ISEおよびCatalyst 9800ワイヤレスLANコントローラを使用したダイナミックVLAN割り当ての設定

内容

概要

このドキュメントでは、ダイナミックVLAN割り当ての概念と、ワイヤレスクライアントにワイヤレスLAN(WLAN)を割り当てるためにCatalyst 9800ワイヤレスLANコントローラ(WLC)とCisco Identity Service Engine(ISE)を設定する方法について説明します。

要件

次の項目に関する知識があることが推奨されます。

- WLCおよびLightweightアクセスポイント(LAP)に関する基本的な知識があること。
- ISEなどのAAAサーバに関する実務知識があること。
- ワイヤレス ネットワークとワイヤレスのセキュリティ問題に関する全般的な知識があること.

- ダイナミックVLAN割り当てに関する実務知識があること。
- Control and Provisioning for Wireless Access Point(CAPWAP)に関する基本的な知識があること。

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いています。

- ファームウェアリリース16.12.4aが稼働するCisco Catalyst 9800 WLC(Catalyst 9800-CL)。
- ローカルモードのCisco 2800シリーズLAP。
- ネイティブWindows 10サプリカント。
- バージョン2.7が稼働するCisco Identity Service Engine(ISE)。
- ファームウェアリリース16.9.6が稼働するCisco 3850シリーズスイッチ

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

RADIUS サーバによるダイナミック VLAN 割り当て

ほとんどのWireless Local Area Network（WLAN；無線ローカルエリアネットワーク）システムでは、各WLANにService Set Identifier（SSID；サービスセット識別子）に関連付けられたすべてのクライアントに適用されるスタティックポリシーがあります。 この方式は強力ですが、異なるQoSおよびセキュリティポリシーを継承するためにクライアントを異なるSSIDに関連付ける必要があるため、制限があります。

一方、Cisco WLAN ソリューションでは、アイデンティティ ネットワーキングがサポートされています。これにより、ネットワークは単一のSSIDをアドバタイズし、特定のユーザはユーザクレデンシャルに基づいて異なるQoSまたはセキュリティポリシーを継承できます。

ダイナミック VLAN 割り当ては、ユーザが入力したクレデンシャルに基づいてワイヤレス ユーザを特定の VLAN に割り当てる機能です。ユーザを特定のVLANに割り当てるタスクは、Cisco ISEなどのRADIUS認証サーバによって処理されます。たとえば、この機能を利用すると、キャンパス ネットワーク内を移動するワイヤレス ホストを同じ VLAN に割り当てることができます。

したがって、クライアントがコントローラに登録されたLAPへの関連付けを試みると、WLCはユーザのクレデンシャルをRADIUSサーバに渡して検証します。認証に成功すると、RADIUS サーバからユーザに特定の Internet Engineering Task Force（IETF）アトリビュートが渡されます。これらのRADIUS属性は、ワイヤレスクライアントに割り当てる必要があるVLAN IDを決定します。ユーザは常にこの事前設定済みのVLAN IDに割り当てられるため、クライアントのSSIDは重要ではありません。

VLAN ID の割り当てに使用される RADIUS ユーザ アトリビュートは次のとおりです。

- IETF 64（Tunnel Type）：これを VLAN に設定します。
- IETF 65（Tunnel Medium Type）：これを 802 に設定します。
- IETF 81（Tunnel Private Group ID）：これを VLAN ID に設定します。

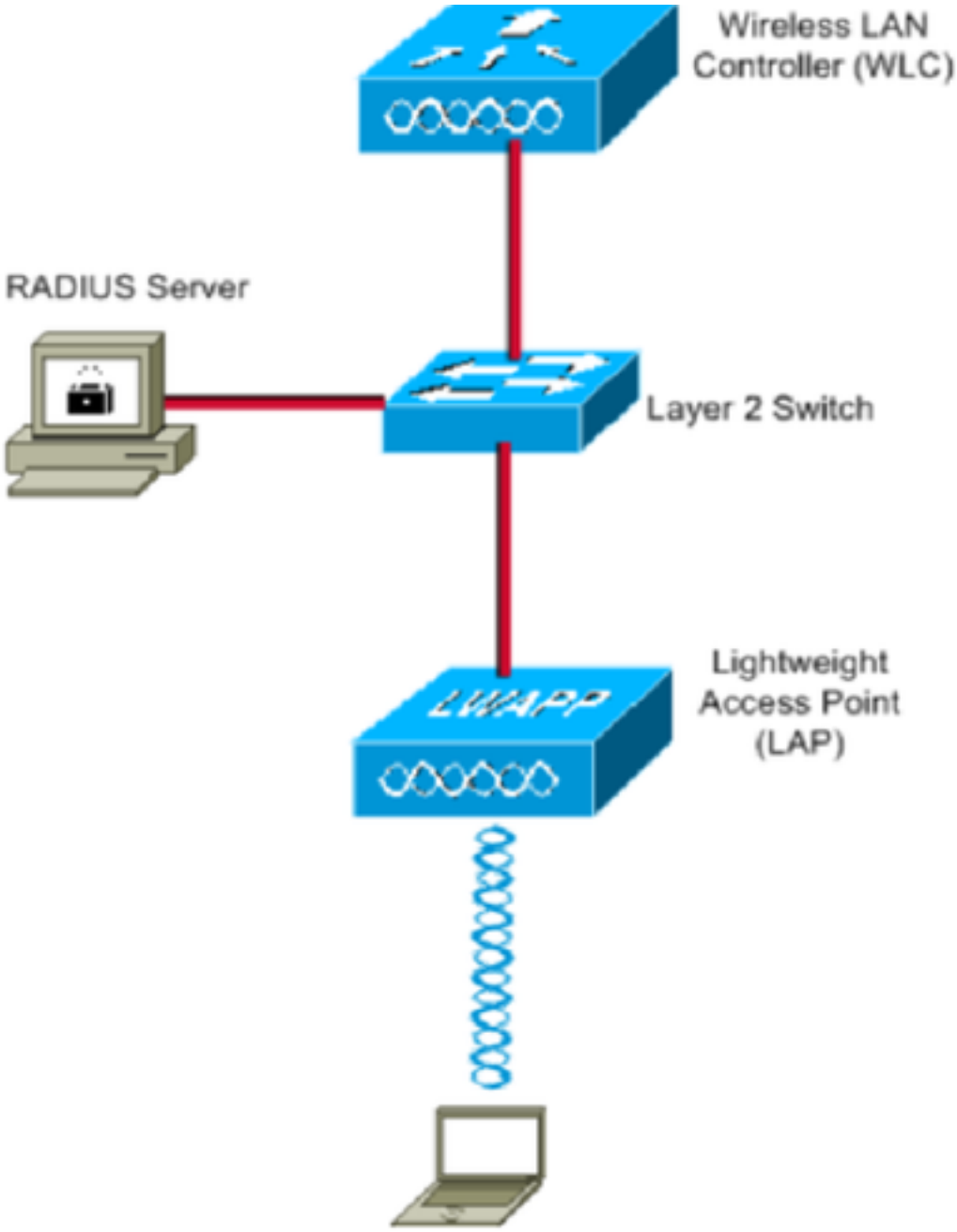
VLAN IDは12ビットで、1 ~ 4094の値を取ります（両端を含む）。Tunnel-Private-Group-IDは文字列型であるため、RFC2868でIEEE 802.1Xで使用するように定義されているように、VLAN IDの整数値は文字列としてエンコードされます。これらのトンネル属性が送信される場合は、[Tag]フィールドに入力する必要があります。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



この図で使用されているコンポーネントの設定の詳細は、次のとおりです。

- Cisco ISE(RADIUS)サーバのIPアドレスは10.10.1.24です。
- WLC の管理インターフェイス アドレスは 10.10.1.17 です。
- コントローラの内部 DHCP サーバは、ワイヤレス クライアントに IP アドレスを割り当てる目的に使用されます。
- このドキュメントでは、セキュリティ メカニズムとして 802.1x と PEAP を使用します。
- VLAN102はこの設定全体で使用されます。ユーザ名jonathga-102は、RADIUSサーバによってVLAN102に配置されるように設定されています。

設定手順

この設定は、次の 4 つのカテゴリに分類されます。

- Cisco ISE の設定.
- 複数の VLAN を使用するためのスイッチの設定.
- Catalyst 9800 WLCの設定。

Cisco ISE の設定

設定には次の手順が必要です。

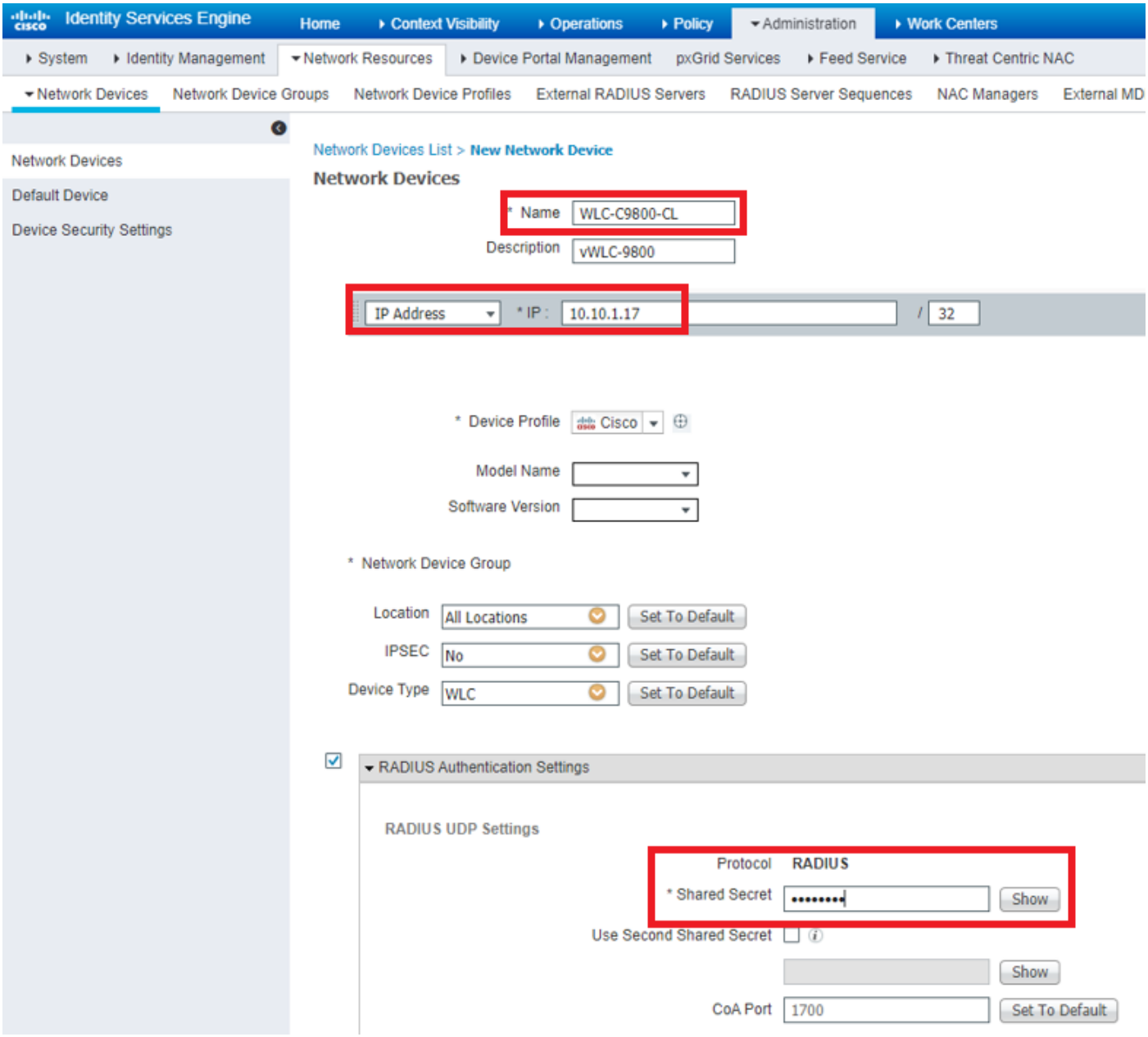
- Catalyst WLCをCisco ISEサーバのAAAクライアントとして設定します。
- Cisco ISEで内部ユーザを設定します。
- Cisco ISEでのダイナミックVLAN割り当てに使用するRADIUS(IETF)アトリビュートを設定します。

ステップ1:Catalyst WLCをCisco ISEサーバのAAAクライアントとして設定します

この手順では、WLCがユーザクレデンシャルをISEに渡すことができるように、WLCをISEサーバ上のAAAクライアントとして追加する方法について説明します。

次のステップを実行します。

1. ISE GUIから、 **Administration > Network Resources > Network Devices**選択 **Add**.
2. 図に示すように、WLC管理IPアドレスとWLCとISEの間のRADIUS共有秘密を使用して設定を完了します。

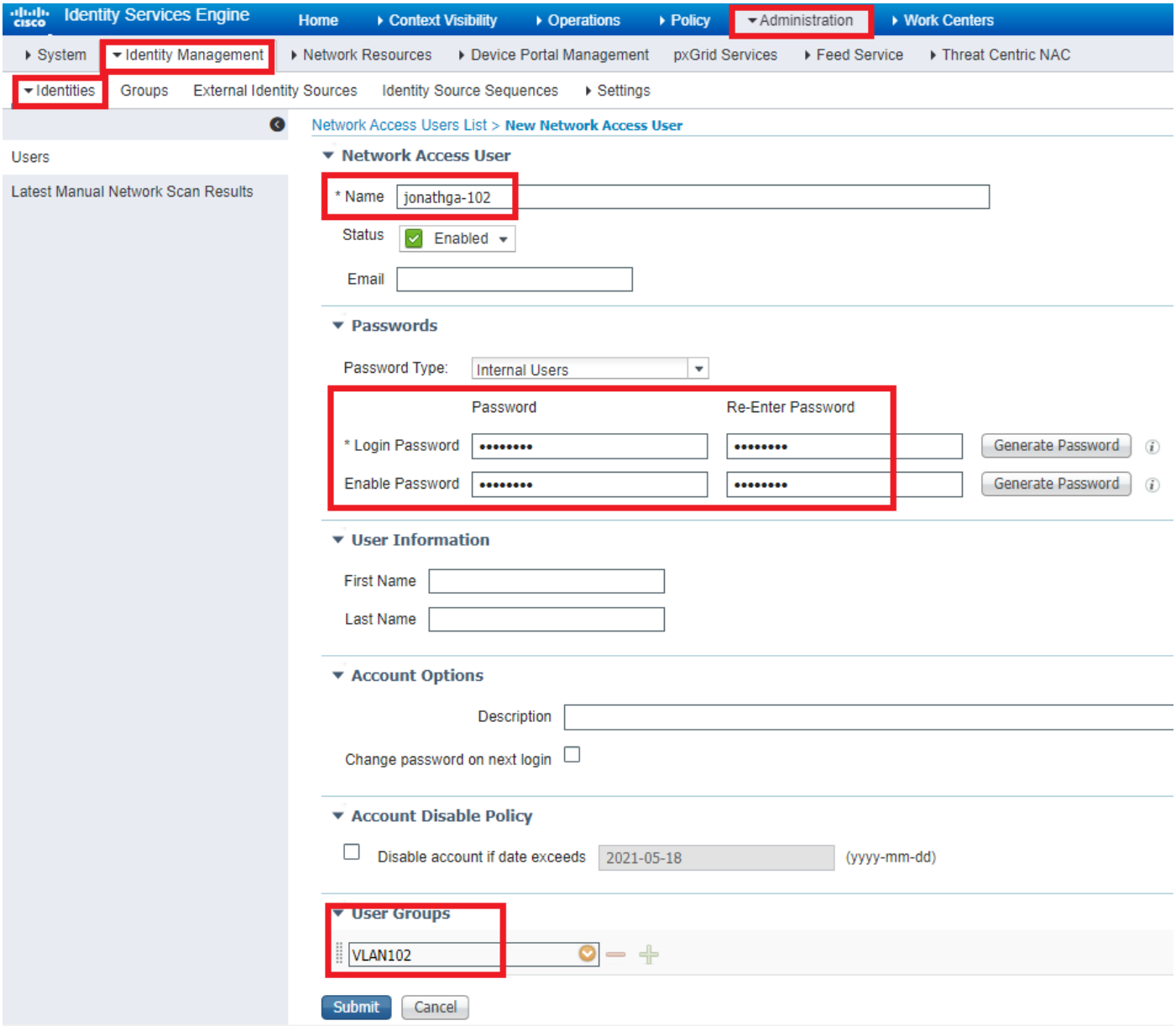


ステップ2:Cisco ISEでの内部ユーザの設定

この手順では、Cisco ISEの内部ユーザデータベースにユーザを追加する方法について説明します。

次のステップを実行します。

1. ISE GUIから、 **Administration > Identity Management > Identities** 選択 **Add**.
2. 次の図に示すように、ユーザ名、パスワード、およびユーザグループで設定を完了します。

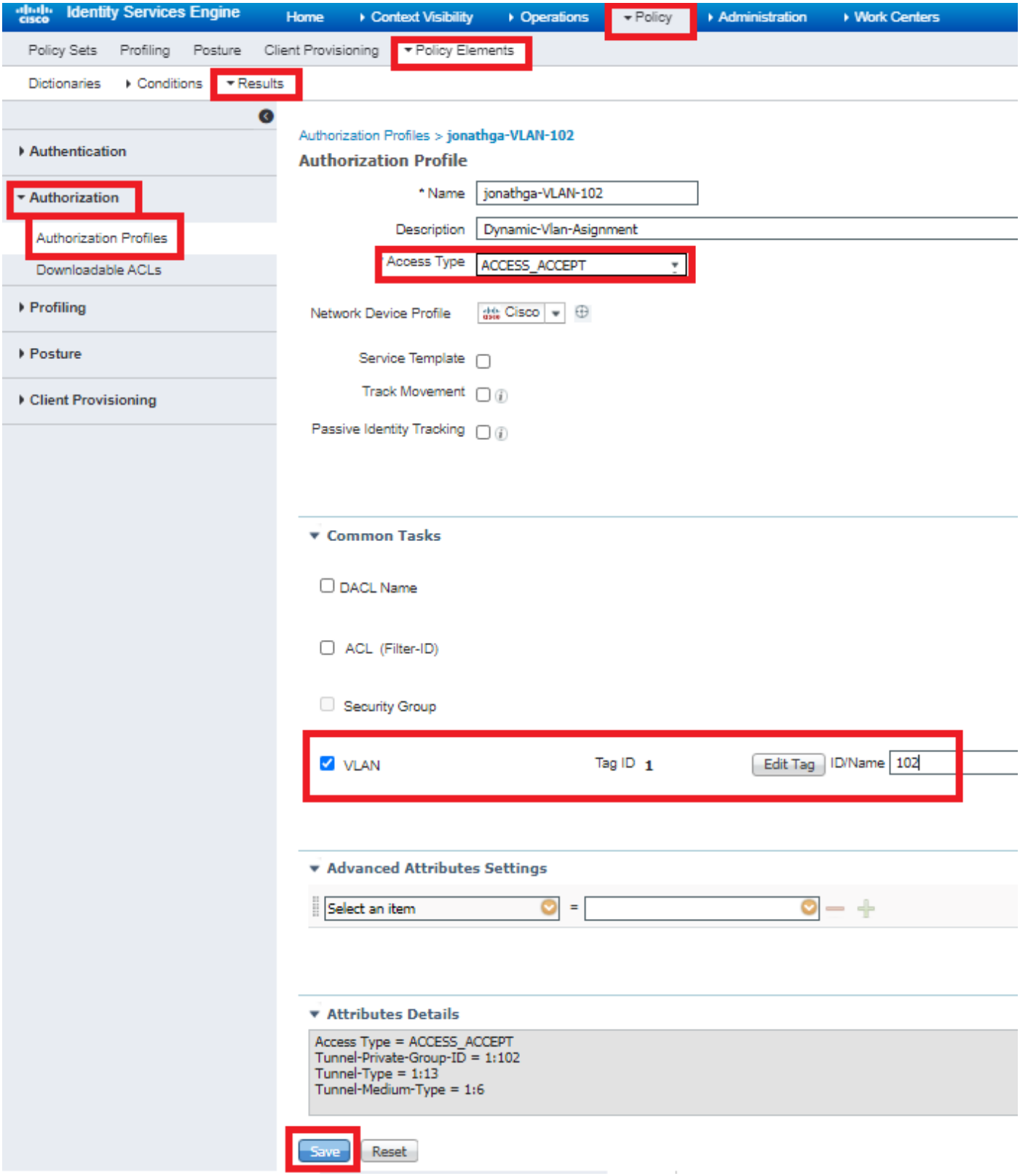


手順3：ダイナミックVLAN割り当てに使用するRADIUS(IETF)アトリビュートを設定する

この手順では、ワイヤレスユーザの認可プロファイルと認証ポリシーを作成する方法について説明します。

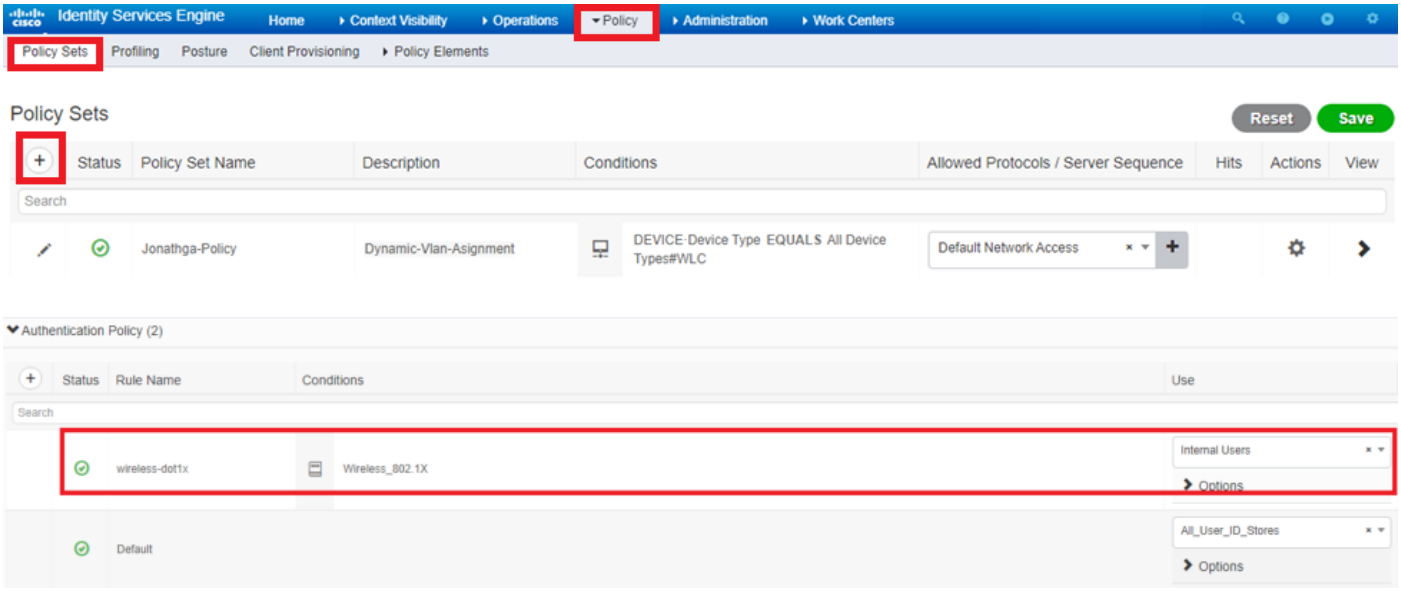
次のステップを実行します。

1. ISE GUIから、 **Policy > Policy Elements > Results > Authorization > Authorization profiles** 選択 **Add** 新しいプロファイルを作成します。
2. それぞれのグループのVLAN情報を使用して、認可プロファイルの設定を完了します。次の図は、 **jonathga-VLAN-102** グループの設定値。



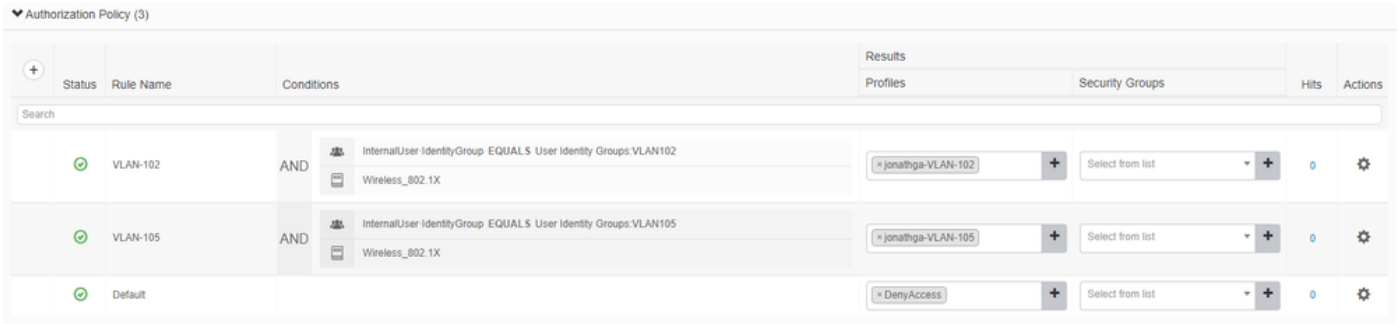
認可プロファイルを設定したら、ワイヤレスユーザの認証ポリシーを作成する必要があります。新しい **Custom** ポリシーを設定するか、 **Default** ポリシーセット。この例では、カスタムプロファイルが作成されます。

3. に移動 **Policy > Policy Sets** 選択 **Add** 図に示すように、新しいポリシーを作成するには、次の手順を実行します。



次に、グループメンバーシップに基づいてそれぞれの認可プロファイルを割り当てるために、ユーザの認可ポリシーを作成する必要があります。

5. を開きます。 **Authorization policy** セクションを参照し、図に示すように、その要件を満たすポリシーを作成します。



複数の VLAN を使用するためのスイッチの設定

スイッチで複数のVLANを許可するには、次のコマンドを発行して、コントローラに接続されているスイッチポートを設定する必要があります。

```
Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation dot1q
```

> **注**：ほとんどのスイッチでは、そのスイッチ上で作成されたすべての VLAN に対してトランク ポートを通過することがデフォルトで許可されます。スイッチに有線ネットワークが接続されている場合は、有線ネットワークに接続されたスイッチ ポートに対しても同じ設定を適用できます。これにより、有線ネットワークとワイヤレス ネットワークの同じ VLAN 間での通信が可能になります。

Catalyst 9800 WLCの設定

設定には次の手順が必要です。

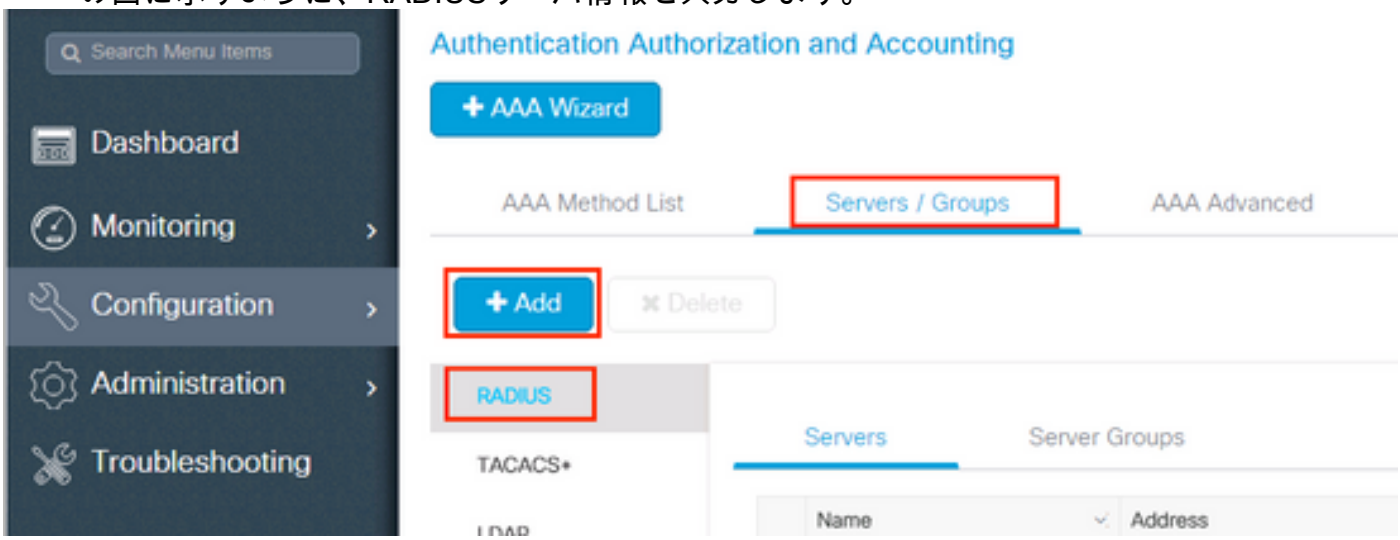
- 認証サーバの詳細を使用して WLC を設定します。
- VLANを設定します。
- WLAN（SSID）の設定
- ポリシープロファイルを設定します。
- ポリスタグを設定します。
- APにポリスタグを割り当てます。

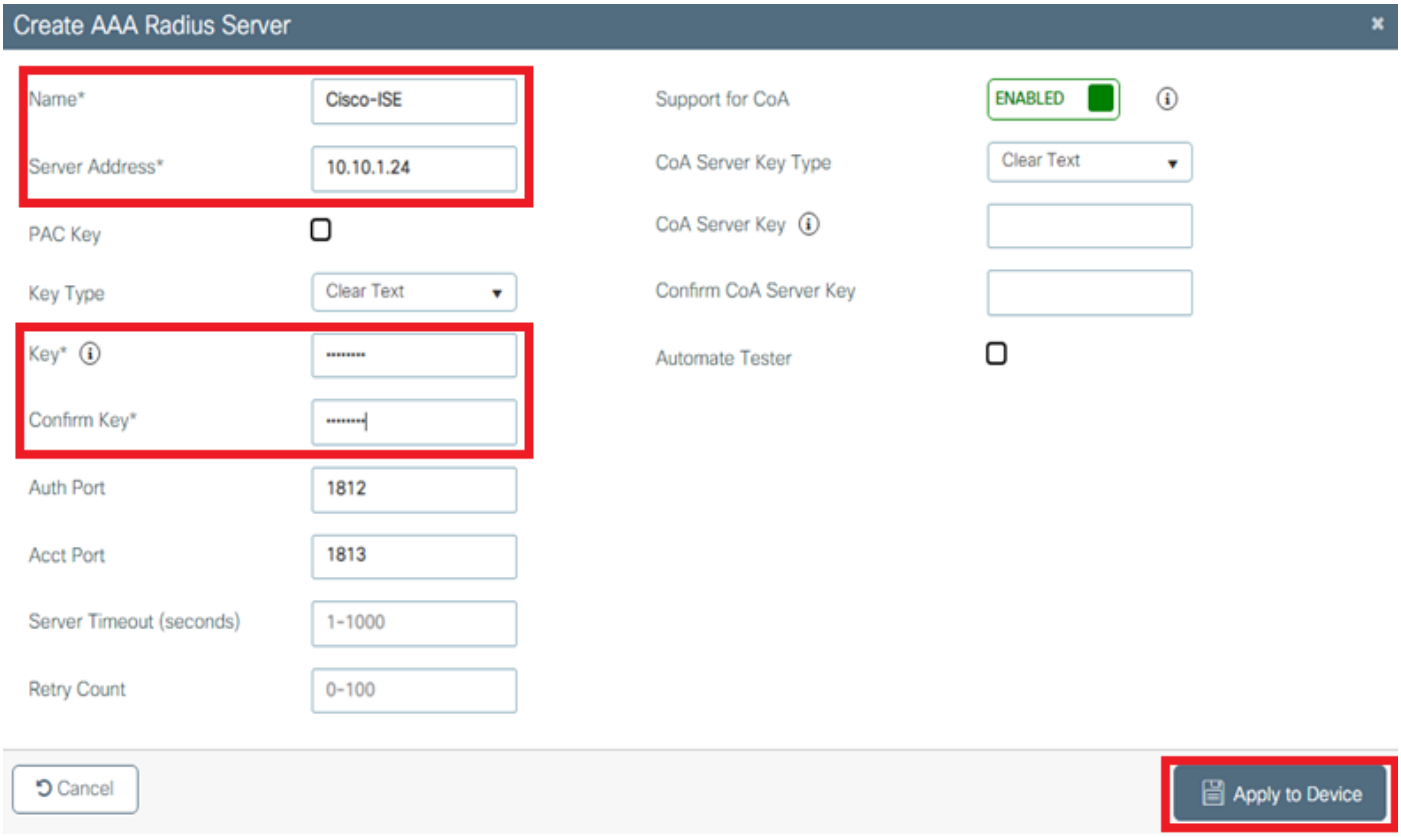
ステップ1：認証サーバの詳細を使用したWLCの設定

クライアントを認証するためにRADIUSサーバと通信できるようにWLCを設定する必要があります。

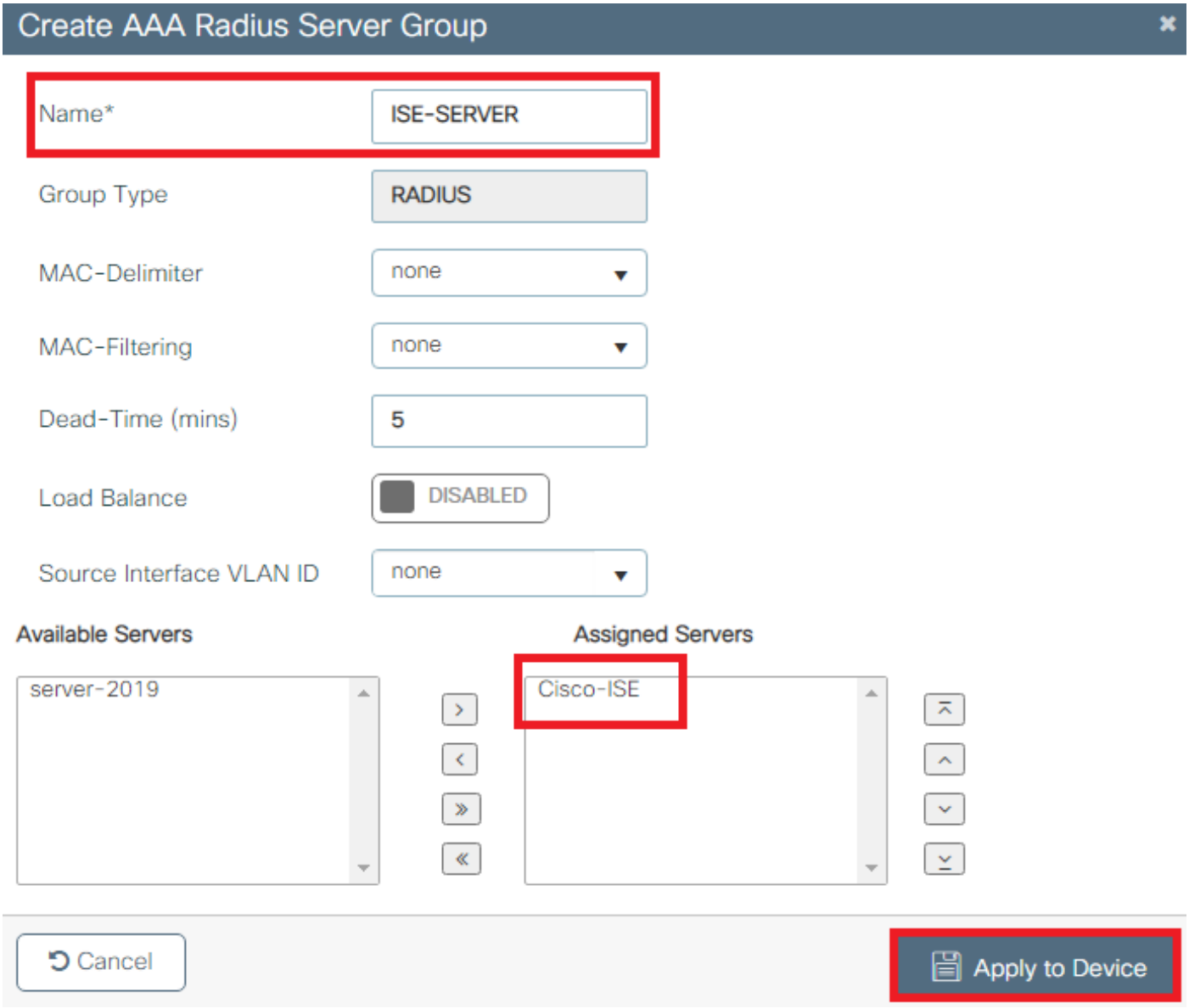
次のステップを実行します。

1. コントローラのGUIで、 **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** 次の図に示すように、RADIUSサーバ情報を入力します。

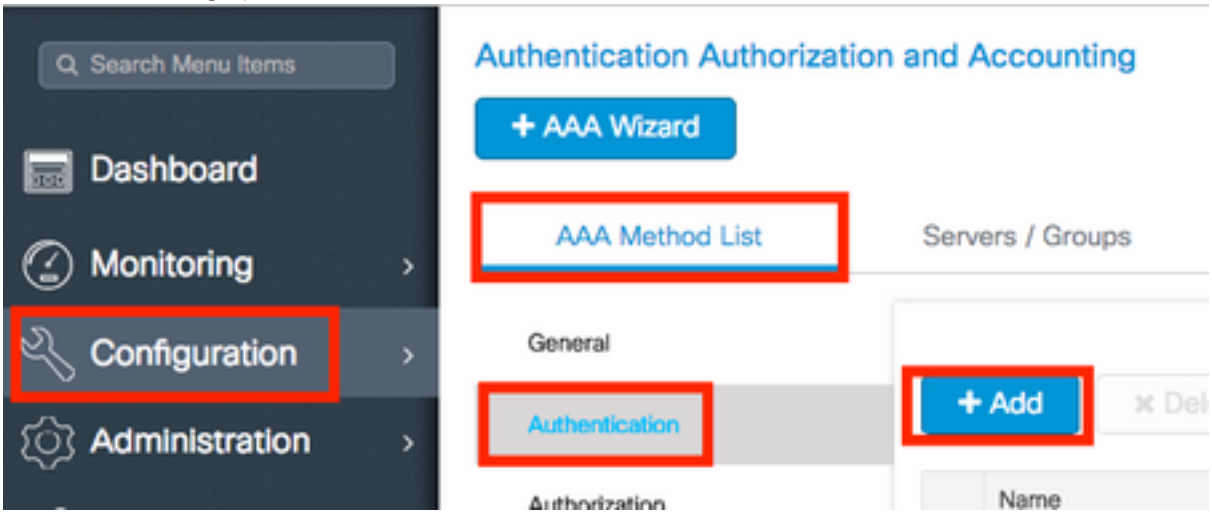


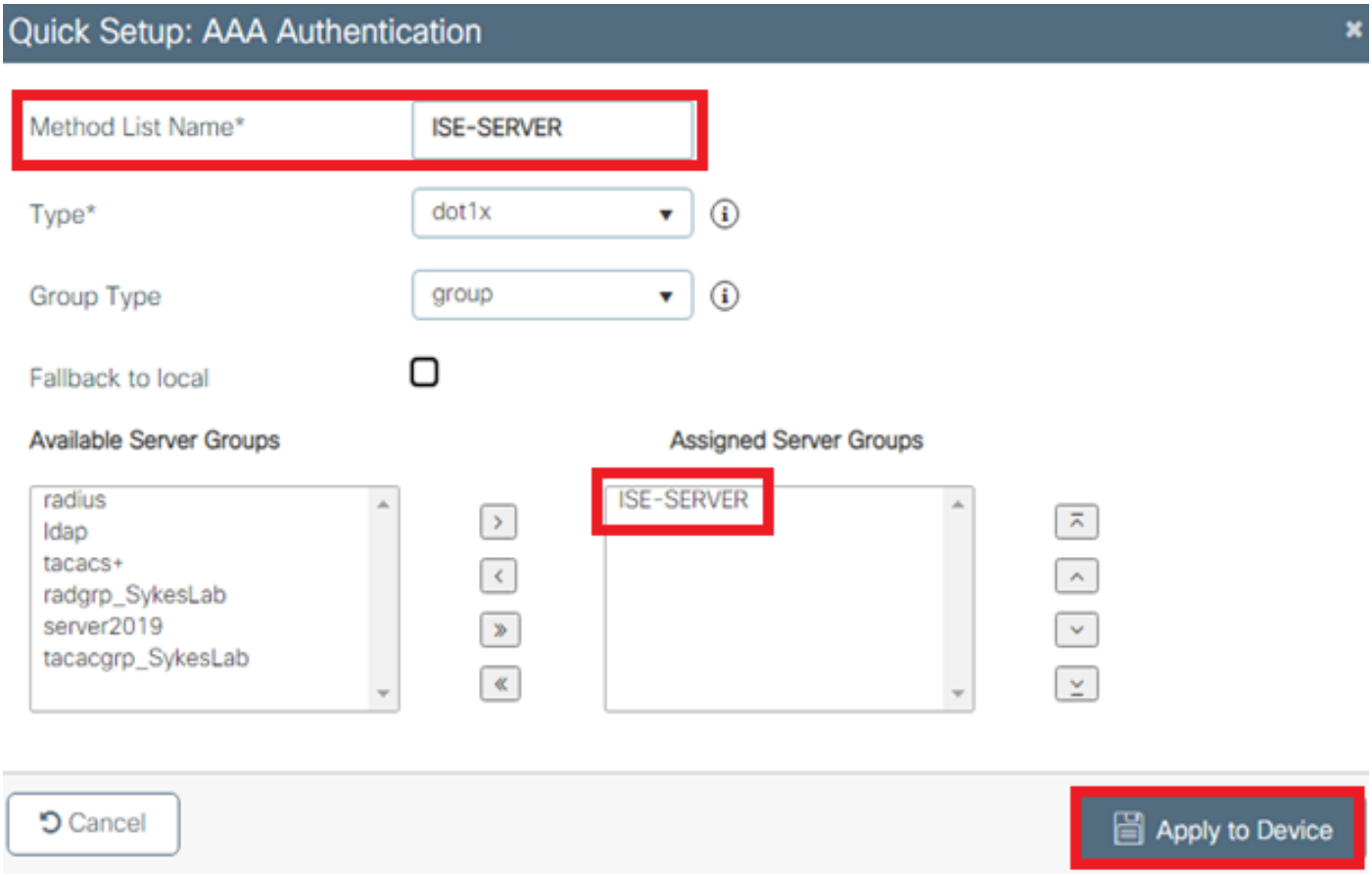


2. RADIUSサーバをRADIUSグループに追加するには、 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** 図に示すように



3. 認証方式リストを作成するには、 **Configuration > Security > AAA > AAA Method List > Authentication > + Add** 図に示すように



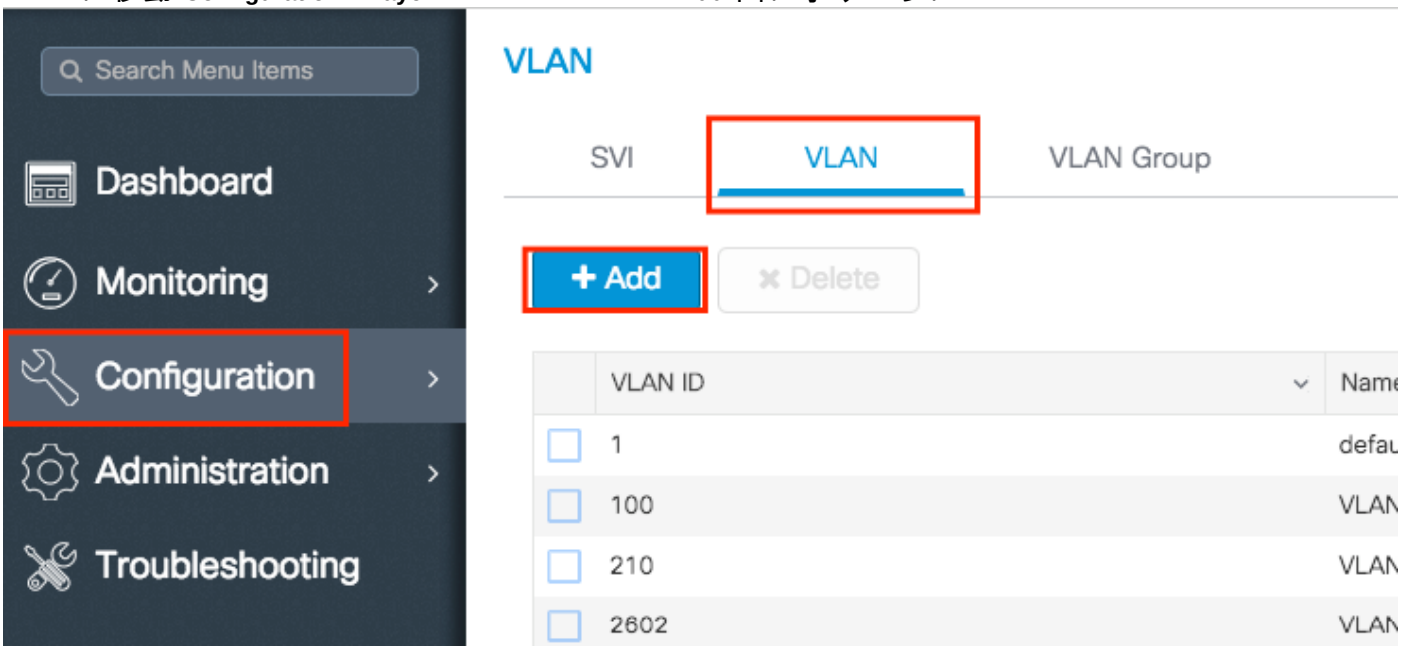


手順2. VLANの設定

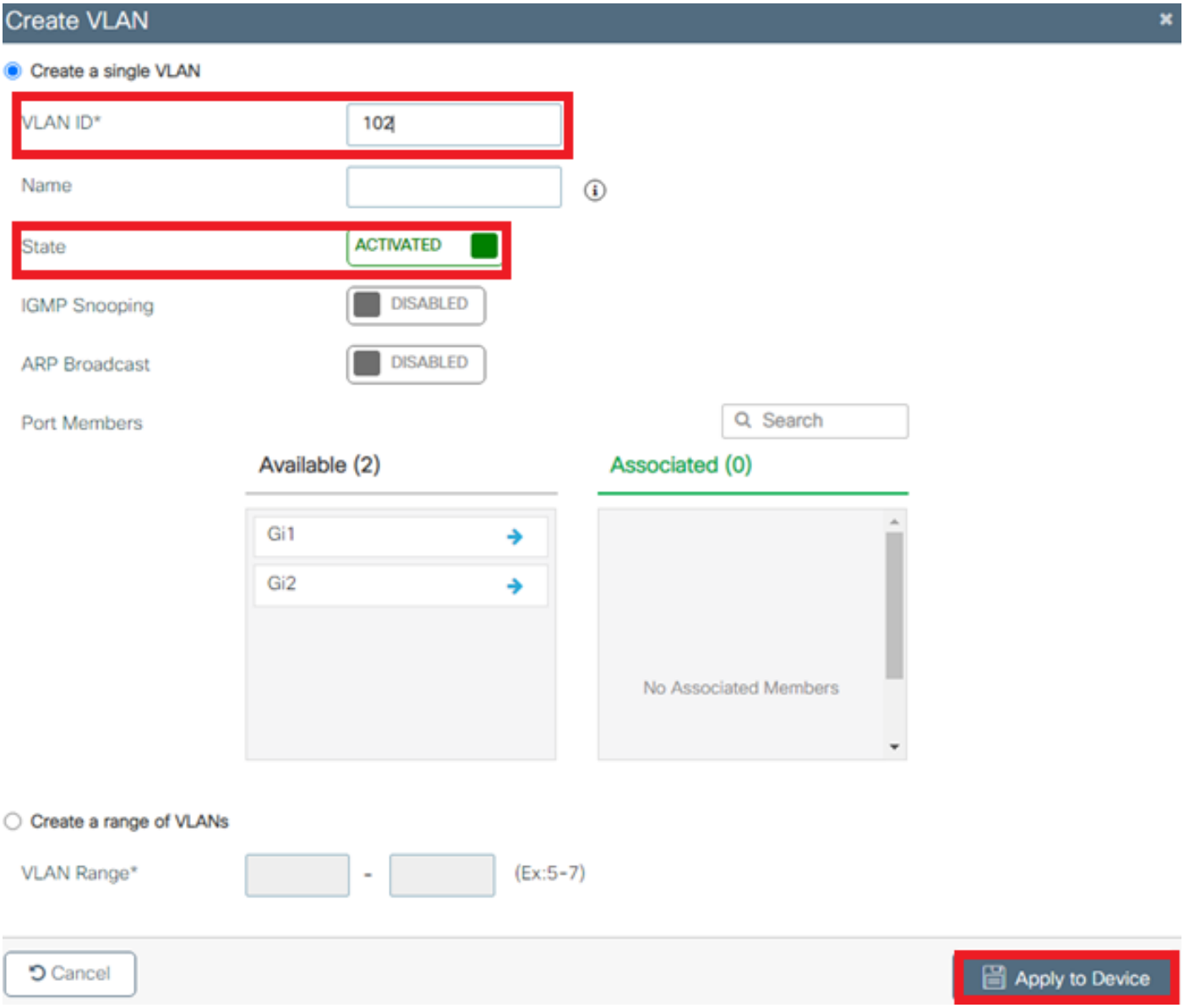
この手順では、Catalyst 9800 WLCでVLANを設定する方法について説明します。このドキュメントですでに説明したように、RADIUS サーバの Tunnel-Private-Group ID 属性で指定された VLAN ID が WLC 内にも存在している必要があります。

この例では、ユーザjonathga-102が **Tunnel-Private-Group ID of 102 (VLAN =102)** 設定します。

1. に移動 **Configuration > Layer2 > VLAN > VLAN > + Add** 図に示すように



2. 図に示すように、必要な情報を入力します。



注：名前を指定しない場合、VLANには自動的にVLANXXXXという名前が割り当てられます。ここで、XXXXはVLAN IDです。

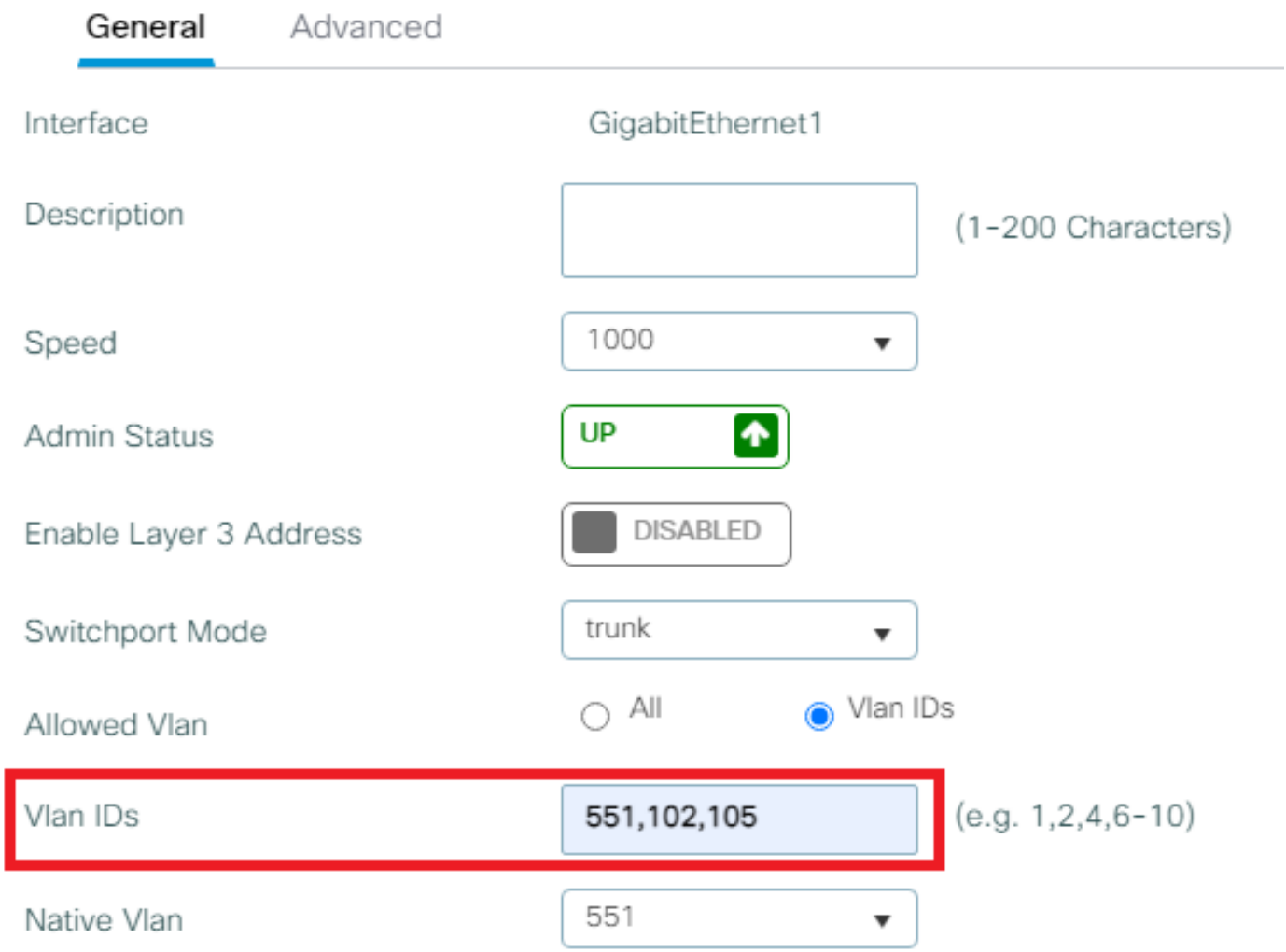
必要なすべてのVLANに対して手順1と2を繰り返します。手順3に進むことができます。

3. VLANがデータインターフェイスで許可されていることを確認します。 ポートチャネルを使用している場合は、 **Configuration > Interface > Logical > PortChannel name > General.**次のように設定されている場合 **Allowed VLAN = All** 設定は完了です。もし分かったら **Allowed VLAN = VLANs IDs**必要なVLANを追加し、その後に **Update & Apply to Device.**ポートチャネルが使用されていない場合は、 **Configuration > Interface > Ethernet > Interface Name > General.**次のように設定されている場合 **Allowed VLAN = All** 設定は完了です。もし分かったら **Allowed VLAN = VLANs IDs**必要なVLANを追加し、その後に **Update & Apply to Device.**

次の図は、Allまたは特定のVLAN IDを使用する場合のインターフェイス設定に関連する設定を示しています。

General Advanced

Interface	GigabitEthernet3
Description	(1-200 Characters)
Admin Status	UP
Port Fast	disable
Enable Layer 3 Address	DISABLED
Switchport Mode	trunk
Allowed Vlan	All / Vlan IDs
Native Vlan	

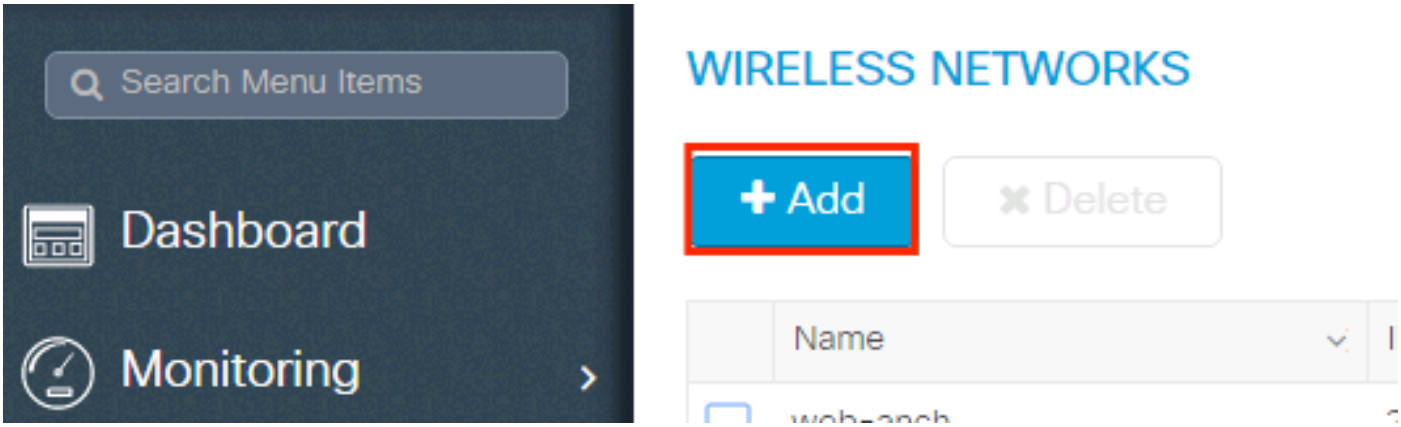


ステップ3:WLAN(SSID)の設定

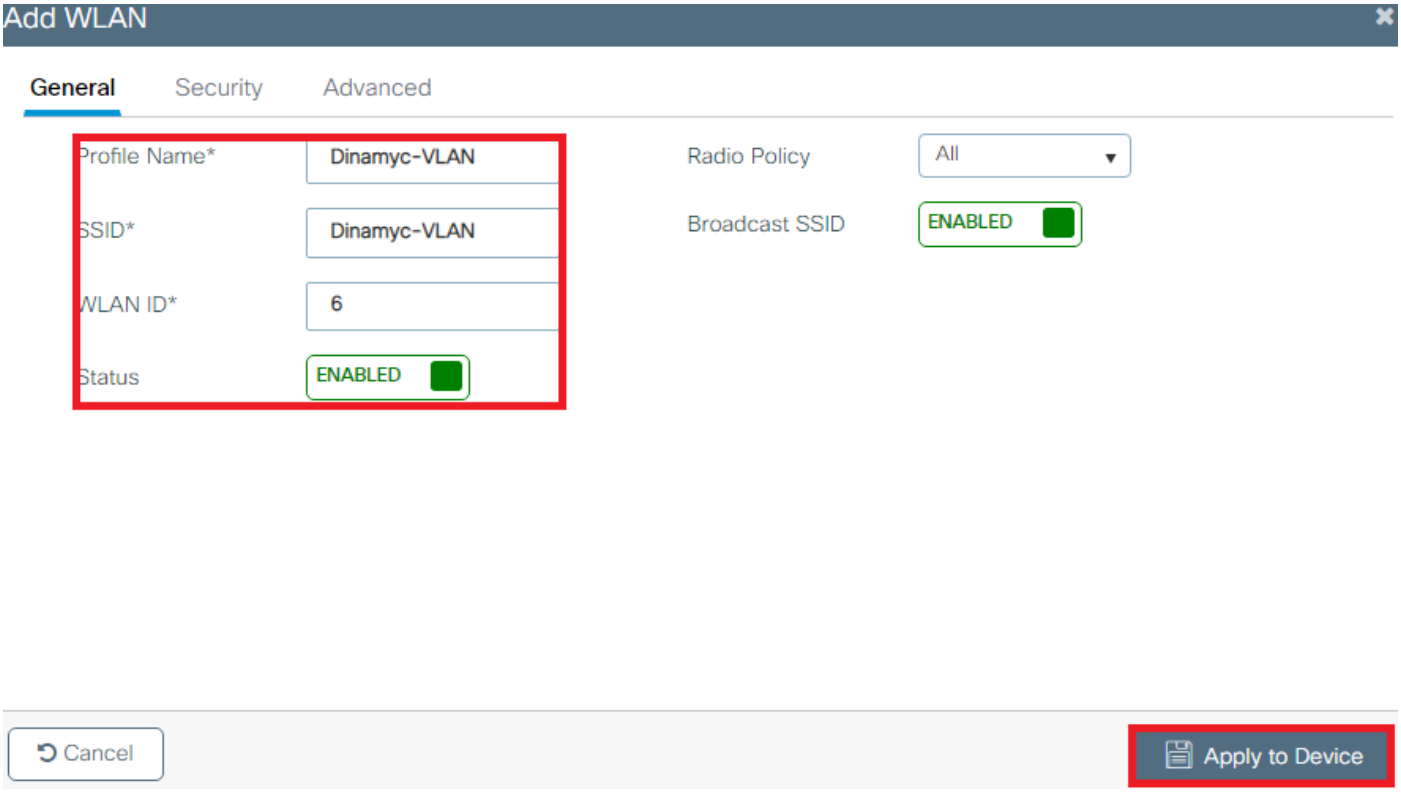
この手順では、WLC で WLAN を設定する方法について説明します。

次のステップを実行します。

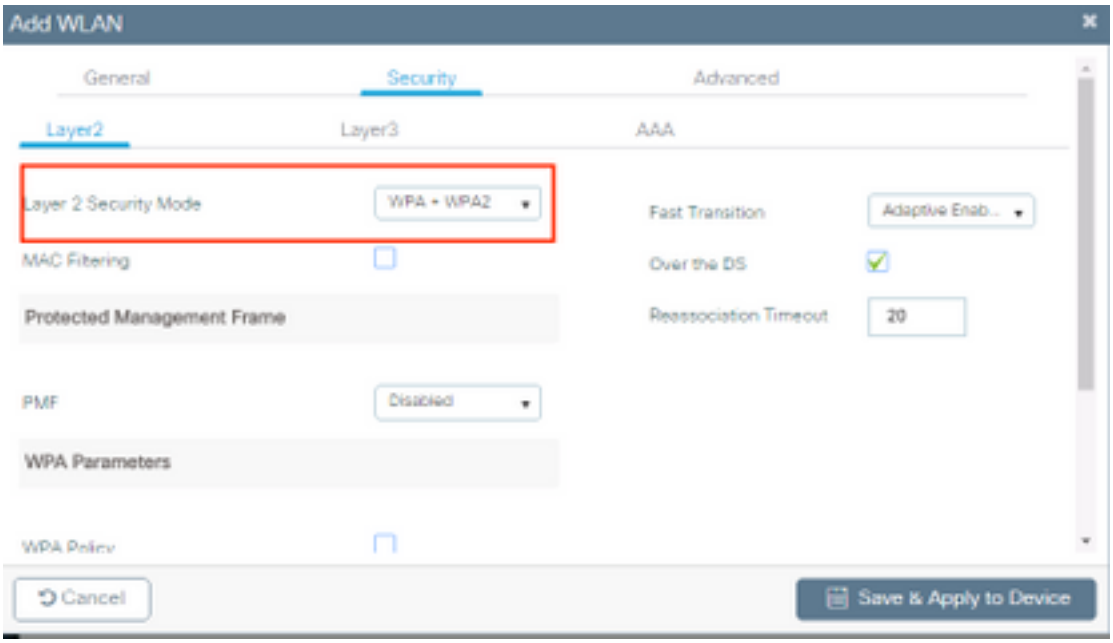
1. WLANを作成します。に移動 **Configuration > Wireless > WLANs > + Add** 必要に応じて、図に示すようにネットワークを設定します。

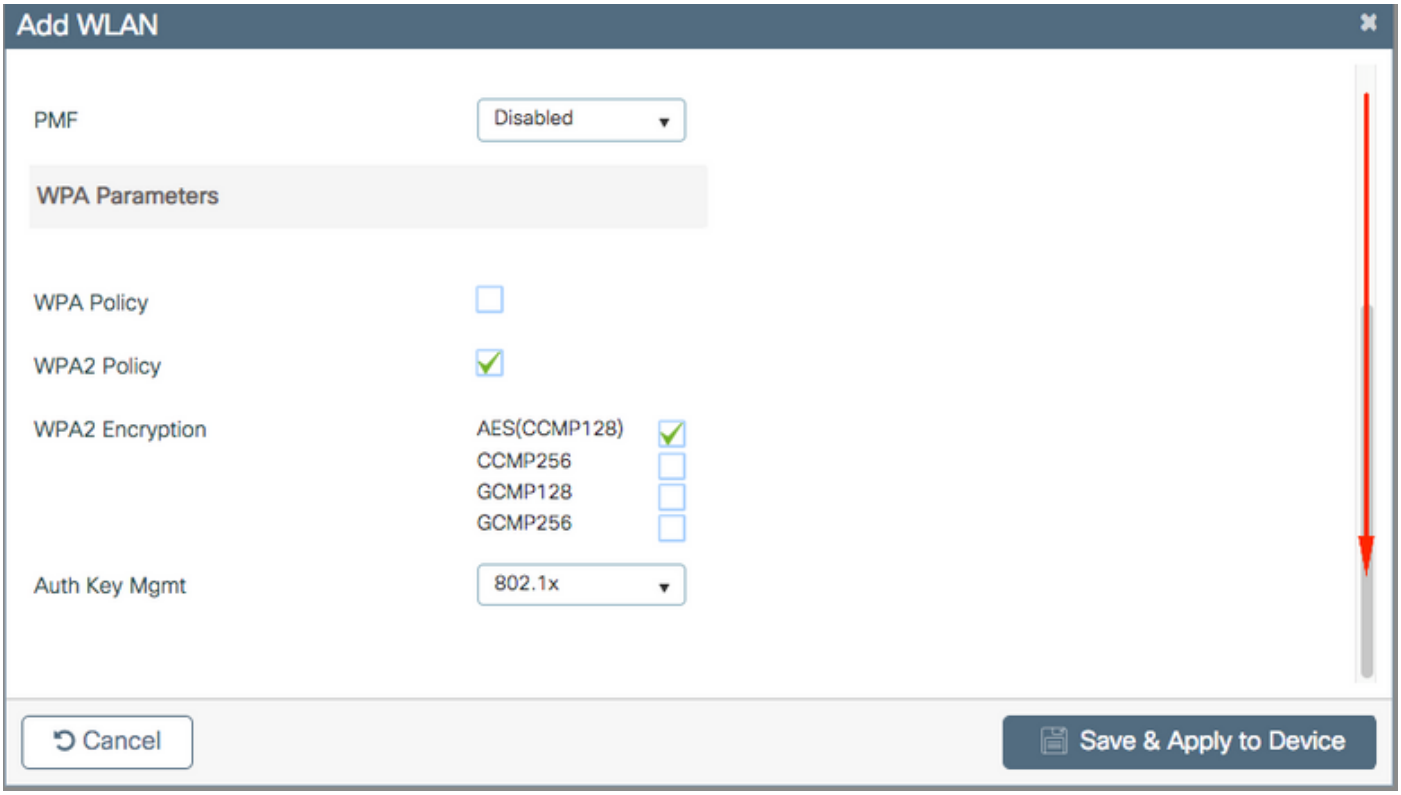


2. 図に示すように、WLAN情報を入力します。

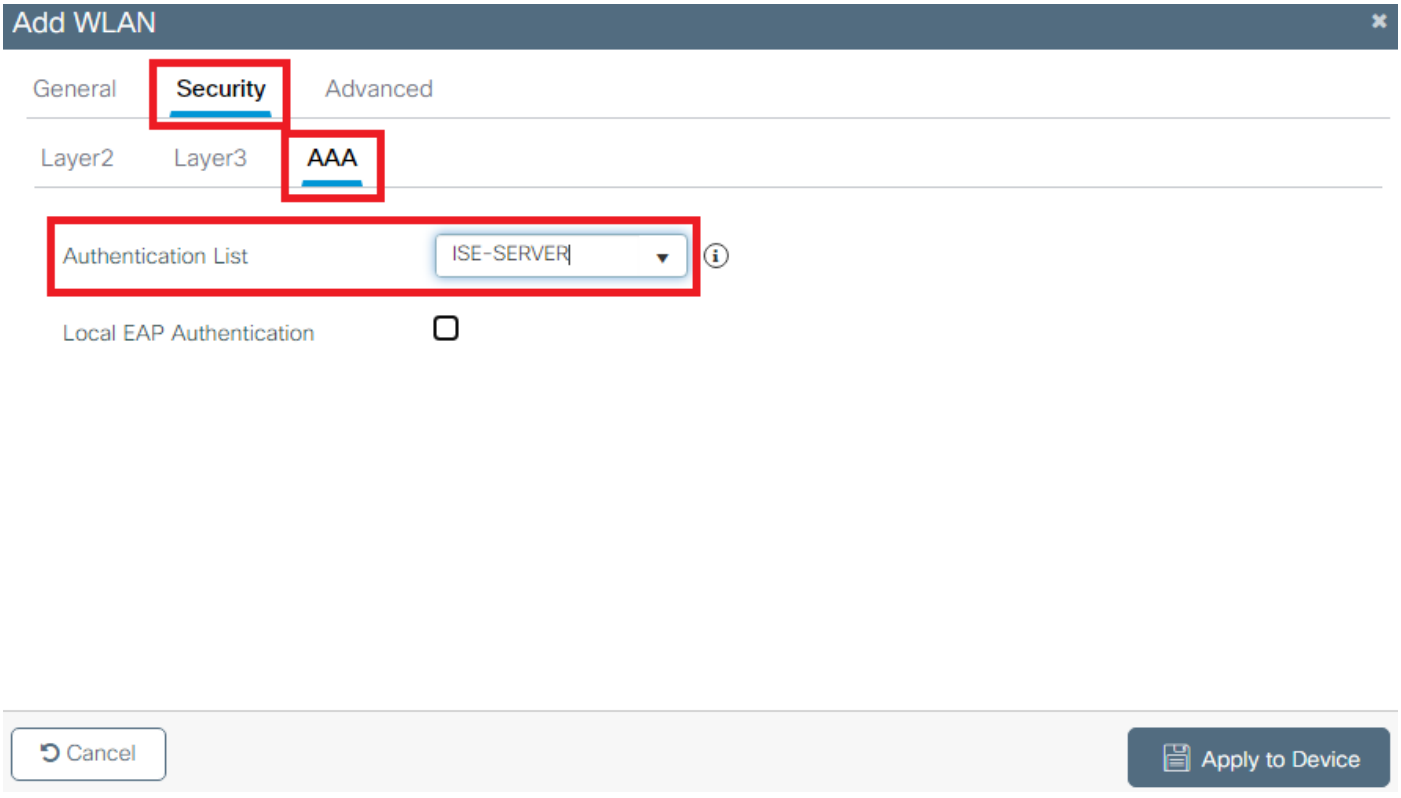


3. に移動 **Security** タブをクリックし、必要なセキュリティ方式を選択します。この場合、次の図に示すように、WPA2 + 802.1xが使用されます。





変更前**Security > AAA** タブで、ステップ3で作成した認証方式を **Configure the WLC with the Details of the Authentication Server** セクションを参照してください。



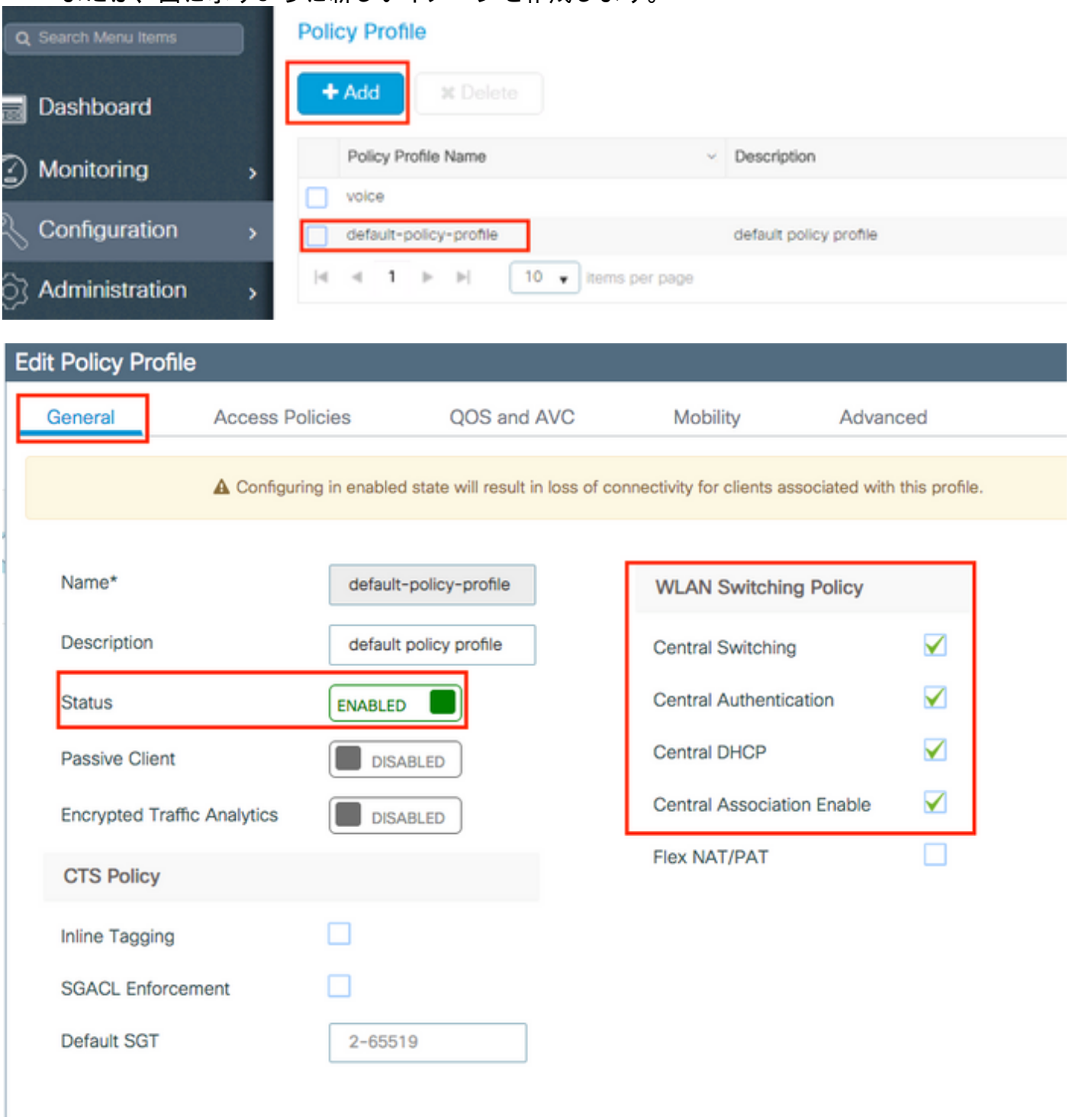
ステップ4：ポリシープロファイルの設定

この手順では、WLCでポリシープロファイルを設定する方法について説明します。

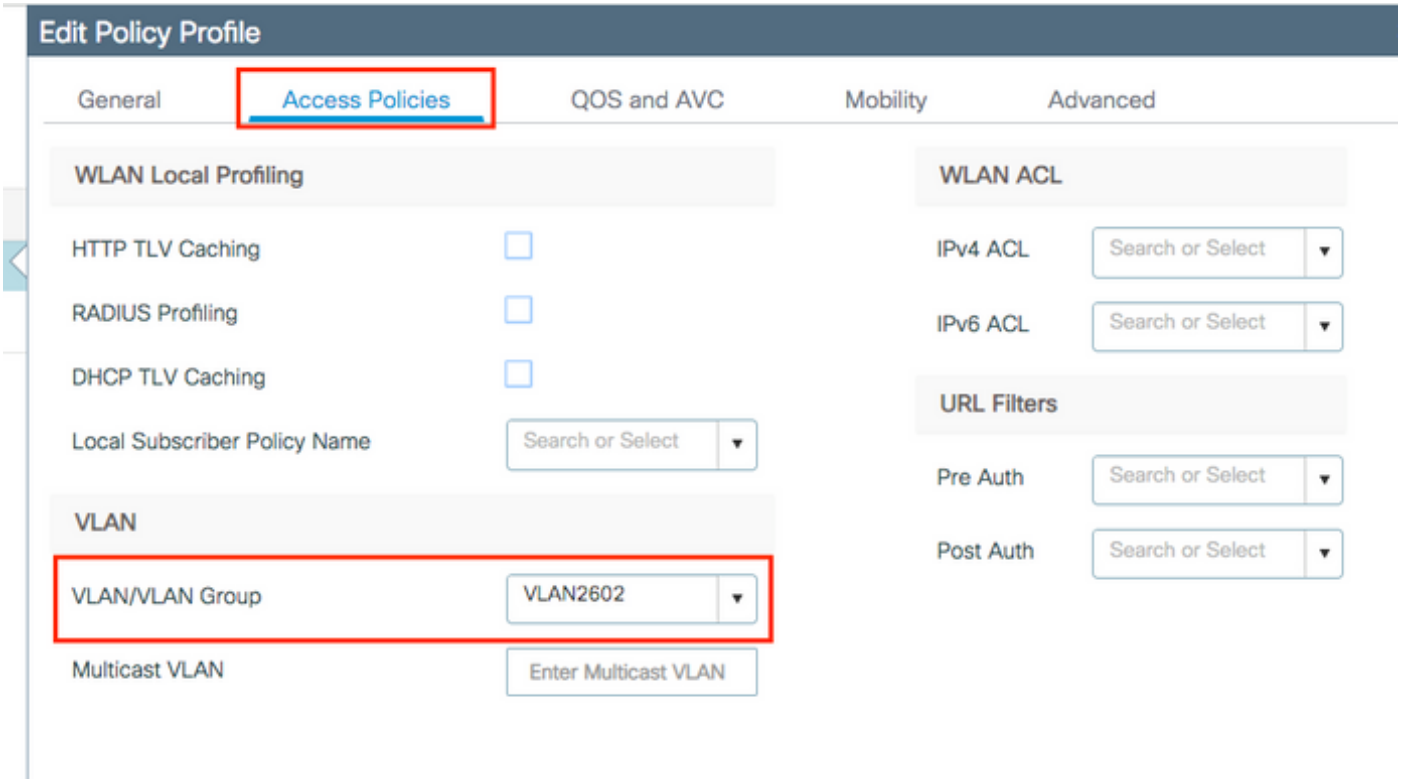
次のステップを実行します。

1. に移動 **Configuration > Tags & Profiles > Policy Profile** 次のいずれかを実行します **default-policy-profile**

または、図に示すように新しいイメージを作成します。

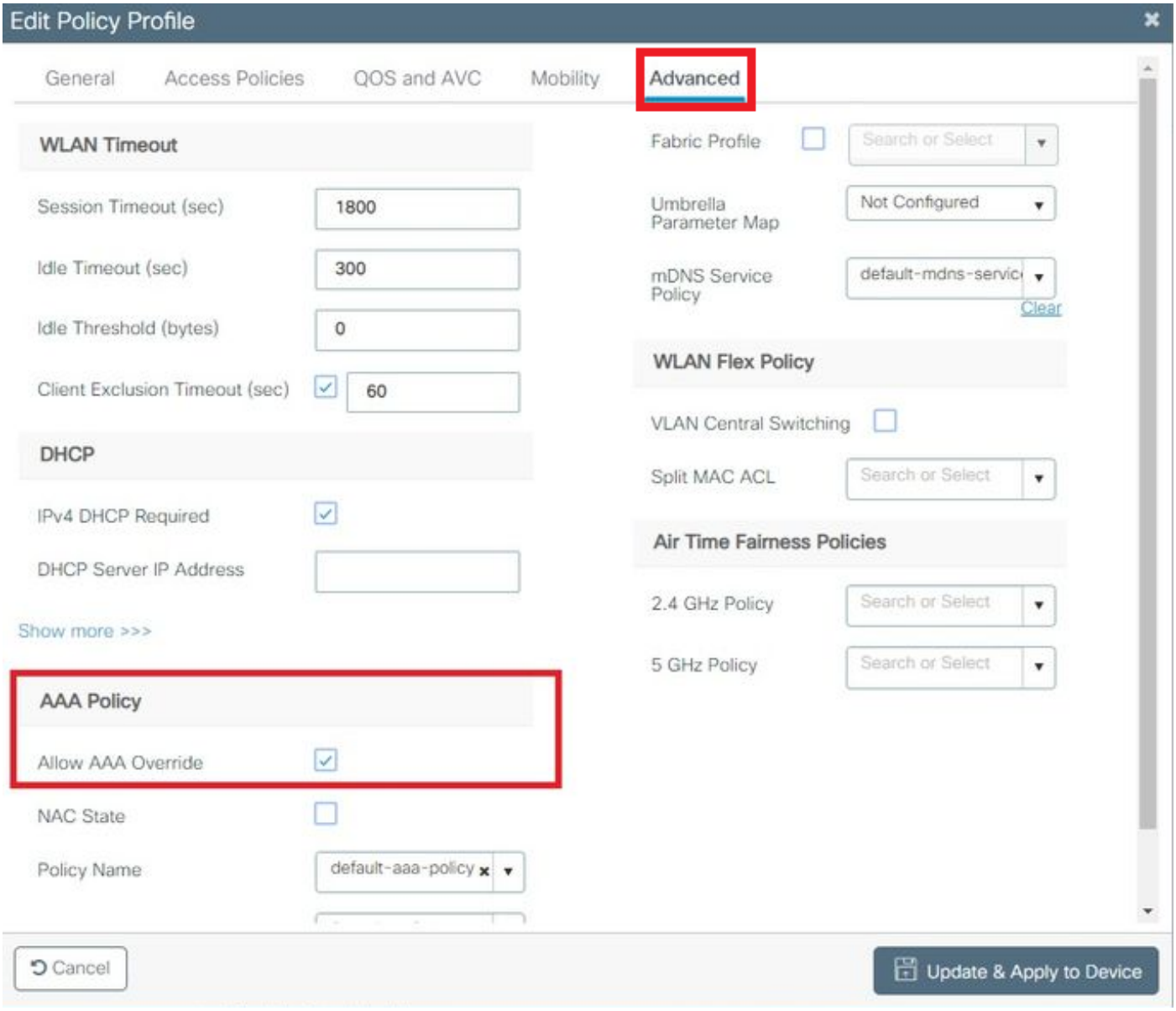


2. **Access Policies** タブでは、図に示すように、ワイヤレスクライアントがこのWLANにデフォルトで接続するときに割り当てられるVLANを割り当てます。



注：この例では、認証が成功した際にワイヤレスクライアントを特定のVLANに割り当てるのがRADIUSサーバの役割です。したがって、ポリシープロファイルに設定されたVLANはブラックホールVLANになり、RADIUSサーバのuser Tunnel-Group-Private-IDフィールドでフィールドに指定されるVLAN

3. **Advance** タブで、 **Allow AAA Override** 図に示すように、radiusサーバがクライアントを適切なVLANに配置するために必要な属性を返す場合にWLC設定をオーバーライドするには、チェックボックスをオンにします。

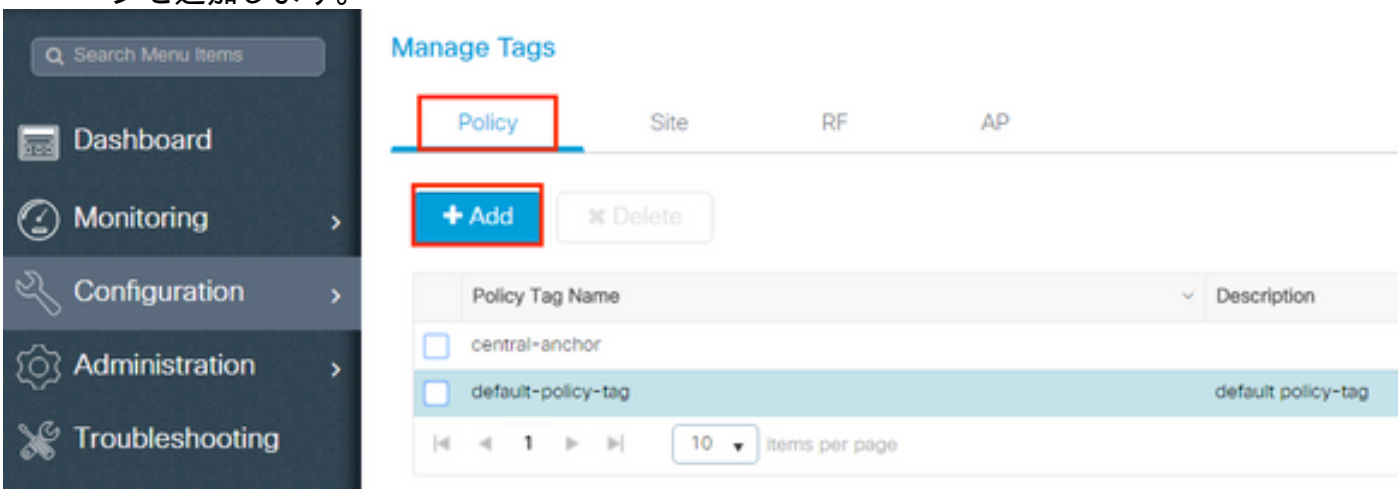


ステップ5：ポリシータグの設定

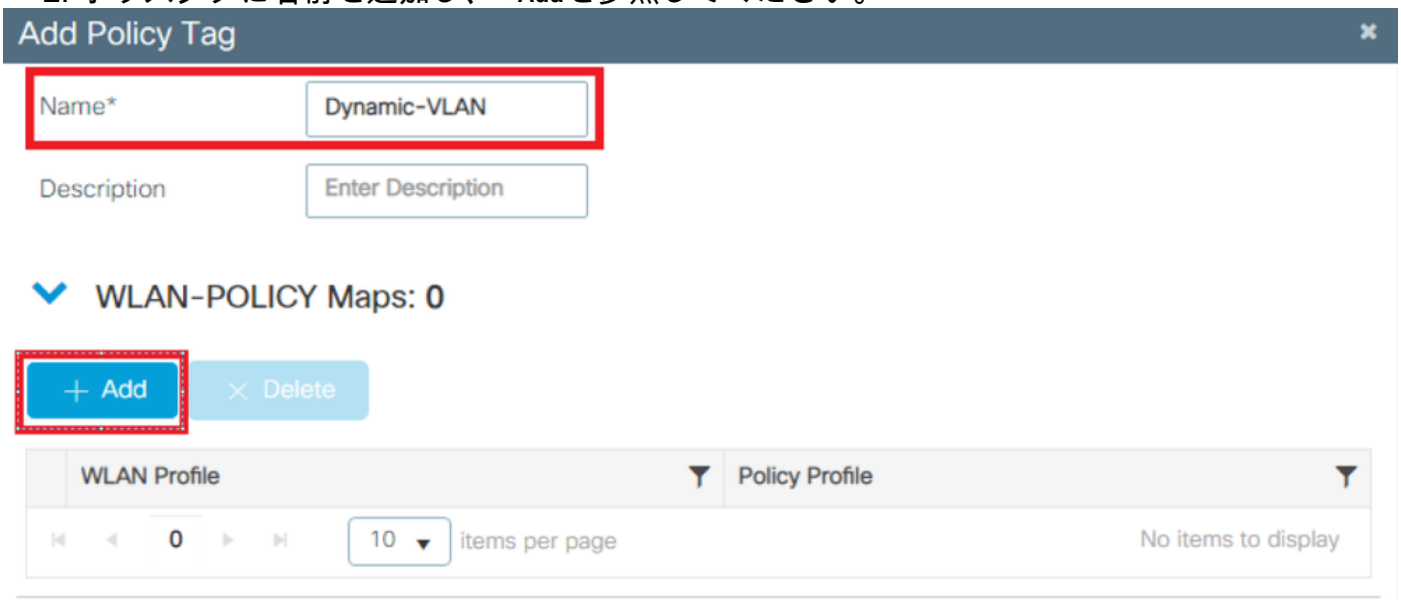
この手順では、WLCでポリスタグを設定する方法について説明します。

次のステップを実行します。

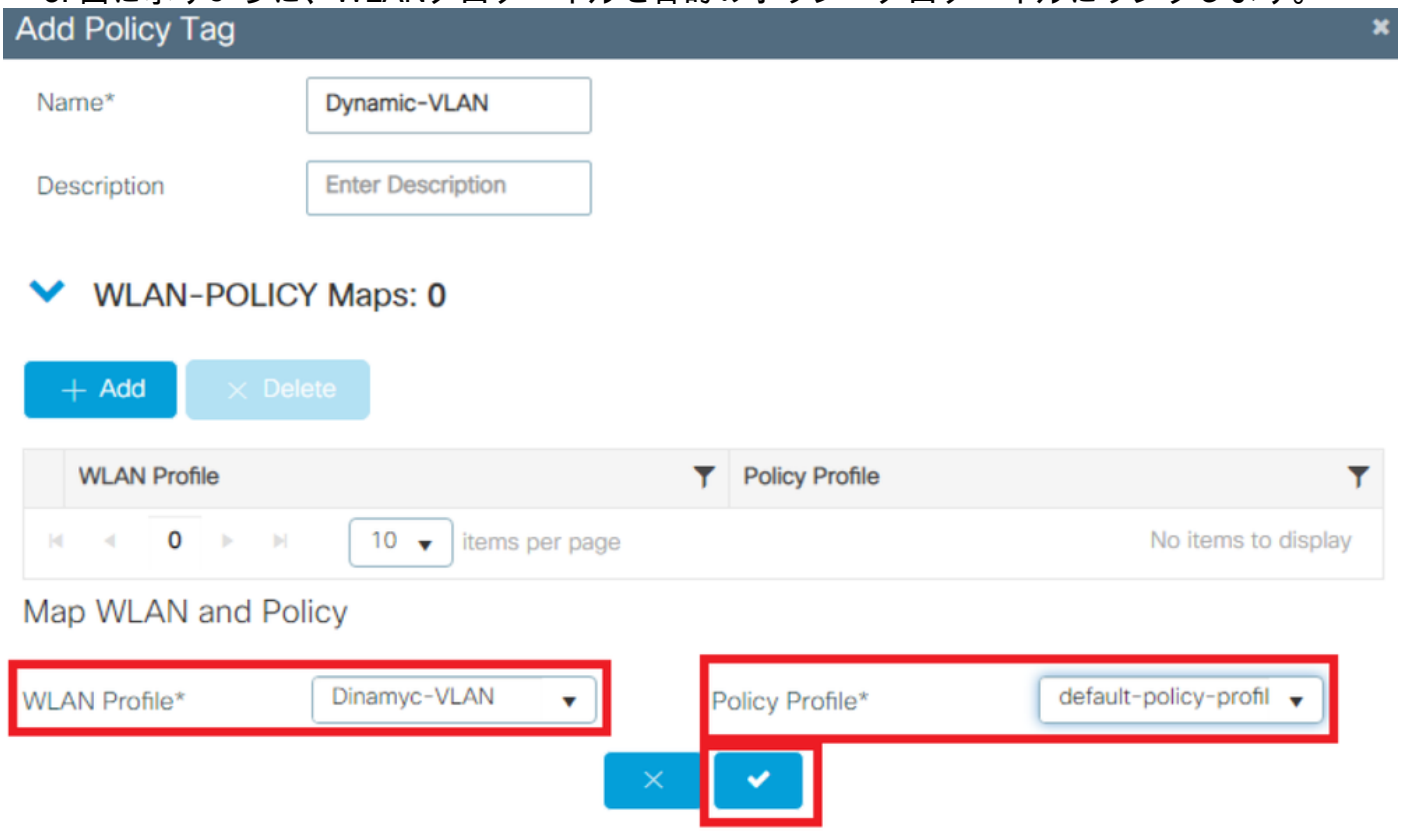
1. に移動 **Configuration > Tags & Profiles > Tags > Policy** 必要に応じて、図に示すように新しいオプションを追加します。

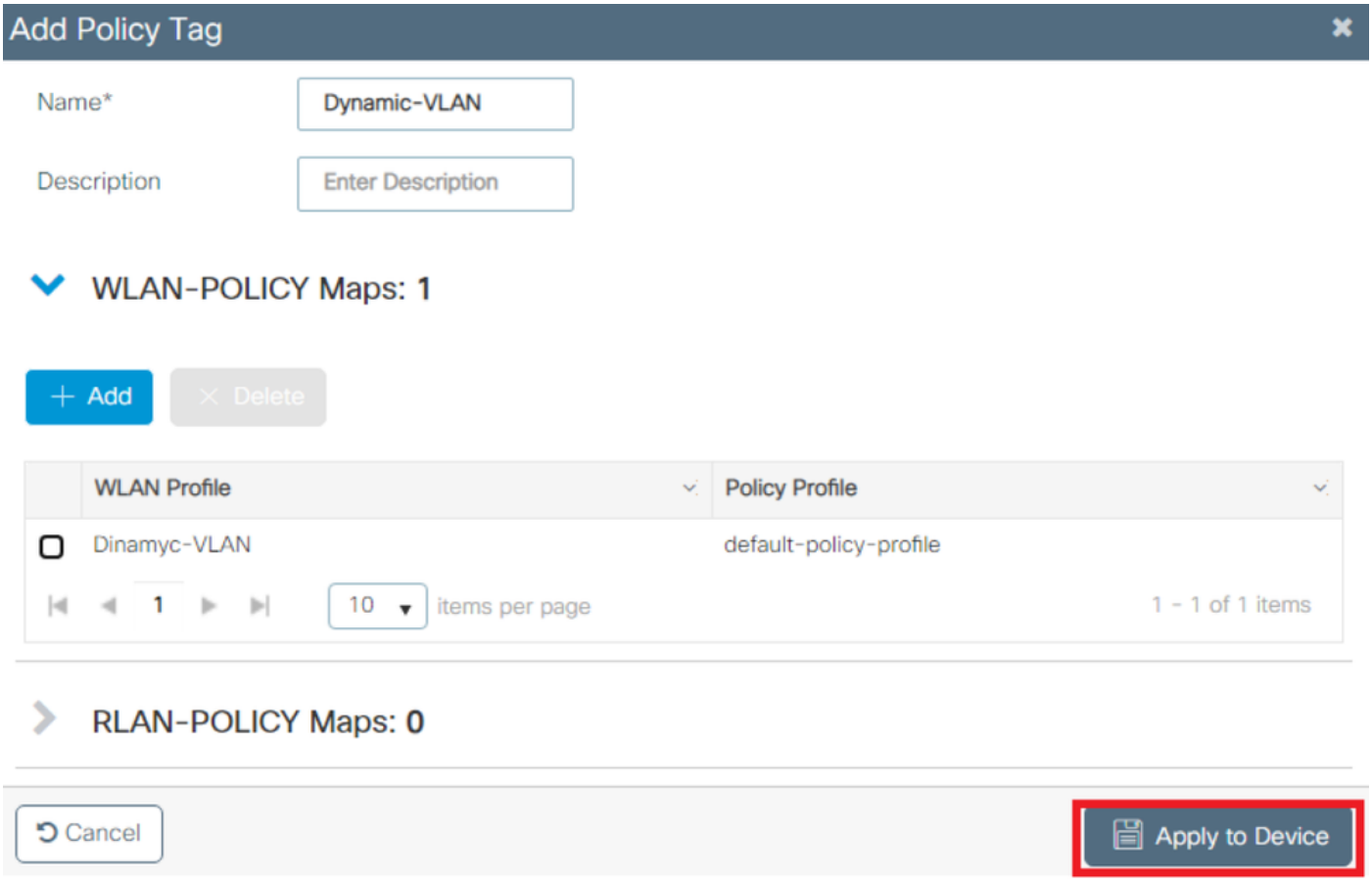


2. ポリスタグに名前を追加し、 **+Add**を参照してください。



3. 図に示すように、WLANプロファイルを目的のポリシープロファイルにリンクします。



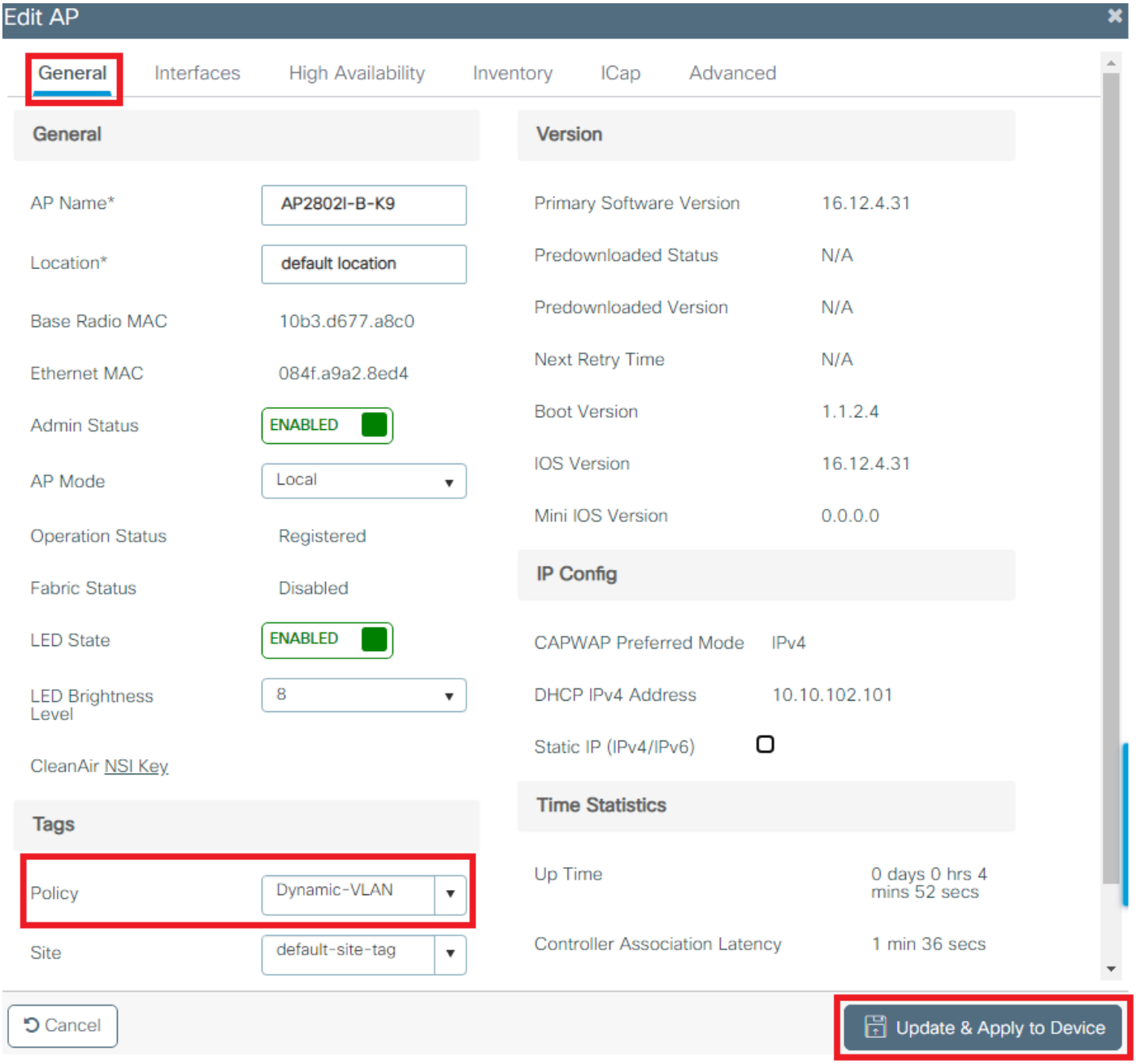


ステップ6:APへのポリスタグの割り当て

この手順では、WLCでポリスタグを設定する方法について説明します。

次のステップを実行します。

1. に移動 **Configuration > Wireless > Access Points > AP Name > General Tags** 関連するポリシータグを割り当て、 **Update & Apply to Device** 図に示すように



注意：APのポリシータグが変更されると、APはWLCへの関連付けを破棄し、再び加入することに注意してください。

確認

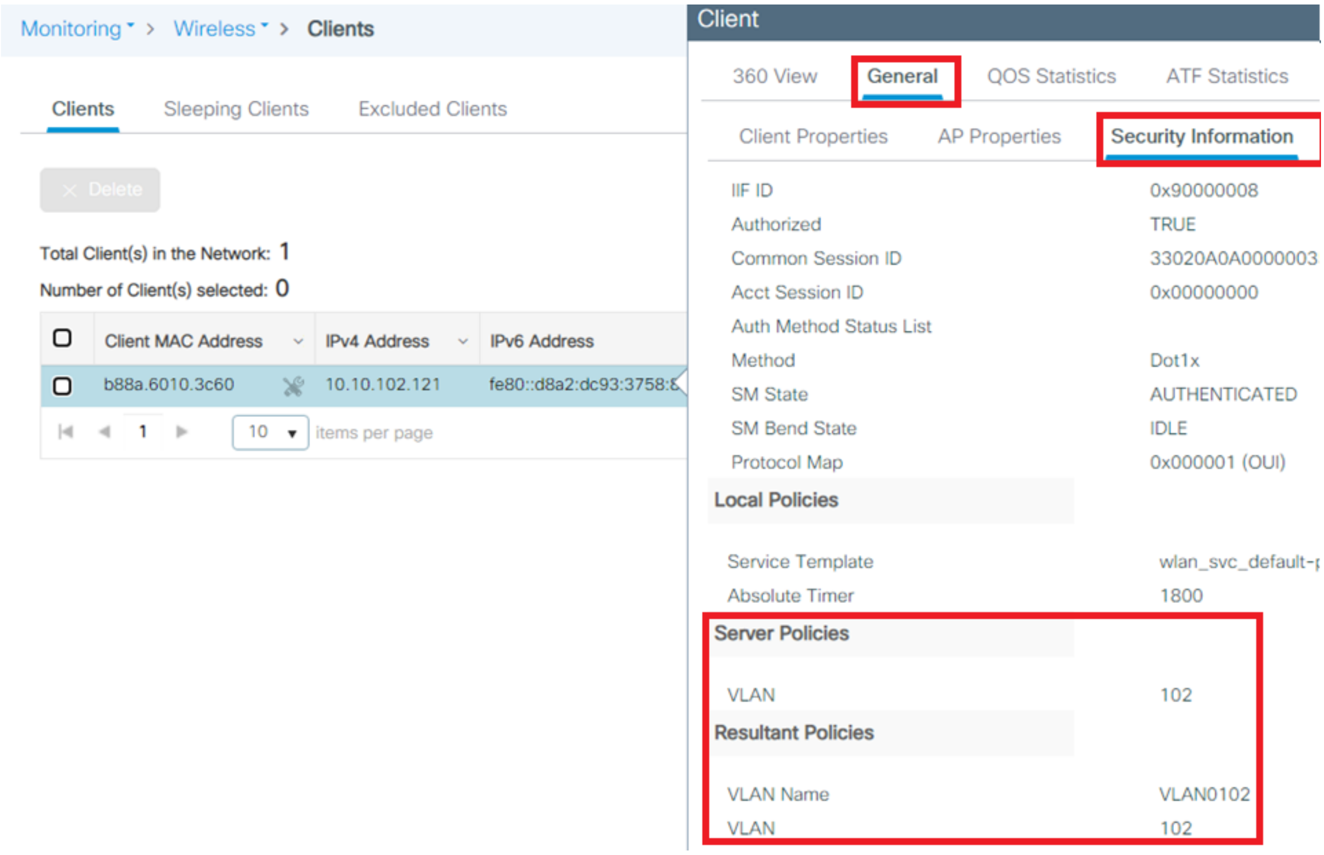
ここでは、設定が正常に機能しているかどうかを確認します。

Windows 10およびネイティブサプリカントとの接続をテストし、ユーザ名とパスワードの入力を求められたら、ISE上のVLANにマッピングされたユーザの情報を入力します。

前の例では、RADIUSサーバで指定されているように、jonathga-102がVLAN102に割り当てられています。この例では、次のユーザ名を使用して認証を受信し、RADIUSサーバによってVLANに割り当てられます。

認証が完了したら、送信されたRADIUS属性に従って、クライアントが適切なVLANに割り当てられていることを確認する必要があります。このタスクを実行するには、次の手順を実行します。

1. コントローラのGUIで、 **Monitoring > Wireless > Clients > Select the client MAC address > General > Security Information** 次の図に示すように、[VLAN]フィールドを探します。



このウィンドウから、RADIUSサーバに設定されているRADIUS属性に従って、このクライアントがVLAN102に割り当てられていることがわかります。CLIから、 **show wireless client summary detail** 図に示すように同じ情報を表示するには、次の手順を実行します。

```
Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1

MAC Address    SSID                AP Name             State        IP Address                        Device-type        VLAN
BSSID          Auth Method         Created    Connected Protocol Channel Width  SGI NSS Rate  CAP  Username
---------------------------------------------------------------------------------------------------------------------------------
[redacted]10.3c60 Dinamyc-VLAN        AIR-AP2802I-A-K9    Run          10.10.105.200                     Intel-Device       105
[redacted]44.4000 [802.1x]            05         06       11n(2.4) 1    20/20  Y/Y 1/1 24.0  E   jonathga-105
```

```
Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1

MAC Address    SSID                AP Name             State        IP Address                        Device-type        VLAN
BSSID          Auth Method         Created    Connected Protocol Channel Width  SGI NSS Rate  CAP  Username
---------------------------------------------------------------------------------------------------------------------------------
[redacted]10.3c60 Dinamyc-VLAN        AIR-AP2802I-A-K9    Run          10.10.102.121                     Intel-Device       102
[redacted]44.4000 [802.1x]            54         55       11n(2.4) 1    20/20  Y/Y 1/1 m5    E   jonathga-102
```

2. この場合は、 **Radioactive traces** RADIUS属性がWLCに正常に転送されるようにします。そのためには、次の手順を実行します。 コントローラのGUIで、 **Troubleshooting > Radioactive Trace > +Add.**ワイヤレスクライアントのMACアドレスを入力します。選択 **Start.**クライアントをWLANに接続します。に移動 **Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log.**

トレース出力のこの部分は、RADIUS属性の正常な送信を保証します。

```
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id
1812/60 10.10.1.24:0, Access-Accept, len 352
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  authenticator e5 5e
```

```
58 fa da 0a c7 55 - 53 55 7d 43 97 5a 8b 17
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  User-Name
[1]     13  "jonathga-102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  State
[24]    40  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Class
[25]    54  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Type
       [64]     6  VLAN                    [13]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Medium-Type
[65]     6  ALL_802                [6]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  EAP-Message
[79]     6  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Message-
Authenticator[80]    18  ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  Tunnel-Private-
Group-Id[81]     6  "102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:  EAP-Key-Name
 [102]   67  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Send-Key
[16]    52  *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS:   MS-MPPE-Recv-Key
[17]    52  *
2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method
name: PEAP on handle 0x0C000008

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:            username   0 "jonathga-102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:               class   0 43 41 43 53 3a 33 33 30 32 30 41 30 41 30 30 30 30 30 30 33 35 35 36
45 32 32 31 36 42 3a 49 53 45 2d 32 2f 33 39 33 33 36 36 38 37 32 2f 31 31 32 36 34 30  ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:         tunnel-type   1 13 [vlan] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute :
tunnel-medium-type   1 6 [ALL_802] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:tunnel-private-group-id   1 "102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:             timeout   0 1800 (0x708) ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [25253]: (info):
[0000.0000.0000:unknown] AAA override is enabled under policy profile
```

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

- エンドユーザガイド