Catalyst 9800でのアンカーを使用した中央Web認証の設定

内容

概要

このドキュメントでは、別のワイヤレスLANコントローラ(WLC)をモビリティアンカーとしてポイントするCatalyst 9800上で、AireOSまたは別の9800 WLCを使用した中央Web認証(CWA)を設定およびトラブルシューティングする方法方法について説明します。

前提条件

要件

9800 WLC、AireOS WLC、およびCisco ISEの基本的な知識があることが推奨されます。CWAアンカー設定を開始する前に、2台のWLC間のモビリティトンネルをすでに確立していることを前提としています。これは、この設定例の範囲外です。この問題に関するヘルプが必要な場合は、ドキュメント「Catalyst 9800コントローラでのモビリティトンネルの構築」を参照してください

使用するコンポーネント

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。

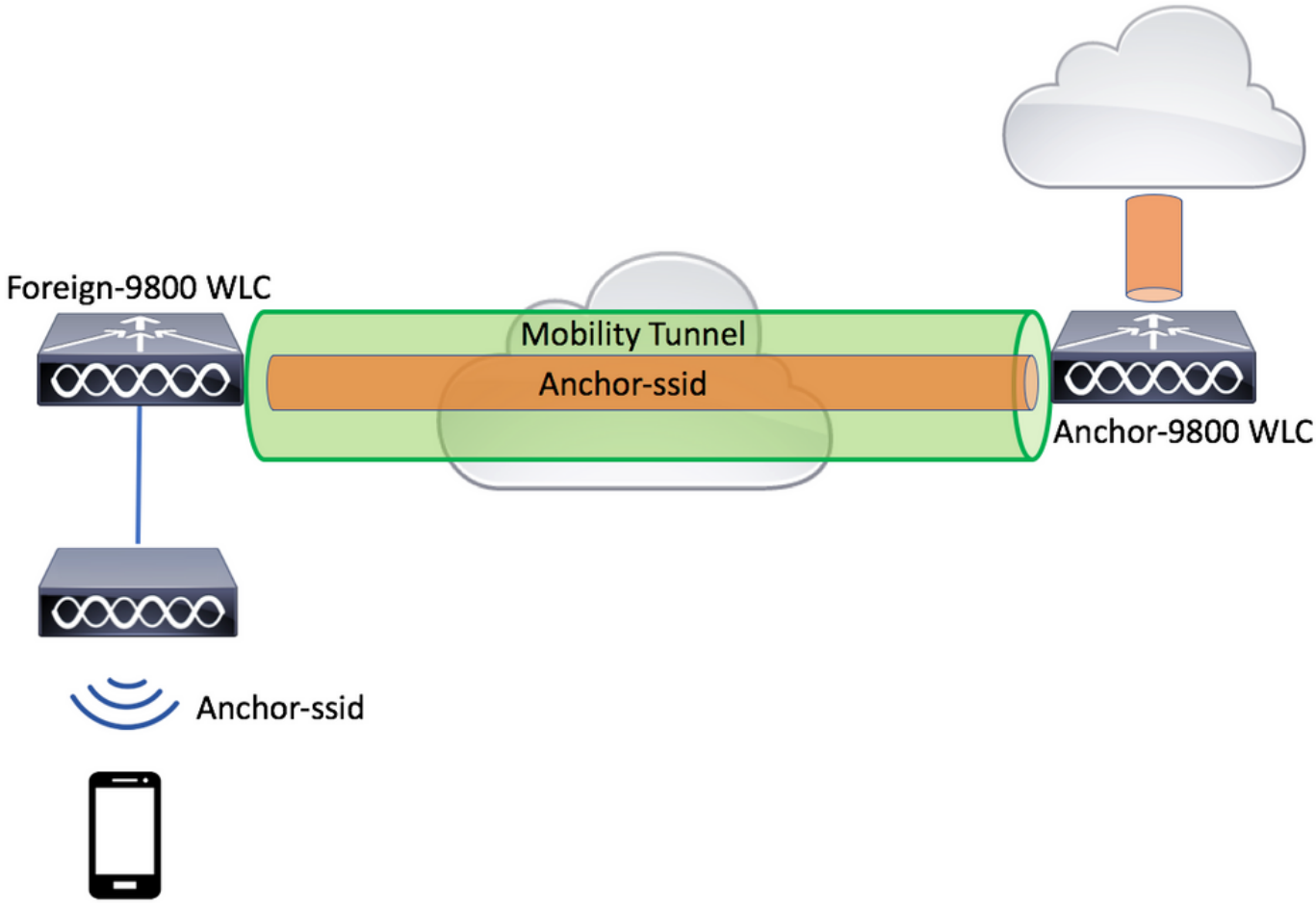
9800 17.2.1

5520 8.5.164 IRCMイメージ

ISE 2.4

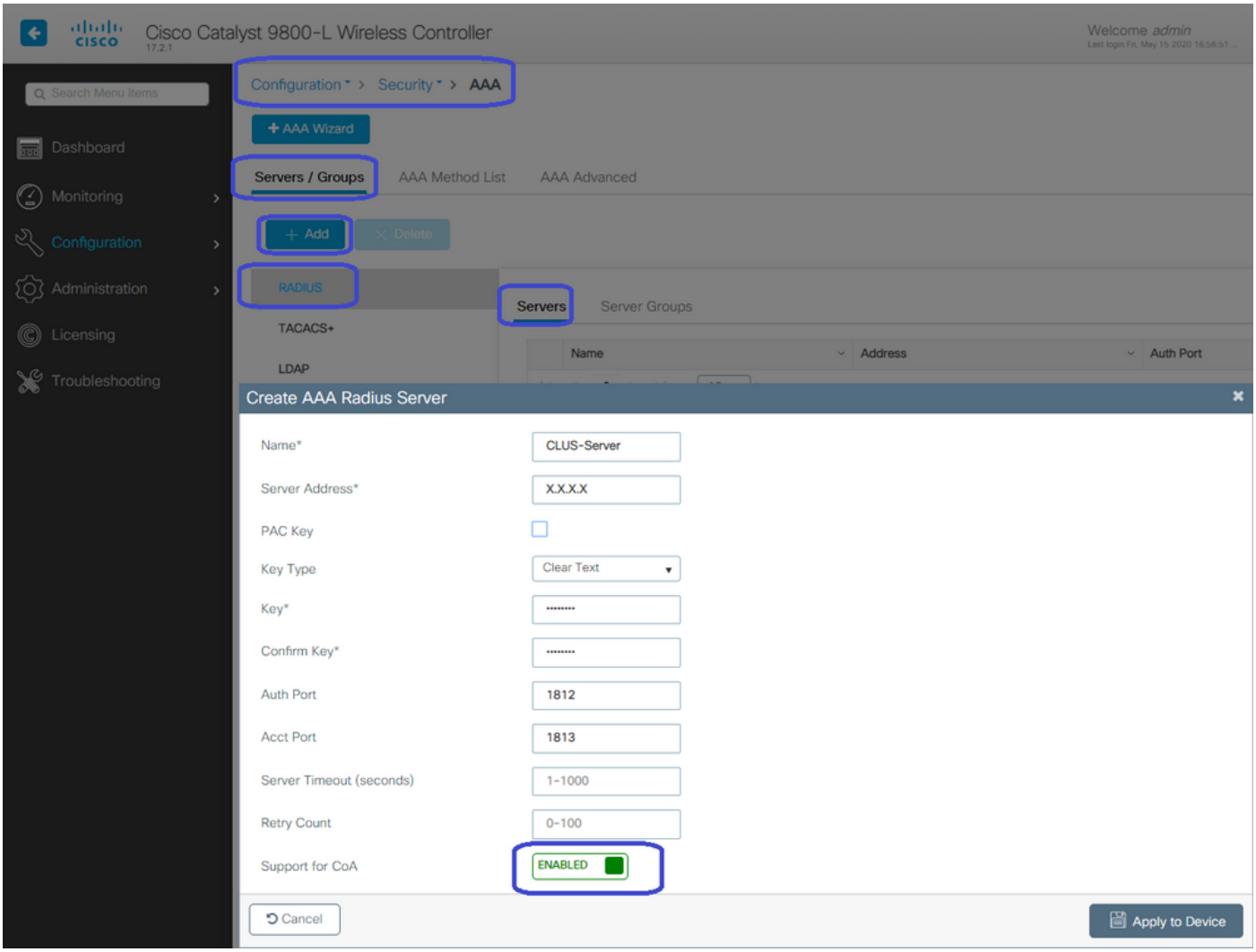
別のCatalyst 9800にアンカーされたCatalyst 9800の設定

ネットワーク図

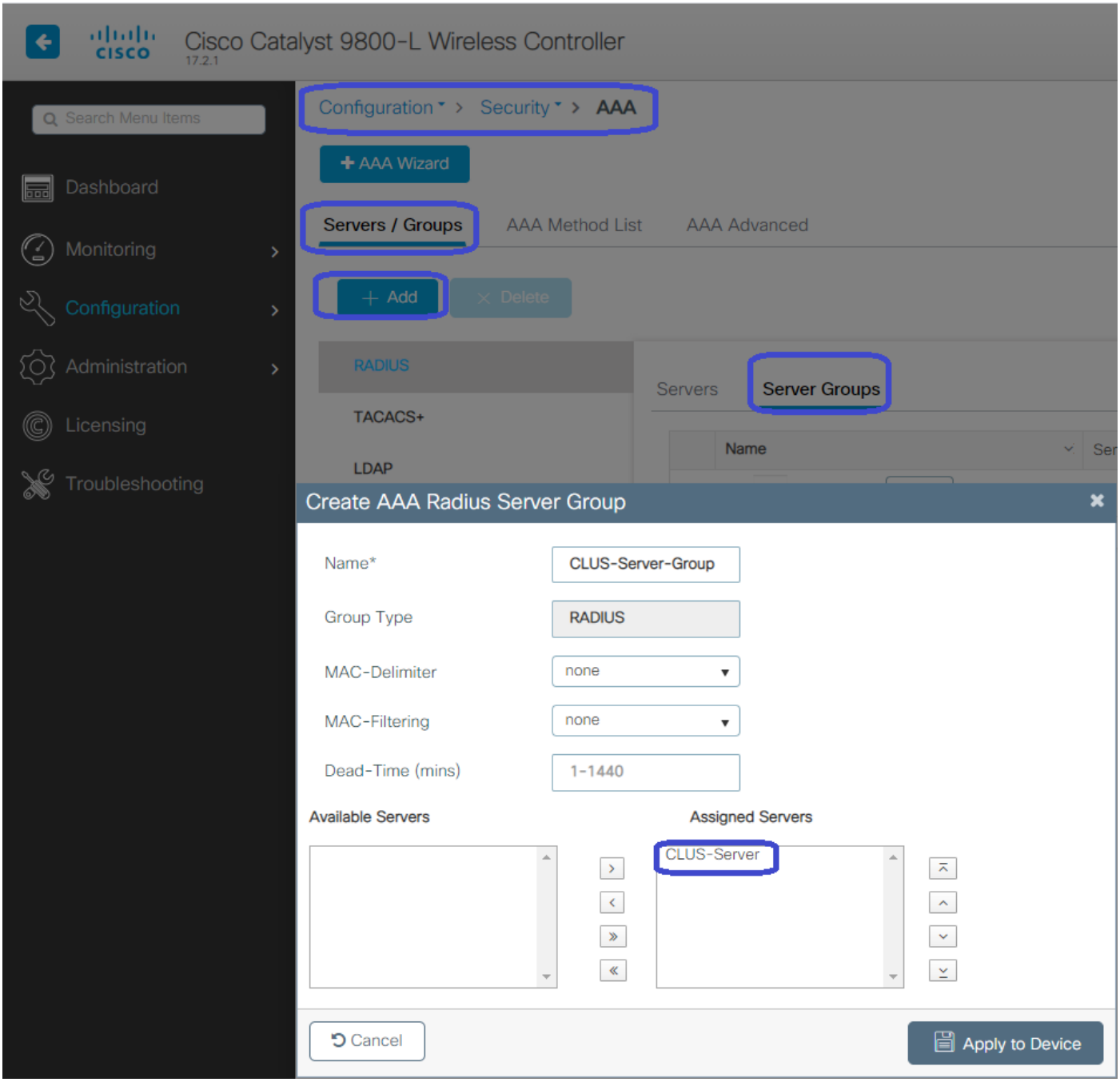


両方の9800でのAAAの設定

アンカーと外部の両方で、まずRADIUSサーバを追加し、CoAが有効になっていることを確認する必要があります。これはメニューで実行できます**[Configuration] > [Security] > [AAA] > [Servers/Groups] > [Servers]> [Add]ボタンをクリックします**

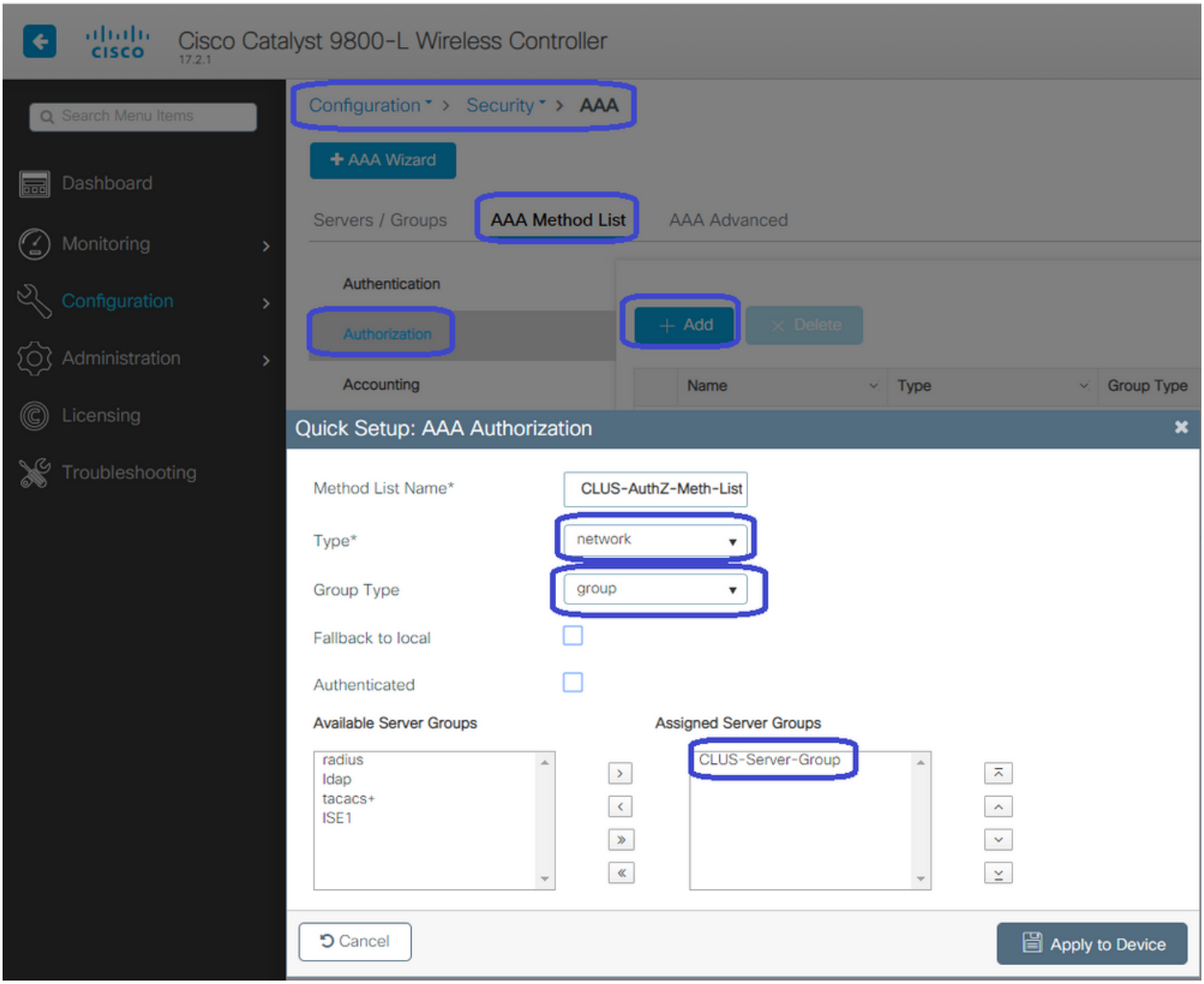


ここで、サーバグループを作成し、設定したサーバをそのグループに配置する必要があります。これは、**[Configuration] > [Security] > [AAA] > [Servers/Groups] > [Server Groups] > [Add]**で行います。

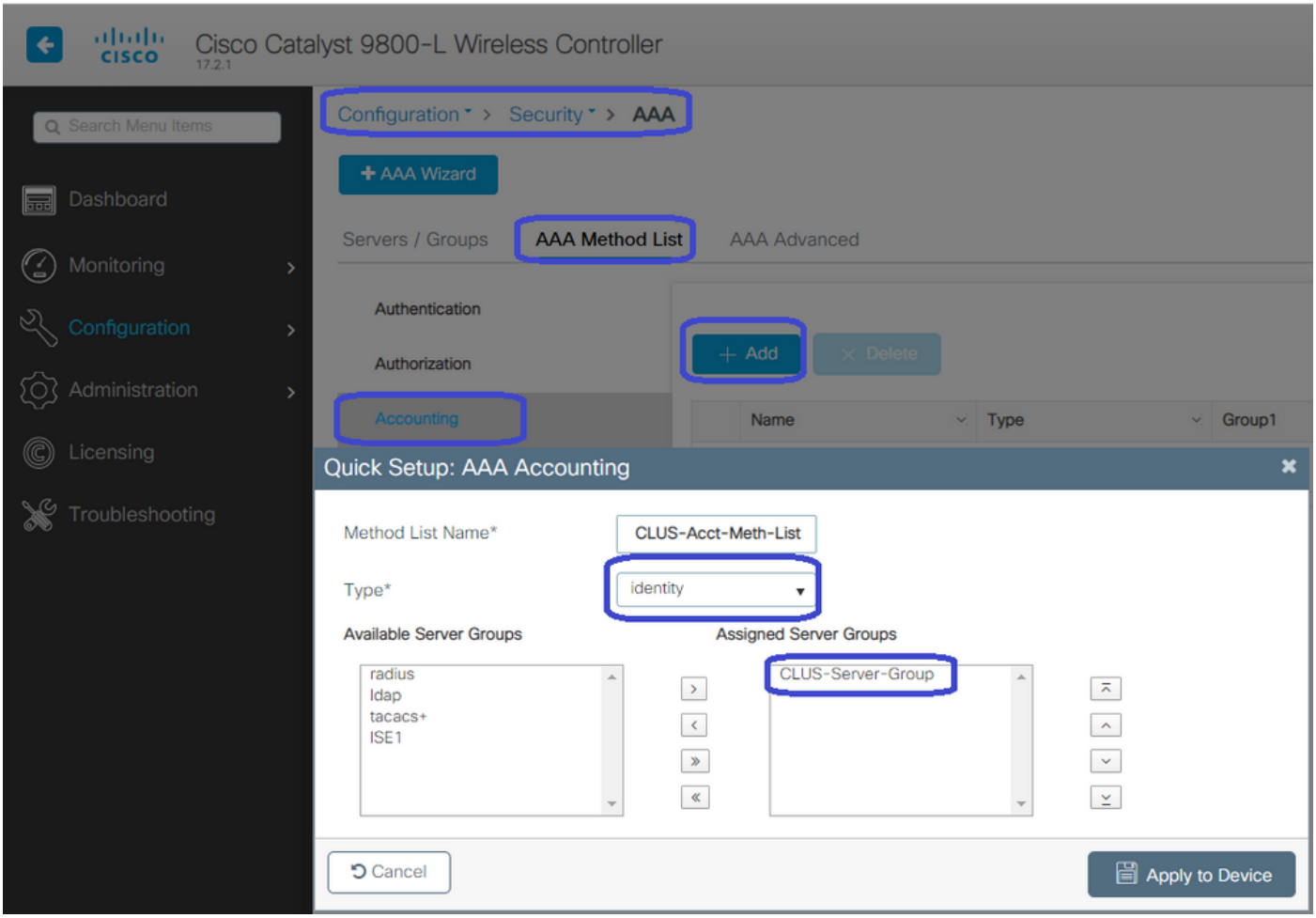


ここで、認証方式リスト**を作成**します（CWAでは認証方式リストは不要です）。タイプがnetwork、グループタイプがgroupです。前のアクションのサーバグループをこのメソッドリストに追加します。

この設定は、**[Configuration] > [Security] > [AAA] > [Servers/AAA Method List] > [Authorization] > [Add]で行います**

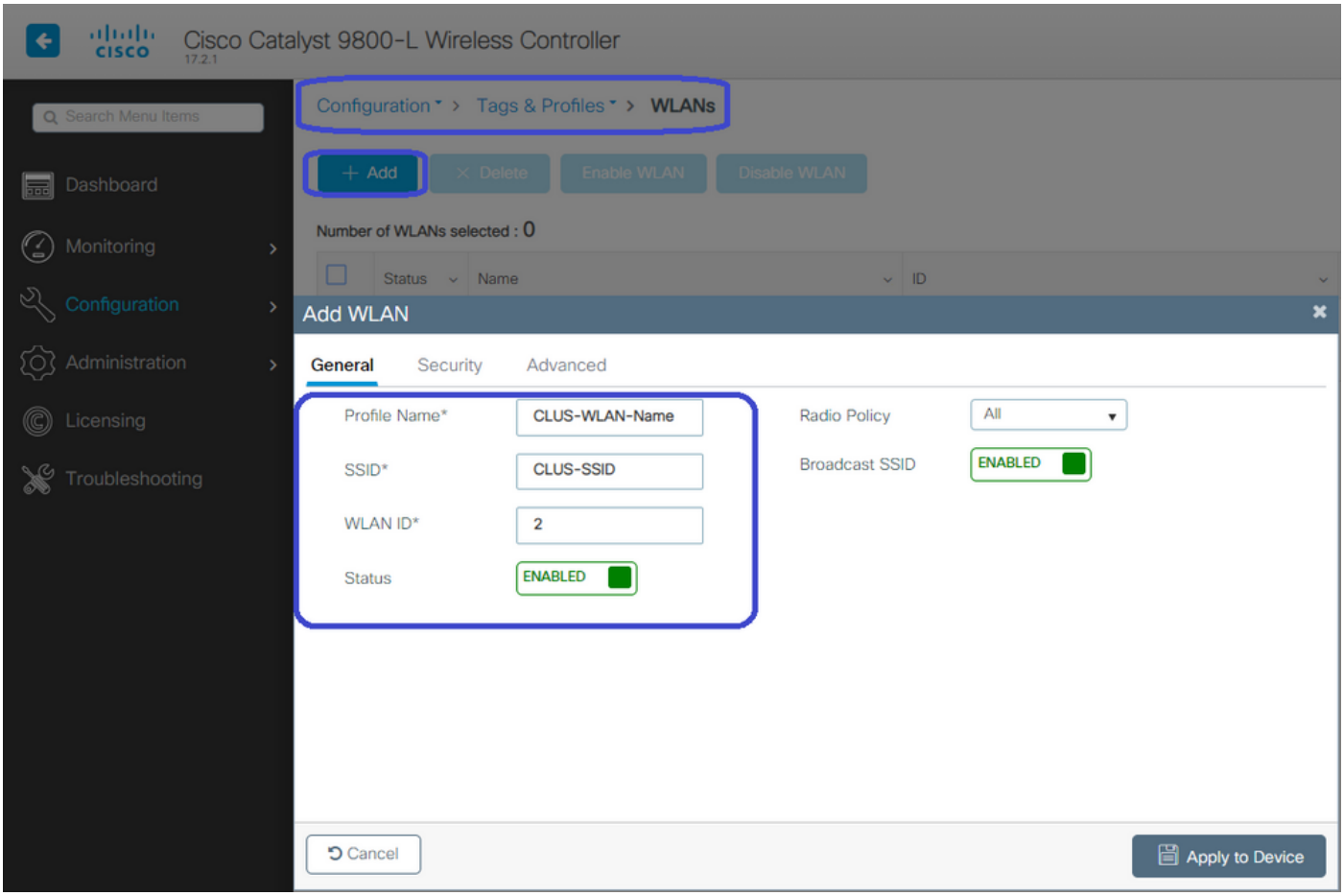


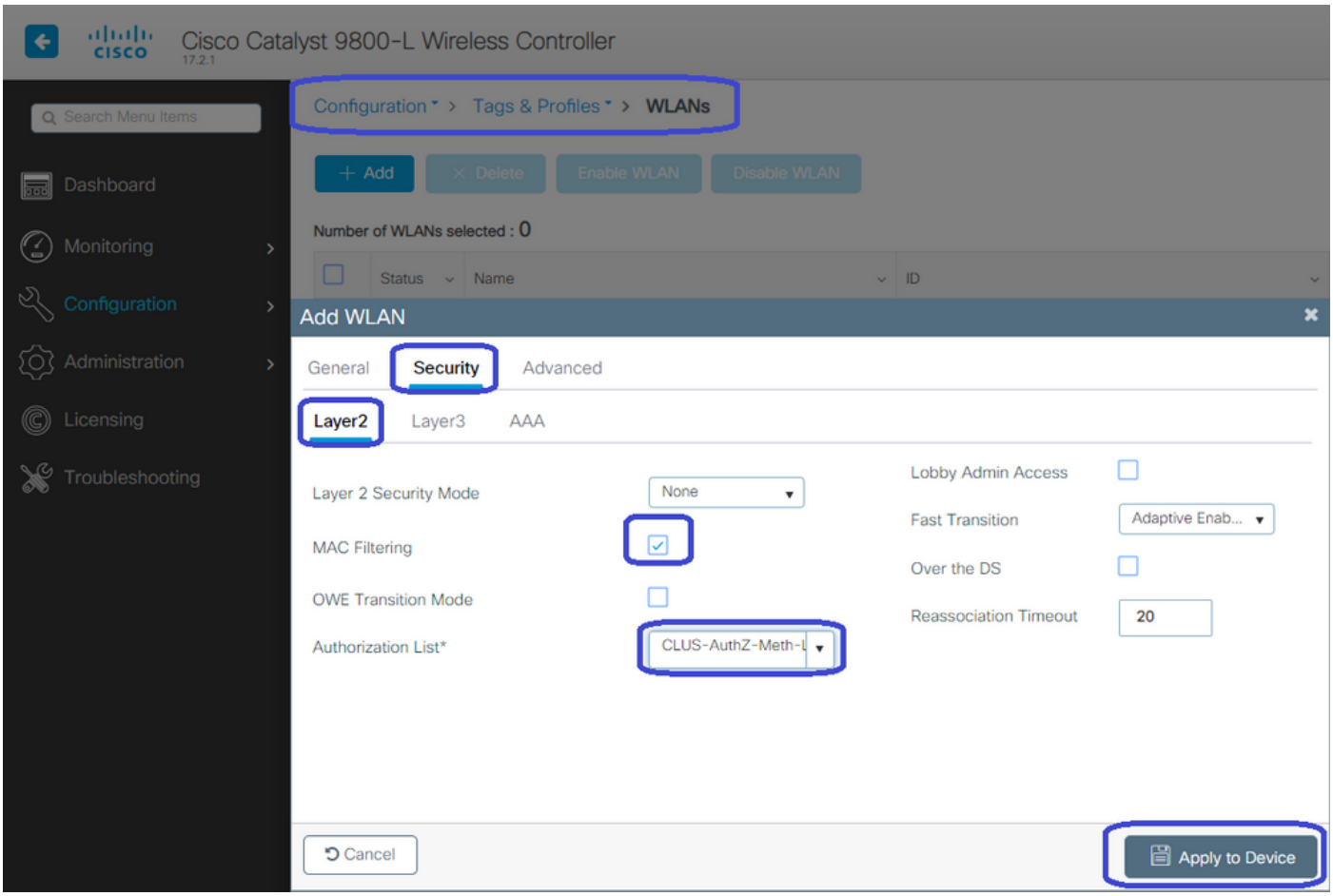
（オプション）認可方式リストと同じサーバグループを使用して、アカウンティング方式リストを作成します。アカウンティングリストは、**[Configuration] > [Security] > [AAA] > [Servers/AAA Method List] > [Accounting] > [Add]で作成できます**



WLCでのWLANの設定

両方のWLCでWLANを作成し、設定します。WLANは両方で一致する必要があります。セキュリティタイプはMACフィルタリングで、前の手順の認可方式リストを適用する必要があります。この設定は、**[Configuration] > [Tags & Profiles] > [WLANs>+Add]で行います**



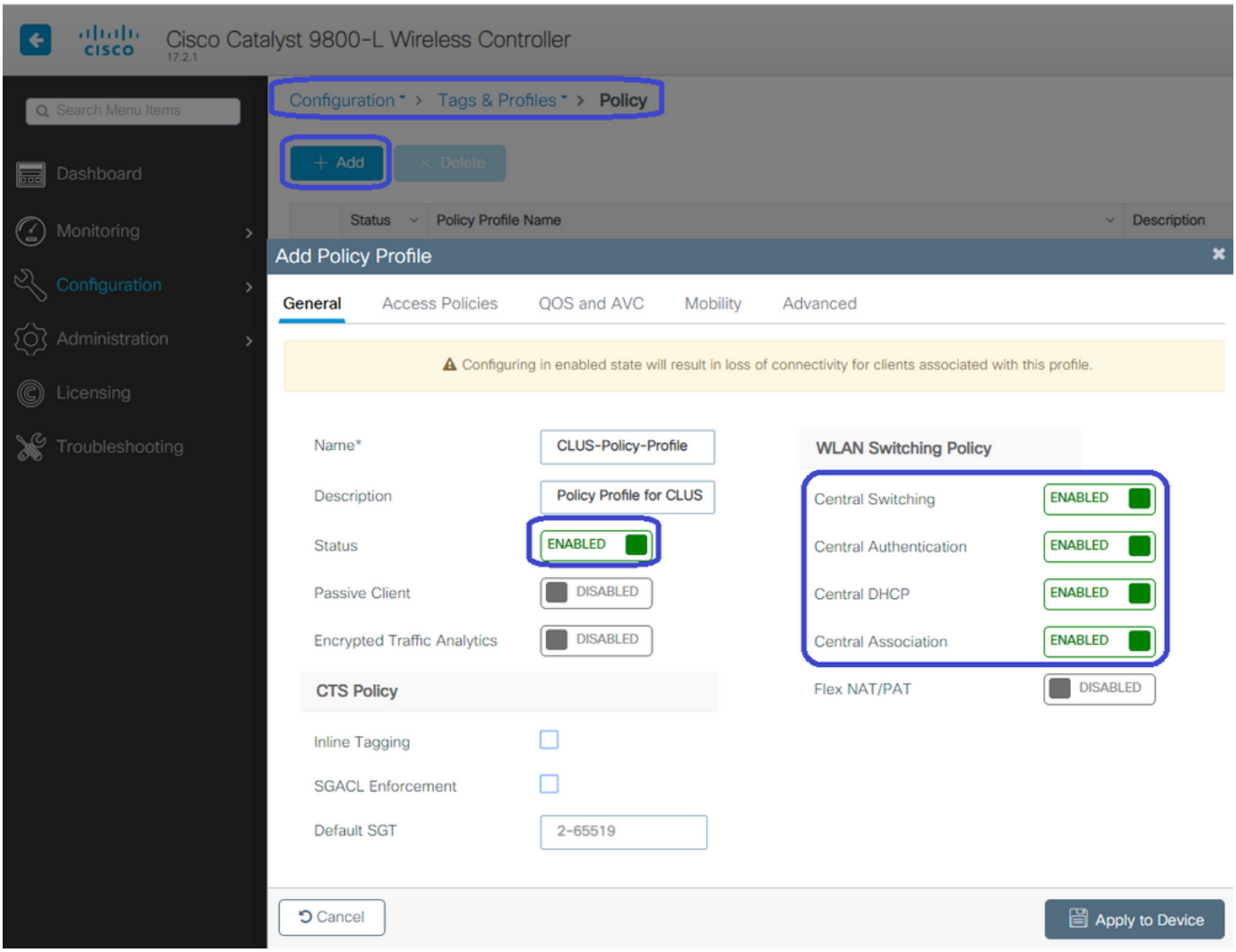


外部WLCでポリシープロファイルとポリシータグを作成します

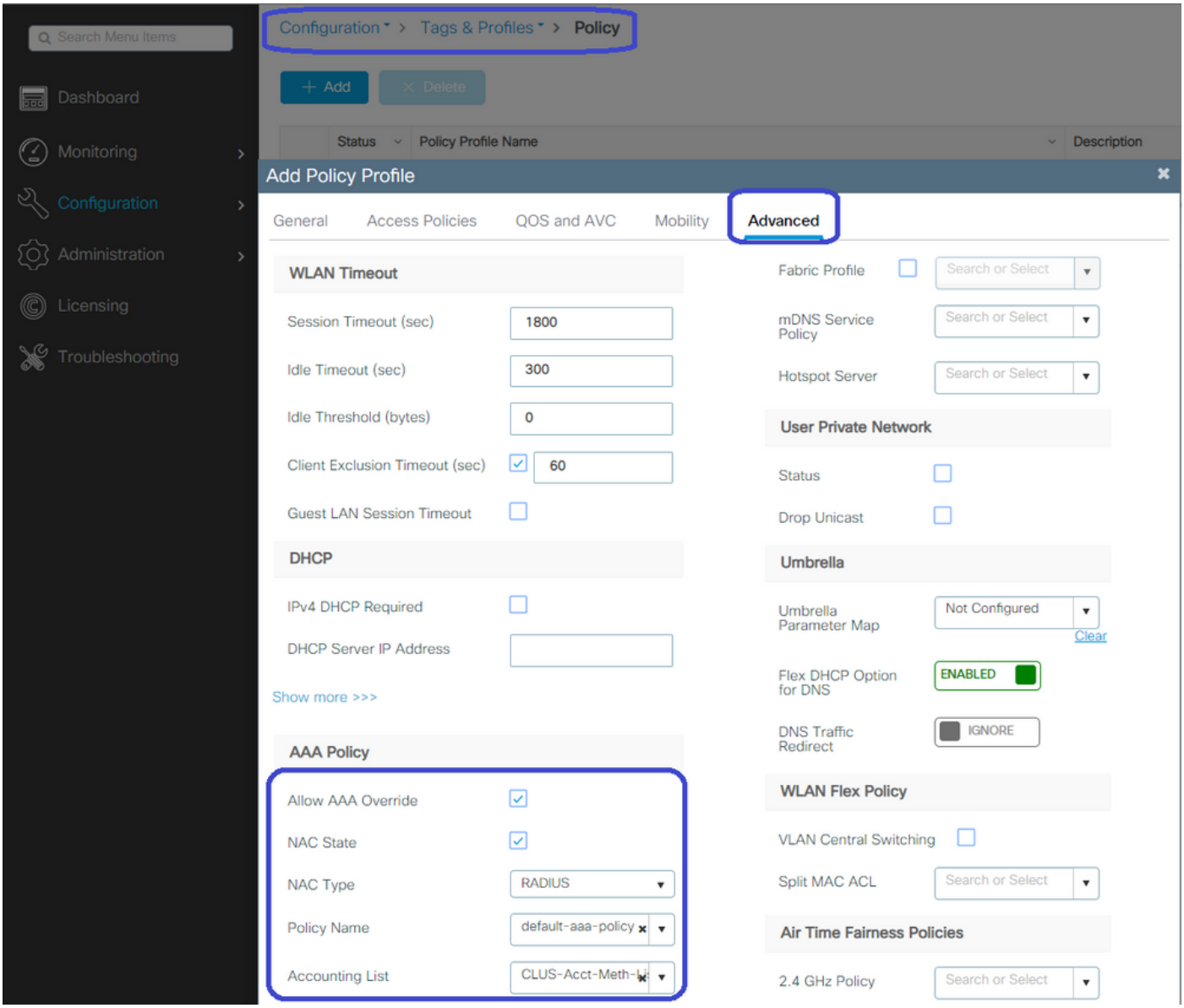
外部WLC Web UIに移動します。

ポリシープロファイルを作成するには、**[Configuration] > [Tags & Profiles] > [Policy] > [Add]に移動します**

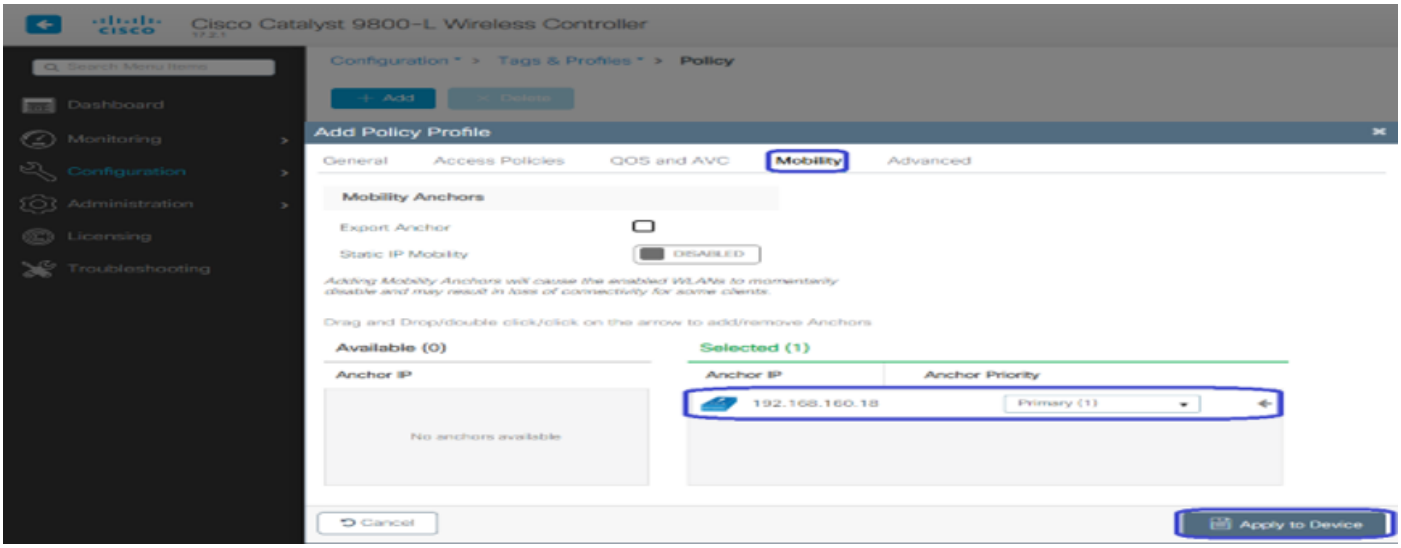
アンカーするときは、中央スイッチングを使用する必要があります。



[Advanced]タブでは、CWAにはAAAオーバーライドとRADIUS NACが必須です。ここでは、アカウンティング方式リストを作成するように選択した場合に、そのリストを適用することもできます。

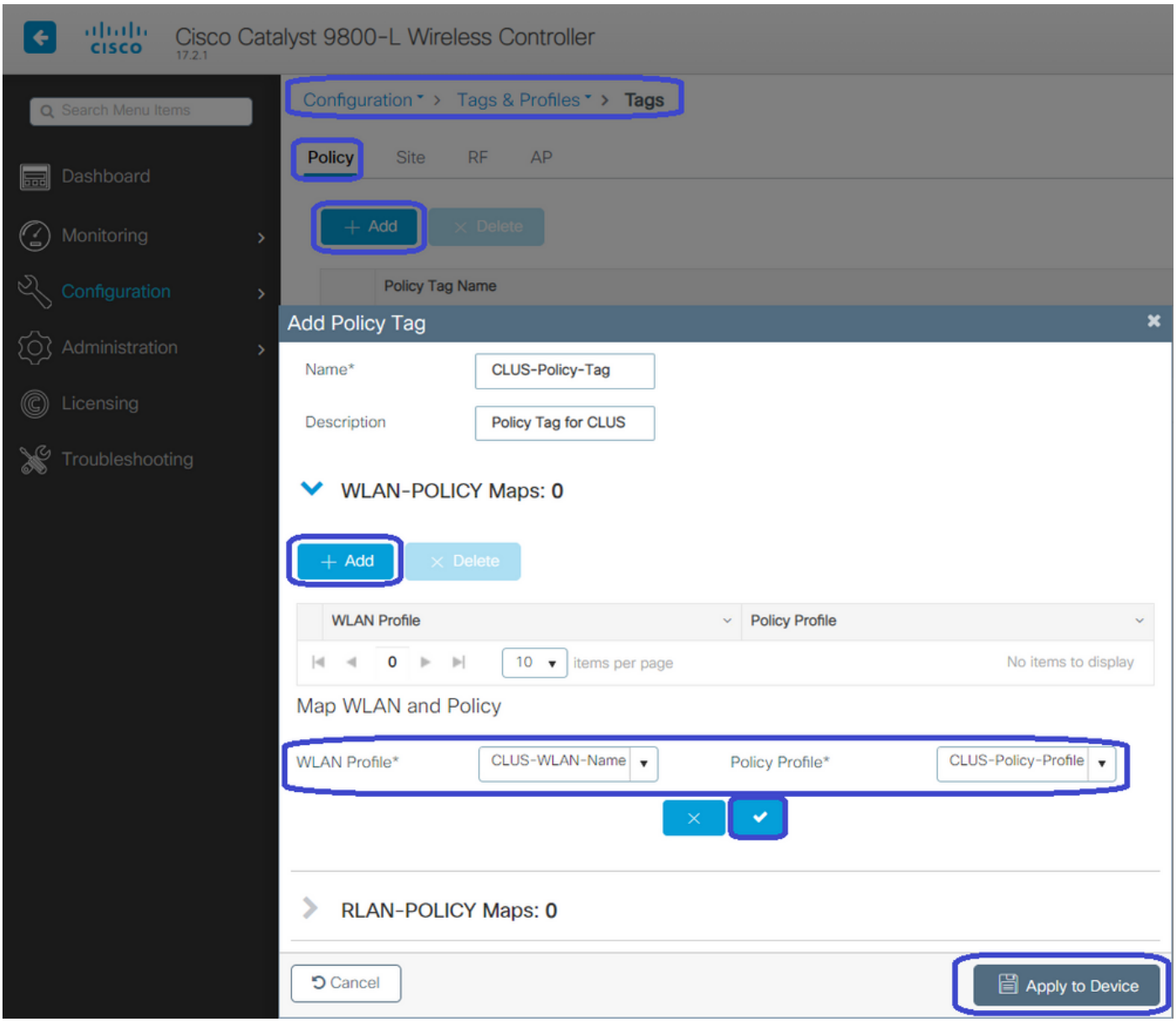


[Mobility]タブで、[**export anchor]チェックボックス**をオンにしないで、アンカーリストにアンカーWLCを追加します。[Apply to Device]を必ず押してください。 この場合、2つのコントローラ間にモビリティトンネルがすでに設定されていることを前提としています

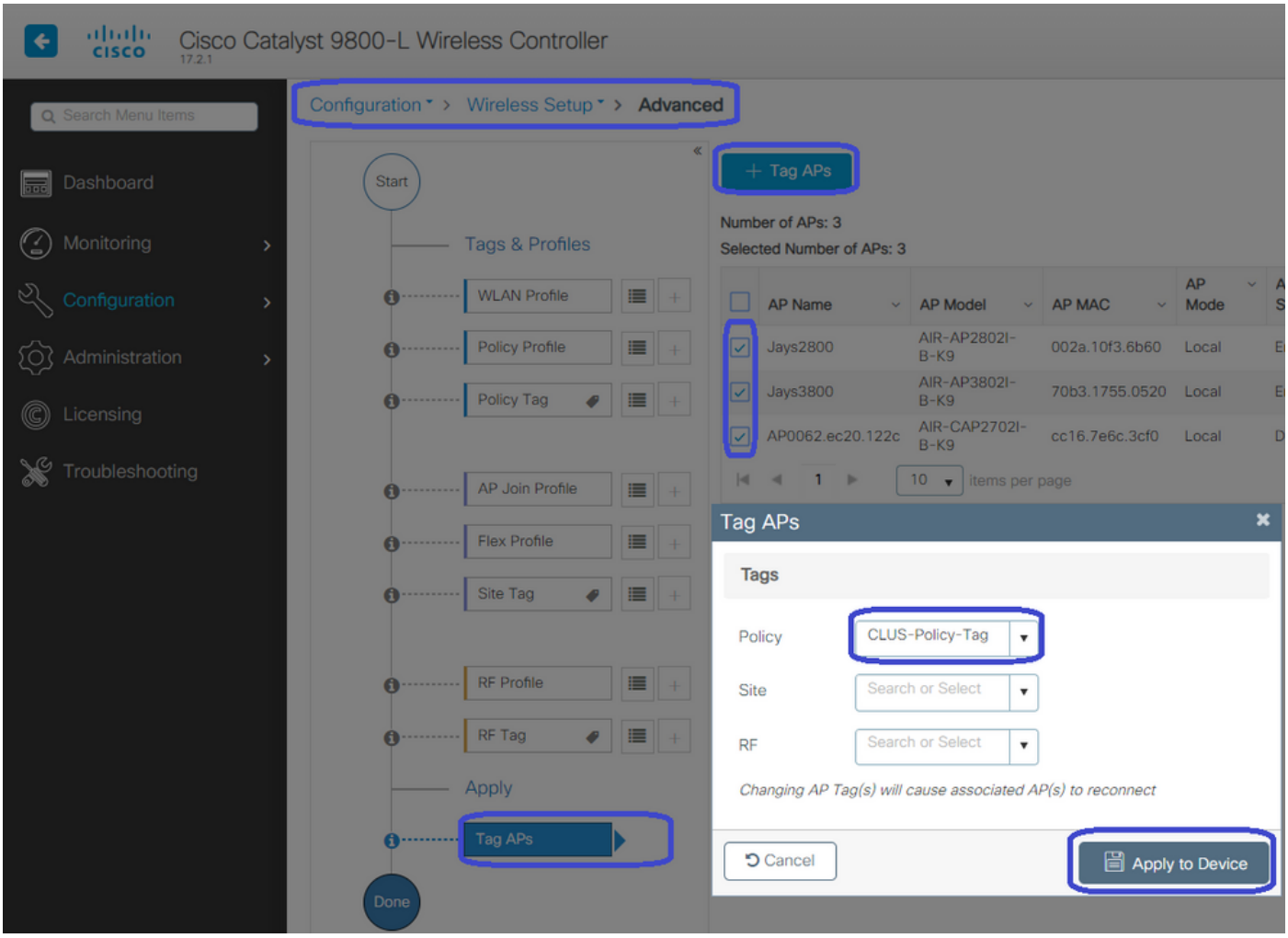


APがこのポリシープロファイルを使用するには、ポリスタグを作成し、使用するAPに適用する必要があります。

ポリシータグを作成するには、[Configuration] > [Tags & Profiles] > [Tags?Policy] > [Add]に移動します



これを複数のAPに同時に追加するには、[Configuration] > [Wireless Setup] > [Advanced] > [Start Now]に移動します。[Tag APs]の横にある箇条書きバーをクリックし、選択したAPにタグを追加します。

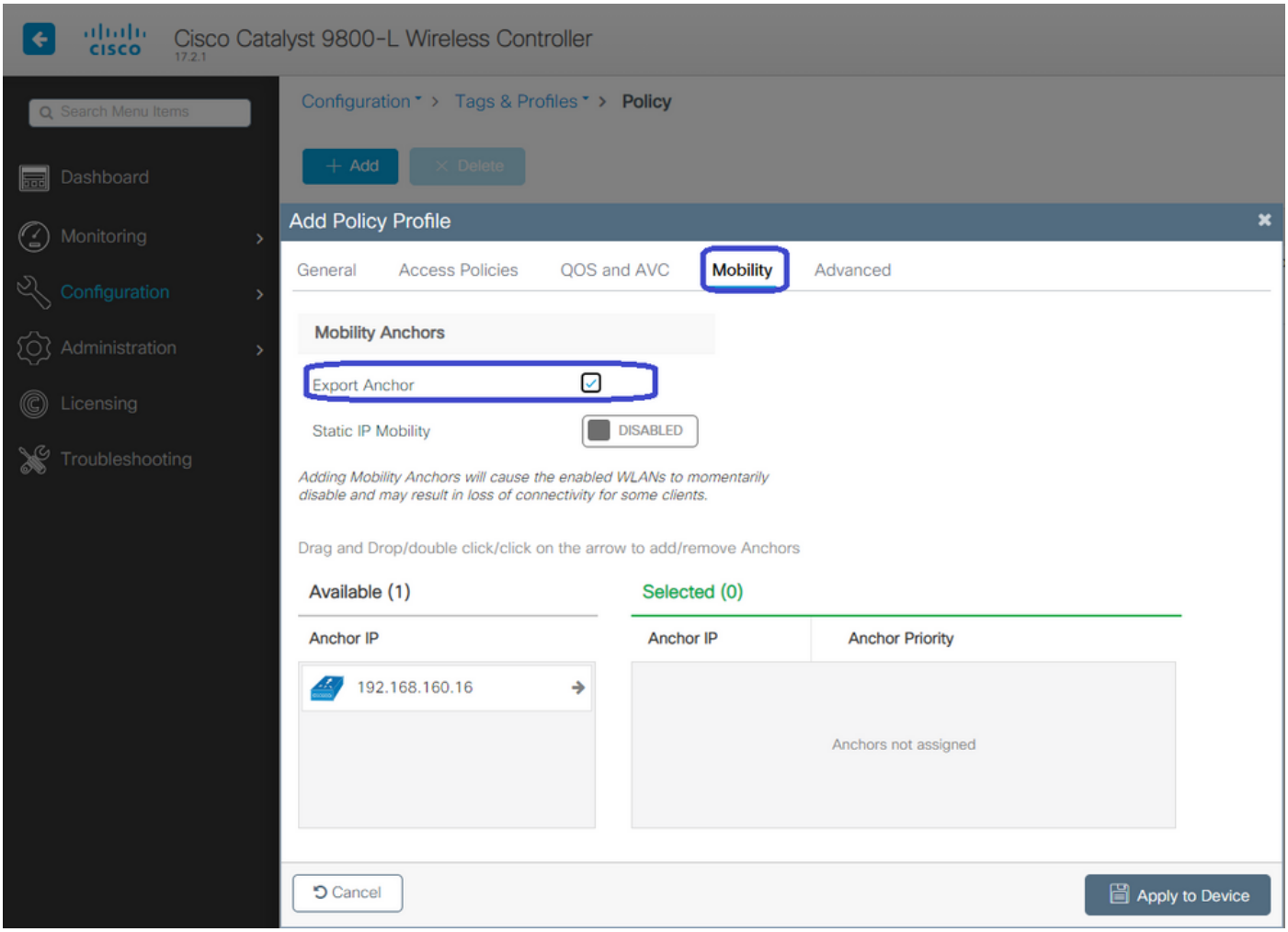


アンカーWLCでポリシープロファイルを作成します

アンカーWLC Web UIに移動します。アンカー9800の[**Configuration**] > [**Tags & Profiles**] > [**Tags**] > [**Policy**] > [**+Add**]**でポリシープロファイルを追加します**。これは、モビリティタブとアカウンティングリストを除き、外部で行われたポリシープロファイルと一致していることを確認します。

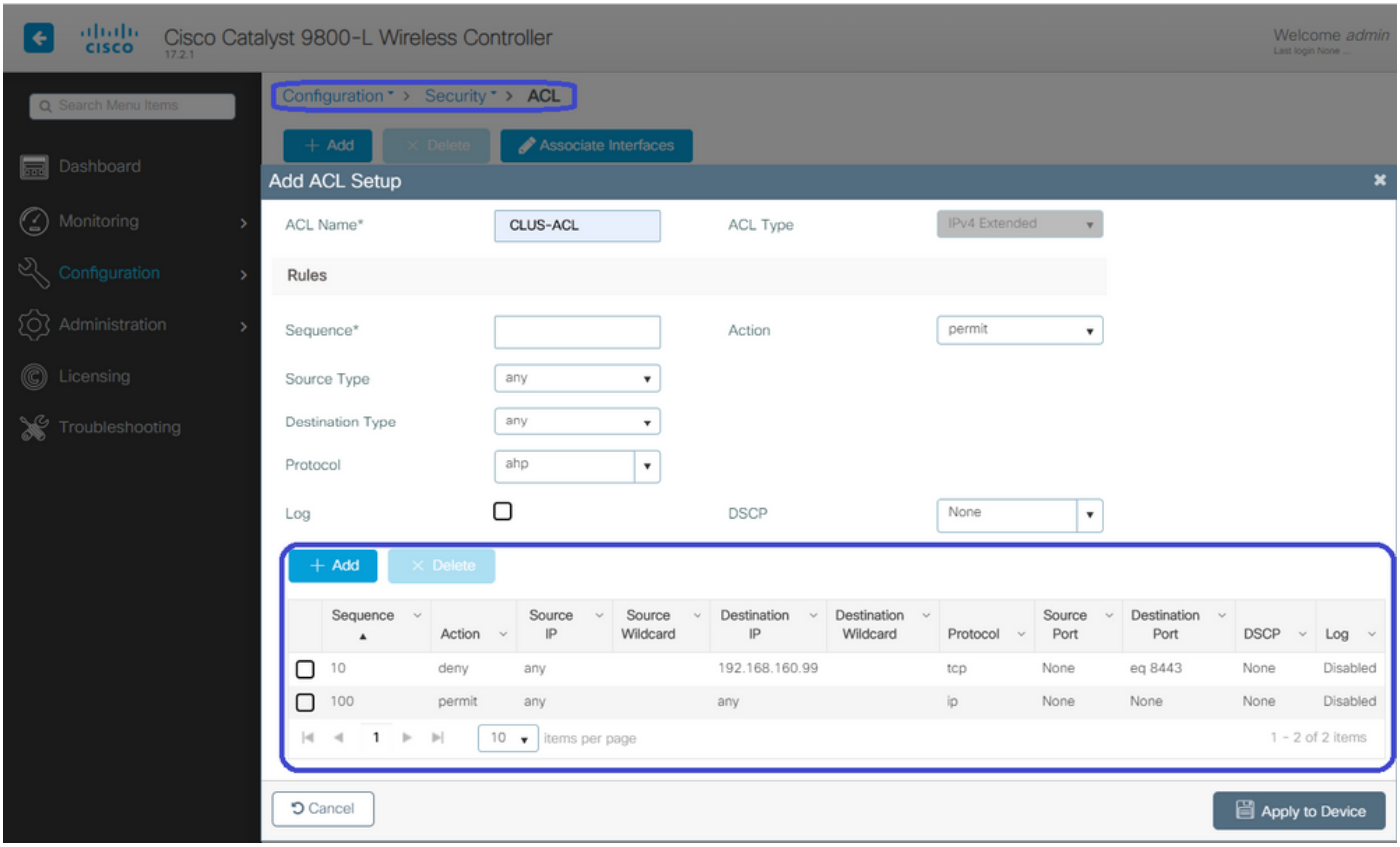
ここではアンカーを追加しませんが、[Export Anchor]チェックボックスはオンにします。ここでアカウンティングリストを追加しないでください。この場合、2つのコントローラ間にモビリティトンネルがすでに設定されていることを前提としています

注：このプロファイルをポリスタグ内のWLANに関連付ける理由はありません。これにより、問題が発生します。このWLC上のAPに同じWLANを使用する場合は、それに対して別のポリシープロファイルを作成します。



両方の9800のリダイレクトACL設定

次に、両方の9800でリダイレクトACL設定を作成する必要があります。ACLをトラフィックに適用するアンカーWLCであるため、外部のエントリは重要ではありません。唯一の要件は、そこにエントリがあるということです。アンカー上のエントリは、ポート8443でISEへのアクセスを「拒否」し、それ以外はすべて「許可」する必要があります。このACLは、クライアントから「着信」するトラフィックにのみ適用されるため、リターントラフィックのルールは必要ありません。DHCPとDNSは、ACLのエントリなしでパススルーします。

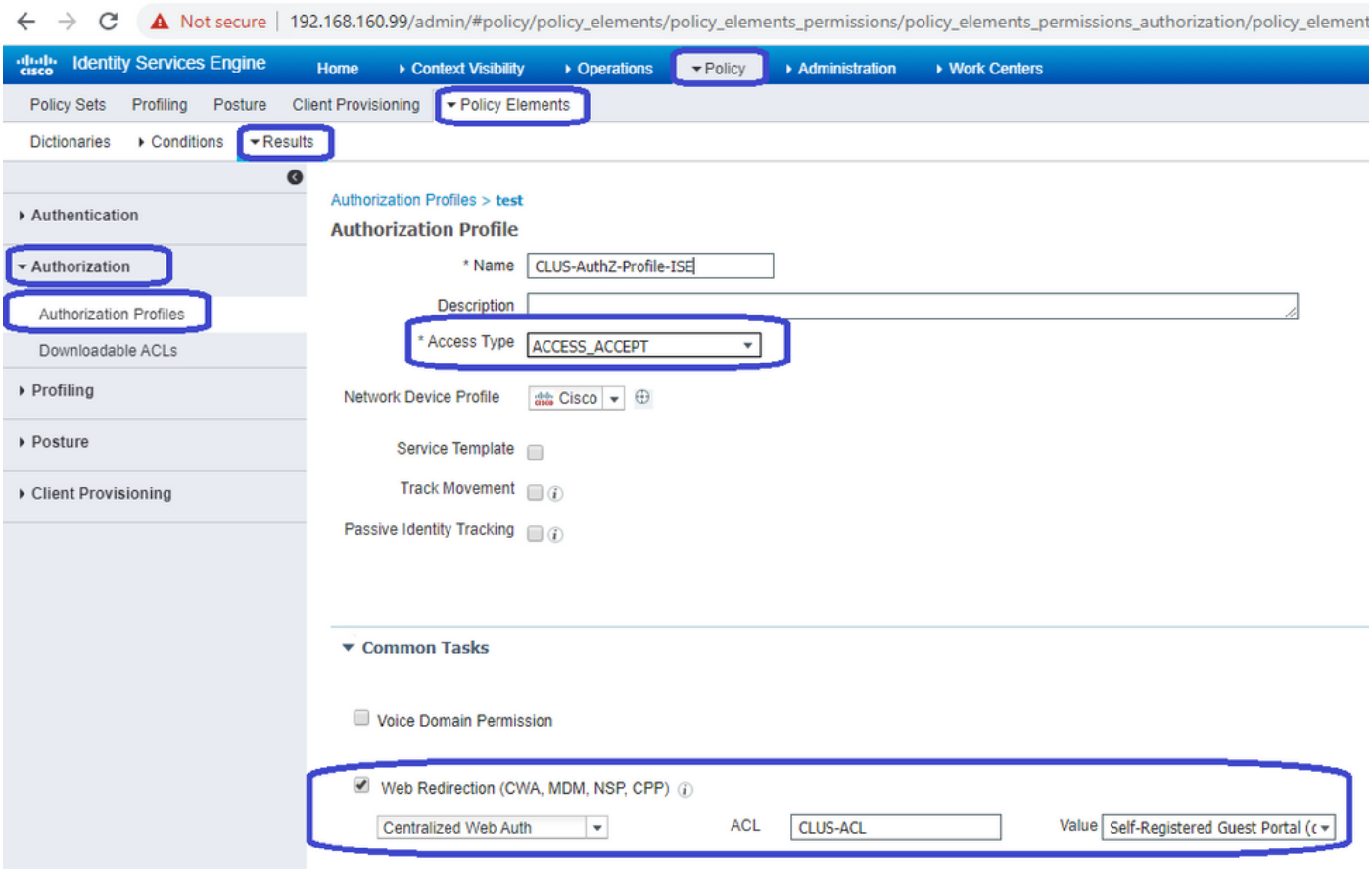


ISE の設定

最後の手順は、CWA用にISEを設定することです。これには多くのオプションがありますが、この例では基本に従い、デフォルトの自己登録ゲストポータルを使用します。

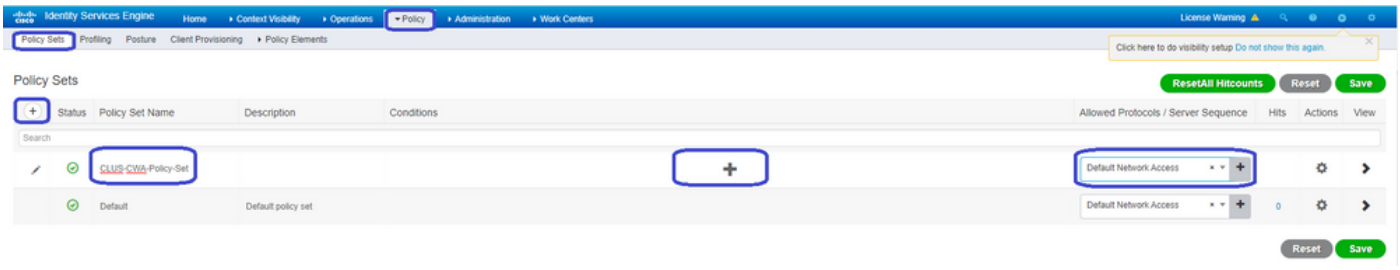
ISEでは、認可プロファイル、認証ポリシーと認可プロファイルを使用する認可ポリシーを含むポリシーセットを作成し、9800（外部）をネットワークデバイスとしてISEに追加し、ユーザ名とパスワードを作成してネットワークにログインする必要があります。

認可プロファイルを作成するには、[Policy] > [Policy Elements] > [Authorization] > [Results] > [Authorization Profiles] > [Add]をクリックします。返されるアクセスタイプが「access_accept」であることを確認し、返信するAVP（属性と値のペア）を設定します。CWAでは、リダイレクトACLとリダイレクトURLは必須ですが、VLAN IDやセッションタイムアウトなどの情報を返信することもできます。ACL名は、外部とアンカー9800の両方のリダイレクトACLの名前と一致することが重要です。

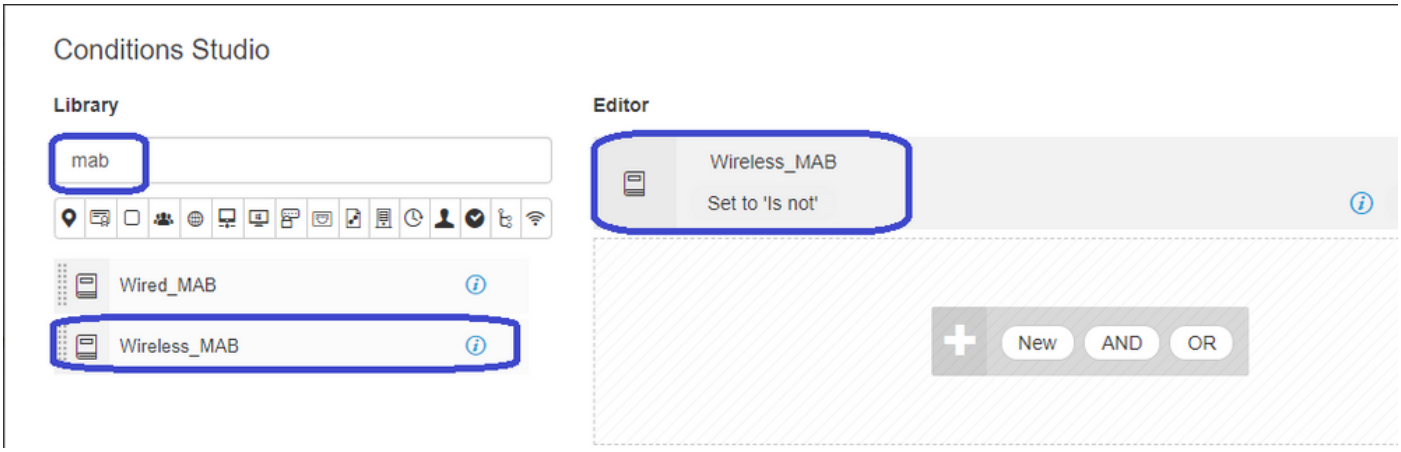


次に、作成した認可プロファイルをCWAを通過するクライアントに適用する方法を設定する必要があります。これを実現するには、MAB使用時に認証をバイパスするポリシーセットを作成し、着信側ステーションIDで送信されるSSID使用時に認証プロファイルを適用する方法があります。繰り返しになりますが、これを実現する方法は数多くありますので、より具体的な方法や、より安全な方法が必要な場合は、これが最も簡単な方法です。

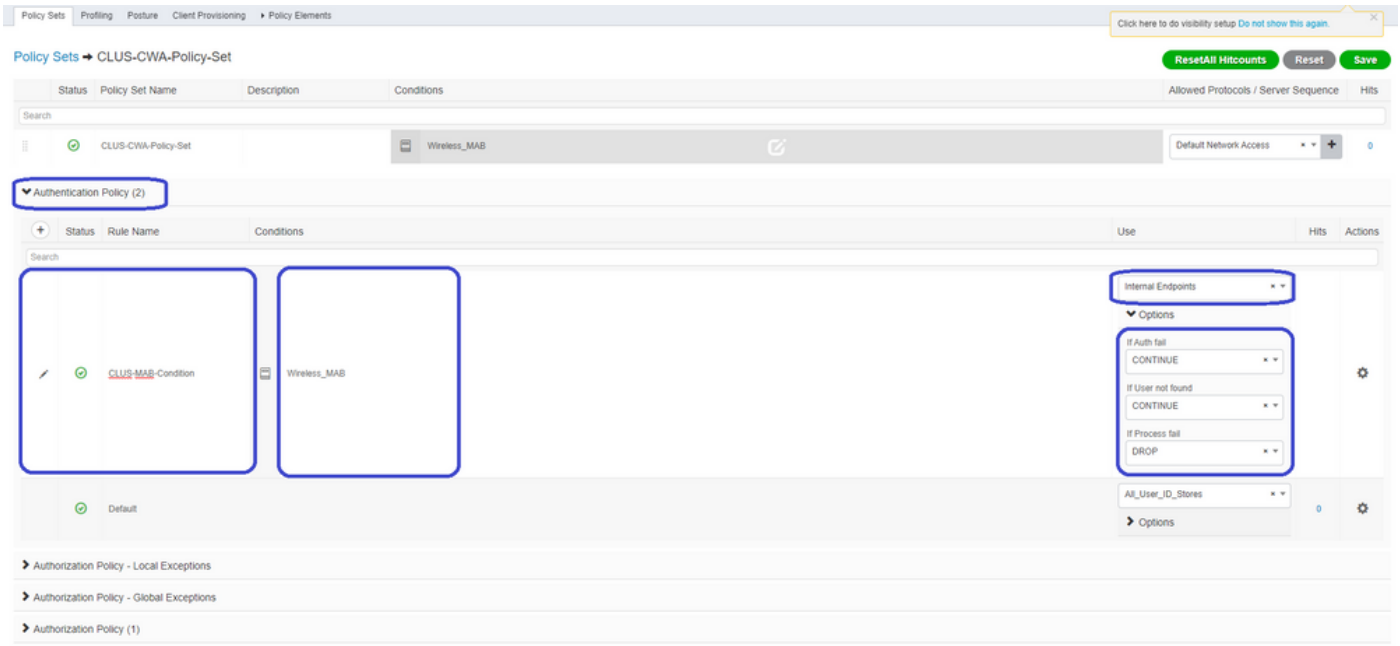
ポリシーセットを作成するには、[Policy] > [Policy Sets]に移動し、画面の左側にある[+]ボタンをクリックします。新しいポリシーセットに名前を付け、「default network access」またはMABの「Process Host Lookup」を許可する許可されたプロトコルリスト（許可されたプロトコルリストを確認するには、[Policy] > [Policy Elements] > [Results] > [Authentication] > [Allowed Protocols]に移動）にします。 作成した新しいポリシーセットの中央にある+記号をクリックします。



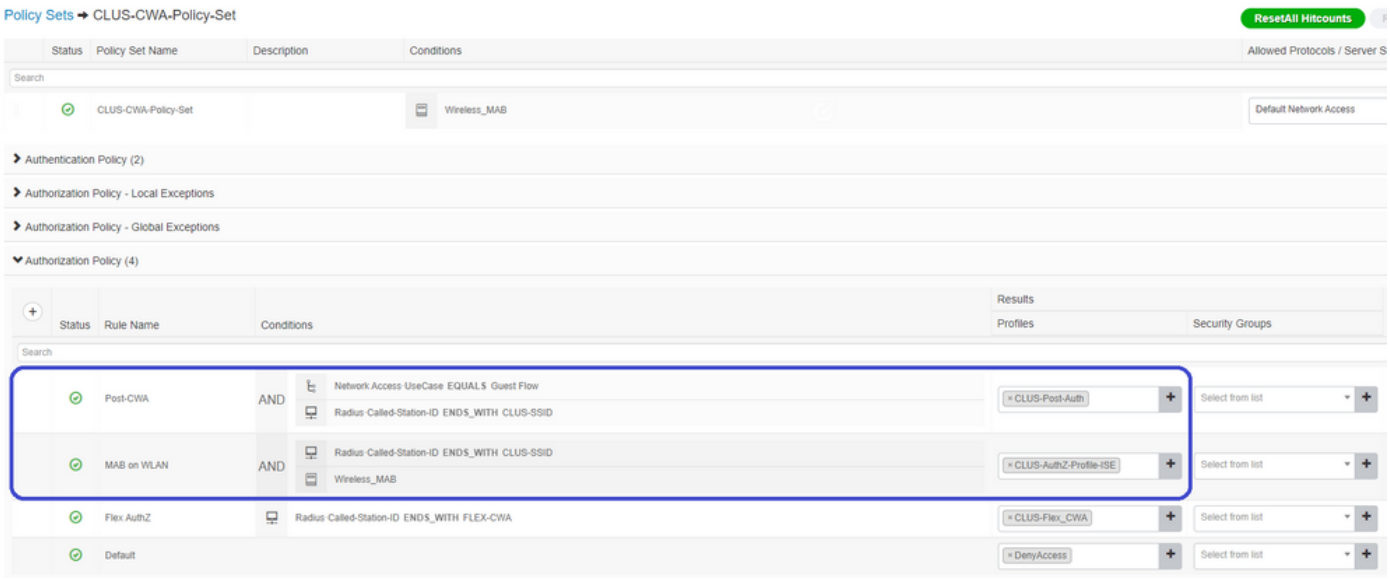
ISEでMABが使用されるたびに、このポリシーセットが通過します。後で、着信側ステーションIDに一致する認可ポリシーを作成して、使用されているWLANに応じて異なる結果を適用できます。このプロセスはカスタマイズ可能で、多くのものをマッチさせることができます。



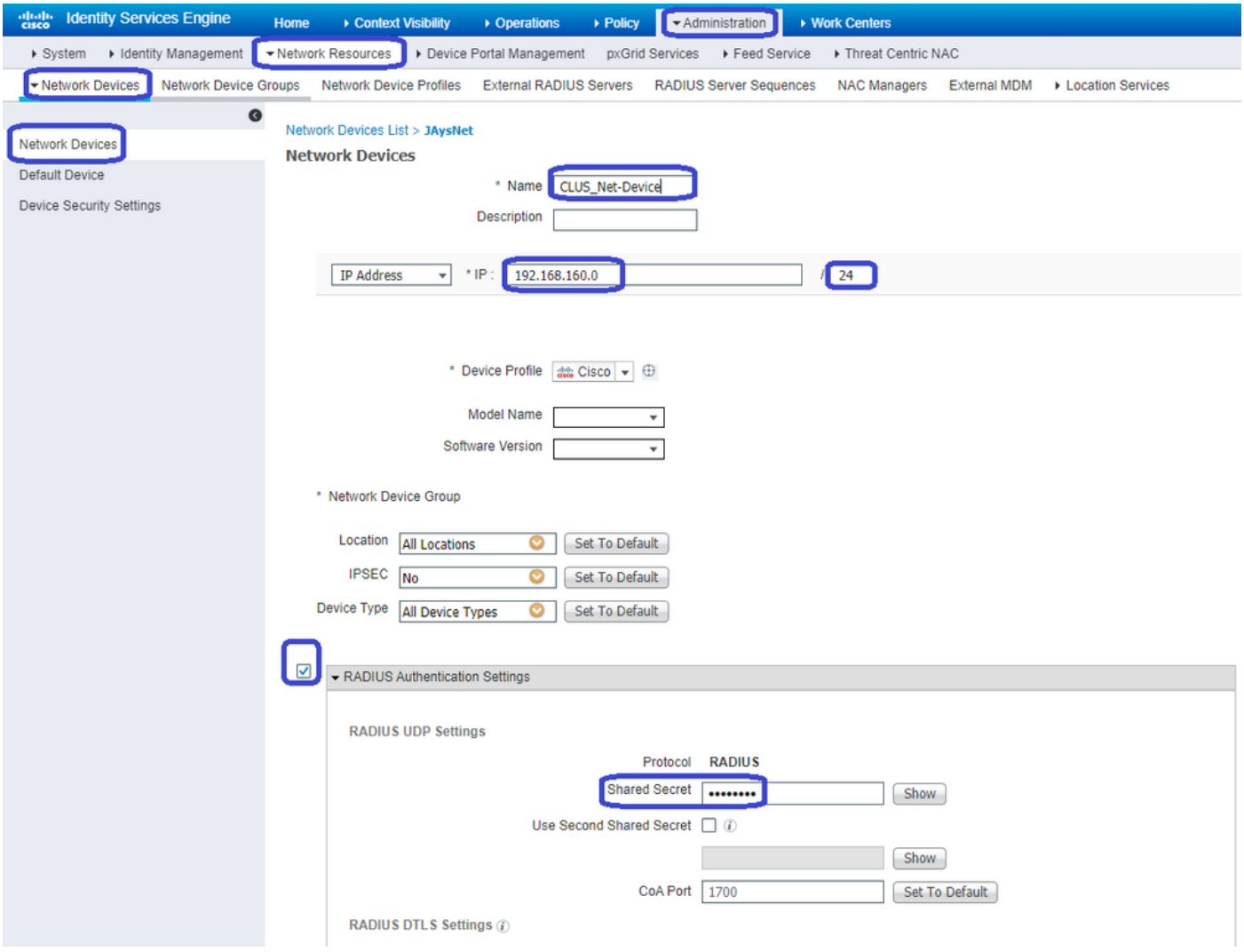
ポリシーセット内で、ポリシーを作成します。認証ポリシーはMABで再度一致しますが、「内部エンドポイント」を使用するようにIDストアを変更し、認証が失敗してユーザが見つからない場合は、オプションを変更する必要があります。



認証ポリシーを設定したら、認可ポリシーに2つのルールを作成する必要があります。このポリシーはACLのように読み取られるので、順序の先頭にポスト認証ルール、末尾にプレ認証ルールが必要です。認証後ルールは、すでにゲストフローを通過したユーザと一致します。これは、すでにサインインしている場合は、ルールにヒットし、そこで停止すると言うことです。ログインしていない場合は、リストをダウンし続け、リダイレクトを受け取る事前認証ルールをヒットします。認証ポリシールールをSSIDで終わる着信側ステーションIDと照合して、設定されたWLANのみにヒットすることをお勧めします。

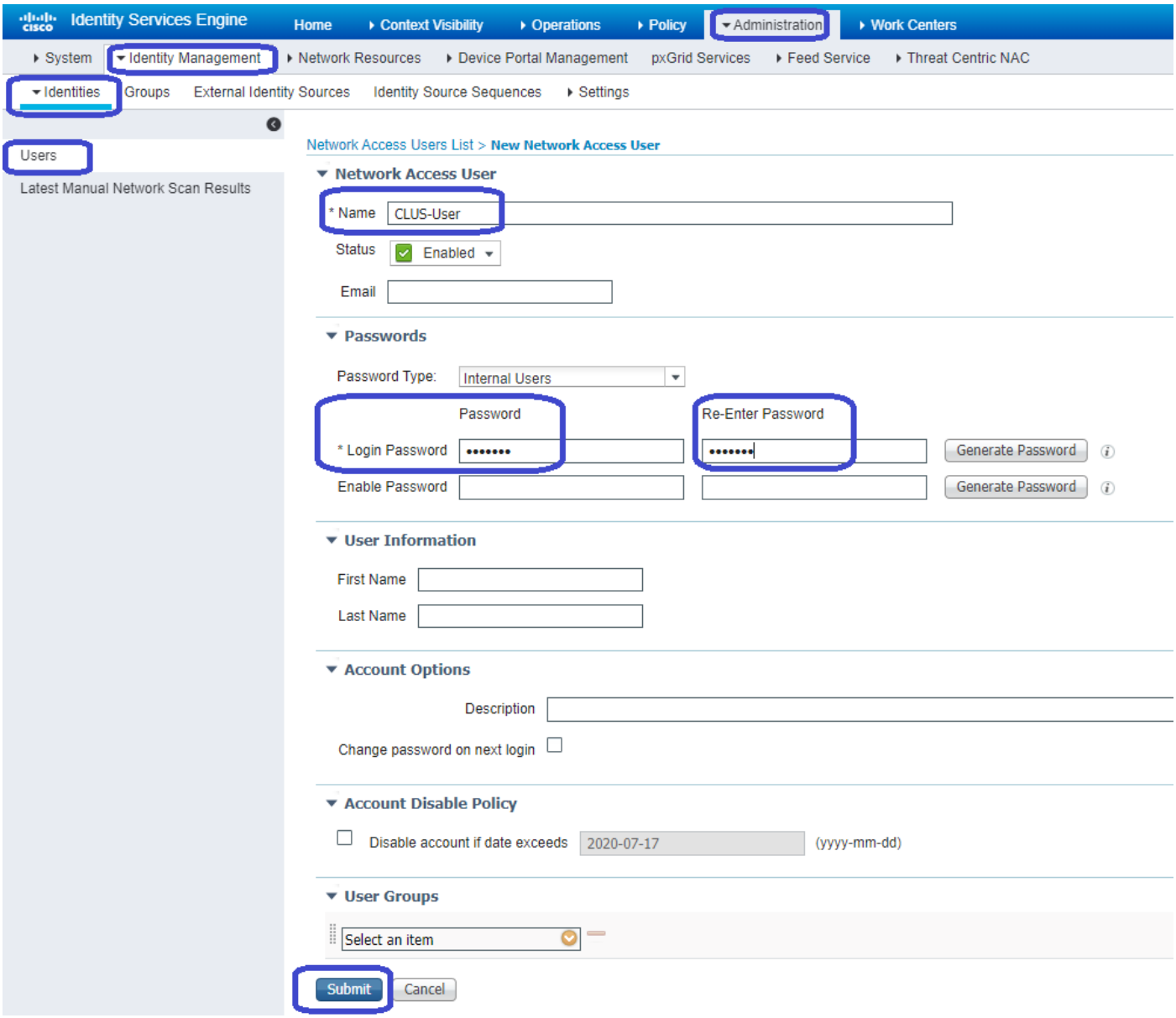


ポリシーセットを設定したら、ISEがオーセンティケータとして信頼できるように、9800（外部）についてISEに通知する必要があります。これは、[Admin] > [Network Resources] > [Network Device] > [+]で実行できます。名前を付け、IPアドレス（この場合はadminサブネット全体）を設定し、RADIUSを有効にし、共有秘密を設定する必要があります。ISEの共有秘密は、9800の共有秘密と一致する必要があります。一致しないと、このプロセスは失敗します。設定を追加したら、送信ボタンを押して保存します。

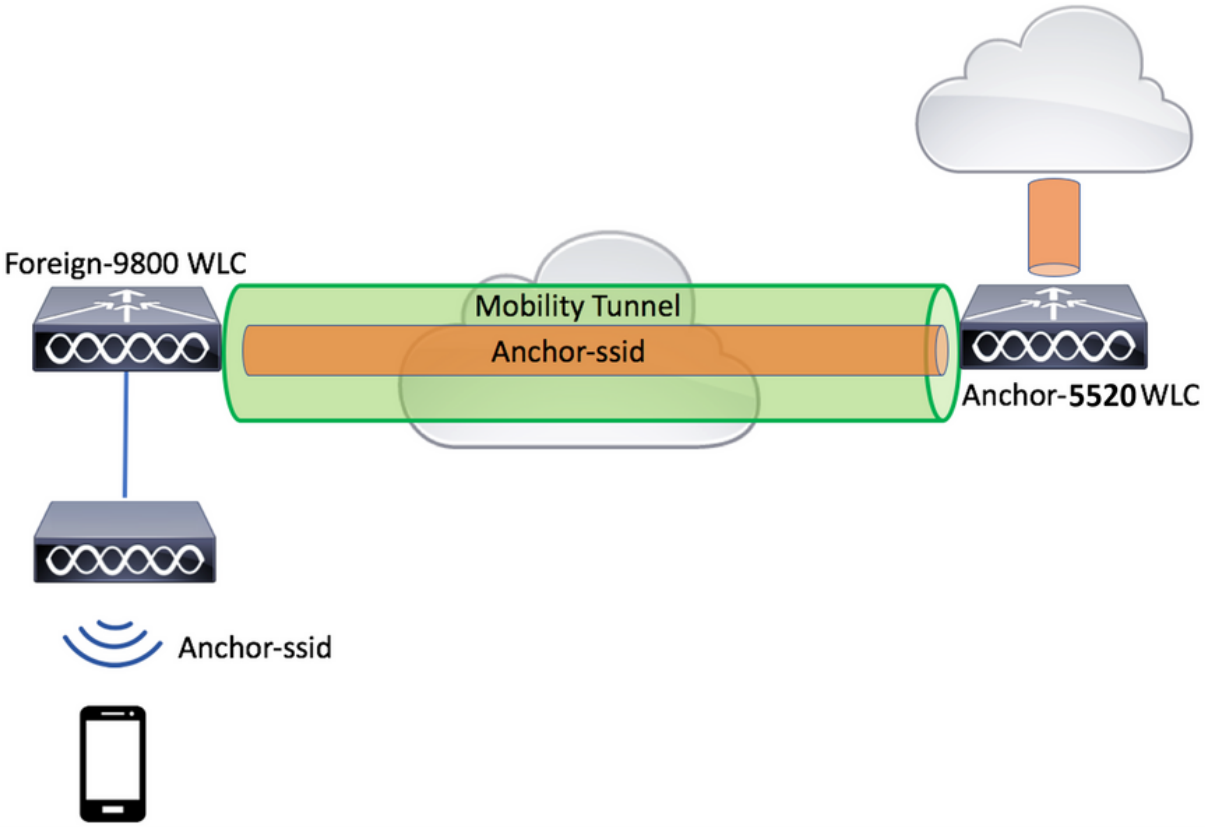


最後に、クライアントがネットワークにアクセスできることを確認するために、クライアントがログインページに入力するユーザ名とパスワードを追加する必要があります。これは、[Admin] >

[Identity Management] > [Identity] > [Users] > [Add] で行います。追加した後で[submit]をクリックしてください。 ISEと同様に、これはカスタマイズ可能で、ローカルに保存する必要はありませんが、もう一度は最も簡単な設定です。



AireOS WLCにアンカーされたCatalyst 9800の設定

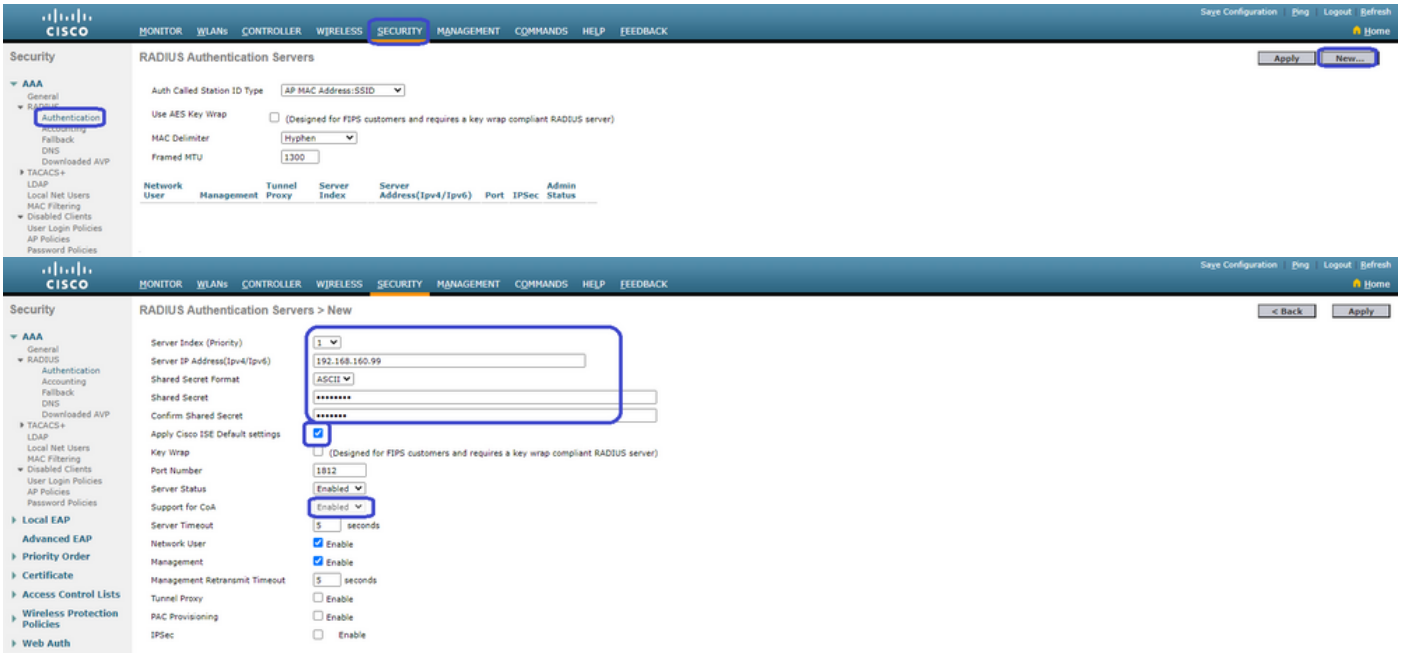


Catalyst 9800の外部設定

「アンカーWLCでのポリシープロファイルの作成」セクションをスキップし、*前述の手順と同じ手順に従ってください。*

アンカーAireOS WLCのAAA設定

[**Security**] > [AAA] > [RADIUS] > [Authentication] > [New]の順に選択して、サーバをWLCに追加します。サーバのIPアドレス、共有秘密、およびCoAのサポートを追加します。

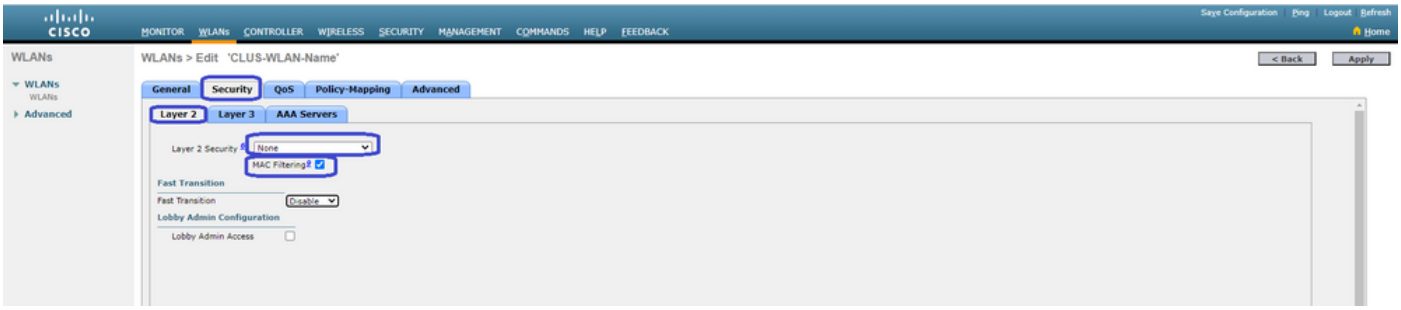


AireOS WLCのWLAN設定

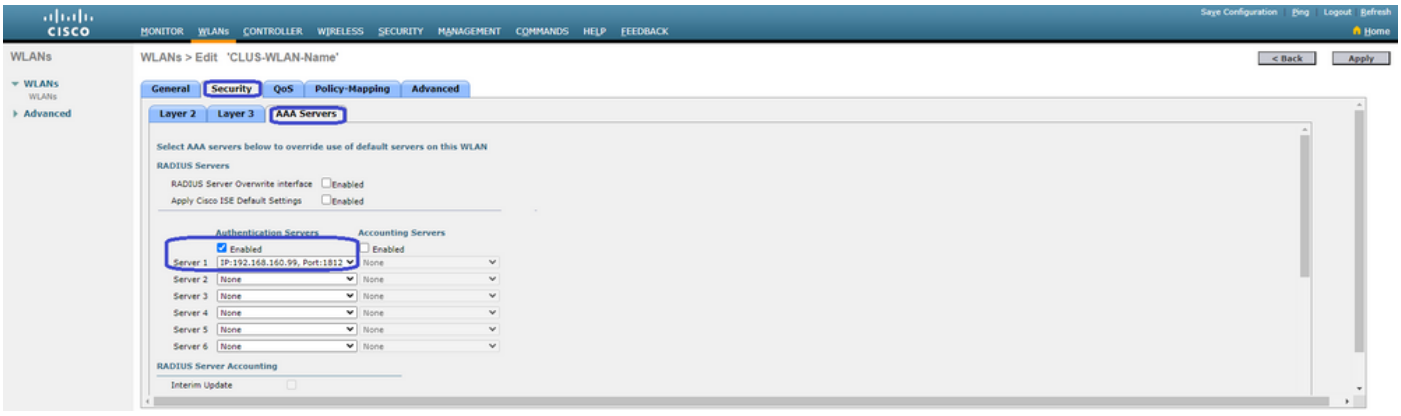
WLANを作成するには、[WLANs] > [**Create New] > [Go]に移動します。**

プロファイル名、WLAN ID、およびSSIDを設定し、[Apply]をクリックします。

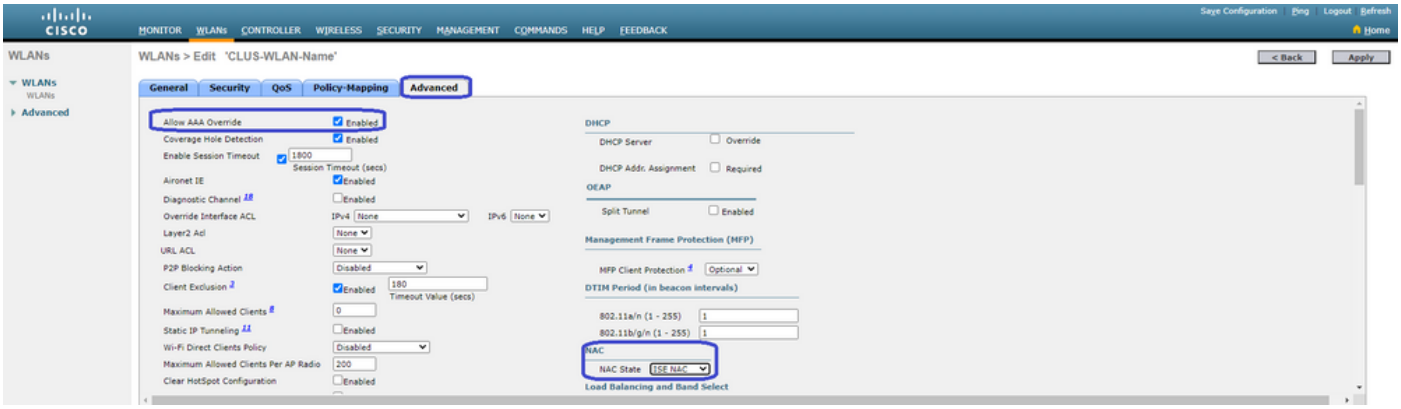
これにより、WLAN設定が表示されます。[General]タブでは、AVPでISEを送信するように設定しない場合に、クライアントで使用するインターフェイスを追加できます。次に、[Security] > [Layer2]タブに移動し、9800で使用した[Layer 2 Security]設定と一致し、[MAC Filtering]を有効にします。



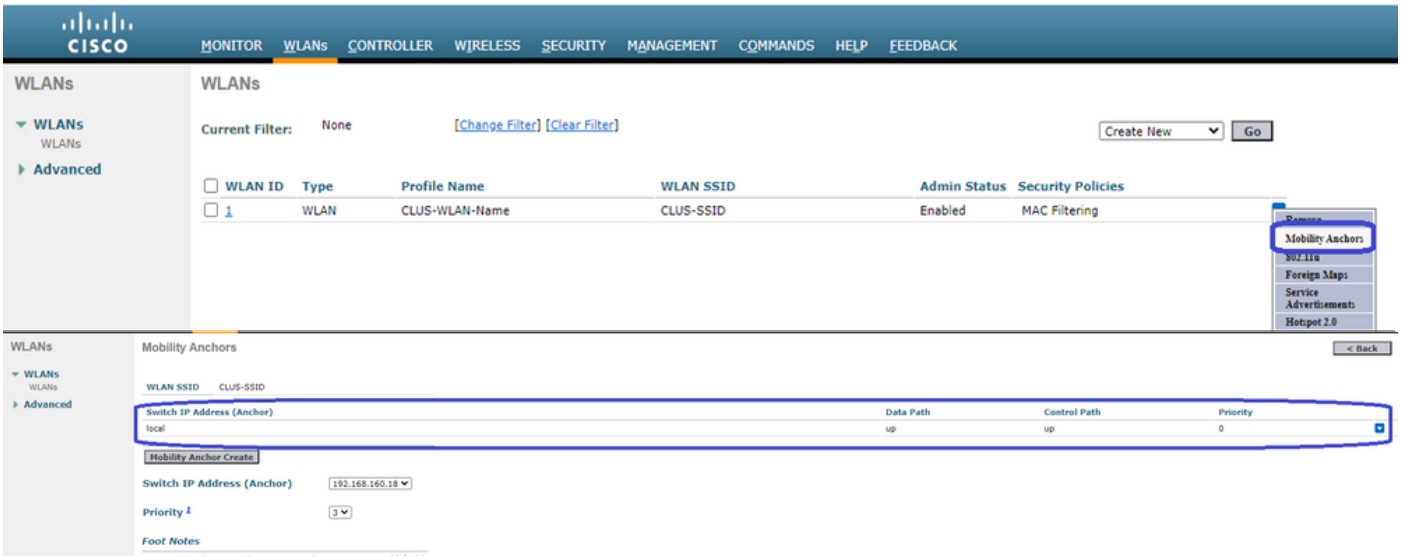
次に、[**Security**] > [**AAA Servers**]タブに移動し、ISEサーバを[Authentication Servers]に設定します。 **Accounting Serversに**は何も設定しないでください。 アカウンティングの[Enable]ボックスをオフにします。



WLANの設定を続けながら、[Advanced]タブに移動し、[Allow AAA Override]を有効にし、[NAC State]を[ISE NAC]に変更します



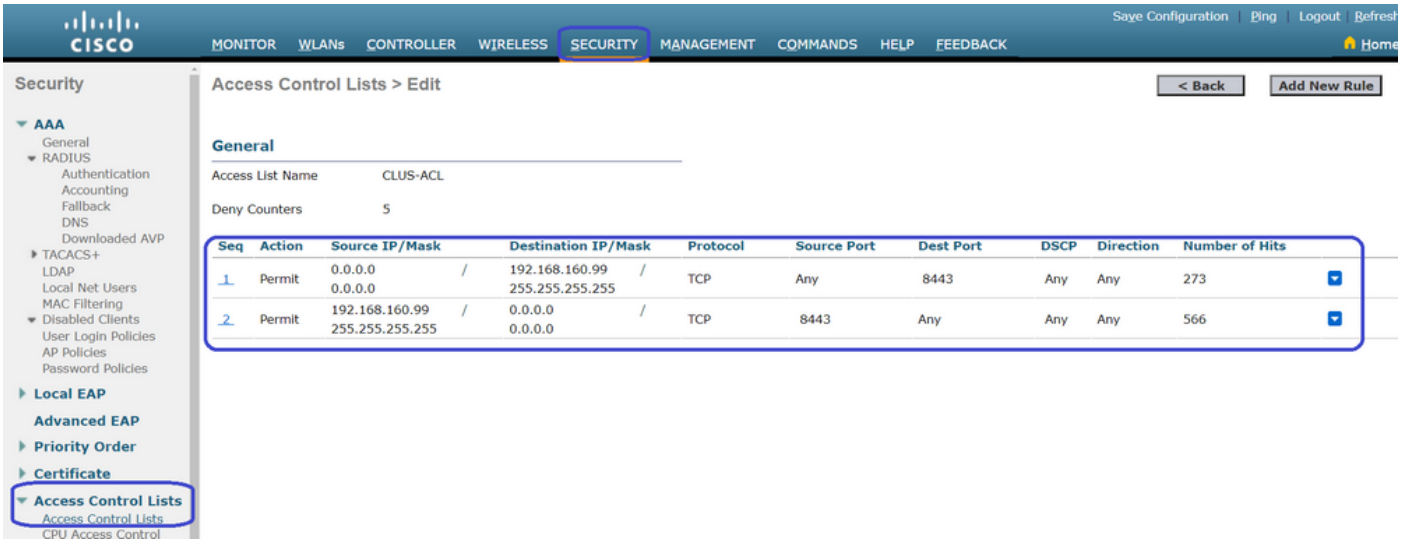
最後に、自分自身に固定します。これを行うには、[**WLANs**]ページに戻り、[WLAN] > [Mobility Anchors]の右側にある青いボックスにカーソルを合わせます。[Switch IP Address (Anchor)]を[local]に設定し、[Mobility Anchor Create]ボタンを押します。次に、プライオリティ0がアンカーされたローカルで表示されます。



AireOS WLCでのリダイレクトACL

これは、AireOS WLCで必要な最終的な設定です。リダイレクトACLを作成するには、[**Security**] > [**Access Control Lists**] > [**Access Control Lists**] > [**New**]**に移動します**。ACL名（これはAVPで送信されるものと一致している必要があります）を入力し、[Apply]をクリックします。

作成したACLの名前をクリックします。[Add New Rule]ボタンをクリックします。9800コントローラとは異なり、AireOS WLCでは、リダイレクトされずにISEに到達できるトラフィックに対してpermit文を設定します。 DHCPとDNSはデフォルトで許可されています。

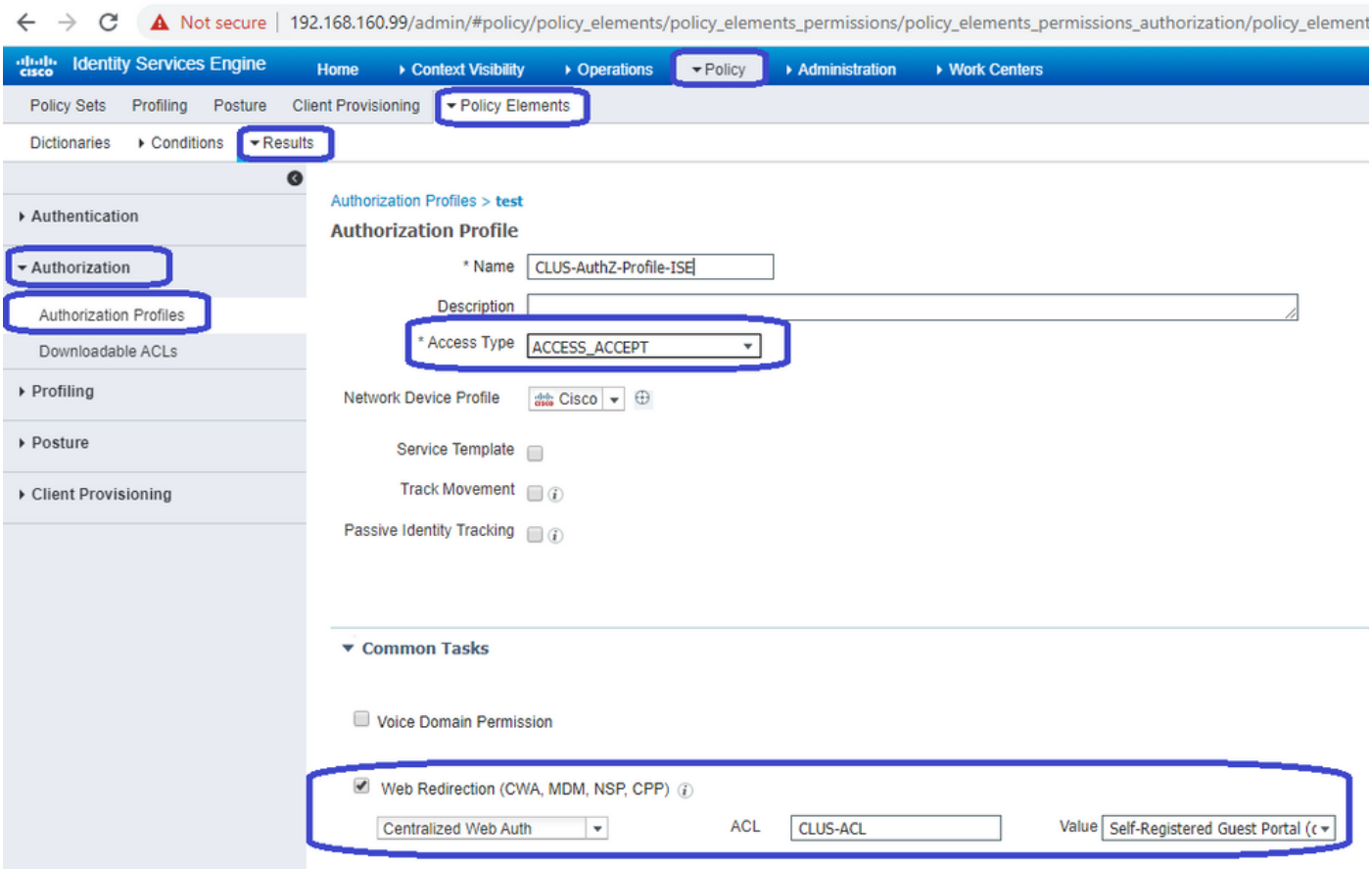


ISE の設定

CWAISE

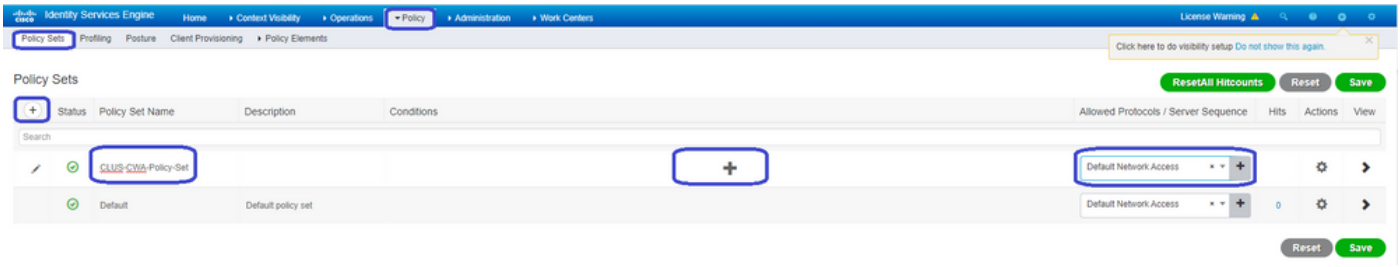
ISE9800ISE

[Policy] > [Policy Elements] > [Authorization] > [Results] > [Authorization Profiles] > [Add] access_acceptAVPCWAACLURLVLAN IDACLWLCWLCACL



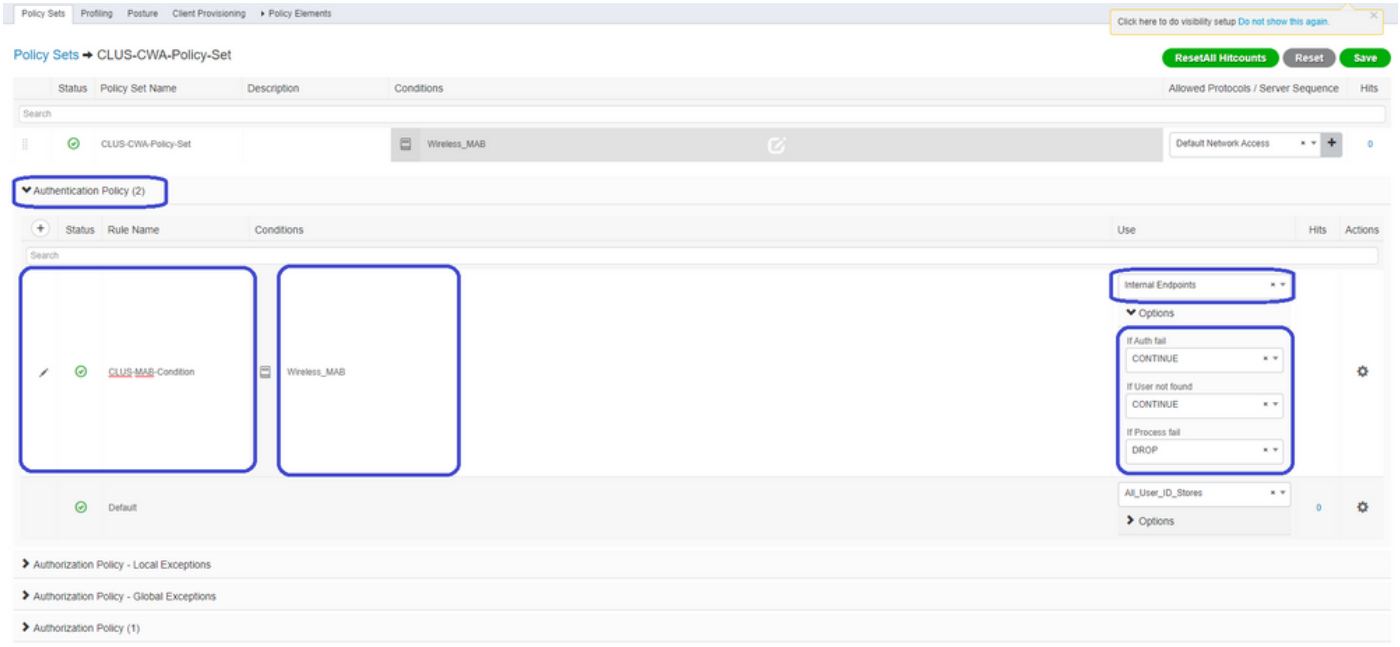
CWAMABIDSSID

[Policy] > [Policy Set]+default network accessMABProcess Host Lookup[Policy] > [Policy Elements] > [Results] > [Authentication] > [Allowed Protocols] +

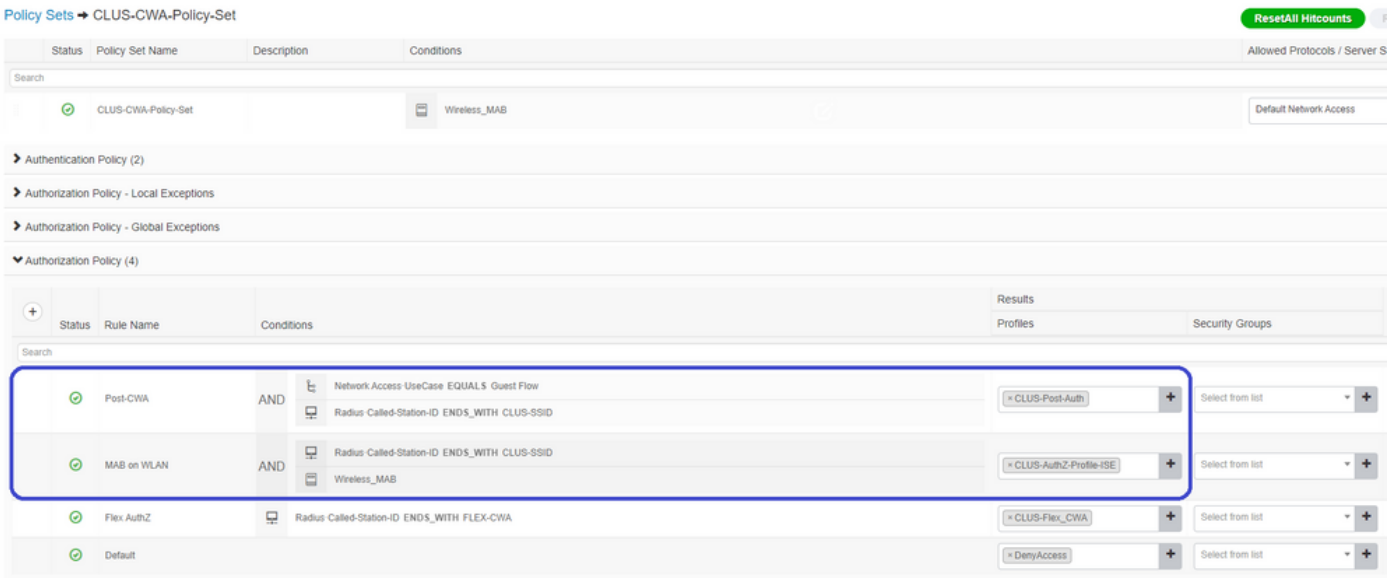


ISEMABIDWLAN

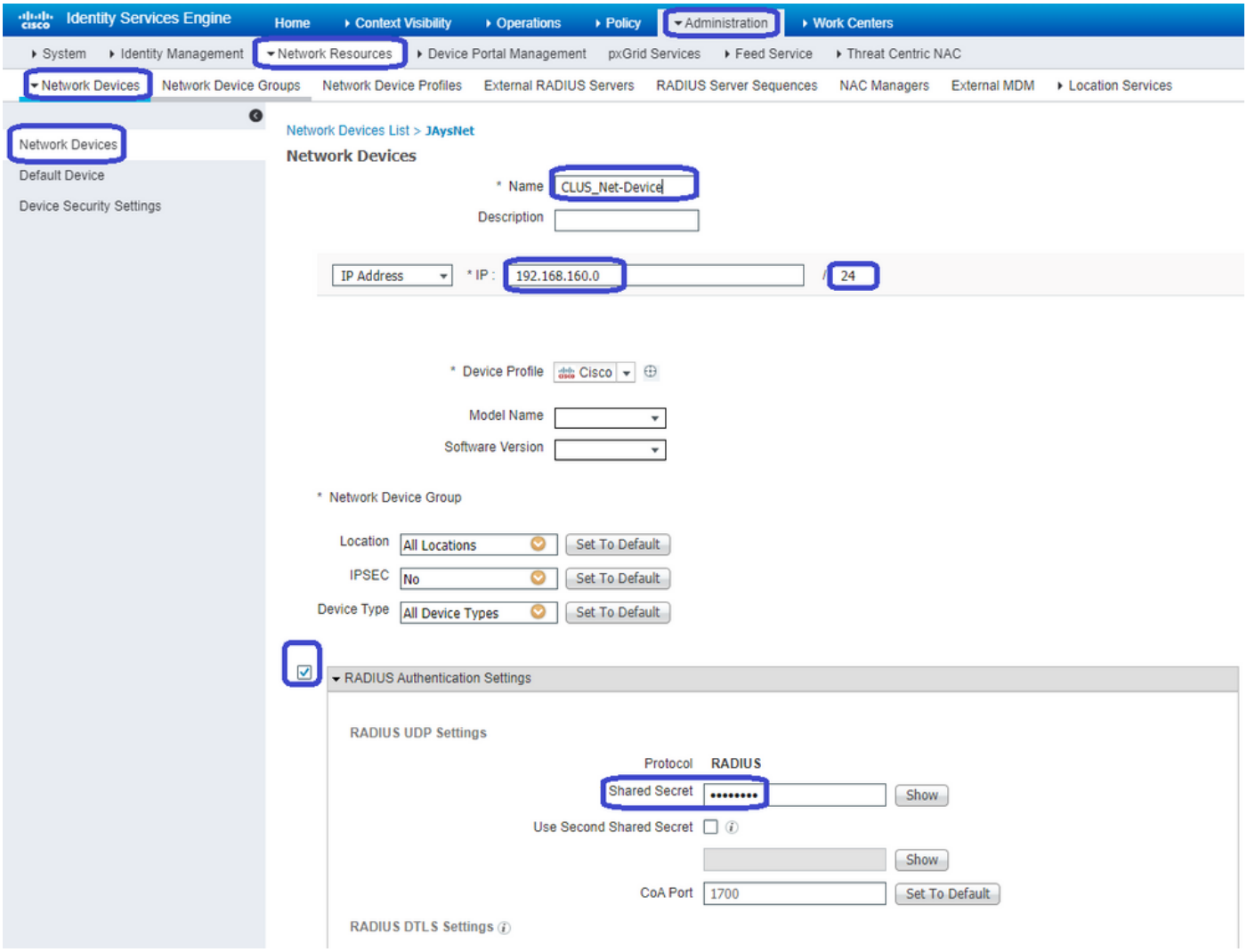
MABID



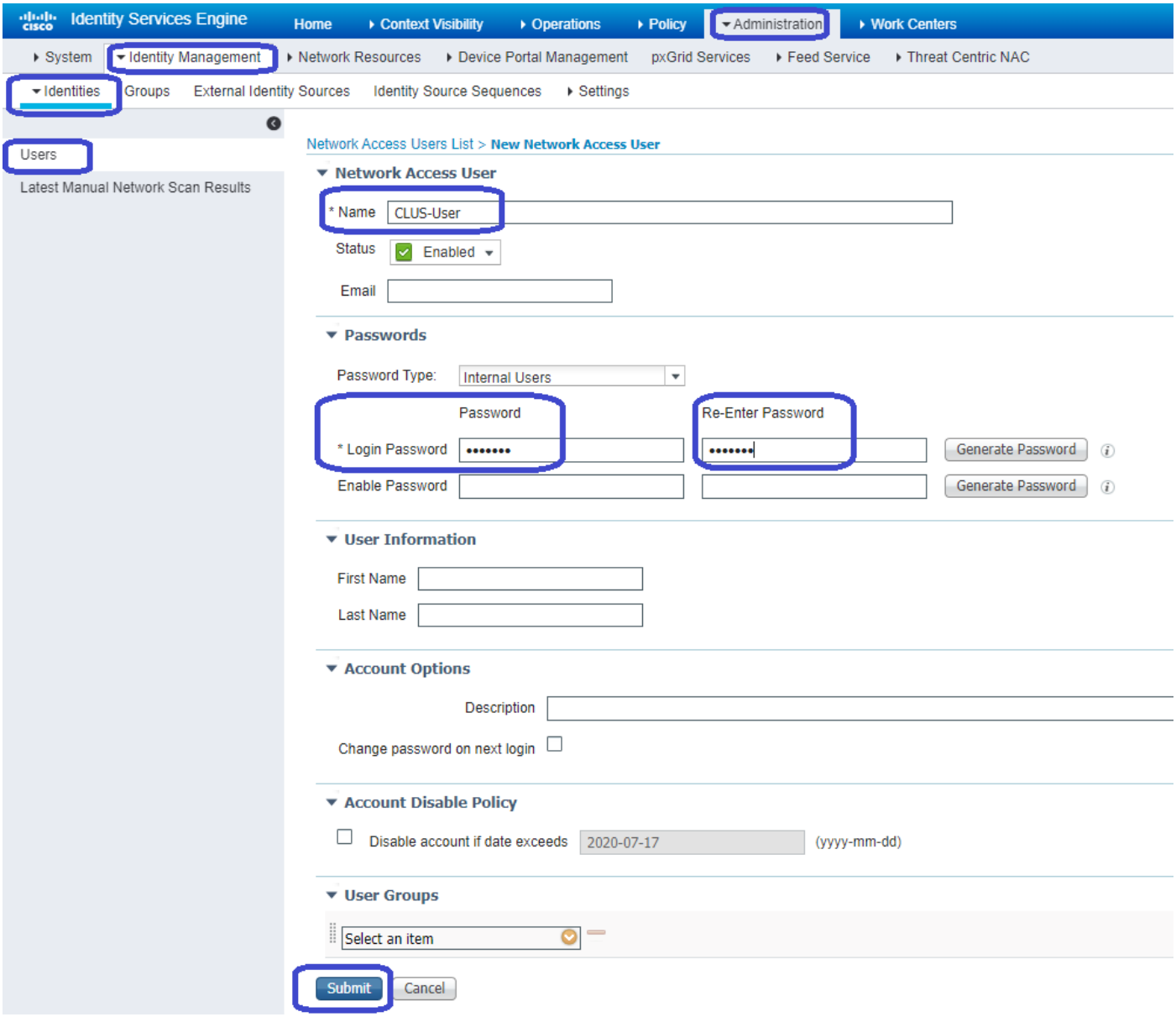
2ACLSSIDIDWLAN



ISE9800ISE**[Admin] > [Network Resources] > [Network Device]**>+.IPadminRADIUSISE9800



[Admin] > [Identity Management] > [Identity] > [Users] > [Add]submit ISE



AireOS WLCが外部で、Catalyst 9800がアンカーである場合の設定の違い

AireOs WLCを外部コントローラにする場合、設定は以前と同じですが、2つの違いがあります。

1. AAAアカウンティングはアンカーで実行されないため、9800ではアカウンティング方式リストが作成されず、AireOS WLCではアカウンティングが有効になり、ISEを指します。
2. AireOSは、それ自体ではなく9800にアンカーする必要があります。[Policy Profile]では、9800のアンカーは選択されていませんが、[Export Anchor]ボックスはオンになっています。
3. AireOS WLCがクライアントを9800にエクスポートするときに、ポリシープロファイルの概念が存在しないことに注意してください。ポリシープロファイル名だけが送信されます。したがって、9800はAireOSから送信されたWLANプロファイル名をWLANプロファイル名とポリシープロファイル名の両方に適用します。つまり、AireOS WLCから9800 WLCへのアンカーの場合、両方のWLCのWLANプロファイル名と9800のポリシープロファイル名がすべて一致している必要があります。

確認

9800 WLC上の設定を確認するには、コマンドを実行します

- [AAA]

```
Show Run | section aaa|radius
```

- WLAN

```
Show wlan id <wlan id>
```

- ポリシープロファイル

```
Show wireless profile policy detailed <profile name>
```

- ポリシータグ

```
Show wireless tag policy detailed <policy tag name>
```

- ACL

```
Show IP access-list <ACL name>
```

- アンカーでモビリティがアップしていることを確認します

```
Show wireless mobility summary
```

AireOS WLCの設定を確認するには、次のコマンドを実行します

- [AAA]

```
Show radius summary
```

注：RFC3576はCoAの設定です

- WLAN

```
Show WLAN <wlan id>
```

- ACL

```
Show acl detailed <acl name>
```

- 外部サーバとのモビリティがアップしていることを確認します

```
Show mobility summary
```

トラブルシュート

トラブルシューティングは、プロセスのどの時点でクライアントが停止するかによって異なります。たとえば、WLCがMABのISEから応答を受信しない場合、クライアントは「Policy Manager State:Associating」と入力すると、アンカーにエクスポートされません。この状況では、外部でのみトラブルシューティングを行い、WLCとISE間のトラフィックに対するRAトレースとパケットキャプチャを収集する場合があります。もう1つの例は、MABが正常に通過したが、クライアントがリダイレクトを受信しないことです。この場合、AVPで外部がリダイレクトを受信し、クライアントに適用していることを確認する必要があります。また、アンカーをチェックして、クライアントが正しいACLを持っているかどうかを確認する必要があります。 このトラブルシュー

ティングの範囲は、このテクニカルドキュメントの設計の範囲外です（一般的なクライアントのトラブルシューティングガイドラインについては、参考資料を参照してください）。

9800 WLCでのCWAのトラブルシューティングの詳細については、Cisco Live!presentation DGTL-TSTOKEN-404

Catalyst 9800のトラブルシューティング情報

クライアント詳細

show wireless client mac-address
ここでは、[Policy Manager State]、[Session Manager]、[Auth Method]、[Mobility Role]を確認します。

この情報は、GUIの[Monitoring] > [Clients]で確認することもできます

Embedded Packet Capture

CLIからコマンドは*#monitor capture <capture name>を起動*し、その後にオプションが表示されます。

GUIから[Troubleshoot] > [Packet Capture] > [Add]に移動します

RadioActiveトレース

CLI を使用する場合

debug wireless mac|ip
コマンドのno形式を使用して停止します。これは、「ra_trace」という名前のブートフラッシュ内のファイルに記録されます。その後、クライアントのMACアドレスまたはIPアドレスと日時が記録されます。

GUIから[Troubleshoot] > [Radioactive Trace] > [Add]に移動します。クライアントのMACアドレスまたはIPアドレスを追加し、applyを押してからstartを押します。プロセスを数回実行した後、トレースを停止し、ログを生成して、デバイスにダウンロードします。

AireOSのトラブルシューティング情報

クライアント詳細

CLIから*show client details <client mac>*

GUIの[Monitor] > [Clients]から

CLIからのデバッグ

Debug client

Debug mobility handoff

Debug mobility config

参考資料

9800コントローラによるモビリティトンネルの構築

9800でのワイヤレスデバッグと口グ収集