FlexConnectモードでのローカル認証の設定

内容

概要

- 背景説明
  - FlexConnectの概要と要件
  - 操作のモード
  - 高速セキュア ローミング
  - FlexConnectハイスケールモード
  - Wi-Fi 7 FlexConnectのサポート
  - FlexConnectの復元力のシナリオ

前提条件

- 要件
- 使用するコンポーネント

設定

- ネットワーク図
- AAAサーバの設定
- リモートサイトでのFlexConnectモードの設定
- 外部RADIUSサーバを使用したローカル認証による802.1x WLANの設定
- ISE の設定
- ローカル認証を使用したPSK WLANの設定

確認

トラブルシューティング

- スタンドアロンシナリオ

関連情報

概要

このドキュメントでは、FlexConnectローカル認証の仕組みと、Cisco Catalyst 9800シリーズワイヤレスコントローラ(WLC)を使用した設定方法について説明します

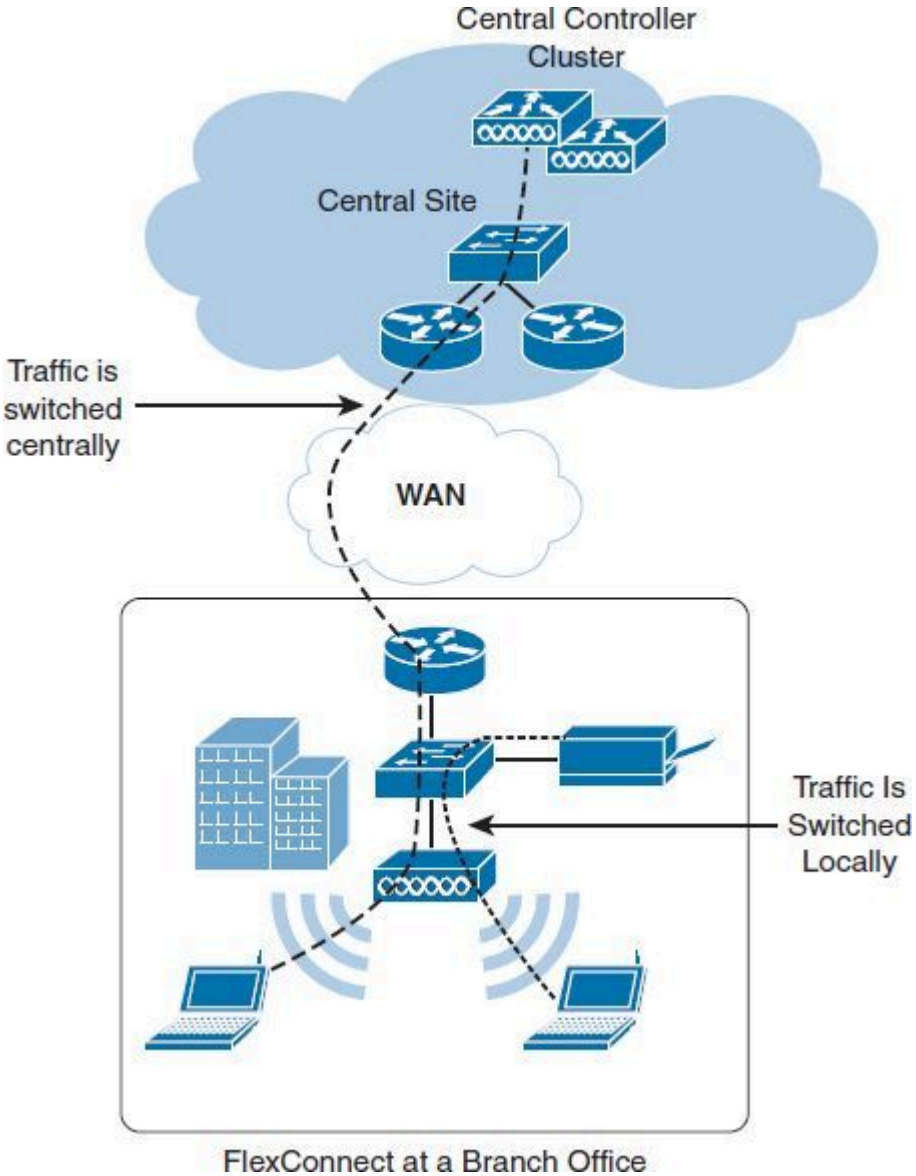
背景説明

FlexConnectの概要と要件

FlexConnectを使用すると、リモートオフィスまたはブランチオフィスのアクセスポイント(AP)を中央のコントローラに接続しながら、ワイヤレストラフィックをローカルで処理できます。すべてのワイヤレストラフィックがCAPWAP(Control and Provisioning of Wireless Access

Points)を使用してコントローラにトンネリングされる従来の中央集中型のワイヤレス展開とは異なり、FlexConnectでは、トラフィックをブランチAPによって直接ローカルにスイッチングおよび処理できます。このローカルスイッチングにより、APはある程度の自律性を持つようになり、セキュリティ、ローミング、Quality of Service(QoS)などの主要なサービスをコントローラから独立して機能させることができます。

FlexConnectは主にローカルトラフィックスイッチング用に設計されていますが、必要に応じて特定のSSID(Service Set Identifier)を中央で柔軟に切り替えることもできます。たとえば、特定のトラフィックが中央のファイアウォールを通過する必要がある場合、これらのSSIDをCAPWAP経由でコントローラに返送して、スイッチングを一元化できます。このデュアル機能により、1つのFlexConnect APで、ローカルと中央の両方でスイッチングされるWLAN(Wireless Local Area Network)を同時にサポートできます。



ブランチに導入されたFlexConnect APは、あるSSIDをローカルにスイッチングし、別のSSIDは中央でスイッチングする

操作のモード

FlexConnect APは、接続モードとスタンドアロンモードの2つのモードで動作します。

- 接続モードの場合、APはCAPWAP制御チャネルを介してコントローラへのアクティブな接続を維持します。
- スタンドアロンモードは、APがコントローラへの接続を失ったときに発生するフォールバック状態です。

通常の状態では、FlexConnect APは接続モードで機能します。このモードでは、コントローラが中央集中型認証、クライアントプロファイリング、Radio Resource Management(RRM)などの重要なサービスを管理します。 ほとんどの場合、APはこのモードのままですが、コントローラとの通信が失われると、自動的にスタンドアロンモードに切り替わります。スタンドアロンモードでは、APは動作を継続し、トラフィックをローカルでスイッチングして、クライアントの接続を維持できます。APは、認証要求をセントラルコントローラに転送せずに、クライアントを個別に認証します。ただし、RRMや集中型クライアント認証など、コントローラに依存する特定のサービスは一時的に使用できなくなります。

たとえば、WAN（ワイドエリアネットワーク）の障害によってAPとコントローラの間の接続が中断されても、インターネットアクセスがアクティブなままの場合、APはスタンドアロンモードに移行し、中断されることなくローカルでスイッチングされるトラフィックを処理し続けます。既存のクライアントは接続されたままですが、中央認証を必要とする新しいクライアントは、ローカル認証が設定されていない限り、ネットワークに参加できません。FlexConnect APは、WANの障害時にローカル認証を実行するように設定できるため、コントローラに到達できない場合でもサービスを継続できます。

スタンドアロンモードの場合、APでは次の機能を使用できません。

- クライアントWeb認証
- ゲスト認証（ポータルリダイレクション）
- 中央でスイッチングされるSSID
- RRM
- IPv6レイヤ3モビリティ
- ネイティブプロファイリング
- ポリシーの分類
- サービス検出ゲートウェイ
- 構成の更新

スタンドアロンモード（ローカル認証）でサポートされる機能およびWLAN設定の完全なリストについては、機能マトリックス「Ciscoワイヤレスアクセスポイントの機能マトリックス」を参照してください。

一般的なFlexConnectの障害シナリオでは、WANの完全な喪失または著しい劣化が発生し、CAPWAP制御チャネルが中断されます。WANの問題が原因でAPからコントローラへの接続が失われると、APはただちにスタンドアロンモードに切り替わります。

WAN障害時の主な目的は、コントローラとの通信をできるだけ早く回復し、すべての機能を再開することです。

WANの障害が原因でFlexConnect APがスタンドアロンモードになると、アクティブクライアントは接続されたままになり、FlexConnectドメイン/サイトタグ内のAP間でシームレスにローミングできますが、異なるFlexConnectサイトタグ間でのローミングでは完全な再認証が必要になる場合があります。ただし、中央ロケーションのAAAサーバ(Authentication, Authorization, and Accounting（AAA；認証、認可、アカウンティング）に到達できないため、ローカルでスイッチされるWLANに参加しようとする新しいクライアントは認証できません。

高速セキュア ローミング

EAP(Extensible Authentication Protocol)認証では、AAAサーバとEAPフレームが交換されるため、PSK（事前共有キー）認証よりも遅延が大きくなります。ただし、高速セキュアローミングでは、クライアントはネットワークとの最初の関連付けの間にのみ完全な802.1X/EAP認証を受けます。その後のネイバーAPへのローミングでは、EAP交換がバイパスされて4ウェイハンドシェイクだけが残りますが、これはAAAサーバを含まないため、かなり高速です。次の表は、ローカルモードとFlexConnectの両方の導入で9800 WLCがサポートするさまざまな高速セキュアローミング方式の概要を示しています。

機能	ローカル モード	FlexConnect（接続モード、中央認証）	FlexConnect（接続モード：ローカル認証）	FlexConnect（スタンドアロン）
スティッキーキーキャッシング(SKC)	Not Supported	Not Supported	Not Supported	Not Supported
Opportunistic Key Caching(OKC)	サポート対象	サポート対象	サポート対象	サポート（クライアントセッションの期限が切れるまで）

Cisco Centralized Key Management（CCKM）	サポート対象	サポート対象	サポート対象	Not Supported
FT-802.11r/Adaptive 11r（高速移行）(Over the Air)	サポート対象	サポート対象	サポート対象	サポート（クライアントセッションの期限が切れるまで）
FT-802.11r/Adaptive 11r(Fast Transition)（DS上）	サポート対象	サポート対象	Not Supported	Not Supported

スタンドアロンモードでは、高速ローミングはキャッシュされた有効なキーの内容に依存します。キャッシュされたPMK(Pairwise Master Key)/セッションの有効期限が切れると、コントローラの接続が復元されるまで、APは新しいコントローラ由来のキー情報を取得できません。

FlexConnectハイスケールモード

Cisco IOS XE 17.8.1以降では、300台のAPと3000台の802.1xクライアントに対応するようにフレックスサイトのサイト容量が拡張されました。

PMK伝搬により、同じFlexConnectサイト内のAPがPMK情報を共有できるようになり、ローミング時の完全なEAP交換の必要性が軽減されます。PMK伝達はデフォルトでは有効になっていません。

PMKの伝播を確認し、PMKを有効にするには、次のコマンドを使用します。

- show wireless stats pmk-propagation（オプション）
- pmk伝播

Wi-Fi 7 FlexConnectのサポート

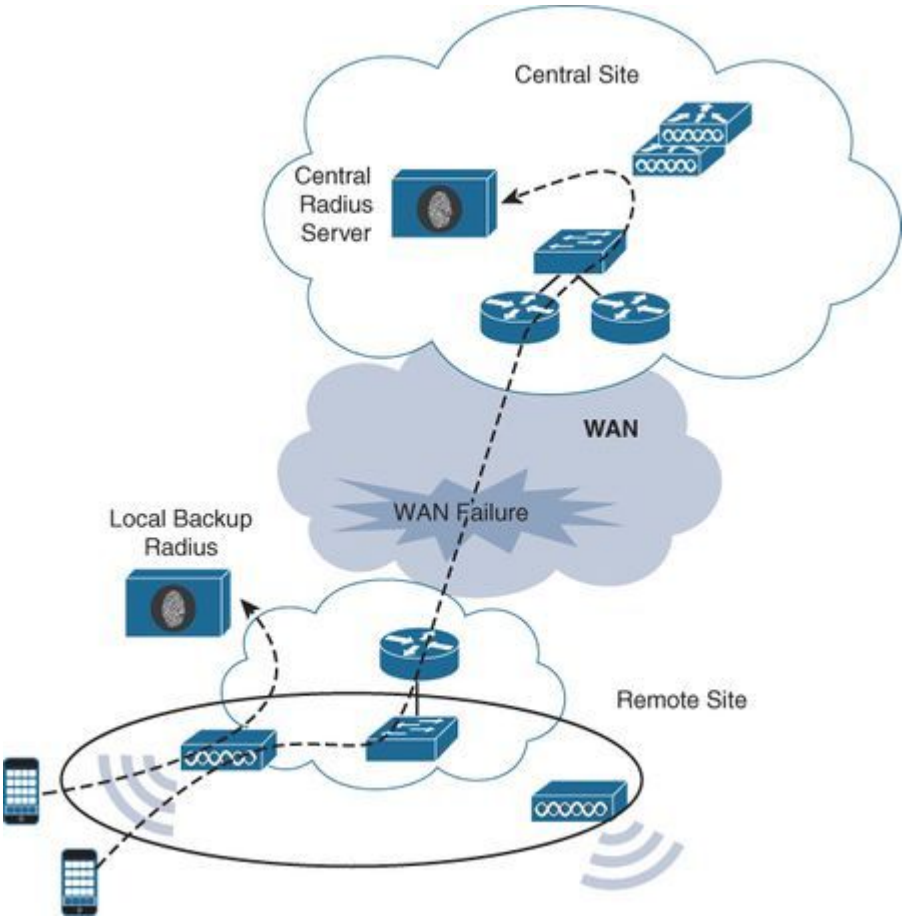
次の表は、CW917x Wi-Fi 7 APファミリでサポートされているFlexConnectの機能をまとめたものです。

機能	サポート
ローカル スイッチング	サポート対象
中央スイッチング	サポート対象

WLAN-VLANマッピング	サポート対象
外部RADIUSを使用したローカル認証	サポート対象
WPA3 – エンタープライズ	サポート対象
FT-802.11r高速ローミング	サポート対象
マルチリンクオペレーション(MLO)	サポート対象
内部RADIUSを使用したローカル認証	Not Supported
WPA3-Enterprise-192	Not Supported

FlexConnectの復元力のシナリオ

1. N+1の復元力の設定では、アクティブなコントローラのいずれかに障害が発生した場合に引き継ぐ共通のバックアップコントローラが複数のアクティブなコントローラで共有されます。プライマリコントローラがオフラインになると、FlexConnect APはただちにスタンドアロンモードに切り替わり、バックアップコントローラの検索を開始します。この切断期間中に、中央でスイッチングされているクライアントがAPから切断されます。APがバックアップコントローラを見つけて同期すると、中央でスイッチングされるSSIDへのアクセスを必要とするクライアントが再接続されます。その間、ローカルでスイッチされるクライアントは影響を受けず、サービスの中断に気づくことなく動作し続けます。
2. FlexConnectグループからアクセス可能なリモートロケーションにバックアップAAAサーバを提供します。ローカル認証がイネーブルになっている場合、このバックアップRADIUSサーバは、APがスタンドアロンモードに入ったときだけ使用され、APが接続モードの間、非アクティブなままになります。FlexConnect APが認証にローカルバックアップAAAサーバを使用する場合、認証キーは、中央集中型AAAサーバの場合と同様に、FlexConnectグループ内のすべてのAPに分散されます。これにより、バックアップRADIUSサーバが使用されている場合でも、新しいクライアントがAP間でシームレスにローミングでき、再認証が不要になります。
3. ローカル認証を可能にする、『シスコワイヤレスアクセスポイントの機能マトリクス』に記載されている方式。



WANの障害により中央のAAAサーバが使用できなくなったときに、クライアントがローカルバックアップAAAサーバに対して認証を行う

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

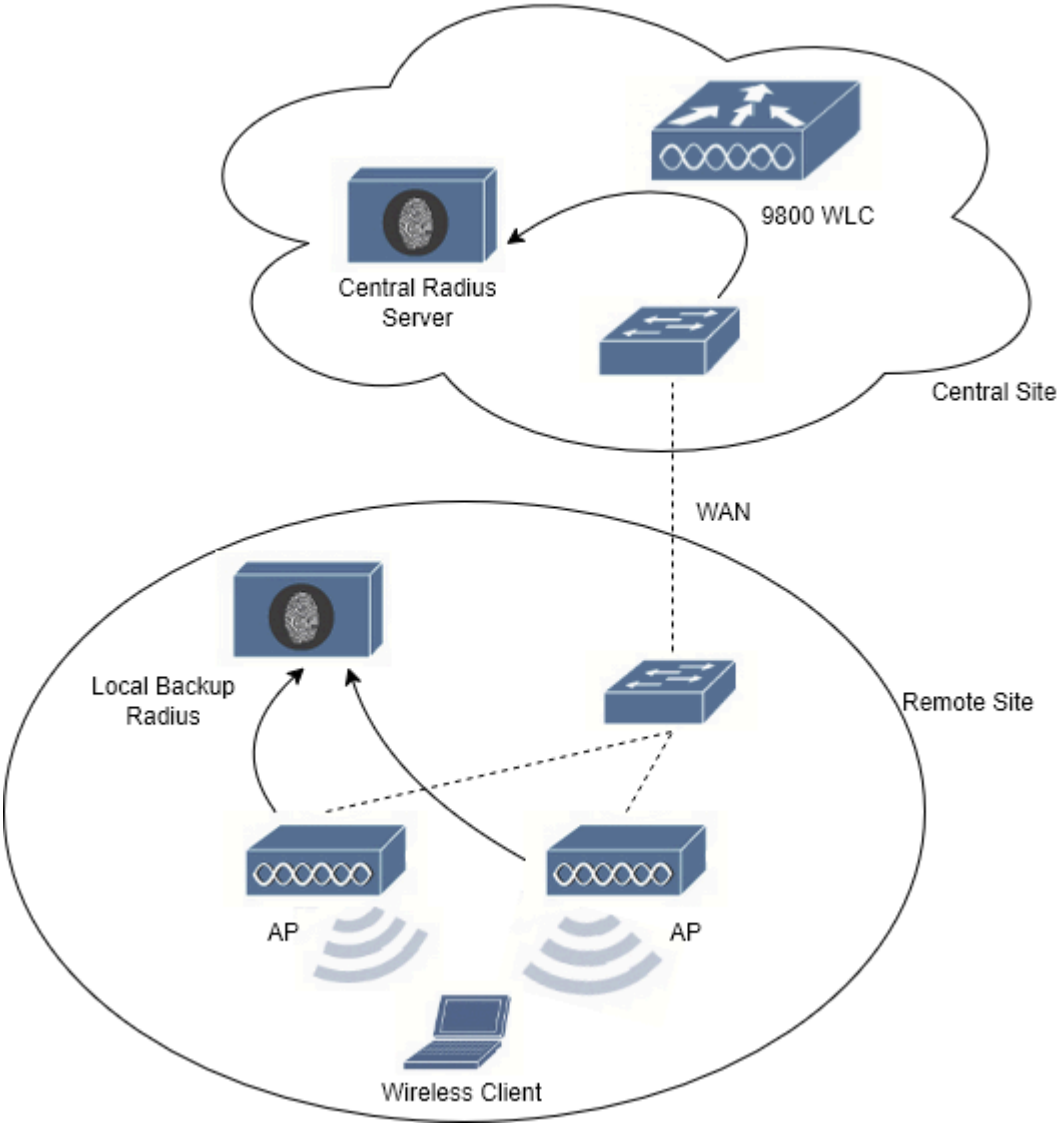
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- クラウド向けCatalyst C9800-CLワイヤレスコントローラ（Cisco IOS® XE Dublin 17.18.3搭載）
- Catalyst CW9164I-ROWアクセスポイントv17.18.3.18
- Aironet® AIR-AP2802I-E-K9アクセスポイントv17.18.3.18
- Identity Services Engine v3.2.0.542 X 2

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。

設定

ネットワーク図



ネットワーク図

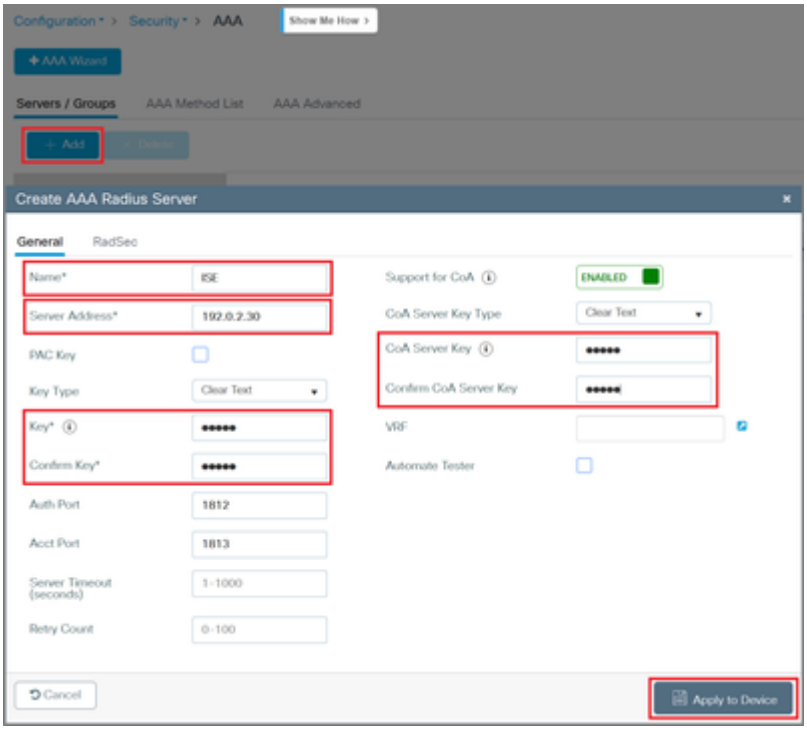
AAAサーバの設定

ステップ 1：802.1x WLANを設定するには、9800 WLC上にAAAサーバグループを作成する必要

があります。

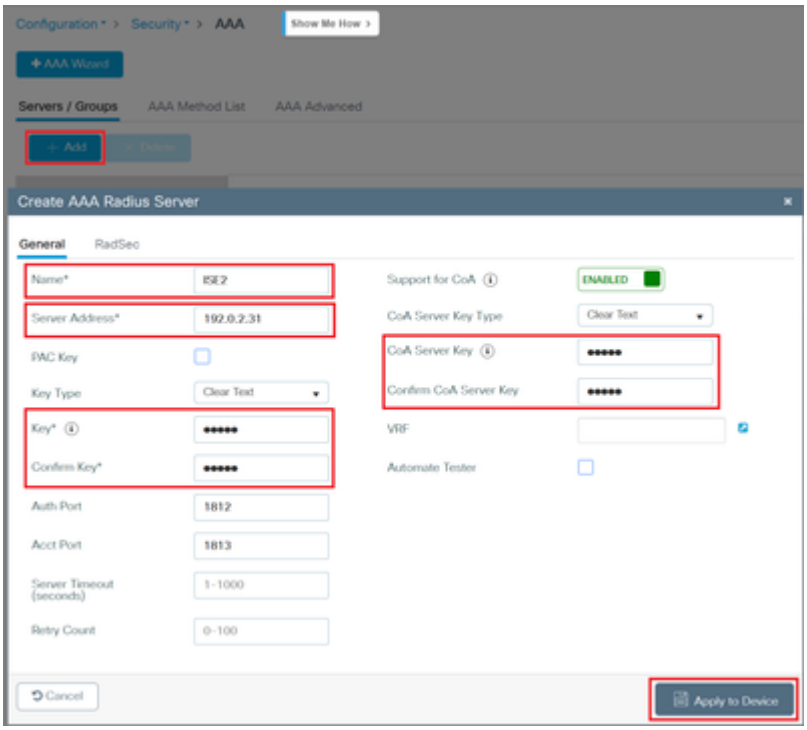
各サイトにAAAサーバを作成します。1つは中央サイトに、もう1つはリモートサイトに作成します。

Configuration > Security > AAA > Server/Groups > Serversの順に移動し、+Addを選択します。サーバに名前、IPアドレス、キー（および確認キー）を指定し、CoA（認可変更）サポートを有効にし、CoAサーバキー（および確認CoAサーバキー）を入力します。 キーは同じにする必要があります。



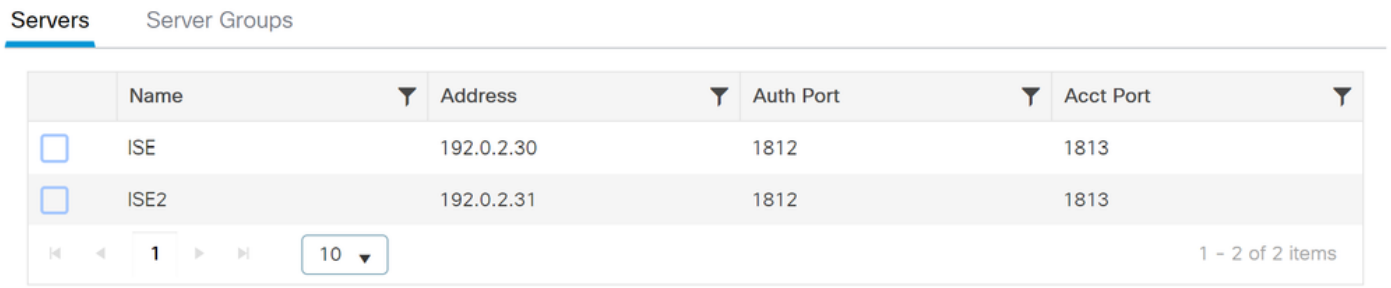
Apply to Deviceをクリックします。

ステップ 2：もう1つのAAAサーバを作成します。

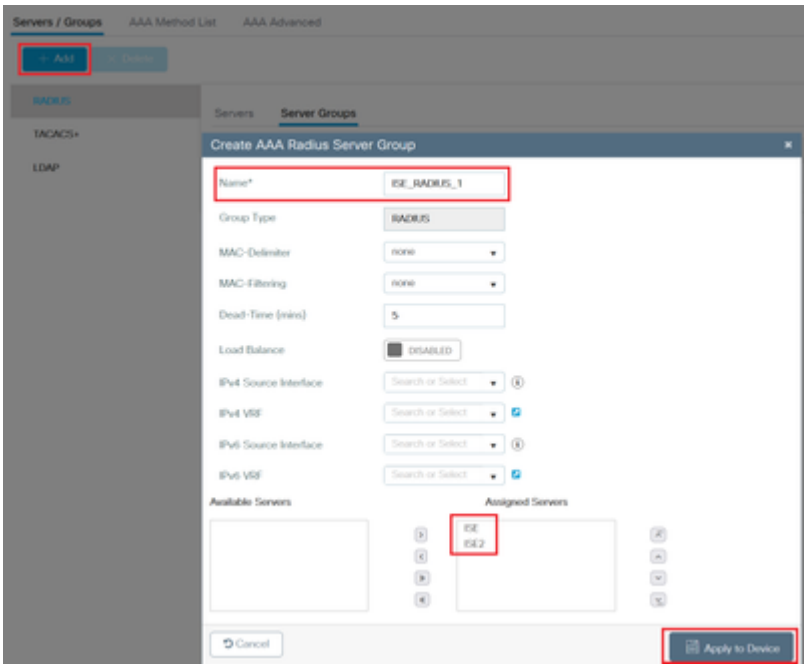


Apply to Deviceをクリックします。

次のように、AAAサーバが設定されていることがわかります。

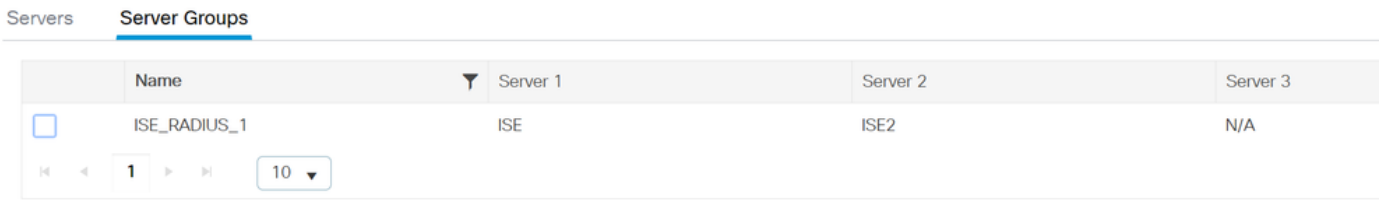


ステップ 3：Configuration > Security > AAA > Server/Groups > Server Groupsの順に移動し、+Addを選択します。 グループサーバに名前を付け、前に作成したAAAサーバをAssigned Serversカラムで選択します。



Apply to Deviceをクリックします。

次のように、AAAサーバグループが設定されていることがわかります。



CLI：

```
aaa new-model
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

リモートサイトでのFlexConnectモードの設定

ステップ 1：最初の手順では、リモートサイトでFlexConnectを設定します。

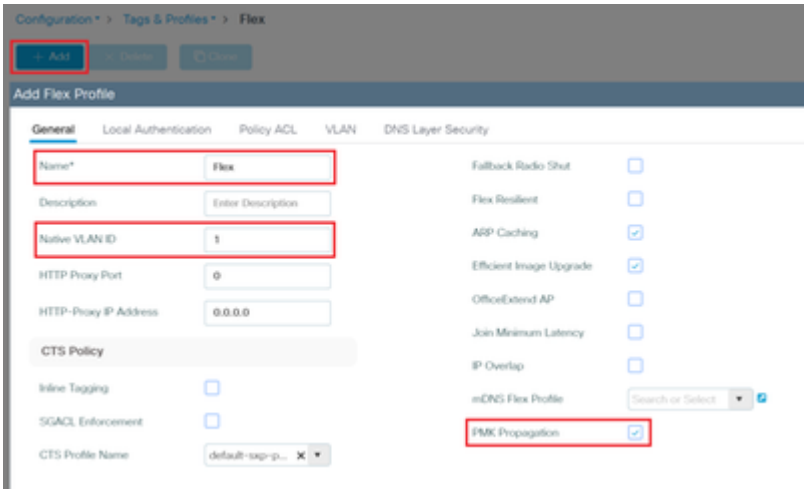
このガイドを使用してAPモードをFlexに変更する方法：Catalyst 9800ワイヤレスコントローラのFlexConnectについて

このガイドまたはラボのAPでは、同じFlex Profileを使用します。

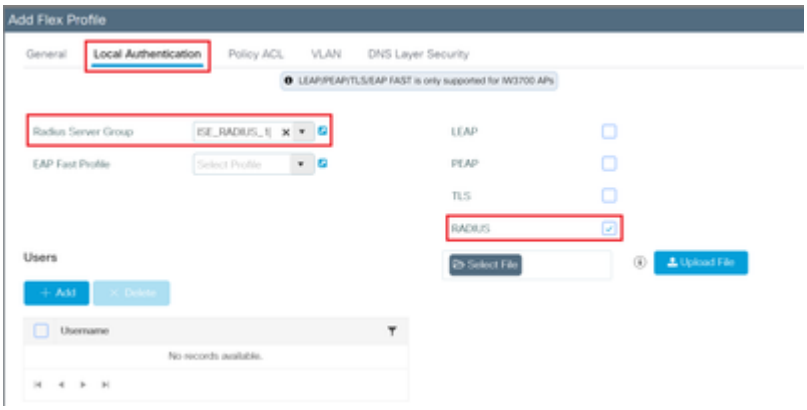
ステップ 2：Configuration > Tags & Profiles > Flexの順に移動します。

+Addを使用して新しいフレックスプロファイル名を作成します。Generalタブで、プロファイルに名前を付け、ネイティブVLAN（仮想ローカルエリアネットワーク）IDを入力し、PMK伝播を有効にします。

単一サイト内のAP間でPMK情報を共有することにより、PMK伝達を有効にして、シームレスなワイヤレスクライアントローミングを促進します。

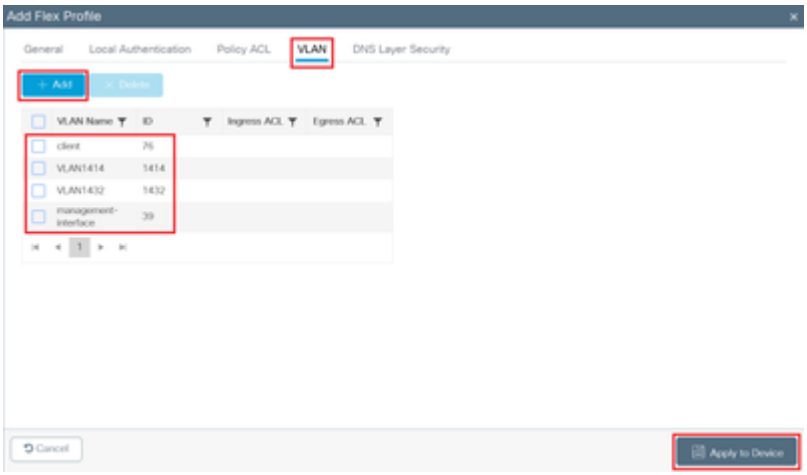


ステップ 3：802.1x WLANの場合、Local Authenticationタブで、RADIUSサーバグループを選択して、RADIUSをイネーブルにします。



ヒント:PSK WLANの場合は、このタブで何も追加する必要はありません。

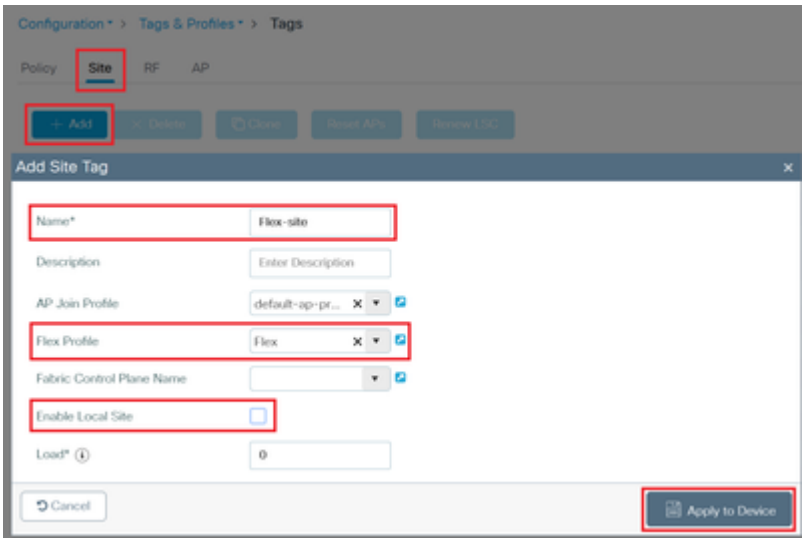
ステップ 4：VLANタブで、クライアント、AP、およびRADIUSサーバで使用されるすべてのVLANを追加します。各VLAN名が正しいVLAN IDに正しく対応していることを確認してください。



最後にUpdate & Apply to Deviceをクリックします。

ステップ 5：Configuration > Tags & Profiles > Tags > Siteの順に移動し、+Addを選択します。

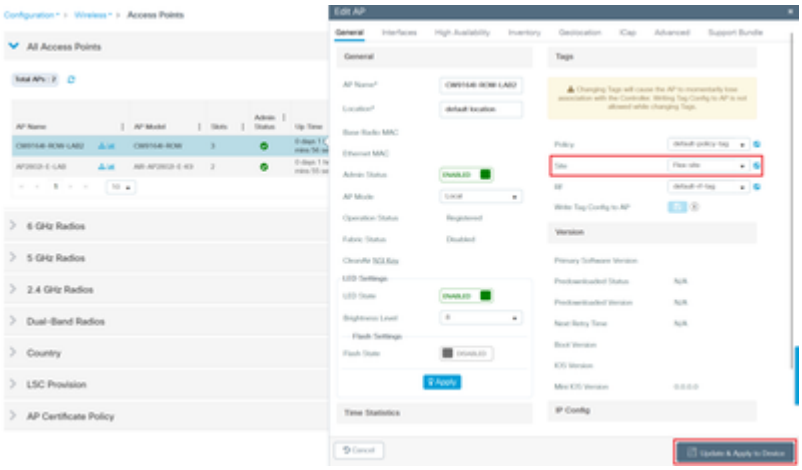
前に作成したFlex Profileを使用してサイトタグを作成します。名前を付け、適切なFlex Profileを選択して、Enable Local Siteを無効にします。AP加入プロファイルが正しいことを確認します。



Apply to Deviceをクリックします。

手順 6：Configuration > Wireless > Access Pointsの順に移動します。

APを選択して、General > Tagsの順に選択し、Site Tagを以前に設定したタグに変更します。



Update & Apply to Deviceをクリックします。

APはWLCから切断され、Flex APモードで再加入します。

同じページで、APが再結合するときに、「AP Mode」列のAPモードを確認できます。

APを選択すると、新しいサイトタグが表示されます。



CLI：

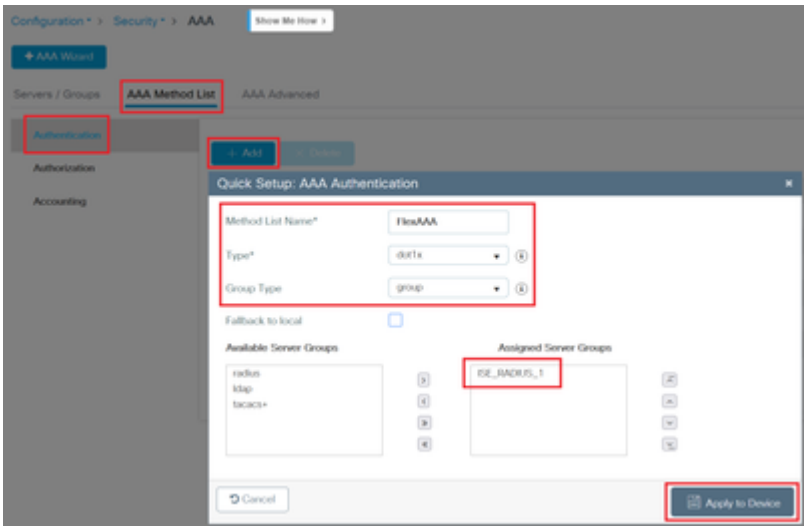
```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

外部RADIUSサーバを使用したローカル認証による802.1x WLANの設定

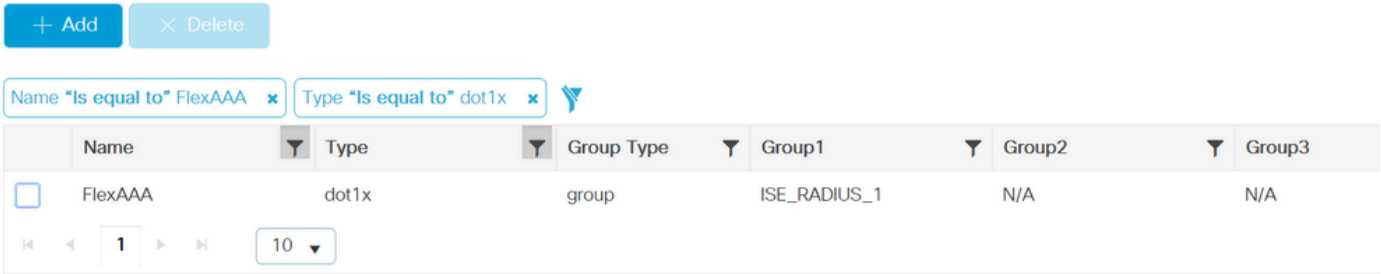
ステップ 1：認証方式リストを作成します。

AAA Method List > Authenticationタブで、Configuration > Security > AAAの順に選択します。

+Addを選択し、方式リストの名前を指定し、タイプとしてdot1xを選択し、グループタイプとしてgroupを選択し、Assigned Server Groups列でAAAサーバグループを割り当てます。



作成されたAAA方式リストが表示されます。



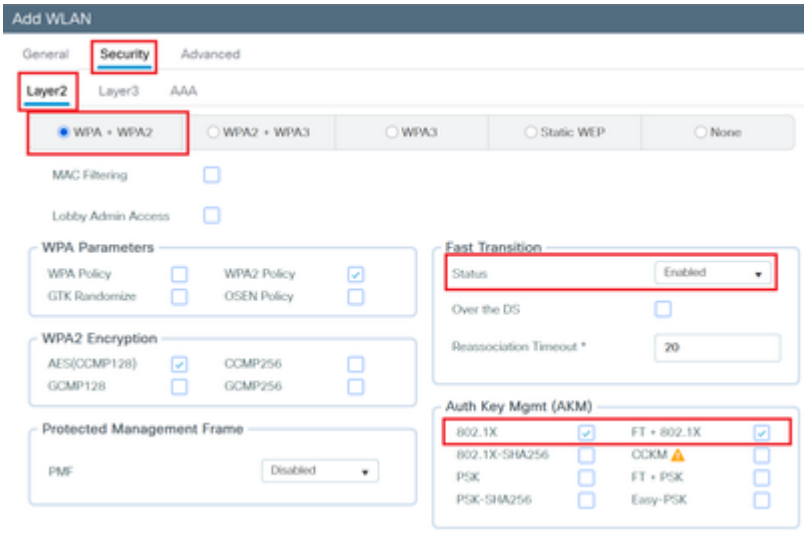
ステップ 2：WLAN を作成します。

Configuration > Tags & Profiles > WLANsの順に移動し、+Addを選択します。

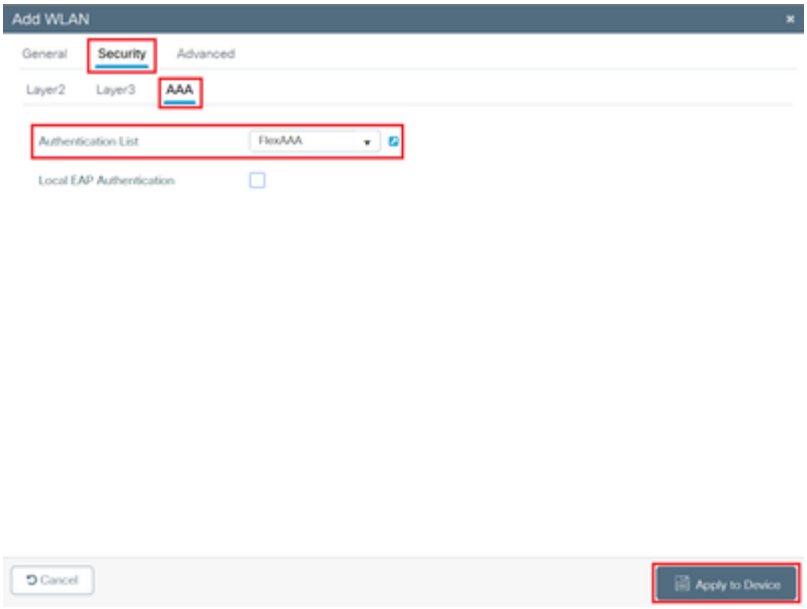
Generalタグで、プロファイル名、SSID、およびイネーブルステータスの名前を作成します。



ステップ 3：Security > Layer 2タブに移動し、WPA+WPA2 (Wi-Fi Protected Access)、Fast Transition as Enabled、Auth Key Mgmt 802.1X and FT+802.1Xの順に選択します。



ステップ 4：Security > AAAタブに移動し、Authentication Listドロップダウンメニューで、前に作成したリストを選択します。



Update & Apply to Deviceをクリックします。

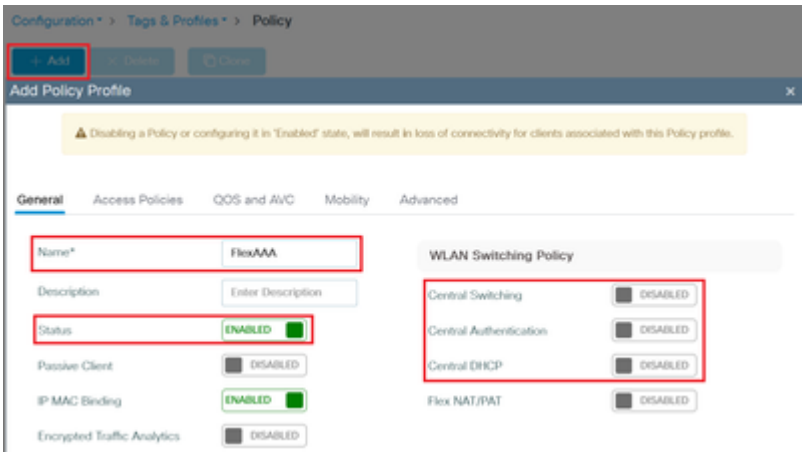
作成されたWLANが表示されます。



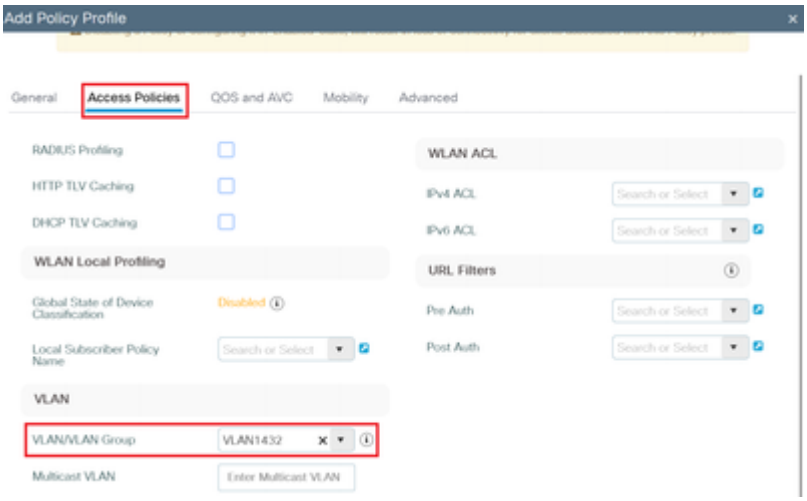
ステップ 5：ポリシープロファイルを作成します。

[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [ポリシー（Policy）] に移動します。

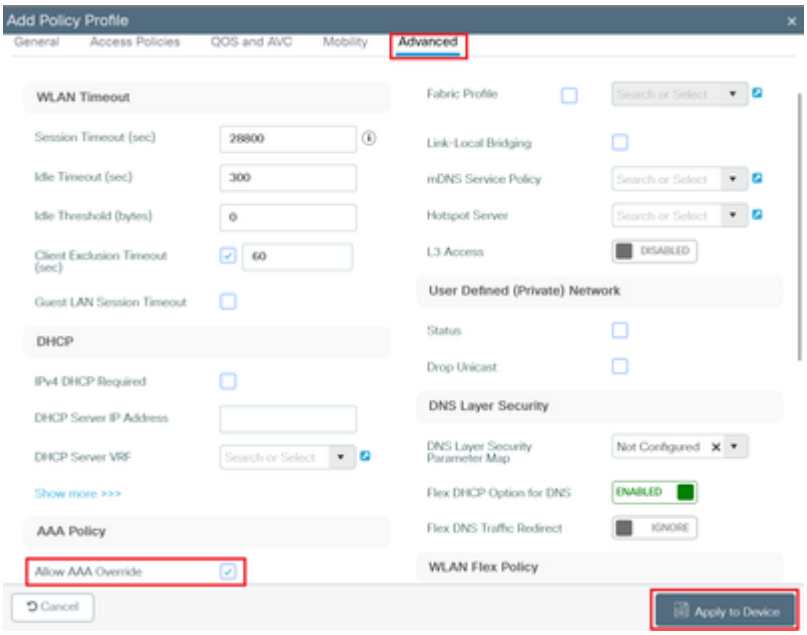
+Addを選択し、Generalタブで、ポリシープロファイルに名前を付け、ステータスを有効にし、中央スイッチング、中央認証、および中央DHCP(Dynamic Host Configuration Protocol)を無効にします。



手順 6：Access Policiesタブに移動し、VLANを選択します。

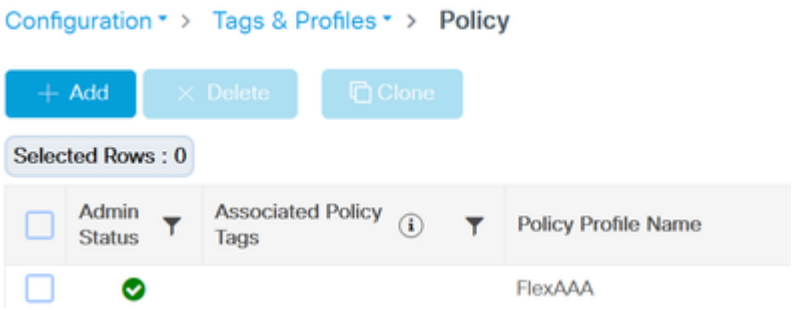


手順 7：Advancedタブに移動し、Allow AAA Overrideをイネーブルにします。



Update & Apply to Deviceをクリックします。

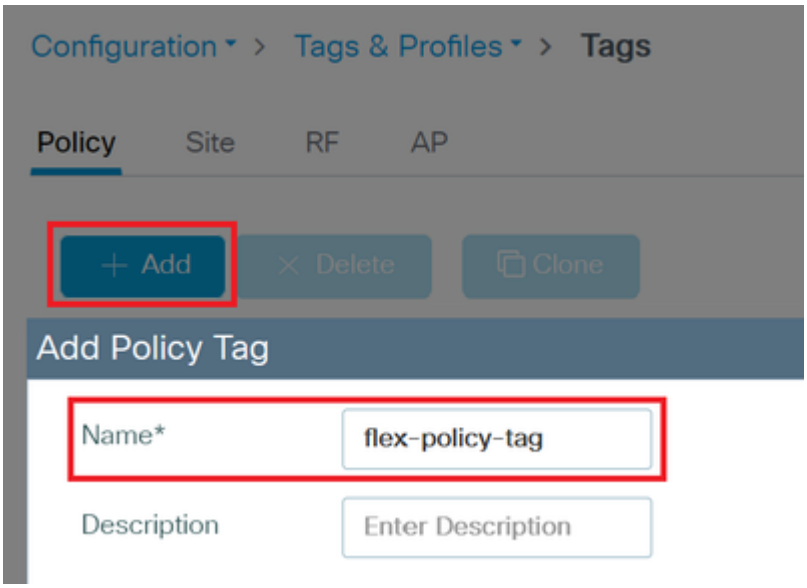
ポリシープロファイルがリストに表示されます。



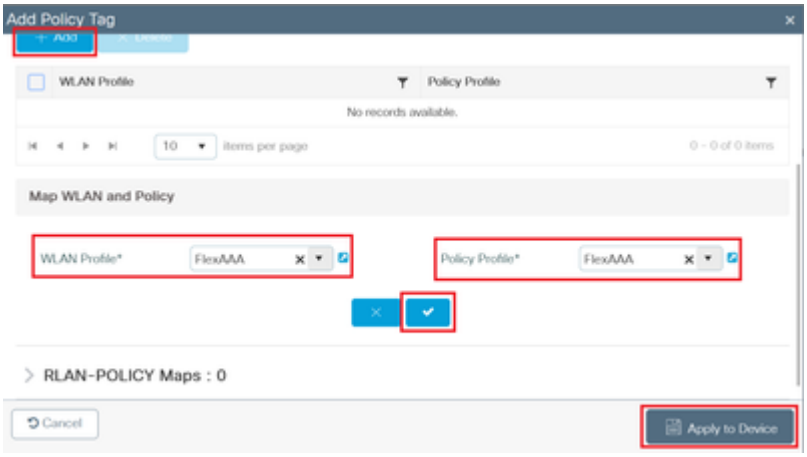
ステップ 8：ポリシータグを作成します。

Configuration > Tags & Profiles > Tagsの順に移動します。

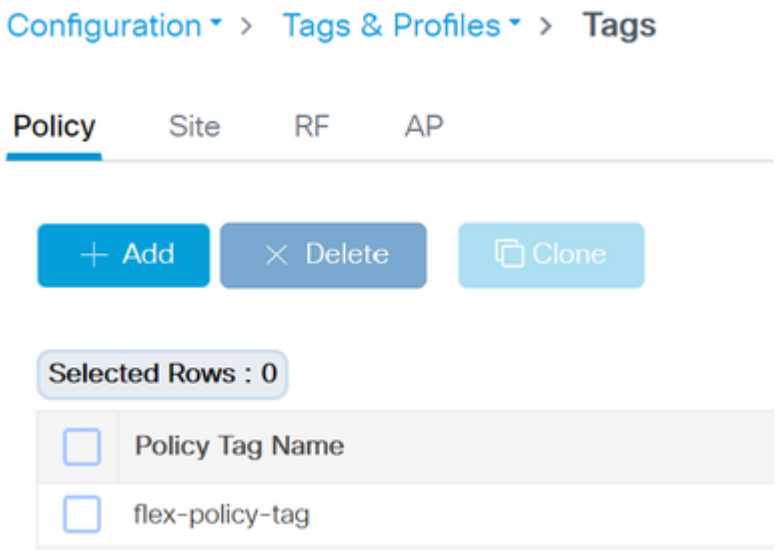
Policyタブで、+Addを選択します。Policy Tagに名前を付けます。



下にスクロールして、WLAN-POLICY Mapsの下で+Addを選択します。WLAN Profileで、ドロップダウンメニューから前に作成したWLANを選択します。Policy Profileで、前に作成したPolicy Profileをドロップダウンメニューから選択します。チェックボタンをクリックし、次にApply to Deviceをクリックします。

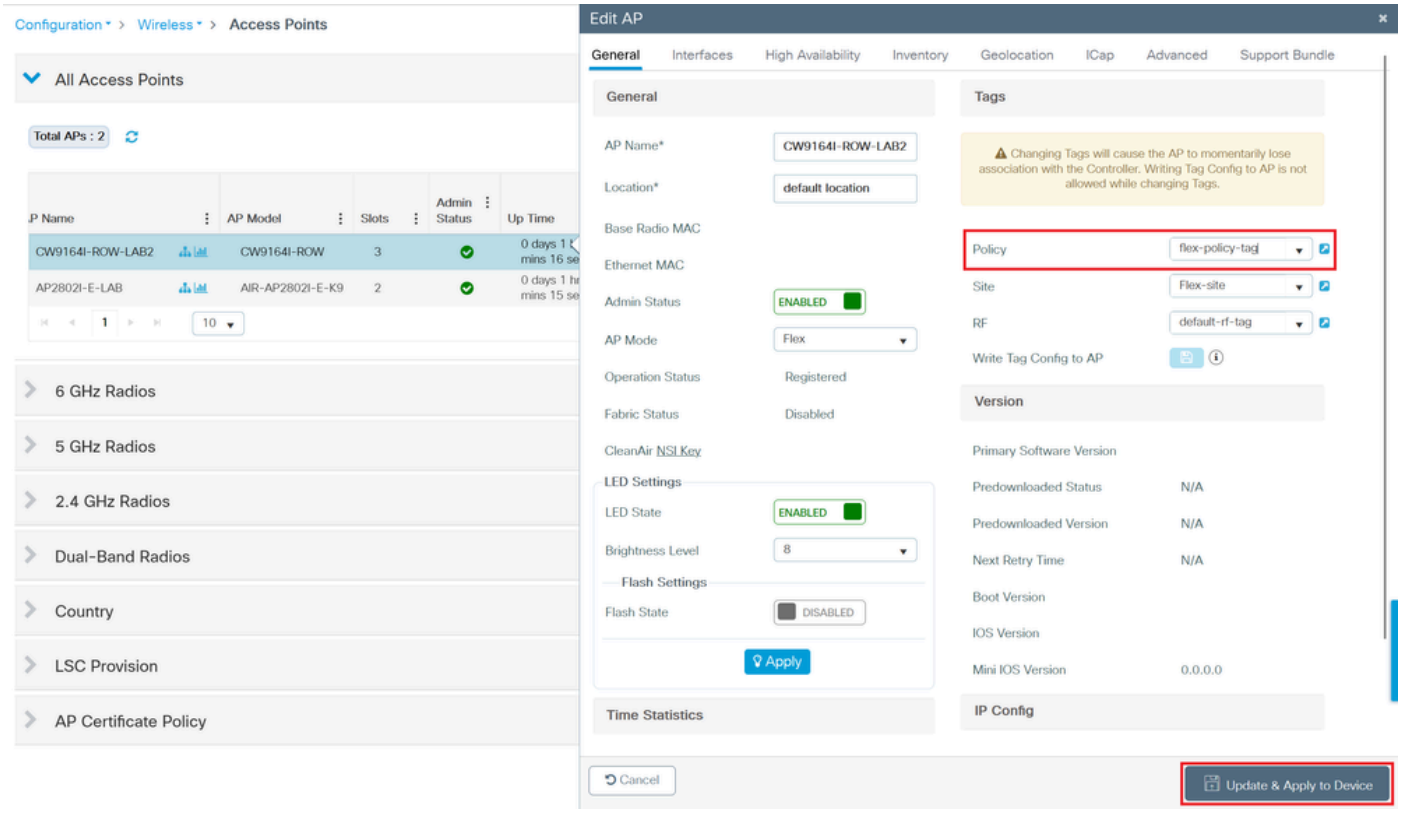


ポリシータグがリストに表示されます。



ステップ 9：APタグにポリシータグを割り当てます。

Configuration > Wireless > Access Pointsの順に移動します。タグを変更するAPを選択します。

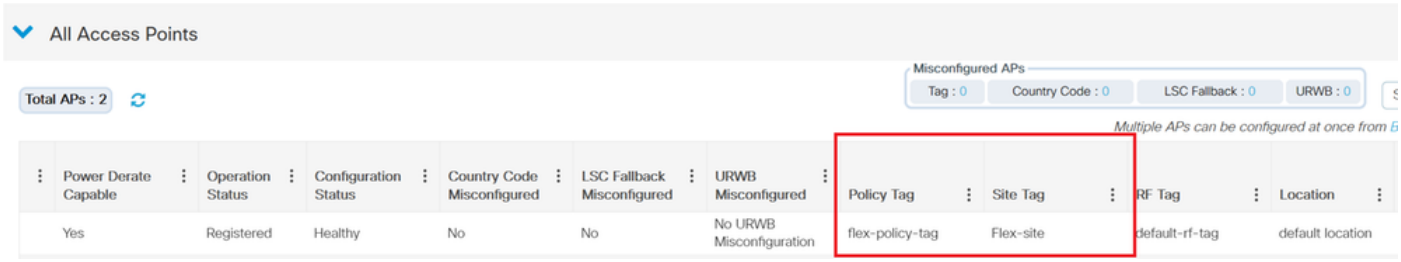


Update & Apply to Deviceをクリックします。

APは新しいポリシータグで分離され、再結合されます。

APが加入したら、アクセスポイントのリストを確認し、APがFlexモードであることを確認して、

タグを割り当てることができます。



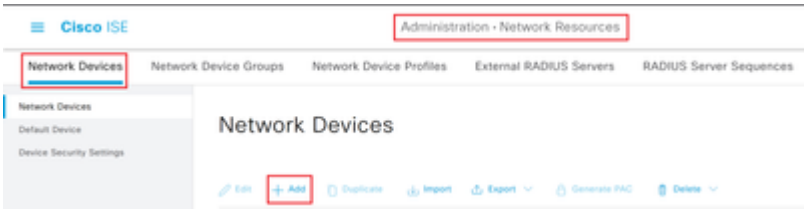
CLI：

```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

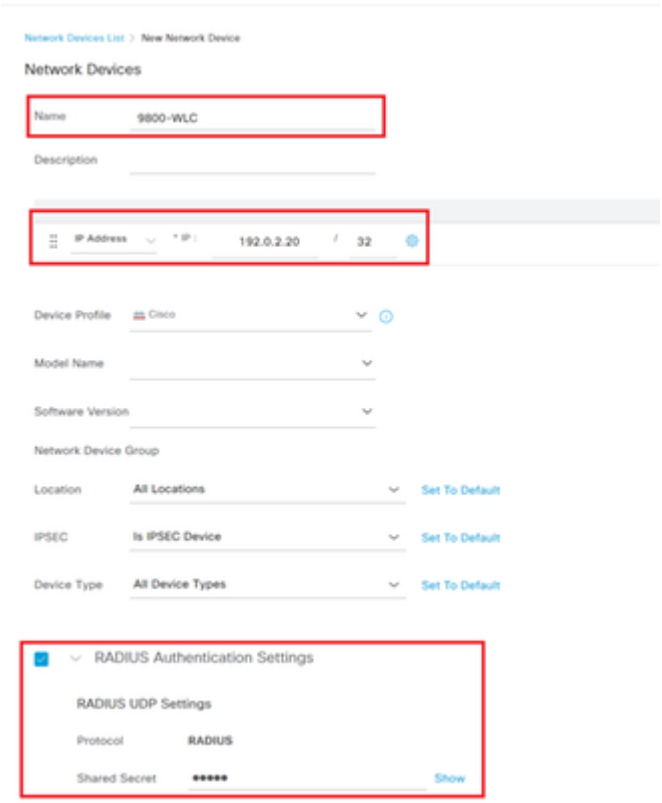
ISE の設定

次に、クライアントがローカル認証中に認証できるようにISEを設定する必要があります。

ステップ1:Administration > Network Resources > Network Devicesの順に移動します。+Addを選択します。



ステップ 2：9800 WLCを追加します。名前を指定し、そのIPアドレスを追加して、RADIUS認証設定を有効にし、共有秘密キーを追加します。このキーは、9800 WLCでAAAサーバを作成したときに設定したものと同じキーである必要があります。



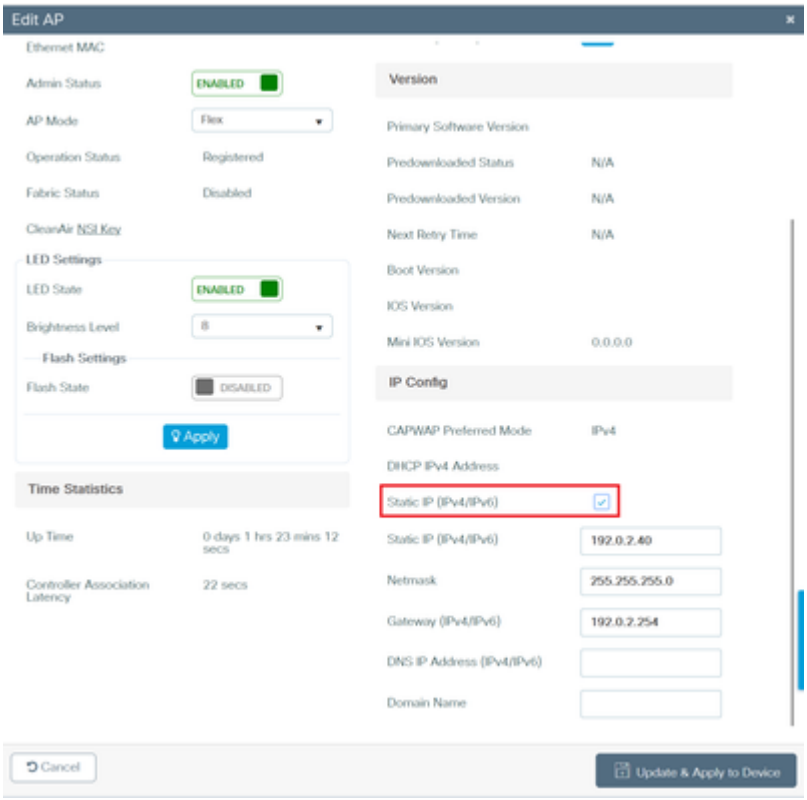
右下のSaveをクリックします。

ステップ 3：リモートサイトでWANリンクが失われた場合（およびAPがスタンドアロンモードに移行した場合）にAAAオーセンティケータ/フォワーダとして機能できるように、APをNetwork Devicesリストに追加する必要があります。

9800 WLC GUIでConfiguration > Wireless > Access Pointsの順に移動し、各APのIPアドレスをメモします。

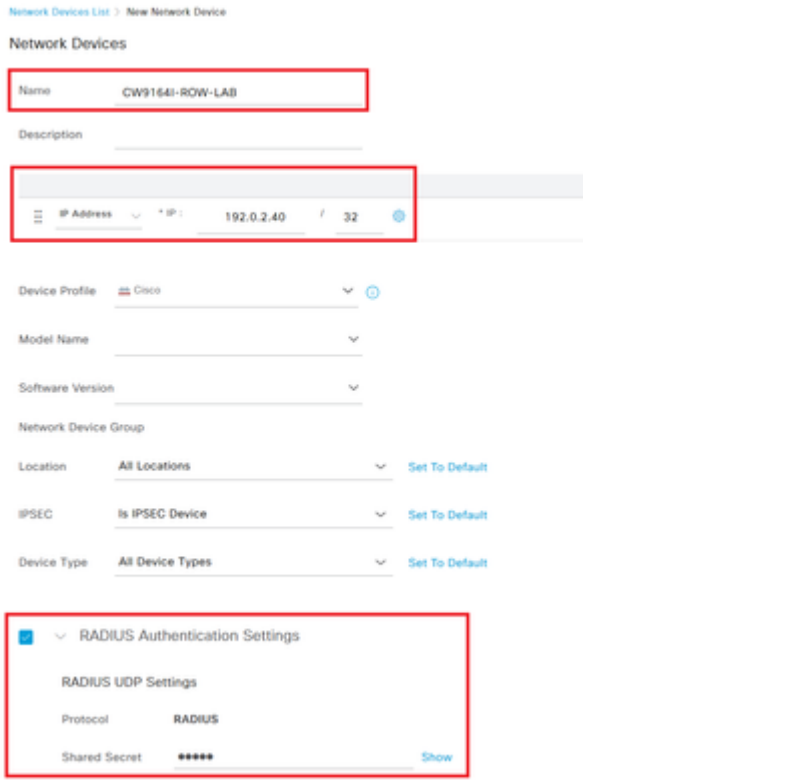
注：各Flex APのIPアドレスをスタティックに設定します。APが切断されて9800 WLCへの接続を再開すると、APはDHCPから別のIPアドレスを使用して戻ってくるため、ISEとの通信が失われる可能性があります。

スタティックIP(IPv4/IPv6)を有効にします。 Update & Apply to Deviceをクリックします。



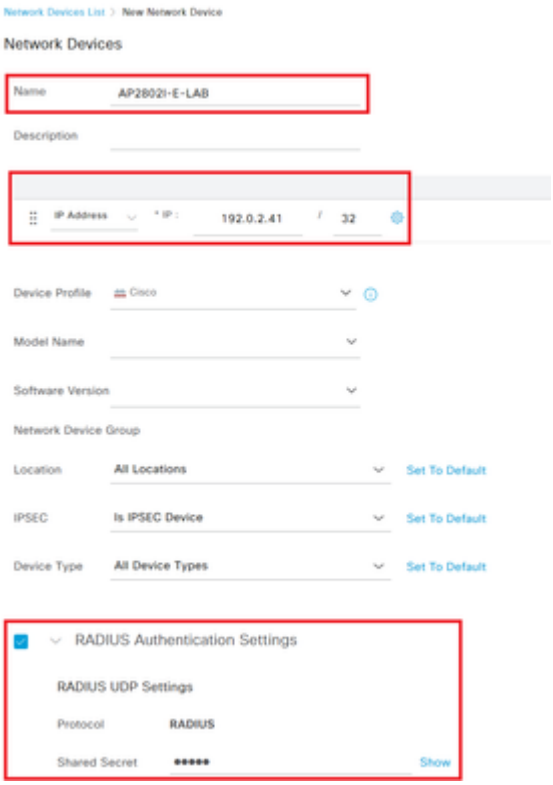
ステップ 4：ISEに戻り、Administration > Network Resources > Network Devicesの順に移動します。+Addを選択します。

9800 WLCと同じ設定で、APをネットワークデバイスとして追加します。



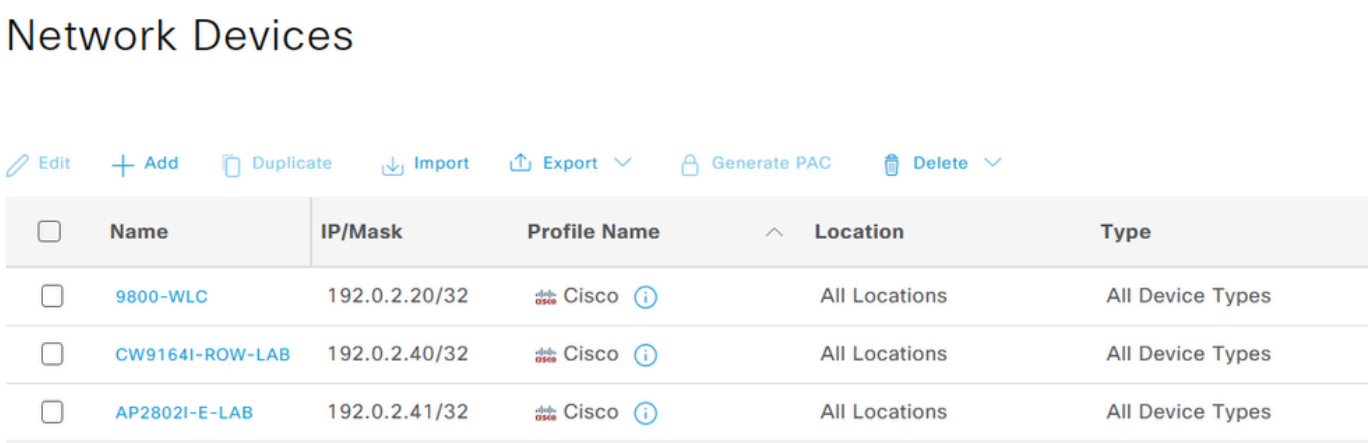
右下のSaveをクリックします。

2番目のAPの場合：



右下のSaveをクリックします。

ネットワークデバイスの次のリストが表示されます。



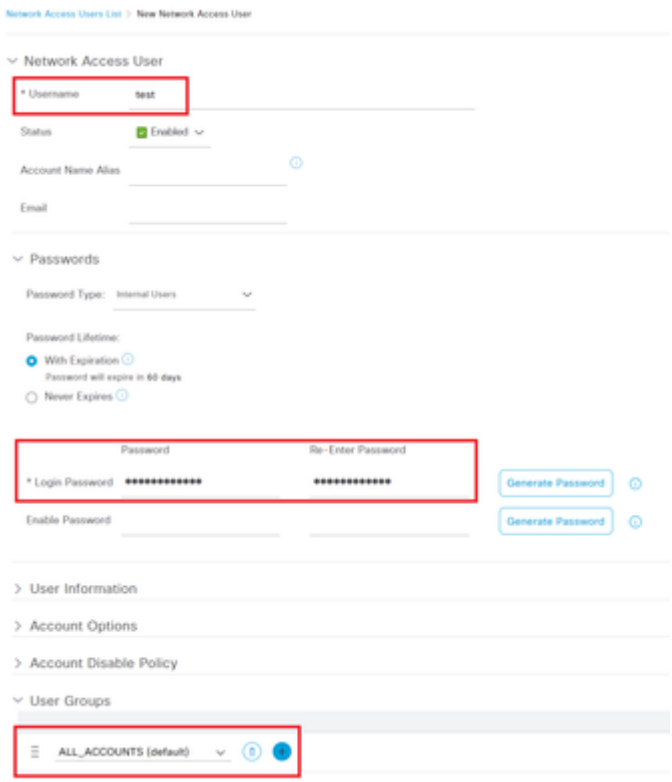
APが連続したIPの範囲内にある場合は、マスク機能を使用して、APのグループ全体（すべてではない場合）に共有秘密を定義する単一のエントリを設定できます。ISEのAPごとに1つのネット

ワークデバイスを設定する必要はありません。ただし、ワイルドカードとマスクを使用することで、不正なデバイスがISEへのフォワーダとして動作する余地が残ることに注意してください。

ステップ 5：Usersタブで、Administration > Identity Management > Identitiesの順に移動し、802.1x認証用のユーザを作成します。+Addを選択します。

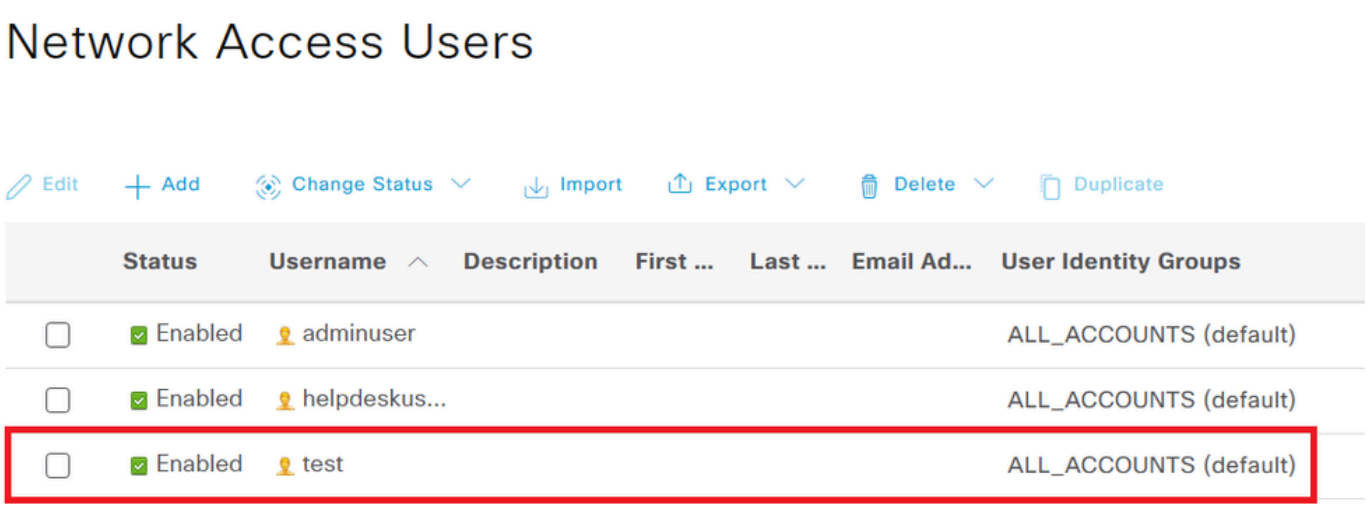


ユーザ名とパスワードを作成し（パスワードの再入力で同じパスワードを入力します）、User GroupsドロップダウンメニューからALL_ACCOUNTS（デフォルト）を選択します。

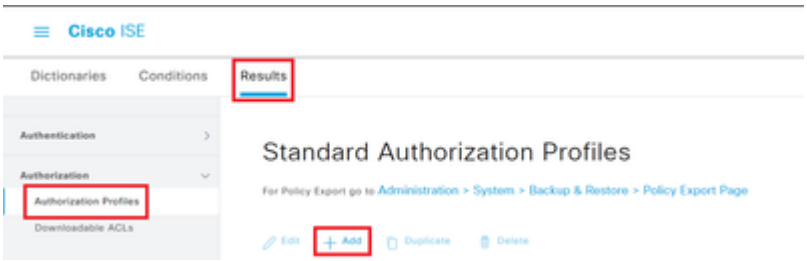


右下のSubmitをクリックします。

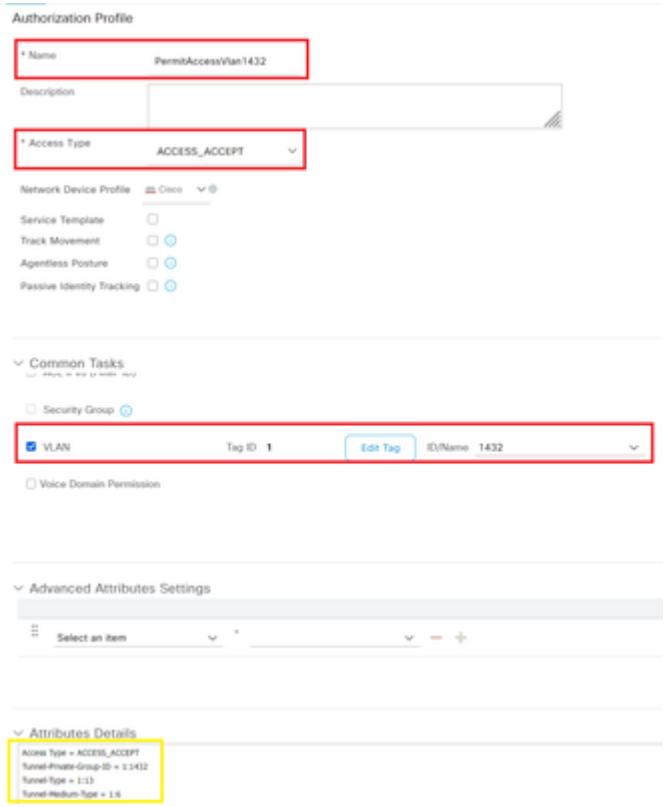
Network Access Usersリストでユーザを確認できます。



手順 6：Policy > Policy Elements > Resultsの順に移動します。Authorization > Authorization Profilesタブで、+Addを選択します。



ローカル認証クライアントが割り当てられているVLANの認可プロファイルを作成します。

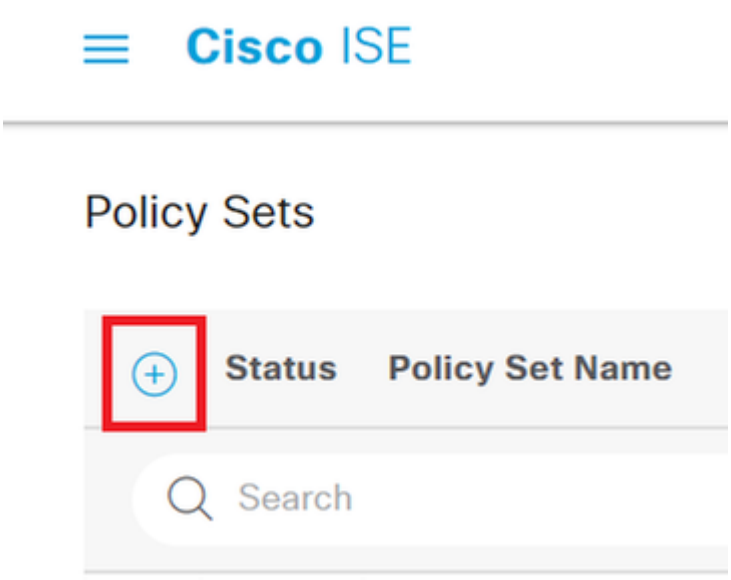


右下のSubmitをクリックします。

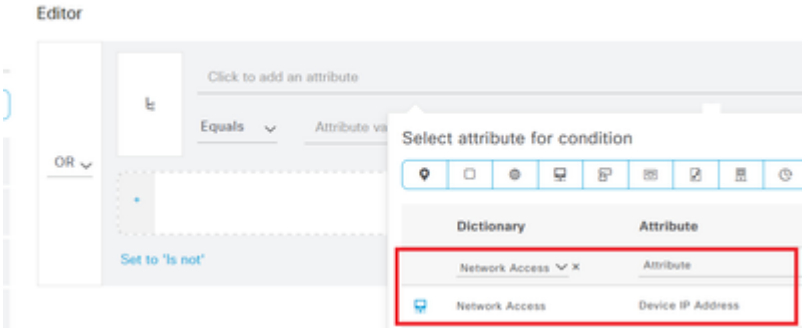
正常なシナリオでISEがWLC/APに送信する属性の詳細が表示されます。

手順 7：Policy > Policy Setsの順に移動します。新しいポリシーセットを作成します。

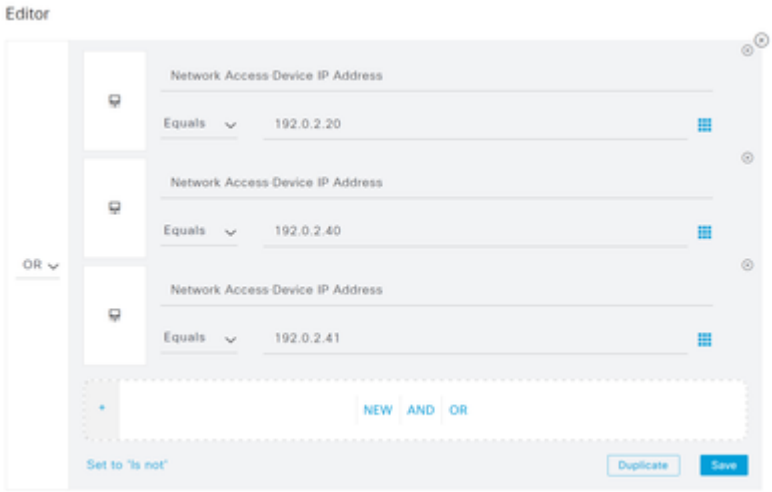
+記号をクリックします。



ポリシーセットに名前を付けます。Conditions列で、ORルールを追加し、Network Accessディクショナリを追加します。次に、Attribute Device IP AddressとともにEqualsを選択します。

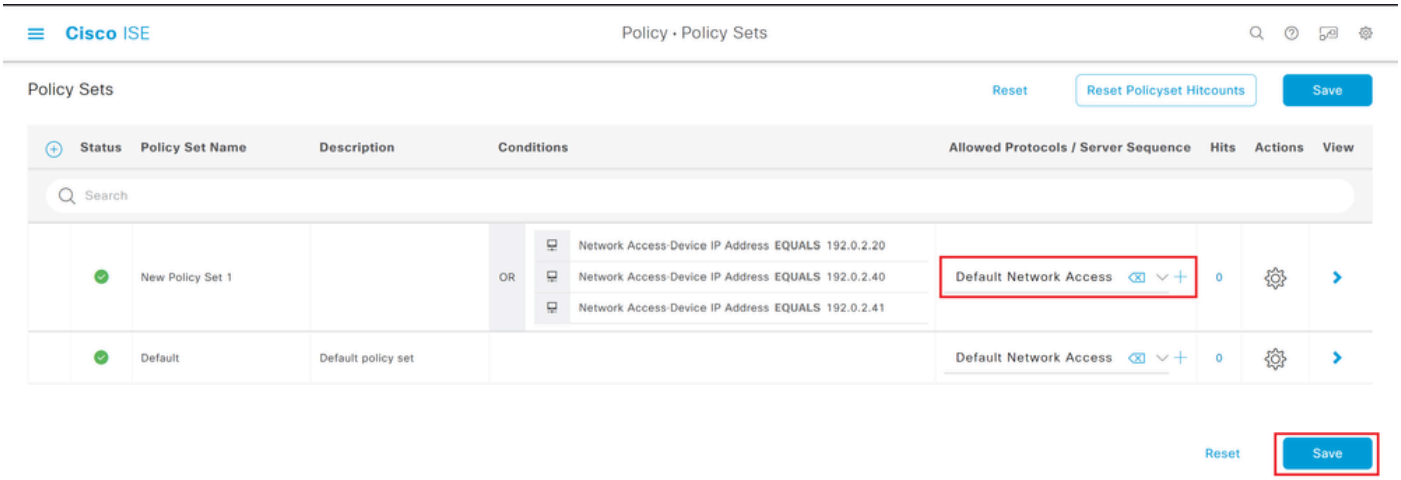


9800 WLCとAPのIPアドレスを追加します。

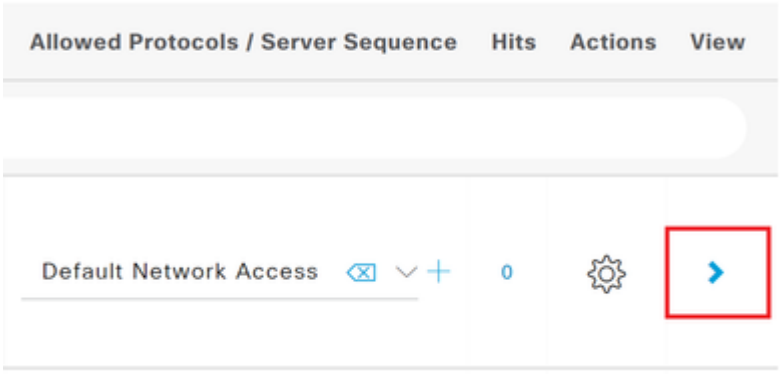


右下のUseをクリックします。

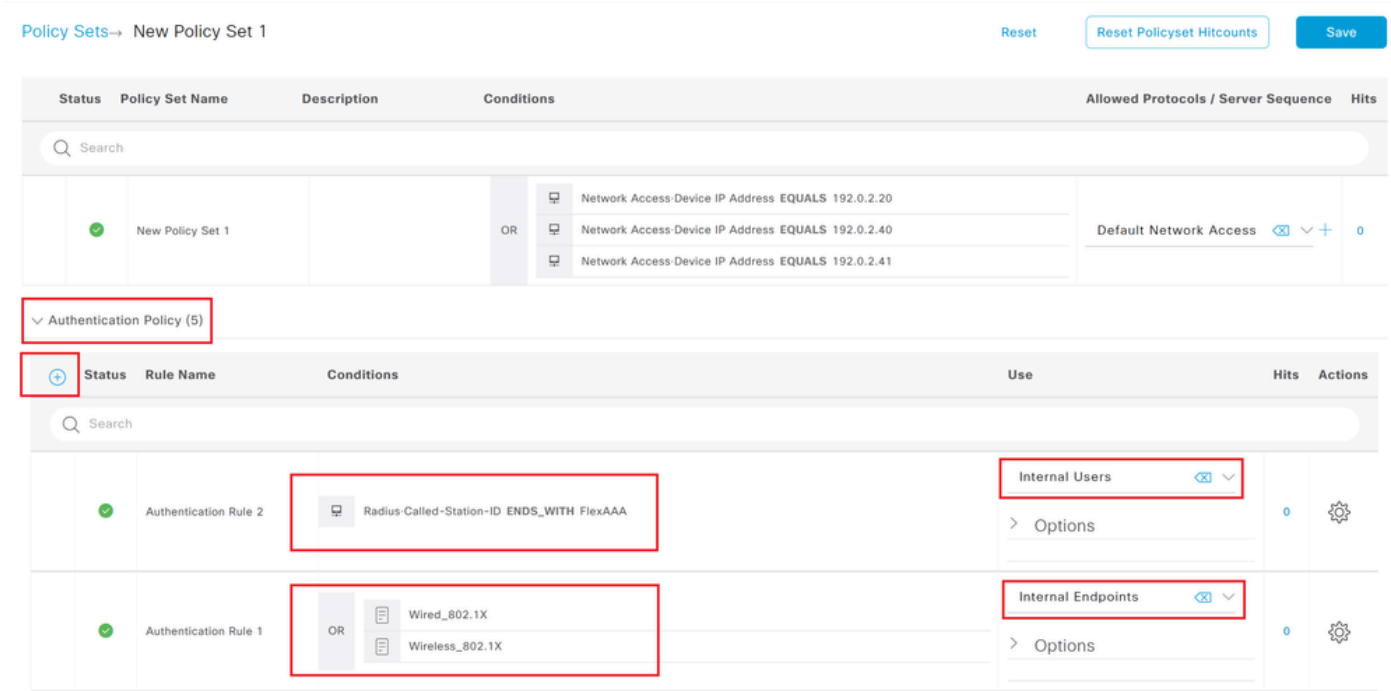
ステップ 8：Allowed Protocols列で、Default Network Accessを選択します。最後にSaveをクリックします。



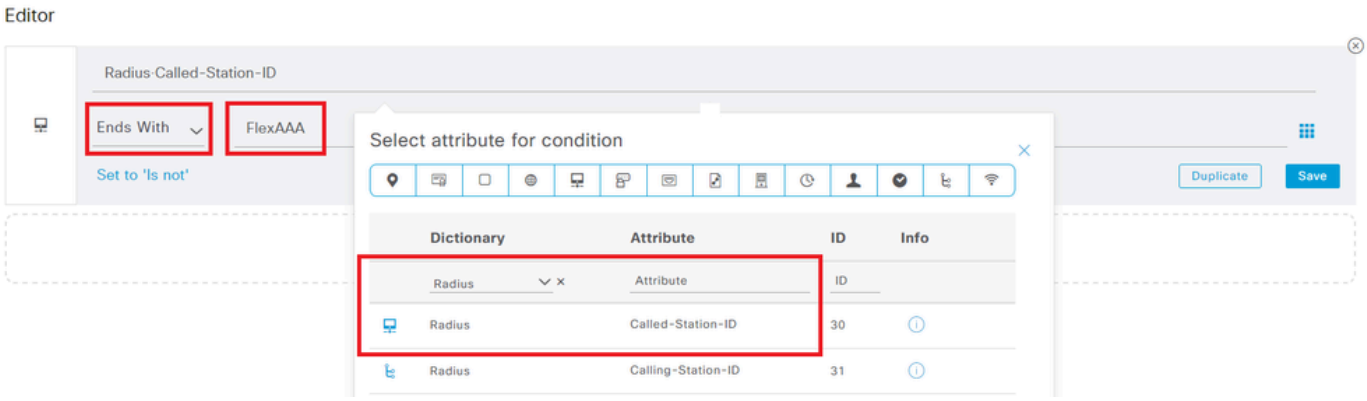
ステップ 9：列Viewで、矢印記号(



ステップ 10：Authentication Policyを展開し、WLAN名と802.1X設定の2つの新しいポリシーを作成します。

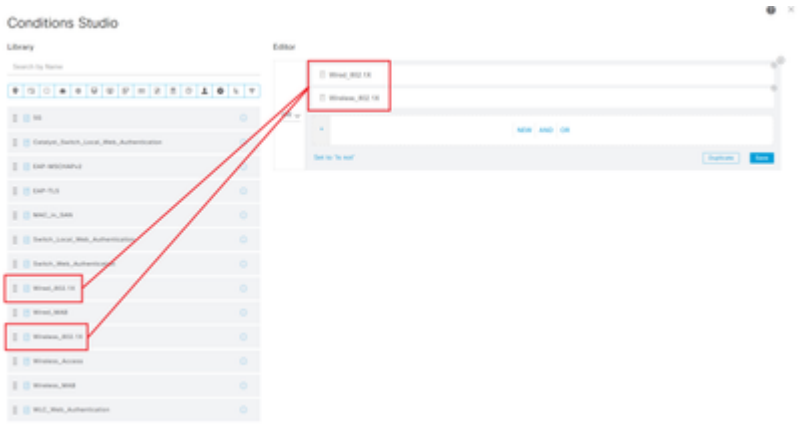


WLAN名の場合、Radiusというディクショナリと Called-Station-IDという属性を持つConditionを作成します。Ends Withを選択し、WLAN名を入力します。



右下のUseをクリックします。このポリシーの場合、Use列でInternal Usersを選択します。

ステップ 11：802.1Xポリシーの場合、ISEで使用可能なWired_802.1XおよびWireless_802.1Xライブラリを使用してConditionを作成します。これらの項目をドラッグアンドドロップして、条件を選択するか、または次の操作を行うことができます。



右下のUseをクリックします。このポリシーの場合、Use列でInternal Endpointsを選択します。

ステップ 12：Authorization Policyまでスクロールダウンして、新しいポリシーを作成します。それに名前を付け、認証ポリシーでWLAN名に作成したものと同じ条件を作成します。

Profiles列で、ドロップダウンメニューからプロファイルPermitAccessVlan1432を選択します。



右下のSaveをクリックします。

ローカル認証を使用したPSK WLANの設定

ステップ 1：最初に、「リモートサイトでのFlexConnectモードの設定」セクションの説明に従って、APをFlexモードで設定します。

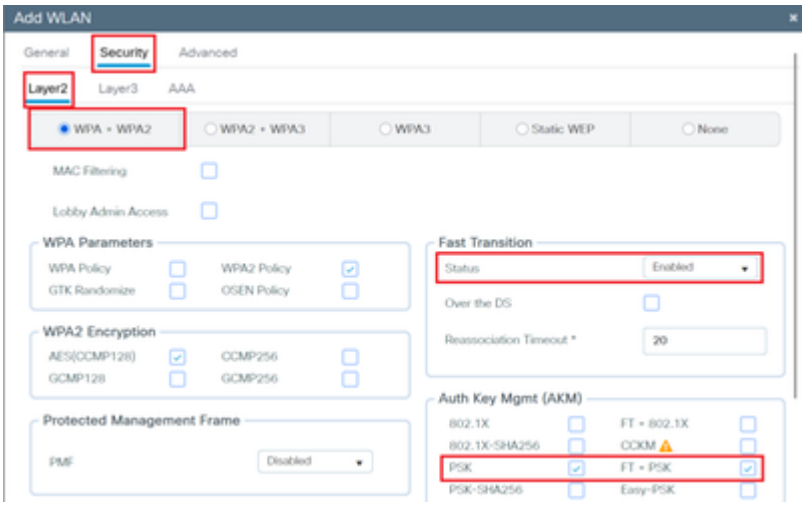
ステップ 2：WLAN を作成します。

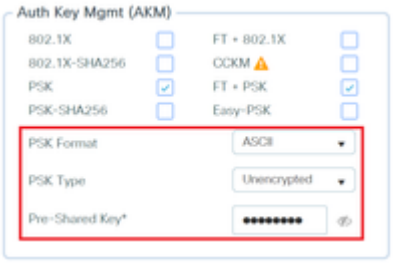
Configuration > Tags & Profiles > WLANsの順に移動し、+Addを選択します。

Generalタグで、プロファイル名、SSID、およびイネーブルステータスの名前を作成します。



ステップ 3：Security > Layer 2の順に移動し、WPA+WPA2、Fast Transition as Enabled、Auth Key Mgmt PSK and FT+PSKを選択し、必要なPSK FormatとPSK Typeを選択して、クライアントで使用する事前共有キーを入力します。





Update & Apply to Deviceをクリックします。

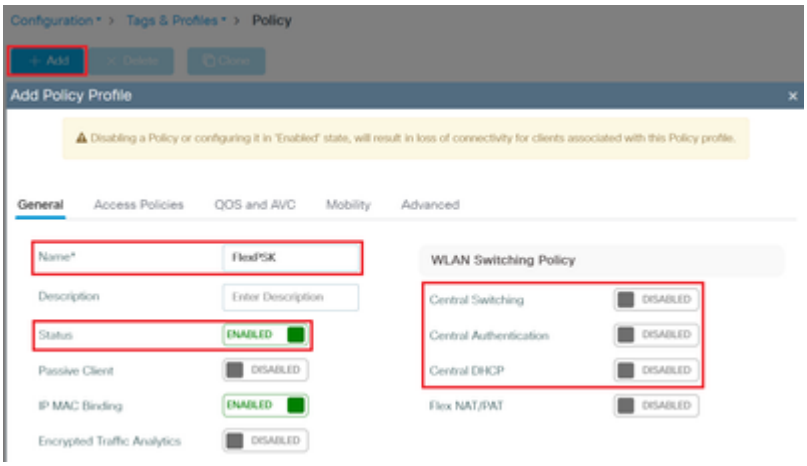
作成されたWLANが表示されます。



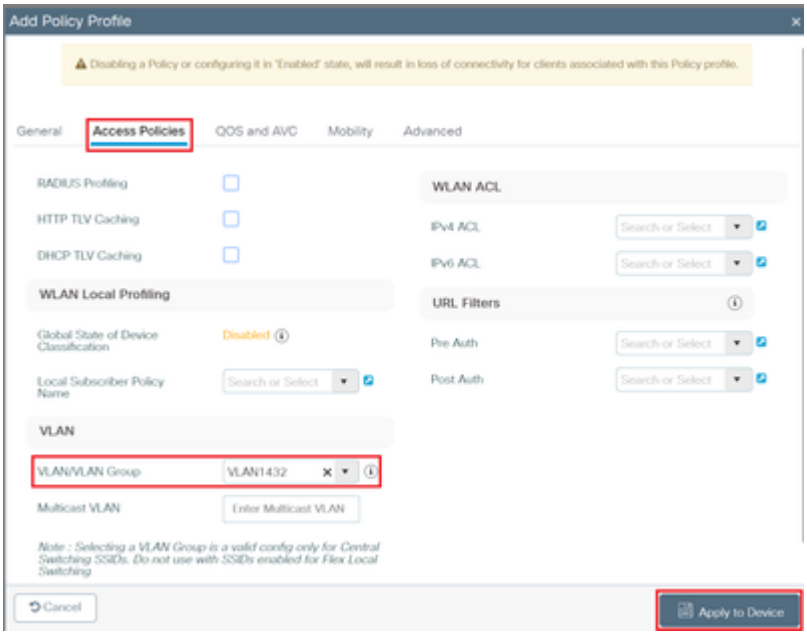
ステップ 4：ポリシープロファイルを作成します。

[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [ポリシー（Policy）] に移動します。

+Addを選択し、Generalタブで、ポリシープロファイルに名前を付け、ステータスを有効にし、中央スイッチング、中央認証、および中央DHCPを無効にします。

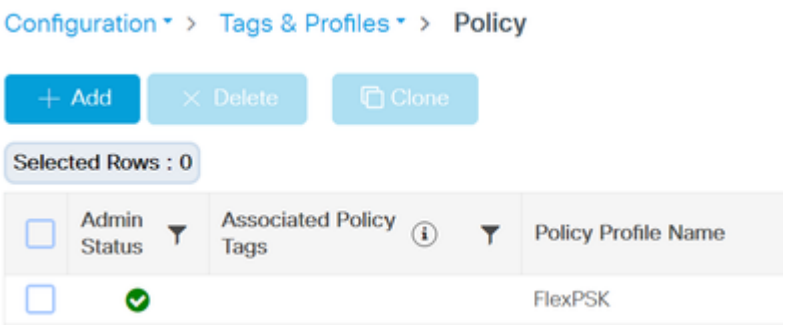


ステップ 5：Access Policiesタブに移動し、VLANを選択します。



Update & Apply to Deviceをクリックします。

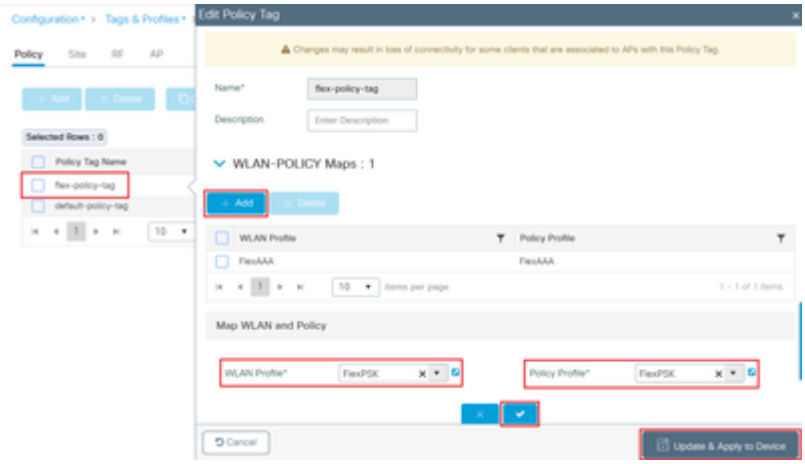
ポリシープロファイルがリストに表示されます。



手順 6：新しいPolicyタグを作成するか、既存のPolicyタグを編集できます。

Configuration > Tags & Profiles > Tagsの順に移動し、既存のポリシータグを編集します。編集するタグを選択します。

WLAN-POLICY Mapsの下で+Addを選択します。WLAN Profileで、ドロップダウンメニューから前に作成したWLANを選択します。Policy Profileで、前に作成したPolicy Profileをドロップダウンメニューから選択します。チェックボタンをクリックし、次にApply to Deviceをクリックします。



ポリシータグがすでにAPに割り当てられている場合は、他の操作は必要ありません。

そうでない場合は、APタグでポリシータグを割り当てます。 Configuration > Wireless > Access Pointsの順に選択します。ポリシータグを変更するAPを選択し、「Update & Apply to Device」をクリックします。

APは新しいポリシータグを使用して分離し、結合して戻ります。

APが加入したら、アクセスポイントのリストを確認し、APがFlexモードであり、正しいタグが割り当てられていることを確認できます。

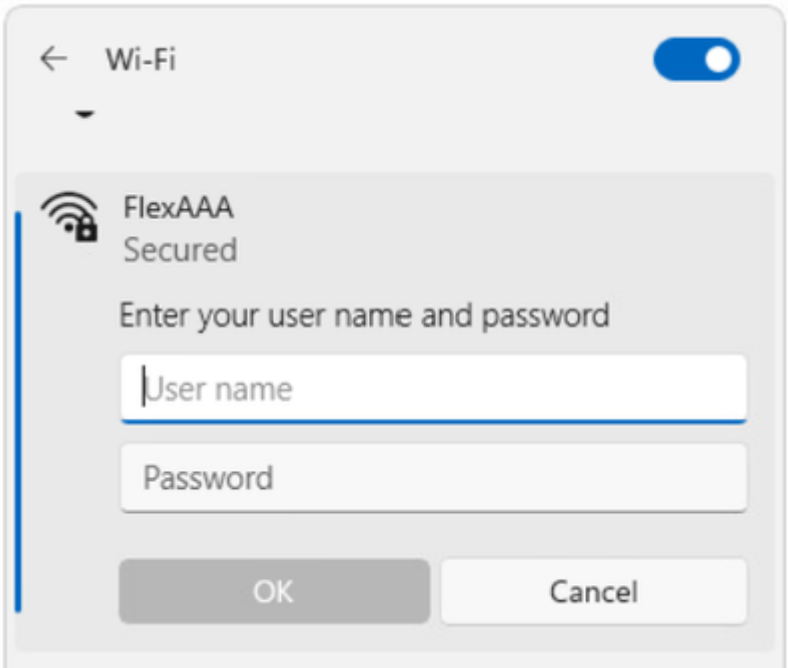
CLI：

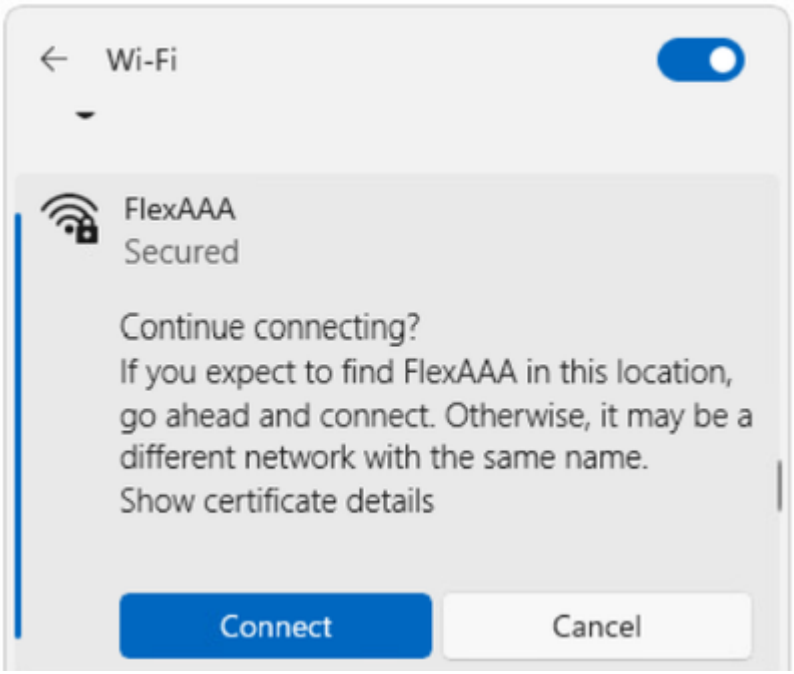
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
```

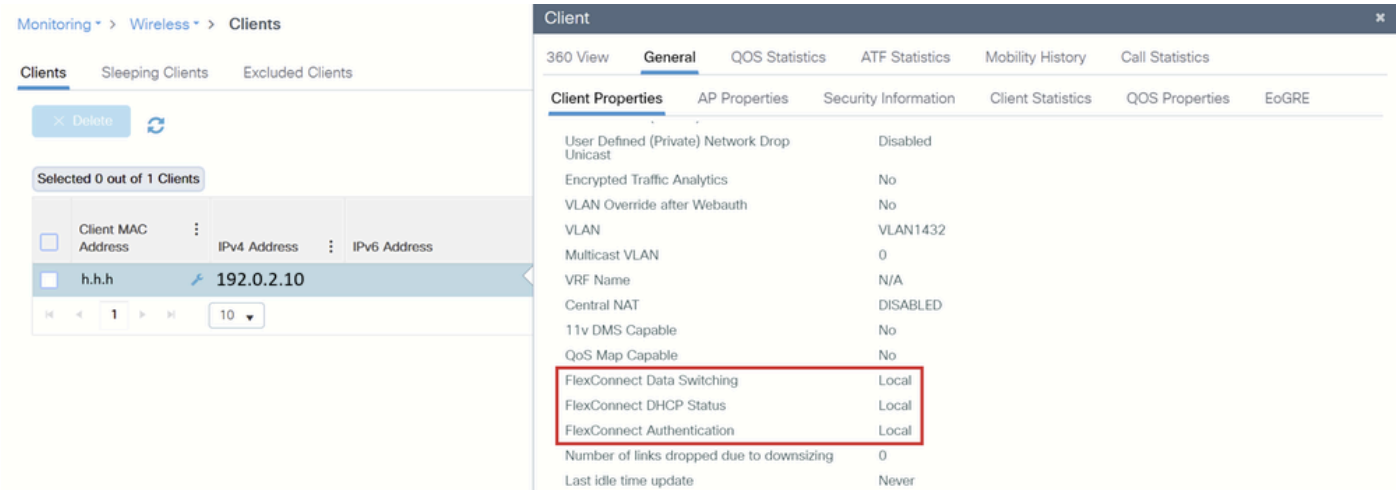
```
no shutdown
!
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

確認

802.1x WLANの場合







CLI :

```
C9800-1#show wireless client mac-address      h.h.h        detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

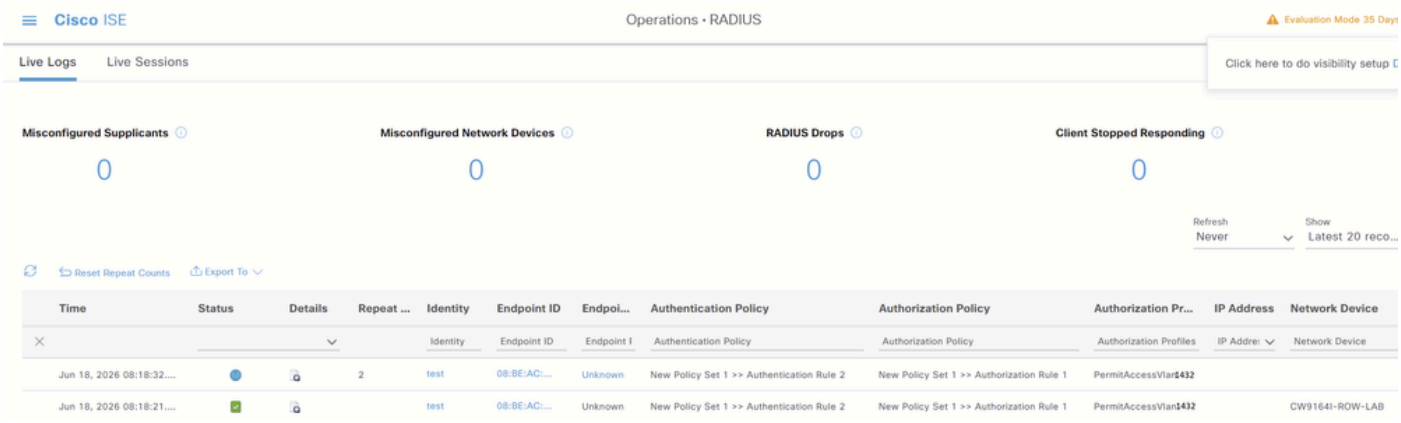
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

AP CLIで、次のコマンドを実行します。

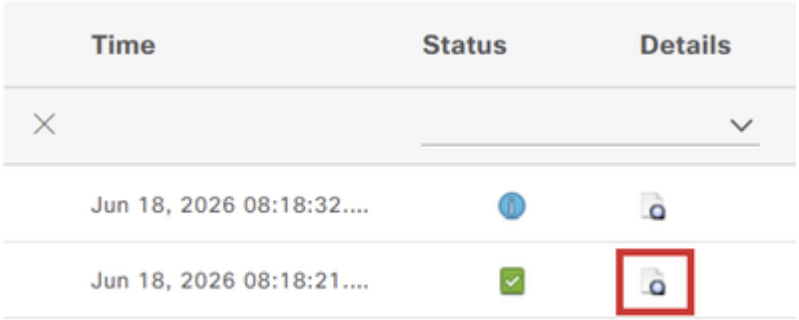
```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
MM:MM:MM:MM:MM:MM          1       1  33   FlexAAA  -45 MCS9ISS          No         No
```

ISE上



IP Address	Network Device	Device Port	Identity Group	Posture ...	Server
IP Addre:	Network Device	Device Port	Identity Group	Posture Sta	Server
		Radio:1Wlan:1			ISE1
	CW9164I-ROW-LAB	Radio:1Wlan:1	User Identity Groups:ALL_ACCOUNTS (default),Unknown		ISE1



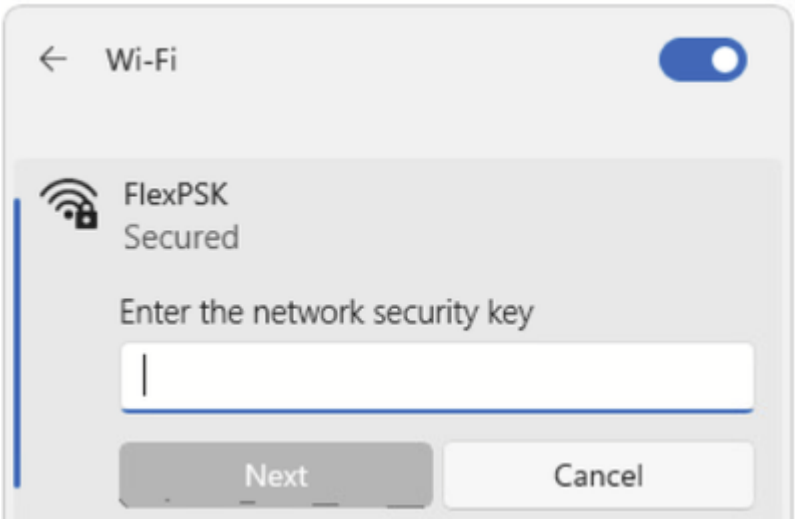
Cisco ISE

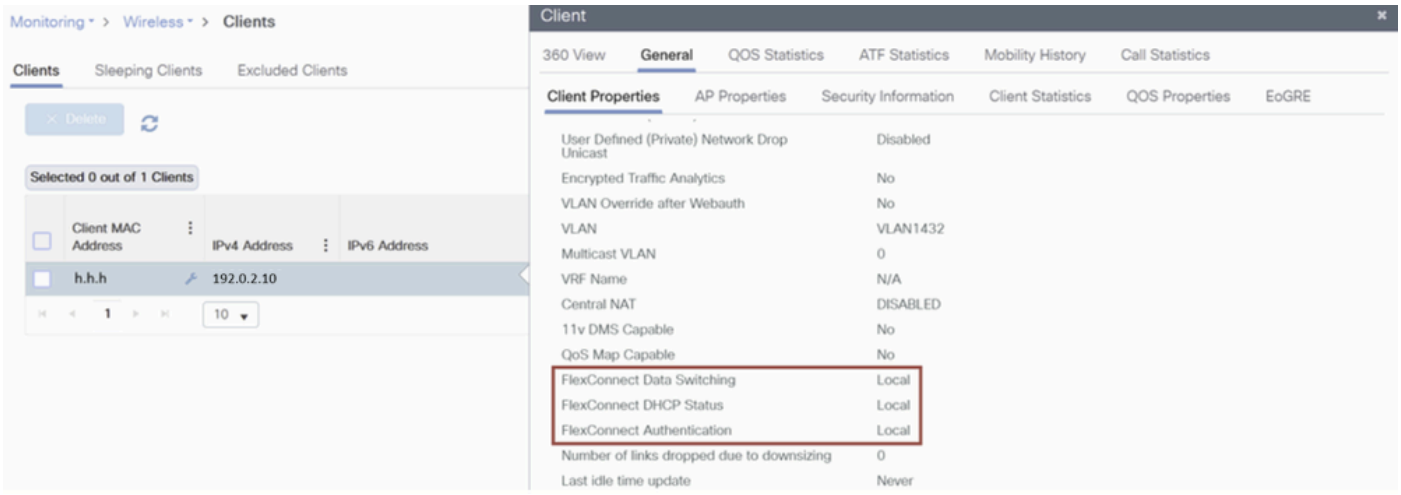
Overview

Event	5200 Authentication succeeded
Username	test
Endpoint Id	HH:HH:HH:HH:HH:HH
Endpoint Profile	Unknown
Authentication Policy	New Policy Set 1 >> Authentication Rule 2
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Authorization Result	PermitAccessVlan1432

Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	CW9164I-ROW-LAB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.0.2.40
NAS Port Id	Radio:1Wlan:1
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccessVlan1432
Response Time	64 milliseconds

PSK WLANの場合：





CLI：

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

AP CLIの場合：

```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
  xxxxxxxxxxxx          1       2  33   FlexPSK  -45 MCS9ISS           No          No
```

トラブルシューティング

同期したクライアントMACアドレスでAPデバッグおよびRAトレースを有効にします。

APで、次のデバッグをイネーブルにします。

FlexConnectイベントのデバッグ
FlexConnect PMKのデバッグ
debug flexconnect dot11r
debug dot11 client management information（クライアント管理情報のデバッグ）
debug dot11 client management critical（必須）
debug dot11 client management errors（クライアント管理エラーのデバッグ）
debug dot11 client management events（クライアント管理イベントのデバッグ）

802.1x WLANの場合

APは、認証が成功したログをデバッグします。

APは802.11ステートマシンとローカルキー管理を処理します。
APはアソシエーションを処理し、クライアントの認証を準備します。

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

APは許可を処理し、VLANオーバーライドを適用して、クライアントをFWD（フォワーディング）状態に移行します。

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

同じ成功した認証のRAトレースログ：

RAトレースは、セッションのWLCのオーケストレーションをログに記録します。WLCがクライアントのIDとポリシーを検証します。
WLCがFlexConnectアソシエーションを認識します。

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

WLCがポリシーをAPにプッシュします。

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

許可の成功。

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

クライアントパラメータ。
2026/06/19 06:49:20.939394217 {wncd_x_R0-1}{1}: [dot11] [18318]: （注）: MAC: hhhh.hhhh.hhhh Client datapath entry params - ssid:FlexAAA,slot_id:1 bssid ifid: 0x0, radio_ifid: 0x90400008, wlan_ifid: 0xf0400004

WLCはローカルDHCP/ARPを介してIPを学習します。
2026/06/19 06:49:21.001000218 {wncd_x_R0-1}{1}: [client-iplearn] [18318]: （注）: MAC: hhhh.hhhh.hhhhクライアントIPラーニングが成功しました。方式：IPスヌーピングIP:192.0.2.10

クライアントは完全に接続されています。
2026/06/19 06:49:21.002363496 {wncd_x_R0-1}{1}: [errmsg] [18318]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/1: wncd：ユーザ名エントリ（テスト）が、MAC: hhhh.hhhhh.hhhh on channel (48)のデバイスのssid（FlexAAAで結合）
2026/06/19 06:49:21.002795009 {wncd_x_R0-1}{1}: [client-orch-state] [18318]: （注）: MAC: hhhh.hhhh.hhhh Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

スタンドアロンシナリオ

APとWLCの接続が失われてから回復するまでの動作。

APがWLCに加入します。クライアントは正常に802.1X認証を実行し、APはクライアントを FWD（転送）状態に移行します。

ISE RADIUSライブログに、クライアントセッションが表示されます。

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

APはWLCに到達できず、再送信カウントを使い果たし、スタンドアロンモードに切り替わります。既存のクライアントはローカルに接続されたままになります。

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

ただし、クライアントは引き続き接続されています。

CW9164I-ROW-LAB2#show dot11 clients

dot11クライアントの合計： 1
クライアントMACスロットID WLAN ID AID WLAN名RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 FlexAAA -40 M7いいえ

スタンドアロンモードでクライアントが別のAPにローミングすると、RADIUSサーバに到達できないため、EAPハンドシェイクが失敗します。クライアントの認証が取り消され、APから削除されます。

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

APはバックアップRADIUSサーバにクライアントセッションを送信します。

APはWLCへの接続を回復します。APは接続モードに戻り、ローカルクライアントセッション情報をWLCと同期します。

クライアントセッションは、AP接続ステータスに基づいて、プライマリISEノードとバックアップISEノードの間で移行します。

APとクライアントはWLC上で接続済みと表示され、APとWLC間の接続がダウンした際にクライアントは切断やフラップを認識しませんでした。

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, ma
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
```

```
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc 4
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc 4
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASSO
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 fo
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-na
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client_
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

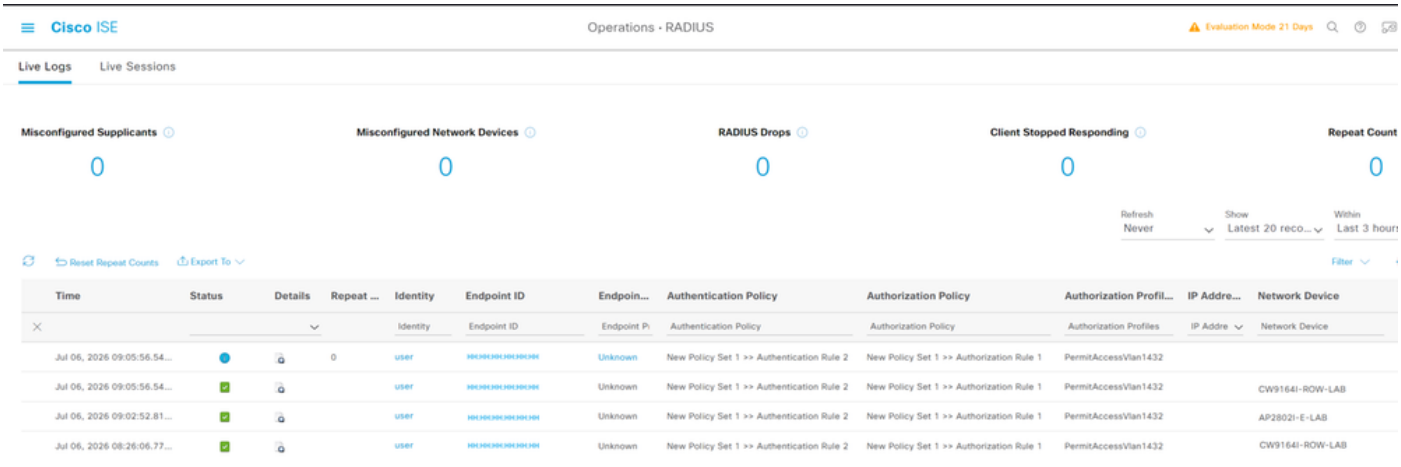
Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No



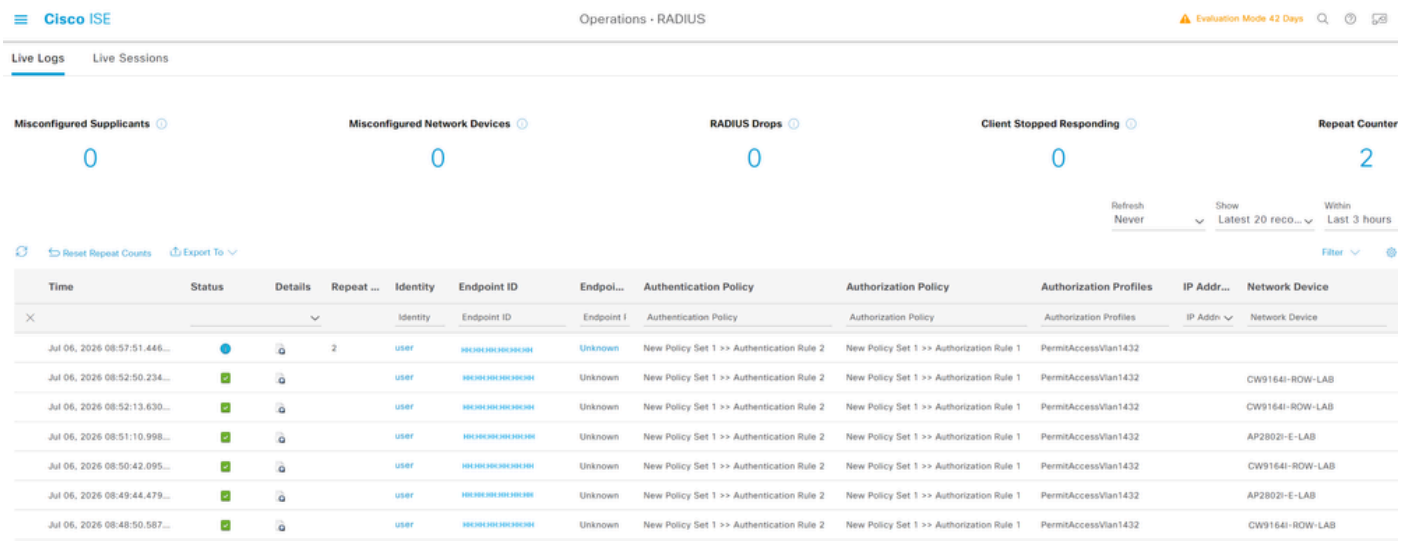

*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716


CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



プライマリISE：初期セッション(08:26:06)と、WLC接続の復元後に再開されたセッション(09:02:52)を記録します。



バックアップISE:APがスタンドアロンモードで動作していた間に、セッションアクティビティ(08:48:50 ~ 08:57:51)をキャプチャします。

最初のセッションは08:26:06でした。その後、APはWLCへの接続を失い、スタンドアロンモードに移行しました。

セッション09:02:52は、APがWLCとの接続を再確立した後の最初のセッションです。

関連情報

- CCNP Enterprise Wireless Design ENWLSD 300-425およびImplementation ENWLSI 300-430 Official Cert Guide、第2版
- Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーション

ガイド、Cisco IOS XE 17.8.x – 章：FlexConnect
- Cisco Catalyst 9800シリーズワイヤレスコントローラ、Cisco IOS XE Cuppertinoリリース17.8.xのリリースノート
- シスコワイヤレスアクセスポイントの機能マトリクス
- シスコのテクニカルサポートとダウンロード

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。