外部認証を使用したローカルWeb認証の設定

内容

概要

このドキュメントでは、9800 WLCおよびISEで外部認証を使用してローカルWeb認証を設定する方法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。

- 9800ワイヤレスLANコントローラ(WLC)の設定
- Lightweightアクセスポイント(LAP)
- 外部WebサーバのIdentity Services Engine(ISE)を設定する方法
- DHCPサーバとDNSサーバのセットアップおよび設定方法

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くものです。

- 9800-40 WLC Cisco IOS® XEバージョン17.18.4a（APSP1およびAPSP2搭載）
- Identity Services Engine(ISE)、バージョン3.2.0.542
- Cisco® Wireless 9172Iシリーズ Wi-Fi 7アクセスポイント、バージョン17.18.4.202

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。

Web 認証

Web認証は、ゲストユーザにネットワークへのアクセスを許可するレイヤ3セキュリティ機能です。

この機能は、ユーザプロファイルを設定せずに、オープンSSIDへの簡単で安全なゲストアクセスを提供するように設計されています。また、レイヤ2セキュリティ方式でも動作します。

Web認証の目的は、セキュリティメカニズムを設定できるゲストWLANを介して、信頼できないデバイス（ゲスト）が制限付きのネットワークアクセス権限でネットワークにアクセスできるようにし、ネットワークのセキュリティが損なわれないようにすることです。ゲストユーザがネットワークにアクセスできるようにするには、正常に認証される必要があります。つまり、正しいクレデンシャルを入力するか、アクセプタブルユースポリシー(AUP)を受け入れて、ネットワークにアクセスする必要があります。

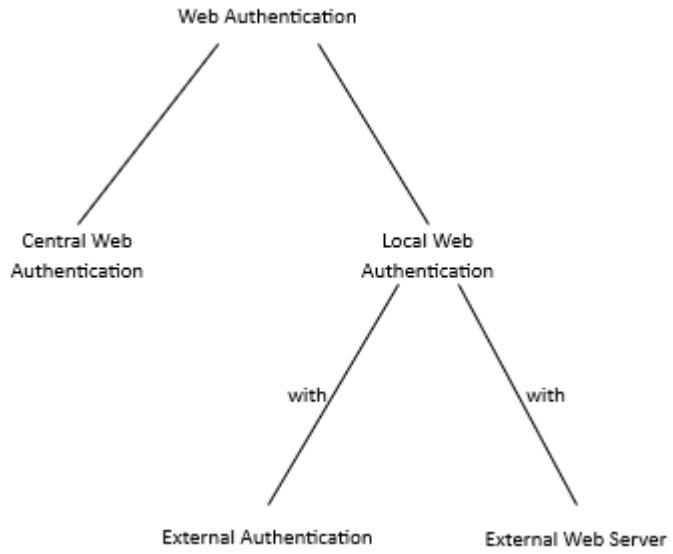
Web認証は企業にとって利点があります。なぜなら、Web認証はユーザロイヤルティを高め、ゲストユーザが受け入れる必要のある免責事項に準拠するよう企業を促し、企業が訪問者と関わることを可能にするからです。

Web認証を導入するには、ゲストポータルと認証の処理方法を考慮する必要があります。一般的な方法には次の2つがあります。

- ローカルWeb認証(LWA)：ゲストユーザをWLCからポータルに直接リダイレクトする方法。リダイレクションとWebAuth前のACLは、WLC上でローカルに設定されます。
- 中央Web認証(CWA)：リダイレクトURLとリダイレクトACLが外部サーバ（ISEなど）で一元的に設定され、RADIUSを介してWLCに通信される、ゲストユーザのリダイレクト方式。中央Web認証では、リダイレクトURLとリダイレクトACLは外部サーバ（RADIUSなど）に一元的に配置されます。 RADIUSサーバは認証を処理するサーバで、WLCに指示を送信します。CWAでは、WLCはローカルWeb認証証明書を必要とせず、中央Webポータルで必要な証明書は1つだけで、ISEなどの中央認証サーバが必要です。CWAの詳細を確認するには、「Catalyst 9800 WLCおよびISEでの中央Web認証(CWA)の設定」に移動します。

ローカルWeb認証では、WebポータルをWLCまたは外部サーバ上に配置できます。外部認証を使用するLWAでは、WebポータルはWLC上に存在します。外部Webサーバを使用するLWAでは、Webポータルは外部サーバ（Cisco DNA Spacesなど）に存在します。 外部Webサーバを使用するLWAの例は、「Catalyst 9800 WLCでのDNAスペースのキャプティブポータルの設定」で詳細に説明されています。

さまざまなWeb認証方式の図：



さまざまなWeb認証方式の図

注:Wi-Fi 7 APをWeb認証付きで9800 WLCに導入する場合、17.18.4a以降などの推奨Cisco IOS XEリリースを実行していることを確認してください。

認証のタイプ

ゲストユーザを認証するには、次の4種類の認証があります。

- Webauth：ユーザ名とパスワードを入力します。
- 同意（Webパススルー）:AUPを受け入れます。
- Authbypass：ゲストユーザデバイスのMACアドレスに基づく認証。
- Webの同意：ユーザ名/パスワードとAUPの受け入れの混在。

webauth	authbypass	consent	webconsent
Username: Password: OK	Client connects to the SSID and gets an IP address, then the 9800 WLC checks if the MAC address is allowed to enter the network, if yes, it is moved to RUN state, if it is not it is not allowed to join. (It won't fall back to web authentication)	banner1 Accept Don't Accept OK	banner login Accept Don't Accept Username: Password: OK

認証用のデータベース

認証用のクレデンシャルは、LDAPサーバ、ローカルのWLC、またはRADIUSサーバに保存できます。

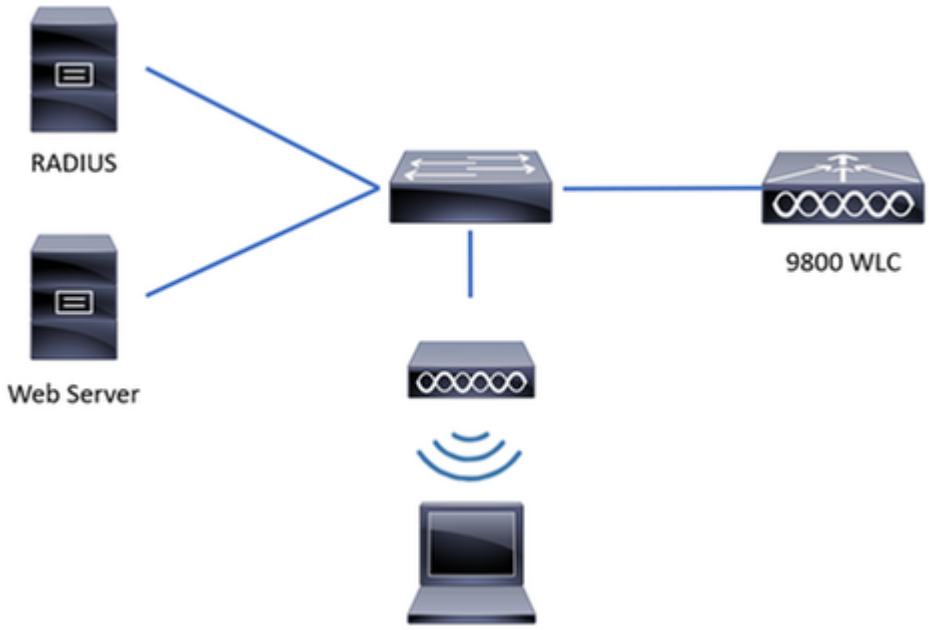
- ローカルデータベース：クレデンシャル（ユーザ名とパスワード）はWLCにローカルに保存されます。
- LDAPデータベース：クレデンシャルはLDAPバックエンドデータベースに保存されます。WLCは、データベース内の特定のユーザのクレデンシャルをLDAPサーバに照会します。
- RADIUSデータベース：クレデンシャルはRADIUSバックエンドデータベースに保存されます。WLCは、データベース内の特定のユーザのクレデンシャルをRADIUSサーバに照会します。

ローカル Web 認証

ローカルWeb認証では、ゲストユーザはWLCから直接Webポータルにリダイレクトされます。

Webポータルは、WLCまたは別のサーバにあります。ローカルにするのは、リダイレクトURLと、トラフィックと一致するACLが（Webポータルの場所ではなく）WLC上にある必要があるということです。 LWAでは、ゲストユーザがゲストWLANに接続すると、WLCがゲストユーザからの接続をインターセプトし、ゲストユーザが認証を求められるWebポータルURLにリダイレクトします。ゲストユーザがクレデンシャル（ユーザ名とパスワード）を入力すると、WLCがクレデンシャルをキャプチャします。WLCは、LDAPサーバ、RADIUSサーバ、またはローカルデータベース（WLCにローカルに存在するデータベース）を使用してゲストユーザを認証します。RADIUSサーバ（ISEなどの外部サーバ）の場合は、クレデンシャルの保存だけでなく、デバイス登録とセルフプロビジョニングのオプションの提供にも使用できます。Cisco DNA Spacesなどの外部Webサーバの場合、Webポータルはそこにあります。LWAでは、WLCとWebポータルにそれぞれ証明書があります。

次の図は、LWAの一般的なトポロジを表しています。



LWAの一般的なトポロジ

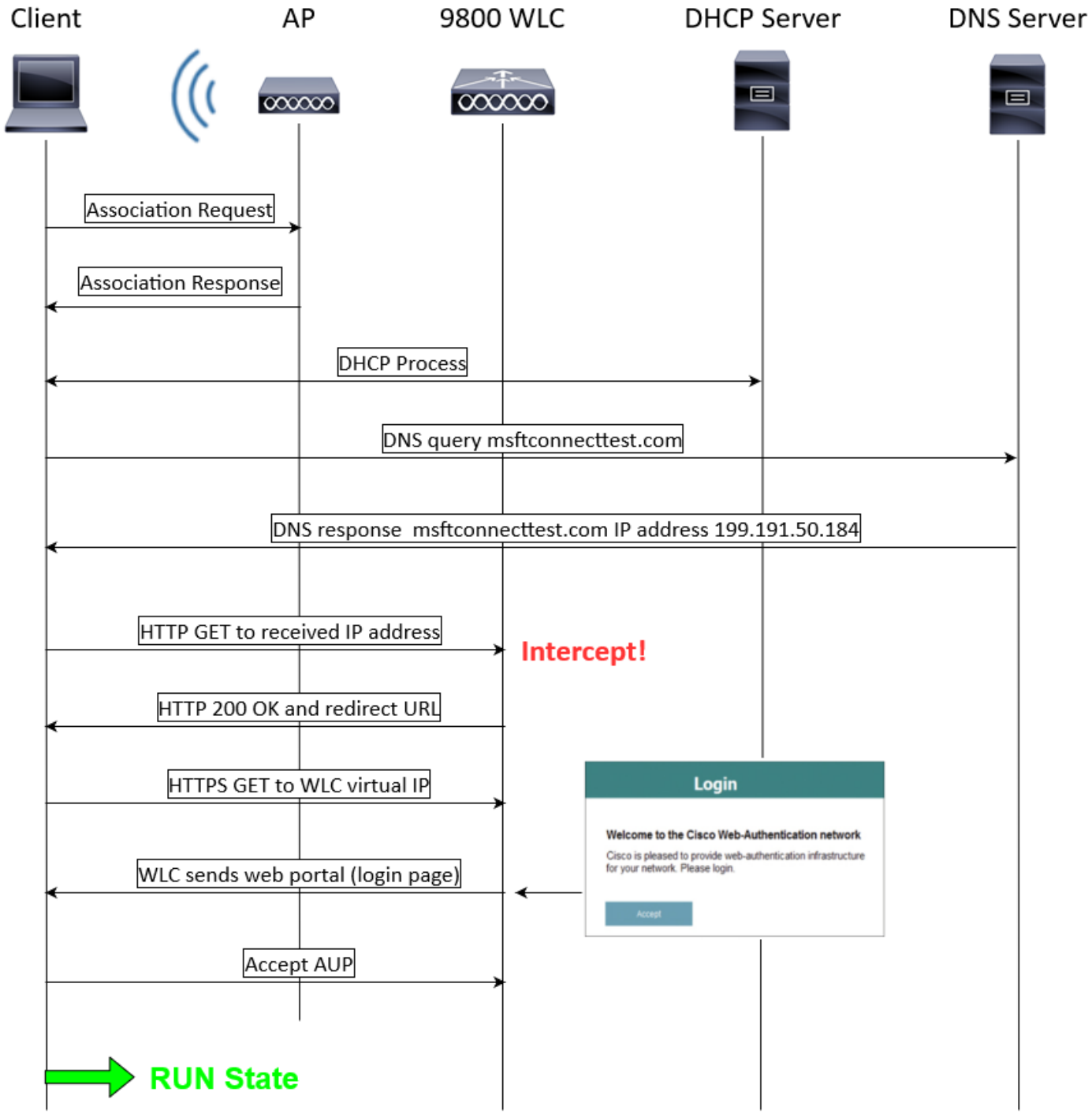
LWAのネットワークトポロジのデバイス：

- クライアント：DHCPおよびDNSサーバに要求を送信し、ゲストWLANへのアクセスを要求し、WLCからの要求に応答します。
- アクセスポイント：スイッチに接続し、ゲストWLANをブロードキャストし、ゲストユーザデバイスにワイヤレス接続を提供します。また、ゲストユーザが認証される前（有効なクレデンシャルを入力する前）にDHCPおよびDNSパケットを許可します。
- WLC:APとクライアントを管理します。WLCは、リダイレクトURLと、トラフィックに一致するACLをホストします。ゲストユーザからのHTTP要求を代行受信し、ゲストユーザの認証が必要なWebポータル（ログインページ）にリダイレクトします。クレデンシャルをキャプチャしてゲストユーザを認証し、クレデンシャルが有効であるかどうかを確認するために外部サーバ、LDAPサーバ、またはローカルデータベースにアクセス要求を送信します。
- 認証サーバ：WLCからのアクセス要求に対して、アクセス許可/拒否で応答します。認証サーバは、ゲストユーザからのクレデンシャルを検証し、クレデンシャルが有効であるか無効であるかをWLCに通知します。クレデンシャルが有効な場合、ゲストユーザはネットワークへのアクセスが許可されます（認証サーバはデバイス登録とセルフプロビジョニングのオプションを提供します）。 クレデンシャルが有効でない場合、ゲストユーザはネットワークへのアクセスを拒否されます。

LWAフロー：

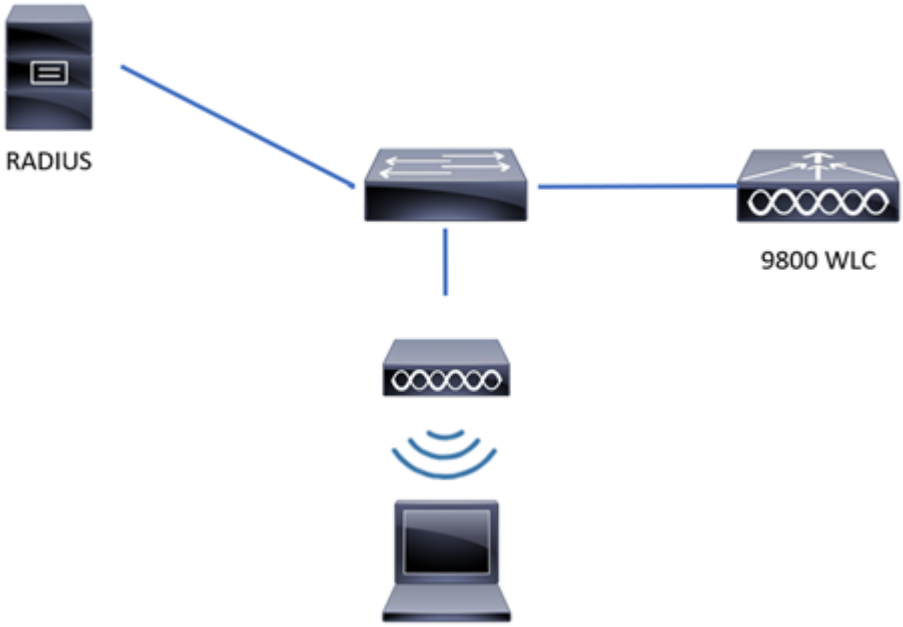
- ゲストユーザは、ゲストWLANをブロードキャストするAPと関連付けられます。
- ゲストユーザはIPアドレスを取得するためにDHCPプロセスを実行します。
- ゲストユーザは、キャプティブポータルへのインターネット接続を確認する必要があります。Appleデバイスの場合はAppleキャプティブポータル、Androidデバイスの場合はAndroidキャプティブポータル、Windowsデバイスの場合はWindows Connectテストポータルが試行

されます。
- ゲストユーザはDNSクエリを送信して、キャプティブポータルのIPアドレスの入力を求めます。DNSサーバは、対応するIPアドレスでクエリに応答します。
- ゲストユーザは、キャプティブポータルのIPアドレスにHTTP GETメッセージを送信します。
- WLCはそのメッセージをインターセプトし、HTTP 200 OKとリダイレクトURLを使用してゲストユーザに応答します。
- ゲストユーザがHTTPS GETメッセージをWLC仮想IPに送信し、WLCがWebポータルで応答します。
- ゲストユーザはWebポータルで認証クレデンシャルを入力するよう求められます。
- Webポータルは、提供されたクレデンシャル（外部Webポータルを使用している場合）を使用してユーザをWLCにリダイレクトして戻します。
- WLCは、ローカルデータベースを介してゲストユーザを認証するか、またはクレデンシャルが正しいかどうか（認証タイプがwebconsentまたはwebauthの場合）を確認するためにRADIUSまたはLDAPサーバにクエリを送信します。
- クレデンシャルが正しければ、WLCはゲストユーザを認証し、RUN状態になります。クレデンシャルが正しくない場合、WLCはゲストユーザを削除します。
- WLCは、Webブラウザに入力された元のURLにクライアントをリダイレクトして戻します。



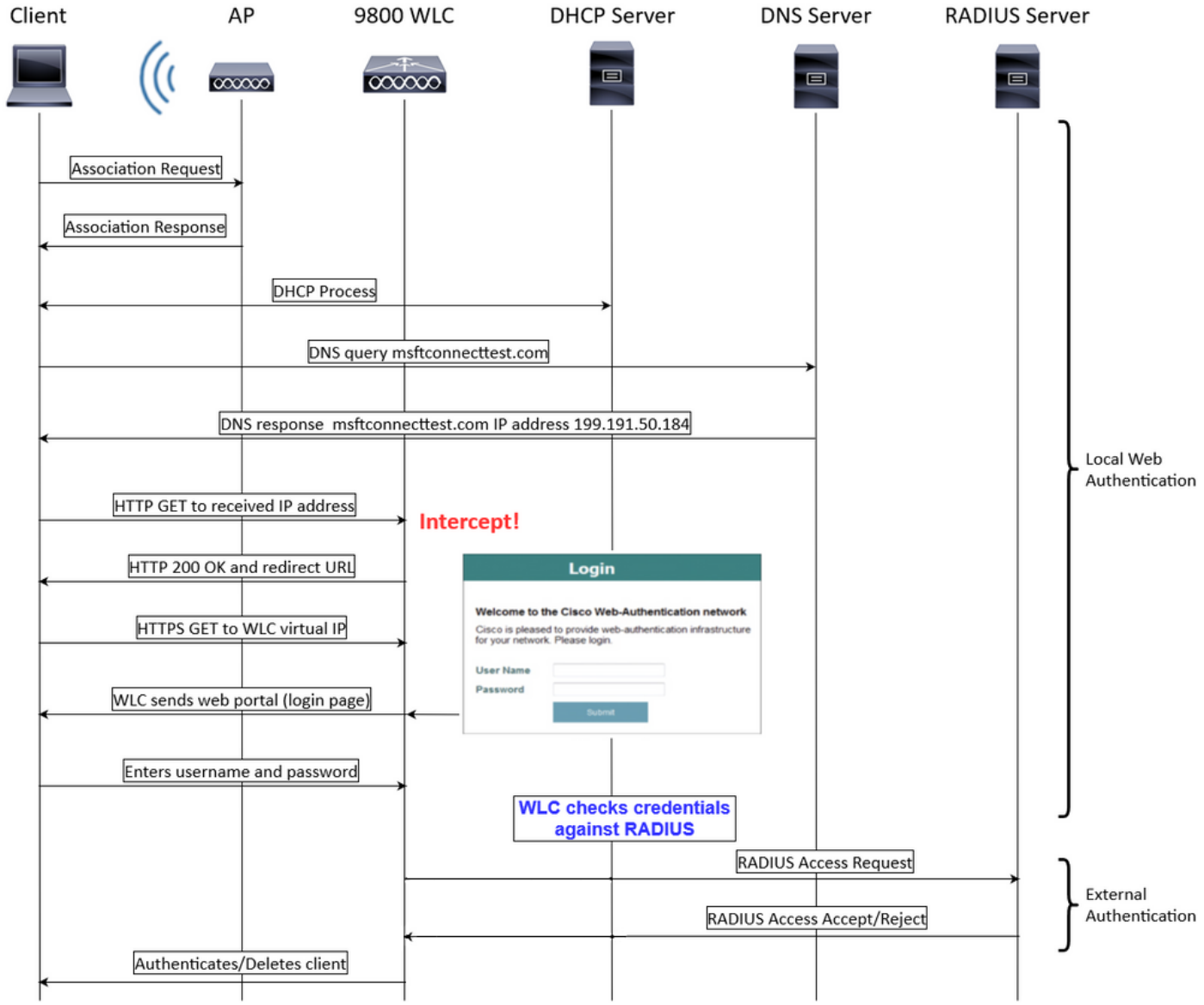
LWAフロー

外部認証を使用したローカルWeb認証



LWA-EAの一般的なトポロジ

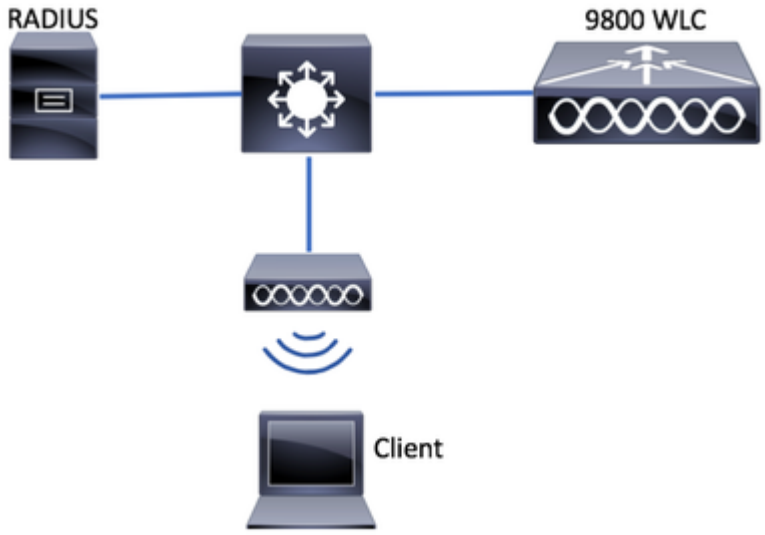
LWA-EAは、WebポータルとリダイレクションURLがWLCにあり、クレデンシャルがISEなどの外部サーバに保存されるLWAの方式です。WLCはクレデンシャルをキャプチャし、外部RADIUSサーバ経由でクライアントを認証します。ゲストユーザがクレデンシャルを入力すると、WLCはクレデンシャルをRADIUSと照合して確認し、RADIUSアクセス要求を送信して、RADIUSサーバからRADIUSアクセス許可/拒否を受信します。その後、クレデンシャルが正しければ、ゲストユーザはRUN状態になります。クレデンシャルが正しくない場合、ゲストユーザはWLCによって削除されます。



LWA-EAフロー

設定

ネットワーク図



ネットワーク図

注：この設定例では、中央スイッチング/認証のみを対象としています。Flex Local Switching設定には、Web認証を設定するための要件がわずかに異なります。

CLIで外部認証を使用したローカルWeb認証を設定する

AAAサーバとサーバグループの設定

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4


      auth-port 1812 acct-port 1813

9800WLC(config-radius-server)#key cisco

9800WLC(config-radius-server)#exit

9800WLC(config)#aaa group server radius RADIUSGROUP

9800WLC(config-sg-radius)#server name RADIUS

9800WLC(config-sg-radius)#end
```

ローカル認証と認可の設定

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

パラメータマップの設定

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#end
```

WLANセキュリティパラメータの設定

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

ワイヤレスポリシープロファイルの作成

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan




9800WLC(config-wireless-policy)#no shutdown


9800WLC(config-wireless-policy)#end
```

ポリシータグの作成

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

APへのポリシータグの割り当て

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap


     >


9800WLC(config-ap-tag)#policy-tag POLICY_TAG


9800WLC(config-ap-tag)#end
```

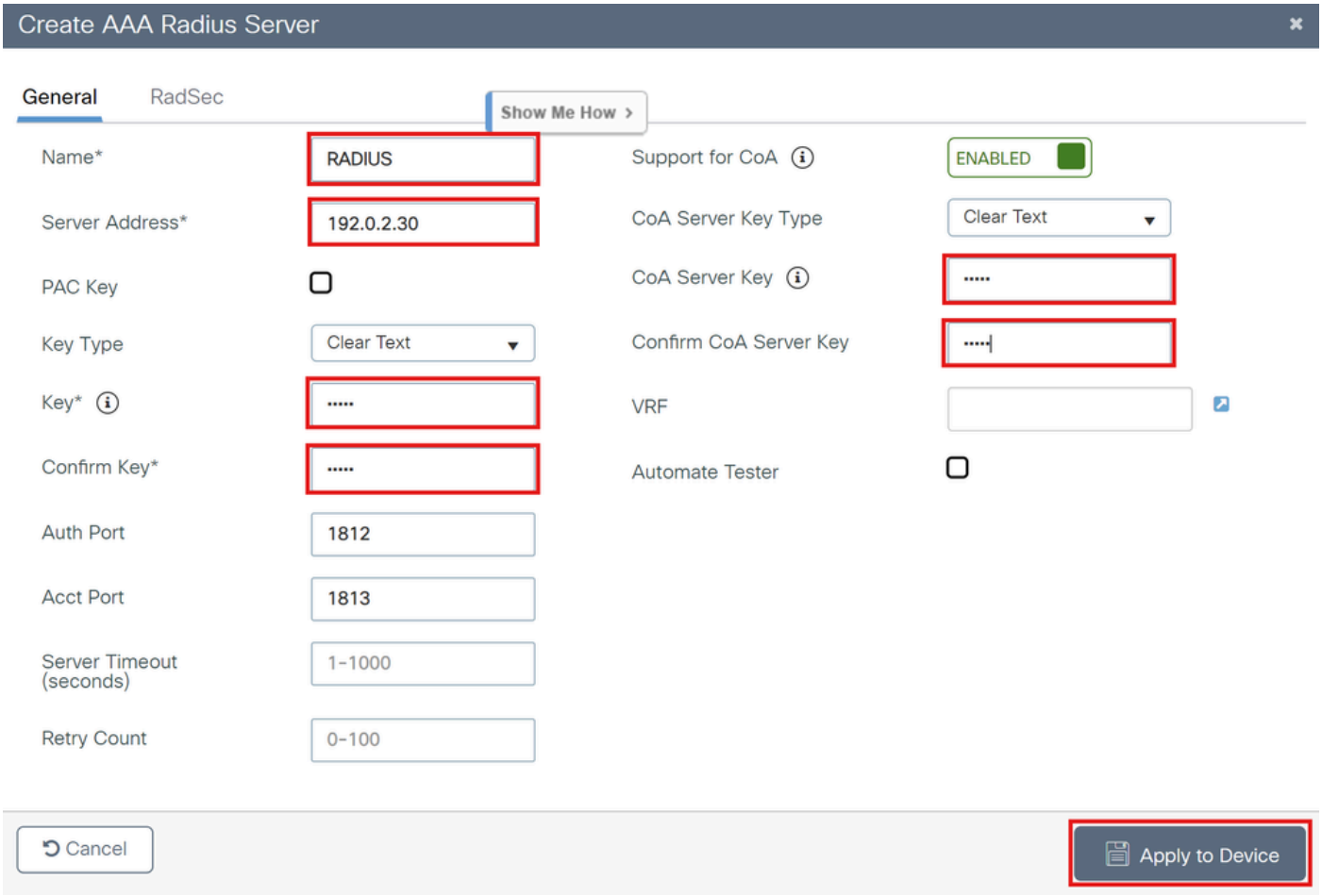
ISE側の設定を完了するには、「ISE設定」セクションにジャンプしてください。

WebUIでの外部認証を使用したローカルWeb認証の設定

9800 WLC での AAA 設定

ステップ 1：ISEサーバを9800 WLC設定に追加します。

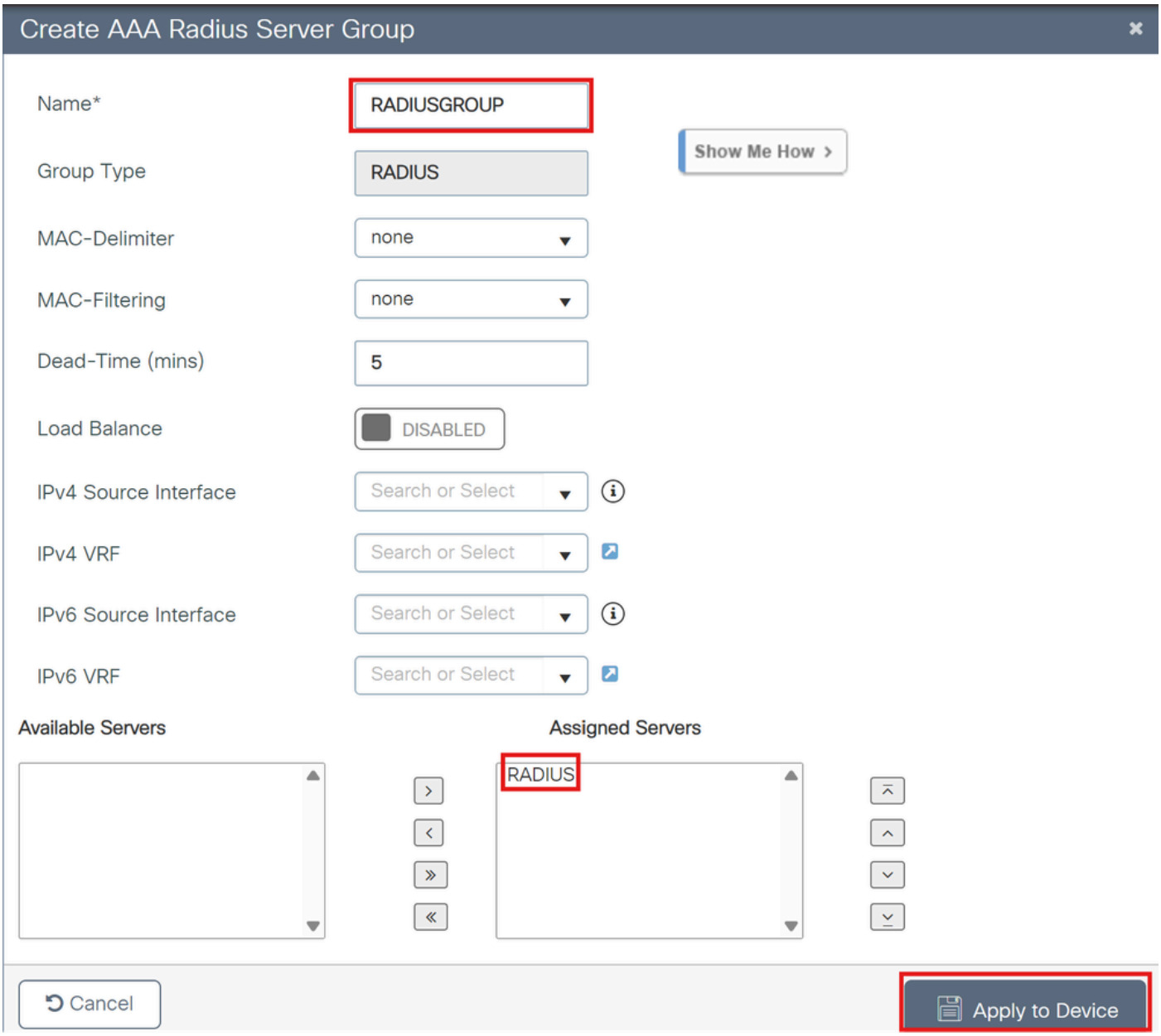
Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Addの順に移動し、図に示すようにRADIUSサーバの情報を入力します。



9800 WLC での AAA 設定

ステップ 2：RADIUSサーバグループを追加します。

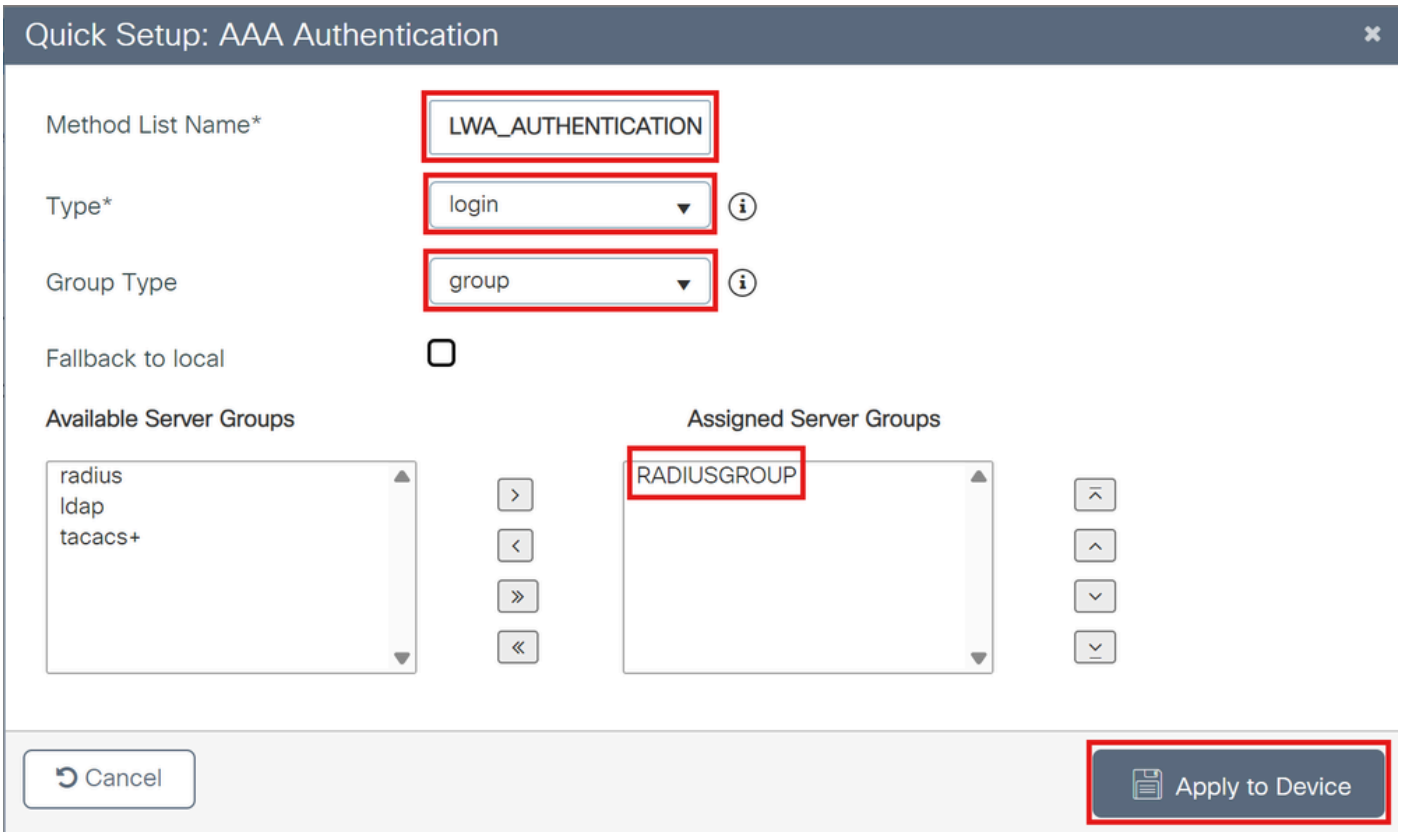
Configuration > Security > AAA > Servers/Groups > RADIUS > Servers Group > + Addの順に移動し、RADIUSサーバグループの情報を入力します。



RADIUSサーバグループの追加

ステップ 3：認証方式リストを作成します。

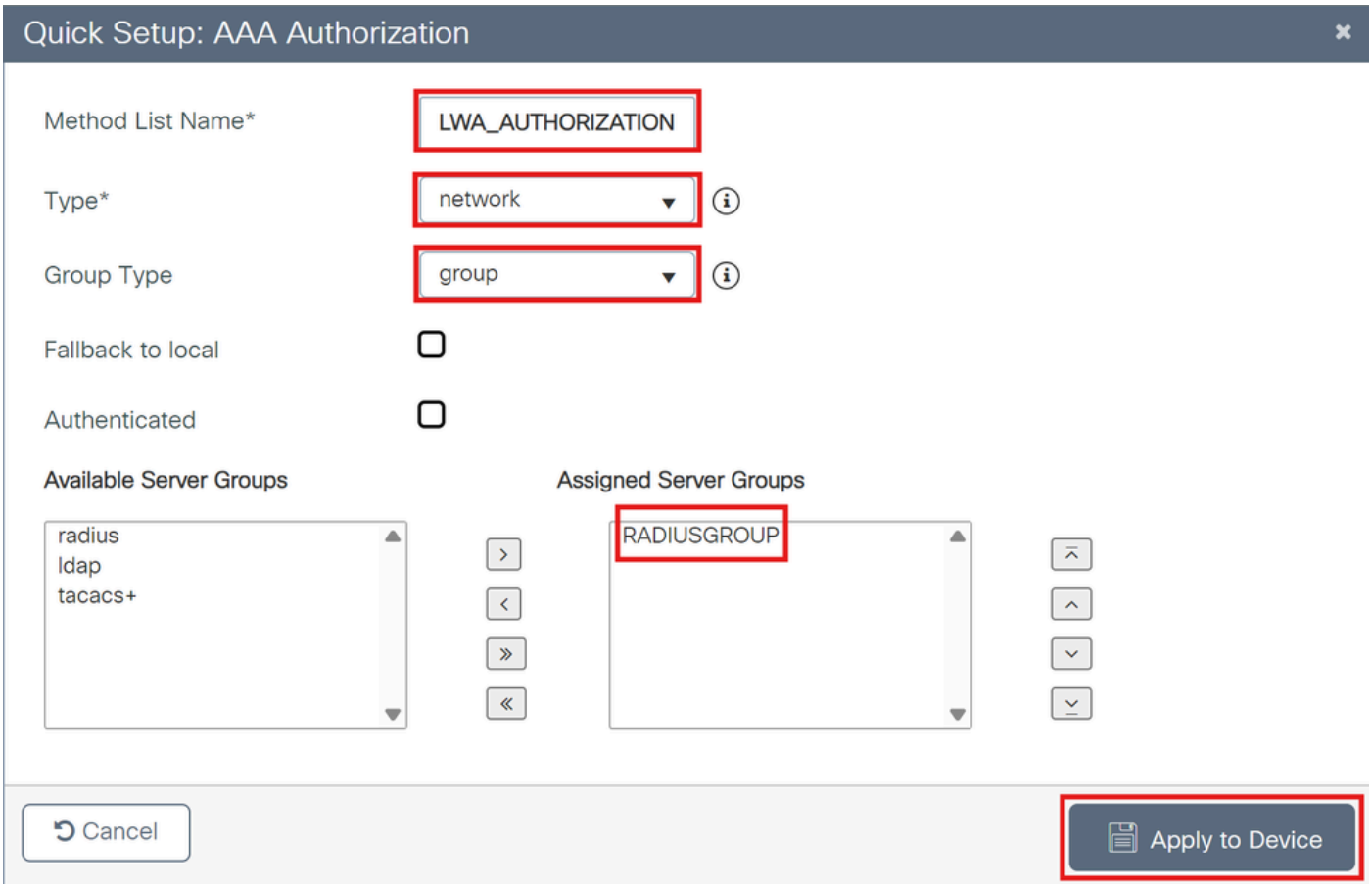
Configuration > Security > AAA > AAA Method List > Authentication > + Add:



認証方式リストの作成

ステップ 4：許可方式リストを作成します。

Configuration > Security > AAA > AAA Method List > Authorization > + Addの順に移動します。

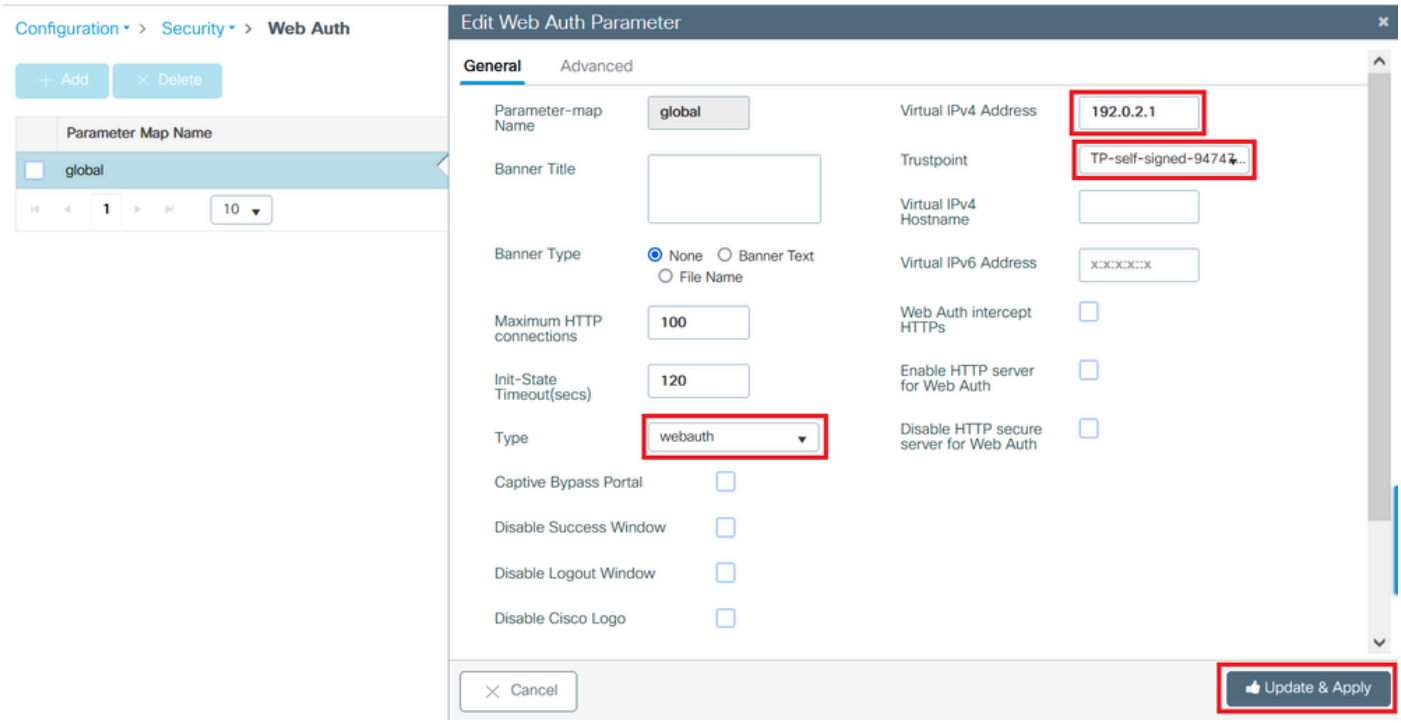


許可方式リストの作成

WebAuthの設定

パラメータマップを作成または編集します。タイプとしてwebauthを選択し、IPアドレスの競合を避けるためにVirtual IPv4 Addressはネットワークで使用されていないアドレスにする必要があり、トラストポイントを追加します。

Configuration > Security > Web Auth > + Addの順に移動するか、パラメータマップを選択します。

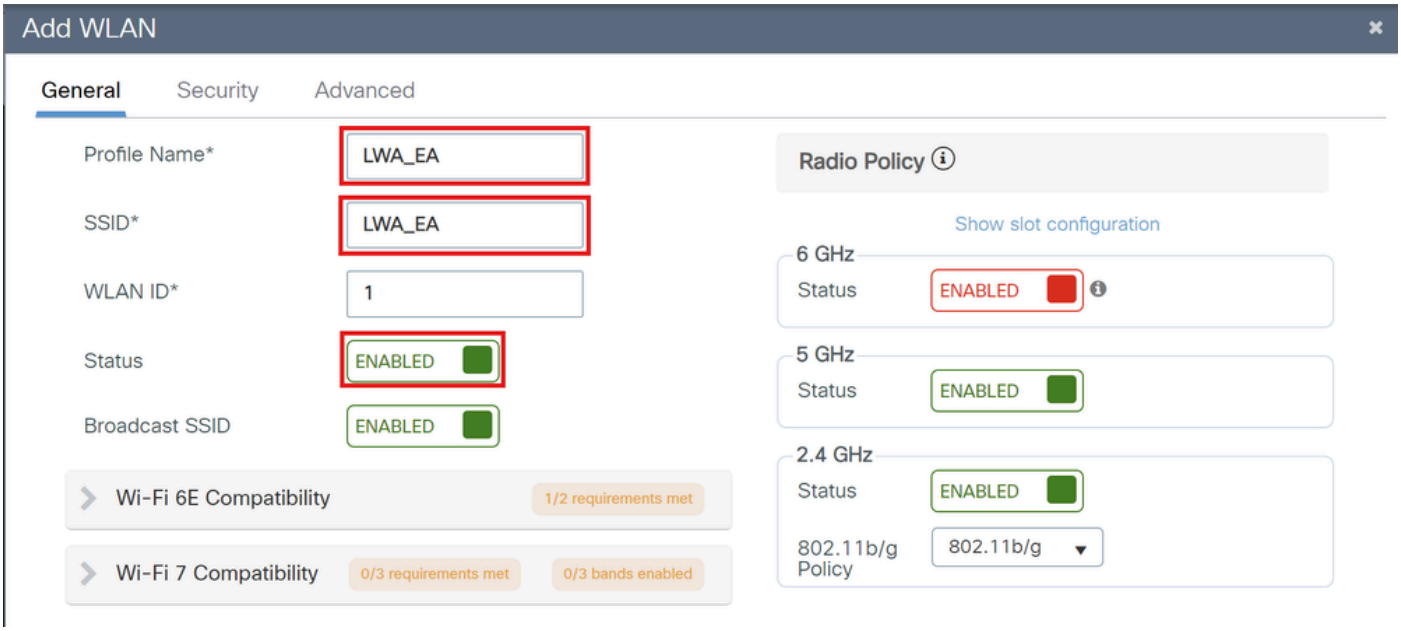


WebAuthの設定

WLAN 設定

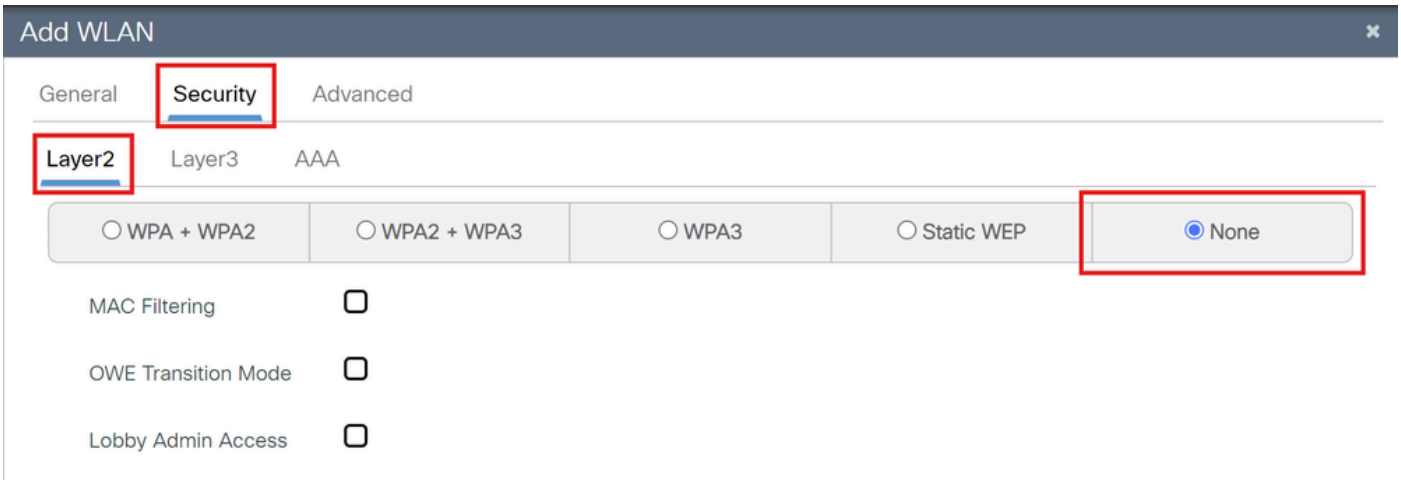
ステップ 1：WLAN を作成します。

[Configuration] > [Tags & Profiles] > [WLANs] > [+ Add] に移動し、必要に応じてネットワークを設定します。



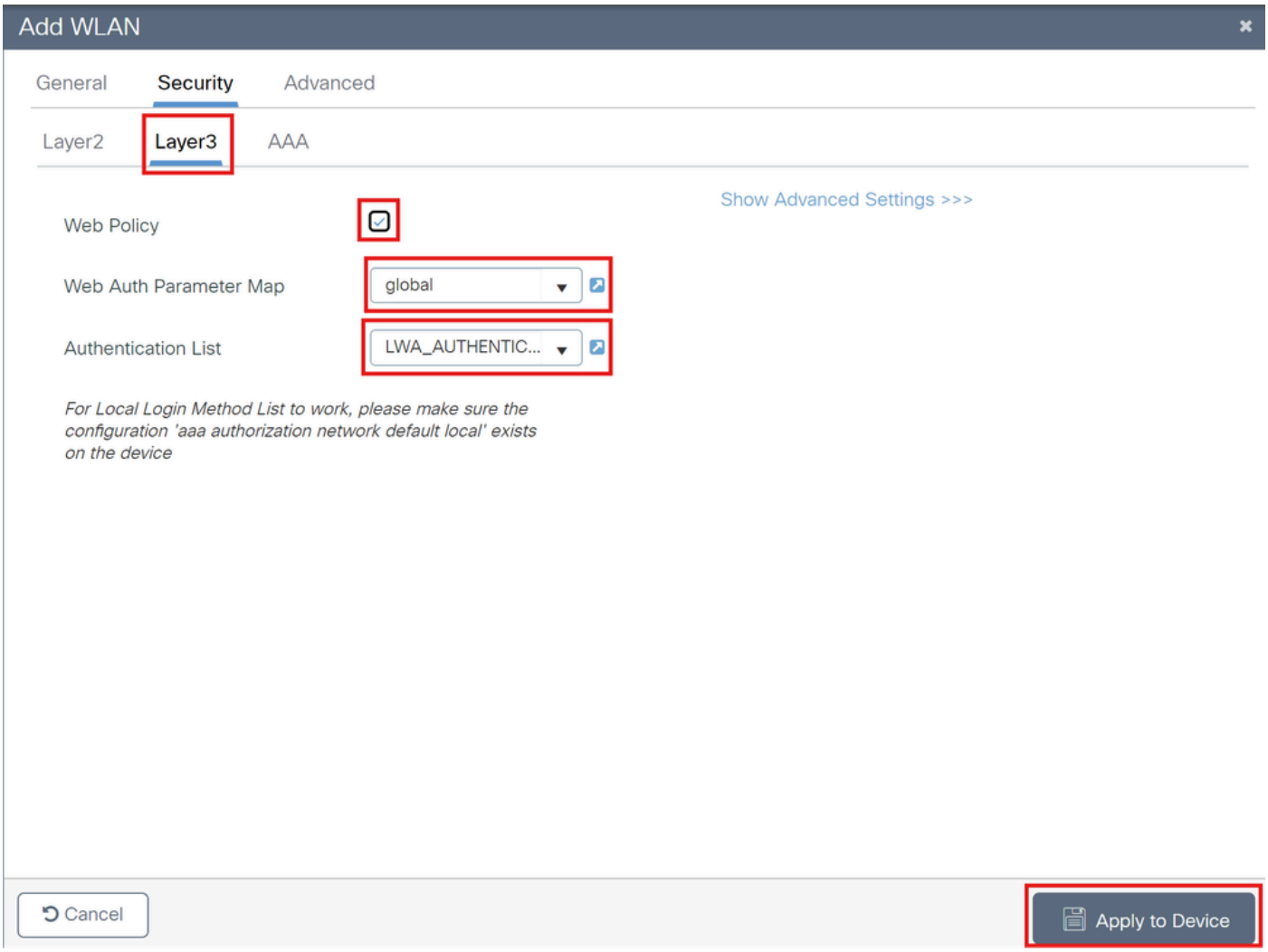
WLANの作成

ステップ 2：Security > Layer2の順に選択し、Layer 2 Security ModeでNoneを選択します。



WLANセキュリティの作成

ステップ 3：Security > Layer3に移動し、Web Policy でボックスにチェックマークを付け、Web Auth Parameter Mapでパラメータ名を選択し、Authentication Listで前に作成した認証リストを選択します。



WLANがWLANリストに表示されます。

作成されたWLAN

ポリシープロファイルの設定

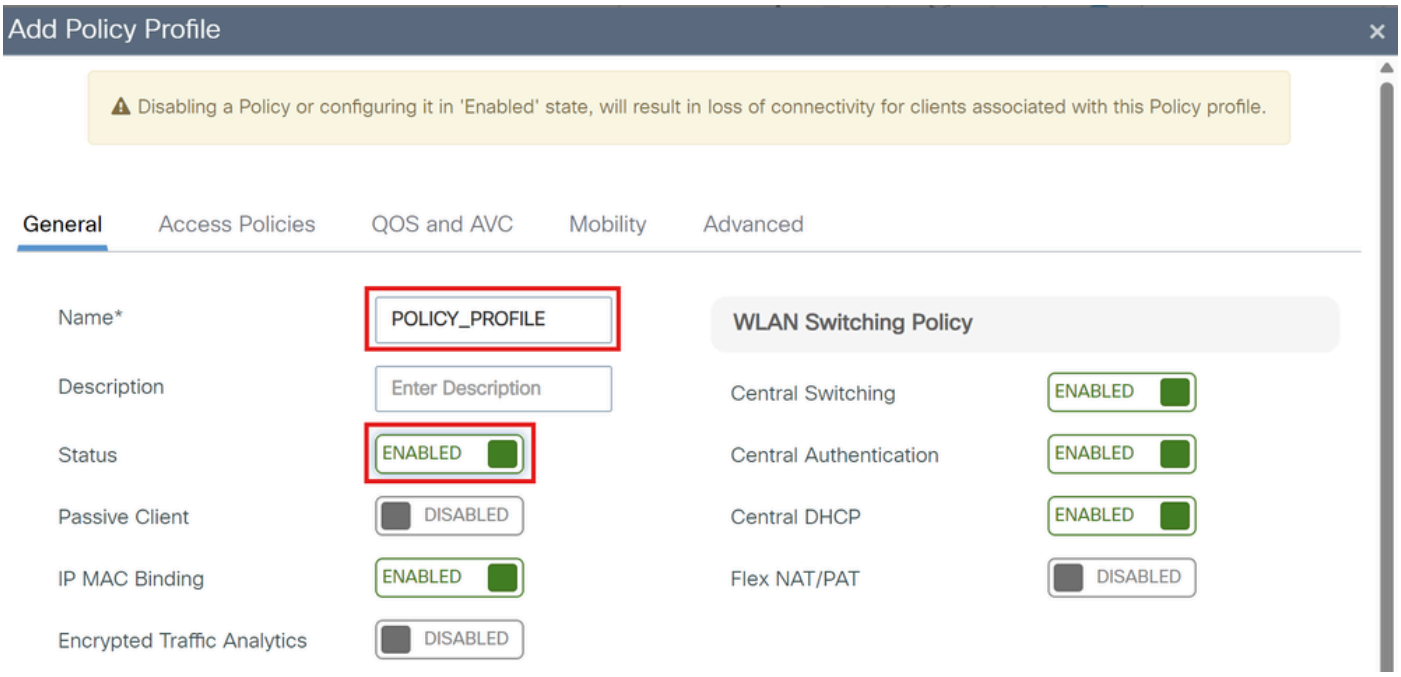
ポリシープロファイル内では、クライアントを割り当てるVLANなどの設定を選択できます。

デフォルトのポリシープロファイルを使用することも、新規に作成することもできます。

ステップ 1：新しいポリシープロファイルを作成します。

Configuration > Tags & Profiles > Policyの順に移動し、デフォルトポリシープロファイルを設定するか、新しいプロファイルを作成します。

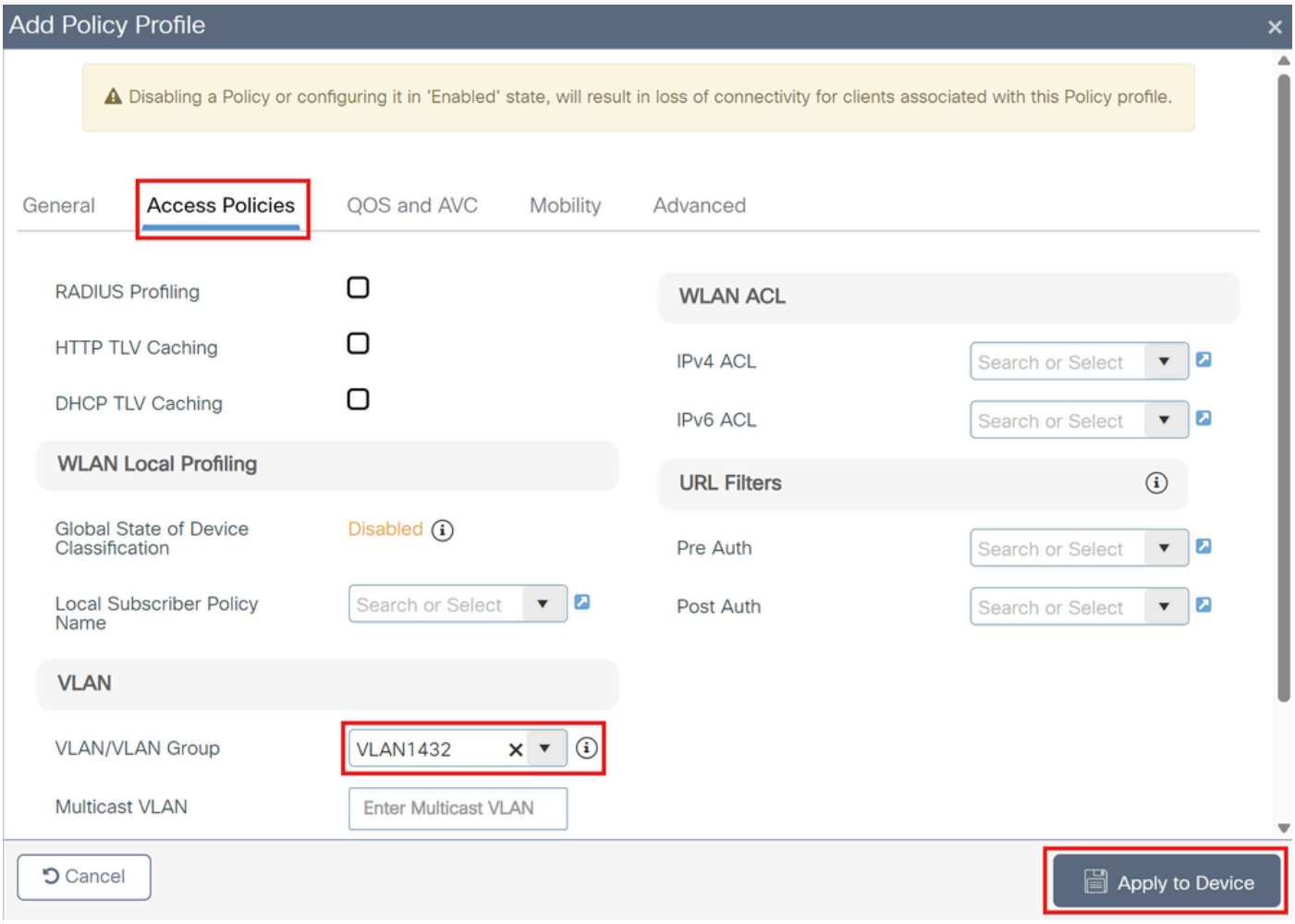
プロファイルを有効にします。



新しいポリシープロファイルの作成

ステップ 2：VLANを選択します。

[Access Policies] タブに移動し、ドロップダウンから VLAN 名を選択するか、VLAN-ID を手動で入力します。



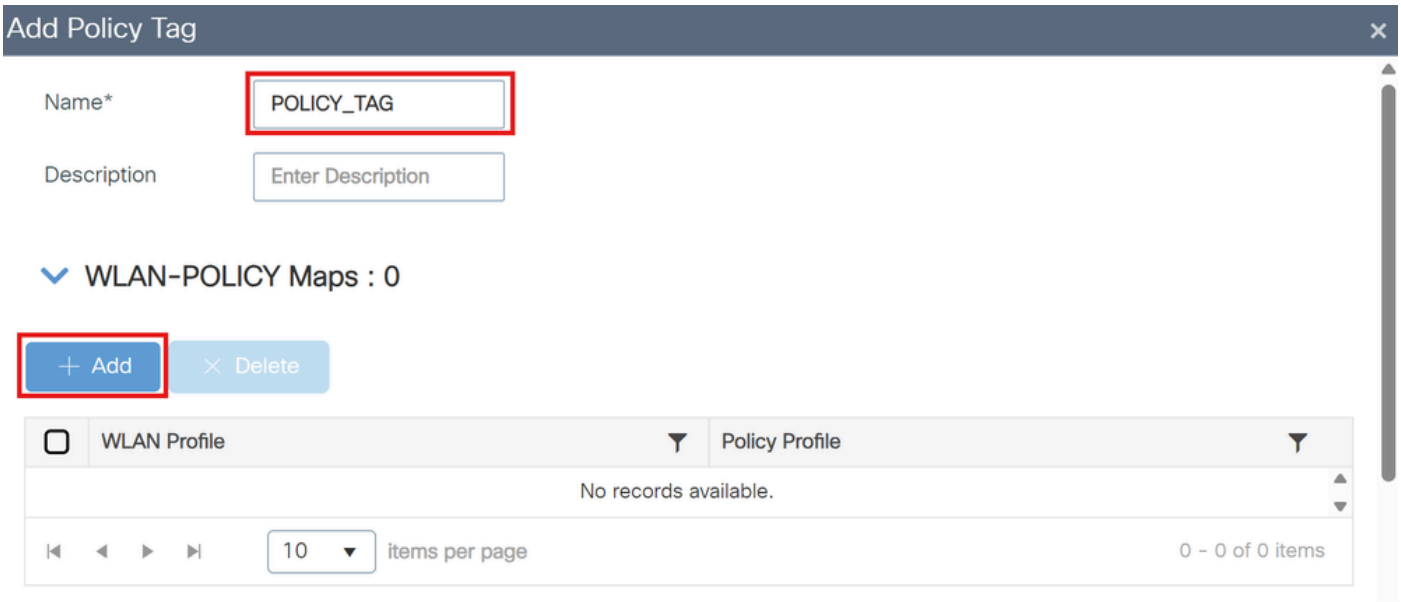
VLANの選択

ポリシータグの設定

ポリシータグで、SSID をポリシープロファイルにリンクします。新しいポリシータグを作成するか、default-policy タグを使用します。

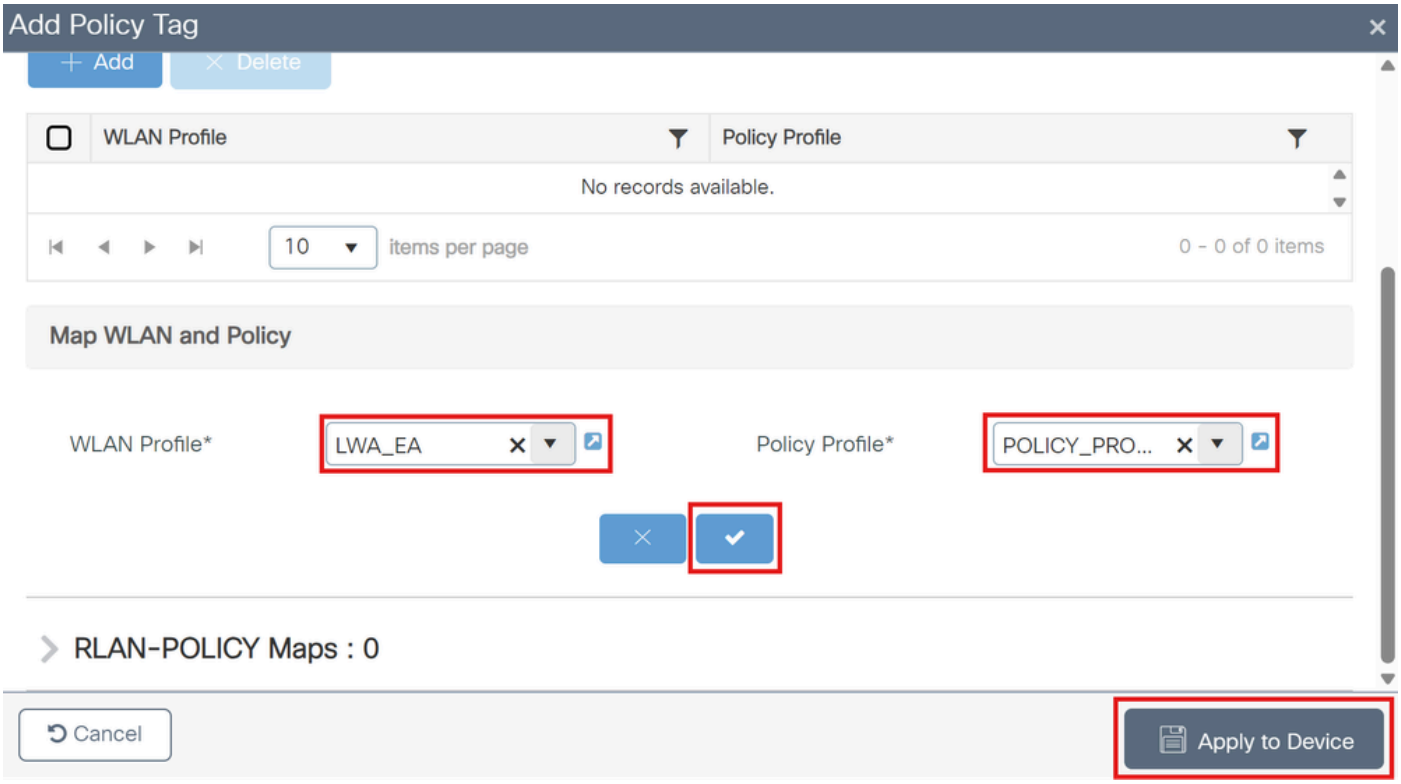
[Configuration] > [Tags & Profiles] > [Tags] > [Policy] に移動して、必要に応じて、図のように新しいタグを追加します。

+追加：



ポリシータグの設定

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。

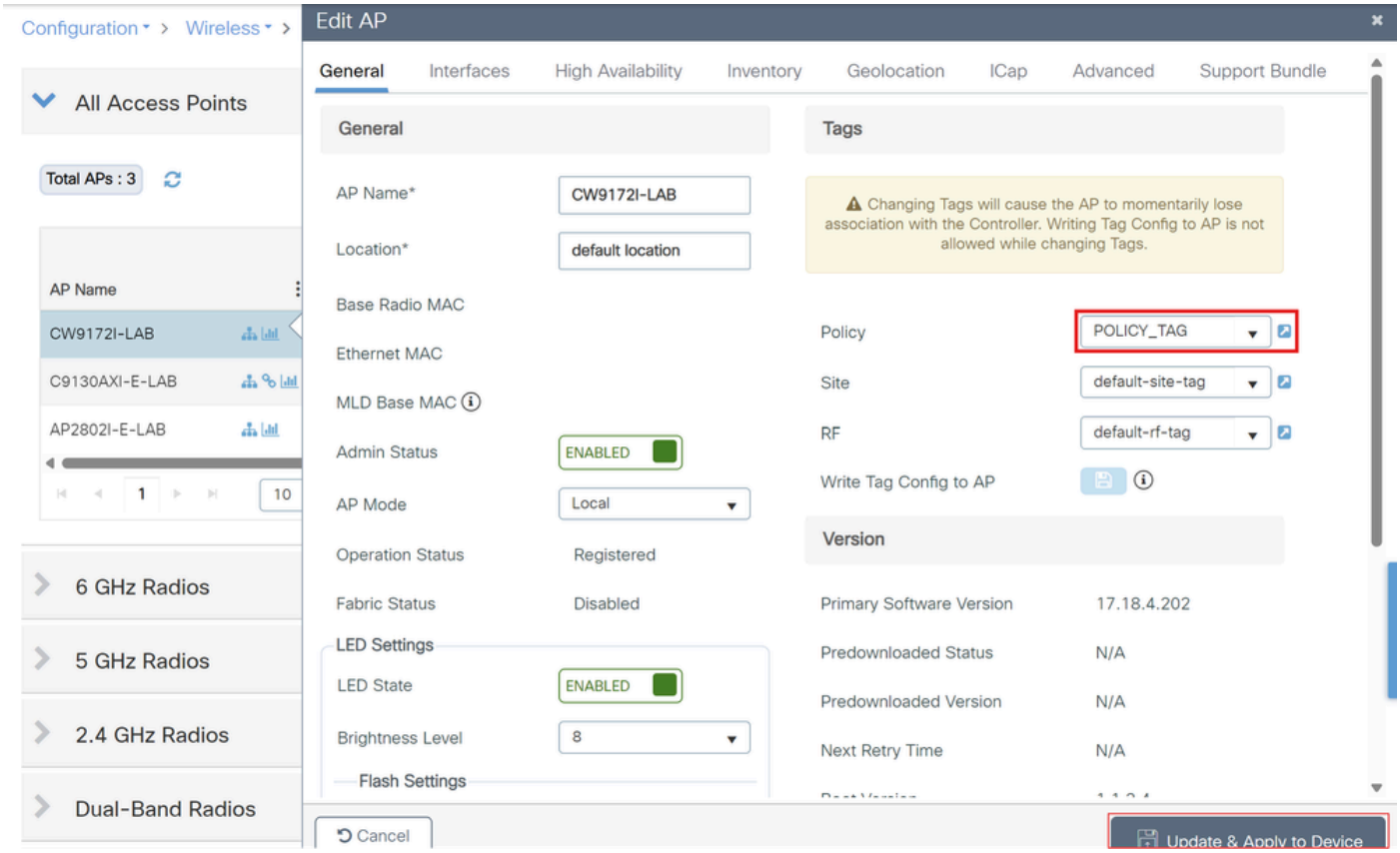


ポリシータグの設定

ポリシータグの割り当て

必要な AP にポリシータグを割り当てます。

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って、[Update & Apply to Device] をクリックします。

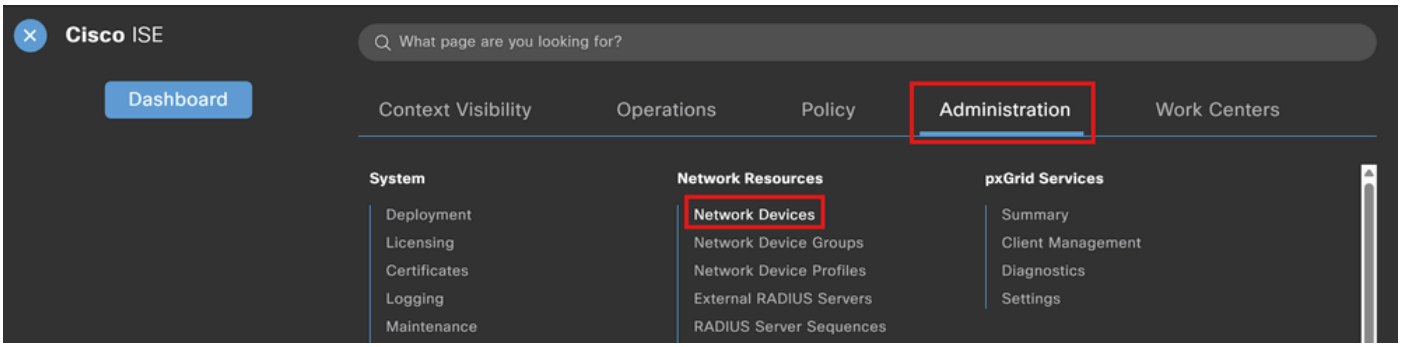


ポリシータグの割り当て

ISE の設定

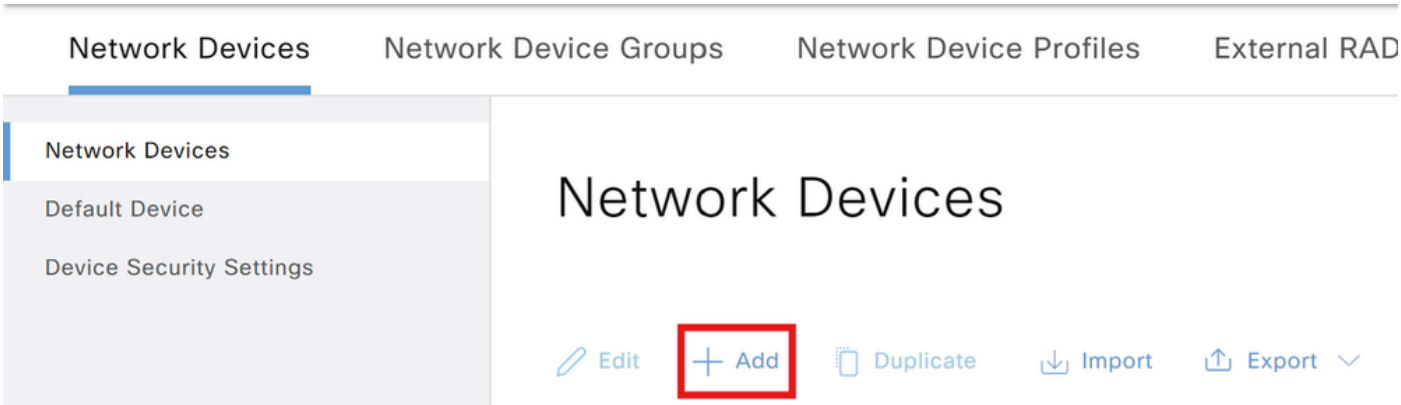
9800 WLC の ISE への追加

ステップ 1：図に示すように、Administration > Network Resources > Network Devicesの順に移動します。



9800 WLC の ISE への追加

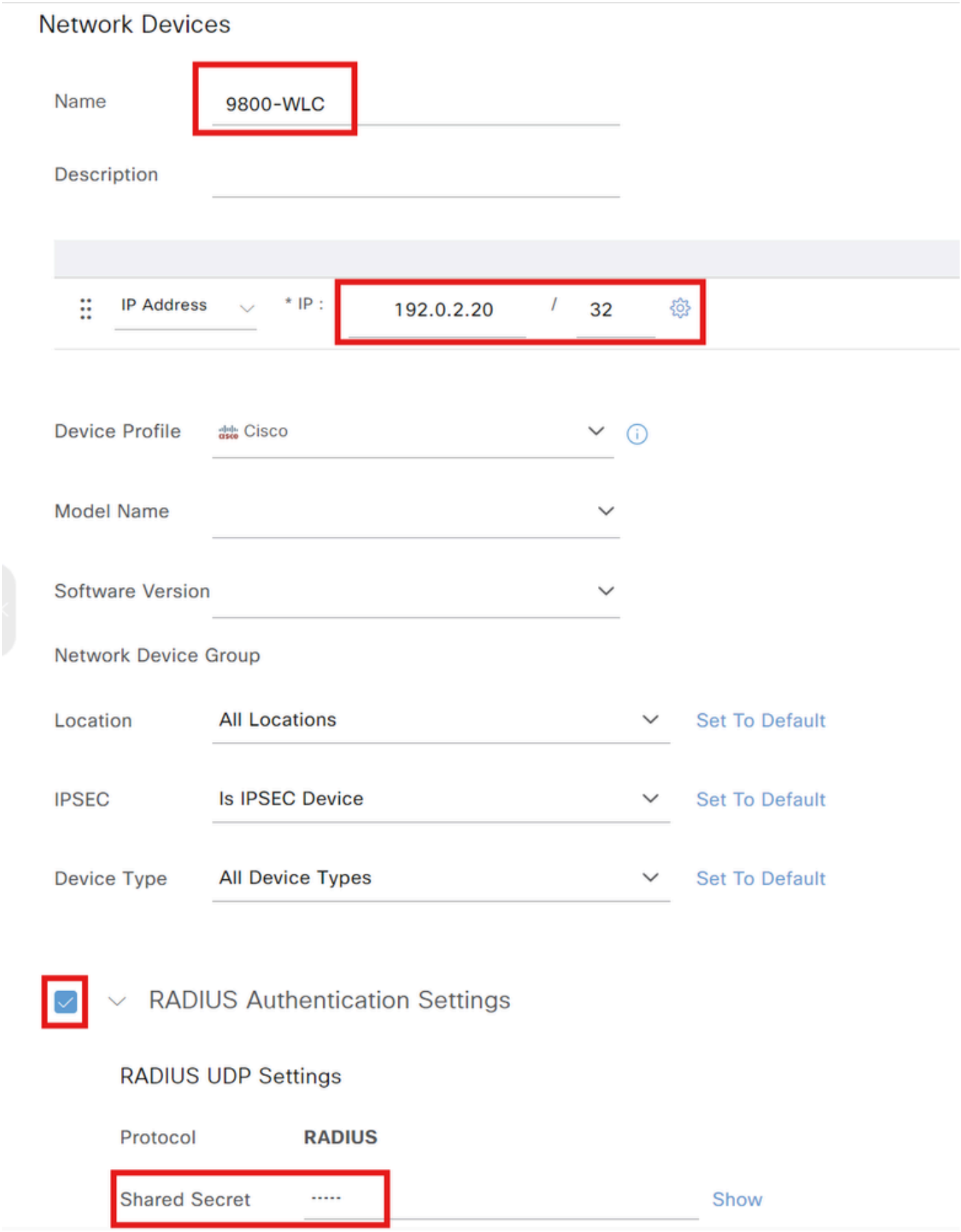
ステップ 2：+Addをクリックします。



ネットワークデバイスの追加

必要に応じてモデル名、ソフトウェアバージョン、説明を入力し、デバイスタイプ、場所、または WLC に基づいてネットワーク デバイス グループを割り当てることができます。

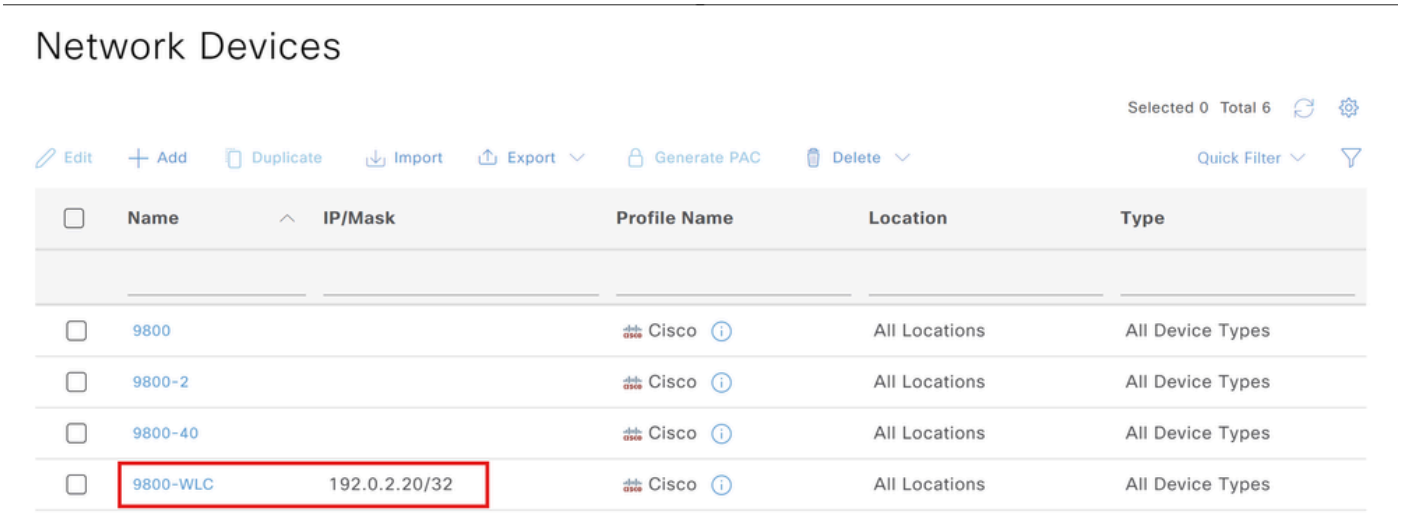
ステップ 3：図に示すように、9800 WLC設定を入力します。WLC側でサーバを作成するときに定義された同じRADIUSキーを入力します。次に、[Submit] をクリックします。



9800 WLCの設定

ステップ 4：Administration > Network Resources > Network Devicesの順に移動すると、ネット

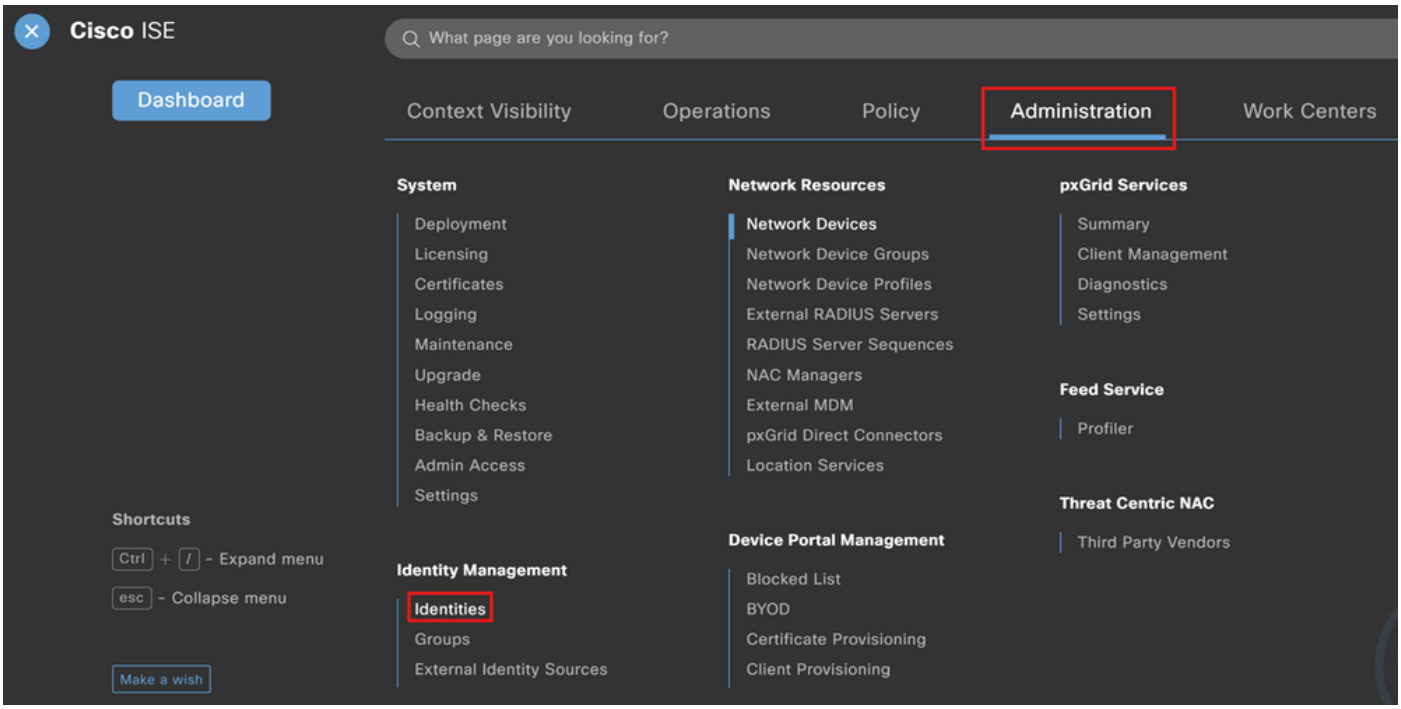
ワークデバイスのリストが表示されます。



ネットワークデバイスのリスト

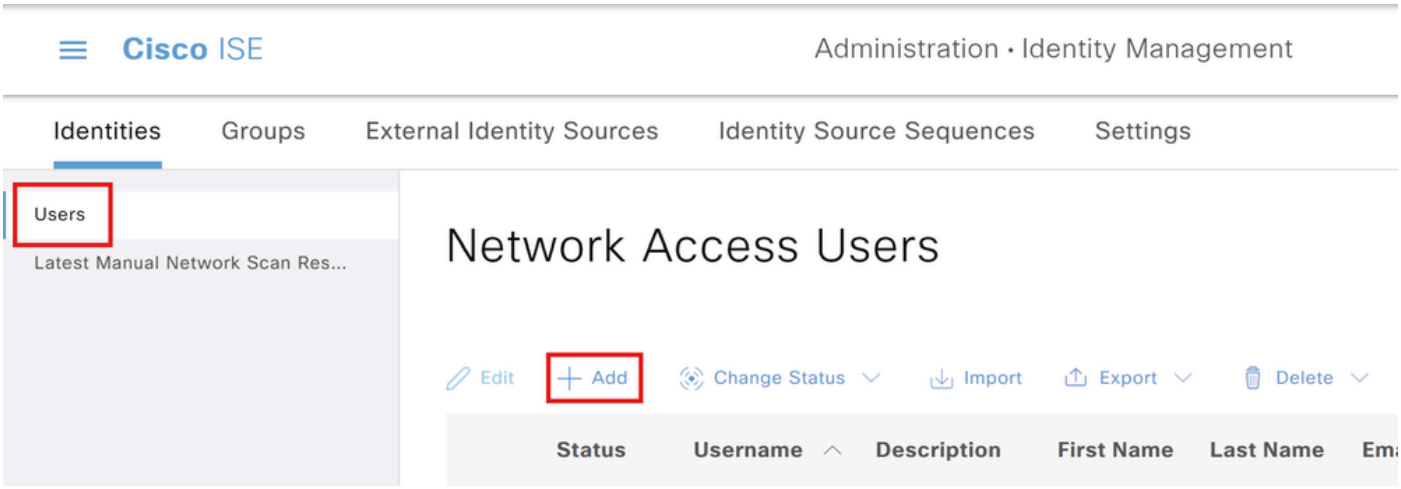
ISE での新しいユーザの作成

ステップ 1：Administration > Identity Management > Identitiesの順に移動します。



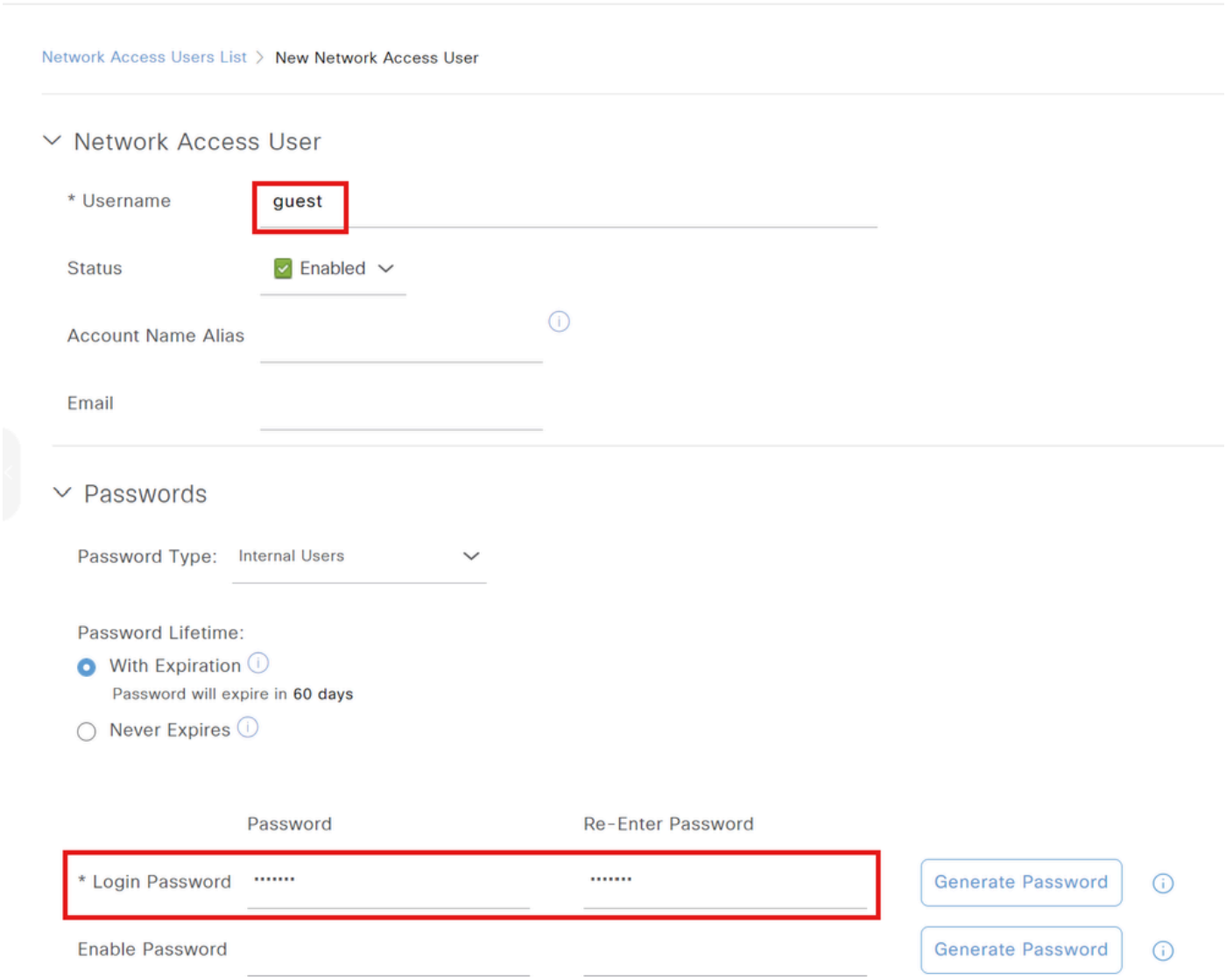
ISE管理：ID

ステップ 2： Usersに移動し、+Addをクリックします。



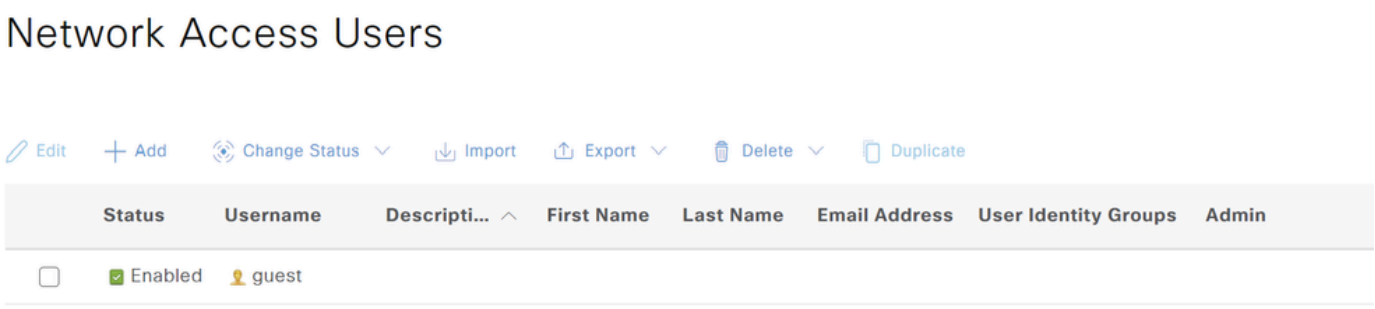
ユーザの追加

ステップ 3： ゲストユーザのユーザ名とパスワードを入力し、Submitをクリックします。



ISE での新しいユーザの作成

ステップ 4：Administration > Identity Management > Identities > Usersの順に移動すると、ユーザリストが表示されます。



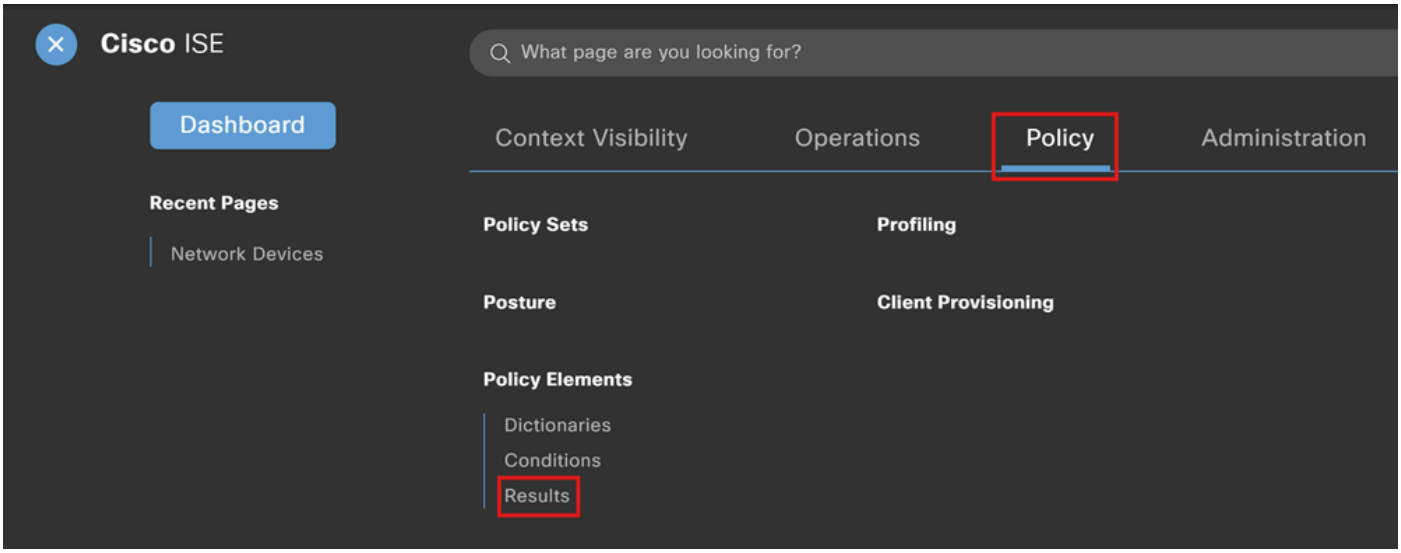
ネットワークアクセスユーザリスト

認証プロファイルの作成

ポリシープロファイルは、パラメータ（MAC アドレス、ログイン情報、使用される WLAN など）に基づいてクライアントに割り当てられる結果です。 仮想ローカルエリアネットワーク（VLAN）、アクセス制御リスト（ACL）、Uniform Resource Locator（URL）リダイレクトなどの特定の設定を割り当てることができます。

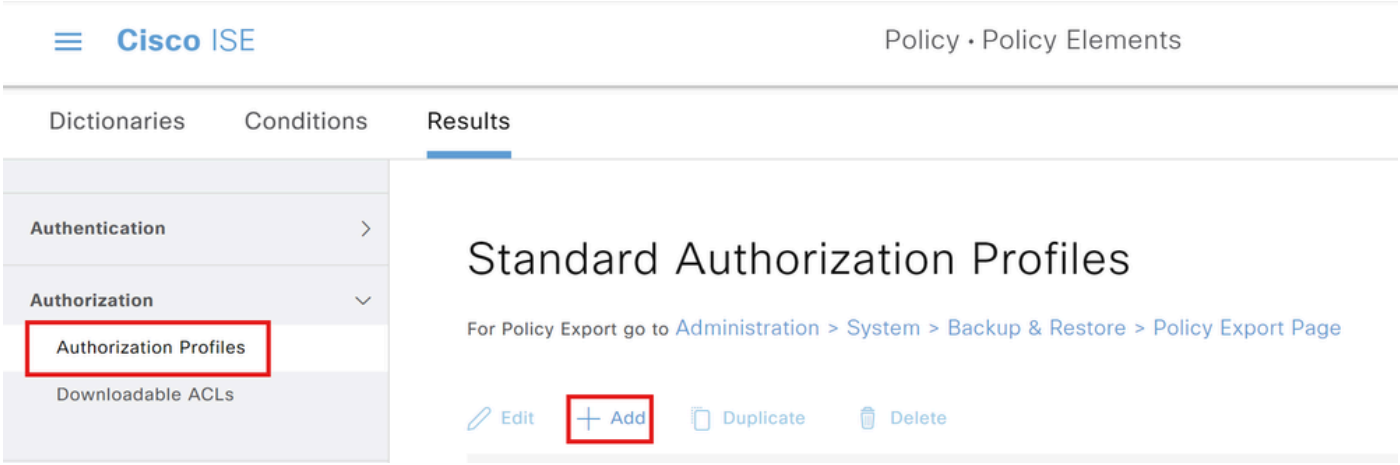
次の手順は、クライアントを認証ポータルにリダイレクトするために必要な認証プロファイルを作成する方法を示しています。ISE の最近のバージョンでは、Cisco_Webauth 許可の結果がすでに存在することに注意してください。WLC で設定したものと一致させるには、ここで編集して、リダイレクト ACL 名を変更します。

ステップ 1：Policy > Policy Elements > Resultsの順に移動します。



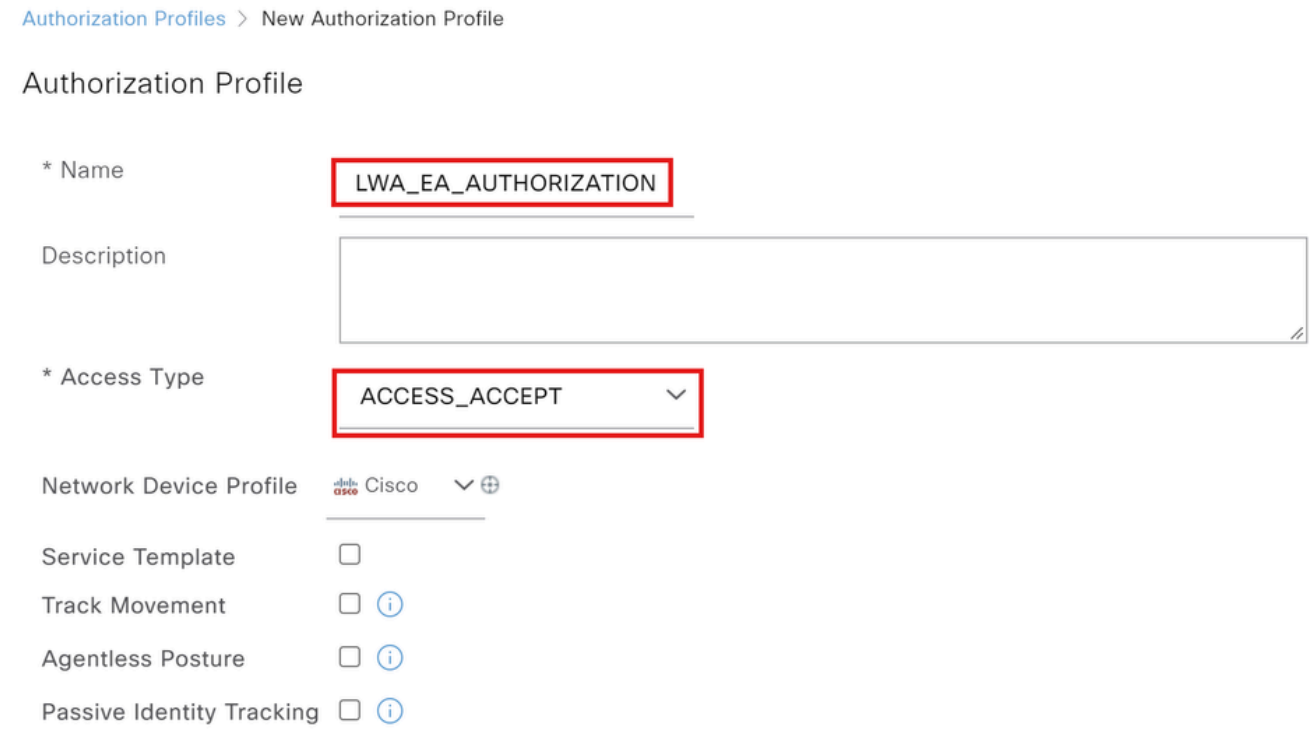
ISEポリシー：結果

ステップ 2： Authorization > Authorization Profilesの順に移動します。許可プロファイルを作成するには、+Addをクリックします。



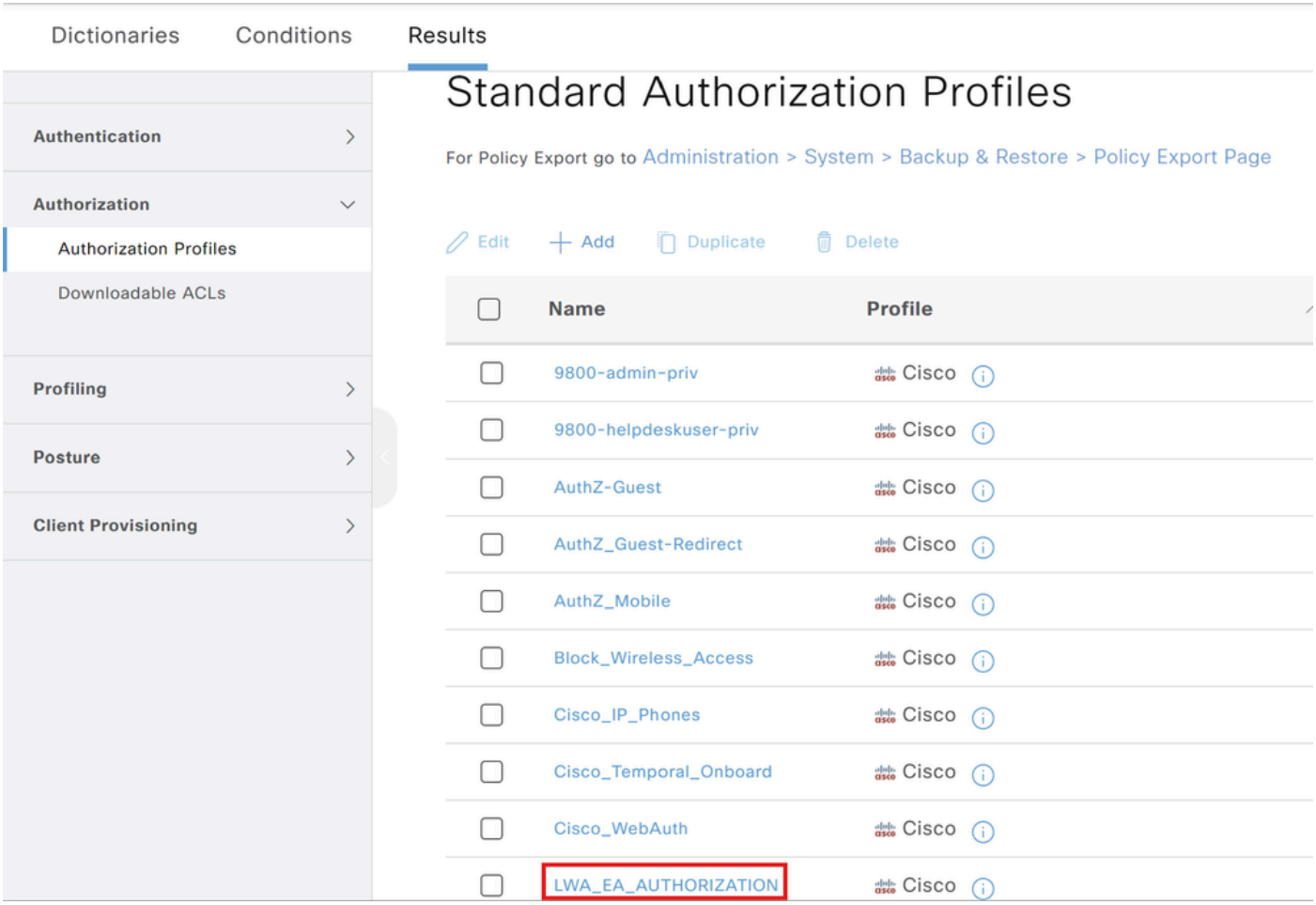
許可プロファイルの追加

ステップ 3：認可プロファイルLWA_EA_AUTHORIZATIONを作成します。属性の詳細は、Access Type=ACCESS_ACCEPTである必要があります。[Submit] をクリックします。



認証プロファイルの作成

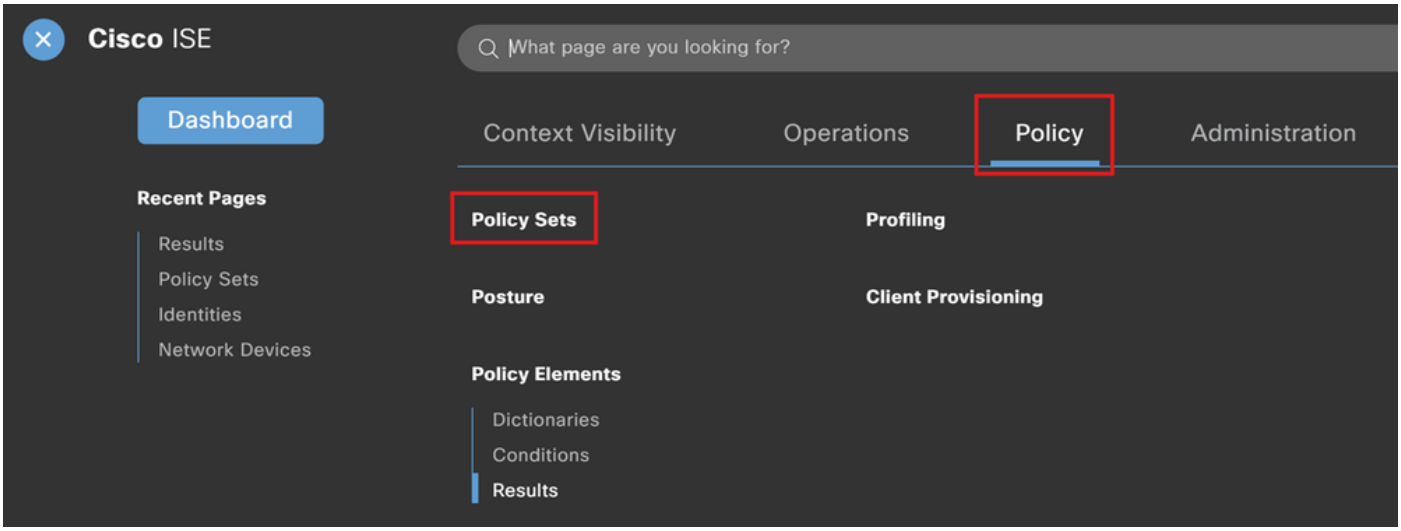
ステップ 4：Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に移動すると、認可プロファイルが表示されます。



許可プロファイルリスト

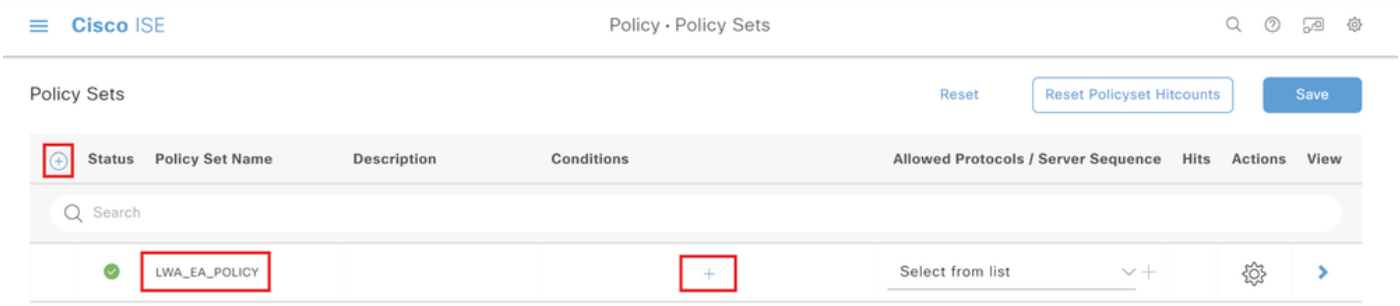
認証ルール（Authentication Rule）の設定

ステップ 1：Policy > Policy Setsの順に移動します。



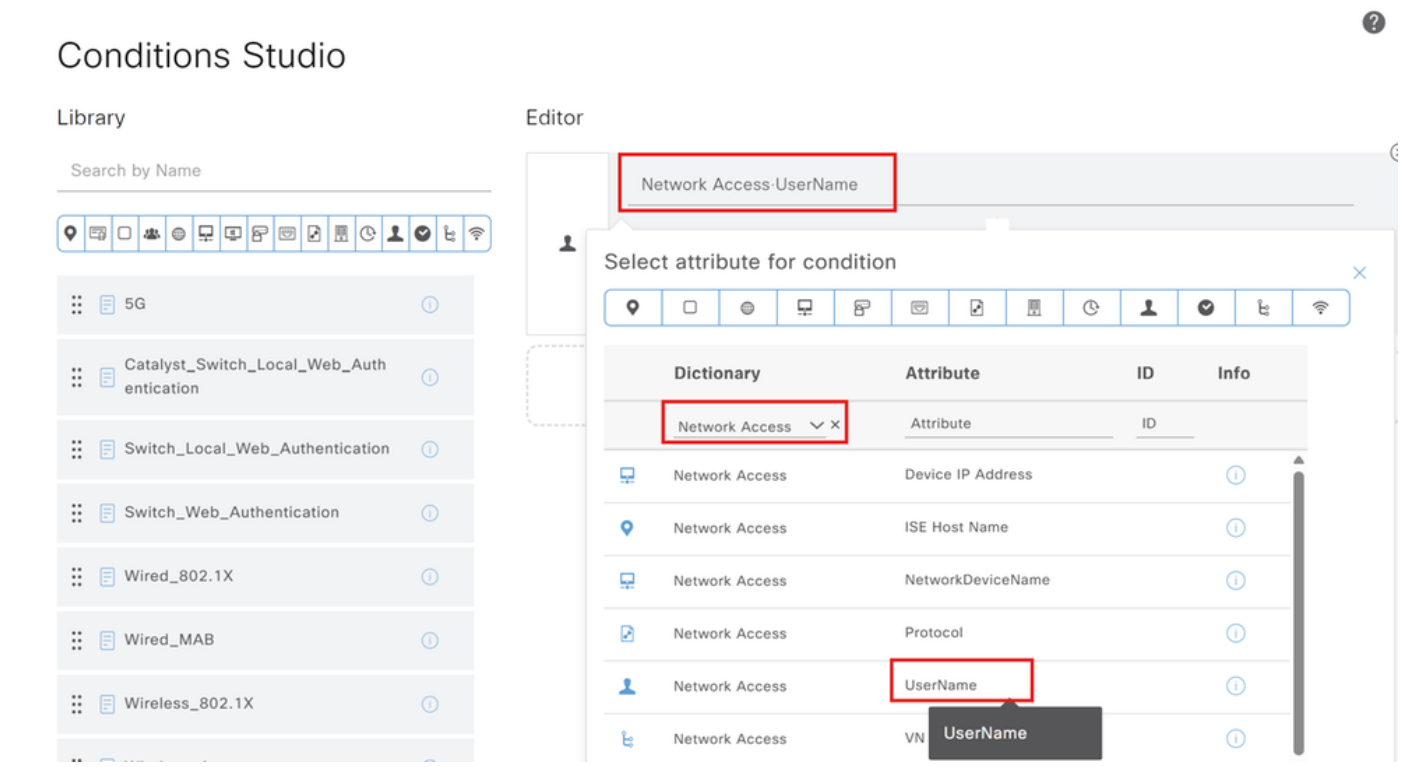
ISEポリシー：ポリシーセット

ステップ 2： +記号を選択し、ポリシーセットLWA_EA_POLICYの名前を入力します。 Conditions列をクリックします。



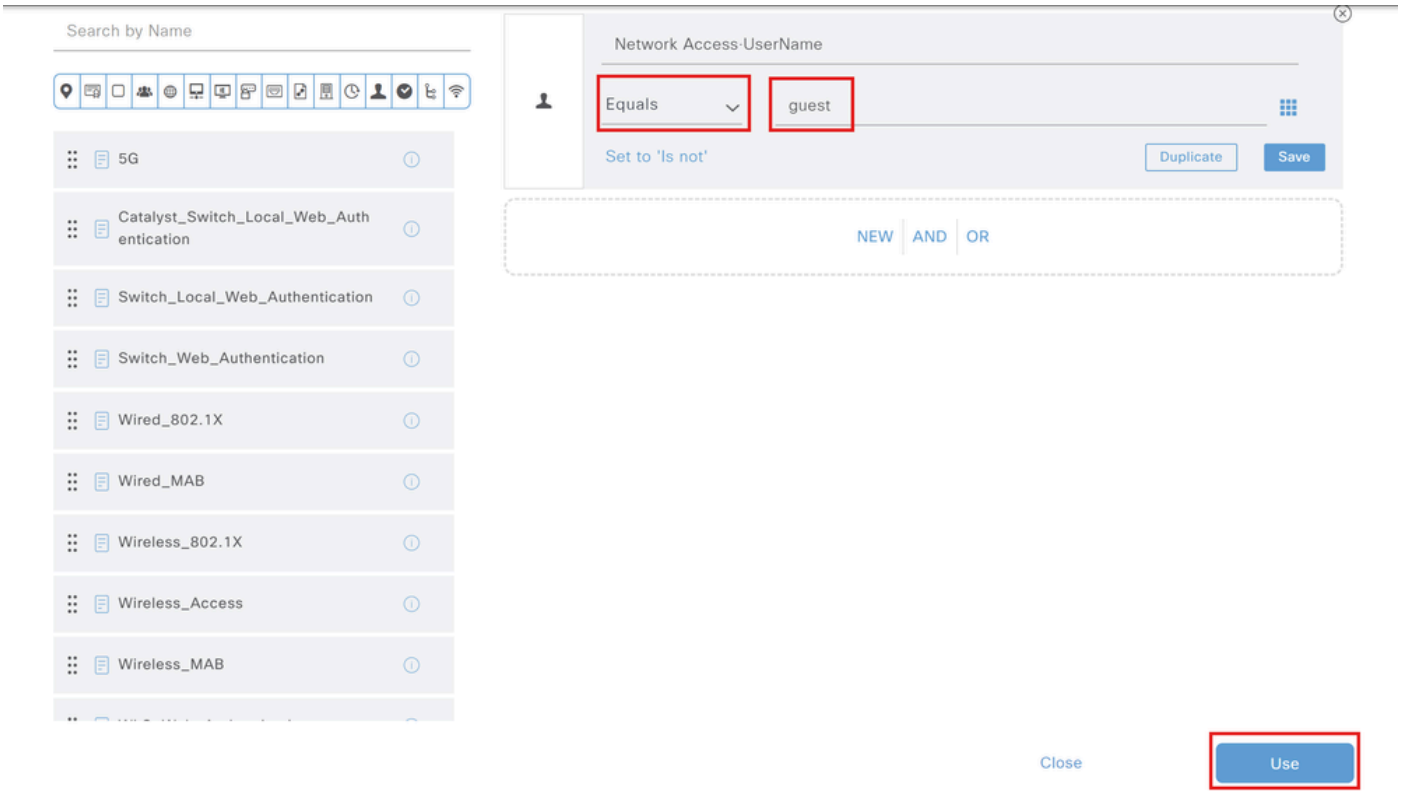
認証ルール（Authentication Rule）の設定

ステップ3:ディクショナリで、Network Accessを選択します。 Attributeで、Usernameを選択します。



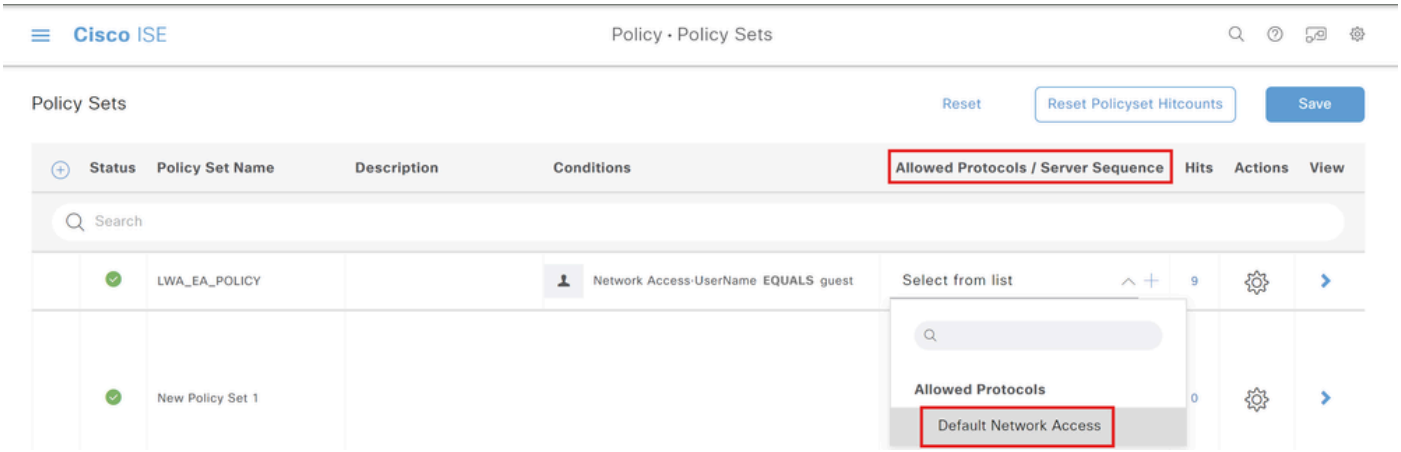
医学的なネットワークアクセス

ステップ 4：Equalsを設定し、テキストボックスにguest（Administration > Identity Management > Identities > Usersで定義されたユーザ名）と入力します。 [Save] をクリックして変更を保存します。



ユーザ名Guest

ステップ 5：Policy > Policy Setsの順に移動します。作成したポリシーセットのAllowed Protocols/Server Sequence列で、Default Network Accessを選択します。



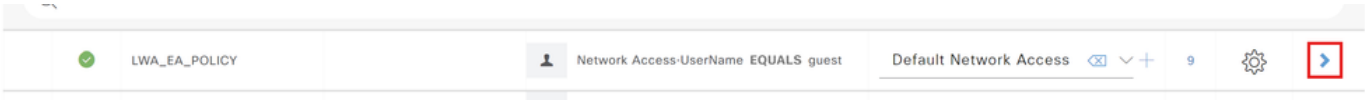
ポリシー セット

手順 6：[Save] をクリックして変更を保存します。

許可ルール（Authorization Rule）の設定

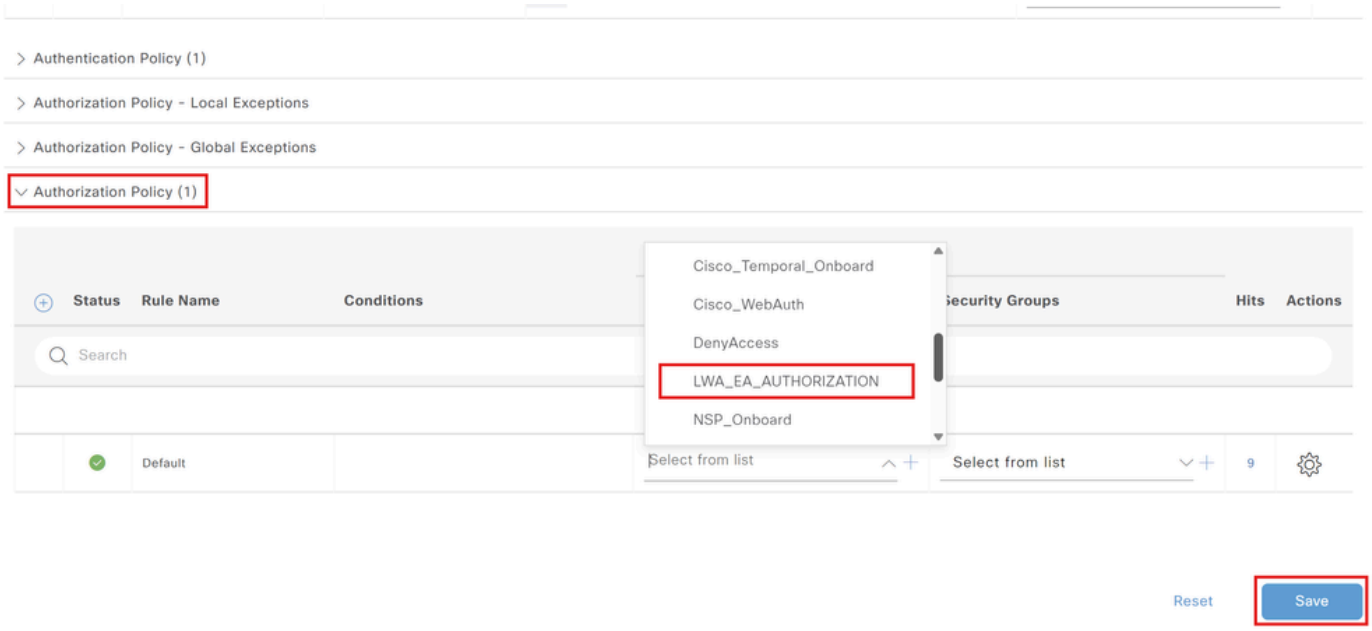
許可ルールは、クライアントに適用される許可（認証プロファイル）の結果を決定するためのものです。

ステップ 1：Policy > Policy Setsの順に移動します。作成したポリシーセットの矢印アイコンをクリックします。



ポリシーセット矢印

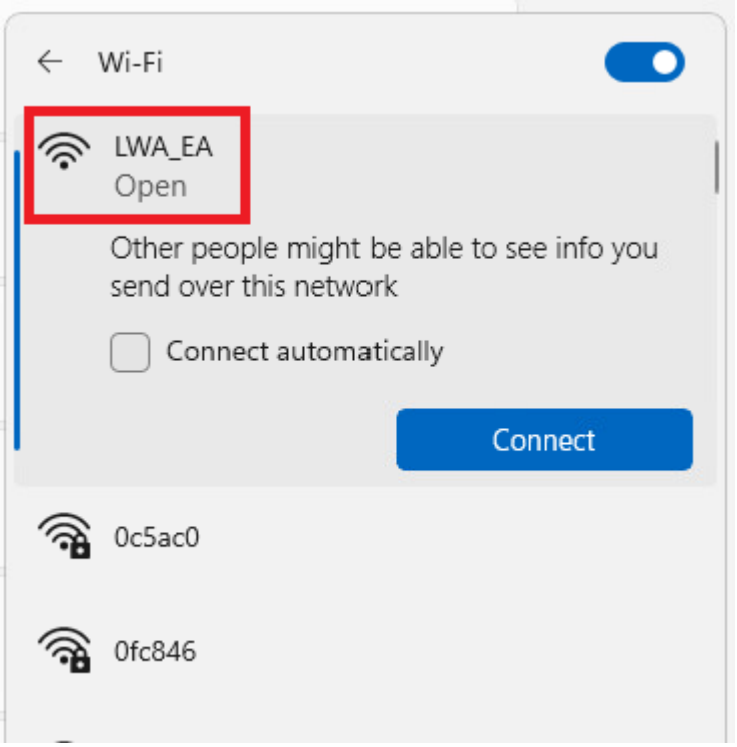
ステップ 2：同じPolicy Setページで、図に示すようにAuthorization Policyを展開します。Profiles列でDenyAccessを削除し、LWA_EA_AUTHORIZATIONを追加します。 [Save] をクリックして変更を保存します。



認可ポリシー

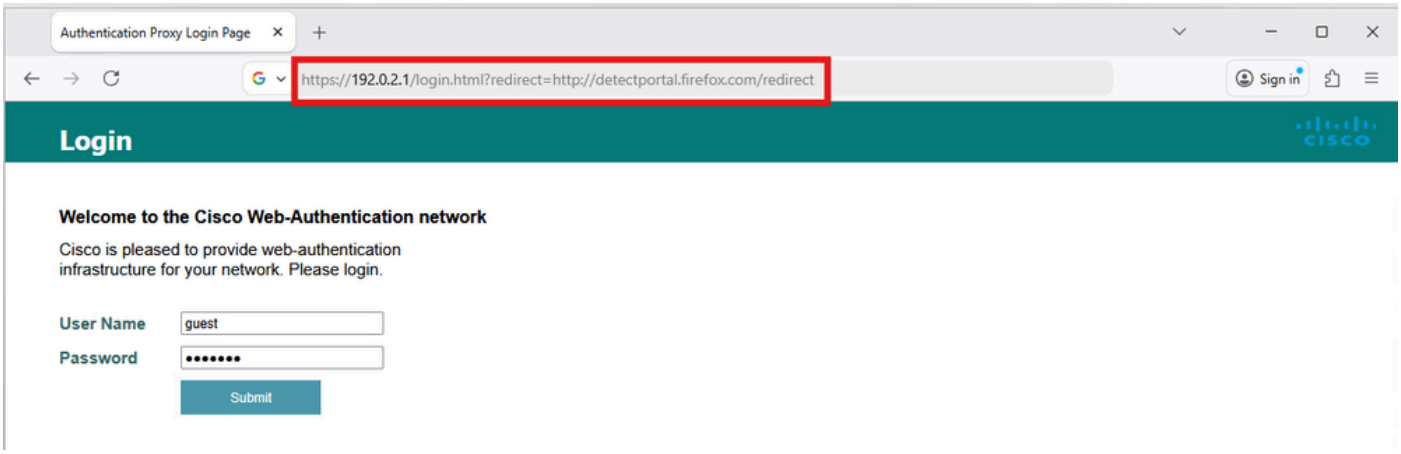
ゲストクライアント接続

ステップ 1：コンピュータまたは電話機で、Wi-Fiネットワークに移動し、SSID LWA_EAを見つけて、Connectを選択します。



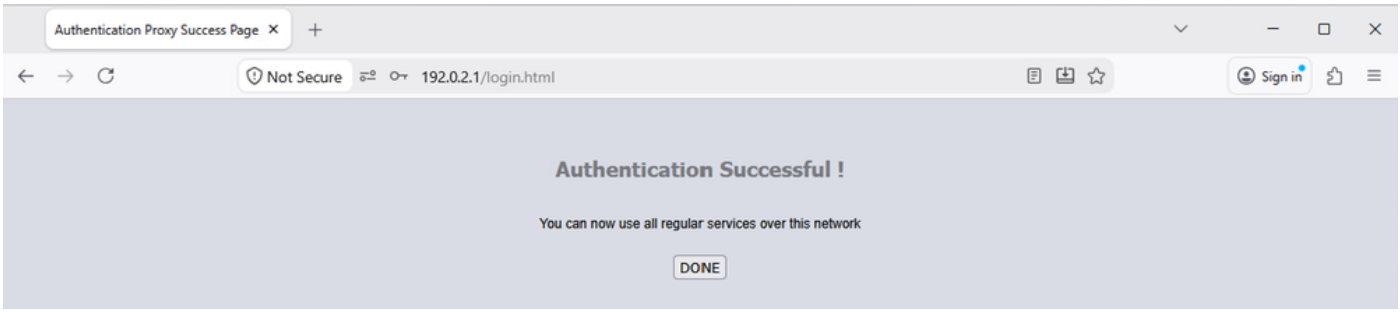
ゲストクライアント接続

ステップ 2：ブラウザウィンドウが表示され、ログインページが表示されます。リダイレクトURLはURLボックス内にあり、ネットワークにアクセスするにはユーザ名とパスワードを入力する必要があります。次にSubmitを選択します。



リダイレクトURLを使用したログインページ

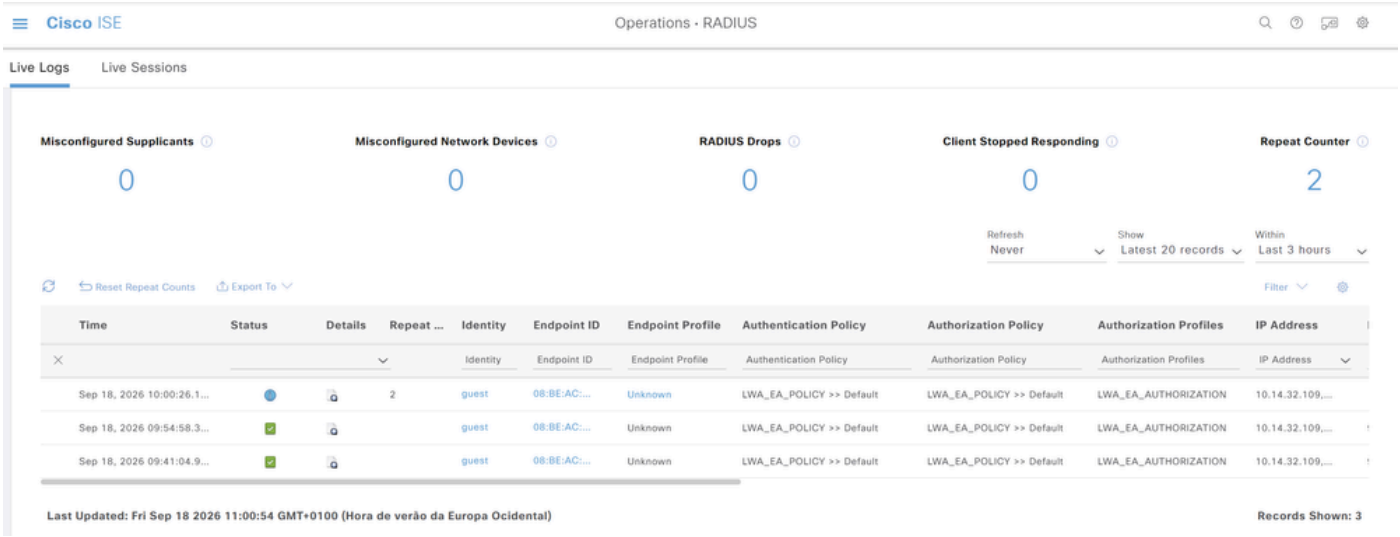
クレデンシャルが正しければ、認証が成功したことを示すページが表示されます。



Authentication Successful Loginページ

注：表示されたURLはWLCによって提供されたものです。これには、WLC仮想IP(VIP)と、Windows接続テストURLのリダイレクトが含まれます。

ステップ 3：Operations > RADIUS > Live Logsの順に移動します。認証されたクライアントデバイスと、その認証および認可ポリシーを確認できます。



RADIUS ライブ ログ

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。

show wlan summary

<#root>

9800WLC#show wlan summary

```
Number of WLANs: 1
```

```
ID Profile Name SSID Status 2.4GHz/5GHz Security
-----------------------------------------------
```

1 LWA_EA LWA_EA UP [open],[Web Auth]

```
9800WLC#
```

show wlan name LWA_EA

```
WLAN Profile Name : LWA_EA
==========================================
Identifier : 1
Description :
Network Name (SSID) : LWA_EA
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
(...)
Accounting list name :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security
```

Web Based Authentication : Enabled

```
OWE Transition Mode : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
```

Webauth Authentication List Name : LWA_AUTHENTICATION

Webauth Authorization List Name : Disabled

Webauth Parameter Map : global

```
(...)
Security-2.4GHz/5GHz
```

802.11 Authentication : Open System

```
Static WEP Keys : Disabled
```

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

```
OSEN : Disabled
PMF Support : Disabled
(...)
Band Select : Disabled
Load Balancing : Disabled
(...)
```

パラメータマップ設定の表示

9800WLC#show running-config | section parameter-map type webauth global

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
trustpoint TP-self-signed-123456
```

AAA情報の表示

<#root>

9800WLC#show aaa method-lists authentication

```
authen queue=AAA_ML_AUTHEN_LOGIN

name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP


authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
(...)
```

9800WLC#show aaa method-lists authorization

```
author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET

name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP


author queue=AAA_ML_AUTHOR_CONN
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
(...)
```

9800WLC#show aaa servers

```
RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS


State: current UP, duration 8421s, previous duration 0s
Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 8421s, previous duration 0s
SMD Platform Dead: total time 0s, count 0
Platform State from WNCD (0) : current UP
(...)
```

トラブルシューティング

一般的な問題

Web認証の問題をトラブルシューティングする方法に関する次のようなガイドがあります。

- ユーザが認証できない。
- 証明書の問題。
- リダイレクトURLが機能しません。
- ゲストユーザはゲストWLANに接続できません。
- ユーザがIPアドレスを取得できない。
- Web認証ログインページへのリダイレクトが失敗します。
- 認証に成功した後、ゲストユーザはインターネットにアクセスできません。

次のガイドは、トラブルシューティングの手順の詳細を説明しています。

- Web認証の一般的な問題のトラブルシューティング
- トラブルシューティングを行うその他の状況

条件付きデバッグ、無線アクティブトレース、および組み込みパケットキャプチャ

条件付きデバッグを有効にして、無線アクティブ(RA)トレースのキャプチャを実行できます。これにより、指定した条件と対話するすべてのプロセス (この場合はクライアントMACアドレス) に対してデバッグレベルのトレースが提供されます。 条件付きデバッグを有効化するには、ガイド「条件付きデバッグおよびRadioActiveトレース」の手順を使用します。

Embedded Packet Capture(EPC)も収集できます。 EPCは、Catalyst 9800 WLCを送受信するパケット、つまりLWA内のDHCP、DNS、HTTP GETパケットを表示できるパケットキャプチャ機能です。これらのキャプチャは、Wireshark によるオフライン分析のために工クスポートできま

す。これを行う方法の詳細な手順については、「組み込みパケットキャプチャ」を参照してください。

成功した試行の例

これは、RADIUSサーバのゲストSSIDに接続しているときに、関連付け/認証プロセスの各フェーズの識別に成功した試行に対するRA_tracesからの出力です。

802.11アソシエーション/認証：

[client-orch-sm] [17062]: （注）: MAC: 08be.ac3fアソシエーションを受信しました。BSSID cc70.edcf.552f、WLAN LWA_EA、スロット1 AP 2ce3.8eb4、CW9172I-LAB
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Dot11関連付け要求を受信しました。処理が開始されました。SSID:LWA_EA、ポリシープロファイル：POLICY_PROFILE、AP名：CW9172I-LAB、AP MACアドレス：2ce3.8eb4BSSID MAC0000.0000.0000wlan ID:1RSSI:-49、SNR:46
[client-orch-state] [17062]: （注）:MAC:08be.ac3fクライアント状態遷移：S_CO_INIT -> S_CO_ASSOCIATING
[dot11-validate] [17062]: (info): MAC: 08be.ac3f Dot11 ie validate ext/supp rates.サポートされているレートradio_type 2の検証に合格しました
[dot11-validate] [17062]: (info): MAC: 08be.ac3f WiFi direct: Dot11 validate P2P IE.P2P IEが存在しません。
[dot11] [17062]: （デバッグ）: MAC: 08be.ac3f dot11が関連付け応答を送信します。resp_status_codeを使用したフレーミング関連付け応答： 0
[dot11] [17062]: （デバッグ）: MAC: 08be.ac3f Dot11機能情報byte1 1, byte2: 11
[dot11-frame] [17062]: （情報）: MAC: 08be.ac3f WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
[dot11] [17062]: （情報）: MAC: 08be.ac3f dot11が関連付け応答を送信します。resp_status_code:0、DOT11_STATUS:DOT11_STATUS_SUCCESSで長さ130のアソシエーション応答を送信しています
[dot11] [17062]: （注）: MAC: 08be.ac3f Association success.AID 1、ローミング= False、WGB = False、11r = False、11w = False高速ローミング= False
[dot11] [17062]: （情報）: MAC: 08be.ac3f DOT11状態遷移： S_DOT11_INIT -> S_DOT11_ASSOCIATED
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Station Dot11 association is successful.

IP学習プロセス：

[client-orch-state] [17062]: （注）: MAC: 08be.ac3fクライアント状態遷移：S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [17062]: （情報）: MAC: 08be.ac3f IP学習状態遷移： S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
[client-auth] [17062]: （情報）: MAC: 08be.ac3fクライアント認証インターフェイスの状態遷移：S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
[client-iplearn] [17062]: （注）: MAC: 08be.ac3fクライアントIP学習が成功しました。方法：DHCP IP:10.14.32.109
[client-iplearn] [17062]: （情報）: MAC: 08be.ac3f IP学習状態遷移： S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f受信ip learn response. method: IPLEARN_METHOD_DHCP

レイヤ3認証：

[client-orch-sm] [17062]: （デバッグ）: MAC: 08be.ac3fがL3認証をトリガーしました。ステータス= 0x0、成功
[client-orch-state] [17062]: （注）: MAC: 08be.ac3fクライアント状態遷移：

S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
[client-auth] [17062]: （注）: MAC: 08be.ac3f L3認証が開始されました。LWA
[client-auth] [17062]: （情報）: MAC: 08be.ac3fクライアント認証インターフェイスの状態遷移：S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[webauth-httpd] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]LOGIN状態のときにrcvdを取得する
[webauth-httpd] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]HTTP GET要求
[webauth-httpd] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]Parse GET, src [10.14.32.109] dst [10.107.221.82] url [http://firefox detect portal/]
[webauth-httpd] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]読み取り完了：parse_request return 8
[webauth-io] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO状態READING ->書き込み
[webauth-io] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO状態WRITING ->読み取り
[webauth-io] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO状態NEW ->読み取り
[webauth-io] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]56539/218イベントを読み取り、メッセージ準備完了
[webauth-httpd] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]LOGIN状態でのPOST rcvd

レイヤ3認証に成功しました。クライアントをRUN状態に移行します。

[auth-mgr] [17062]: （情報）: [08be.ac3f:capwap_90000004]クライアント08be.ac3fのUser-Name guestを受信しました
[auth-mgr] [17062]: （情報）: [08be.ac3f:capwap_90000004] attr auth-domain(954)に対するauth mgr attr add/change通知を受信しました
[auth-mgr] [17062]: （情報）: [08be.ac3f:capwap_90000004] Method webauth changing state from 'Running'から'Authc Success'
[auth-mgr] [17062]: （情報）: [08be.ac3f:capwap_90000004]コンテキストの状態が'Running'から'Authc Success'に変更されました
[auth-mgr] [17062]: （情報）: [08be.ac3f:capwap_90000004] attr add/change通知がattrメソッドに対して受信されました(757)
[auth-mgr] [17062]: （情報）: [08be.ac3f:capwap_90000004]発生イベントAUTHZ_SUCCESS (11)
[auth-mgr] [17062]: （情報）: [08be.ac3f:capwap_90000004]コンテキストの状態が'Authc Success'から'Authz Success'に変更されました
[webauth-acl] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]SVM経由でIPv4ログアウトACLを適用しています。名前：IP-Adm-V4-LOGOUT-ACL、プライオリティ：51、IIF-ID:0
[webauth-sess] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]使用するパラメータマップ：グローバル
[webauth-state] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]使用するパラメータマップ：グローバル
[webauth-state] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]State AUTHC_SUCCESS -> AUTHZ
[webauth-page] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]Webauth成功ページの送信
[webauth-io] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO状態AUTHENTICATING ->書き込み
[webauth-io] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO state WRITING ->終了

[webauth-httpd] [17062]: （情報）: capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO ctxを削除し、ソケットを閉じます。id [99000029]
[client-auth] [17062]: （注）: MAC: 08be.ac3f L3 Authentication Successful.ACL:[]
[client-auth] [17062]: （情報）: MAC: 08be.ac3fクライアント認証インターフェイスの状態遷移：S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
[webauth-httpd] [17062]: （情報）: capwap_90000004[08be.ac3f][10.48.39.243]56538/219 Remove IO ctx and close socket, id [D7000028]
[errmsg] [17062]: （情報）: %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: MACが08be.ac3fのデバイスのssid (LWA_EA)に参加しているユーザー名エントリ(guest)
[aaa-attr-inf] [17062]: （情報）: [適用属性：bsn-vlan-interface-name 0 "VLAN0039"]
[aaa-attr-inf] [17062]: （情報）: [適用属性：タイムアウト0 1800 (0x708)]
[aaa-attr-inf] [17062]: （情報）: [適用属性： url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]
[ewlc-qos-client] [17062]: （情報）: MAC: 08be.ac3fクライアントQoS実行状態ハンドラ
[rog-proxy-capwap] [17062]: （デバッグ）：マネージドクライアントRUN状態通知： 08be.ac3f
[client-orch-state] [17062]: （注）: MAC: 08be.ac3fクライアント状態遷移：S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

関連情報

- シスコのテクニカルサポートとダウンロード

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。