Catalyst 9800ワイヤレスコントローラでの802.1x AAAオーバーライドを使用したFlexConnect WLAN

内容

概要

このドキュメントでは、FlexConnectモードのアクセスポイント(AP)を使用するElastic Wireless LAN Controller(9800 WLC)と、仮想ローカルエリアネットワーク(VLAN)認証、許可、アカウンティング(AAA)オーバーライドを使用してローカルにスイッチングされる802.1x無線LANをを設定します。

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。

- 9800 WLCコンフィギュレーションモード
- FlexConnect

使用するコンポーネント

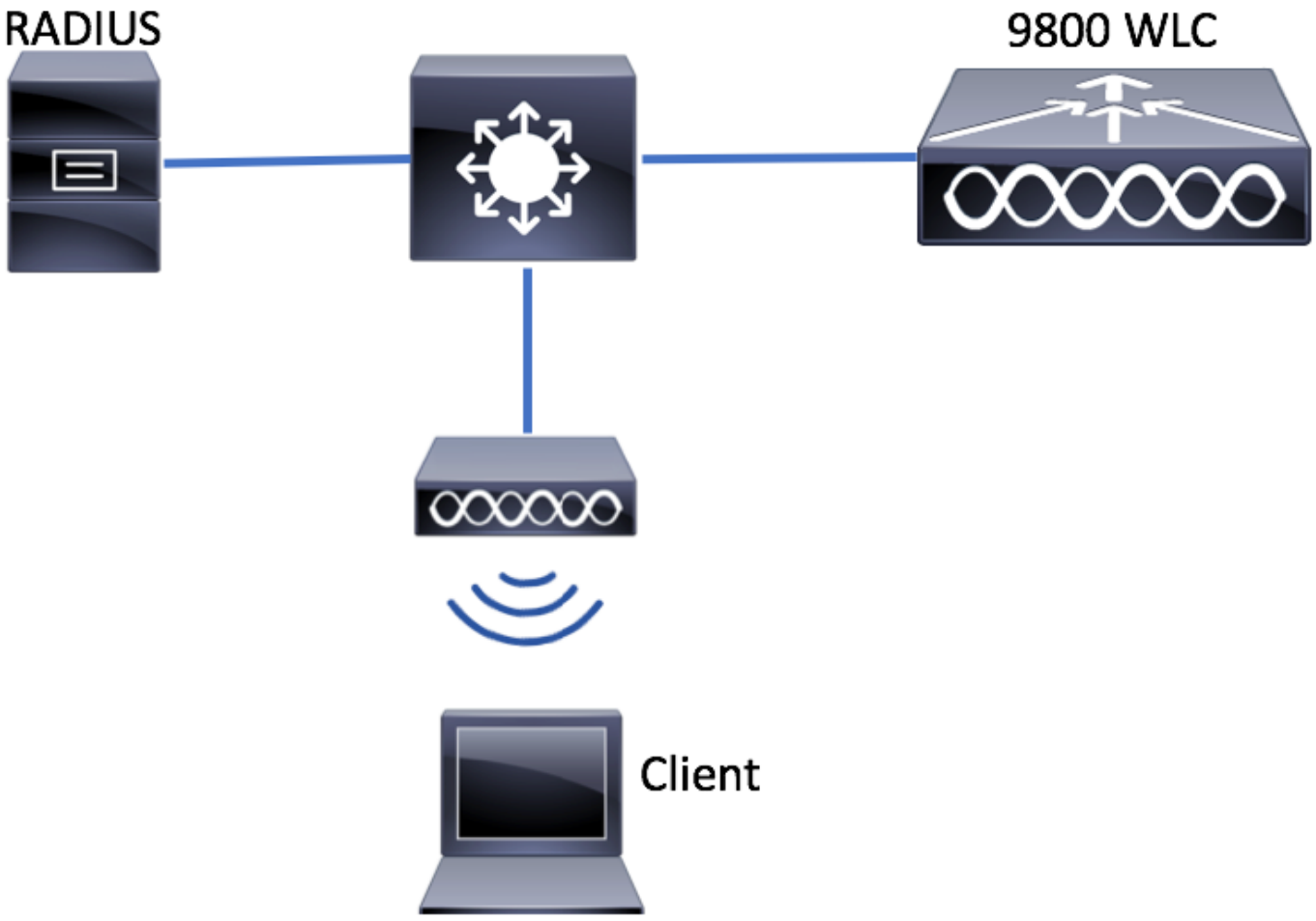
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 9800 WLC v16.10

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



コンフィギュレーション

9800 WLCでのAAA設定

次のリンクの手順に従ってください。

9800 WLCでのAAA設定

WLAN 設定

次のリンクの手順に従ってください。

WLAN 設定

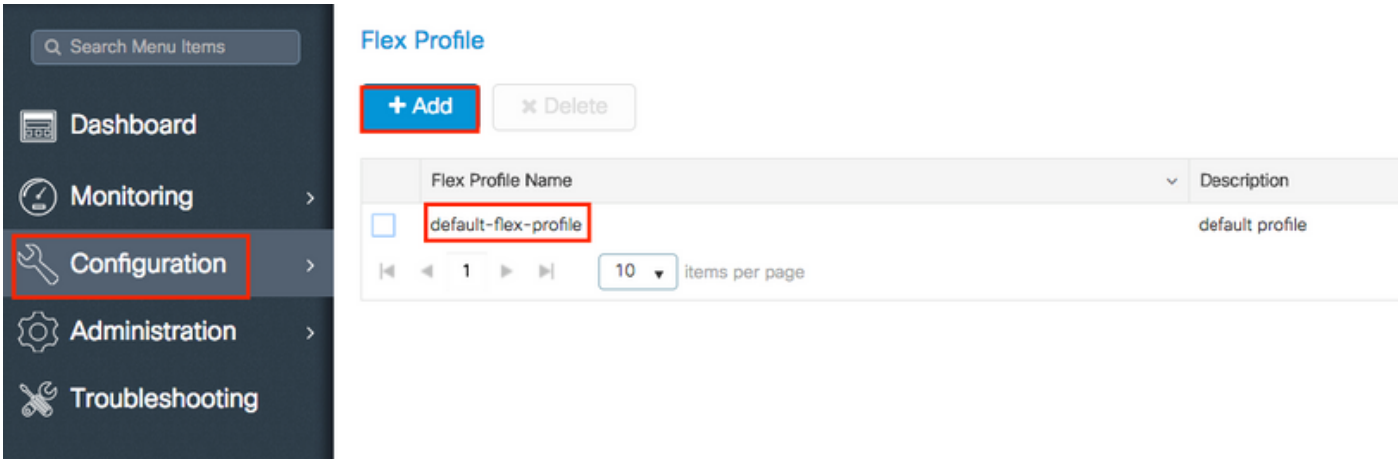
APをFlexConnectモードに設定

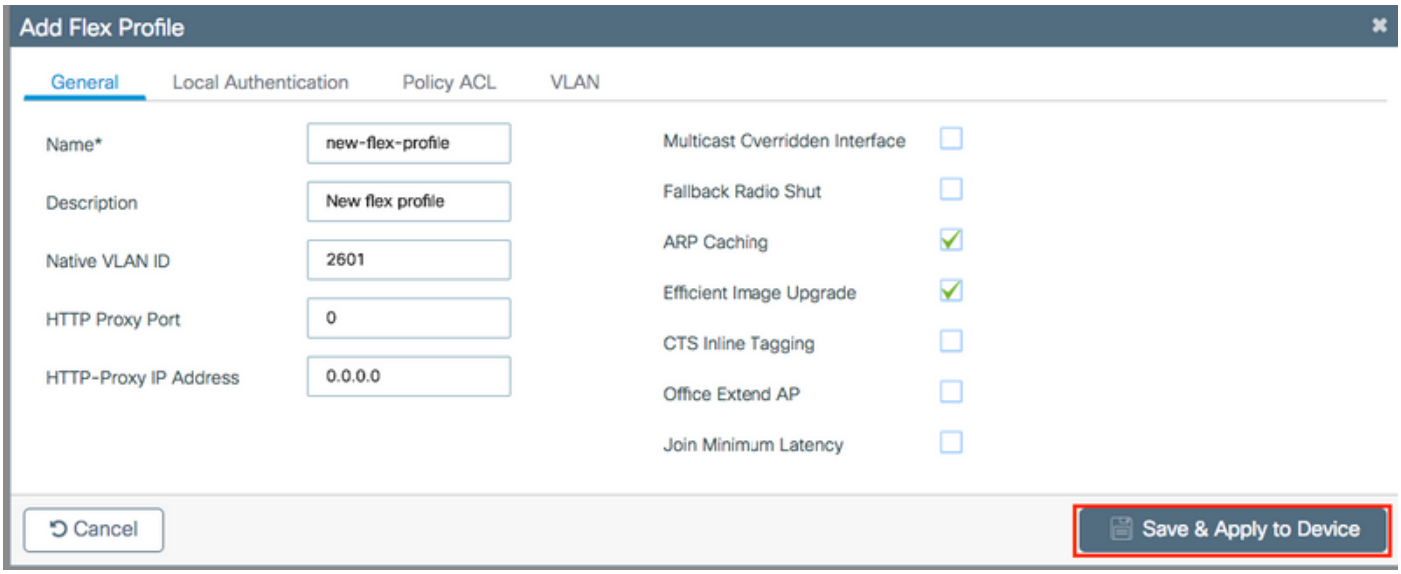
AireOSの設定とは異なり、9800 WLCでは、APから直接APローカルモードまたはflexconnectモードを設定することはできません。FlexConnectモードでAPを設定するには、次の手順を実行します。

GUI

ステップ1:Flexプロファイルを設定します。

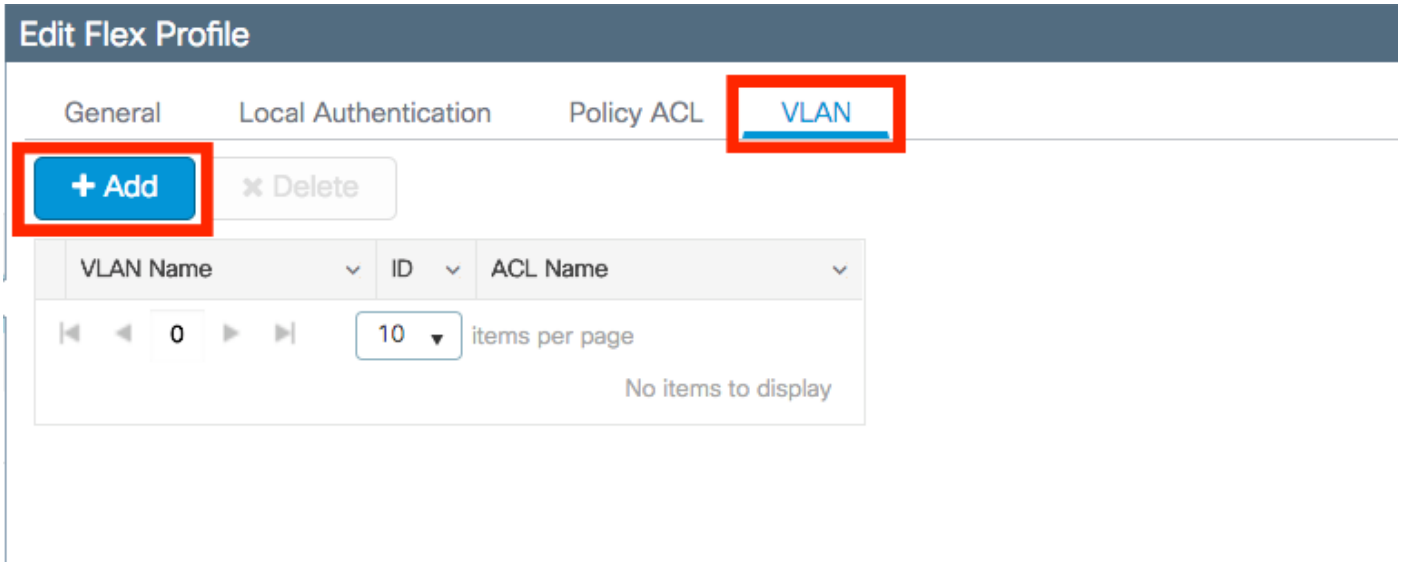
に移動 **[Configuration] > [Tags & Profiles] > [Flex]** default-flex-profileを変更するか、**[+ Add]をクリックして新しいプロファイル**を作成します。



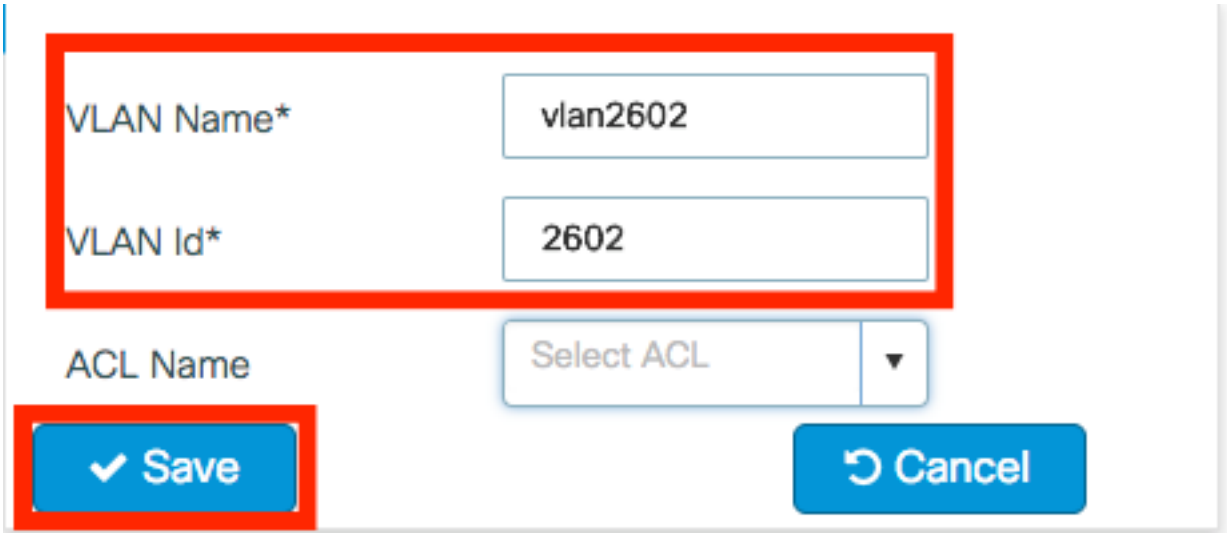


ステップ2：必要なVLAN（デフォルトのWLANのVLANまたはISEからプッシュされたVLANの両方）を追加します。

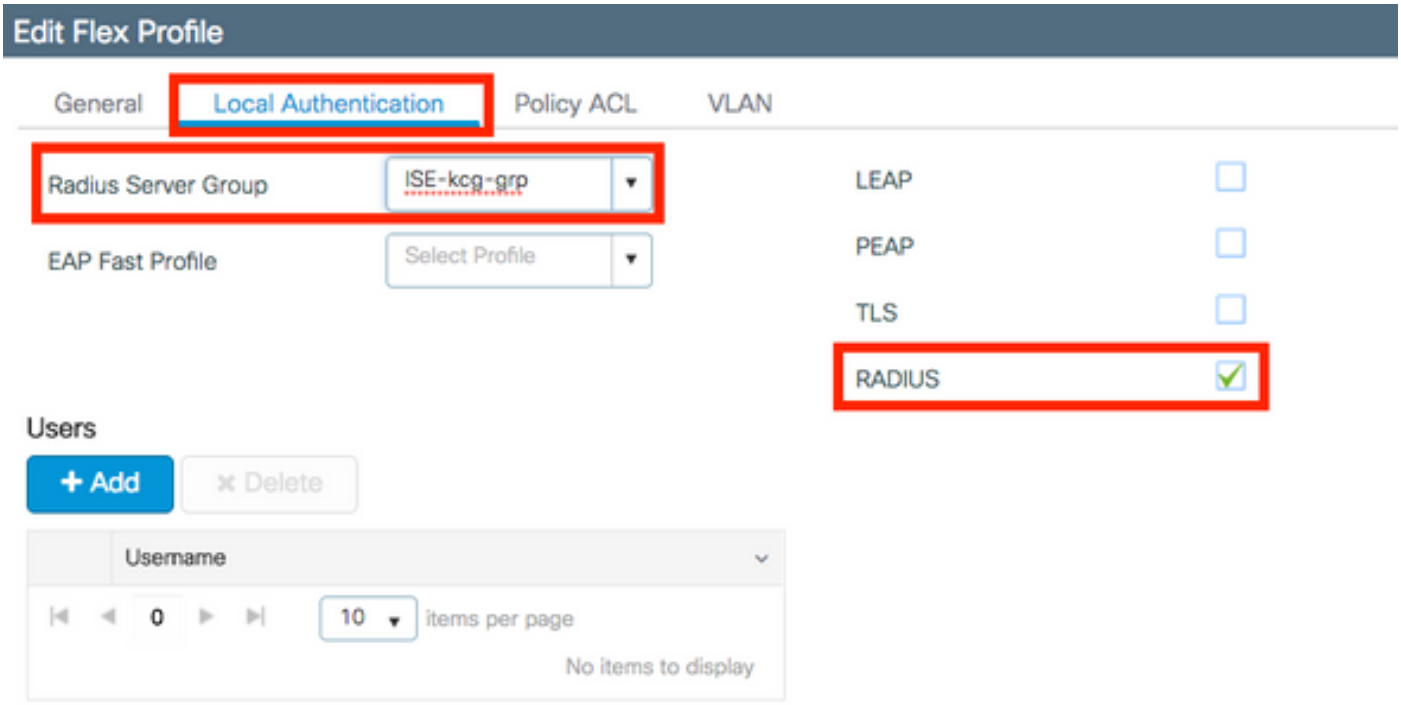
> **注**:[Policy Profile Configuration]セクションのステップ3で、SSIDに割り当てられたデフォルトのVLANを選択します。この手順でVLAN名を使用する場合は、Flex Profile設定で同じVLAN名を使用していることを確認してください。使用しない場合、クライアントはWLANに接続できません。



オプションで、VLANごとに特定のACLを追加できます。

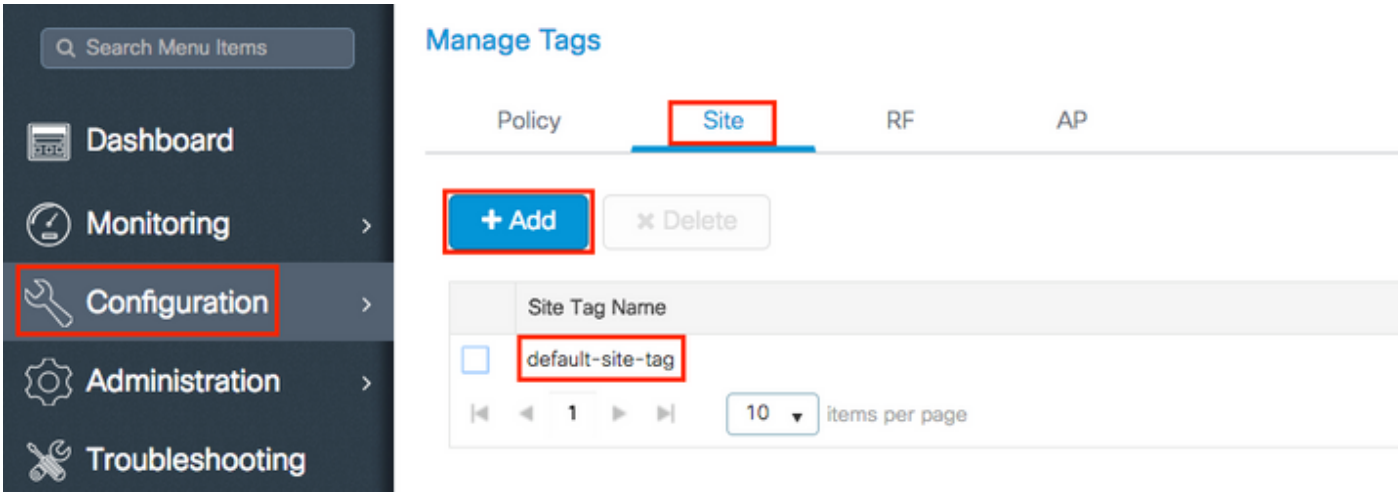


オプションで、FlexConnect APがローカル認証を実行できるように、RADIUSサーバグループを割り当てます。



ステップ3：サイトタグを設定します。

[Configuration] > [Tags & Profiles] > [Tags] > [Site]に移動します。default-site-tag（すべてのAPにデフォルトで割り当てられているタグ）を変更するか、新しいタグを作成します(新しいタグを作成するには**+Addをクリックします**)。

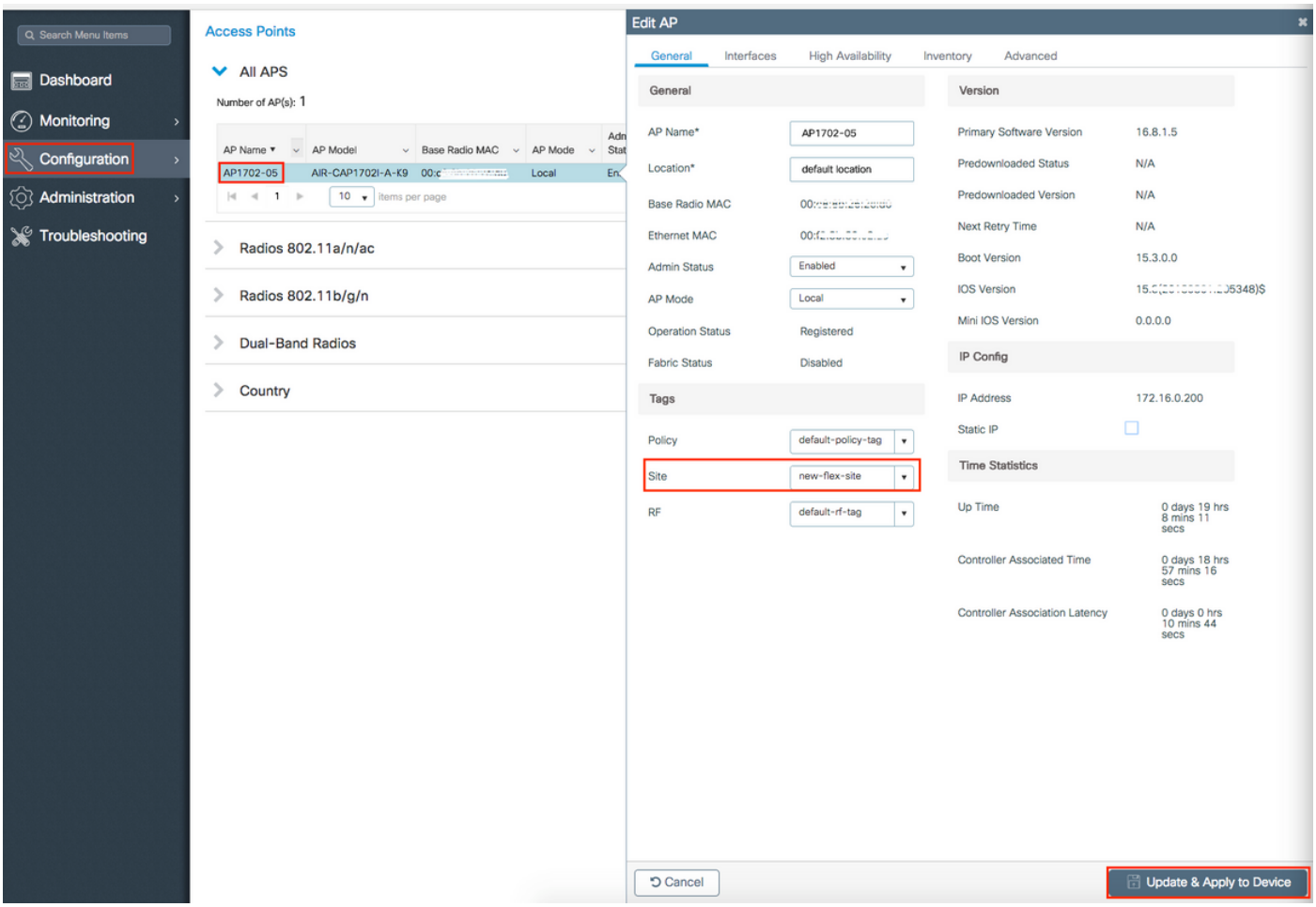


[ローカルサイトを有効**にする]オプション**を無効にする必要があります。それ以外の場**合、[フレックスプロフ**ァイル]オプションは使用できません。

注：[Enable Local Site]が有効になっているサイトタグを**取得する**APは、ローカルモードとして設定されます。同様に、[ローカルサイトを有効にする(Enable **Local Site**)]が無効になっている**サイトタグを取得する**すべてのAPは、flexconnectモードとして設定されます。

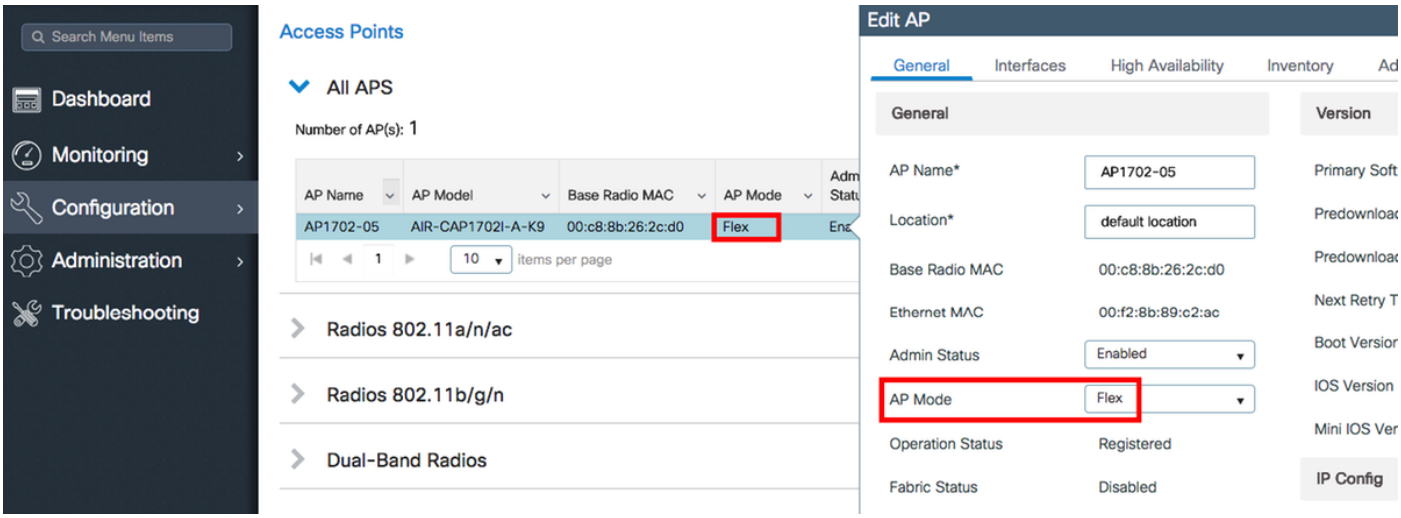
ステップ4:APを9800 WLCに関連付け、ステップ2で設定したサイトタグを割り当てます。

[Configuration] > [Wireless] > [Access Points] > [AP name]に移動し、サイトタグを設定します。次に、[Update & Apply to Device]をクリックして変更を設定します。



注:APでタグを変更すると、9800 WLCへの関連付けが失われ、約1分以内に再び参加することに注意してください。

ステップ5:APが再び加入したら、APモードがFlexであることに注意してください



CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode                                         : FlexConnect
```

スイッチの設定

APが接続されているスイッチのインターフェイスを設定します。

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
# spanning-tree portfast trunk
# end
```

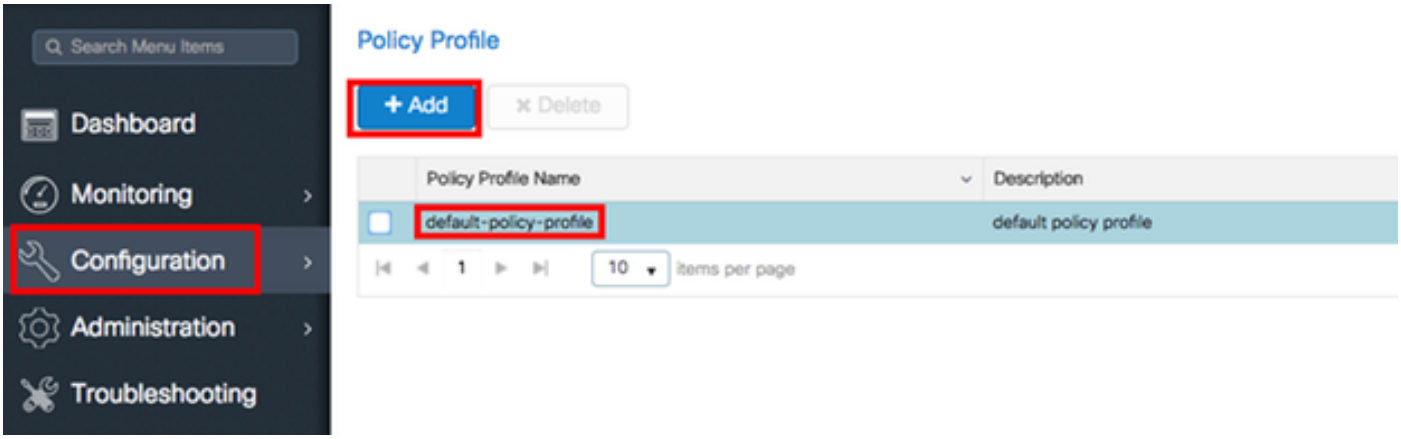
ポリシープロファイルの設定

ポリシープロファイル内では、アクセスコントロールリスト(ACL)、Quality of Service(QoS)、モビリティアンカー、タイマーなど、クライアントを割り当てるVLANを設定できます。

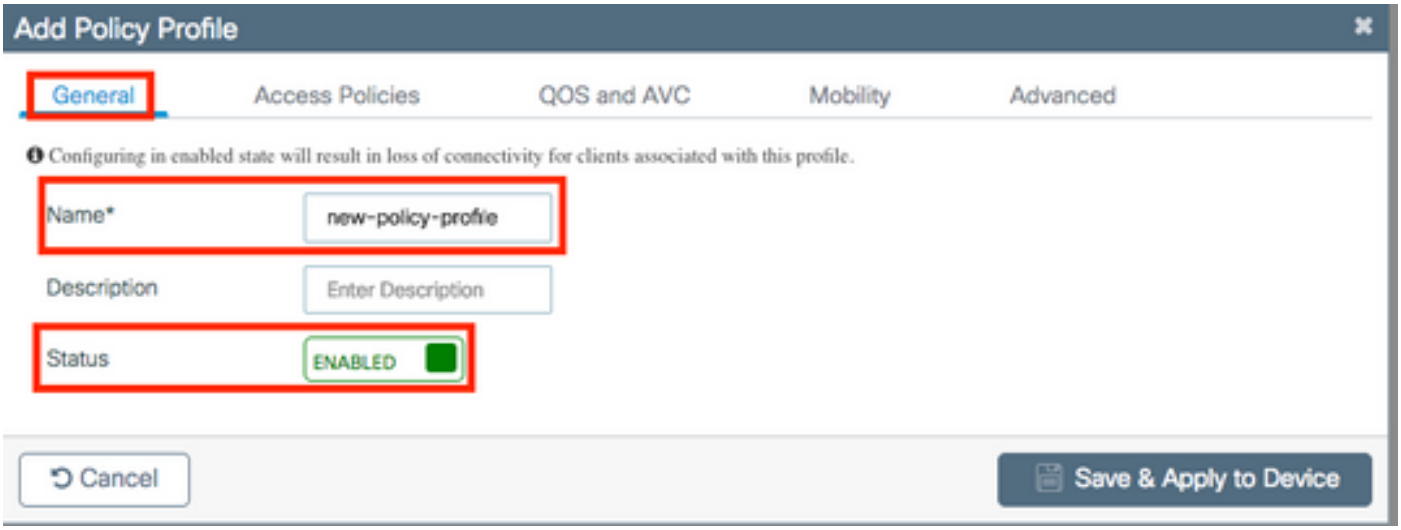
GUI

ステップ1:WLANに割り当てるポリシープロファイルを設定します。

[Configuration] > [Tags & Profiles] > [Policy]に移動し、新しいプロファイルを作成するか、default-policy-profileを変更します。



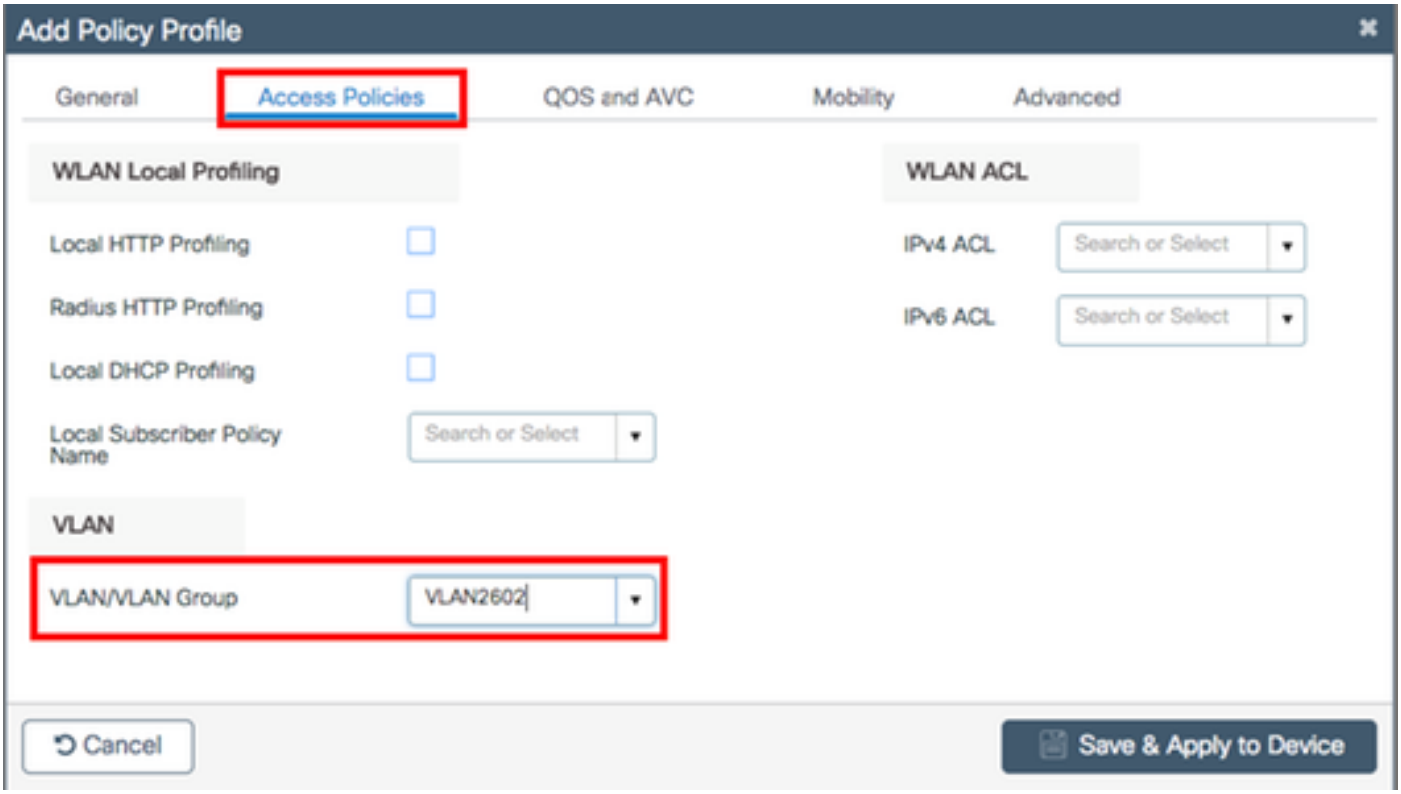
ステップ2:**[General]タブで、ポリシープロファイルに名前を割り当て、そのステータスを**[ENABLED]に変更**します。**



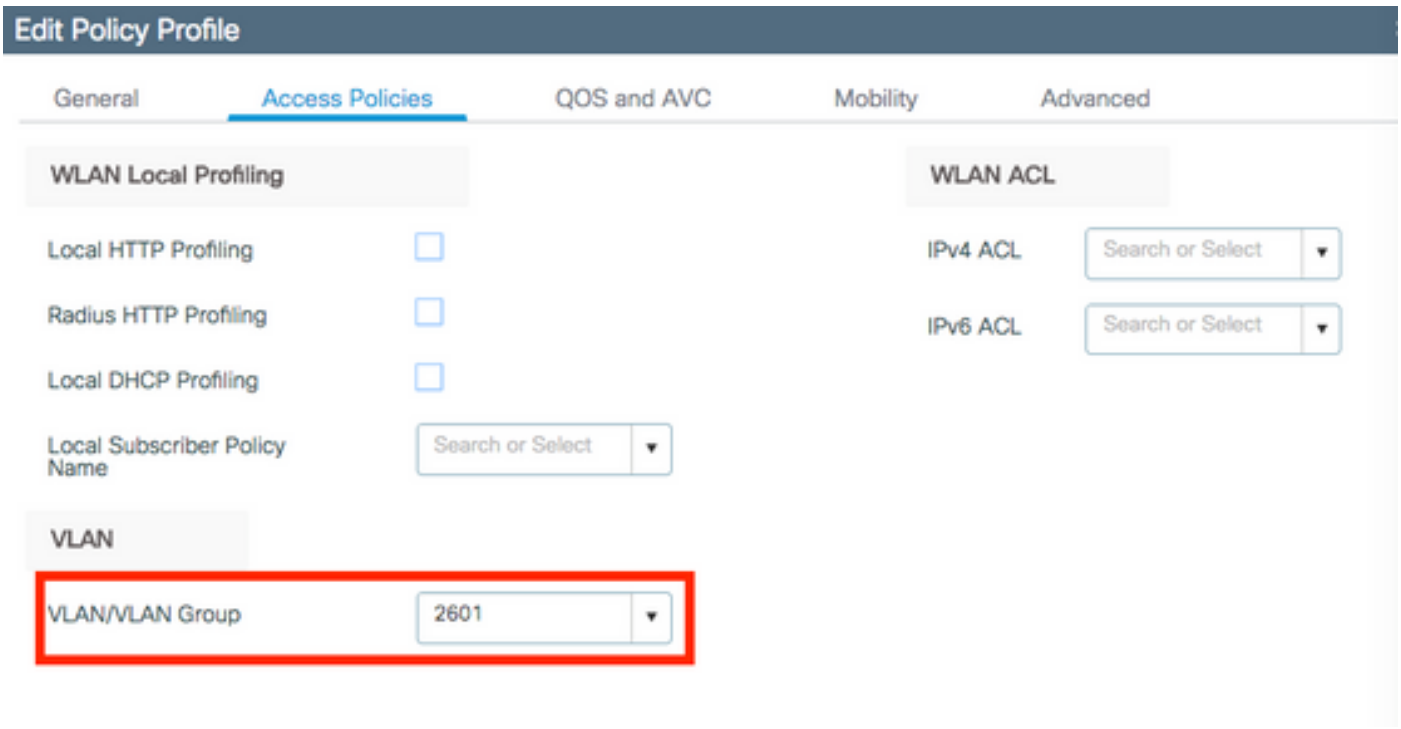
ステップ3:**[Access Policies]**タブで、デフォルトでこのWLANに接続するときにワイヤレスクライアントが割り当てられるVLANを割り当てます。

ドロップダウンからVLAN名を1つ選択するか、手動でVLAN IDを入力できます。

> **注**：ドロップダウンからVLAN名を選択する場合は、**「FlexConnectモードとしてAPを設定」セクションのステップ2で使用したVLAN名と一致することを確認してください。**

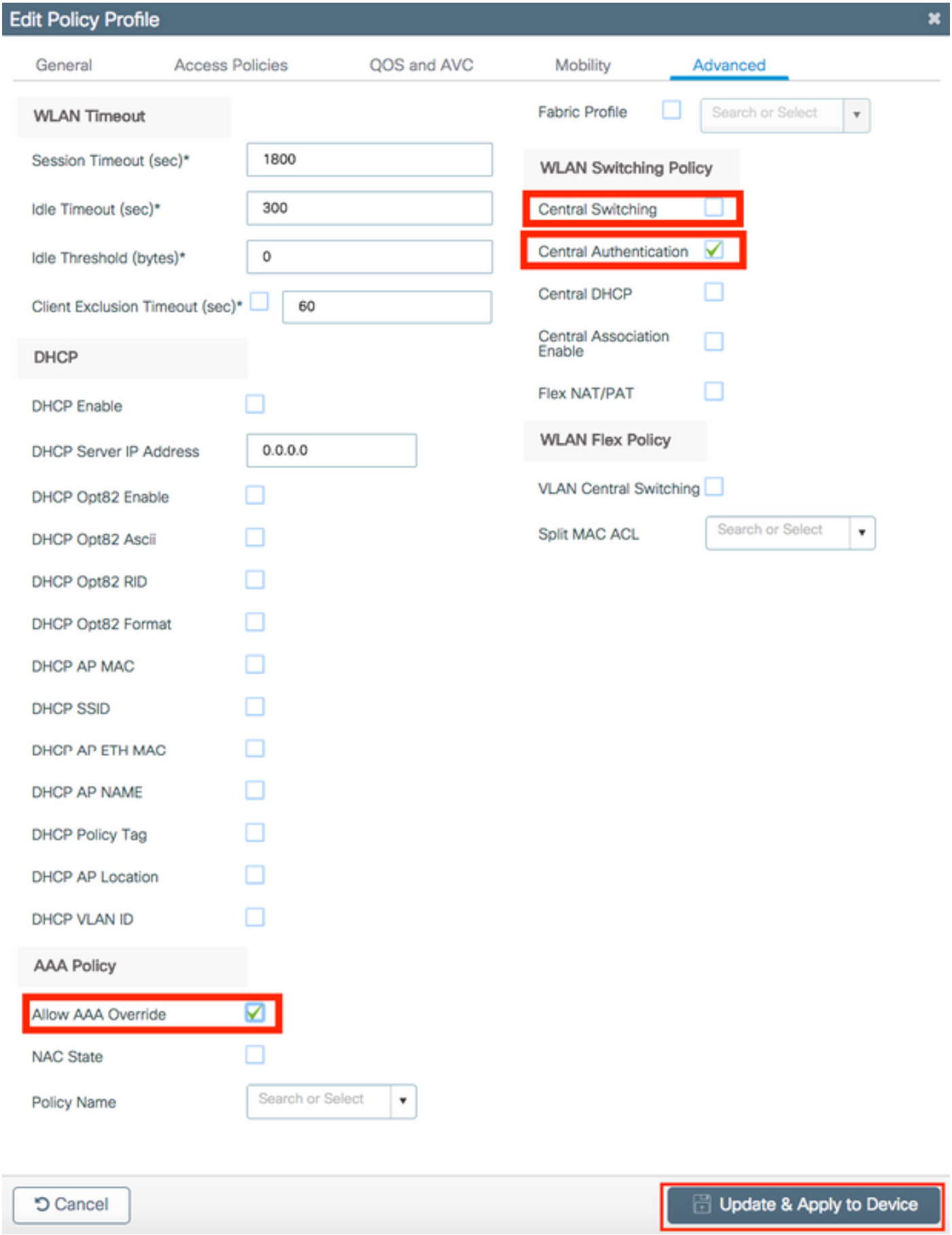


または



ステップ4:[Advanced]タブに移動し、[Central Authentication Enable]および[Allow AAA Overrideoptions]を有効にします。**中央スイッチング**を無効にする必要があります。

認証プロセスを9800 WLCで中央で実行する場合は、中央認証を有効にする必要があります。FlexConnect APでワイヤレスクライアントを認証する場合は、これを無効にします。



CLI

```
# config t
# wireless profile policy new-policy-profile # central association # vlan <vlan-id or vlan-name>
```

```
# no shutdown
```

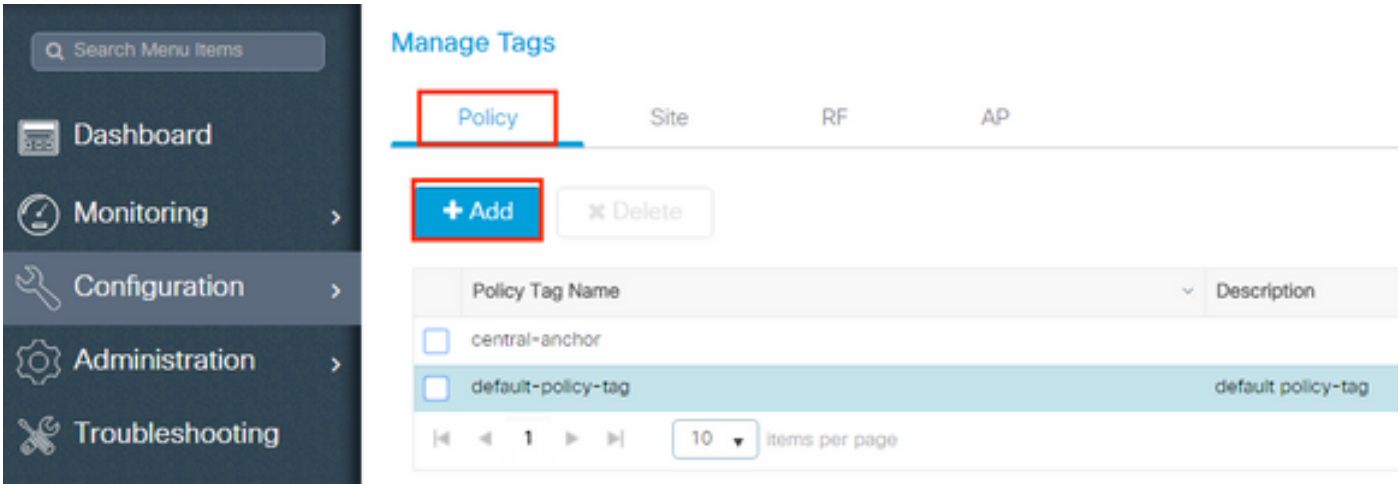
ポリシータグの設定

ポリシータグは、SSIDをポリシープロファイルにリンクするために使用されます。新しいポリスタグを作成するか、default-policyタグを使用します。

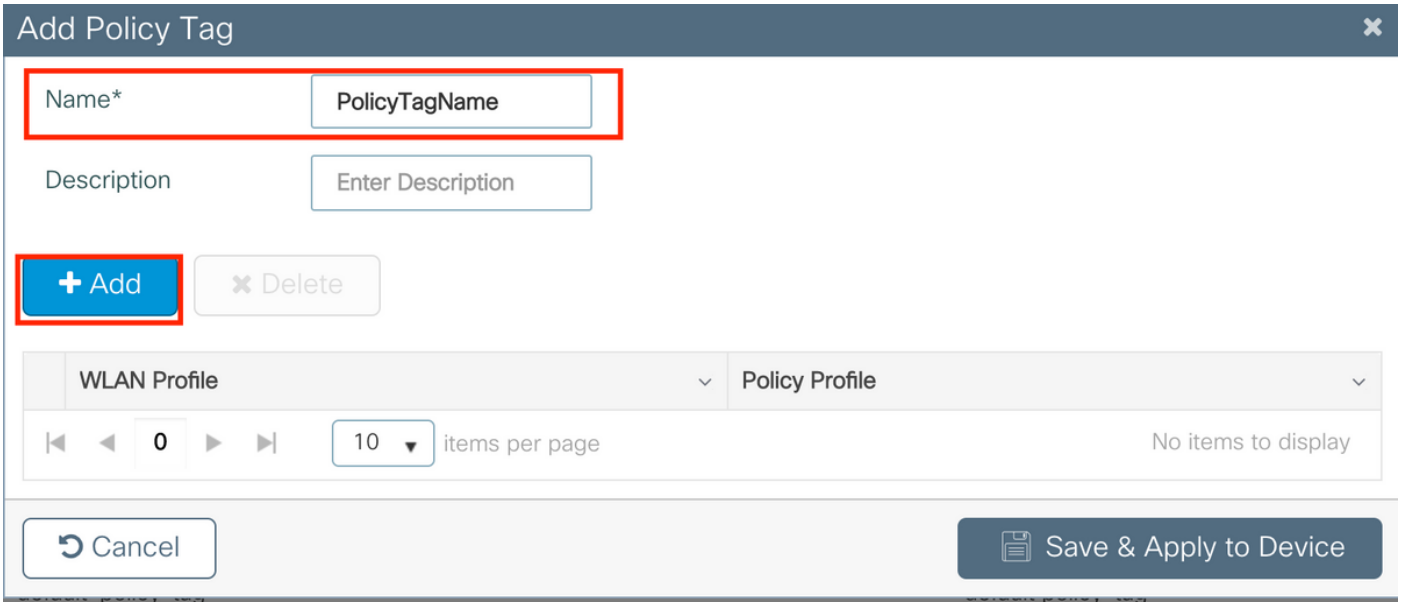
> **注**:default-policy-tagは、WLAN IDが1 ～ 16のSSIDをdefault-policy-profileに自動的にマッピングします。IDが17以上のWLANがある場合は、default-policy-tagを使用できません。

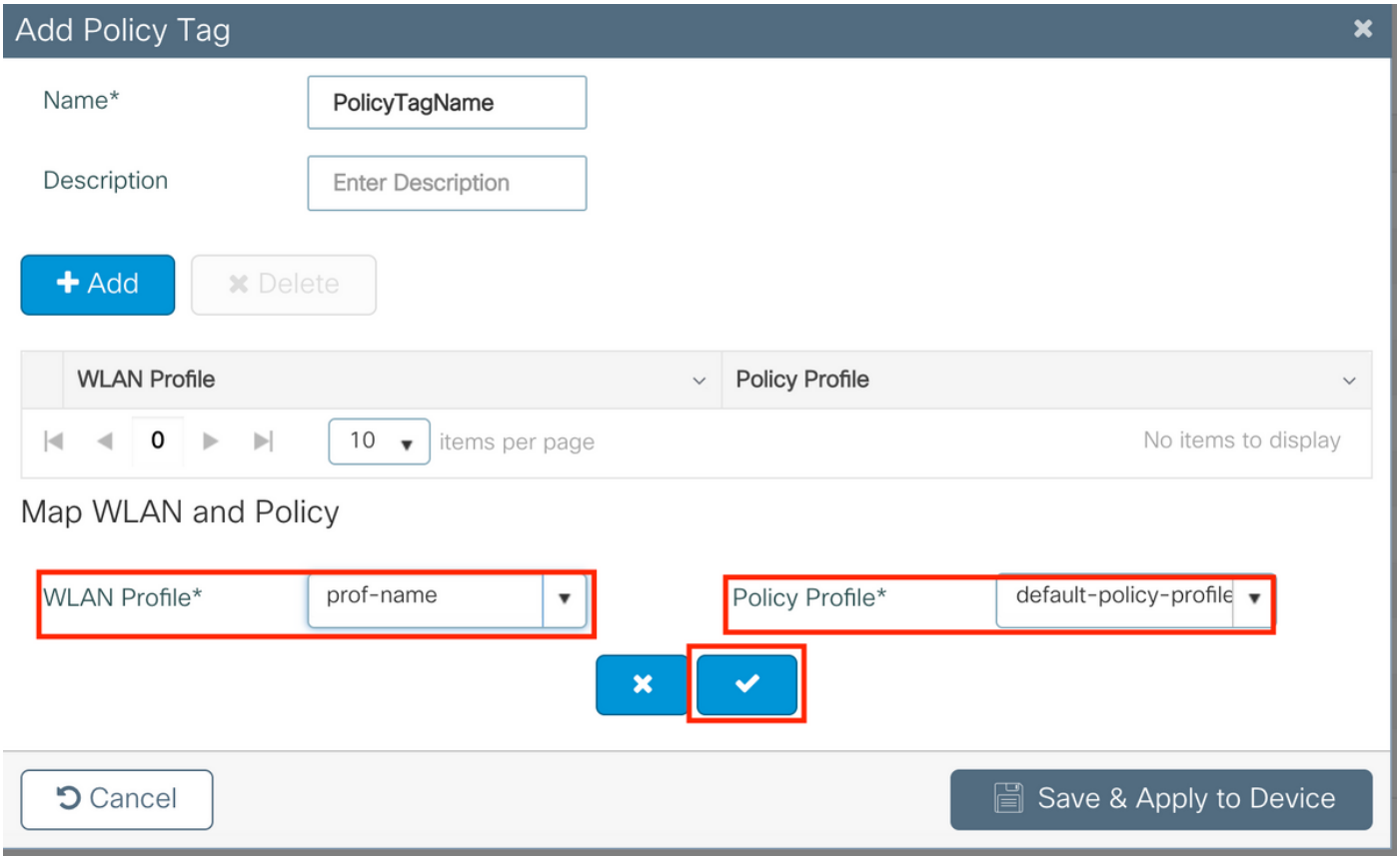
GUI：

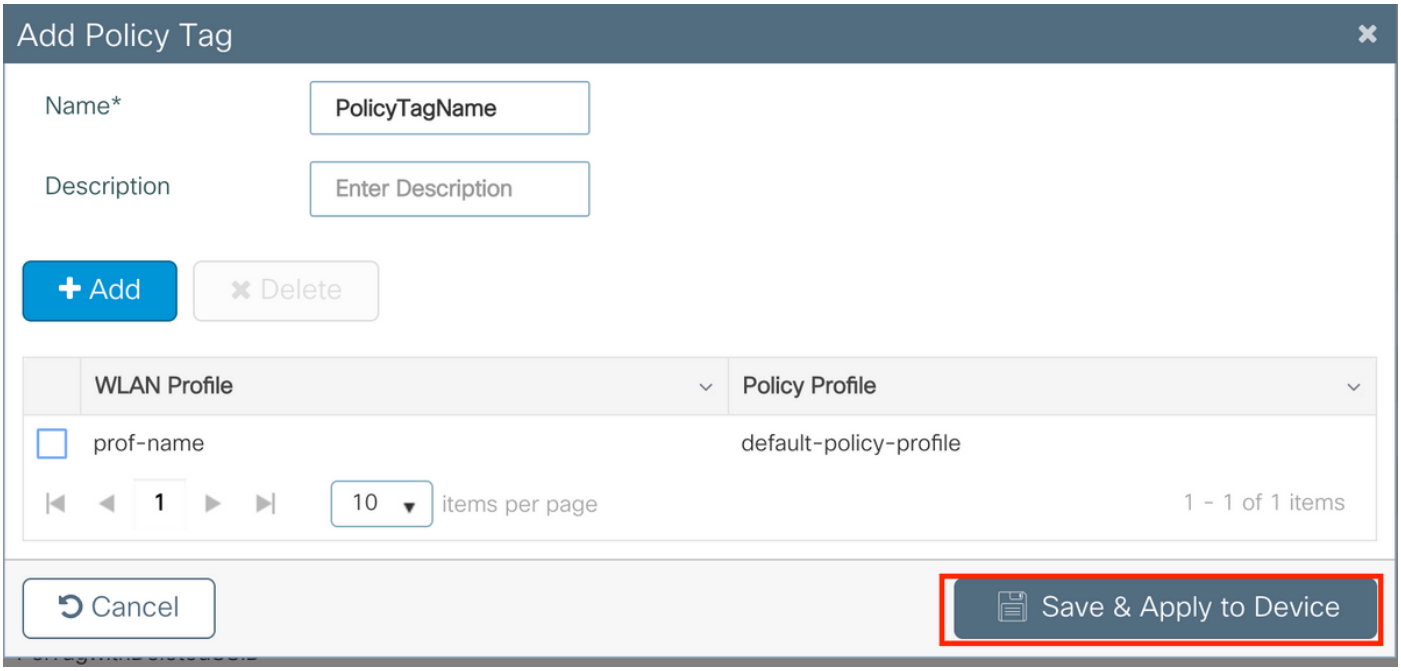
[Configuration] > [Tags & Profiles] > [Tags] > [Policy]に移動し、必要に応じて新しいタグを追加します。



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。







CLI：

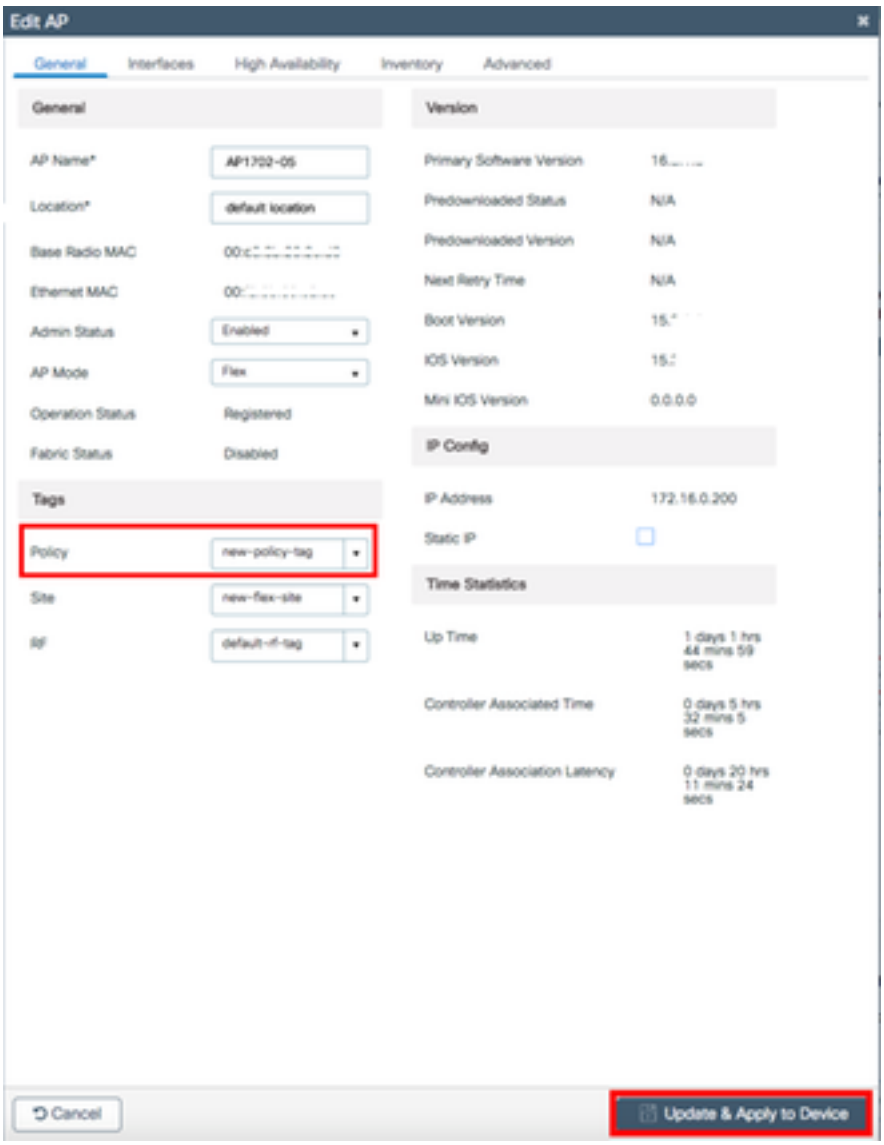
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

ポリスタグの割り当て

APにポリスタグを割り当てます

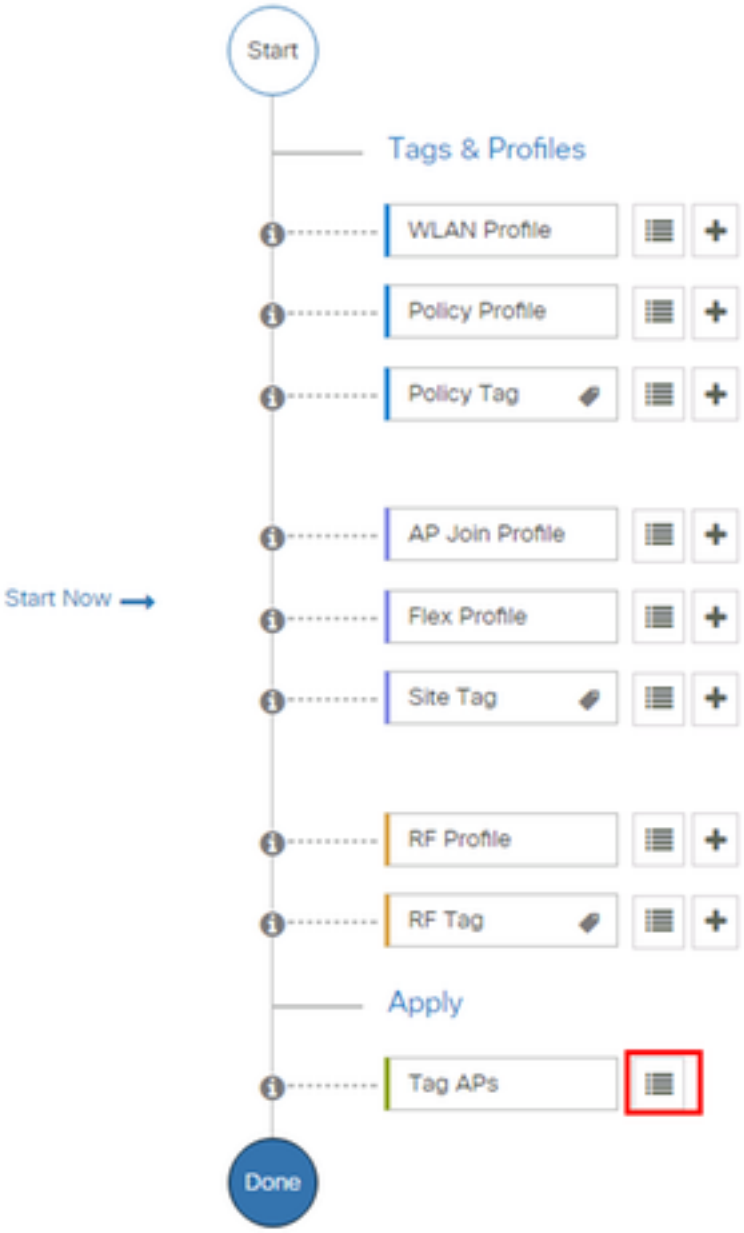
GUI

タグを1つのAPに割り当てるには、[Configuration] > [Wireless] > [Access Points] > [AP Name] > [General Tags]に移動し、必要な割り当てを行い、[Update & Apply to Device]をクリックします。

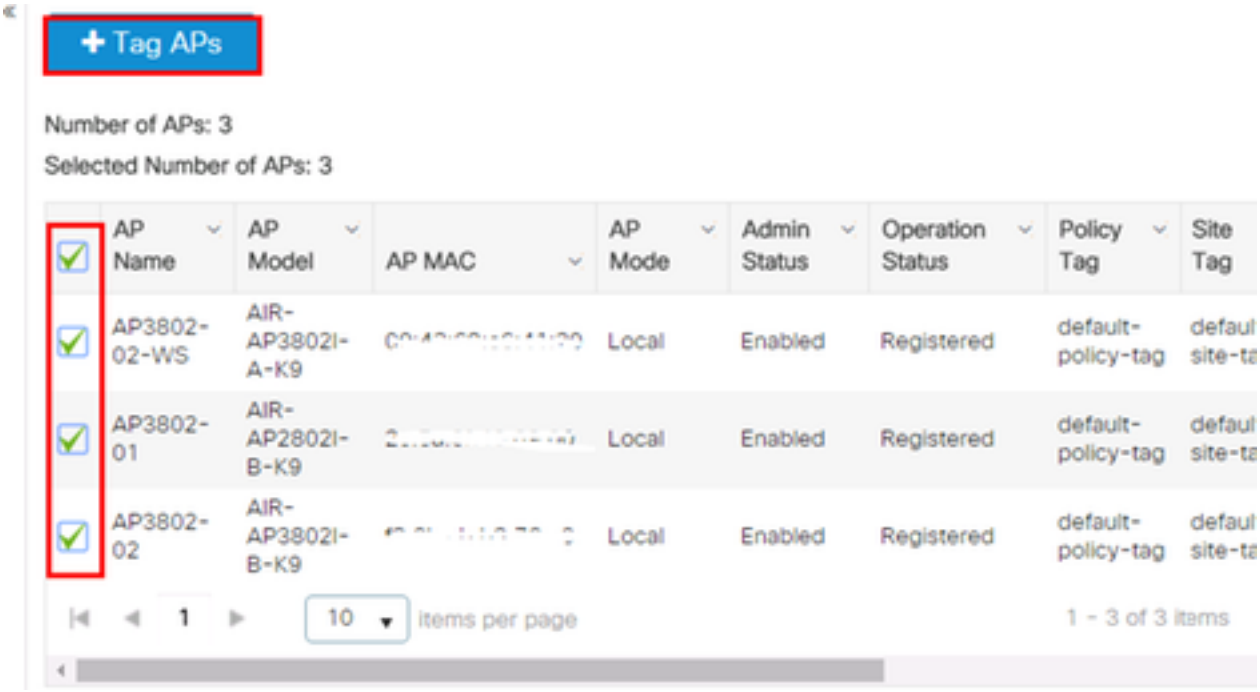


> **注**:APでポリスタグを変更すると、9800 WLCへの関連付けが失われ、約1分以内に再び参加することに注意してください。

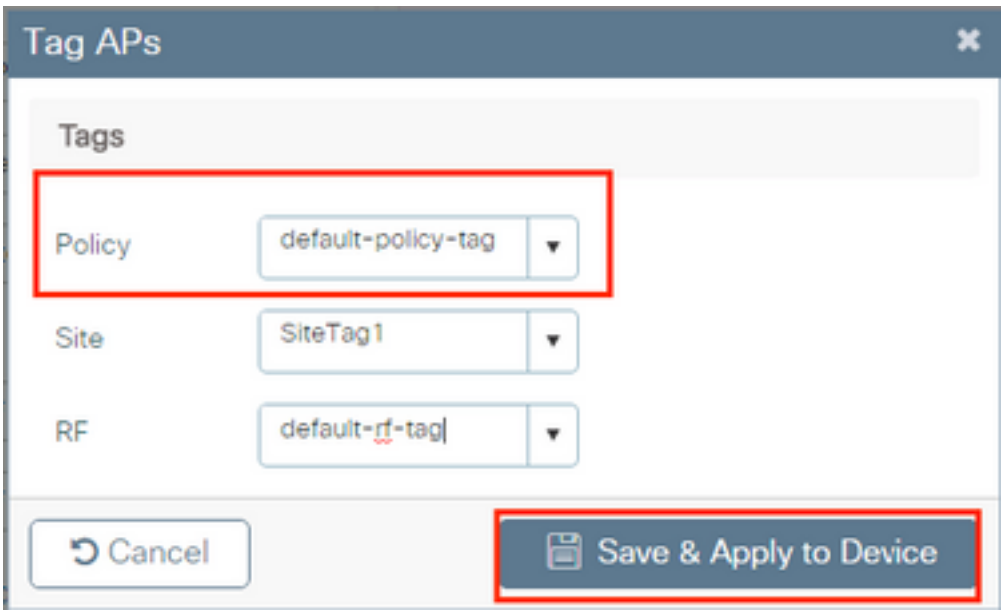
複数のAPに同じポリシータグを割り当てるには、[Configuration] > [Wireless] > [Wireless Setup] > [Start Now] > [Apply]に移動します。



タグを割り当てるAPを選択し、[+ Tag APs]をクリックします



白いタグを選択し、[Save & Apply to Device]をクリックします



CLI

```
# config t
# ap <ethernet-mac-addr>
# policy-tag <policy-tag-name>
# end
```

ISE の設定

ISE v1.2設定の場合は、次のリンクを確認します。

ISE の設定

確認

次のコマンドを使用して、現在の設定を確認できます

```
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

トラブルシュート

WLC 9800には、ALWAYS-ONトレース機能が備わっています。これにより、すべてのクライアント接続関連のエラー、wanringおよび通知レベルのメッセージが常に記録され、インシデントまたは障害発生後のログを表示できます。

注：生成されるログの量に応じて、数時間から数日を遡ることができます。

9800 WLCがデフォルトで収集したトレースを表示するには、SSH/Telnet経由で9800 WLCに接続し、次の手順に従います（セッションをテキストファイルにロギングしていることを確認してください）。

ステップ1：コントローラの現在の時刻を確認して、問題が発生した時刻に戻る時刻にログを追跡します。

```
# show clock
```

ステップ2：システム設定の指示に従って、コントローラのバッファまたは外部syslogからsyslogを収集します。これにより、システムの状態やエラーが表示されます（存在する場合）。

```
# show logging
```

ステップ3：デバッグ条件が有効になっているかどうかを確認します。

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

注：何らかの条件が表示されている場合は、有効な条件（MACアドレス、IPアドレスなど）に遭遇するすべてのプロセスについて、トレースがデバッグレベルまで記録されているこ

とを意味します。 これにより、ログの量が増加します。したがって、アクティブにデバッグしていない場合は、すべての条件をクリアすることをお勧めします

ステップ4：テスト中のMACアドレスがステップ3の条件としてリストされなかったと仮定して、特定のMACアドレスのalways-on noticeレベルのトレースを収集します。

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file
always-on-<FILENAME.txt>
```

セッションの内容を表示することも、ファイルを外部TFTPサーバにコピーすることもできます。

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

条件付きデバッグと無線アクティブトレース

常にオンのトレースが十分な情報を得ずに調査中の問題のトリガーを判断できない場合は、条件付きデバッグを有効にして、Radio Active(RA)トレースをキャプチャできます。このトレースは、指定された条件（クライアントMACアドレス）と対話します。 条件付きデバッグを有効にするには、次の手順を実行します。

ステップ5：デバッグ条件が有効になっていないことを確認します。

```
# clear platform condition all
```

ステップ6：モニタするワイヤレスクライアントMACアドレスのデバッグ条件を有効にします。

このコマンドは、指定されたMACアドレスの監視を30分（1800秒）開始します。 この時間は、オプションで最大2085978494秒まで増やすことができます。

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

注:複数のクライアントを同時に監視するには、MACアドレスごとにdebug wireless mac <aaaa.bbbb.cccc>コマンドを実行します。

注:後で表示するために、すべてが内部でバッファリングされるため、ターミナルセッションでのクライアントアクティビティの出力は表示されません。

ステップ7：監視する問題または動作を再現します。

ステップ8：デフォルトまたは設定済みのモニタ時間がアップする前に問題が再現された場合は、デバッグを停止します。

```
# no debug wireless mac <aaaa.bbbb.cccc>
```
モニタ時間が経過するか、デバッグワイヤレスが停止すると、9800 WLCは次の名前のローカルファイルを生成します。

ra_trace_MAC_aaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

ステップ9:MACアドレスアクティビティのファイルを収集します。ra trace .logを外部サーバにコピーするか、出力を画面に直接表示できます。

RAトレースファイルの名前を確認します

```
# dir bootflash: | inc ra_trace
```
ファイルを外部サーバにコピーします。

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```
コンテンツを表示します。

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```
ステップ10：根本原因がまだ明らかでない場合は、デバッグレベルのログのより詳細なビューである内部ログを収集します。クライアントを再度デバッグする必要はありません。これは、すでに収集され、内部に保存されているデバッグログを詳細に調べるためです。

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }
to-file ra-internal-<FILENAME>.txt
```

> **注**：このコマンド出力は、すべてのプロセスのすべてのロギングレベルのトレースを返し、非常に大量です。これらのトレースの解析に役立つように、Cisco TACにご連絡ください。

ra-internal-FILENAME.txtを外部サーバにコピーするか、出力を画面に直接表示します。

ファイルを外部サーバにコピーします。

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```
コンテンツを表示します。

```
# more bootflash:ra-internal-<FILENAME>.txt
```
ステップ11：デバッグ条件を削除します。

```
# clear platform condition all
```

> **注**：トラブルシューティングセッションの後は、必ずデバッグ条件を削除してください。