Catalyst 9800ワイヤレスLANコントローラでのメッシュの設定

内容

はじめに
前提条件
- 要件
- 使用するコンポーネント

設定
- ケーススタディ1：ブリッジモード
  - コンフィギュレーション
  - 確認
  - トラブルシュート
- ケーススタディ2:Flex +ブリッジ
  - 設定
  - 確認
  - トラブルシュート

はじめに

このドキュメントでは、メッシュアクセスポイント(AP)をCatalyst 9800ワイヤレスLANコントローラ(WLC)に加入させる方法の基本的な設定例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ることが推奨されます。

- Catalyst Wireless 9800設定モデル
- LAPの設定
- Control And Provision of Wireless Access Points(CAPWAP)
- 外部 DHCP サーバの設定
- Ciscoスイッチの設定

使用するコンポーネント

この例では、Catalyst 9800 WLCに加入するためにルートAP(RAP)またはメッシュAP(MAP)として設定できるLightweightアクセスポイント（1572APおよび1542）を使用します。手順は1542または1562のアクセスポイントで同じです。RAPは、Cisco Catalystスイッチを介してCatalyst 9800 WLCに接続されます。

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。

- C9800-CL v16.12.1
- Cisco レイヤ 2 スイッチ
- Cisco Aironet 1572シリーズLightweightブリッジ用屋外アクセスポイントのセクション
- Flex+Bridgeセクション用Cisco Aironet 1542

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、クリアな（デフォルト）設定で作業を開始しています。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

ケーススタディ1：ブリッジモード

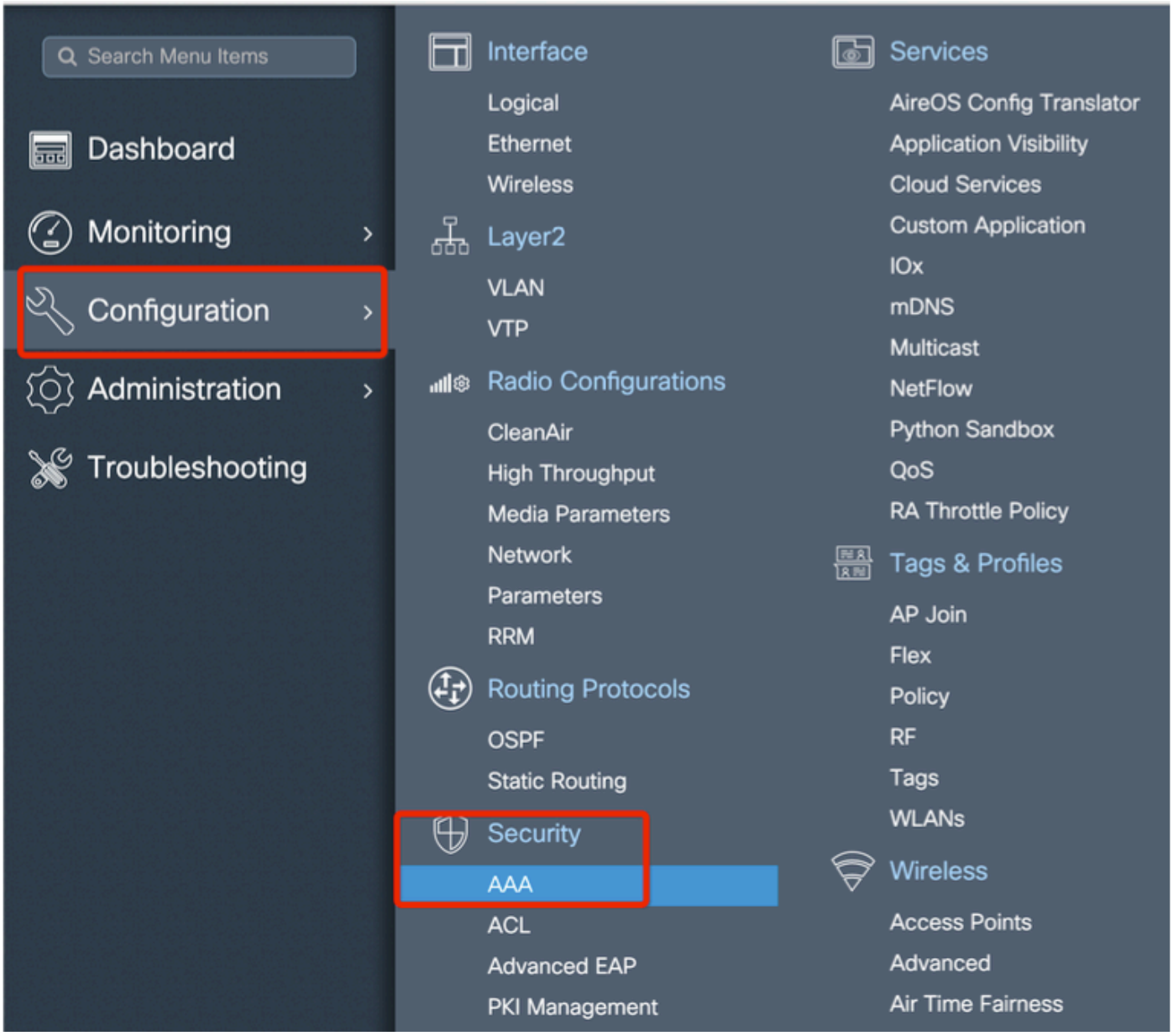
コンフィギュレーション

メッシュAPは、9800コントローラに加入するために認証される必要があります。このケーススタディでは、最初にローカルモードでAPをWLCに加入させ、次にAPをブリッジ（別名）メッシュモードに変換することを検討します。

AP加入プロファイルの割り当てを回避するには、この例を使用しますが、任意のメッシュAPがコントローラに加入できるように、デフォルトのaaa authorization credential-download methodを設定します。

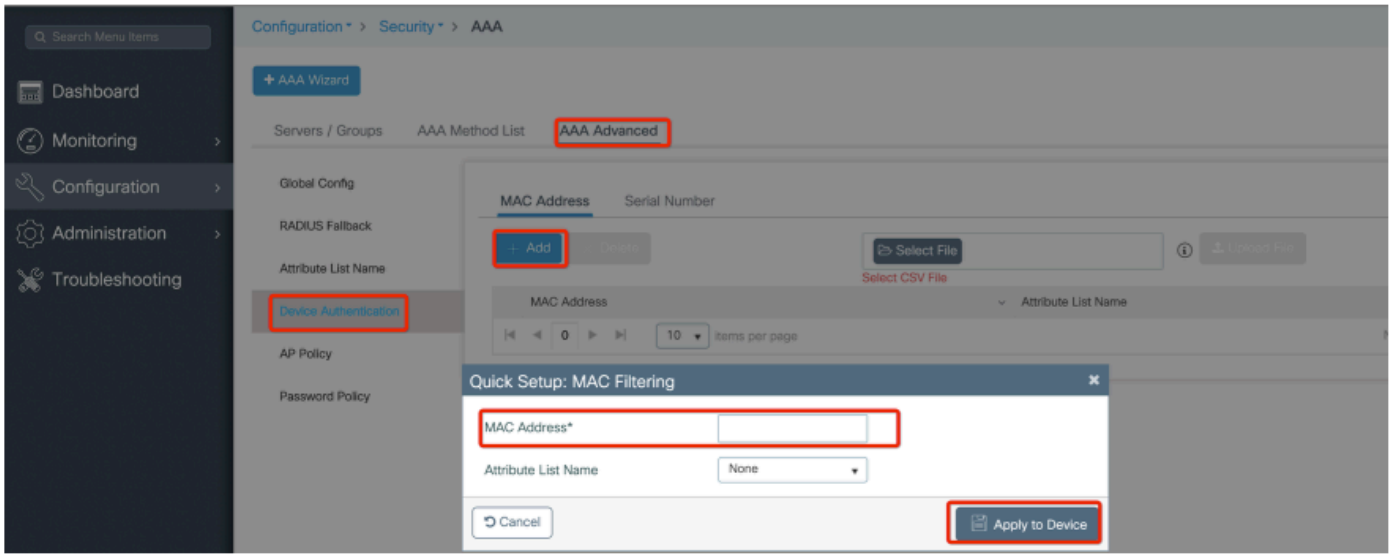
手順1:デバイス認証でRAP/MAP MACアドレスを設定します。

Configuration > AAA > AAA Advanced > Device Authenticationの順に選択します。



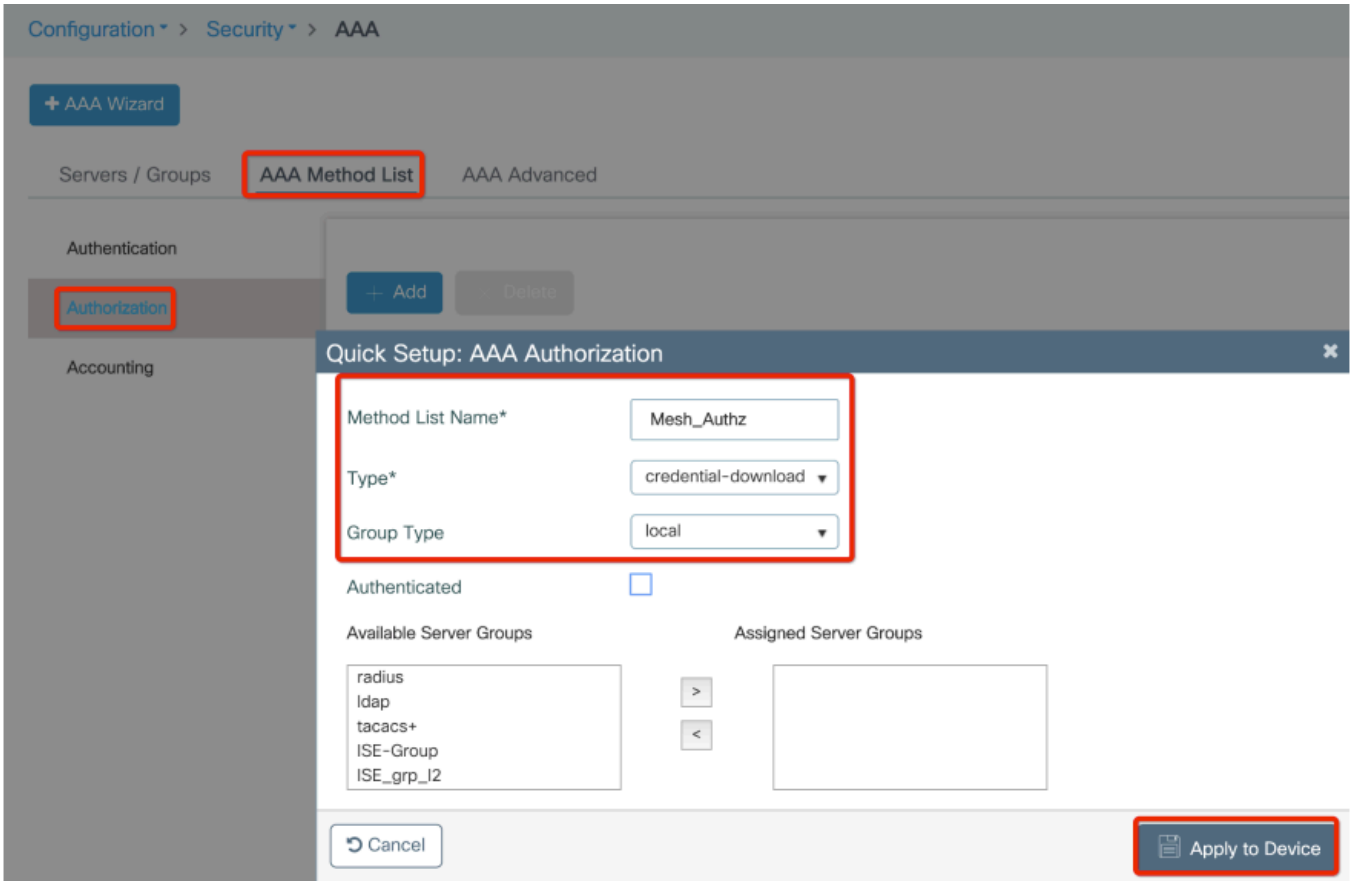
メッシュアクセスポイントのベースイーサネットMACアドレスを追加し、特殊文字（「。」または「:」）を付けずに追加します。

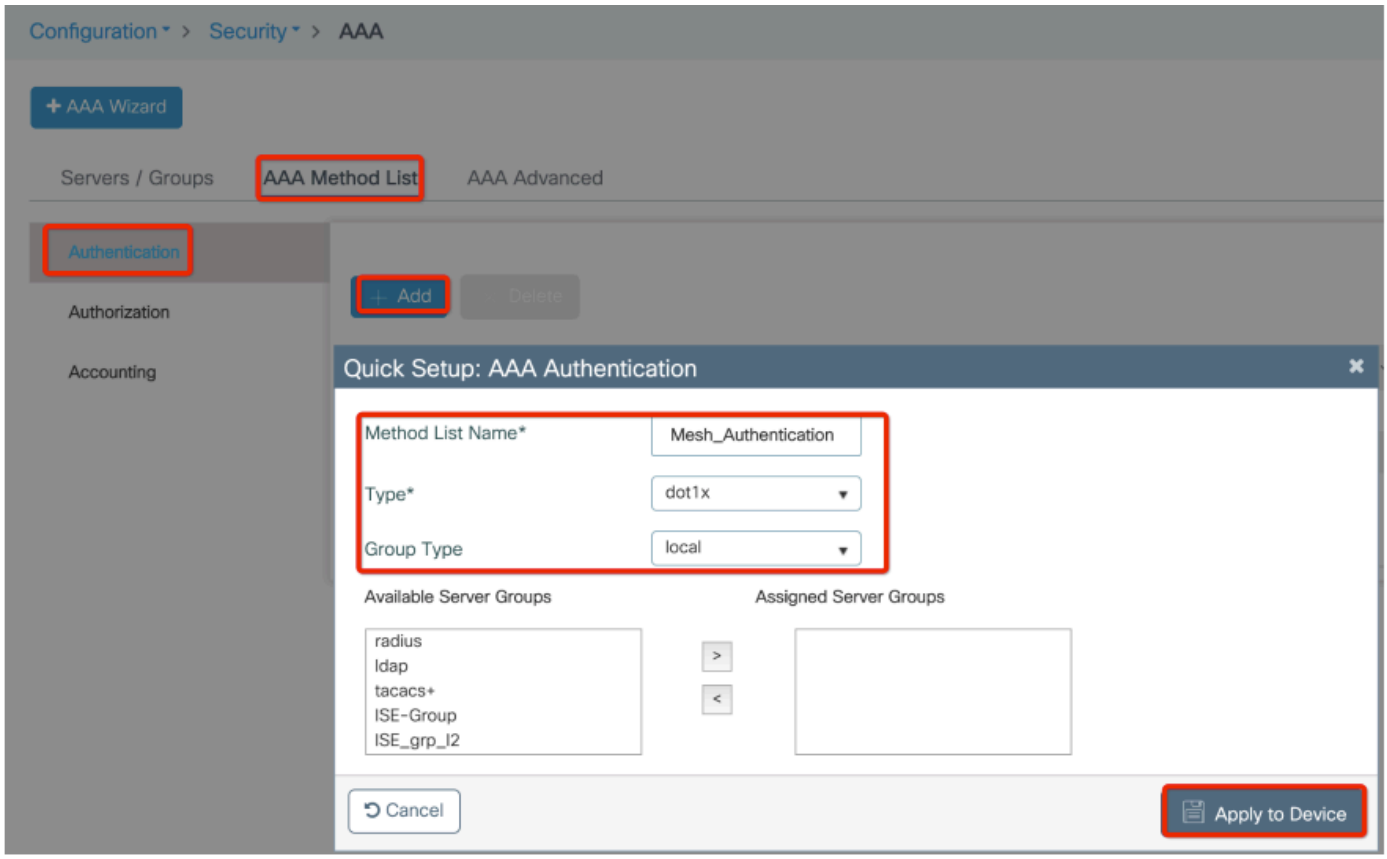
重要:17.3.1リリース以降では、「。」、「:」、「 – 」などのMACアドレス区切り文字が追加されると、APは加入できなくなります。これに対して、現在2つの機能拡張が公開されています。Cisco Bug ID CSCvv43870とCisco Bug ID CSCvr07920です。将来的には、9800はすべてのMACアドレス形式を受け入れます。



ステップ2:認証および許可方式リストを設定します。

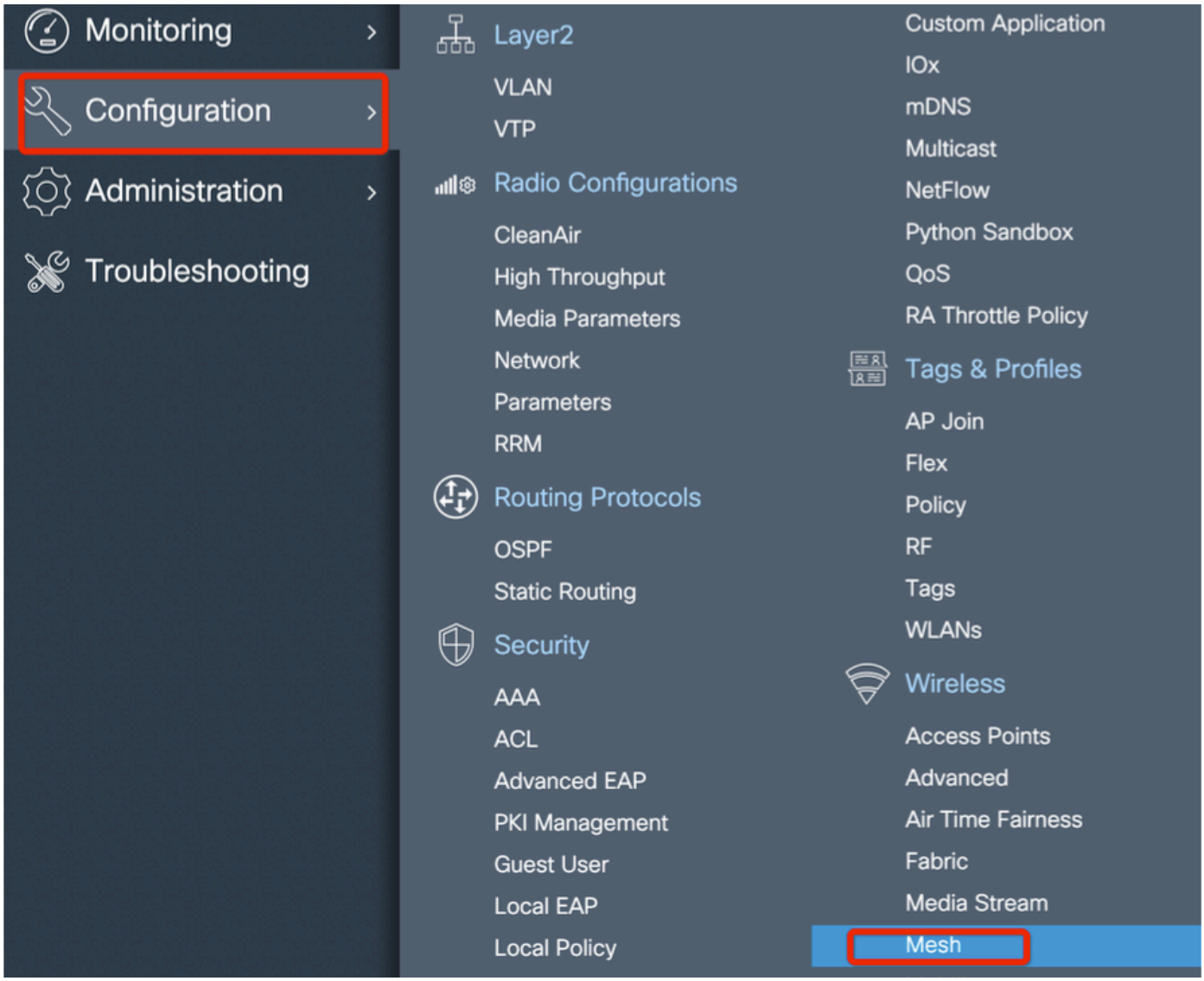
Configuration > Security > AAA > AAA Method list > Authenticationの順に選択し、認証方式リストと許可方式リストを作成します。



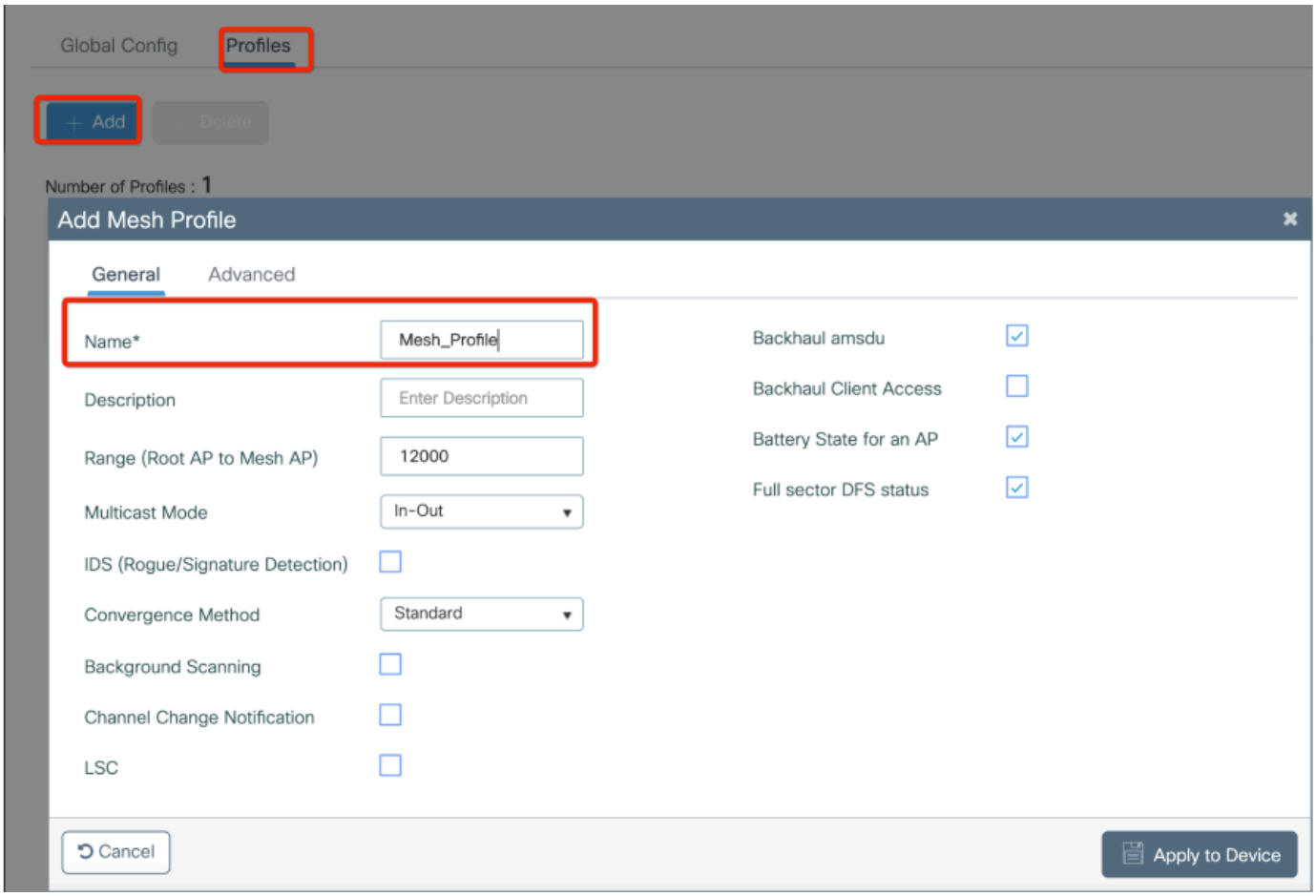


ステップ3:グローバルメッシュパラメータを設定します。

Configuration> Mesh> Globalの順に選択します。最初は、これらの値をデフォルトのままにしておくことができます。

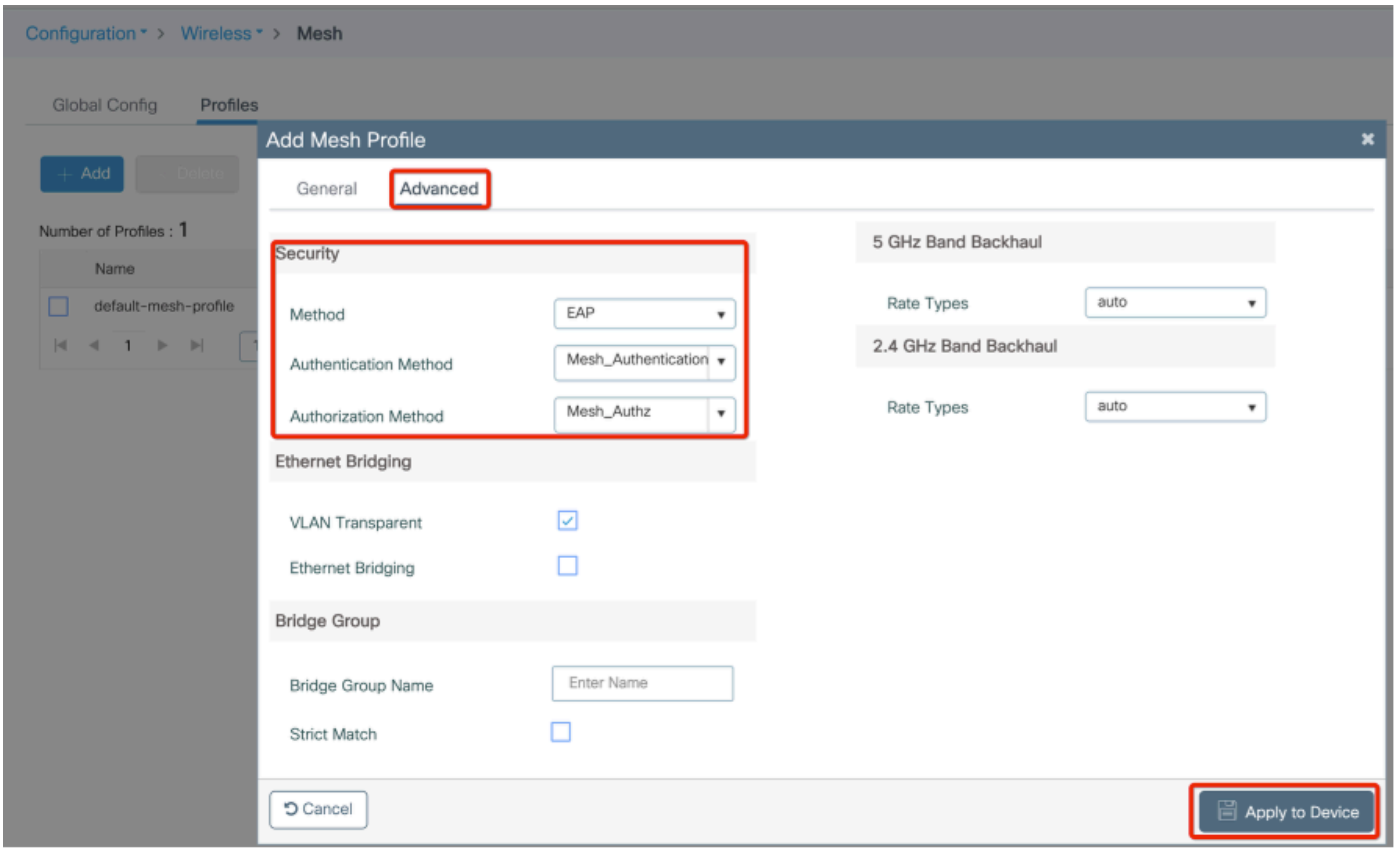


ステップ4:Configuration > Mesh > Profile > +Addで新しいメッシュプロファイルを作成します。

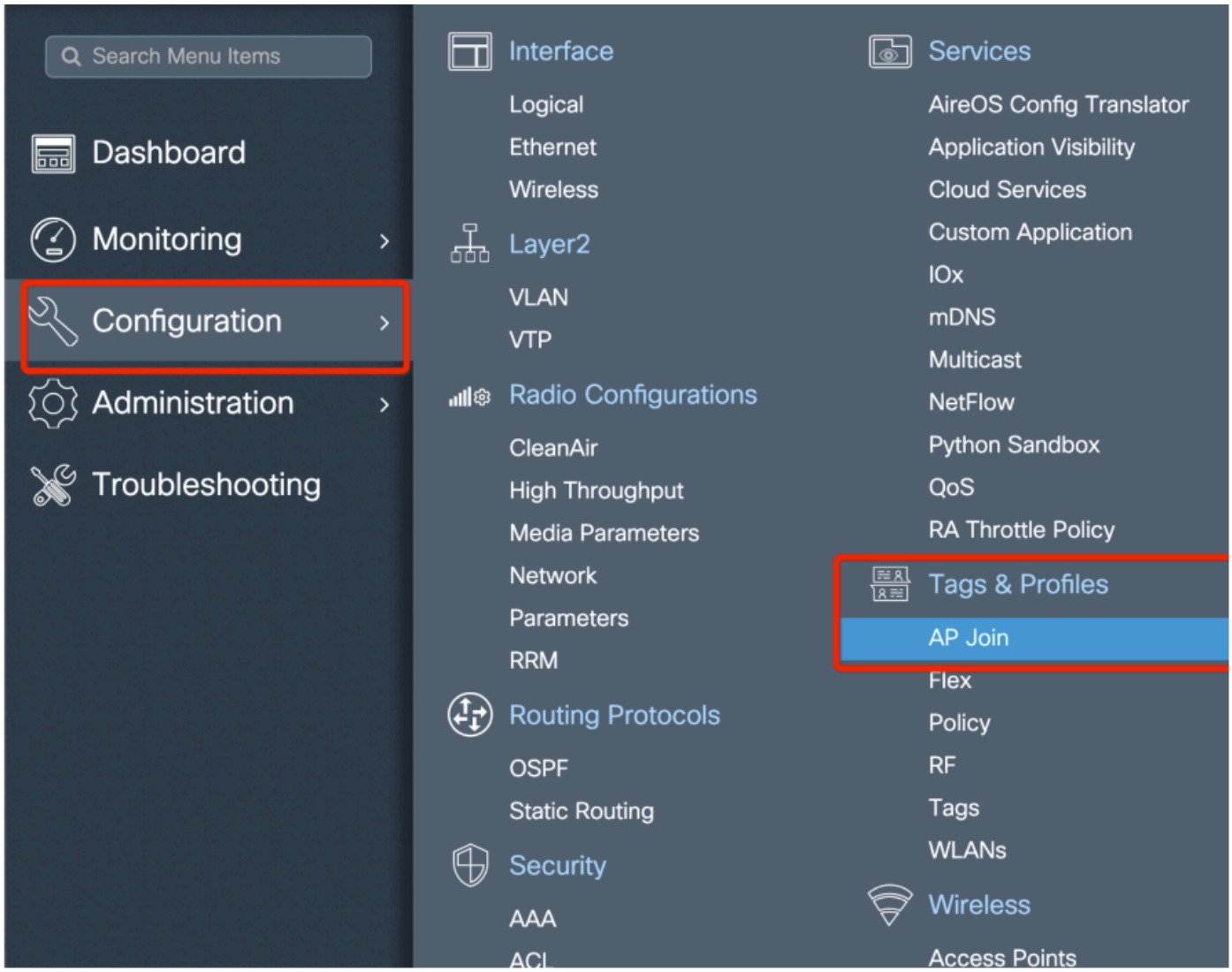


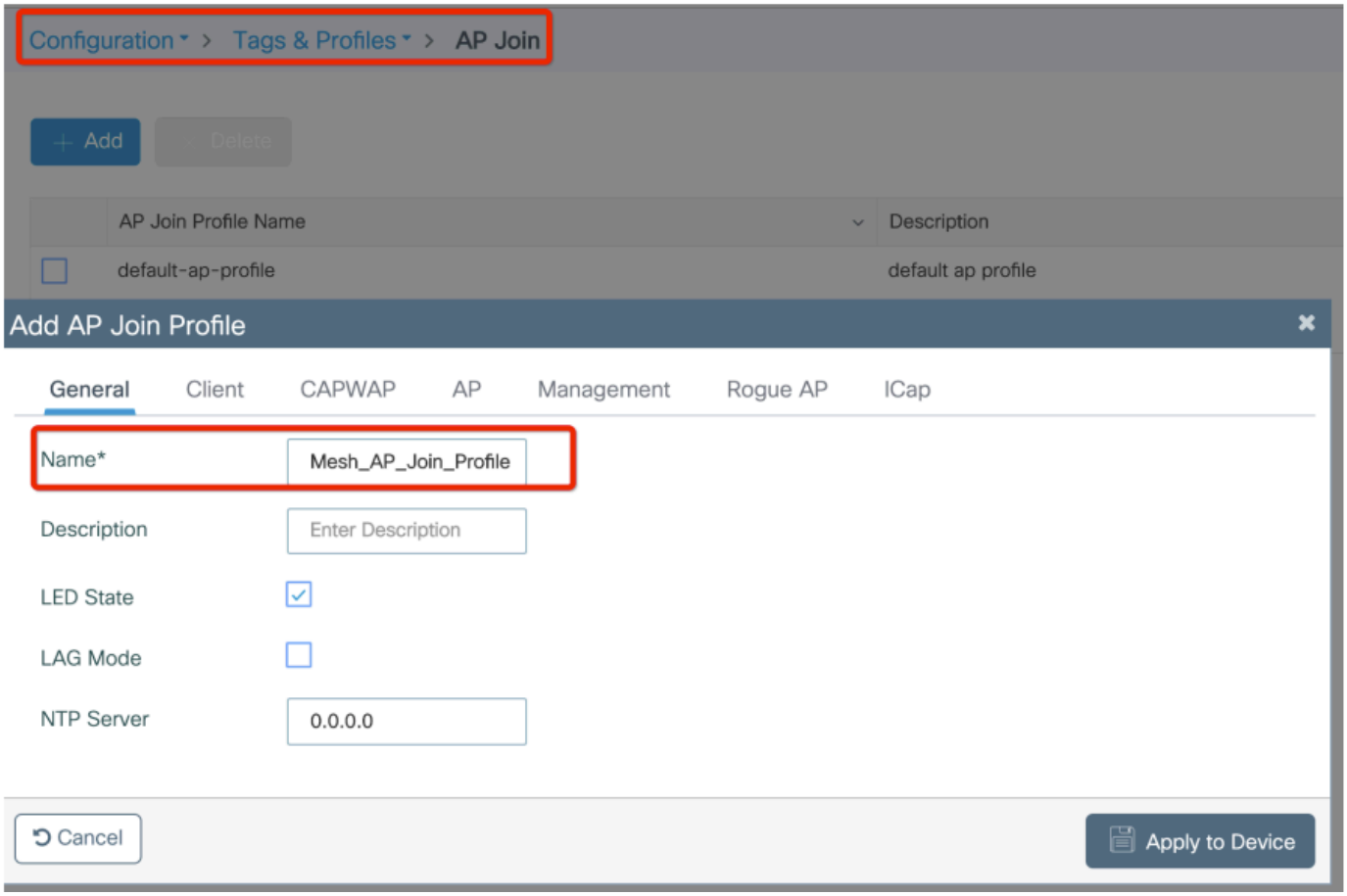
作成したメッシュプロファイルをクリックして、メッシュプロファイルのGeneralおよびAdvanced設定を編集します。

図では、前に作成した認証および認可プロファイルをメッシュプロファイルにマッピングする必要があります

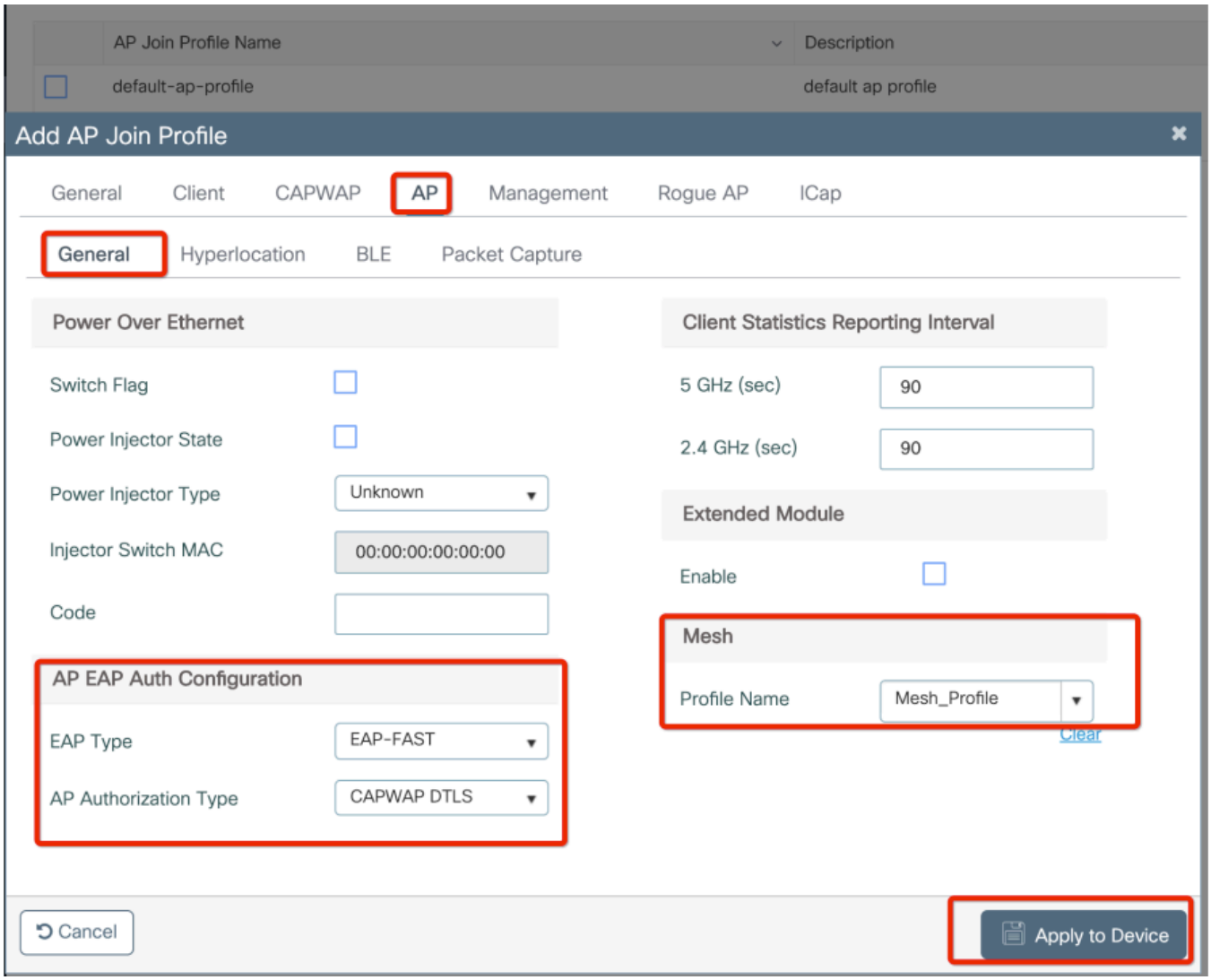


ステップ5:新しいAP加入プロファイルを作成します。Configure > Tags and Profiles: AP Joinの順に選択します。

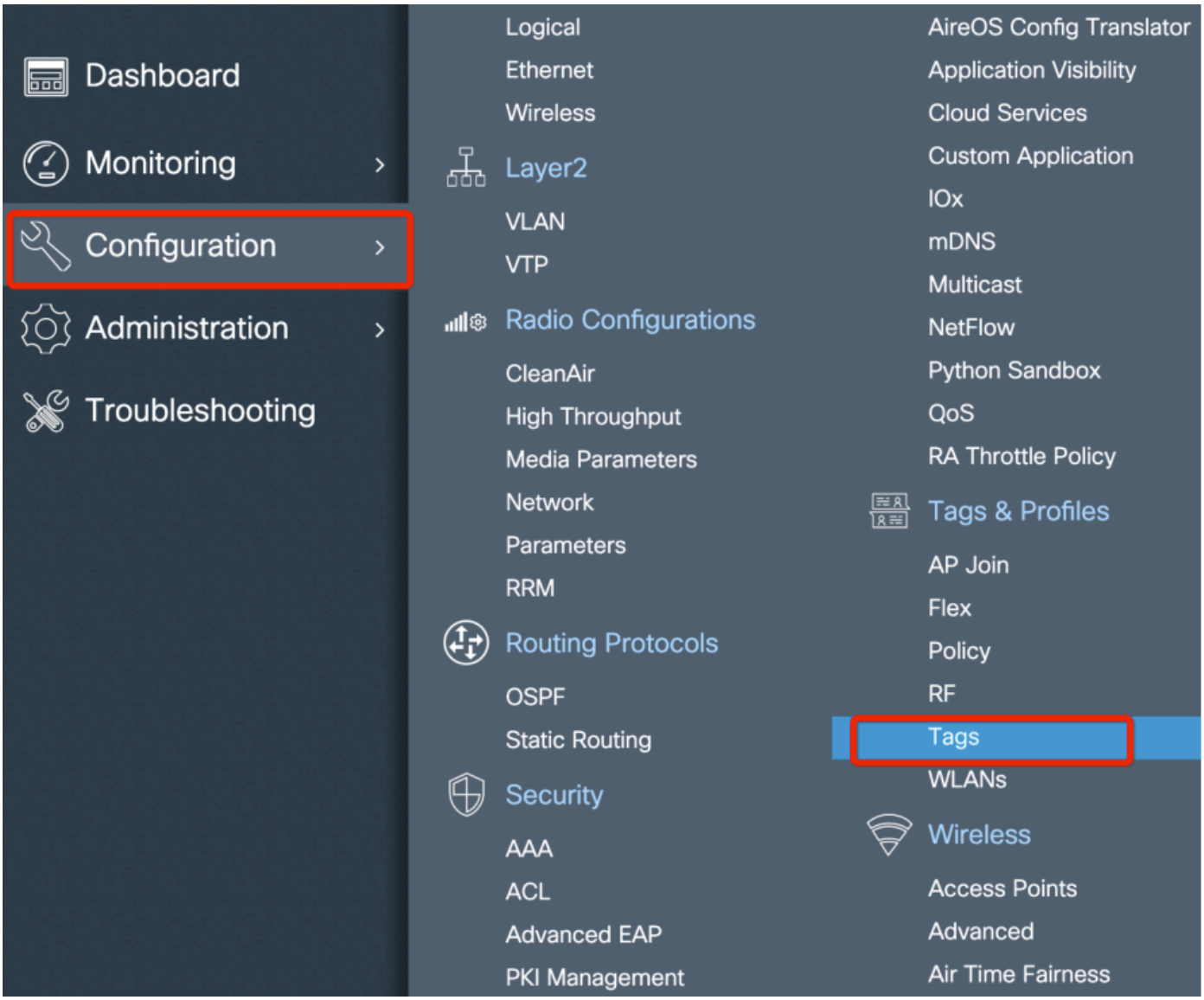

Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Interface
Logical
Ethernet
Wireless
Layer2
VLAN
VTP
Radio Configurations
CleanAir
High Throughput
Media Parameters
Network
Parameters
RRM
Routing Protocols
OSPF
Static Routing
Security
AAA
ACL
Services
AireOS Config Translator
Application Visibility
Cloud Services
Custom Application
IOx
mDNS
Multicast
NetFlow
Python Sandbox
QoS
RA Throttle Policy
Tags & Profiles
AP Join
Flex
Policy
RF
Tags
WLANs
Wireless
Access Points



以前に設定したメッシュプロファイルを適用し、AP EAP認証を設定します。

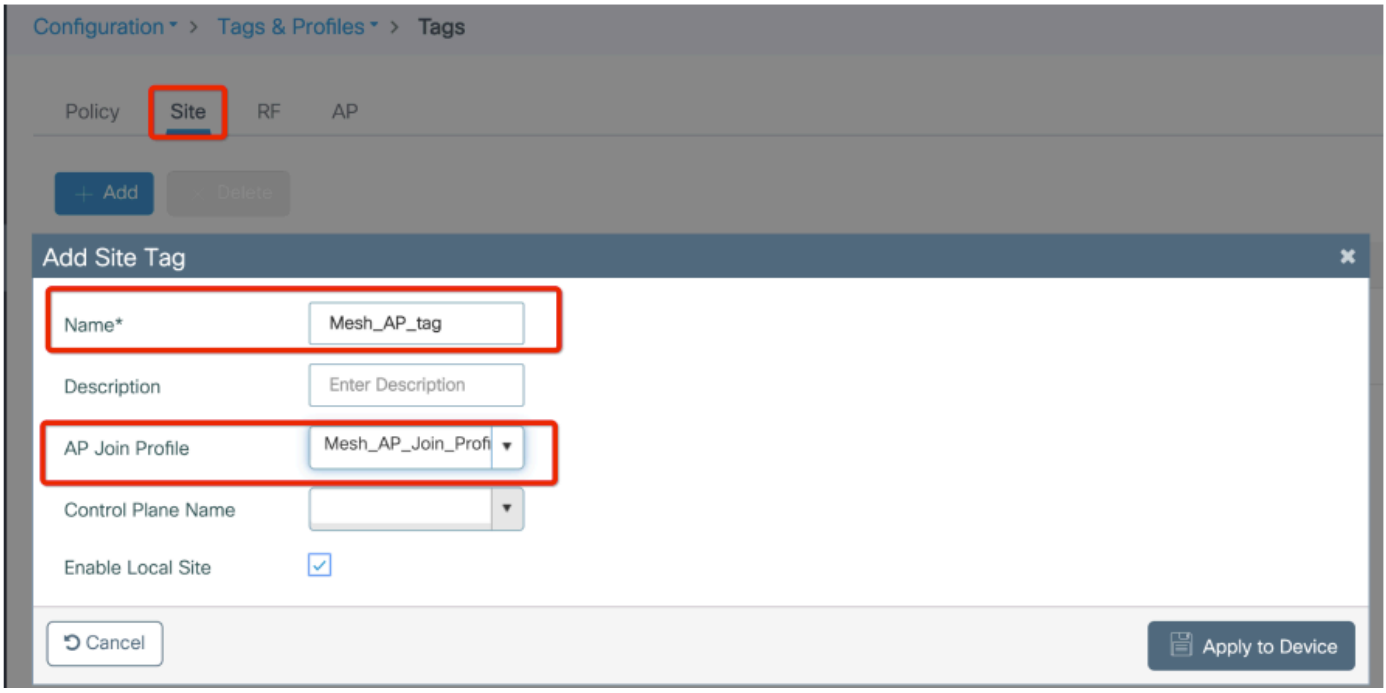


ステップ6:図のように、メッシュ位置タグを作成します。

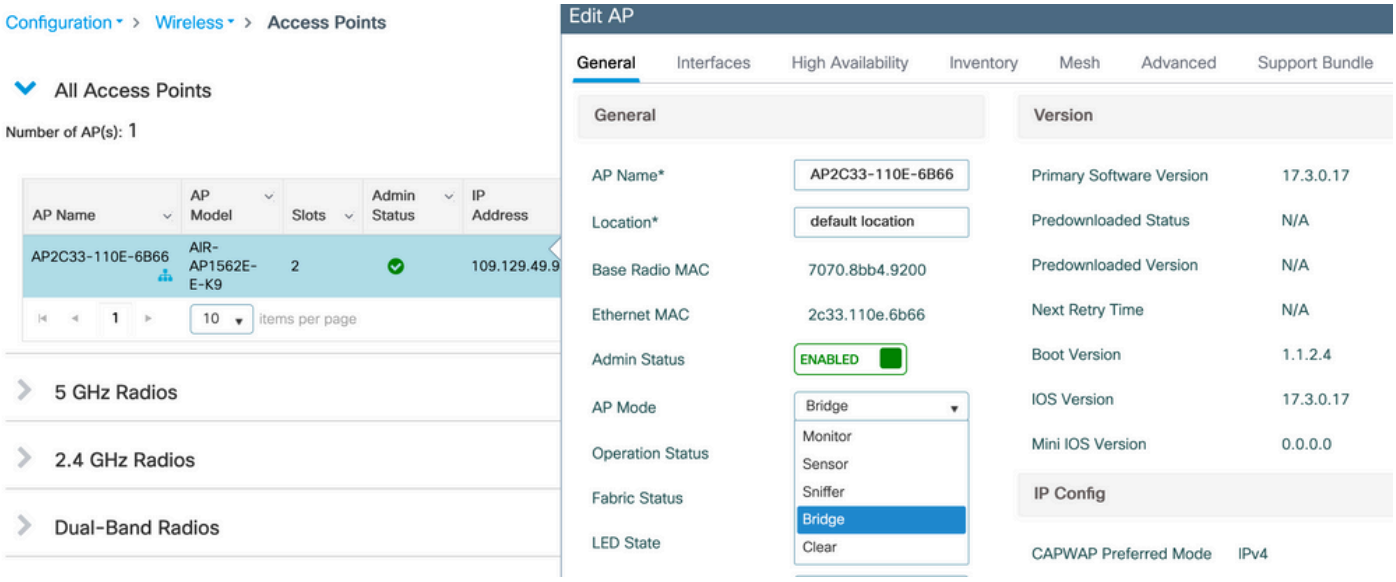


設定ステップ6で作成したメッシュ位置タグをクリックして設定します。

Got to Siteタブで、以前に設定したメッシュAP加入プロファイルを適用します。



手順 7：APをブリッジモードに変換します。



cliを使用して、APで次のコマンドを実行できます。

```
capwap ap mode bridge
```

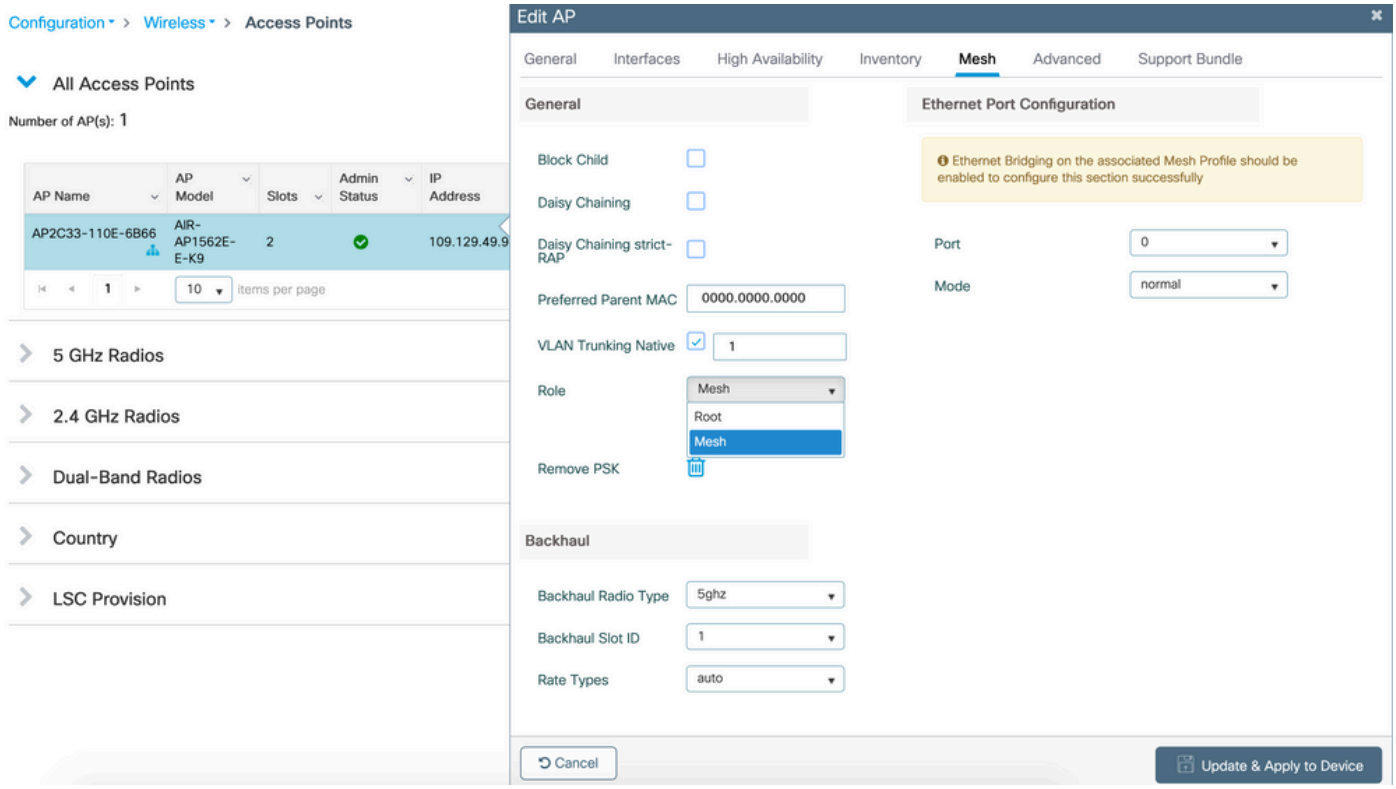
APがリブートし、ブリッジモードで復帰します。

ステップ 8：APのロール（ルートAPまたはメッシュAP）を定義できるようになりました。

ルートAPはWLCへの有線接続を行うAPですが、メッシュAPはルートAPへの接続を試行する無線を介してWLCに参加します。

メッシュAPは、プロビジョニングの目的で、無線を介してルートAPを見つけることに失敗すると、有線インターフェイスを介してWLCに参加できます。

デフォルトのVLAN 1と異なる場合は、AP設定でトランクのネイティブVLANを必ず指定してください

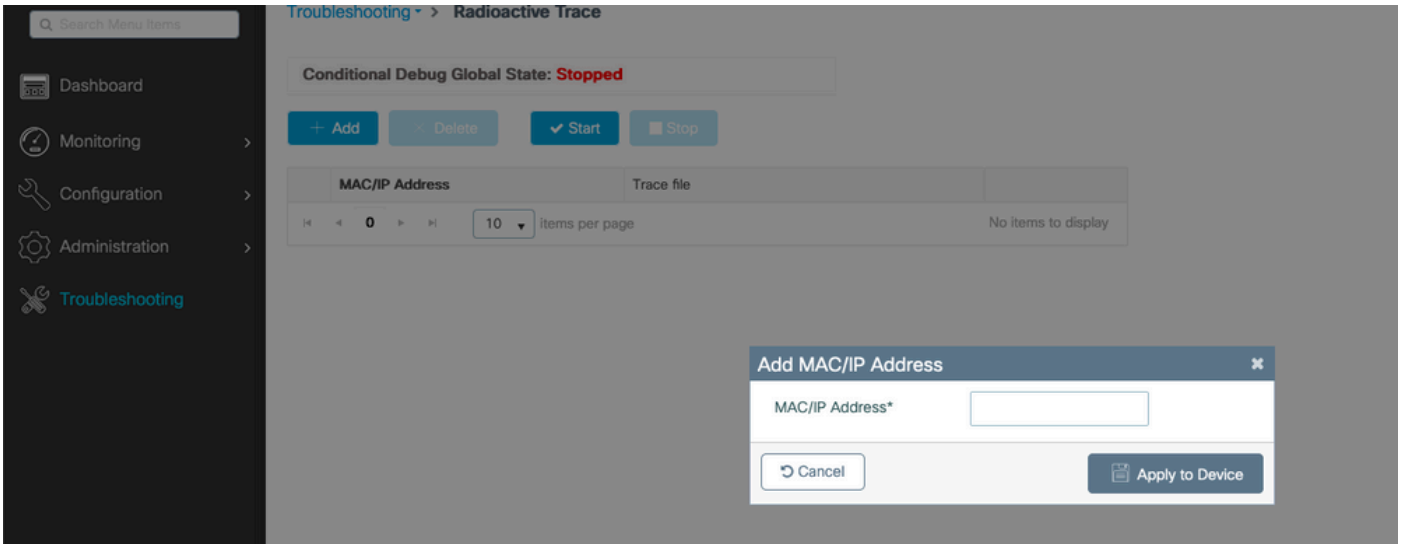


確認

```
aaa new-model
aaa local authentication default authorization default
!
!
aaa authentication dot1x default local
aaa authentication dot1x Mesh_Authentication local
aaa authorization network default local
aaa authorization credential-download default local
aaa authorization credential-download Mesh_Authz local
username 111122223333 mac
wireless profile mesh Mesh_Profile
 method authentication Mesh_Authentication
 method authorization Mesh_Authz
wireless profile mesh default-mesh-profile
 description "default mesh profile"
wireless tag site Mesh_AP_Tag
 ap-profile Mesh_AP_Join_Profile
ap profile Mesh_AP_Join_Profile
 hyperlocation ble-beacon 0
 hyperlocation ble-beacon 1
 hyperlocation ble-beacon 2
 hyperlocation ble-beacon 3
 hyperlocation ble-beacon 4
 mesh-profile Mesh_Profile
```

トラブルシュート

Troubleshoot > Radioactive Trace Web UIページでaddをクリックし、APのMACアドレスを入力します。



Startをクリックし、APがコントローラへの加入を再試行するまで待機します。

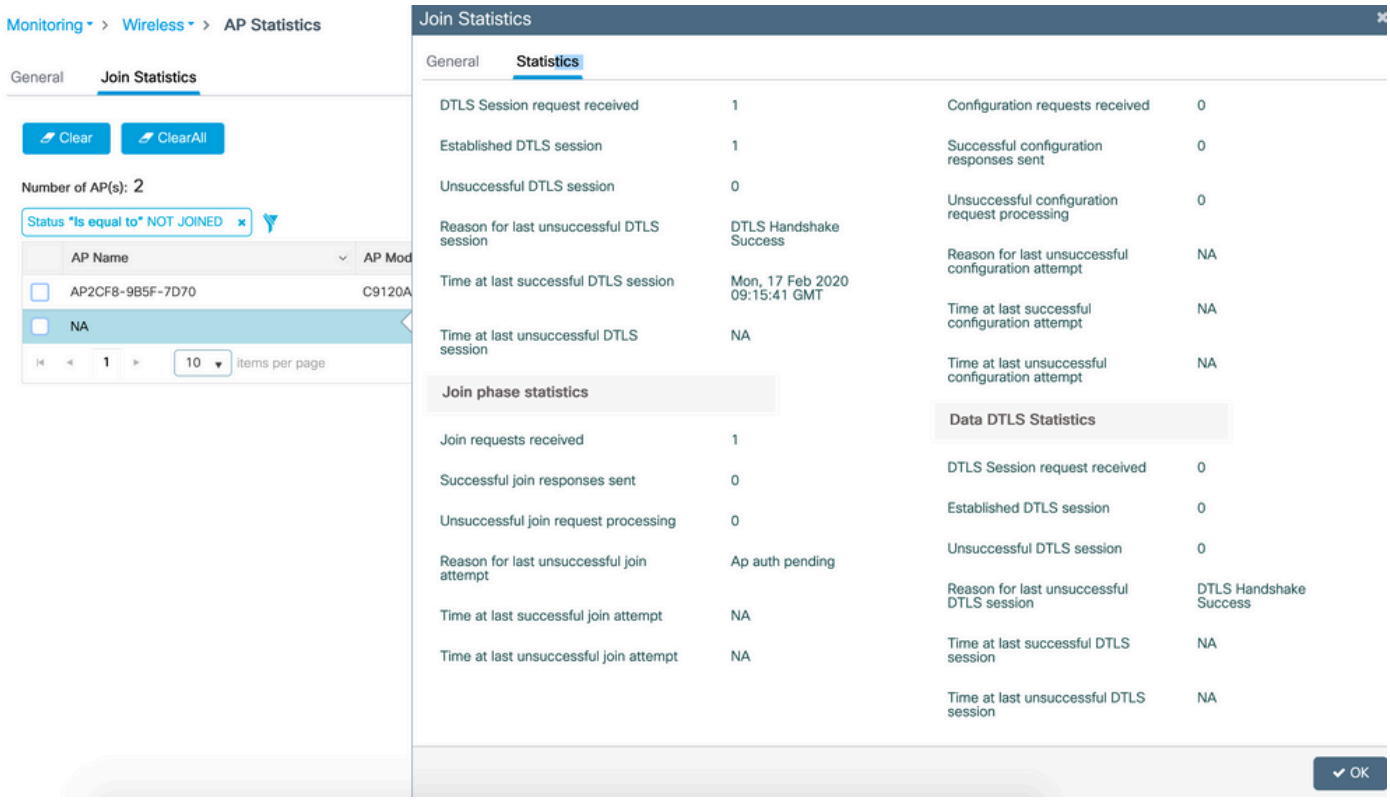
完了したら、Generateをクリックして、ログを収集する期間を選択します（過去10分または30分など）。

トレースファイル名をクリックして、ブラウザからダウンロードします。

次に、誤ったaaa認可方式の名前が定義されたために加入していないAPの例を示します。

```
019/11/28 13:08:38.269 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [23388]: (info): DTLS record type: 23, appli
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (info): 00a3.8e95.6c40 Ap auth p
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): Failed to initialize auth
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): 00a3.8e95.6c40 Auth reque
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get wtp r
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get ap ta
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (ERR): Session-IP: 192.168.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (info): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.
2019/11/28 13:08:38.289 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [23038]: (debug): instance :0 port:38932MAC
```

Web UIダッシュボードで未参加のAPをクリックすると、同じことが簡単に確認できます。「Ap auth pending」は、AP自体の認証をポイントするヒントです。

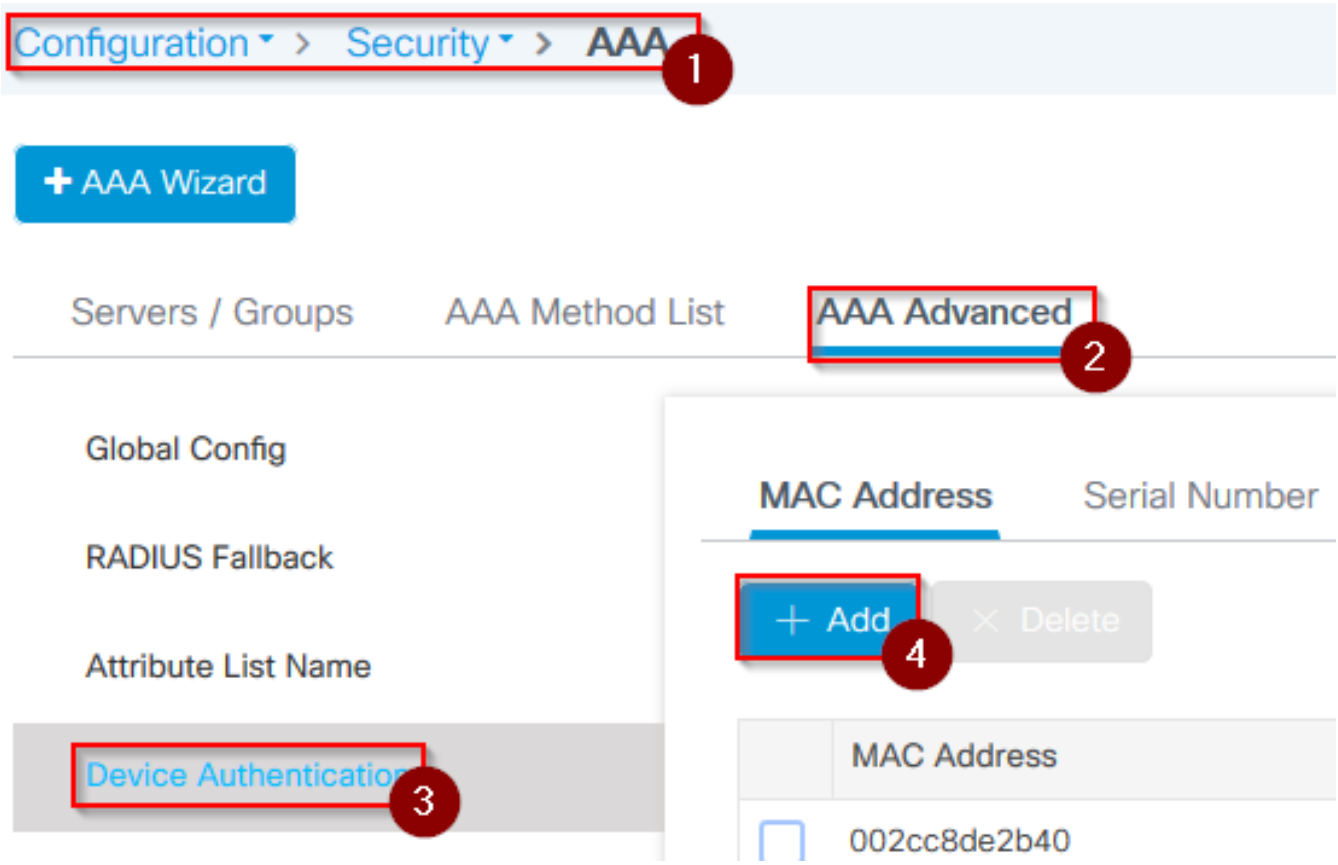


ケーススタディ2:Flex +ブリッジ

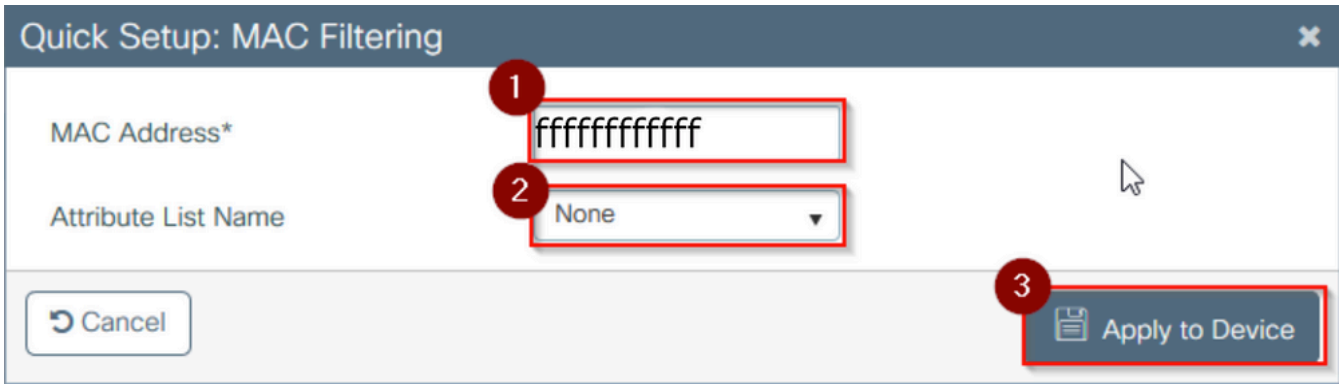
このセクションでは、WLCでローカルに実行されるEAP認証を使用したFlex+ブリッジモードでの1542 APの加入プロセスについて説明します。

設定

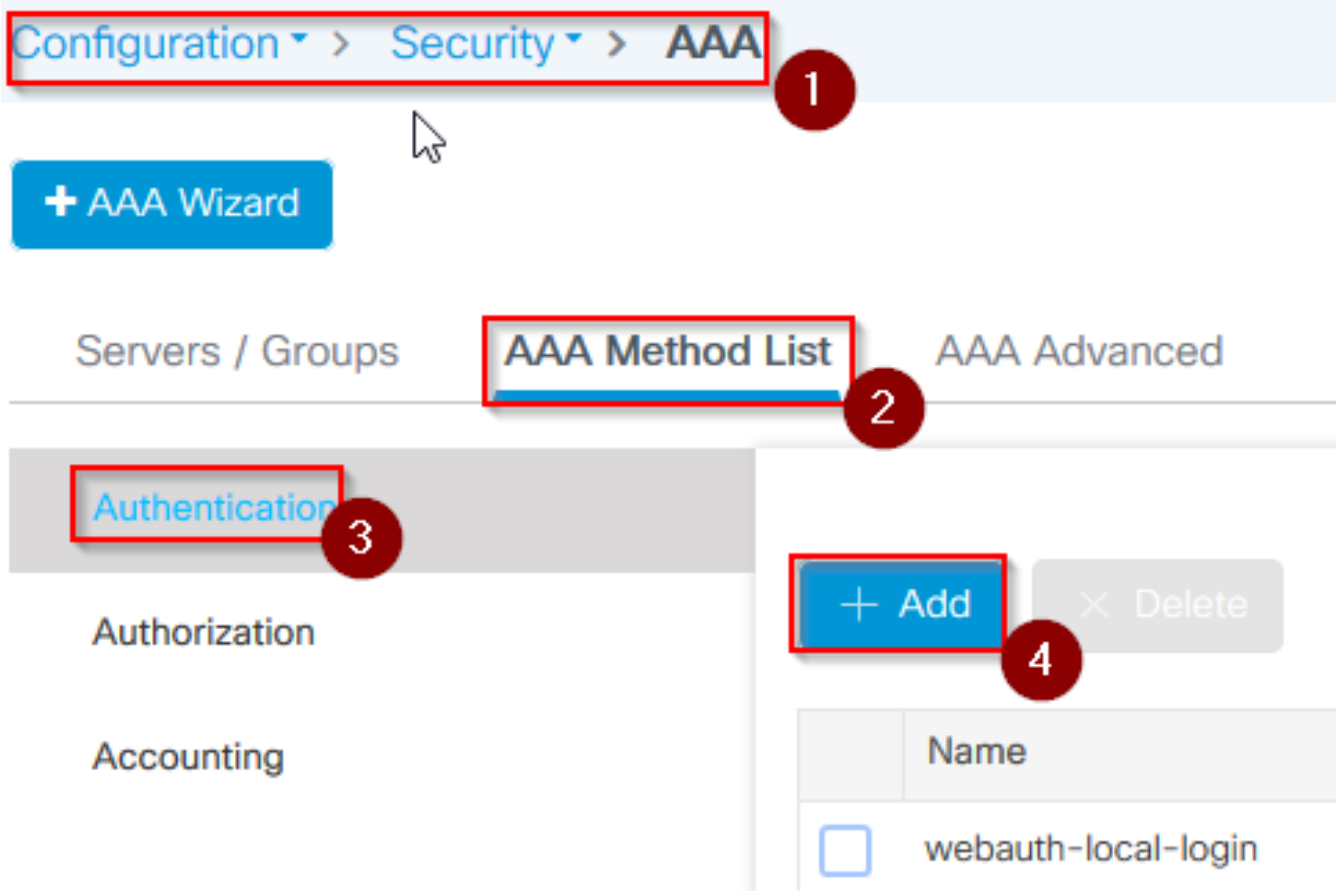
- ステップ 1：Configuration > Security > AAA > AAA Advanced > Device Authenticationの順に移動します



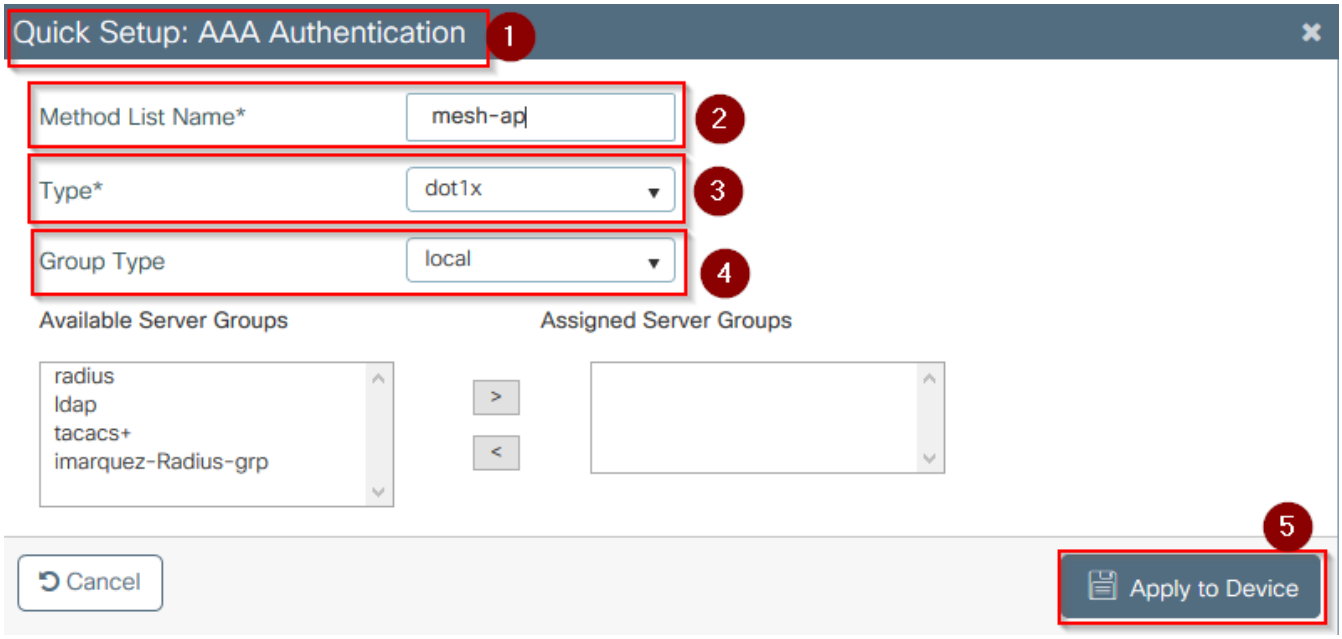
- ステップ 2：Device Authenticationを選択し、Addを選択します
- ステップ 3：WLCに加入するAPのベースイーサネットMACアドレスを入力し、Attribute List Nameを空白のままにして、Apply to Deviceを選択します



- ステップ 4：Configuration > Security > AAA > AAA Method List > Authenticationの順に移動します
- ステップ 5：Addを選択すると、AAA Authenticationポップアップが表示されます



- 手順 6：Method List Nameに名前を入力し、Type*ドロップダウンから802.1xを選択し、Group TypeにlocalをAssigned Server Groups選択して、最後にApply to Deviceを選択します

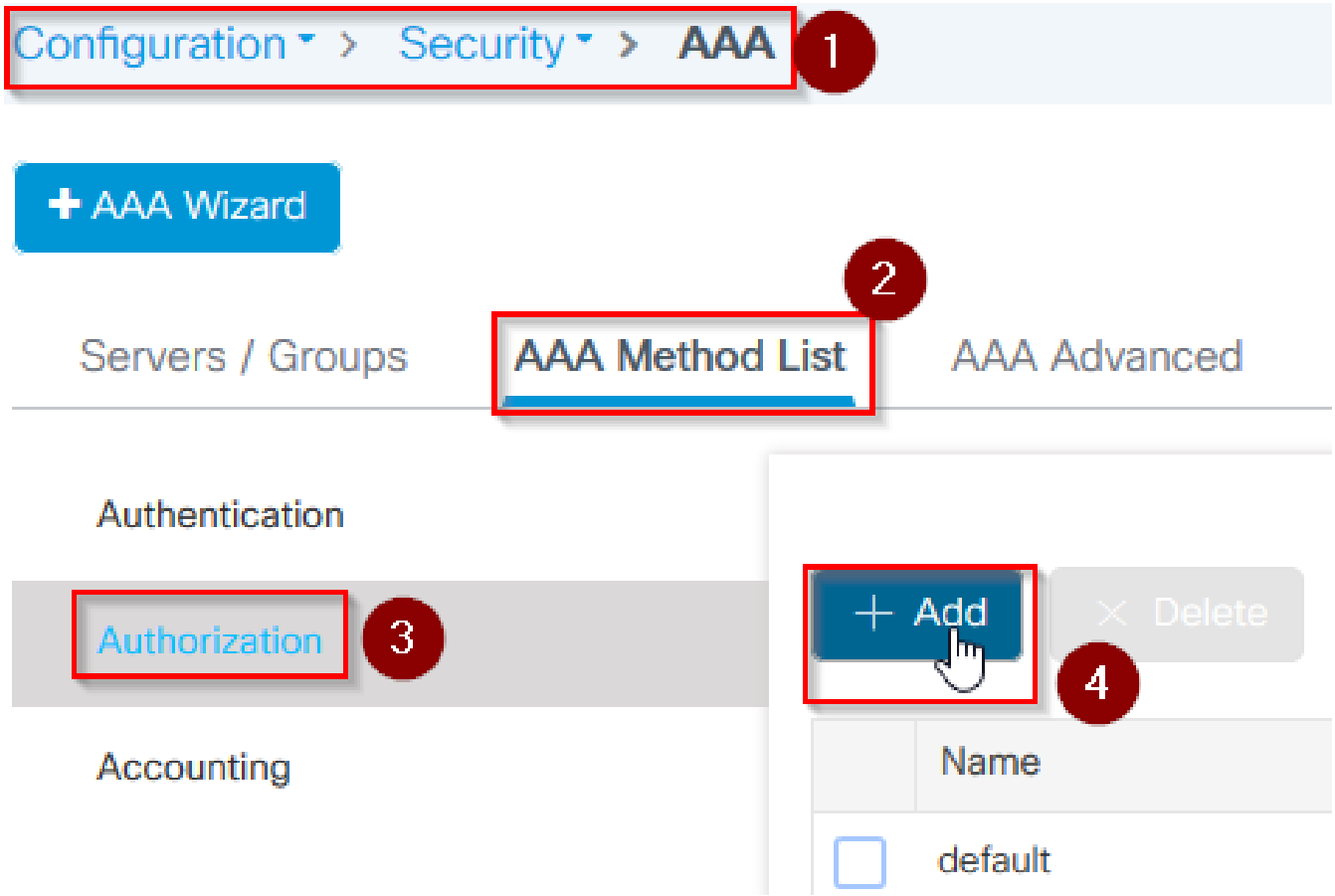


- ステップ6b:APがブリッジモードとして直接加入していて、以前にサイトとポリシータグが割り当てられていなかった場合は、デフォルト方式でステップ6を繰り返します。
- ローカルを指すdot1x aaa認証方式を設定します(CLI aaa authentication dot1x default local)。

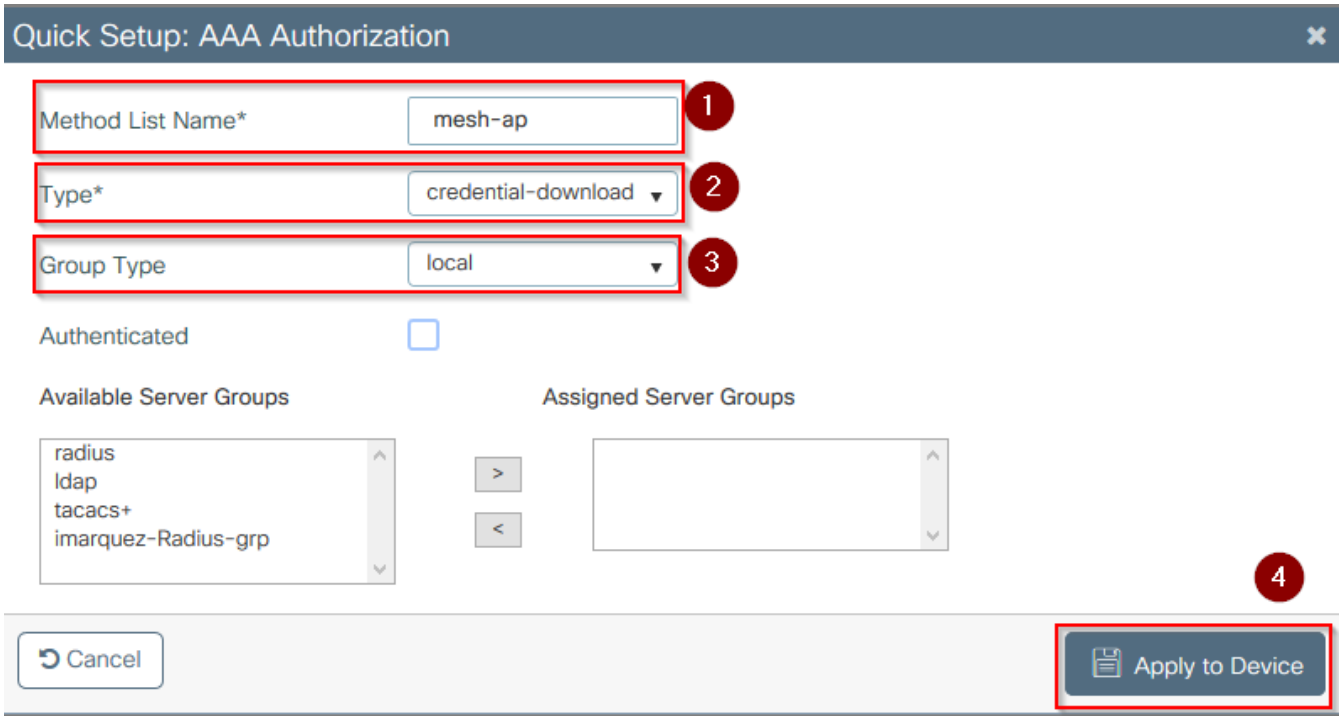
- 手順 7：Configuration > Security > AAA > AAA Method List > Authorizationの順に移動しま

す

- ステップ 8：Addを選択すると、AAA Authorization ポップアップが表示されます



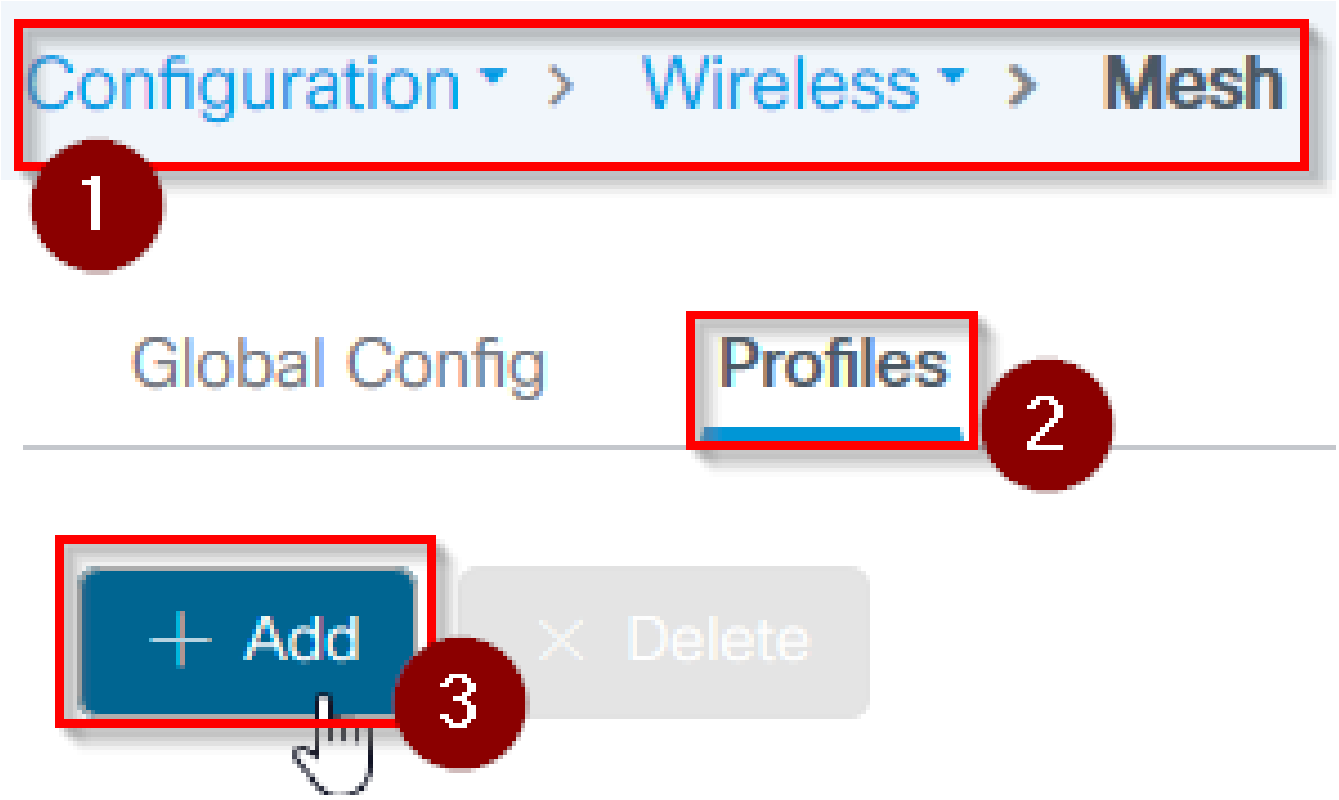
- ステップ 9：Method List Nameに名前を入力し、Type*ドロップダウンからcredeential downloadを選択し、Group Typeにlocalを選択してから、Apply to Deviceを選択します



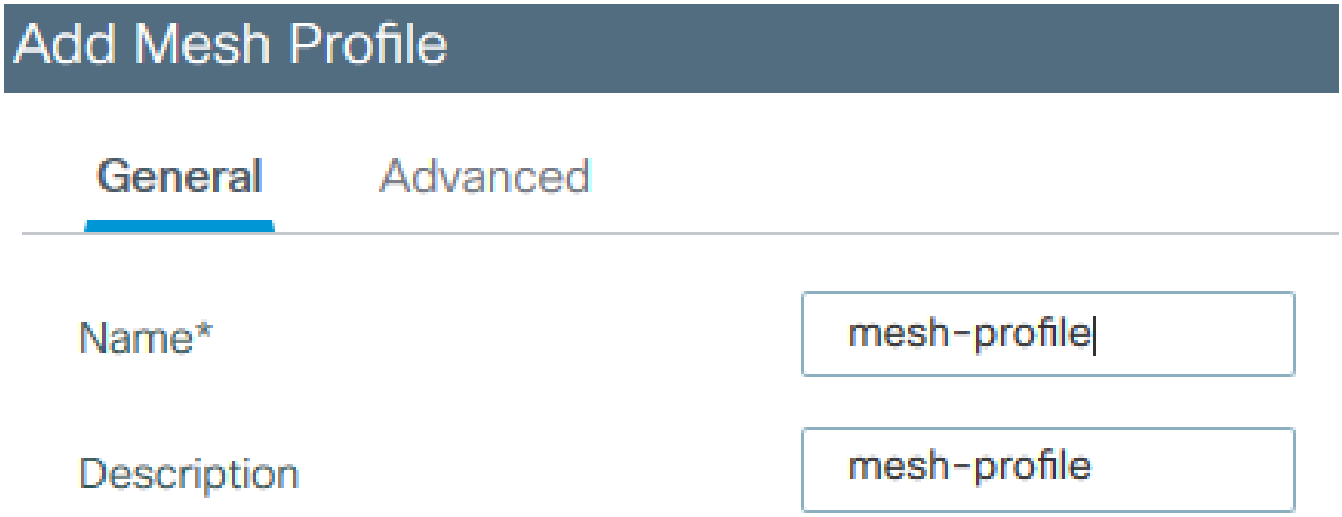
- ステップ9b:APがブリッジモードで直接加入する（つまり、最初にローカルモードで加入し

ない）場合、デフォルトのクレデンシャルダウンロード方式(CLI aaa authorization credential-download default local)でステップ9を繰り返します

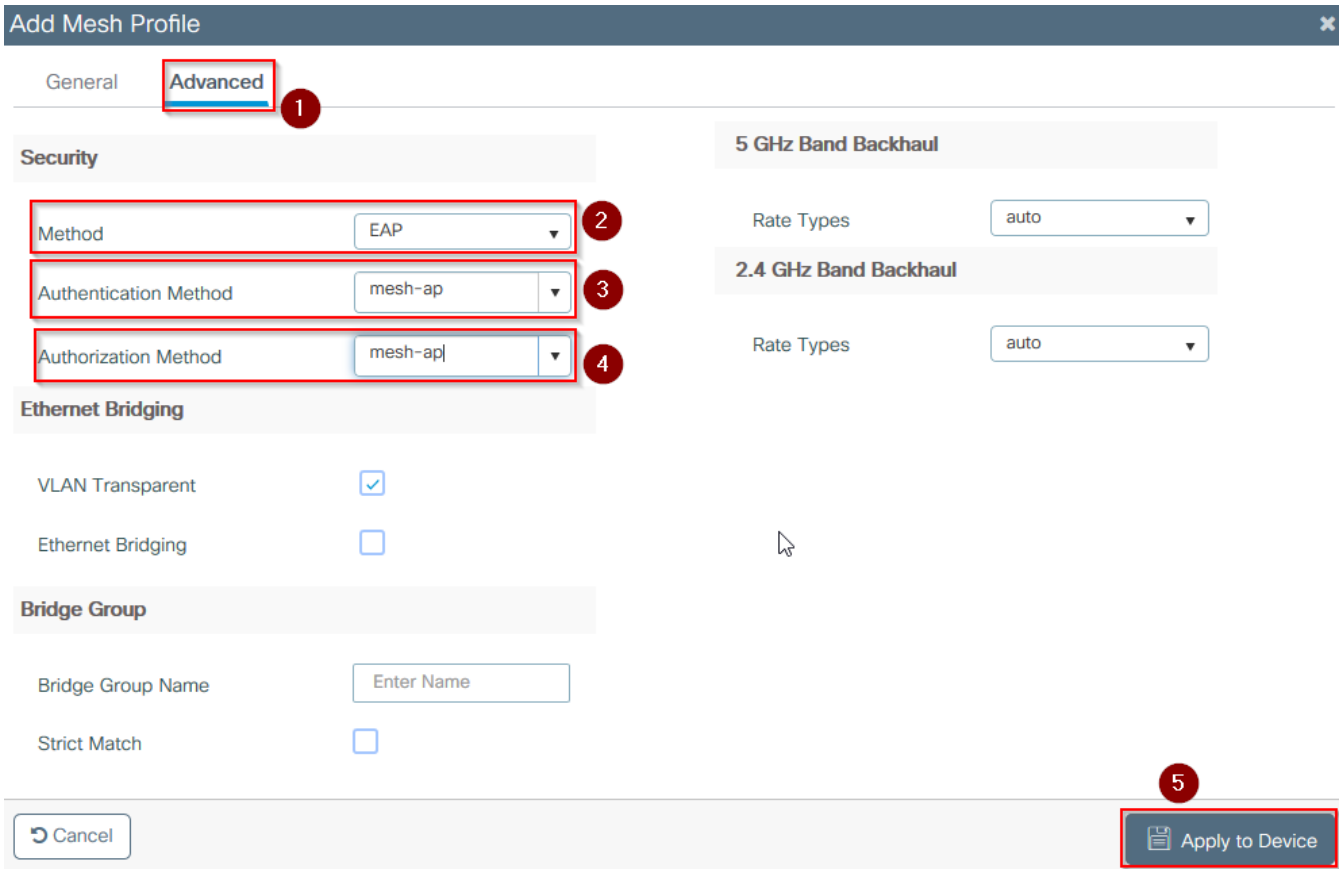
- ステップ 10：Configuration > Wireless > Mesh > Profilesの順に移動します
- ステップ 11Addを選択すると、Add Mesh Profileポップアップが表示されます



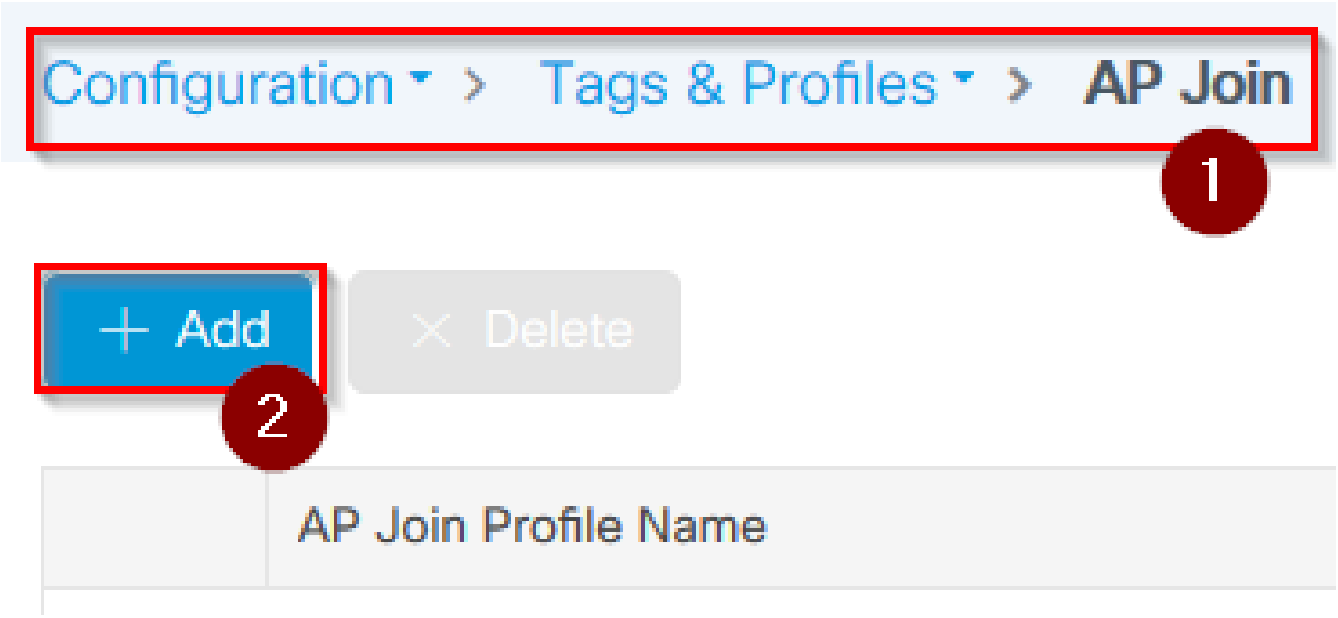
- ステップ 12Generalタブで、メッシュプロファイルの名前と説明を設定します

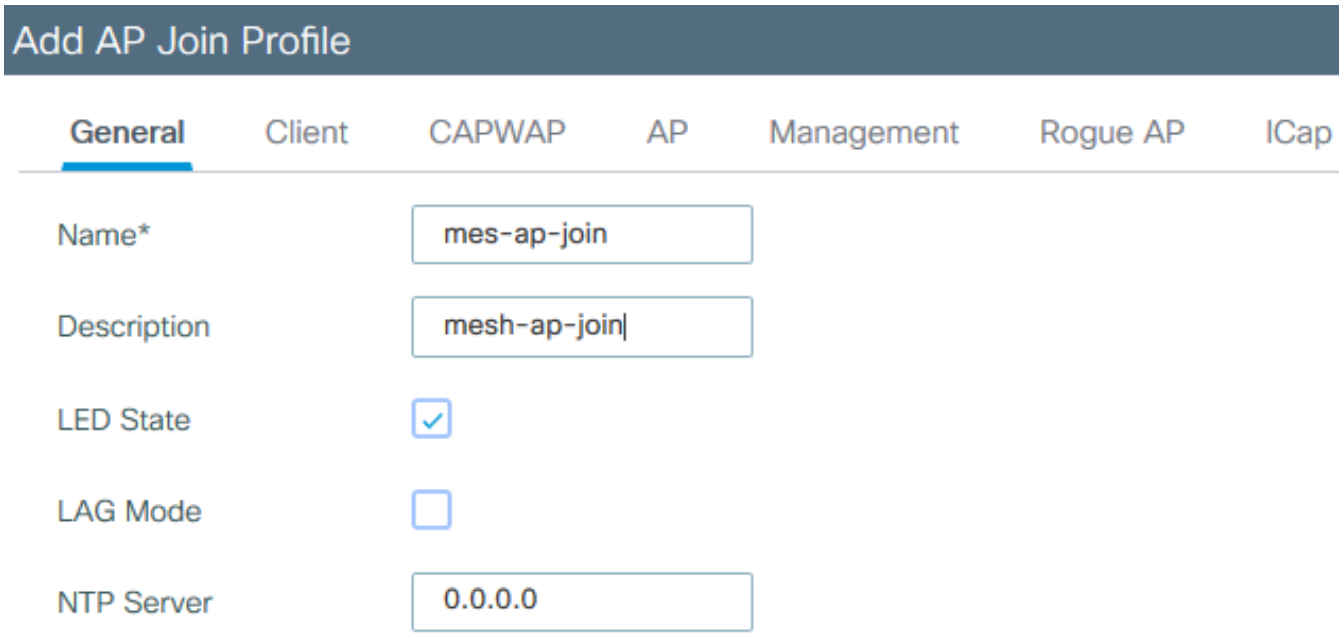


- ステップ 13Advancedタブで、MethodフィールドにEAPを選択します
- ステップ 14：ステップ6と9で定義したAuthorizationおよびAuthenticationプロファイルを選択し、Apply to Deviceを選択します

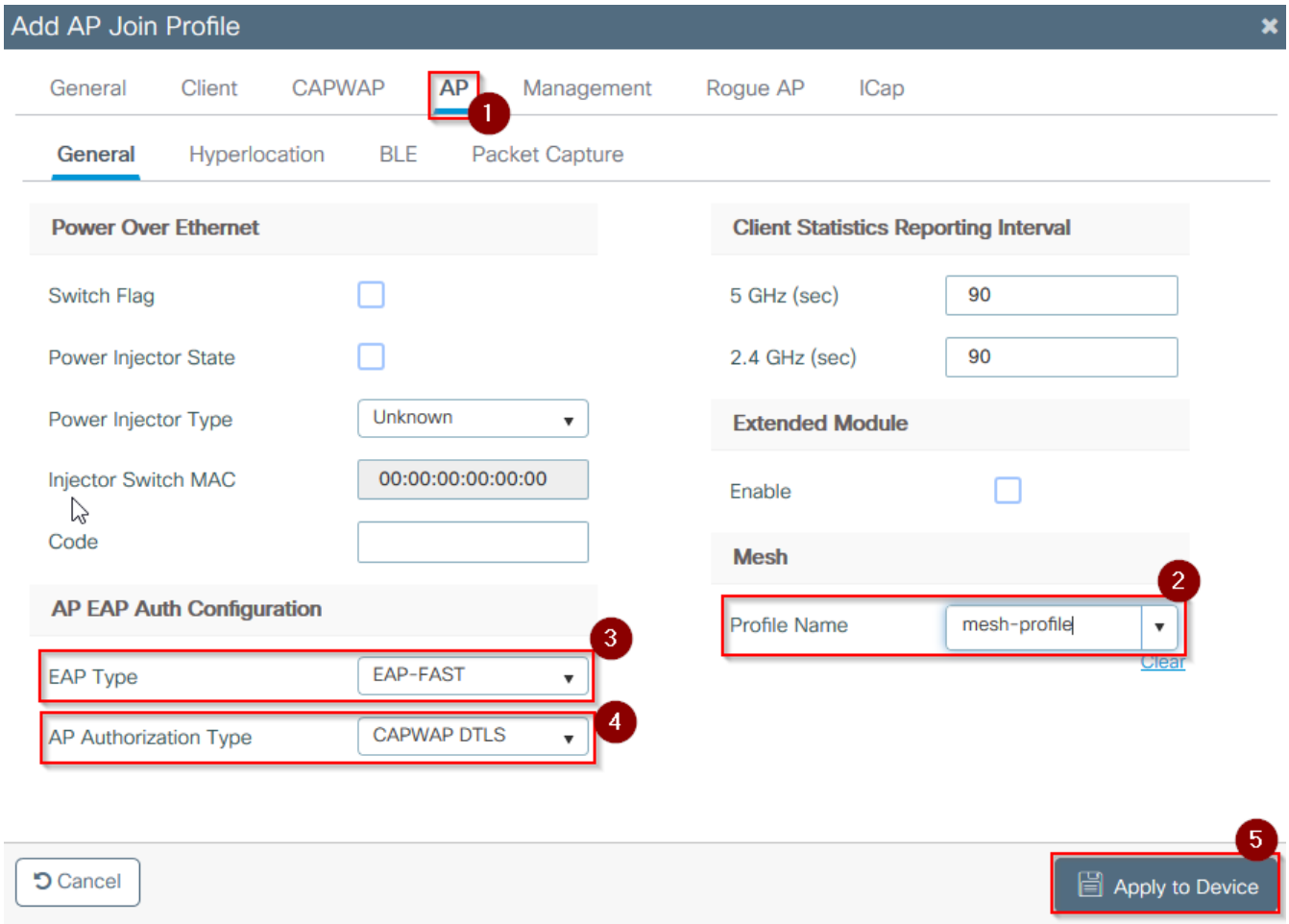


- ステップ 15：Configuration > Tag & Profiles > AP Join > Profileの順に移動します。
- ステップ 16：Addを選択すると、AP Join Profileポップアップが表示され、AP Joinプロファイルの名前と説明を設定します



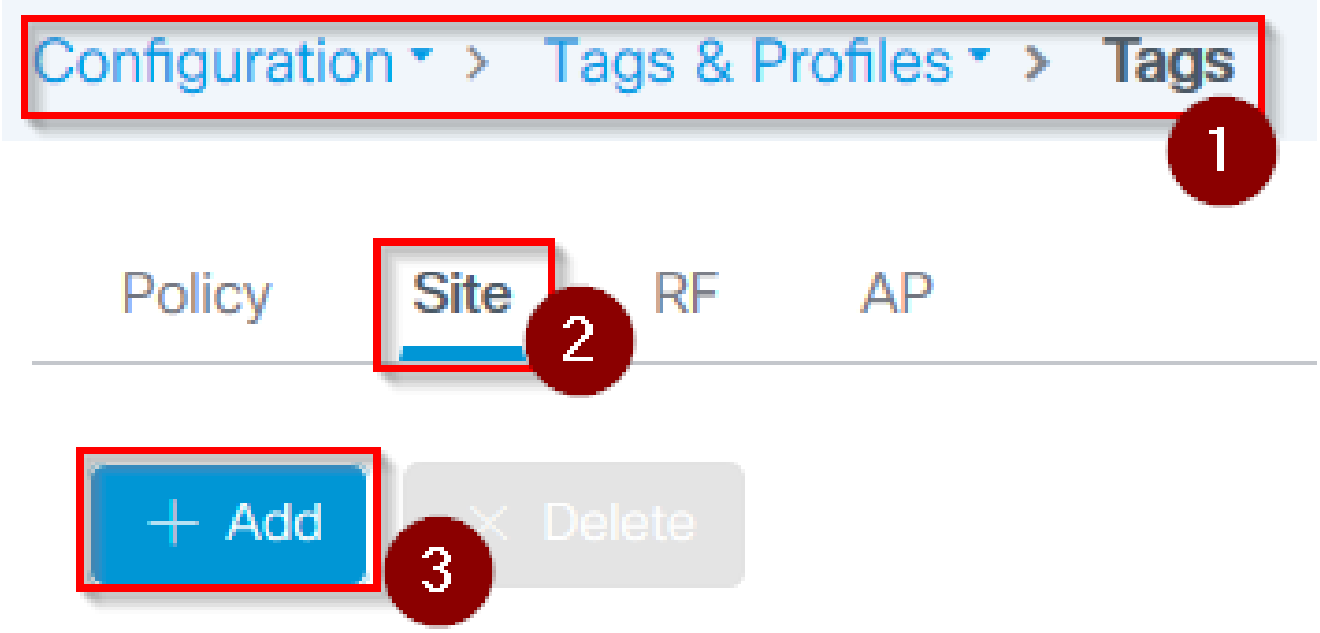


- ステップ 17：APタブに移動し、Mesh Profile Nameドロップダウンから、ステップ12で作成したMesh Profileを選択します
- ステップ 18：EAP-FASTフィールドとCAPWAP DTLSフィールドがそれぞれEAP TypeとAP Authorization Typeに設定されていることを確認します
- ステオ19.Apply to Deviceを選択します。

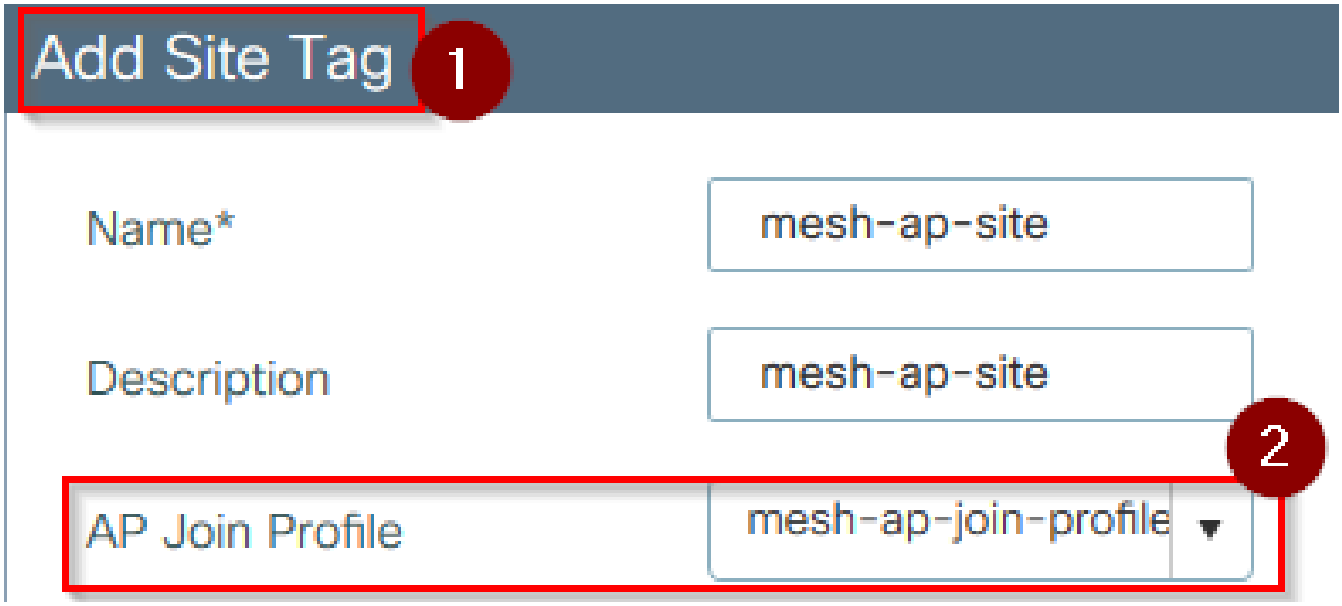


- ステップ 20：Configuration > Tag & Profiles > Tags > Siteの順に移動します。

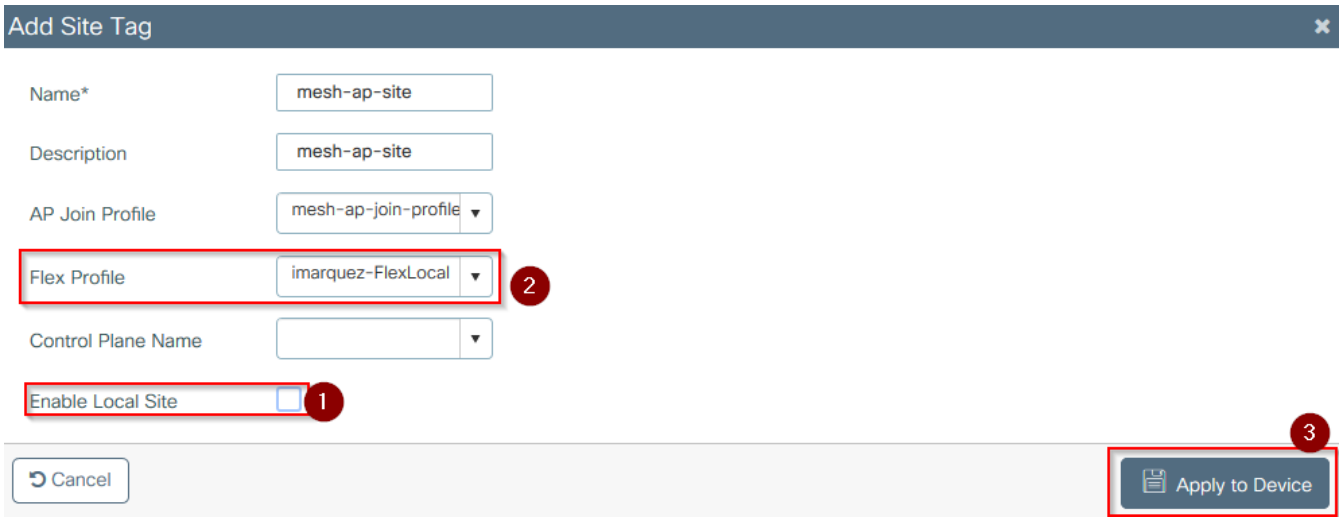
- ステップ 21：Addを選択すると、Site Tagポップアップが表示されます



-
- ステップ 22：サイトタグの名前と説明を入力します



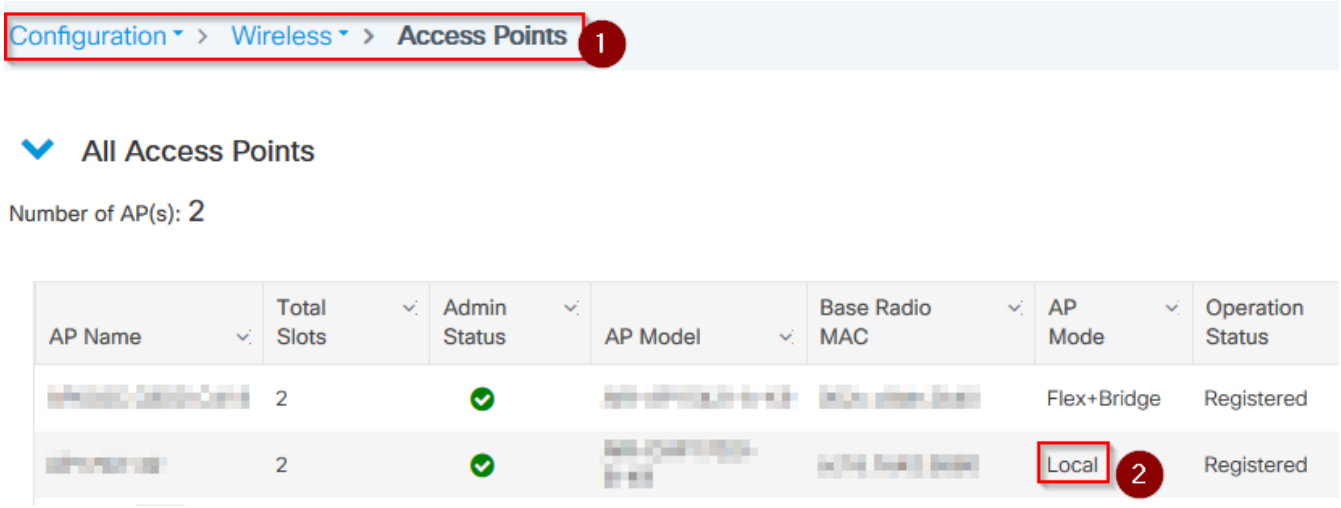
- ステップ 23：AP Join Profileドロップダウンから、ステップ16で作成したAP Join Profileを選択します
- ステップ 24：サイトタグポップアップの下部でEnable Local Siteチェックボックスのチェックマークを外して、Flex Profileドロップダウンを有効にします。
- ステップ 35：Flex Profileのドロップダウンから、APに使用するFlex Profileを選択します



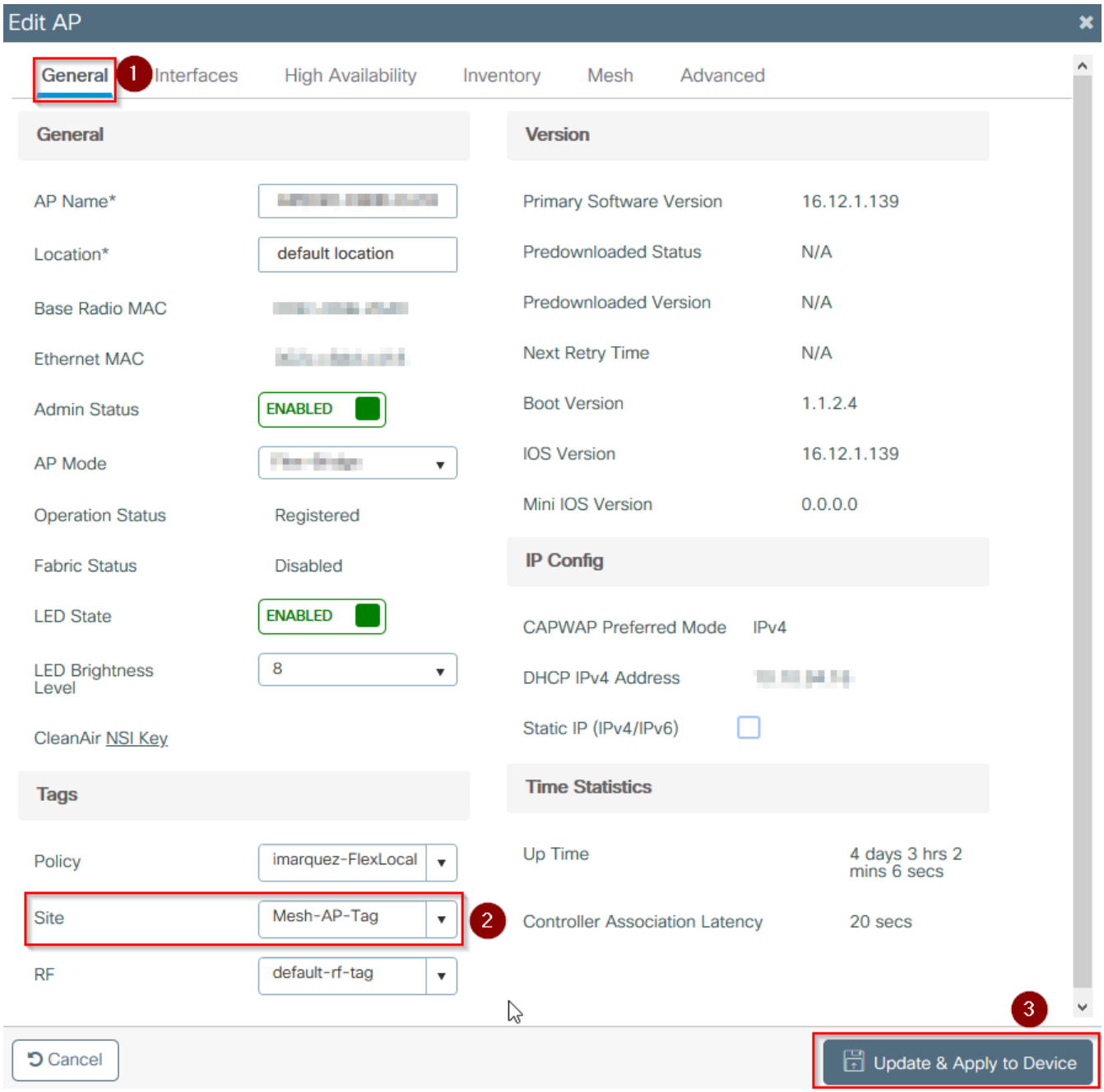
- ステップ 36：APをネットワークに接続し、APがローカルモードであることを確認します。
- ステップ 37：APがローカルモードであることを確認するには、capwap ap mode localコマンドを発行します。

  APは、L2ブロードキャスト、DHCPオプション43、DNS解決、または手動設定のいずれかの方法でコントローラを検出できる必要があります。

- ステップ 38：APがWLCに加入します。APリストにAPがリストされていることを確認し、Configuration > Wireless > Access Points > All Access Pointsの順に移動します



- ステップ 39：APを選択すると、APポップアップが表示されます。
- ステップ 40：APポップアップ内のGeneral > Tags > Siteタブで、ステップ22で作成したSite Tagを選択し、Update and Apply to Deviceを選択します



- ステップ 41：APがリブートし、Flex +ブリッジモードでWLCに再度参加する必要があります

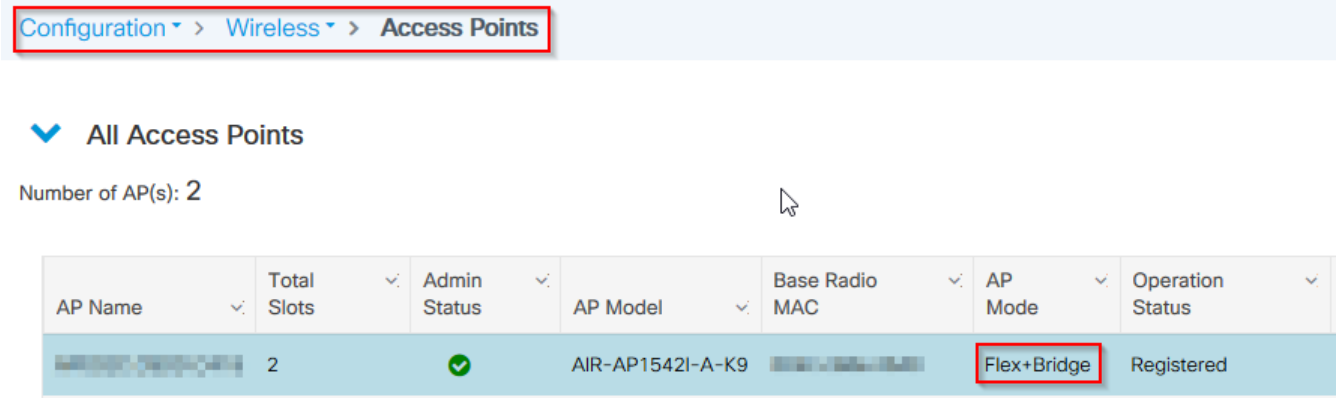
この方式では、まずローカルモードでAPに加入し（dot1x認証は行われません）、メッシュプロファイルでサイトタグを適用してから、APをブリッジモードに切り替えます。

ブリッジ（またはFlex+Bridge）モードでスタックしているAPに加入するには、デフォルト方式(aaa authentication dot1x default localおよびaaa authorization cred default local)を設定します。

これでAPが認証できるようになり、その後でタグを割り当てることができます。

確認

次の図に示すように、APモードがFlex + Bridgeと表示されていることを確認します。



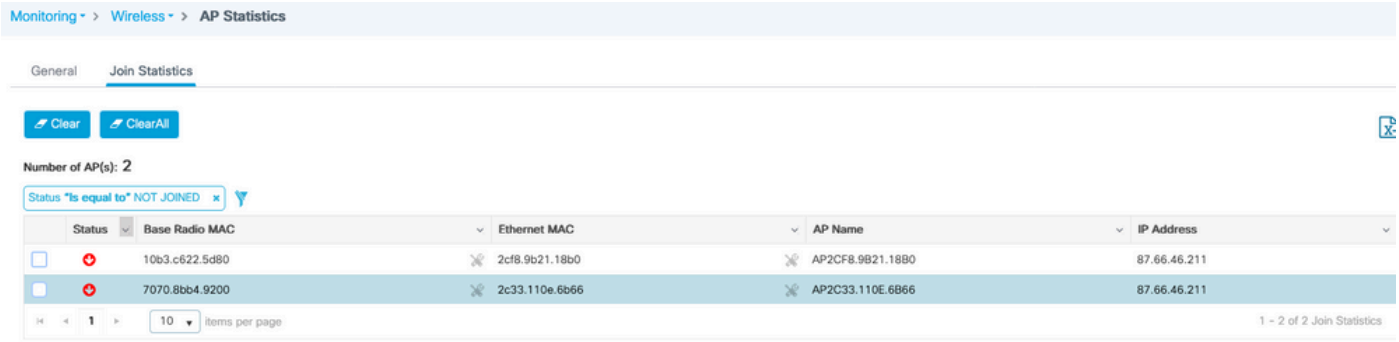
WLC 9800 CLIから次のコマンドを実行し、AP Mode属性を探します。Flex+Bridgeとしてリストされている必要があります。

```
aaa authorization credential-download mesh-ap local
aaa authentication dot1x mesh-ap local
wireless profile mesh default-mesh-profile
 description "default mesh profile"
wireless tag site meshsite
 ap-profile meshapjoin
 no local-site
ap profile meshapjoin
 hyperlocation ble-beacon 0
 hyperlocation ble-beacon 1
 hyperlocation ble-beacon 2
 hyperlocation ble-beacon 3
 hyperlocation ble-beacon 4
 mesh-profile mesh-profile
```

トラブルシュート

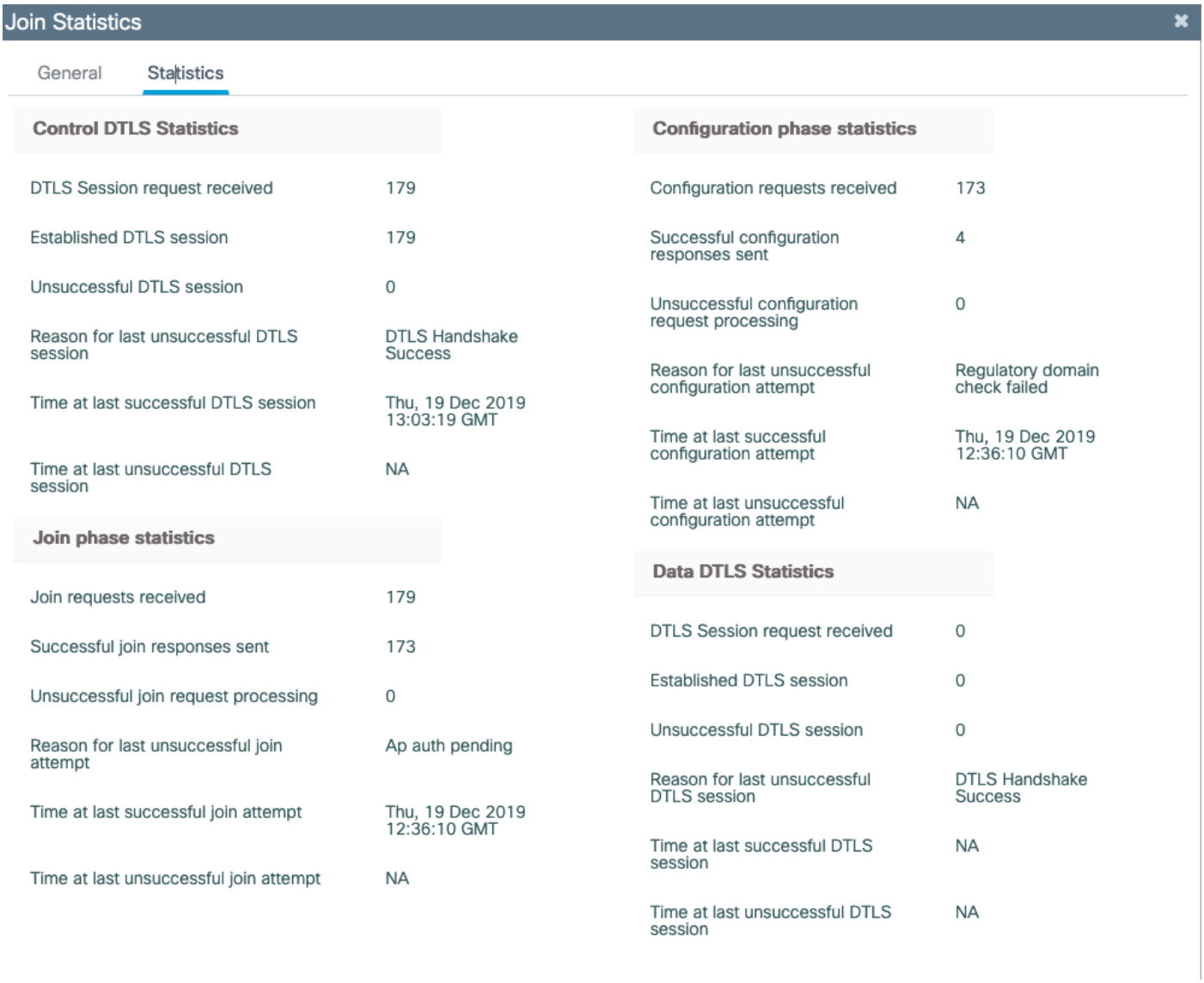
aaa authentication dot1x default localコマンドとaaa authorization cred default localコマンドがあることを確認します。ローカルモードでAPが事前参加していない場合に必要です。

メインの9800ダッシュボードには、参加できないAPを表示するウィジェットがあります。このアイコンをクリックすると、参加に失敗したAPのリストが表示されます（図1を参照）。



特定のAPをクリックして、加入していない理由を確認します。この場合、サイトタグがAPに割り当てられていないため、認証の問題（AP認証保留中）が発生しています。

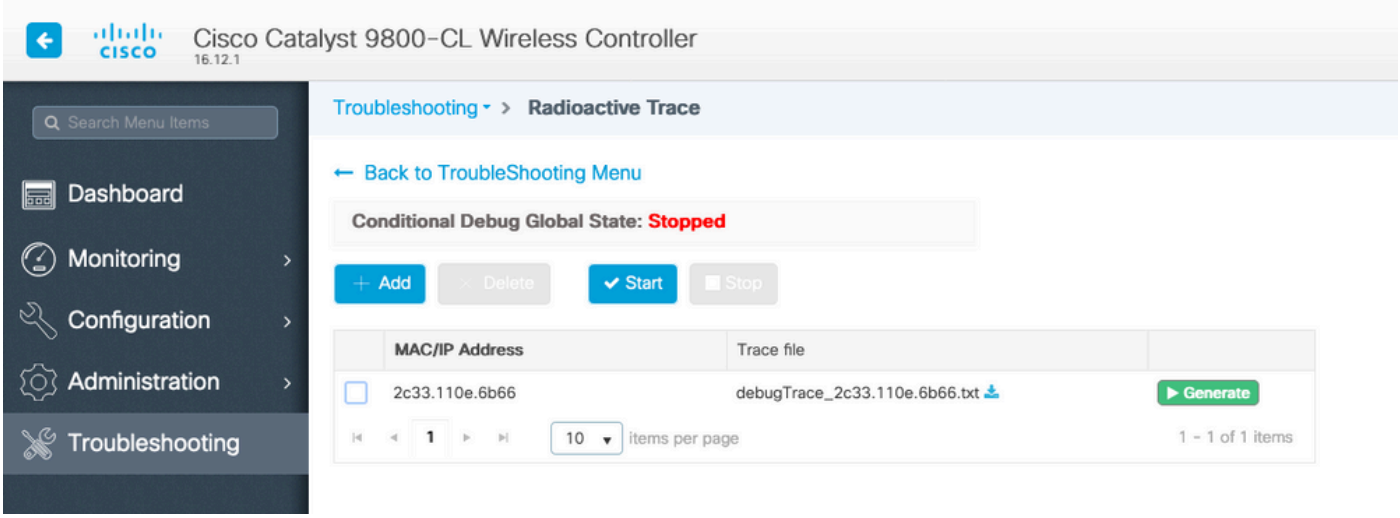
したがって、9800では、APの認証に名前付き認証/許可方式を選択しませんでした（APの認証に使用する名前付き認証/許可方式は選択されていません）。



より高度なトラブルシューティングを行うには、Web UIでTroubleshooting > Radioactive Traceページに移動します。

APのMACアドレスを入力すると、すぐにファイルを生成して、加入を試行するAPの常時接続ログ（通知レベル）を取得できます。

Startをクリックして、そのMACアドレスに対する高度なデバッグを有効にします。次にログが生成されるときにログを生成します。APの結合に関するデバッグレベルのログが表示されます。


Cisco Catalyst 9800-CL Wireless Controller
16.12.1
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Troubleshooting
Radioactive Trace
Back to TroubleShooting Menu
Conditional Debug Global State: Stopped
Add
Delete
Start
Stop
MAC/IP Address
Trace file
2c33.110e.6b66
debugTrace_2c33.110e.6b66.txt
Generate
1
10
items per page
1 - 1 of 1 items

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。