Catalyst 9800およびFlexConnect OEAPスプリットトンネリングの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[概要](#)
[背景説明](#)
[設定](#)
[ネットワーク図](#)
[設定](#)
[スプリットトンネリング用のアクセスコントロールリスト(ACL)の定義](#)
[定義されたACLへのACLポリシーのリンク](#)
[ワイヤレスプロファイルポリシーとスプリットMAC ACL名の設定](#)
[WLANのポリシープロファイルへのマッピング](#)
[AP加入プロファイルの設定とサイトタグとの関連付け](#)
[アクセスポイントへのポリシータグとサイタグの接続](#)
[確認](#)
[関連資料](#)

概要

このドキュメントでは、屋内アクセスポイント(AP)をFlexConnect Office Extend(OEAP)として設定する方法と、スプリットトンネリングを有効にして、ホームオフィスでローカルにスイッチングできるトラフィックと、WLCで中央でスイッチングする必要があるトラフィックを定義する方法について説明します。

前提条件

要件

このドキュメントの設定では、NATが有効なDMZでWLCがすでに設定されており、APがホームオフィスからWLCに参加できることを前提としています。

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。

- Cisco IOS-XE 17.3.1ソフトウェアが稼働するワイヤレスLANコントローラ(WLC)9800。
- Wave1 AP:1700/2700/3700.
- Wave2 AP:1800/2800/3800/4800、およびCatalyst 9100シリーズ。

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。

概要

Cisco OfficeExtendアクセスポイント(Cisco OEAP)は、Cisco WLCからリモートのCisco APへのセキュアな通信を提供し、企業WLANをインターネット経由で従業員の自宅にシームレスに拡張します。ホームオフィスでのユーザエクスペリエンスは、企業オフィスでのユーザエクスペリエンスとまったく同じです。アクセスポイントとコントローラ間のDatagram Transport Layer Security(DTLS)暗号化により、すべての通信のセキュリティが最高レベルになります。
FlexConnectモードの屋内APは、OEAPとして機能できます。

背景説明

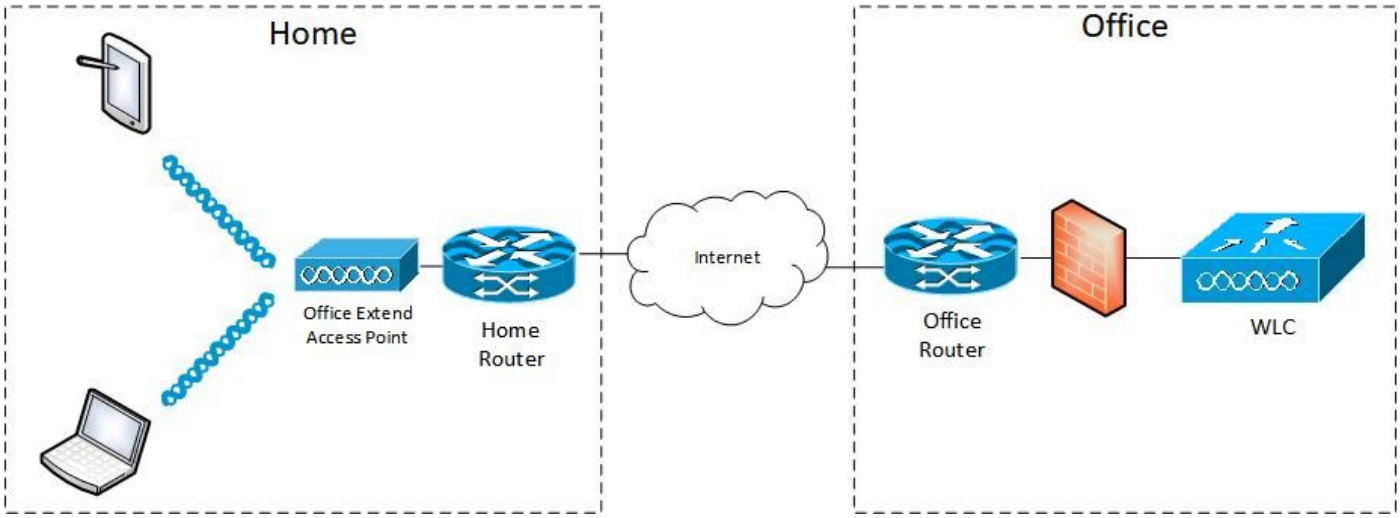
FlexConnectとは、アクセスポイント(AP)がWAN経由などでリモートロケーションで動作しながらワイヤレスクライアントを処理する機能のことです。また、ワイヤレスクライアントからのトラフィックをAPレベル（ローカルスイッチング）でネットワークに直接配置するか、またはトラフィックを9800コントローラ（中央スイッチング）に集中してWAN経由でWLANごとに送信するかを決定できます。

FlexConnectの詳細については、このドキュメントの「Catalyst 9800ワイヤレスコントローラでのFlexConnectについて」を参照してください。

OEAPモードは、FlexConnect APで使用できるオプションで、ホームアクセス用の個人用ローカルSSIDなどの追加機能を使用できます。また、スプリットトンネリング機能を使用して、ホームオフィスでローカルにスイッチングするトラフィックとWLCで中央でスイッチングするトラフィックを定義できます

設定

ネットワーク図



設定

スプリットトンネリング用のアクセスコントロールリスト(ACL)の定義

ステップ1:[Configuration] > [Security] > [ACL]を選択します。[Add]を選択します。

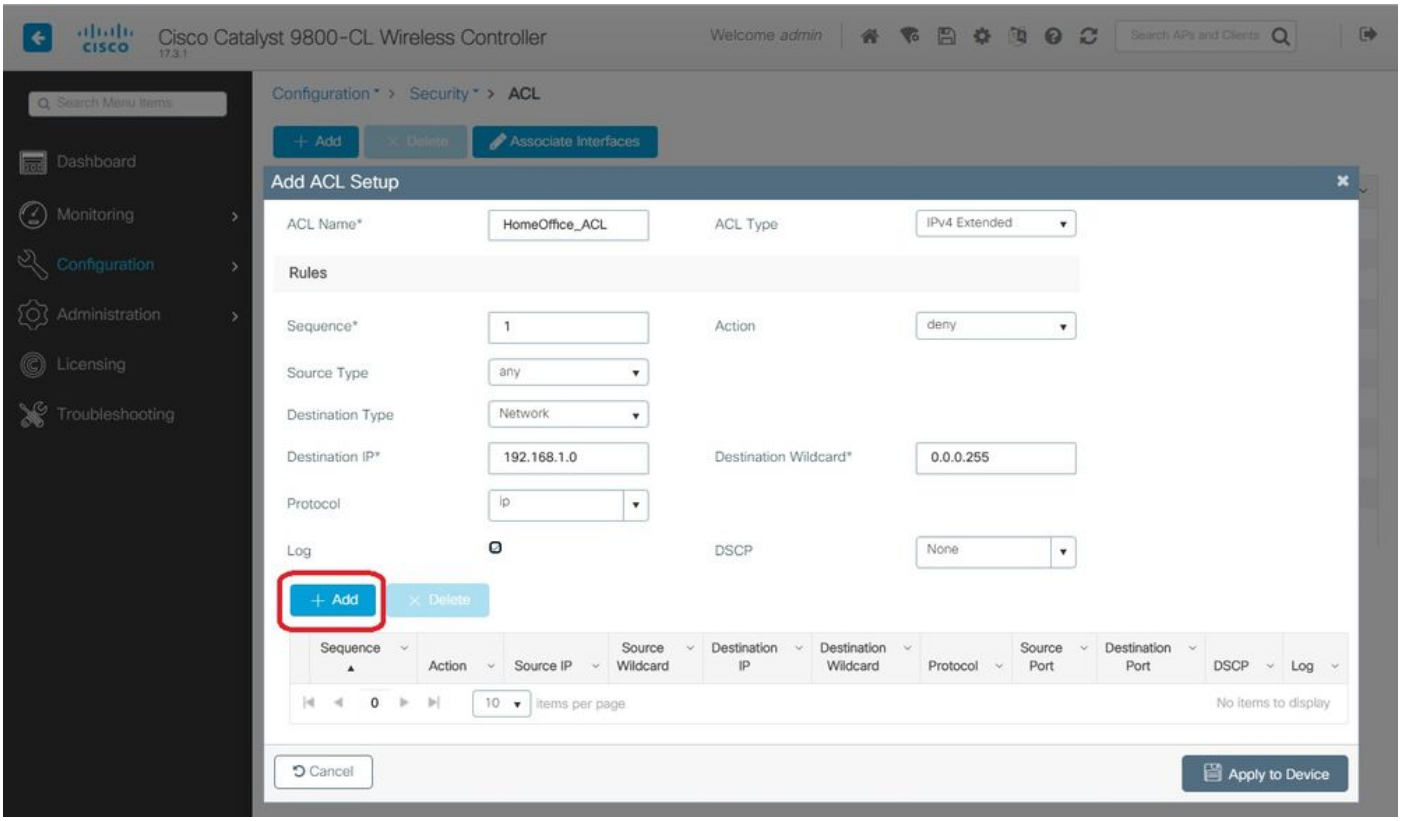
ステップ2:[Add ACL Setup]ダイアログボックスで、[ACL Name]を入力し、[ACL Type]ドロップダウンリストからACLタイプを選択し、[Rules]設定で[Sequence number]を入力します。次に、[Action]で[permit]または[deny]を選択します。

ステップ3:[Source Type]ドロップダウンリストから必要なソースタイプを選択します。

送信元タイプとして[Host]を選択した場合は、[Host Name/IP]を入力する必要があります。

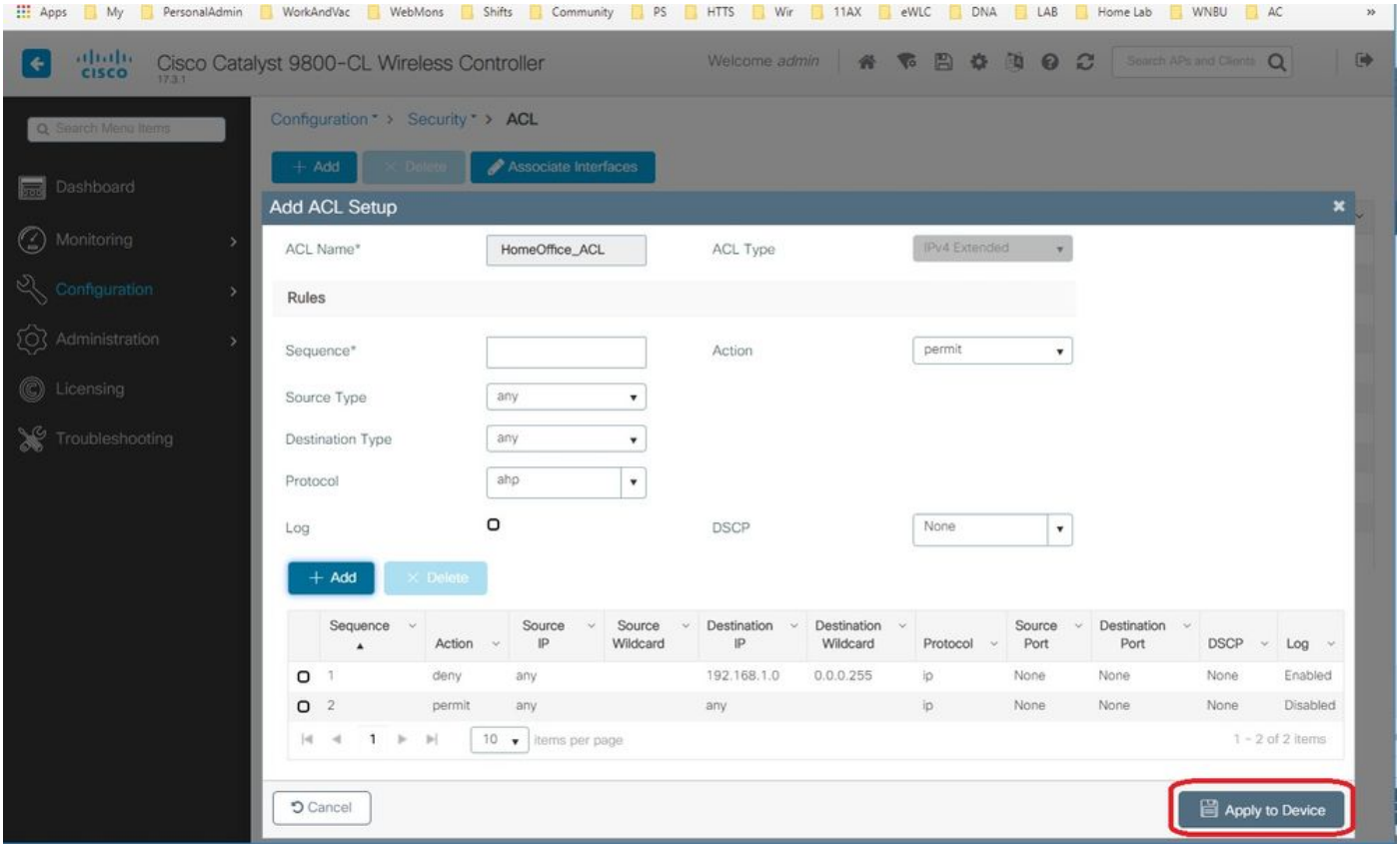
送信元タイプとして[Network]を選択した場合は、送信元IPアドレスと送信元ワイルドカードマスクを指定する必要があります。

この例では、任意のホストからサブネット192.168.1.0/24へのすべてのトラフィックが中央でスイッチング（拒否）され、残りのトラフィックはすべてローカルでスイッチング（許可）されます。



ステップ4：ログが必要な場合は[Log]チェックボックスをオンにし、[Add]を選択します。

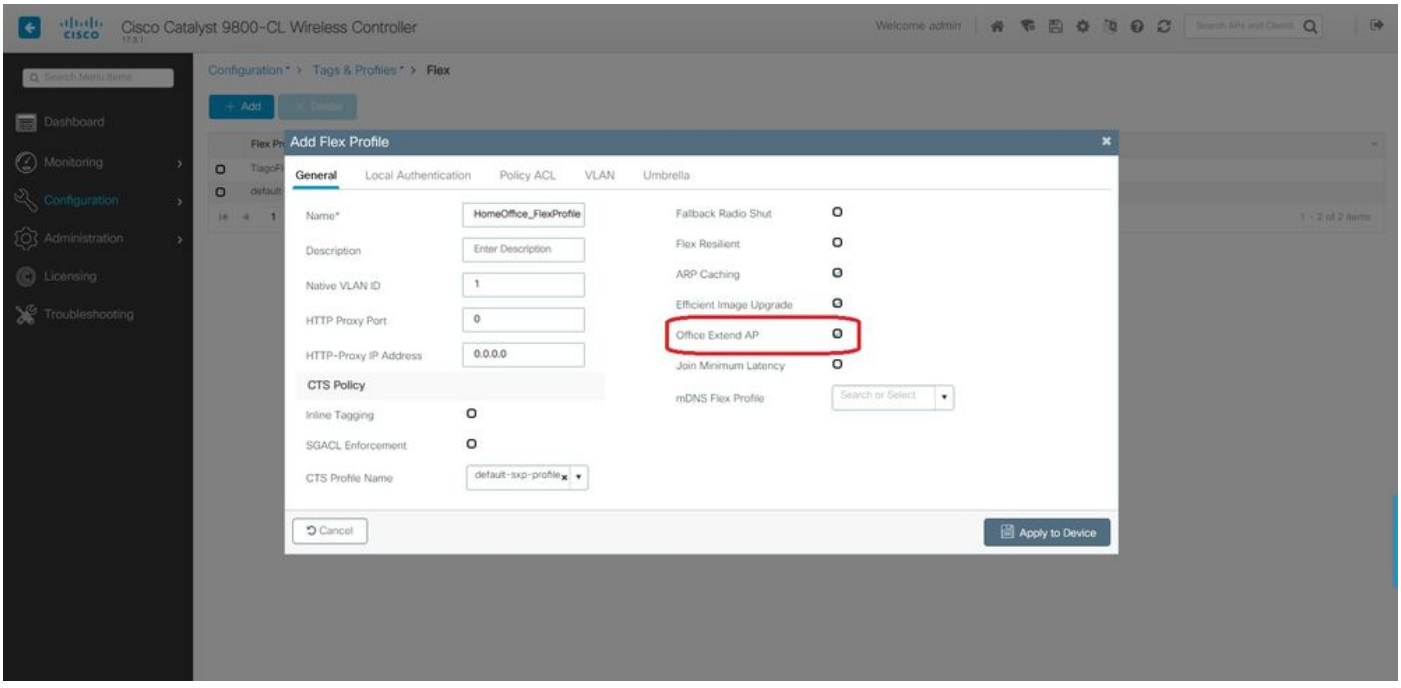
ステップ5：残りのルールを追加し、[Apply to Device]を選択します。



定義されたACLへのACLポリシーのリンク

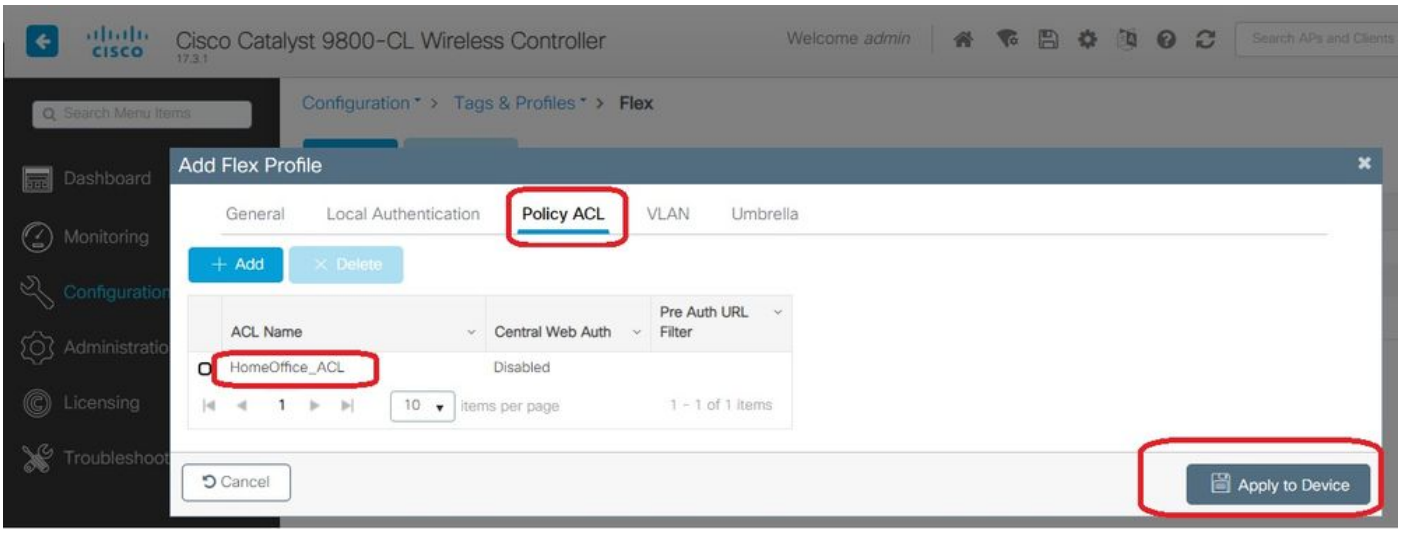
ステップ1：新しいFlexプロファイルを作成します。[Configuration] > [Tags & Profiles] > [Flex]に移動します。[Add]を選択します。

ステップ2：名前を入力し、OEAPを有効にします。また、ネイティブVLAN IDがAPスイッチポートのVLAN IDであることを確認します。



注：Office-Extendモードを有効にすると、リンク暗号化もデフォルトで有効になり、AP加入プロファイルでリンク暗号化を無効にしても変更できません。

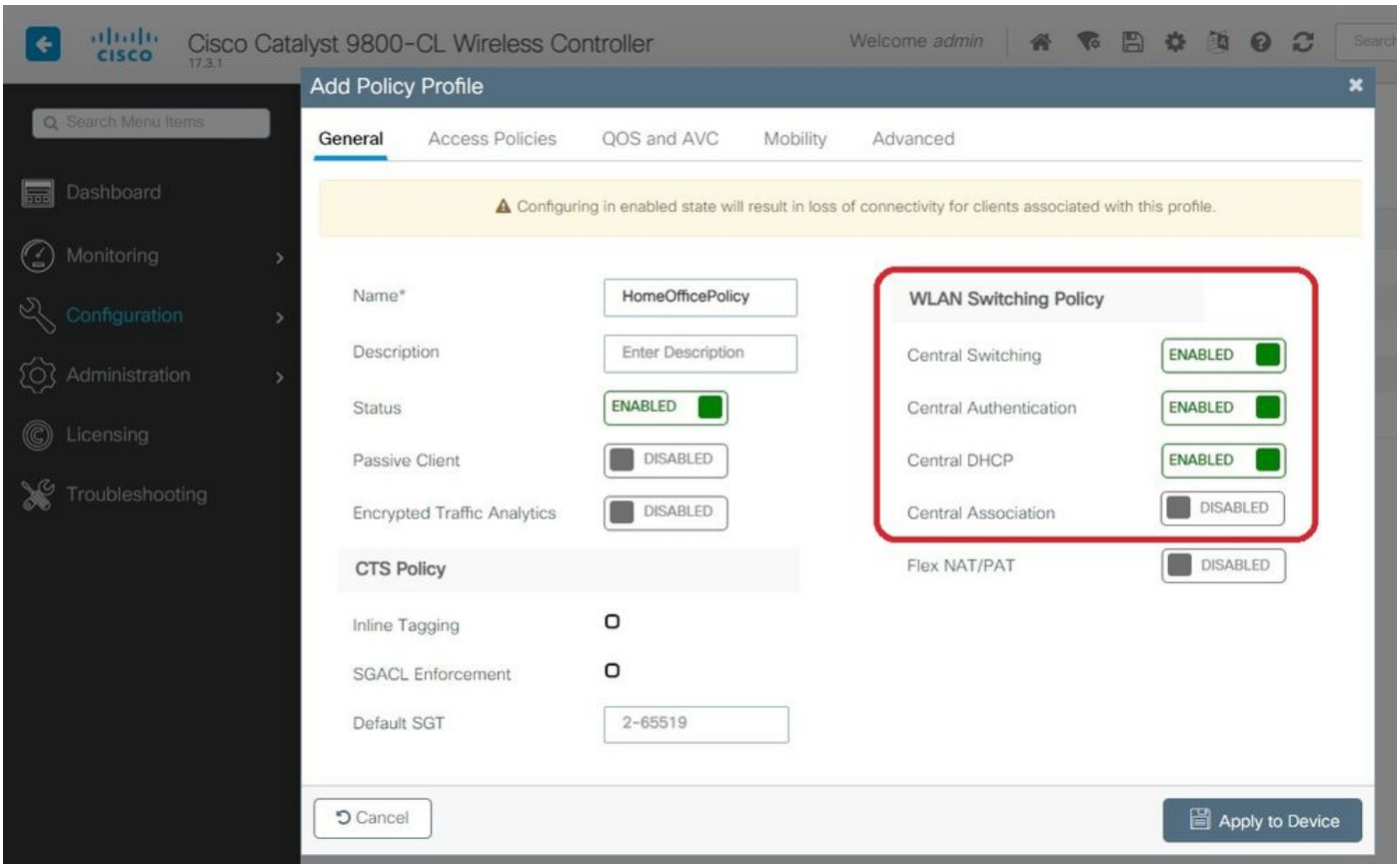
ステップ3:[Policy ACL]タブに移動し、[Add]を選択します。ここでは、ACLをプロファイルに追加し、デバイスに適用します。



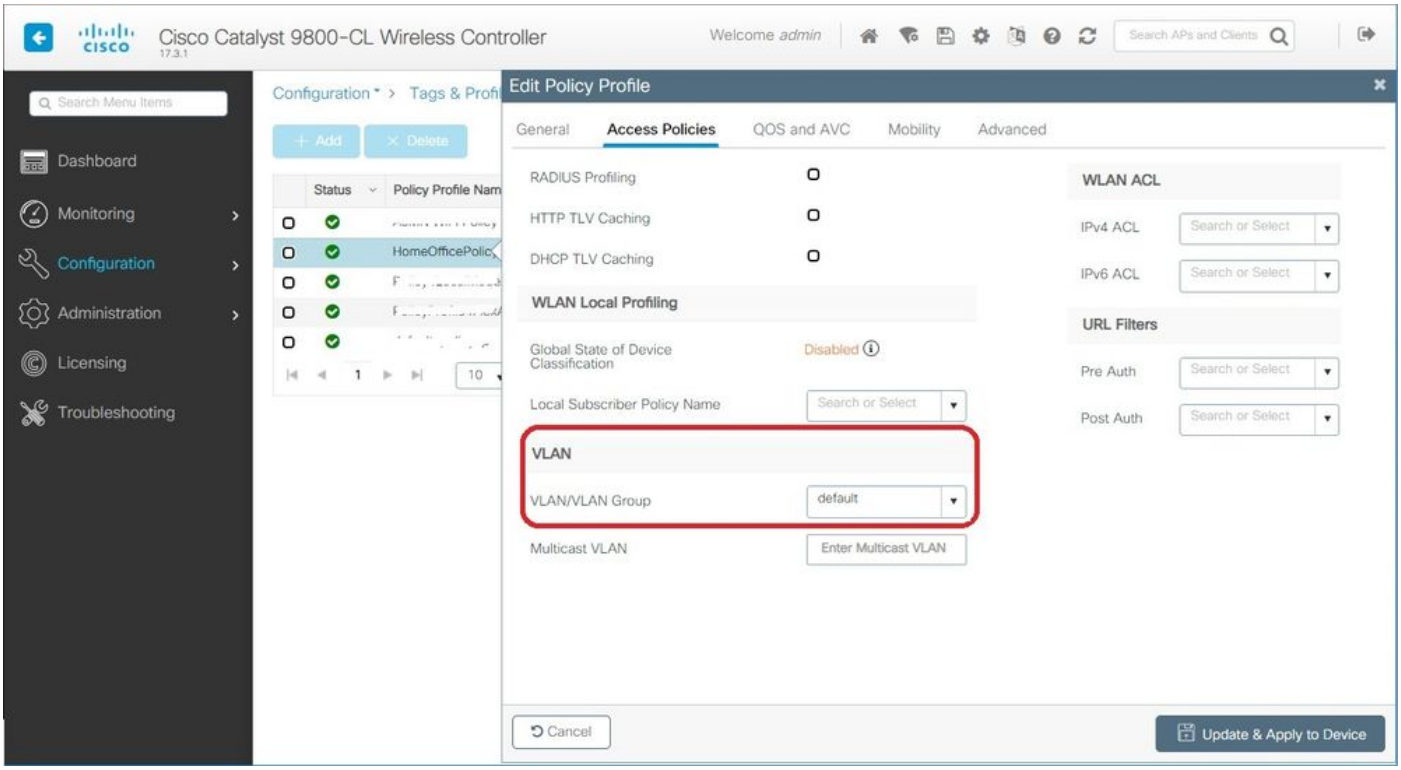
ワイヤレスプロファイルポリシーとスプリットMAC ACL名の設定

ステップ1:WLANプロファイルの作成。この例では、HomeOfficeという名前のSSIDとWPA2-PSKセキュリティを使用しています。

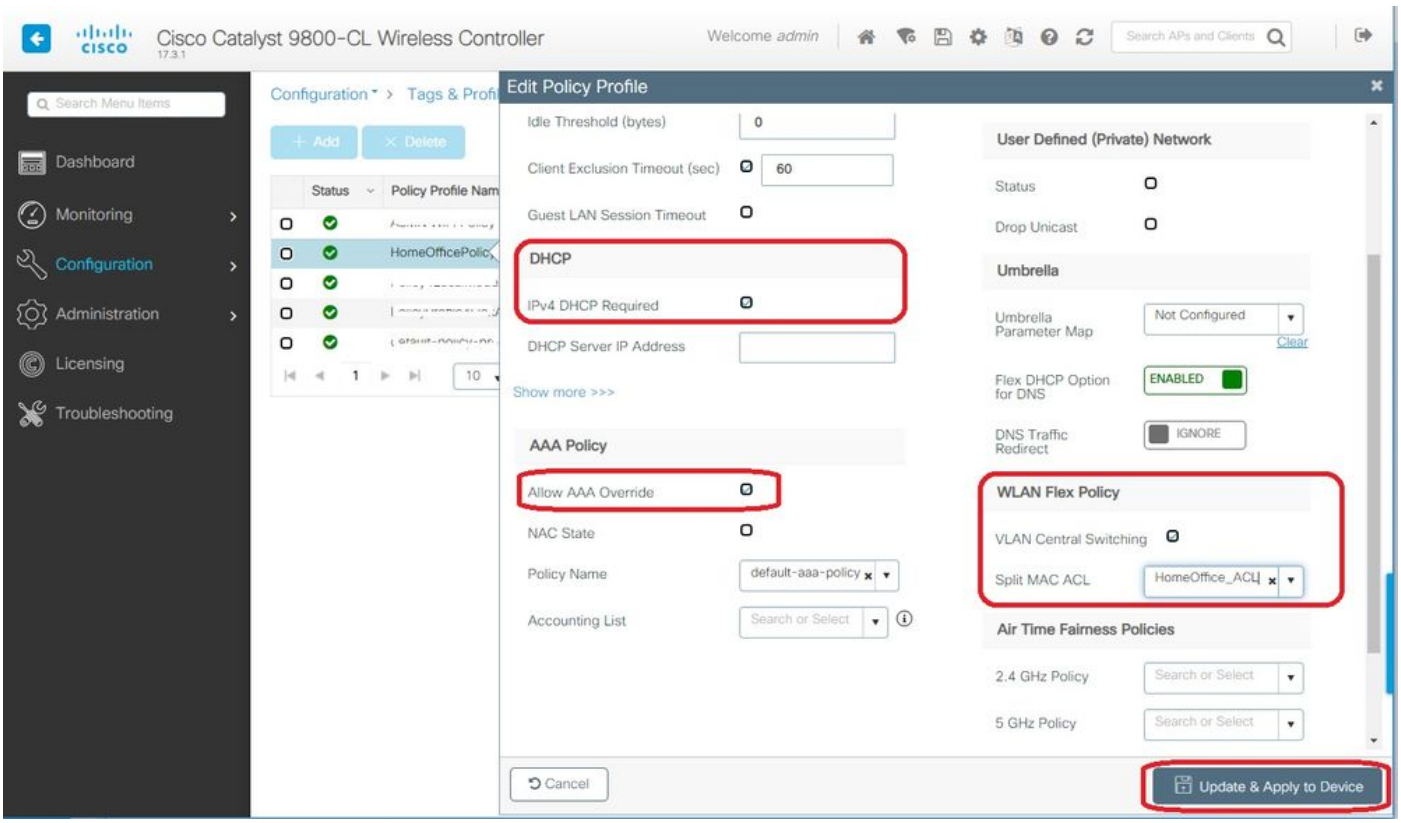
ステップ2：ポリシープロファイルを作成します。[Configuration] > [Tags] > [Policy]に移動し、[Add]を選択します。次の例に示すように、[General]の下で、このプロファイルが中央で切り替えられたポリシーであることを確認します。



ステップ3：ポリシープロファイル内で、[Access Policies]に移動し、中央でスイッチングされるトラフィックのVLANを定義します。クライアントは、このVLANに割り当てられたサブネットのIPアドレスを取得します。



ステップ4:APでローカルスプリットトンネリングを設定するには、WLANでDCHP Requiredが有効になっていることを確認する必要があります。これにより、スプリットWLANに関連付けられているクライアントがDHCPを実行します。このオプションは、[Policy Profile]の[Advanced]タブで有効にできます。[IPv4 DHCP Required]チェックボックスをオンにします。[WLAN Flex Policy]設定で、[Split MAC ACL]ドロップダウンリストから、以前に作成したスプリットMAC ACLを選択します。[Apply to Device]を選択します。



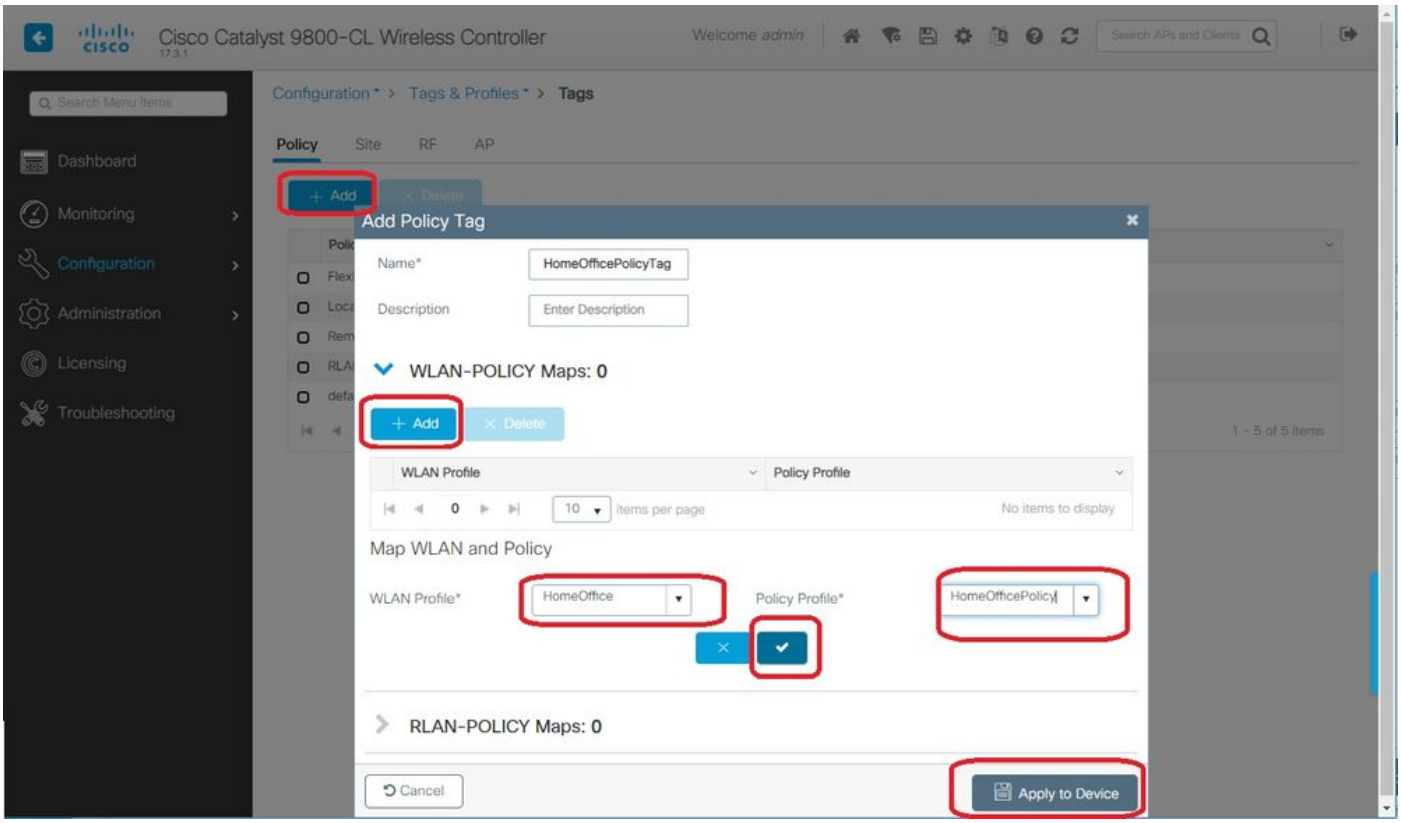
注：Apple iOSクライアントがスプリットトンネリングを機能させるには、DHCPオファーでオプション6(DNS)を設定する必要があります。

WLANのポリシープロファイルへのマッピング

ステップ1:[Configuration] > [Tags & Profiles] > [Tags]を選択します。[Policy]タブで[Add]を選択します。

ステップ2：タグポリシーの名前を入力し、[WLAN-POLICY Maps]タブで[Add]を選択します。

ステップ3:[WLAN Profile]ドロップダウンリストからWLANプロファイルを選択し、[Policy Profile]ドロップダウンリストからポリシープロファイルを選択します。[ティック]アイコンを選択し、[デバイスに適用]を選択します。

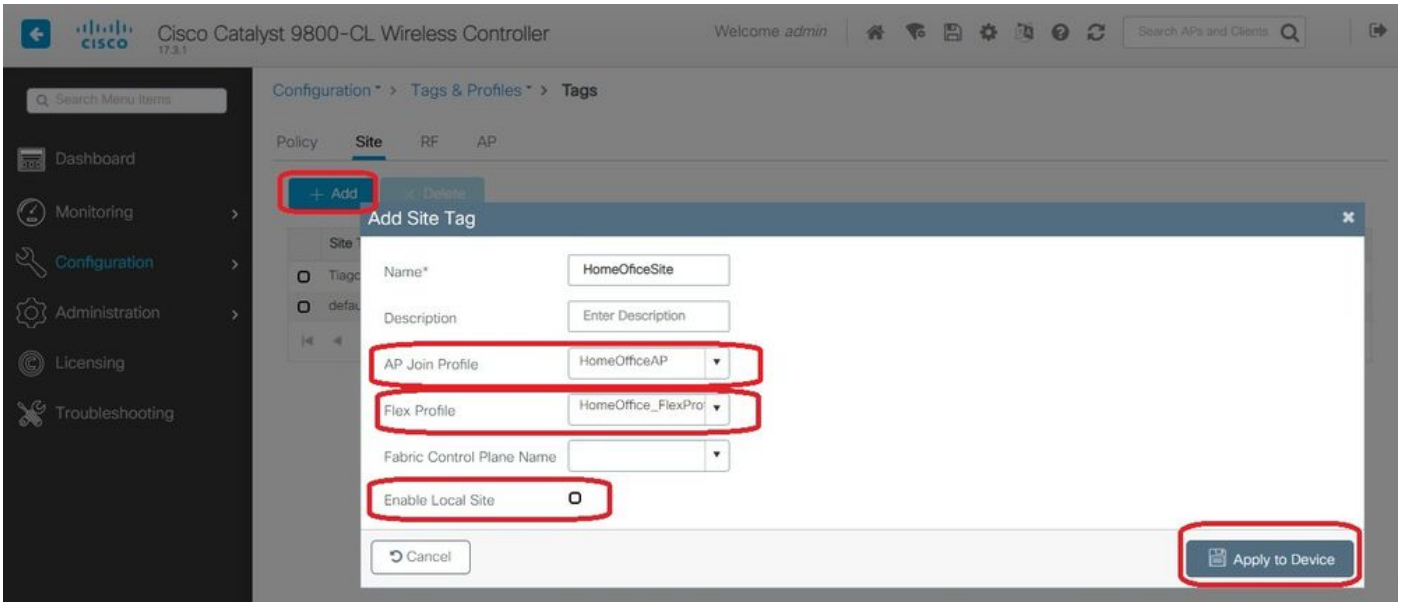


AP加入プロファイルの設定とサイトタグとの関連付け

ステップ1:[Configuration] > [Tags & Profiles] > [AP Join]に移動し、[Add]を選択します。名前を入力します。必要に応じて、SSHを有効にしてトラブルシューティングを許可し、必要がなければ後で無効にできます。

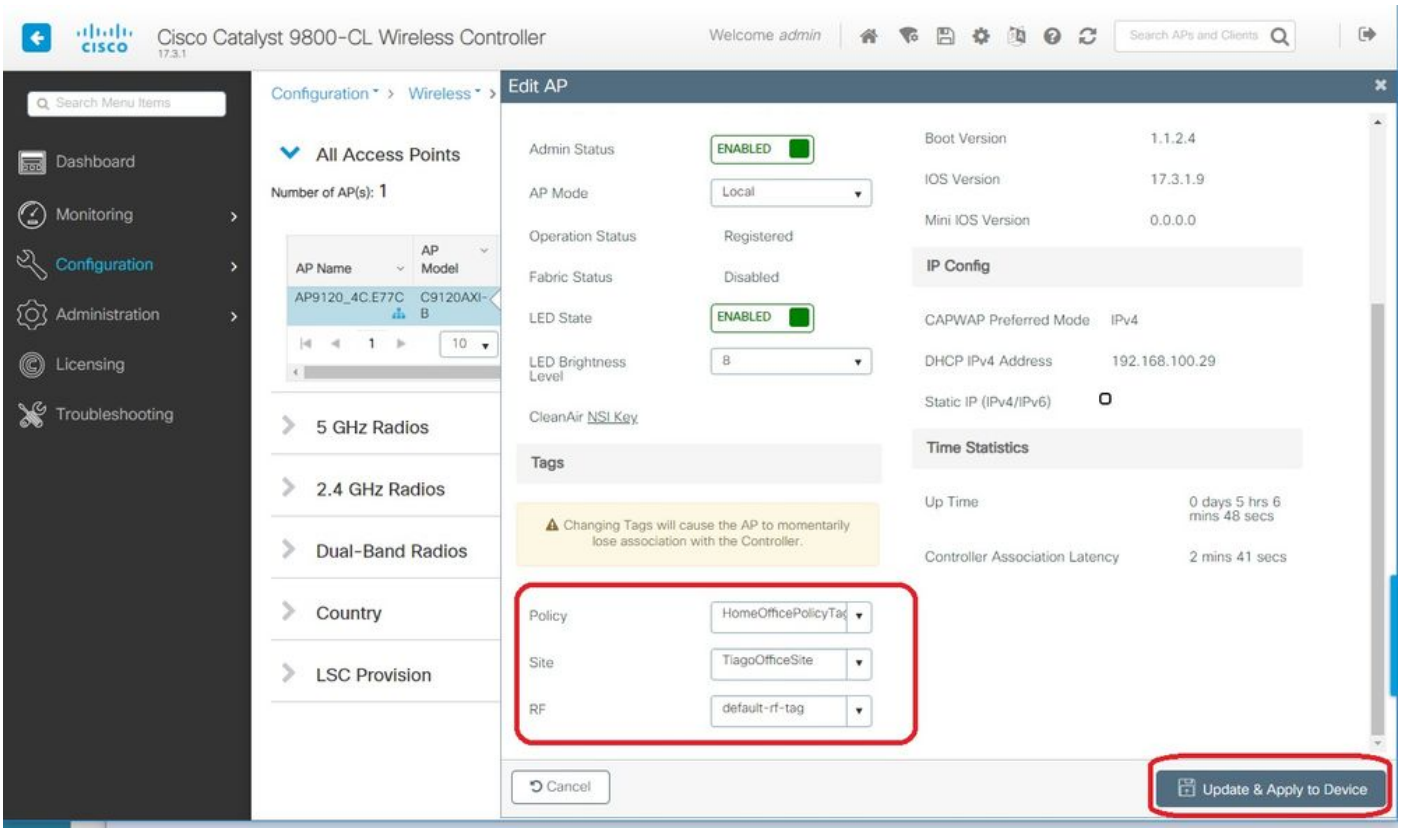
ステップ2:[Configuration] > [Tags & Profiles] > [Tags]を選択します。[Site]タブで[Add]を選択します。

ステップ3：サイトタグの名前を入力し、[Enable Local Site]のチェックマークを外し、ドロップダウンリストから[AP Join Profile]と[Flex Profile]（以前に作成）を選択します。[Apply to Device]を選択します。

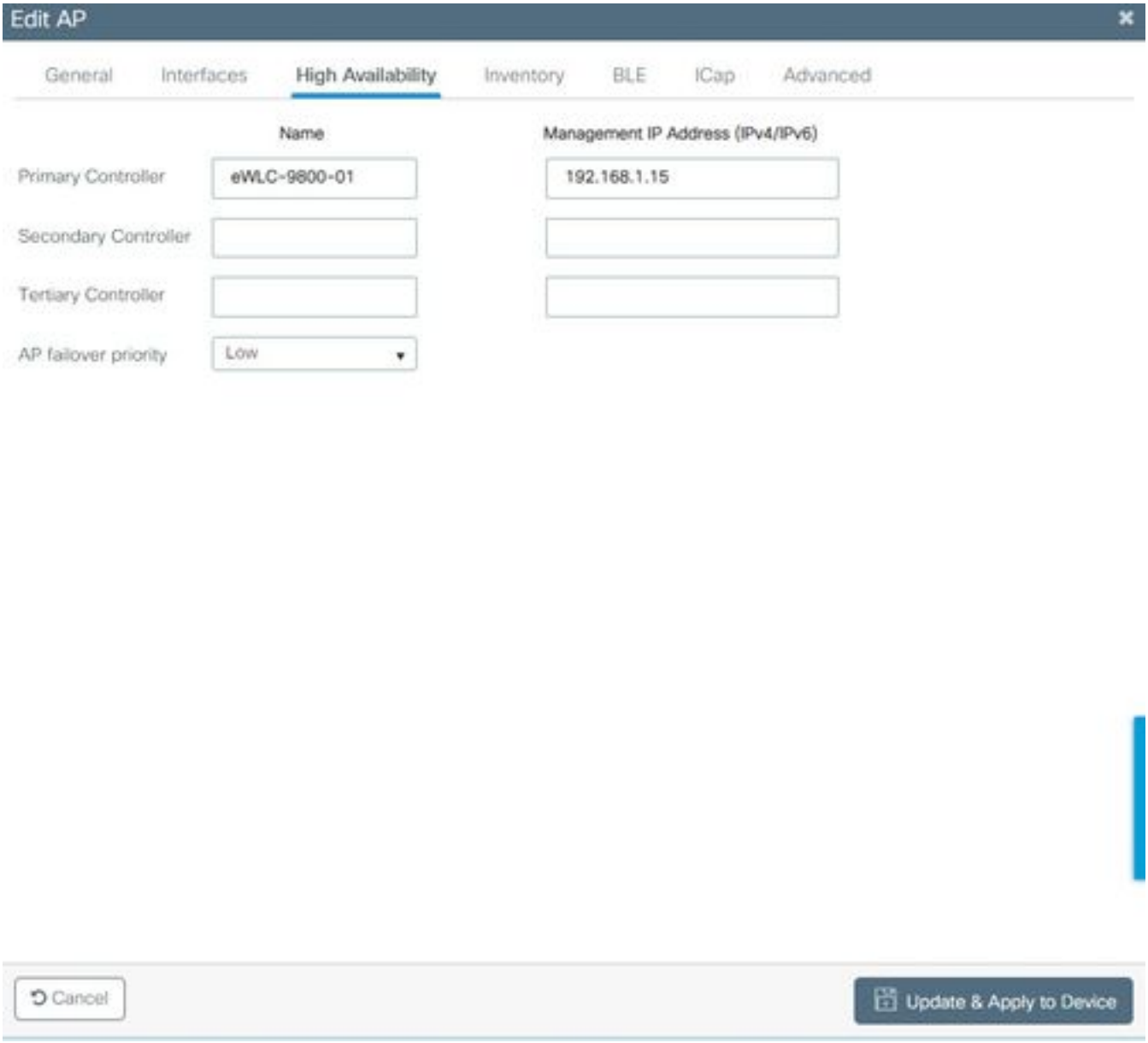


アクセスポイントへのポリシータグとサイタグの接続

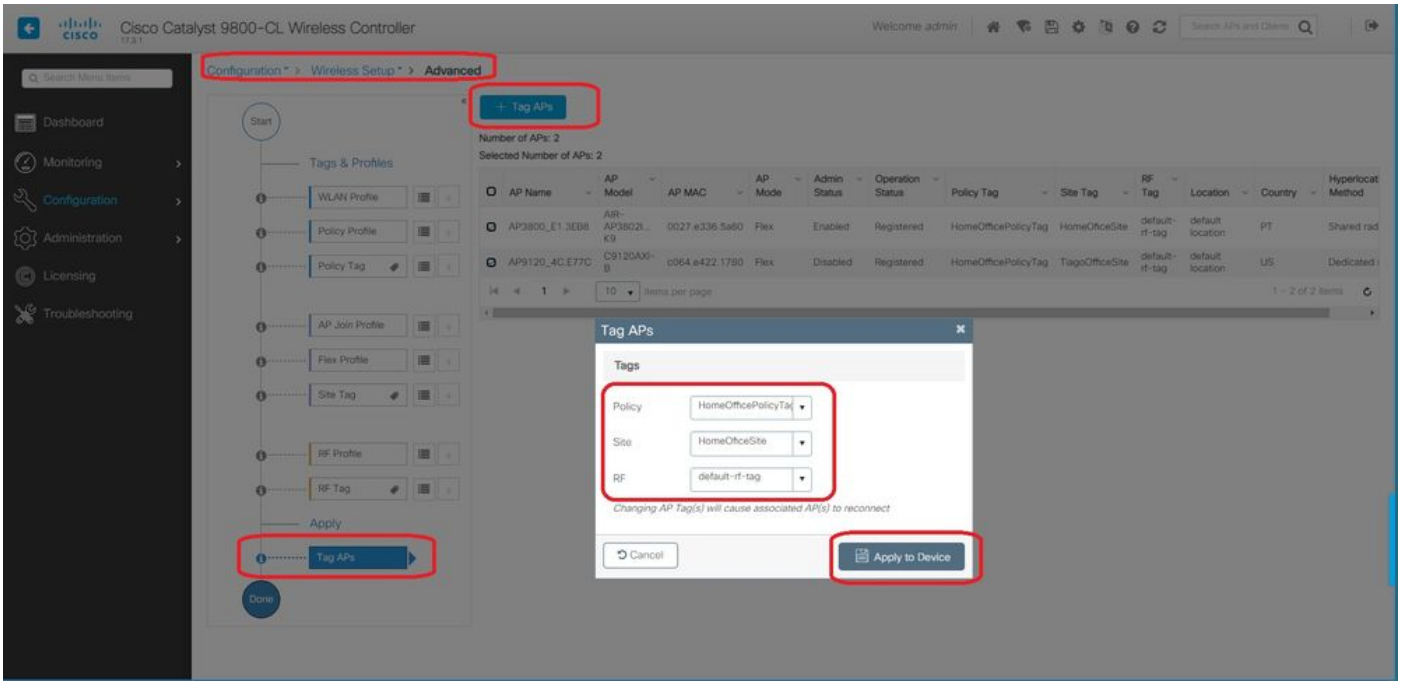
オプション1：このオプションでは、一度に1つのAPを設定する必要があります。[Configuration] > [Wireless] > [Access Points]に移動します。ホームオフィスに移動するAPを選択し、[Home Office Tags]を選択します。[Update and Apply to Device]を選択します。



また、APがホームオフィスに導入された後に到達するWLCのIP/名前を認識できるように、プライマリコントローラを設定することを推奨します。この編集は、APを直接[High Availability]タブに移動して行うことができます。



オプション2：このオプションでは、複数のAPを同時に設定できます。[Configuration] > [Wireless Setup] > [Advanced] > [Tag APs]に移動します。前に作成したタグを選択し、[Apply to Device]を選択します。



APがリブートし、新しい設定でWLCに再接続します。

確認

GUIまたはCLIを使用して設定を確認できます。CLIでの設定は次のようになります。

```
!
ip access-list extended HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255 log
2 permit ip any any log
!
wireless profile flex HomeOffice_FlexProfile
acl-policy HomeOffice_ACL
office-extend
!
wireless profile policy HomeOfficePolicy
no central association
aaa-override
flex split-mac-acl HomeOffice_ACL
flex vlan-central-switching
ipv4 dhcp required
vlan default
no shutdown
!
wireless tag site HomeOficeSite
flex-profile HomeOffice_FlexProfile
no local-site
!
wireless tag policy HomeOfficePolicyTag
wlan HomeOffice policy HomeOfficePolicy
!
wlan HomeOffice 5 HomeOffice
security wpa psk set-key ascii 0 xxxxxxx
no security wpa akm dot1x
security wpa akm psk
no shutdown
!
ap 70db.98e1.3eb8
```

```
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
ap c4f7.d54c.e77c
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
```

AP設定を確認しています。

```
eWLC-9800-01#show ap name AP3800_E1.3EB8 config general

Cisco AP Name : AP3800_E1.3EB8
=================================================

Cisco AP Identifier : 0027.e336.5a60
...
MAC Address : 70db.98e1.3eb8
IP Address Configuration : DHCP
IP Address : 192.168.1.99
IP Netmask : 255.255.255.0
Gateway IP Address : 192.168.1.254
...
SSH State : Enabled
Cisco AP Location : default location
Site Tag Name : HomeOficeSite
RF Tag Name : default-rf-tag
Policy Tag Name : HomeOfficePolicyTag
AP join Profile : HomeOfficeAP
Flex Profile : HomeOffice_FlexProfile
Primary Cisco Controller Name : eWLC-9800-01
Primary Cisco Controller IP Address : 192.168.1.15
...
AP Mode : FlexConnect
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : IPv4
CAPWAP UDP-Lite : Not Configured
AP Submode : Not Configured
Office Extend Mode : Enabled
...
```

APに直接接続し、設定を確認することもできます。

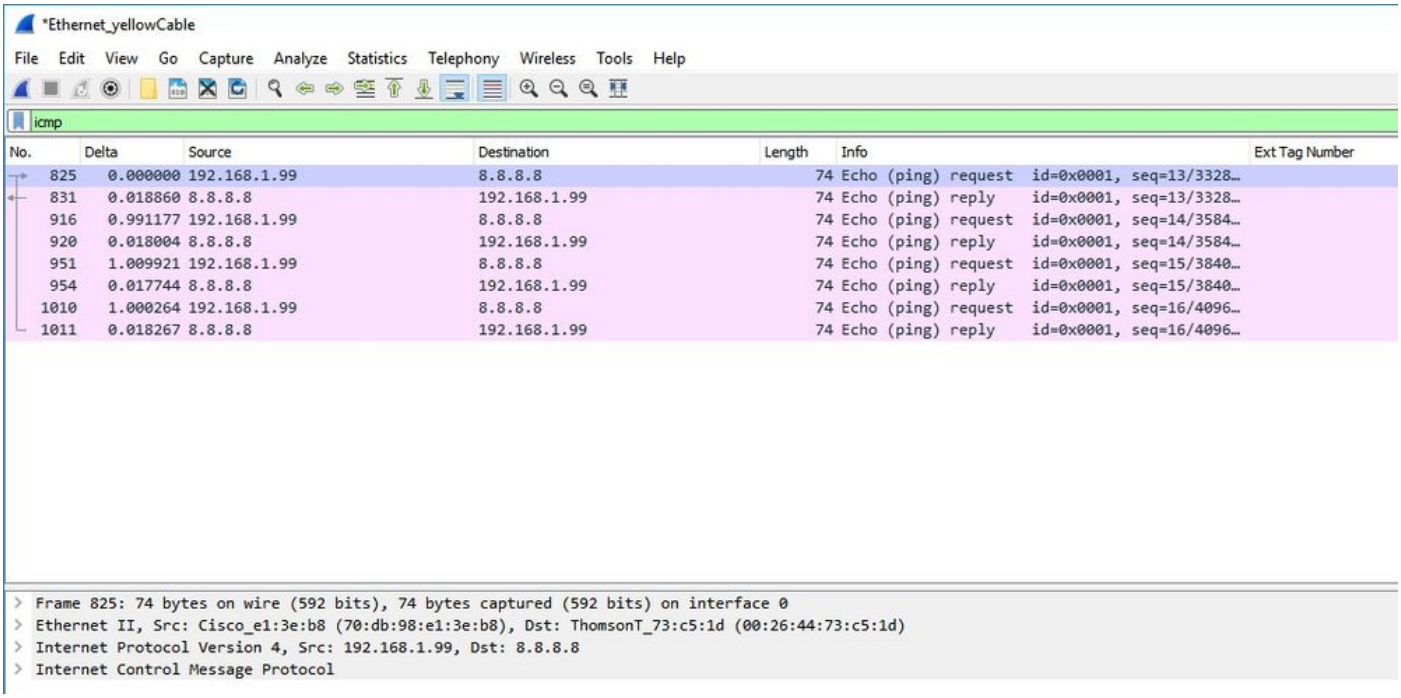
```
AP3800_E1.3EB8#show ip access-lists
Extended IP access list HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255
2 permit ip any any

AP3800_E1.3EB8#show capwap client detailrcb
SLOT 0 Config

SSID : HomeOffice
Vlan Id : 0
Status : Enabled
...
otherFlags : DHCP_REQUIRED VLAN_CENTRAL_SW
...
Profile Name : HomeOffice
...
```

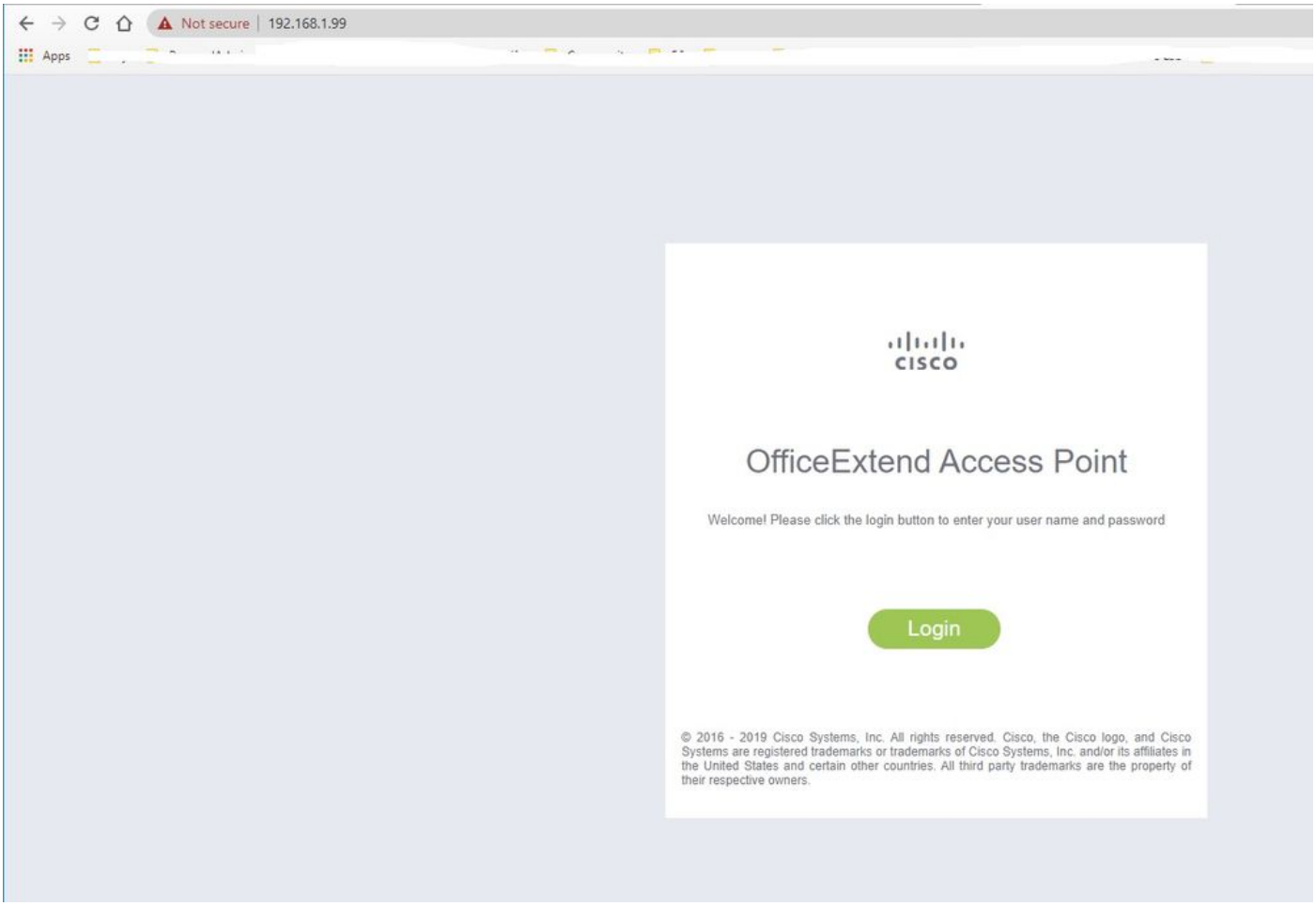
```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name :
ssh status : Enabled
ApMode : FlexConnect
ApSubMode : Not Configured
Link-Encryption : Enabled
OfficeExtend AP : Enabled
Discovery Timer : 10
Heartbeat Timer : 30
...
```

ローカルでスイッチングされるトラフィックを示すパケットキャプチャの例を次に示します。ここで行われたテストは、IP 192.168.1.98のクライアントからGoogle DNSサーバへ、次に192.168.1.254へ「ping」でした。AP NATがローカルでトラフィックを送信するため、AP IPアドレス192.168.1.99のIPを送信元とするICMPを確認できます。トラフィックがDTLSトンネルで暗号化され、アプリケーションデータフレームのみが表示されるため、192.168.1.254へのicmpはありません。

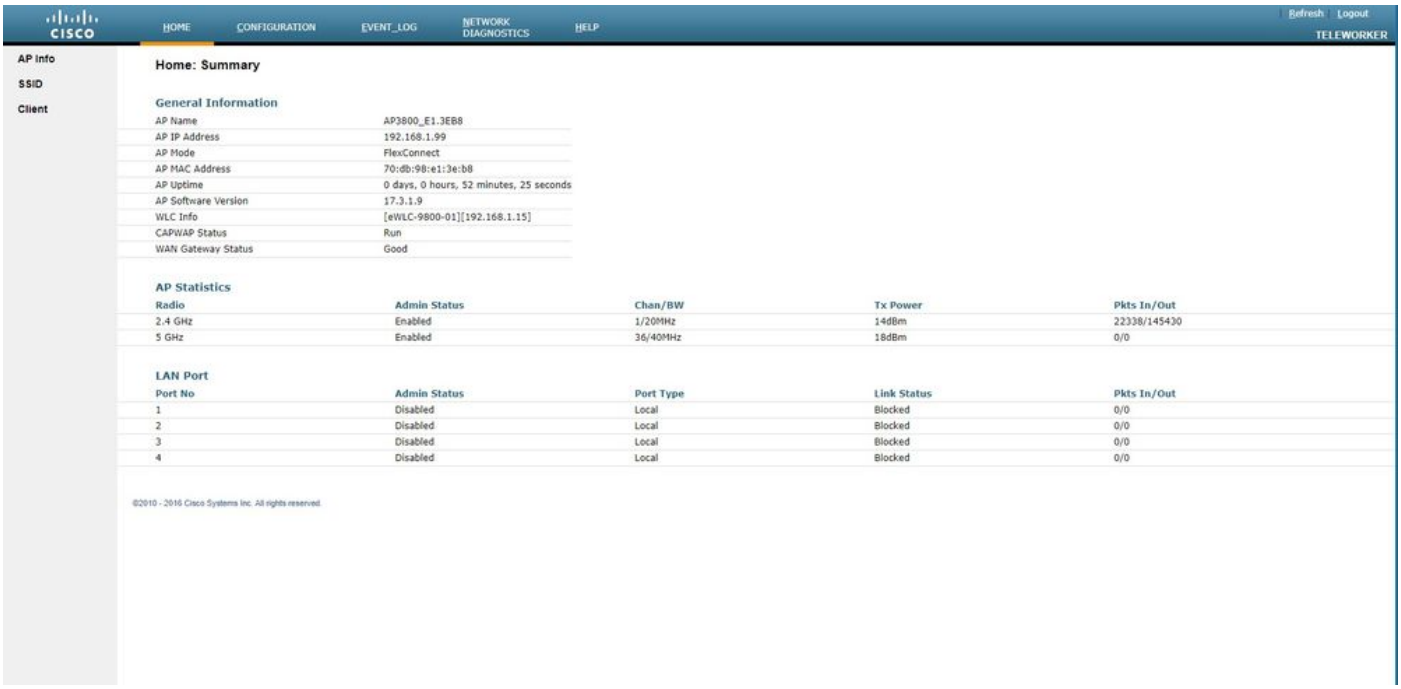


> **注**：ローカルにスイッチングされるトラフィックはAPによってNAT処理されます。これは、通常のシナリオでは、クライアントサブネットがOfficeネットワークに属し、ホームオフィスのローカルデバイスがクライアントサブネットへの到達方法を認識しないためです。APは、ローカルホームオフィスのサブネットにあるAP IPアドレスを使用してクライアントトラフィックを変換します。

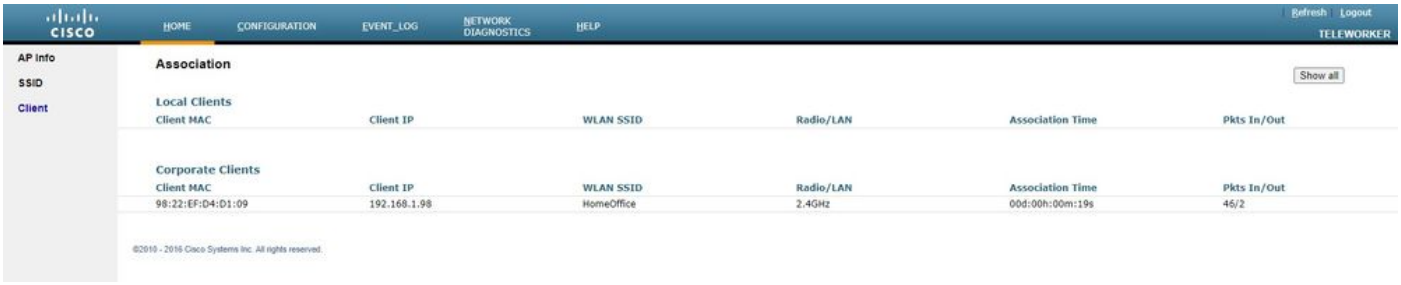
OEAP GUIにアクセスしてブラウザを開き、URLにAPのIPアドレスを入力できます。デフォルトのクレデンシャルはadmin/adminで、初期ログイン時に変更する必要があります。



ログインすると、GUIにアクセスできます。



OEAPの一般的な情報（AP情報、SSID、接続クライアントなど）にアクセスできます。



関連資料

Catalyst 9800ワイヤレスコントローラでのFlexConnectについて

FlexConnectのスプリットトンネリング

Catalyst 9800 WLCでのOEAPおよびRLANの設定