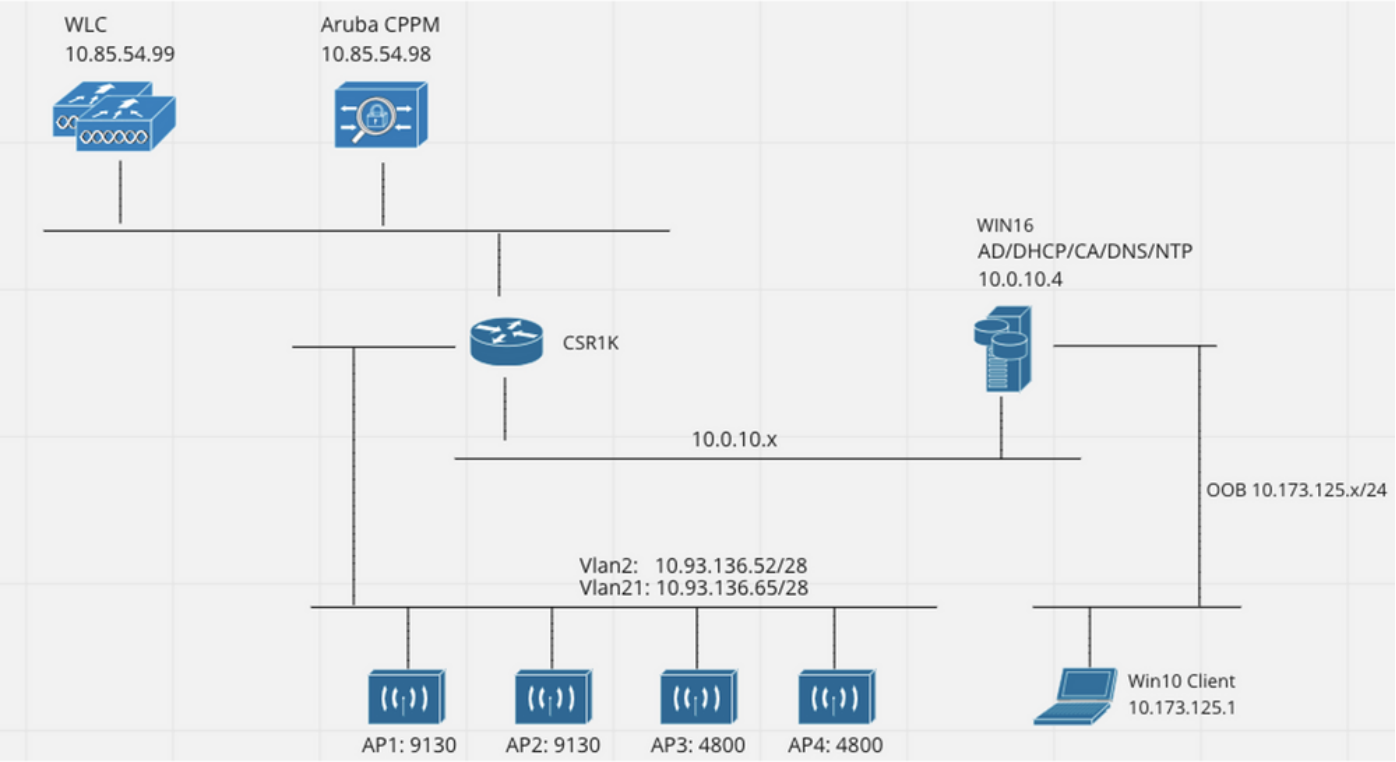
背景説明

Traffic flow

複数のブランチオフィスを持つ一般的な企業の導入では、各ブランチオフィスは企業の従業員にdot1xアクセスを提供するように設定されています。この設定例では、PEAPを使用して、中央データセンター(DC)に導入されたClearPassインスタンスを介して企業ユーザにdot1xアクセスを提供します。 マシン証明書は、Microsoft ADサーバに対する従業員のクレデンシャルの検証とともに使用されます。

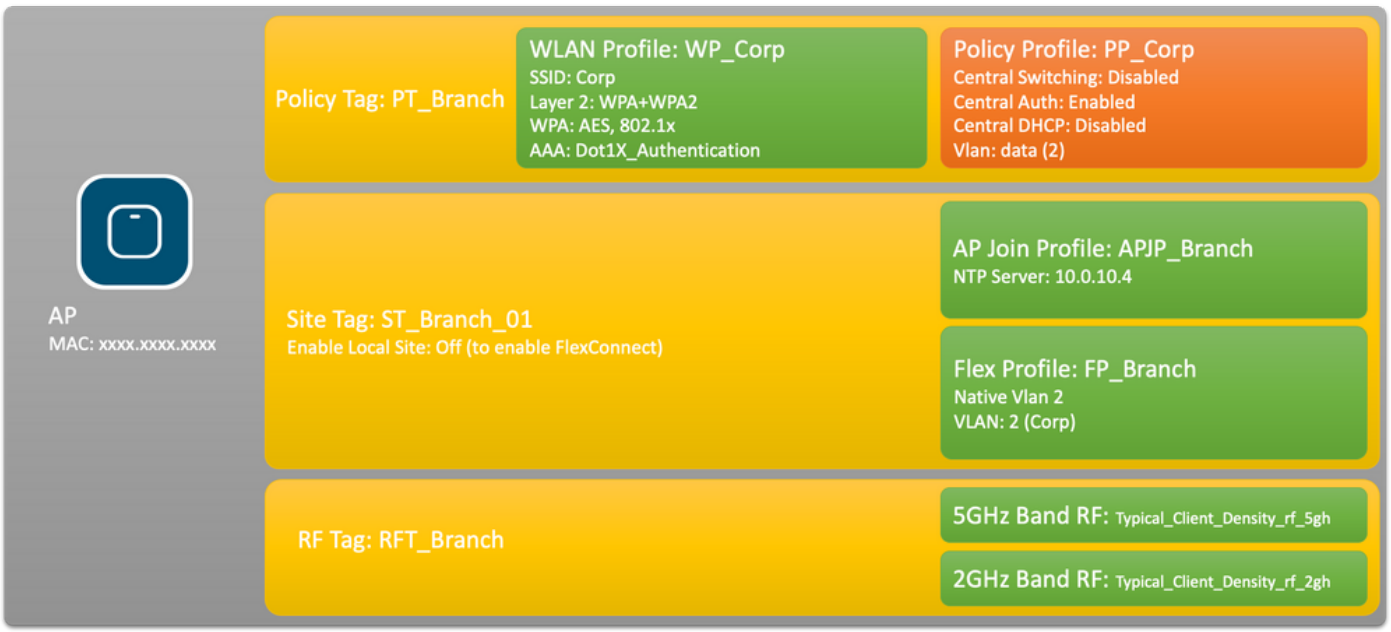


ネットワーク図



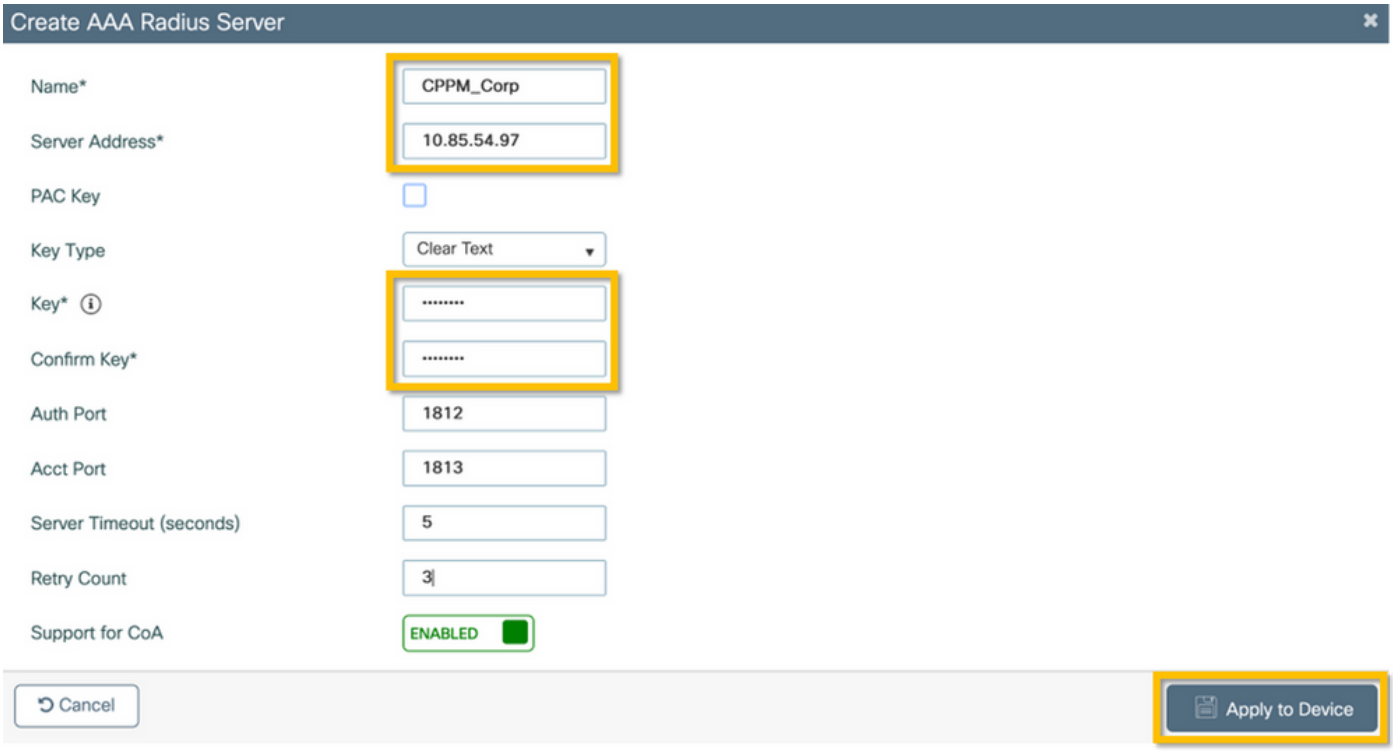
Catalyst 9800ワイヤレスコントローラの設定

この設定例では、C9800の新しい設定モデルを利用して、企業のブランチにdot1x企業アクセスを提供するために必要なプロファイルとタグを作成します。結果の設定を図にまとめます。

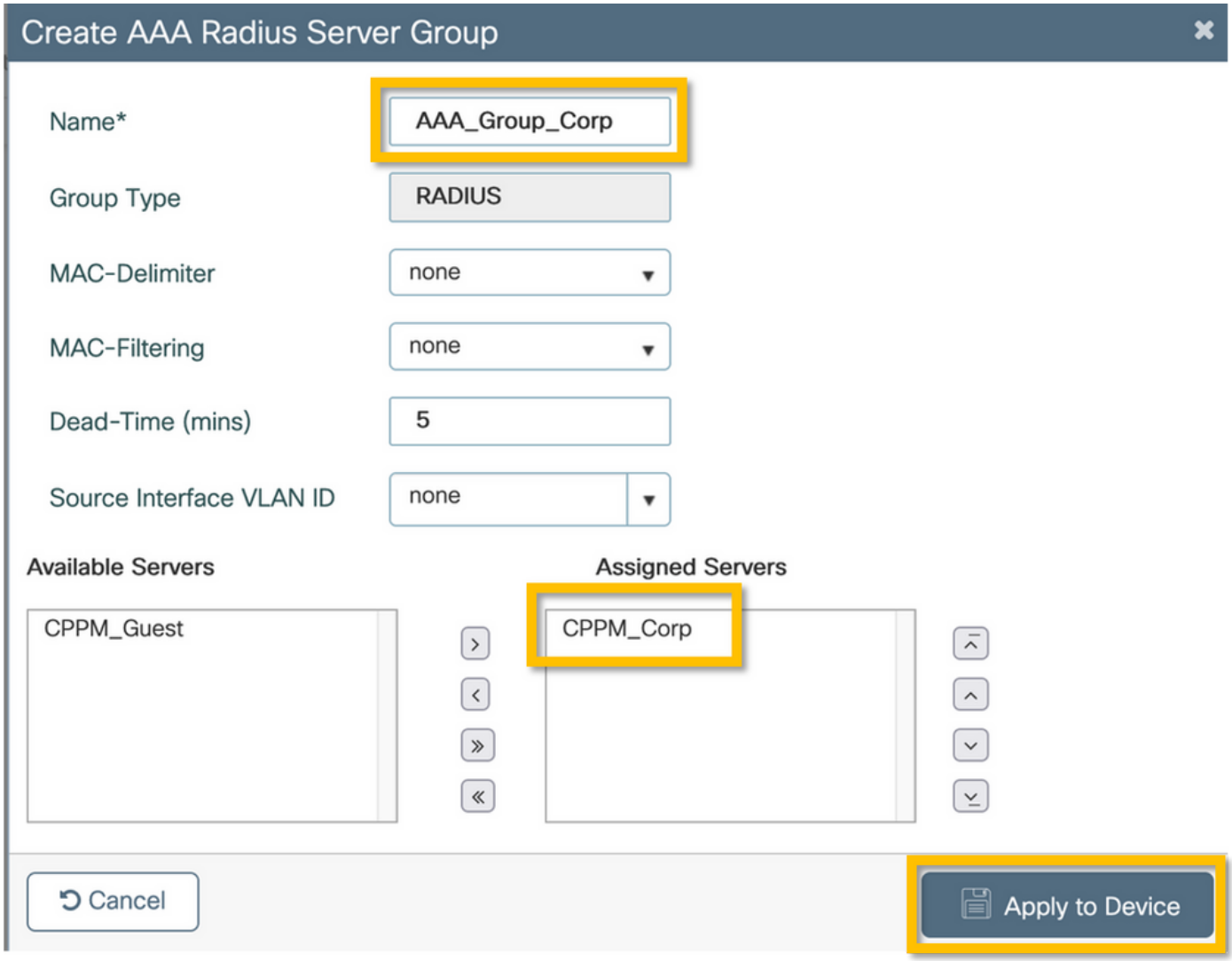


C9800:dot1xのAAAパラメータの設定

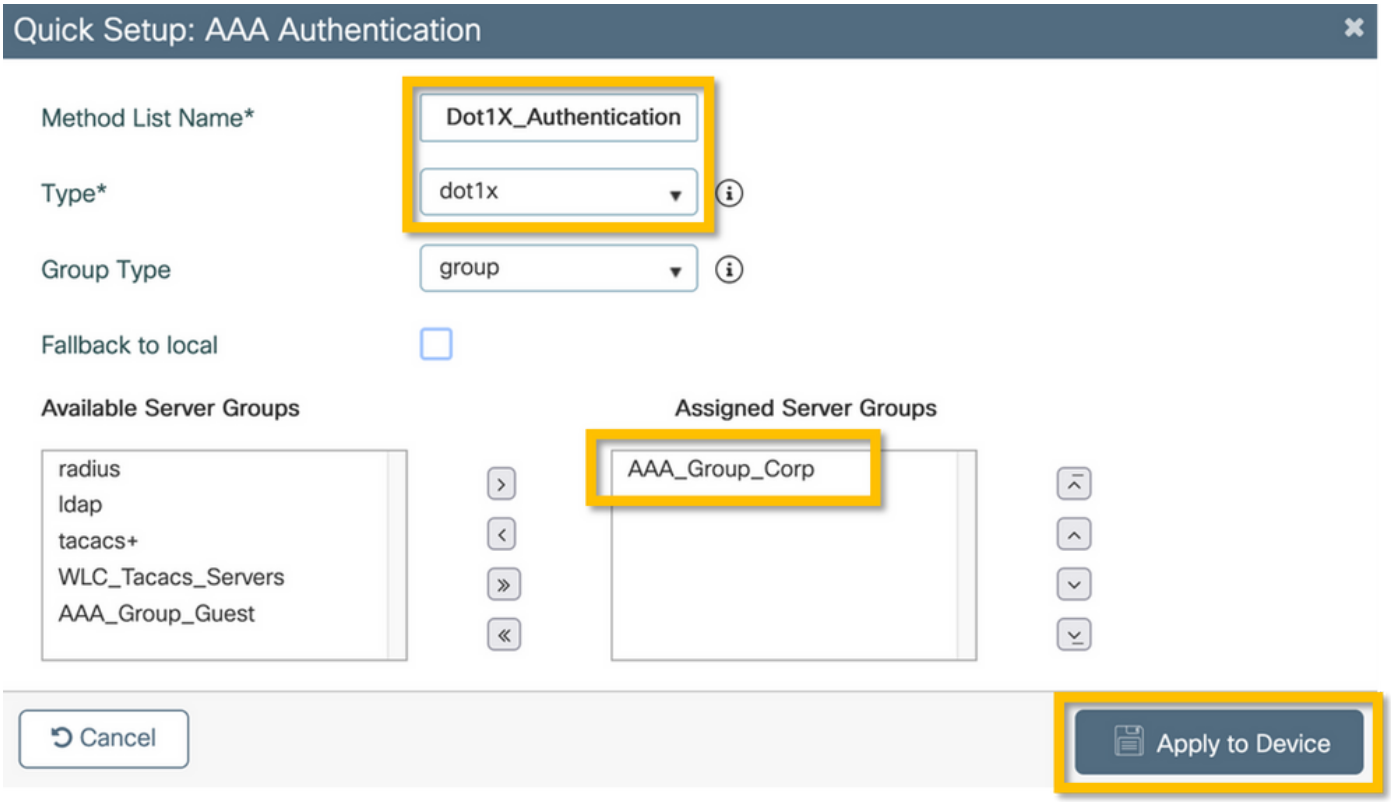
ステップ1:Aruba ClearPass Policy Manager「Corp」サーバを9800 WLC設定に追加します。[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Servers] に移動します。[+Add]をクリックし、RADIUSサーバ情報を入力します。次の図に示すように、[Apply to Device] ボタンをクリックします。



ステップ2：企業ユーザ用のAAAサーバグループを定義します。[Configuration] > [Security] > [AAA] > [Servers/Groups] > [RADIUS] > [Groups] に移動し、[+Add] をクリックして、RADIUSサーバグループ名を入力し、RADIUSサーバ情報を割り当てます。次の図に示すように、[Apply to Device] ボタンをクリックします。

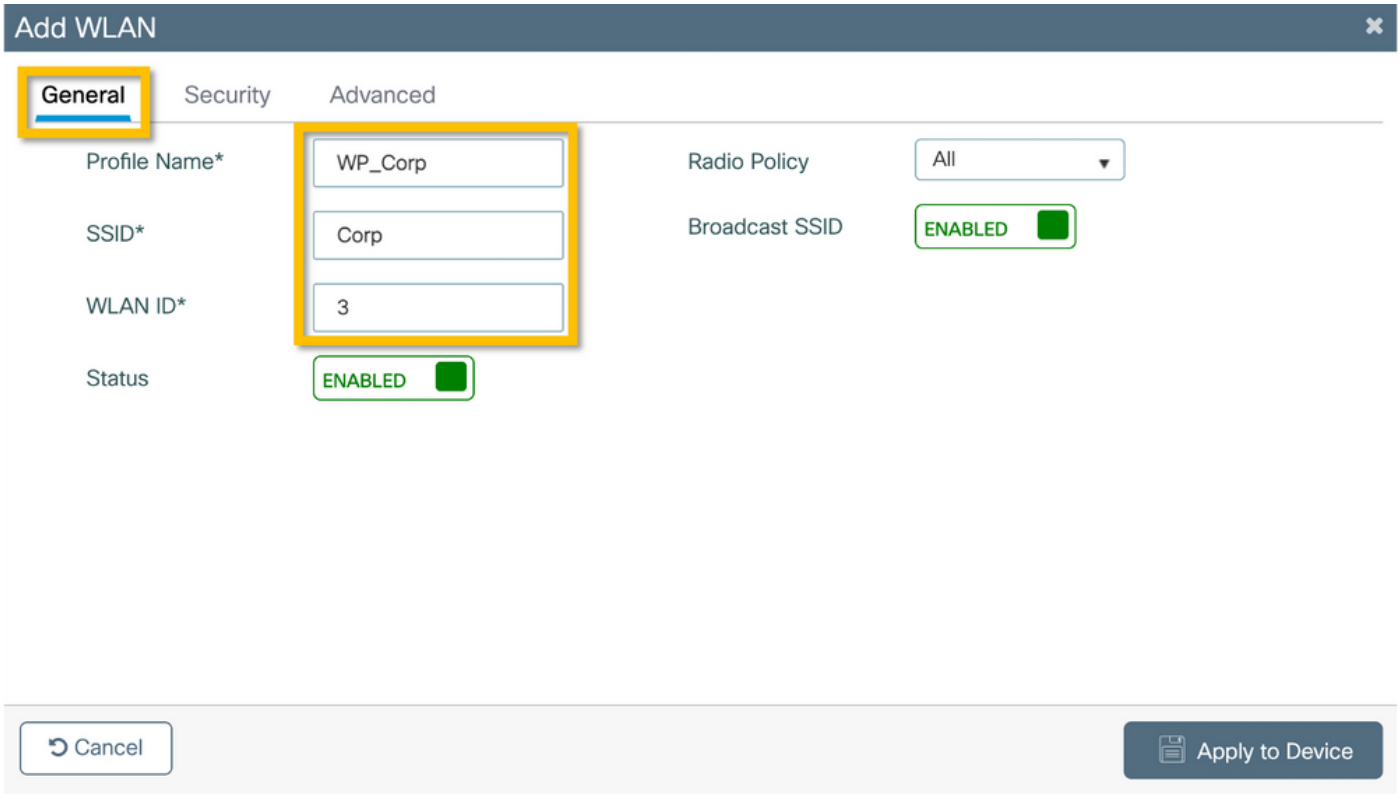


ステップ3：企業ユーザのdot1x認証方式リストを定義します。[Configuration] > [Security] > [AAA] > [AAA Method List] > [Authentication] に移動し、[+Add] をクリックします。ドロップダウンメニューから[Type dot1x] を選択し、次の図に示すように[Apply to Device] ボタンをクリックします。

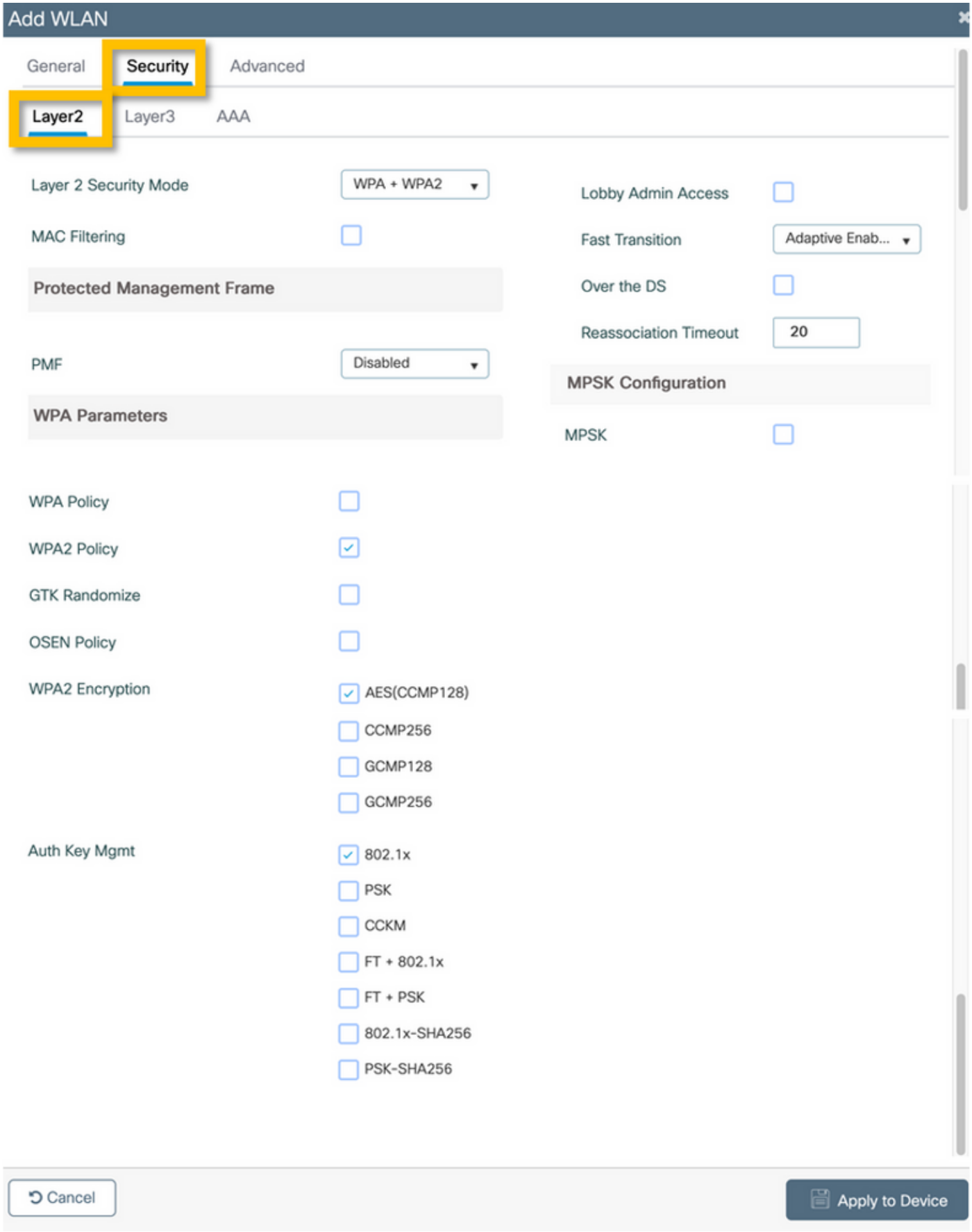


C9800:「Corp」WLANプロファイルの設定

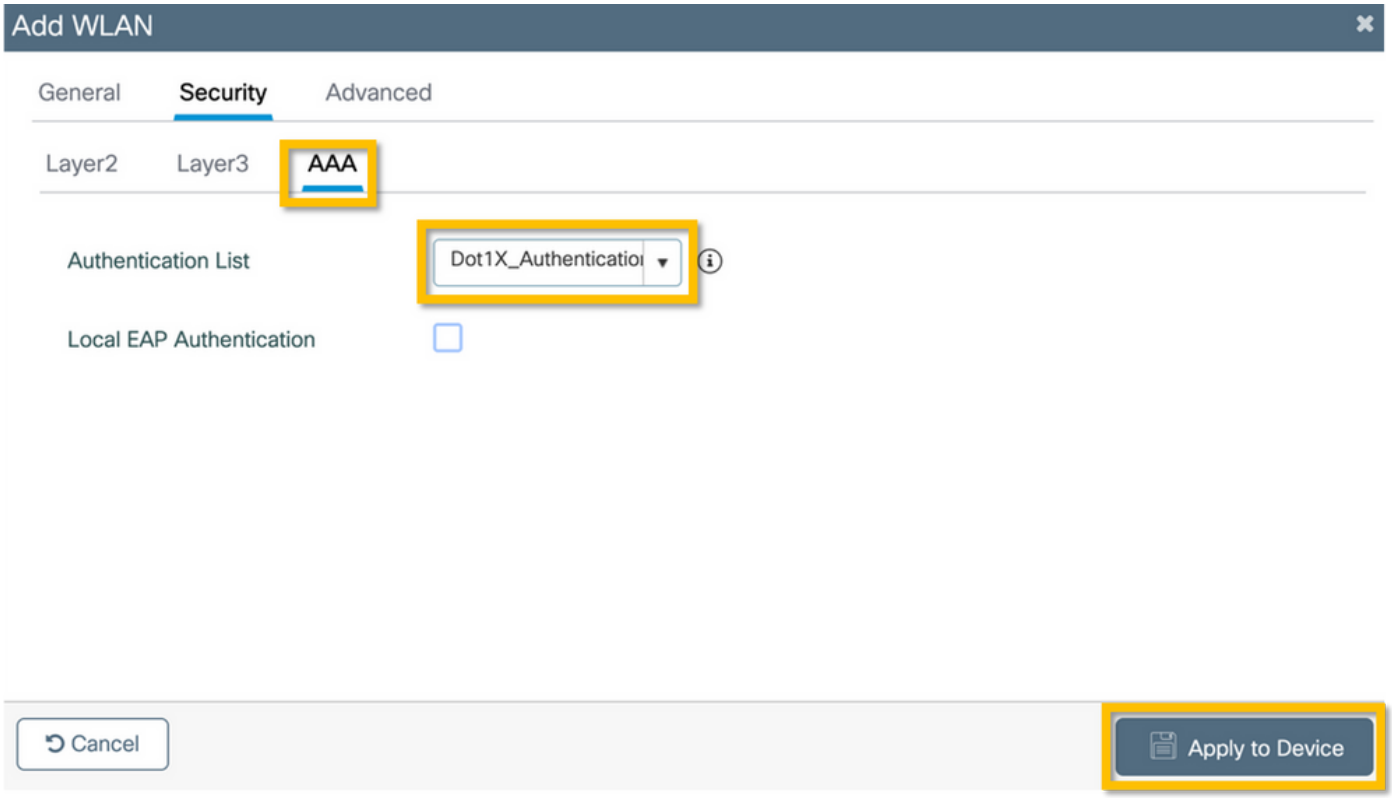
ステップ1:[Configuration] > [Tags & Profiles] > [Wireless] に移動し、[+Add] をクリックします。プロファイル名、SSID「Corp」、および未使用のWLAN IDを入力します。



ステップ2:[Security] タブと[Layer2] サブタブに移動します。この設定例のデフォルトパラメータを変更する必要はありません。

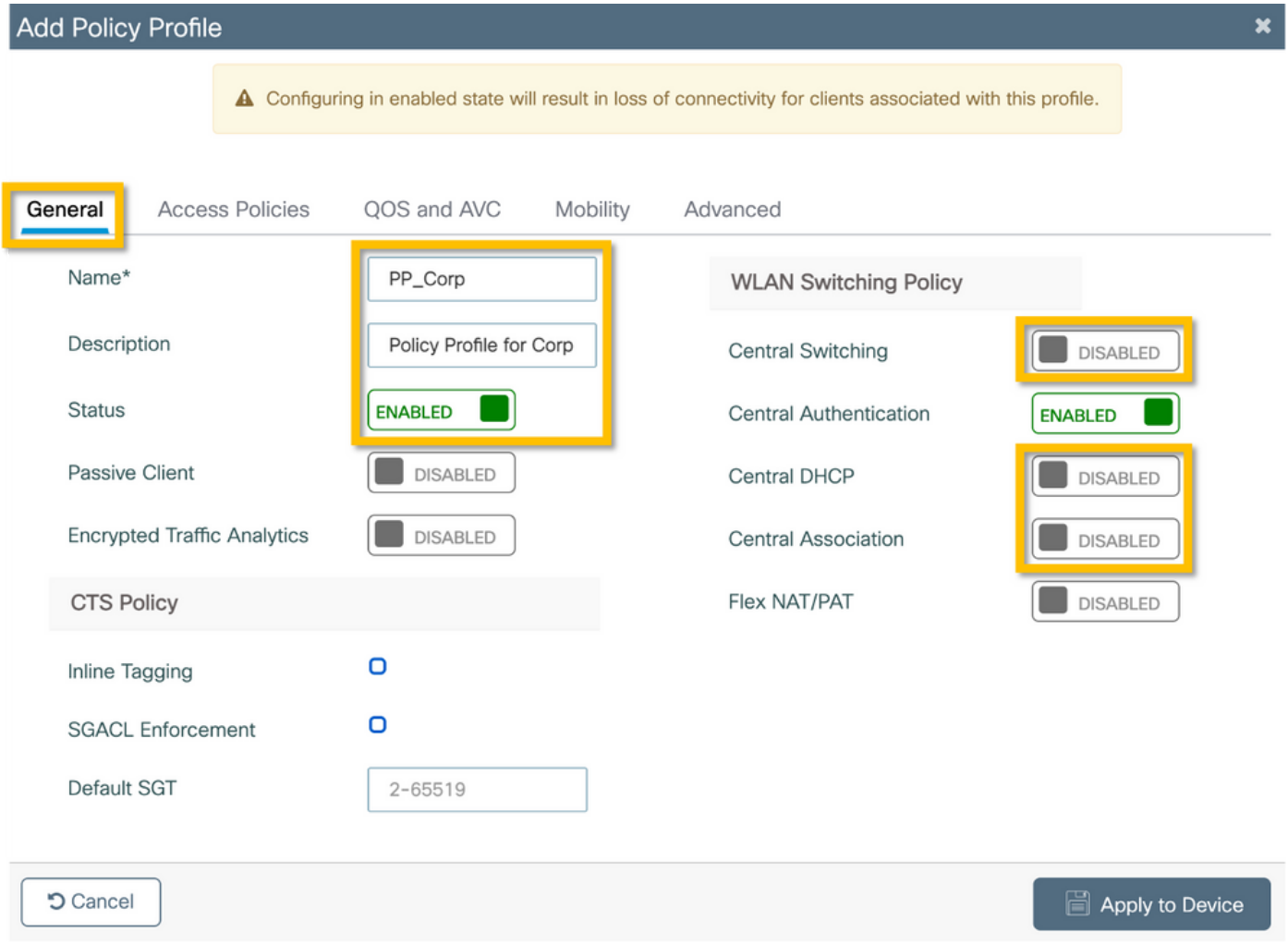


ステップ3:[AAA] サブタブに移動し、以前に設定した認証方式リストを選択します。次の図に示すように、[Apply to Device] ボタンをクリックします。

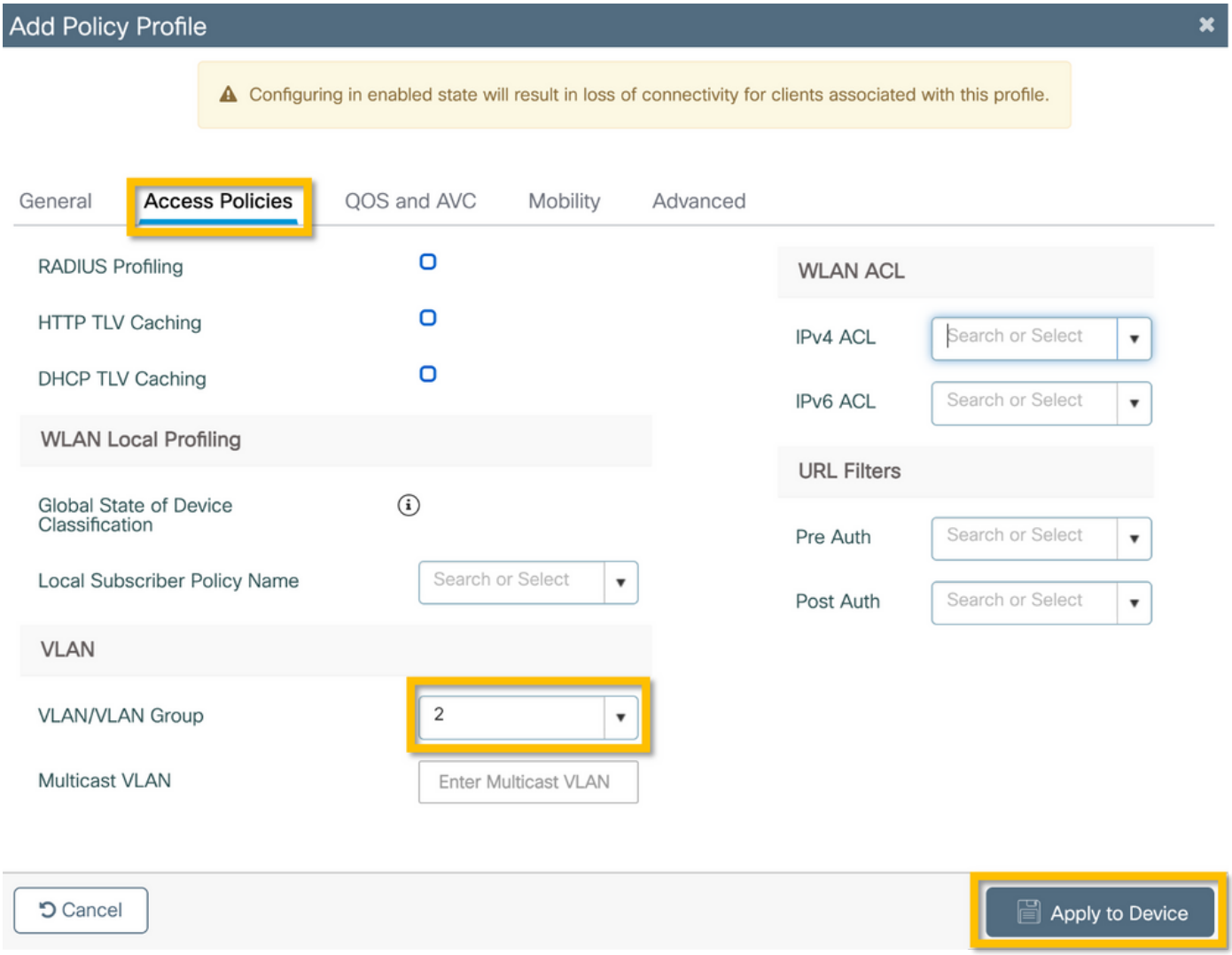


C9800：ポリシープロファイルの設定

ステップ1:[Configuration] > [Tags & Profiles] > [Policy] に移動し、[Add] をクリックして、ポリシープロファイルの名前と説明を入力します。図に示すように、企業ユーザトラフィックがAPでローカルにスイッチングされるため、ポリシーを有効にし、中央スイッチング、DHCP、およびアソシエーションを無効にします。



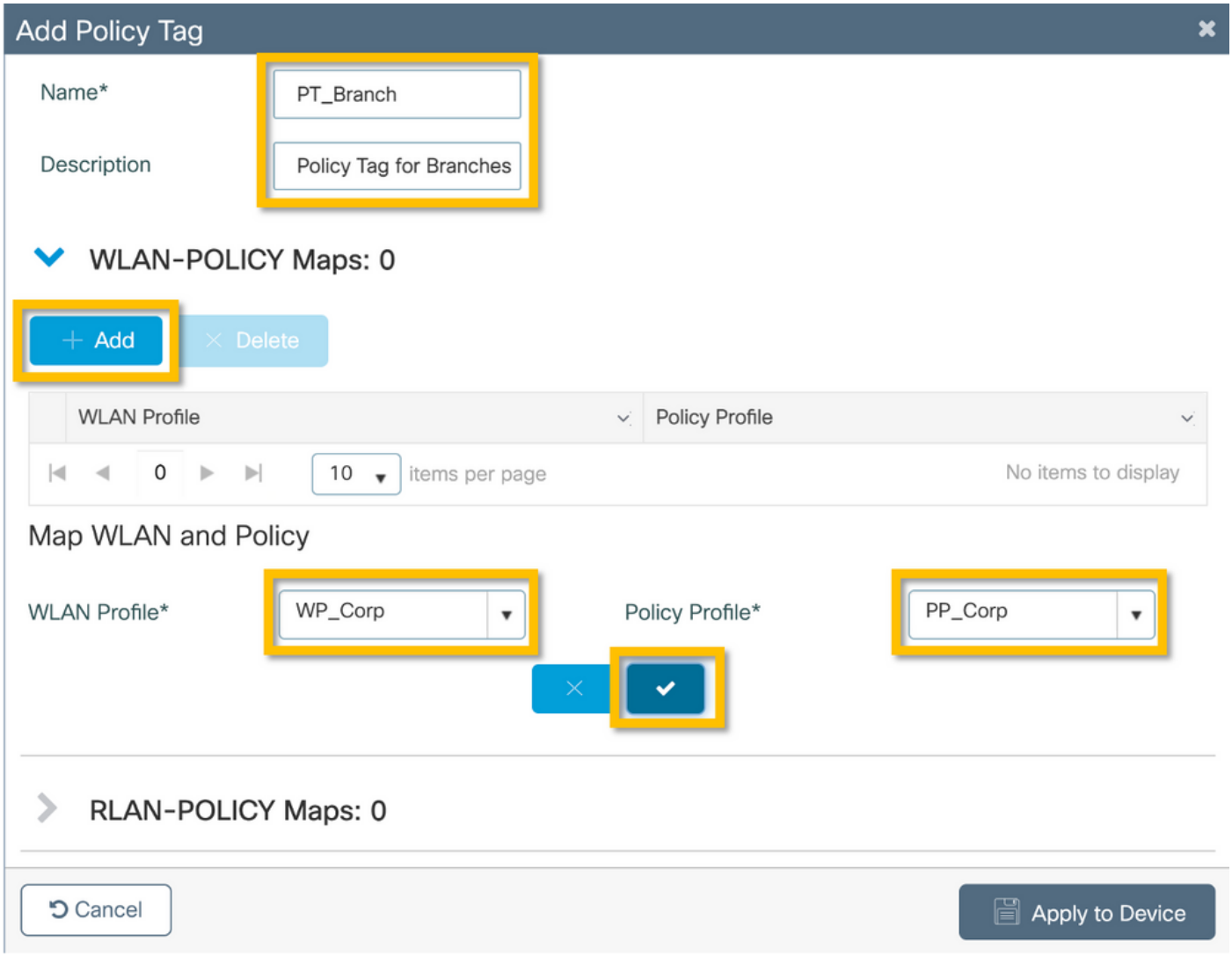
ステップ2:[Access Policies] タブに移動し、ブランチで企業ユーザトラフィックに使用するVLANのIDを手動で入力します。このVLANは、C9800自体で設定する必要はありません。詳細に従って、Flex Profileで設定する必要があります。ドロップダウンリストからVLAN名を選択しないでください(Cisco Bug ID CSCvn48234を参照)。 を参照してください)。 次の図に示すように、[Apply to Device] ボタンをクリックします。



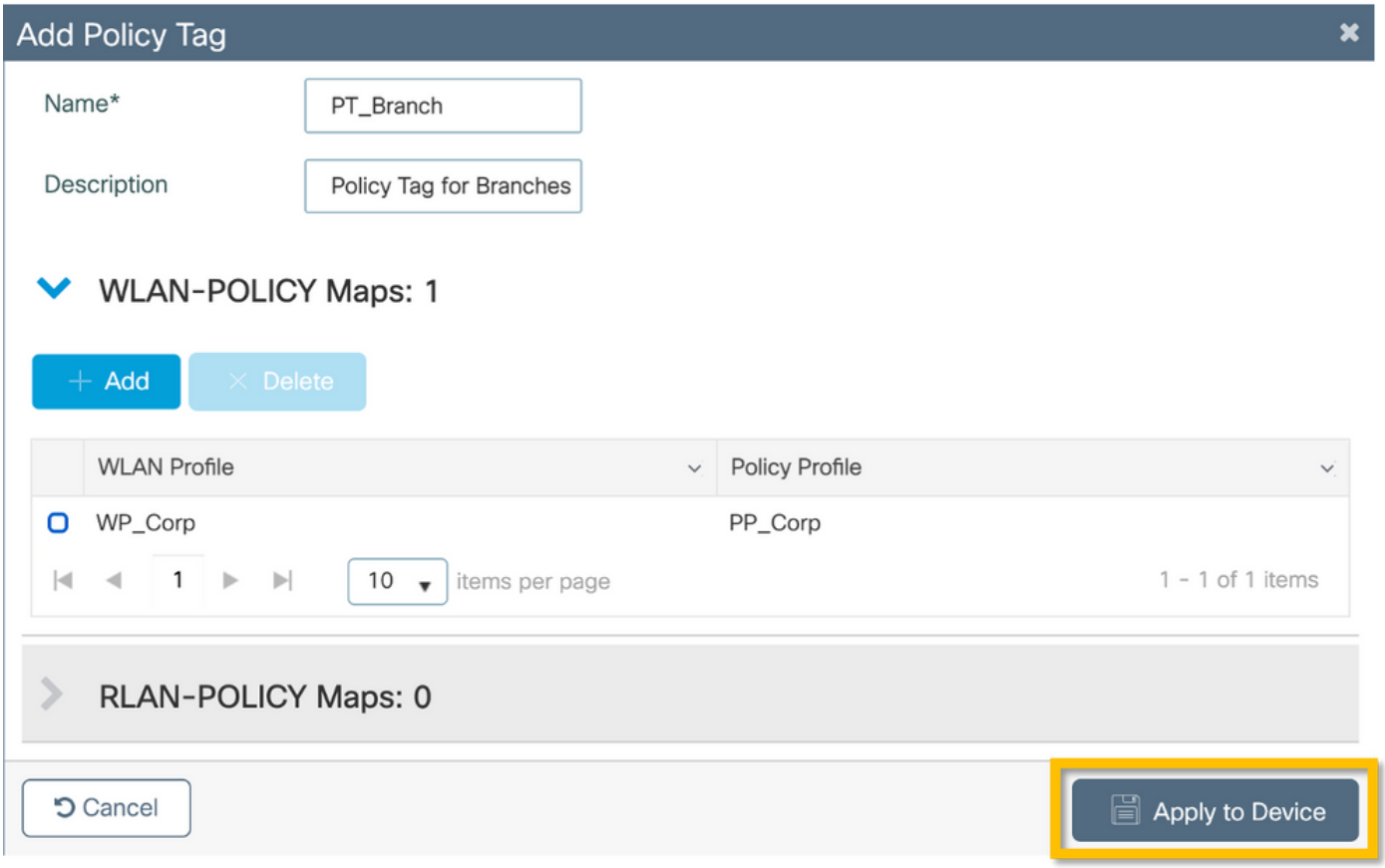
C9800：ポリシータグの設定

WLANプロファイル(WP_Corp)とポリシープロファイル(PP_Corp)を作成したら、これらのWLANとポリシープロファイルをバインドするためにポリシータグを作成する必要があります。このポリシータグは、アクセスポイントに適用されます。このポリシータグをアクセスポイントに割り当て、アクセスポイント上で選択したSSIDを有効にするこれらの設定をトリガーします。

ステップ1:[Configuration] > [Tags & Profiles] > [Tags] に移動し、[Policy] タブを選択して、[Add] をクリックします。ポリシータグの名前と説明を入力します。[WLAN-POLICY Maps] の下の [Add] をクリックします。先ほど作成したWLANプロファイルとポリシープロファイルを選択し、次の図に示すようにチェックマークボタンをクリックします。



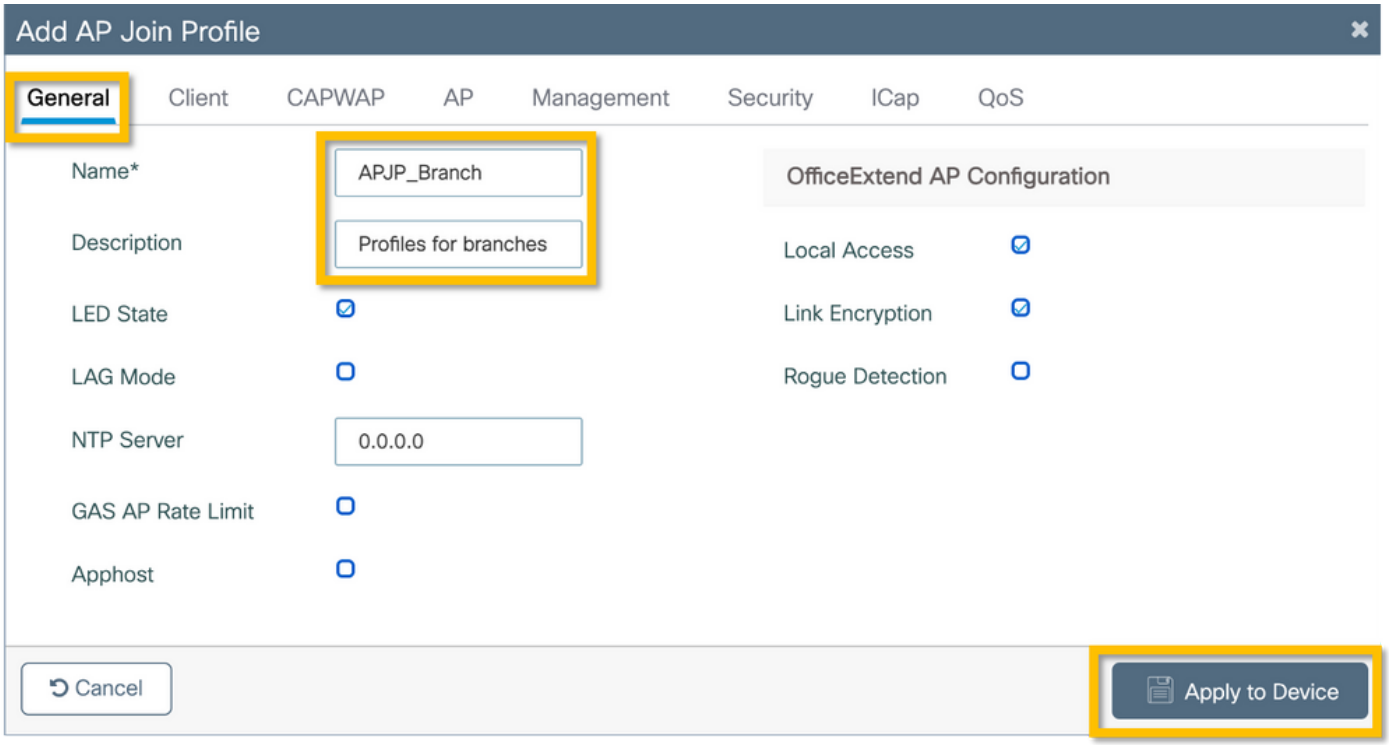
ステップ2：確認し、次の図に示すように[Apply to Device] ボタンをクリックします。



C9800:AP加入プロファイル

AP加入プロファイルとFlexプロファイルを設定し、サイトタグを使用してアクセスポイントに割り当てる必要があります。ブランチ内で802.11r Fast Transition(FT)をサポートし、そのブランチのAP間でのクライアントPMKの配布だけを制限するには、ブランチごとに異なるサイトタグを使用する必要があります。複数のブランチ間で同じサイトタグを再利用しないことが重要です。AP加入プロファイルを設定します。すべてのブランチが類似している場合は単一のAP加入プロファイルを使用でき、設定パラメータの一部が異なっている必要がある場合は複数のプロファイルを作成できます。

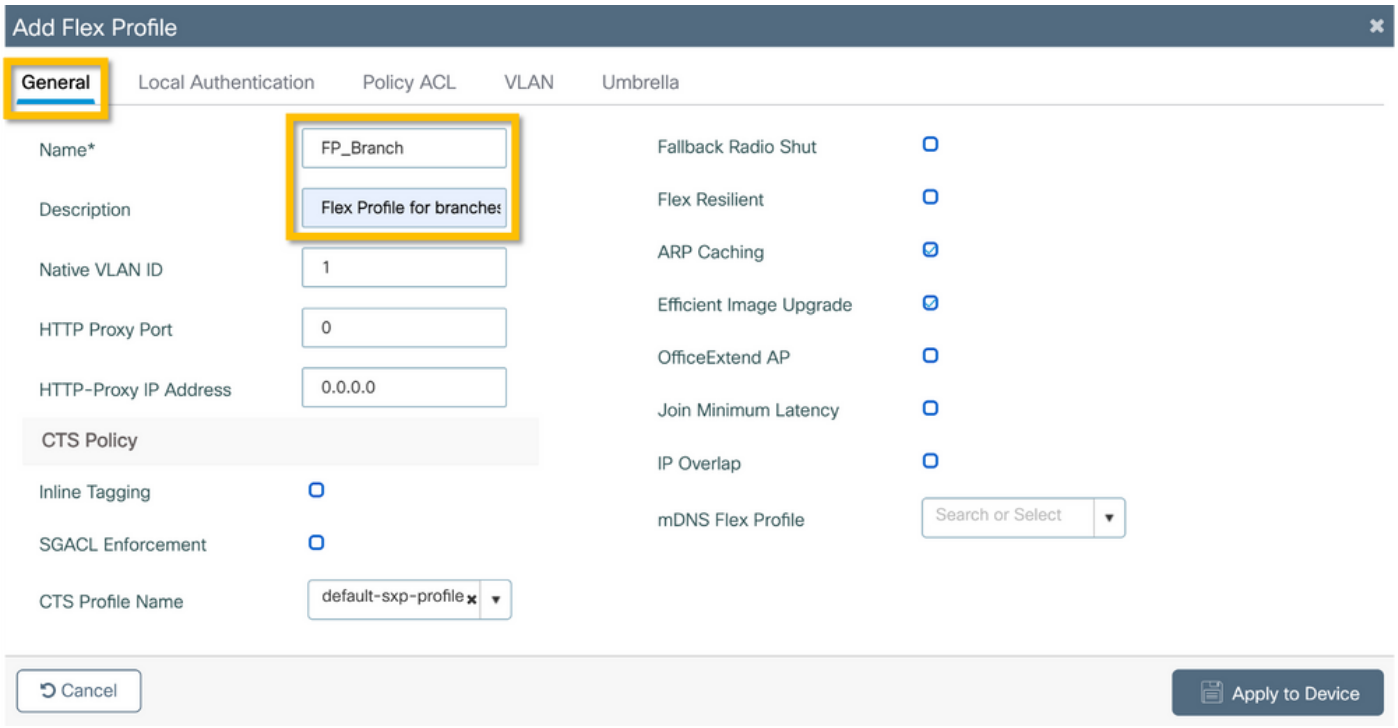
ステップ1:[Configuration] > [Tags & Profiles] > [AP Join] に移動し、[Add] をクリックします。AP加入プロファイルの名前と説明を入力します。次の図に示すように、[Apply to Device] ボタンをクリックします。



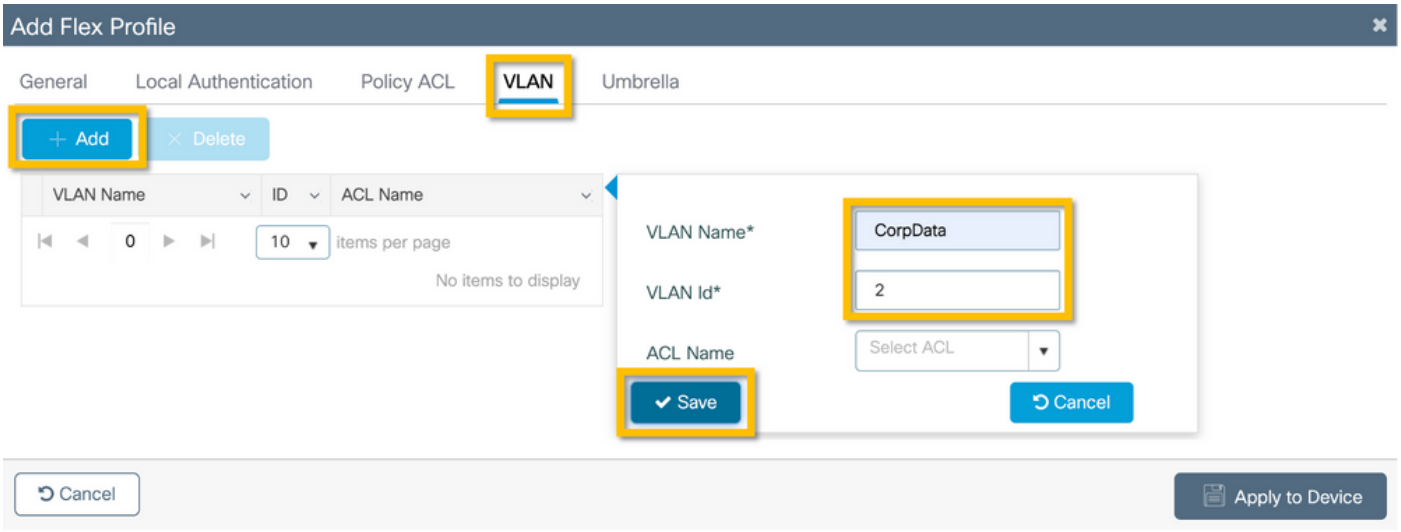
C9800:Flexプロファイル

次に、Flex Profileを設定します。ここでも、すべてのブランチが類似していて、同じVLAN/SSIDマッピングを持つ場合は、単一のプロファイルを使用できます。また、VLAN割り当てなどの設定パラメータが異なる場合は、複数のプロファイルを作成できます。

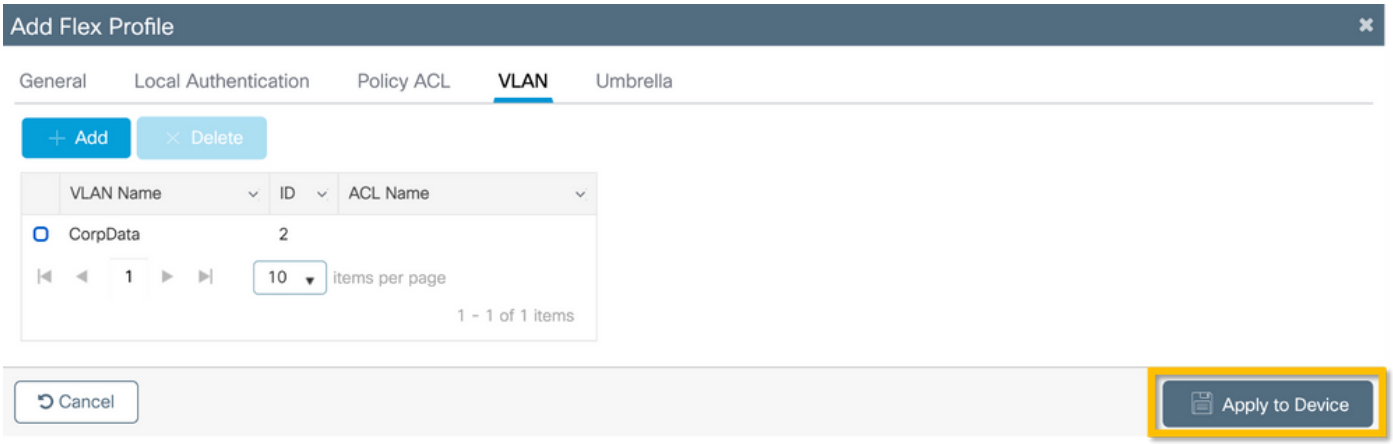
ステップ1:[Configuration] > [Tags & Profiles] > [Flex] に移動し、[+Add] をクリックします。Flexプロファイルの名前と説明を入力します。



ステップ2:[VLAN] タブに移動し、[Add] をクリックします。APが企業ユーザトラフィックをローカルでスイッチするために使用する必要がある、ブランチのローカルVLANのVLAN名とIDを入力します。次の図に示すように、[Save] ボタンをクリックします。



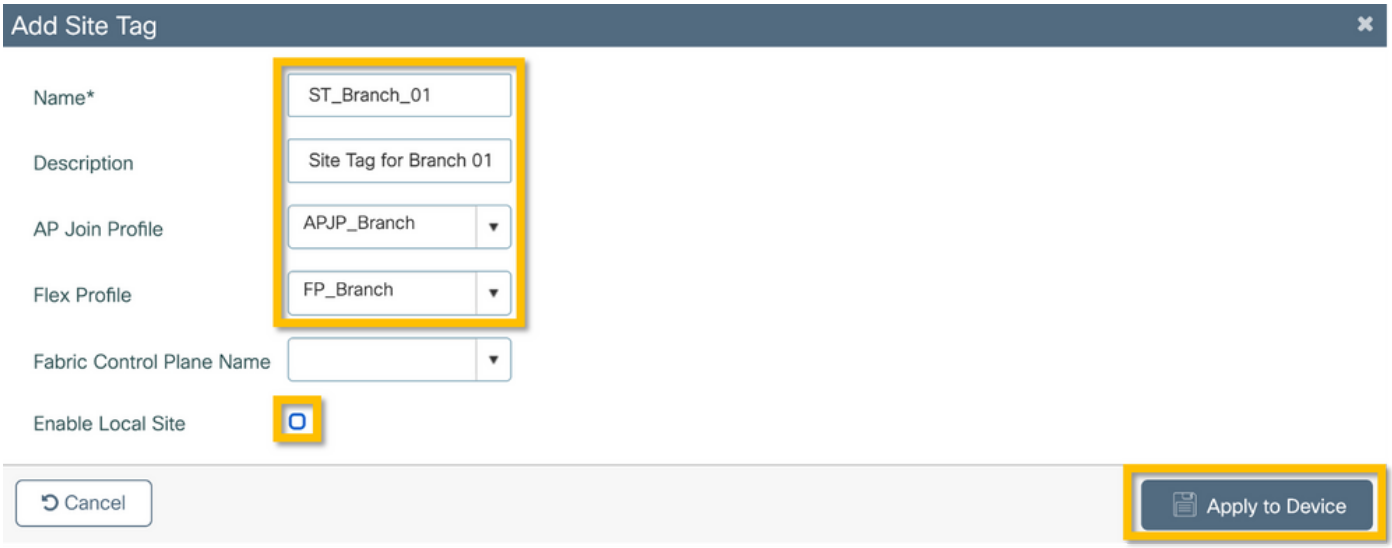
ステップ3：確認し、次の図に示すように[Apply to Device] ボタンをクリックします。



C9800 – サイトタグ

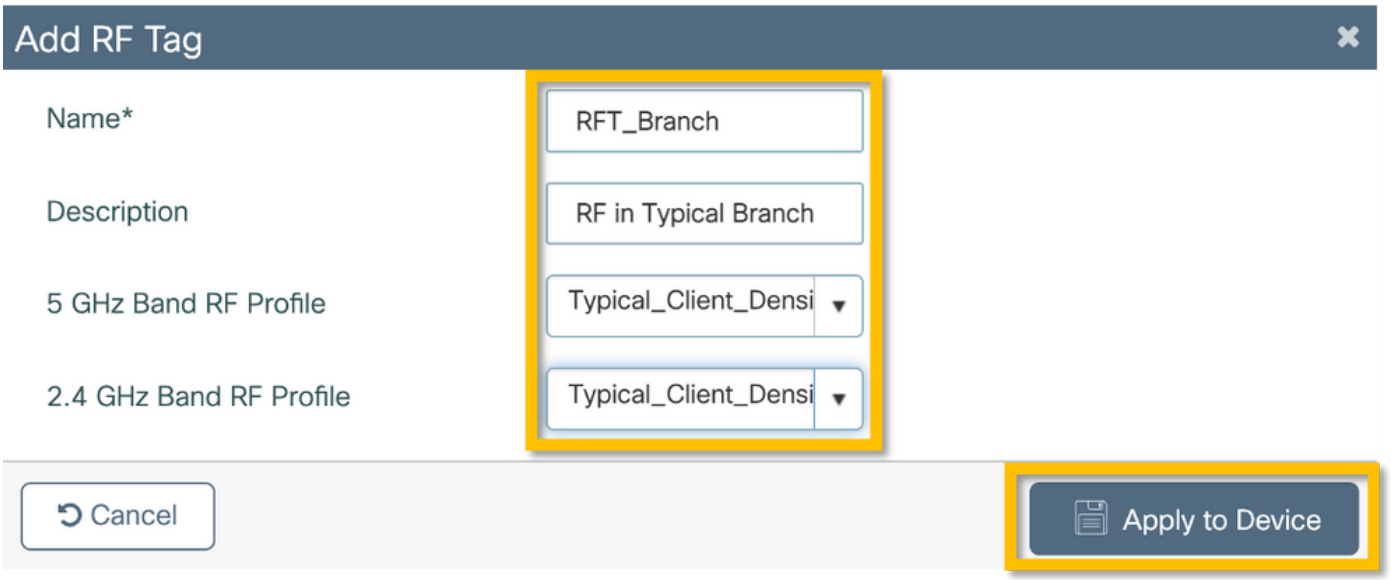
サイトタグは、接続プロファイルとFlexプロファイルをアクセスポイントに割り当てるために使用されます。前に説明したように、ブランチ内で802.11r Fast Transition(FT)をサポートし、そのブランチのAP間でのクライアントPMKの配布だけを制限するには、ブランチごとに異なるサイトタグを使用する必要があります。

ステップ1:[Configuration] > [Tags & Profiles] > [Tags] に移動し、[Site] タブを選択して、[Add] をクリックします。サイトタグの名前と説明を入力し、作成したAP加入プロファイルを選択し、[Enable Local Site] ボックスのチェックマークを外して、最後に以前に作成したFlexプロファイルを選択します。[Enable Local Site] ボックスをオフにして、アクセスポイントを[Local Mode] から[FlexConnect] に変更します。最後に、次の図に示すように[Apply to Device] ボタンをクリックします。



C9800 - RFタグ

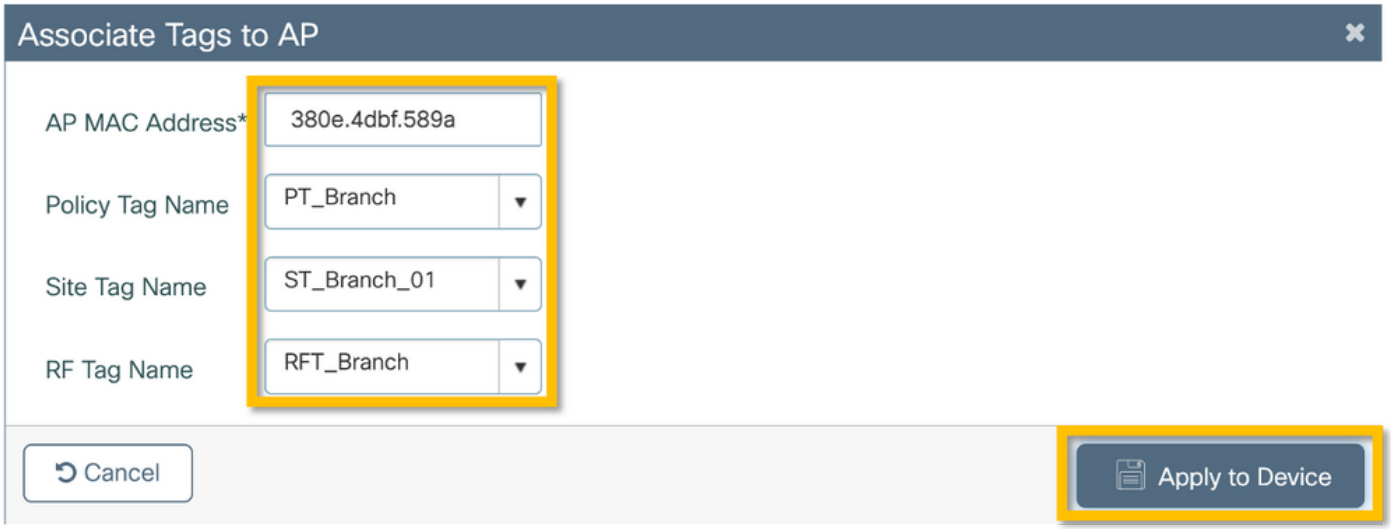
ステップ1:[Configuration] > [Tags & Profiles] > [Tags] に移動し、[RF] タブを選択して、[Add] をクリックします。RFタグの名前と説明を入力します。ドロップダウンメニューからシステム定義の**RFプロファイルを選択します。**次の図に示すように、[Apply to Device] ボタンをクリックします。



C9800:APへのタグの割り当て

これで、アクセスポイントの設定に必要なさまざまなポリシーとプロファイルを含むタグが作成されました。これらのタグをアクセスポイントに割り当てる必要があります。このセクションでは、アクセスポイントに割り当てられたスタティックタグを、そのイーサネットMACアドレスに基づいて手動で実行する方法を示します。製品の実稼働環境では、Cisco DNA Center AP PNP Workflowを使用するか、9800で使用可能な静的バルクCSVアップロード方式を使用することをお勧めします。

ステップ1:[Configure] > [Tags & Profiles] > [Tags] に移動し、[AP] タブ、[Static] タブの順に選択します。**+Add**をクリックし、APのMACアドレスを入力して、以前に定義したPolicy Tag、Site Tag、およびRF Tagを選択します。次の図に示すように、**Apply to Device**ボタンをクリックします。



Aruba CPPMの設定

Aruba ClearPass Policy Managerサーバの初期設定

Aruba clearpassは、次のリソースを使用してESXiサーバ上のOVFテンプレート経由で導入されます。

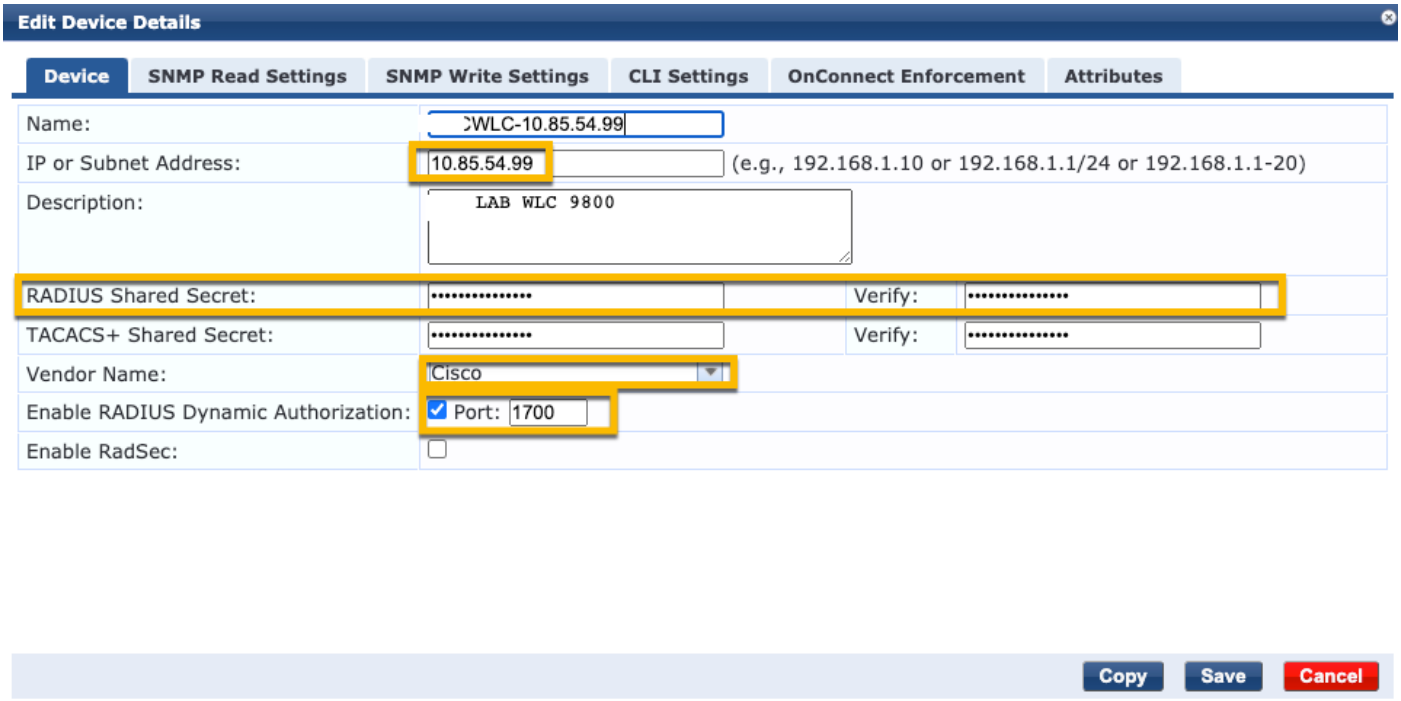
- 予約済み仮想CPU X 2
- メモリ 6 GB
- 80 GBディスク（マシンの電源を入れる前に、最初のVM導入後に手動で追加する必要がある）

ライセンスの適用

プラットフォームライセンスを適用するには、[Administration] > [Server Manager] > [Licensing] を選択します。アクセスの**追加とオンボード**

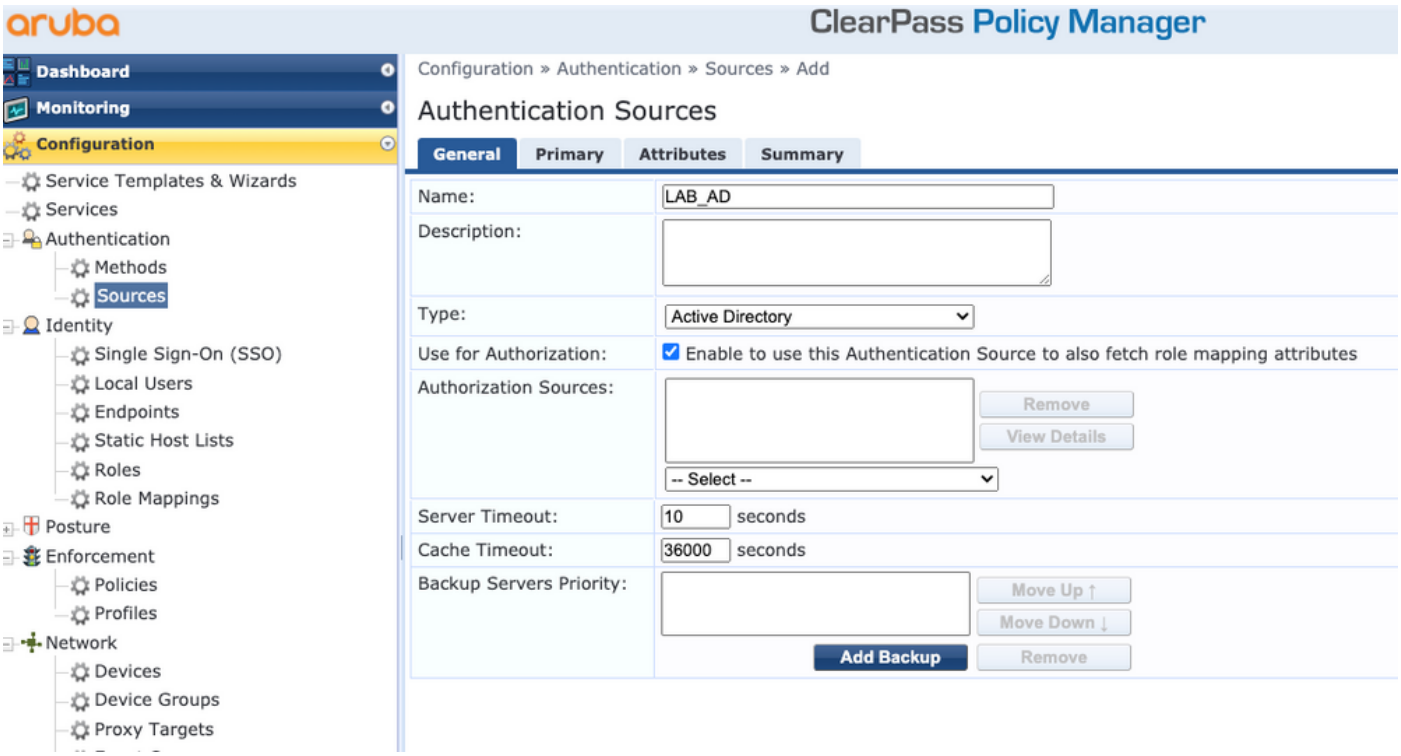
C9800ワイヤレスコントローラをネットワークデバイスとして追加する

次の図に示すように、[Configuration] > [Network] > [Devices] > [Add] に移動します。



Windows ADを認証ソースとして使用するためのCPPMの設定

[Configuration] > [Authentication] > [Sources] > [Add] に移動します。タイプでActive Directoryを選択します。



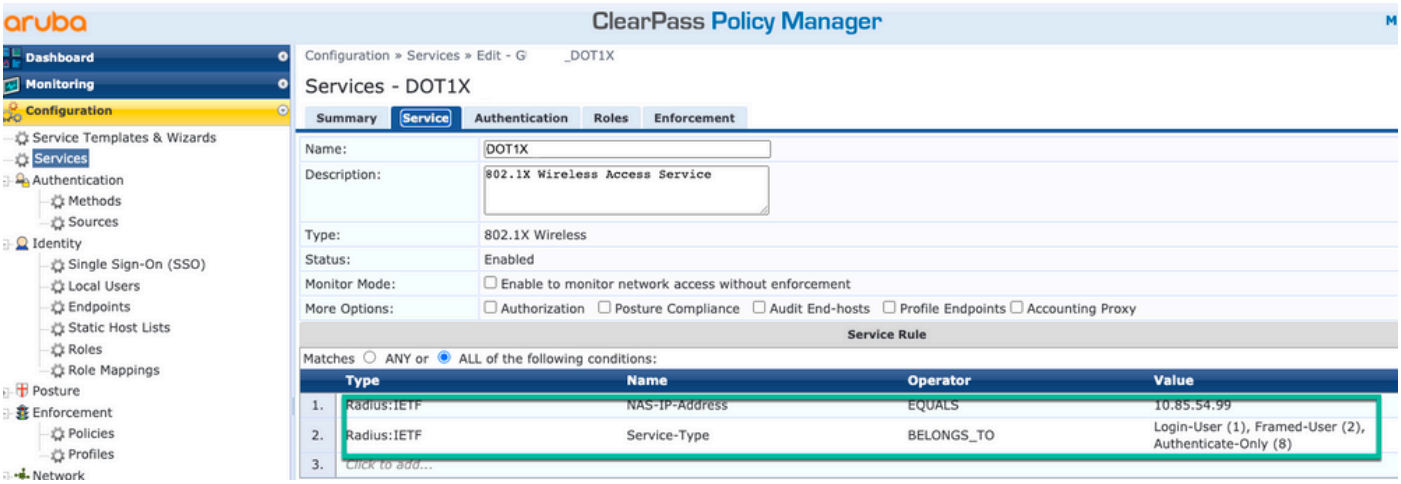
CPPMの設定 Dot1X認証サービス

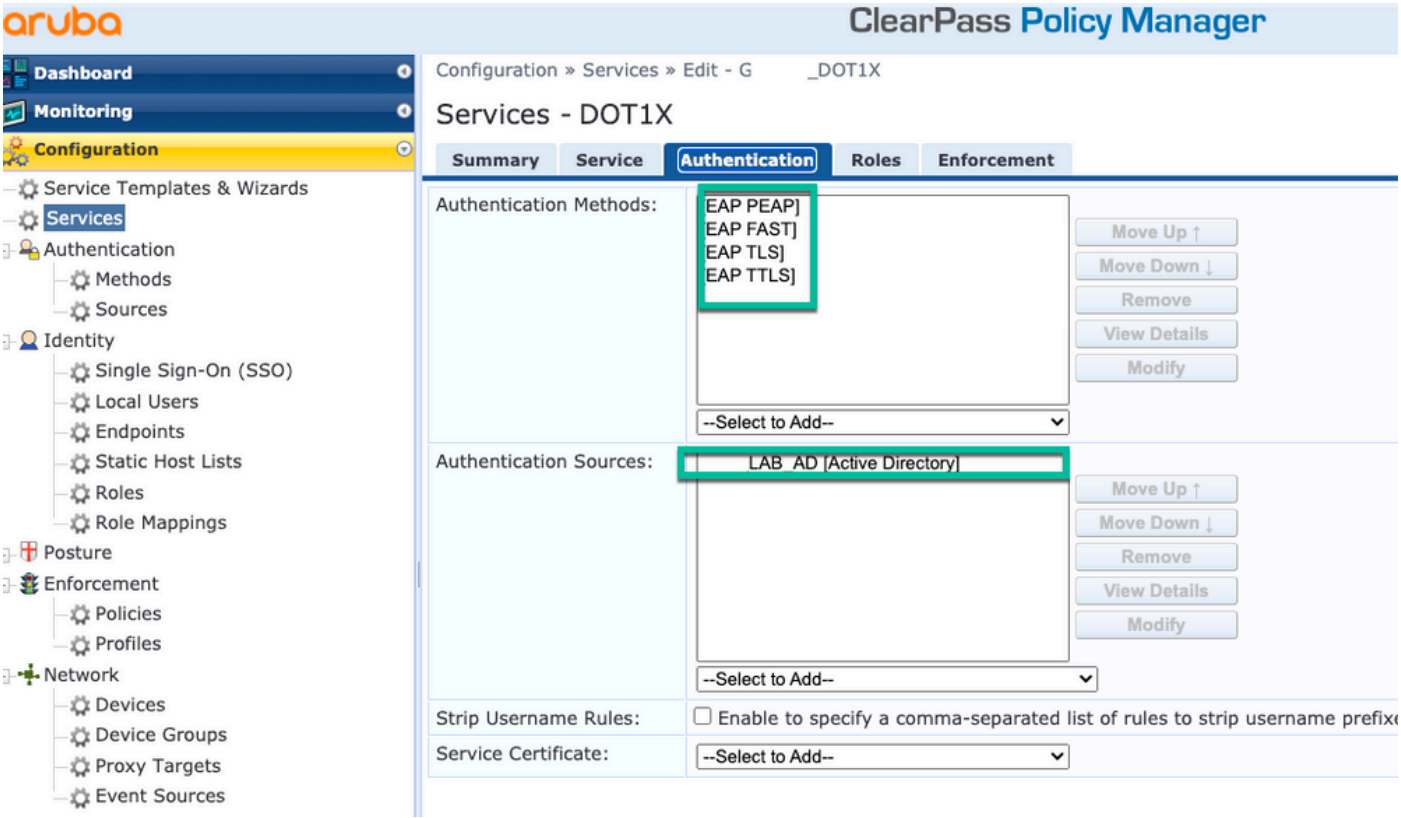
ステップ1：複数のRADIUS属性に一致する「サービス」を作成します。

- 半径：IETF |名前：nas-ip-address | EQUALS | <IPアドレス>
- 半径：IETF |名前：Service-Type | EQUALS |1,2,8

ステップ2：実稼働環境では、「NAS-IP-Address」ではなくSSID名を照合して、1つの条件で十

分なマルチWLC環境を実現することをお勧めします。Radius:Cisco:Cisco-AVPair | cisco-wlan-ssid | Dot1XSSID





確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- 『Cisco 9800 Deployment Best Practices Guide』

- Catalyst 9800ワイヤレスコントローラの設定モデルについて
- Catalyst 9800ワイヤレスコントローラでのFlexConnectについて
- **テクニカル サポートとドキュメント – Cisco Systems**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。