ISEを使用したCatalyst 9800 WLC iPSKの設定

内容

概要

このドキュメントでは、Cisco ISEをRADIUSサーバとして使用するCisco 9800ワイヤレスLANコントローラ(WLC)でのiPSKで保護されたWLANの設定について説明します。

前提条件

要件

このドキュメントでは、読者が9800上のWLANの基本設定に精通し、その設定を導入に適応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

- 17.6.3が稼働するCisco 9800-CL WLC
- Cisco ISE 3.0

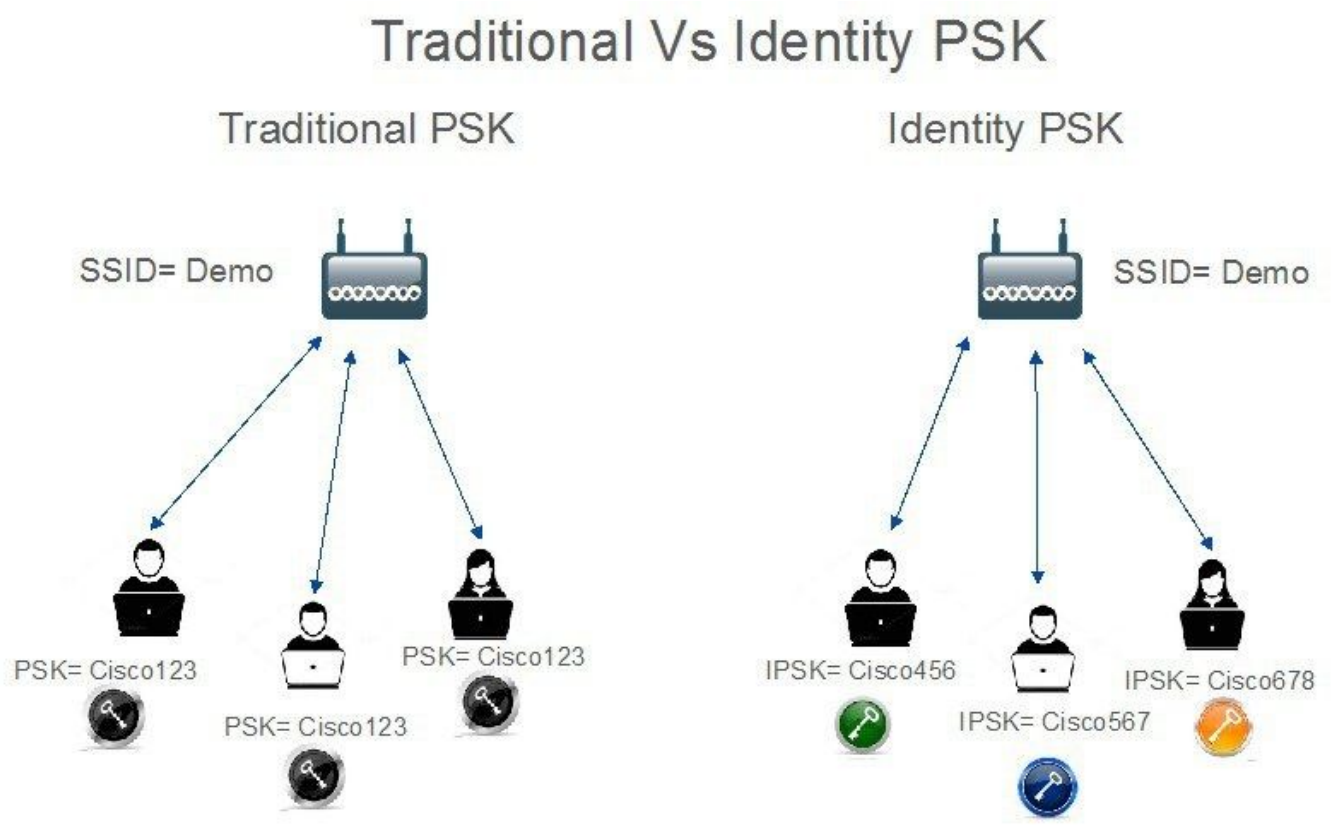
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

iPSKとは何か、どのシナリオに適合するかを理解する

従来の事前共有キー(PSK)で保護されたネットワークでは、接続されたすべてのクライアントに同じパスワードが使用されます。その結果、不正ユーザとキーを共有することで、セキュリティ違反やネットワークへの不正アクセスが発生する可能性があります。この侵害の最も一般的な緩和策は、PSK自体の変更です。この変更は、ネットワークに再びアクセスするために多くのエンドデバイスを新しいキーで更新する必要があるため、すべてのユーザに影響を与えます。

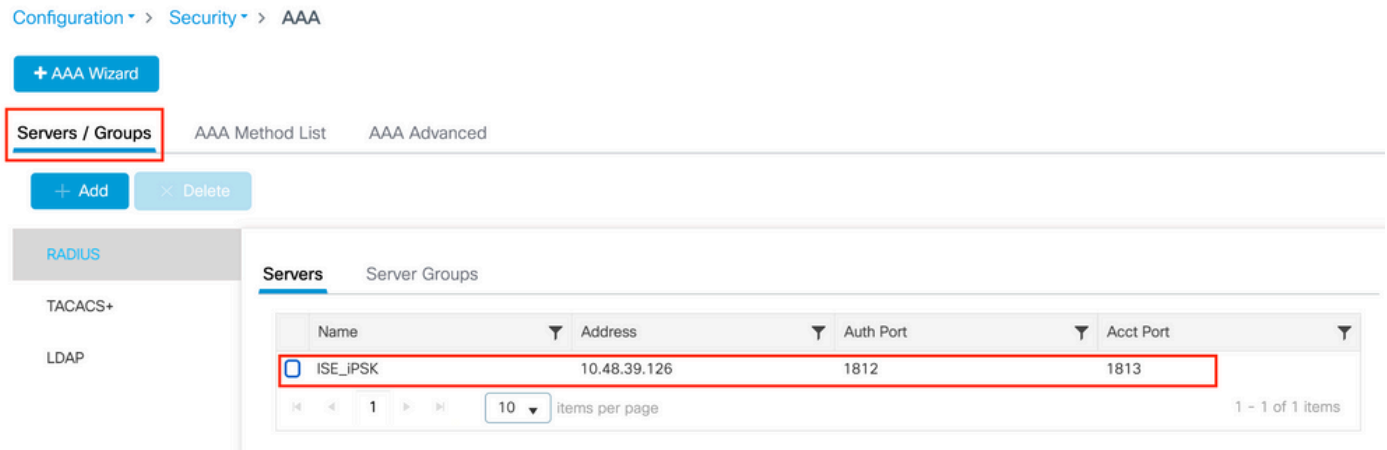
Identity PSK(iPSK)では、RADIUSサーバを使用して、同じSSID上の個人またはユーザグループに

対して一意の事前共有キーが作成されます。この種の設定は、エンドクライアントデバイスがdot1x認証をサポートしないが、よりセキュアで詳細な認証方式が必要なネットワークで非常に便利です。クライアントの観点からは、このWLANは従来のPSKネットワークと同じように見えます。いずれかのPSKが侵害された場合、影響を受ける個人またはグループだけがPSKを更新する必要があります。WLANに接続されている残りのデバイスは影響を受けません。

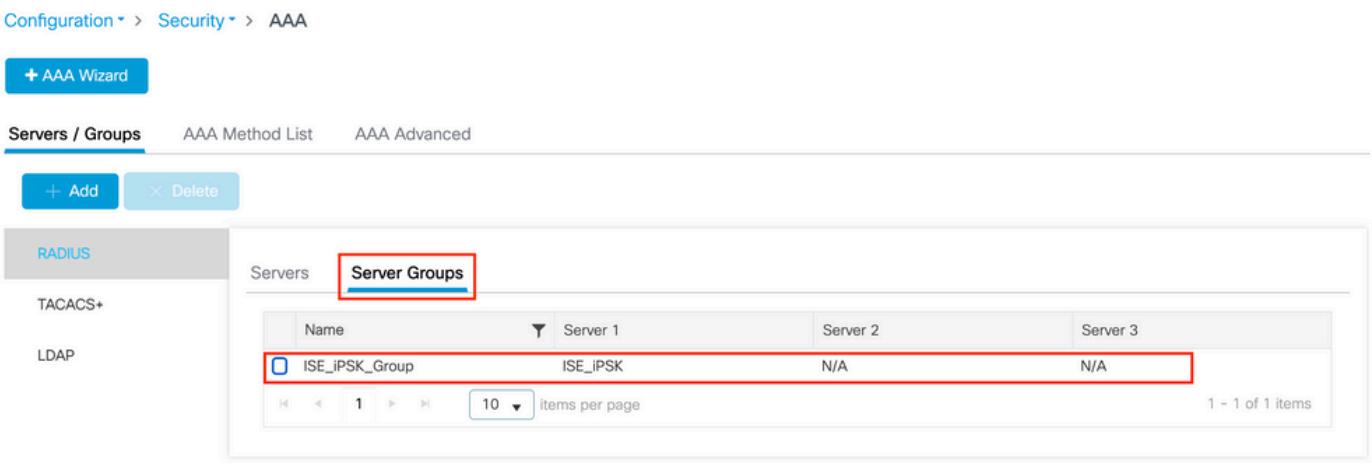


9800 WLCの設定

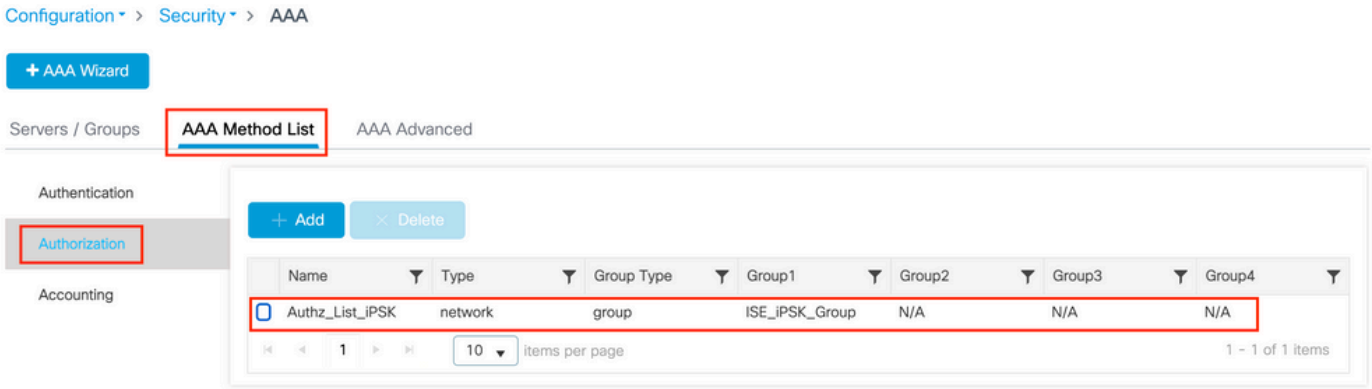
[Configuration] > [Security] > [AAA] > [Servers/Groups] > [Servers] で、ISEをRADIUSサーバとして追加します。



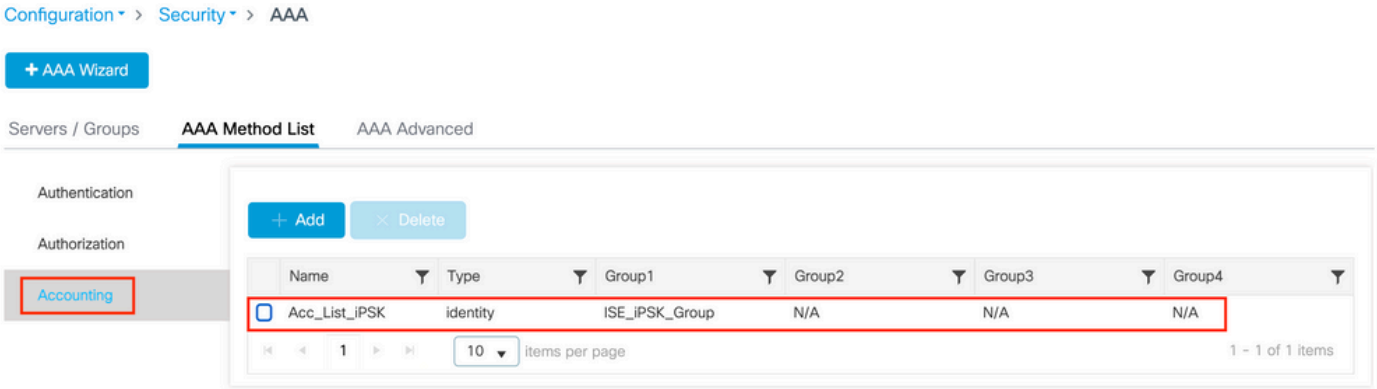
[Configuration] > [Security] > [AAA] > [Servers/Groups] > [Server Groups] で、RADIUSサーバグループを作成し、以前に作成したISEサーバを追加します。



[AAA Method List] タブで、以前に作成したRADIUSサーバグループを指すタイプ「**network**」とグループタイプ「**group**」を持つ**Authorization**リストを作成します。



アカウンティングの設定はオプションですが、タイプを「**identity**」に設定し、同じRADIUSサーバグループを指定することで実行できます。



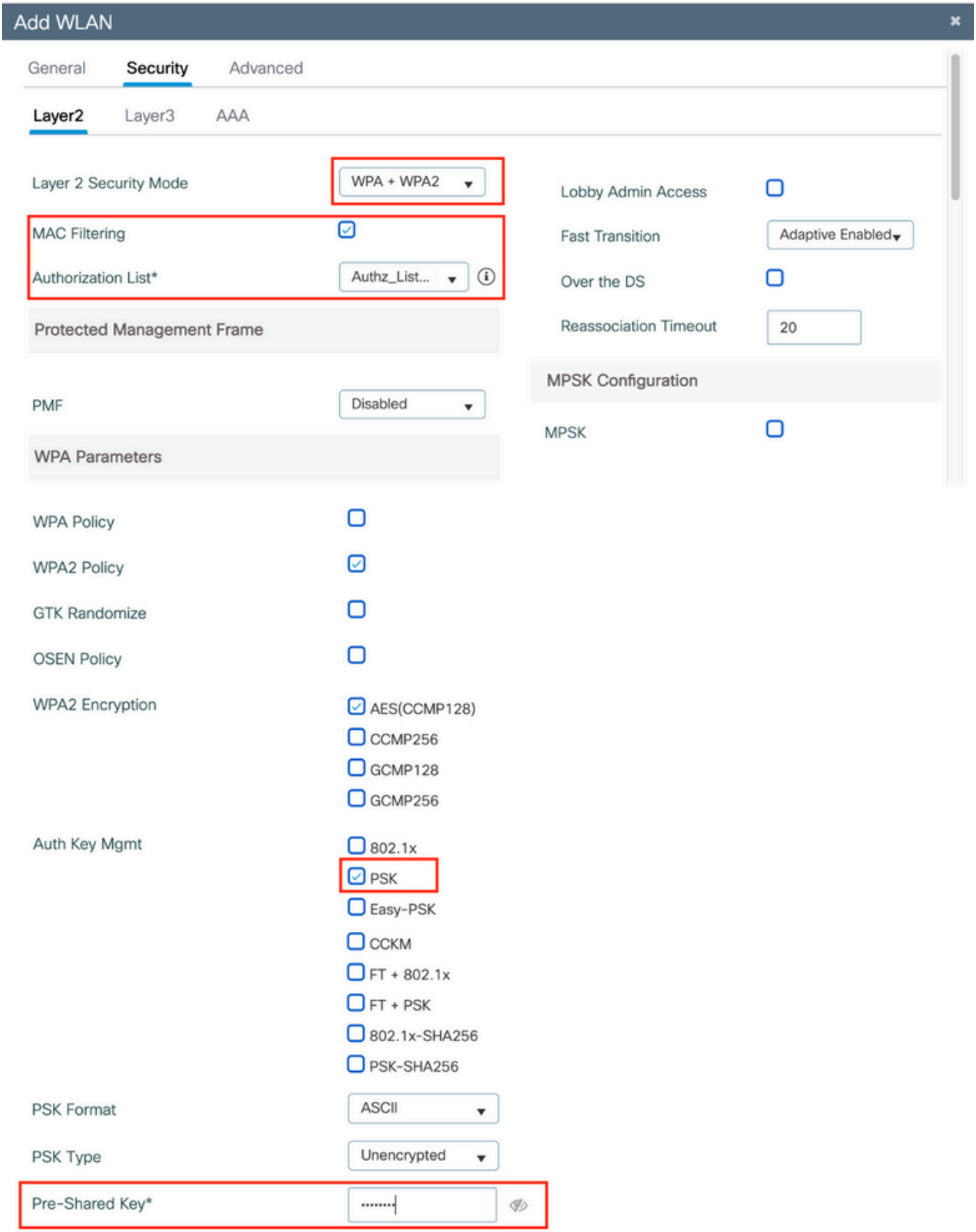
これは、次のコマンドを使用してコマンドラインから実行することもできます。

```
radius server
```

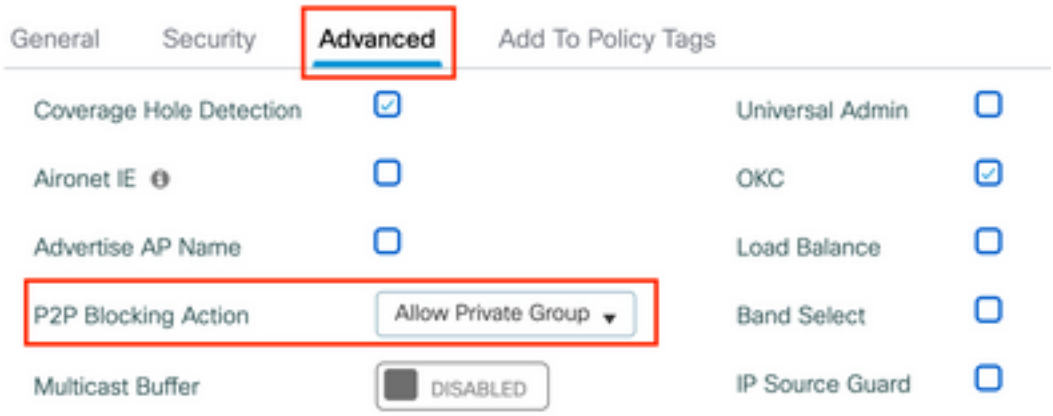
[Configuration] > [Tags & Profiles] > [WLANs] で、新しいWLANを作成します。 [Layer 2 configuration]で、次の操作を実行します。

- MACフィルタリングを有効にし、以前に作成した許可リストを設定します
- [Auth Key Mgmt] で[PSK] を有効にします。
- 事前共有キーフィールドには、任意の値を入力できます。これは、Webインターフェイス設計の要件を満たすためだけに行われます。ユーザはこのキーを使用して認証できません。こ

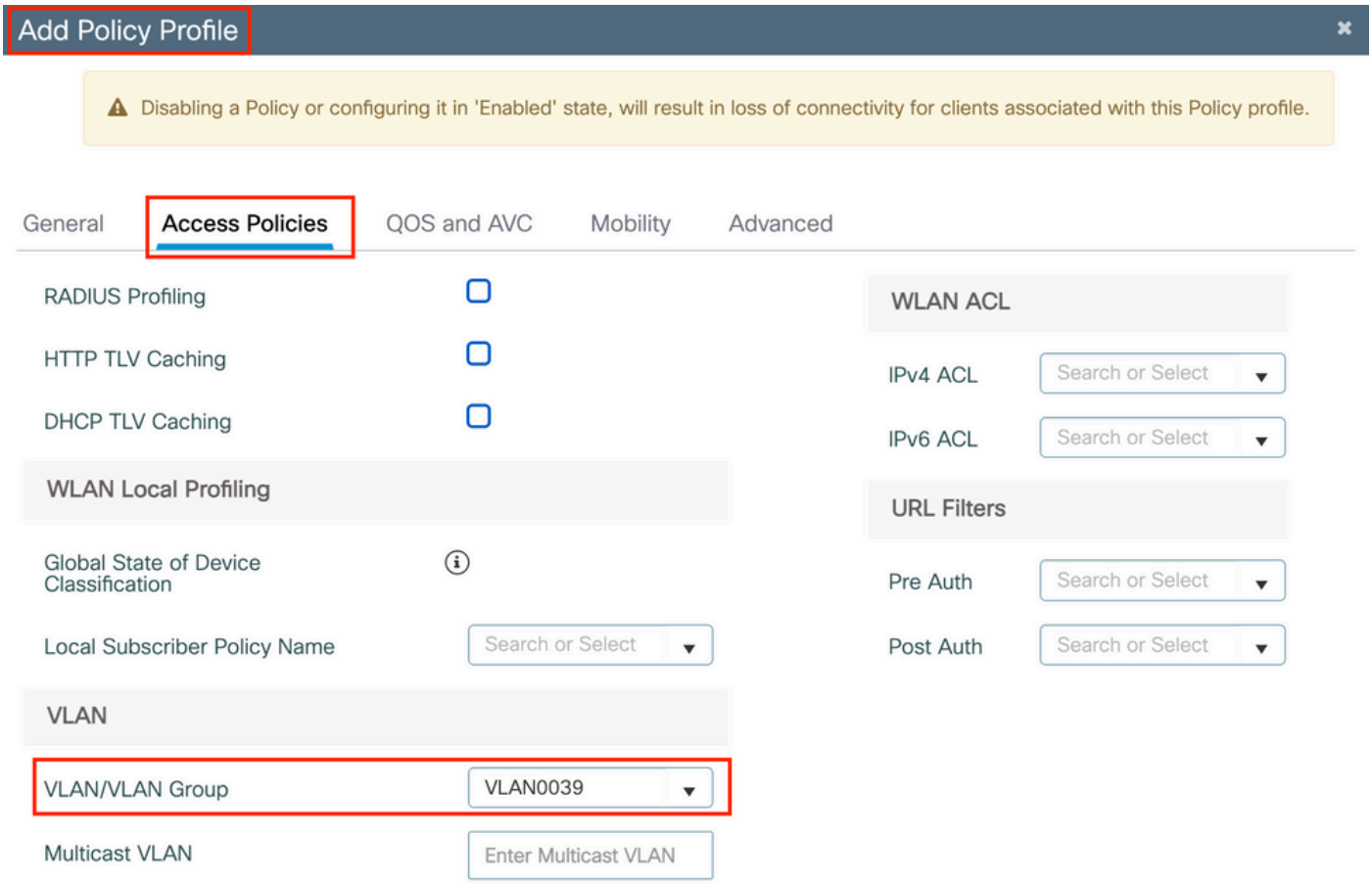
の場合、事前共有キーは「12345678」に設定されています。



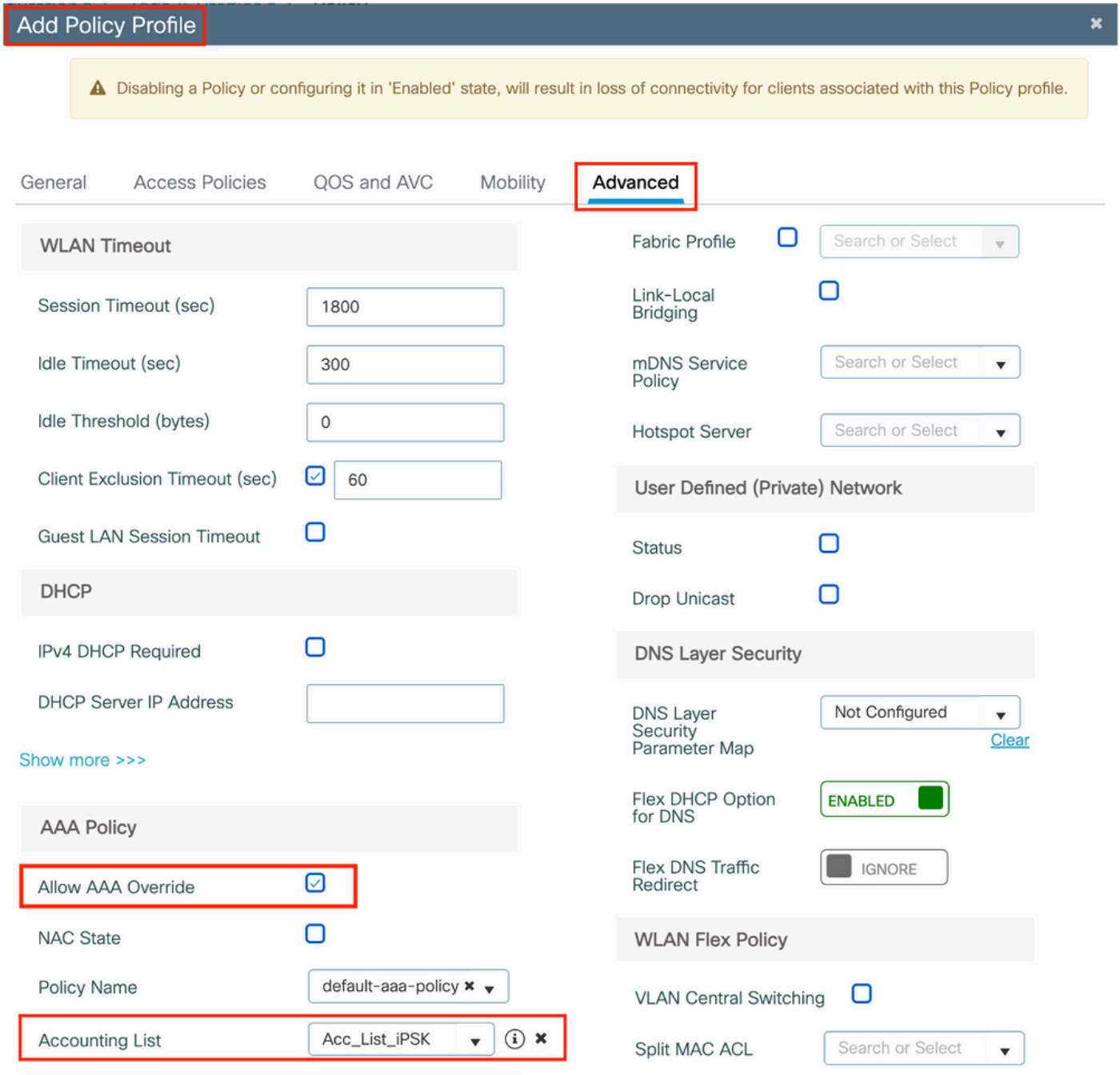
ユーザの分離は、[Advanced] タブで実行できます。[Allow Private Group]に設定すると、同じPSKを使用しているユーザが相互に通信できるようになりますが、異なるPSKを使用しているユーザはブロックされます。



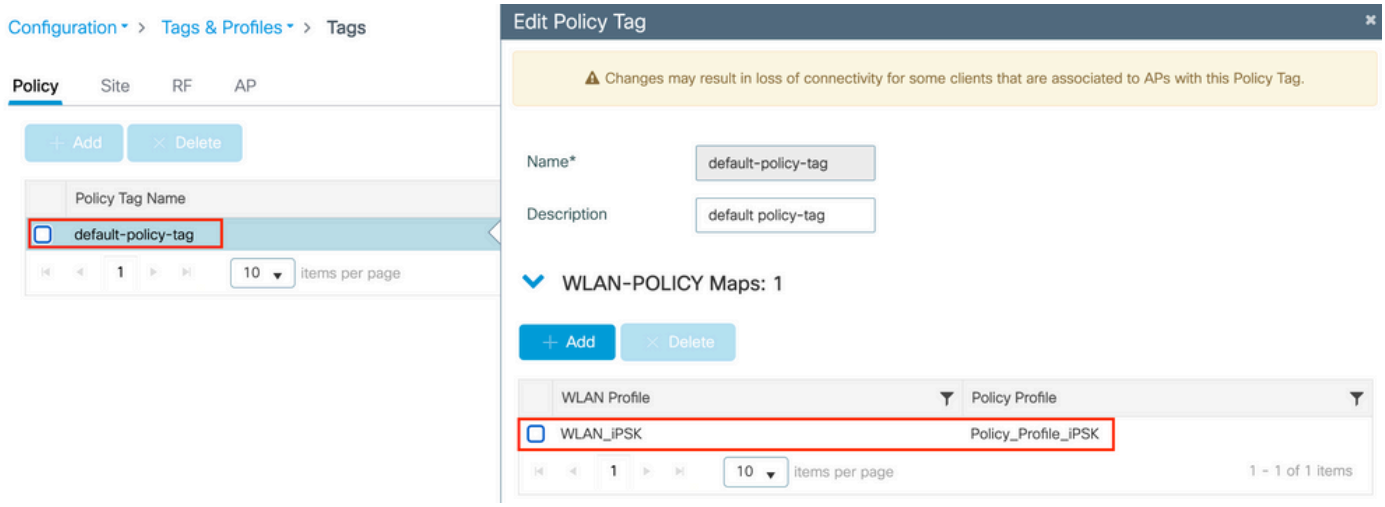
[Configuration] > [Tags & Profiles] > [Policy] で、新しいポリシープロファイルを作成します。
[Access Policies] タブで、このWLANが使用しているVLANまたはVLANグループを設定します。



[Advanced] タブで、[AAA Override]を有効にし、作成済みの場合はアカウンティングリストを追加します。



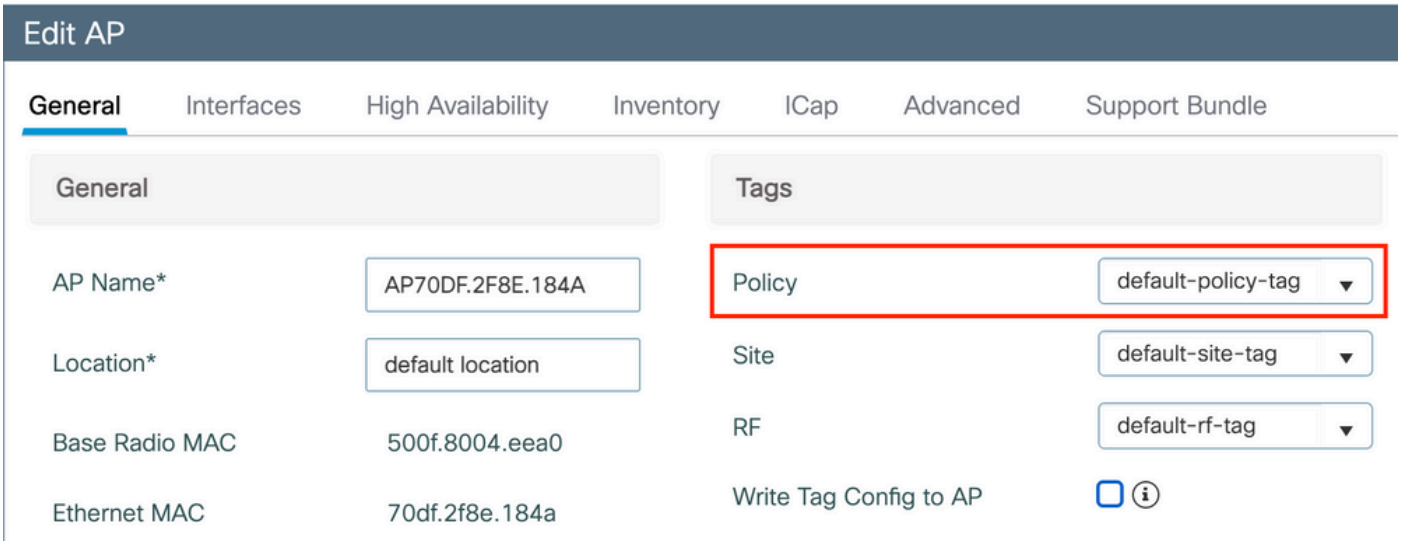
[Configuration] > [Tags & Profiles] > [Tags] > [Policy] で、作成したポリシープロファイルにWLANがマッピングされていることを確認します。



これは、次のコマンドを使用してコマンドラインから実行することもできます。

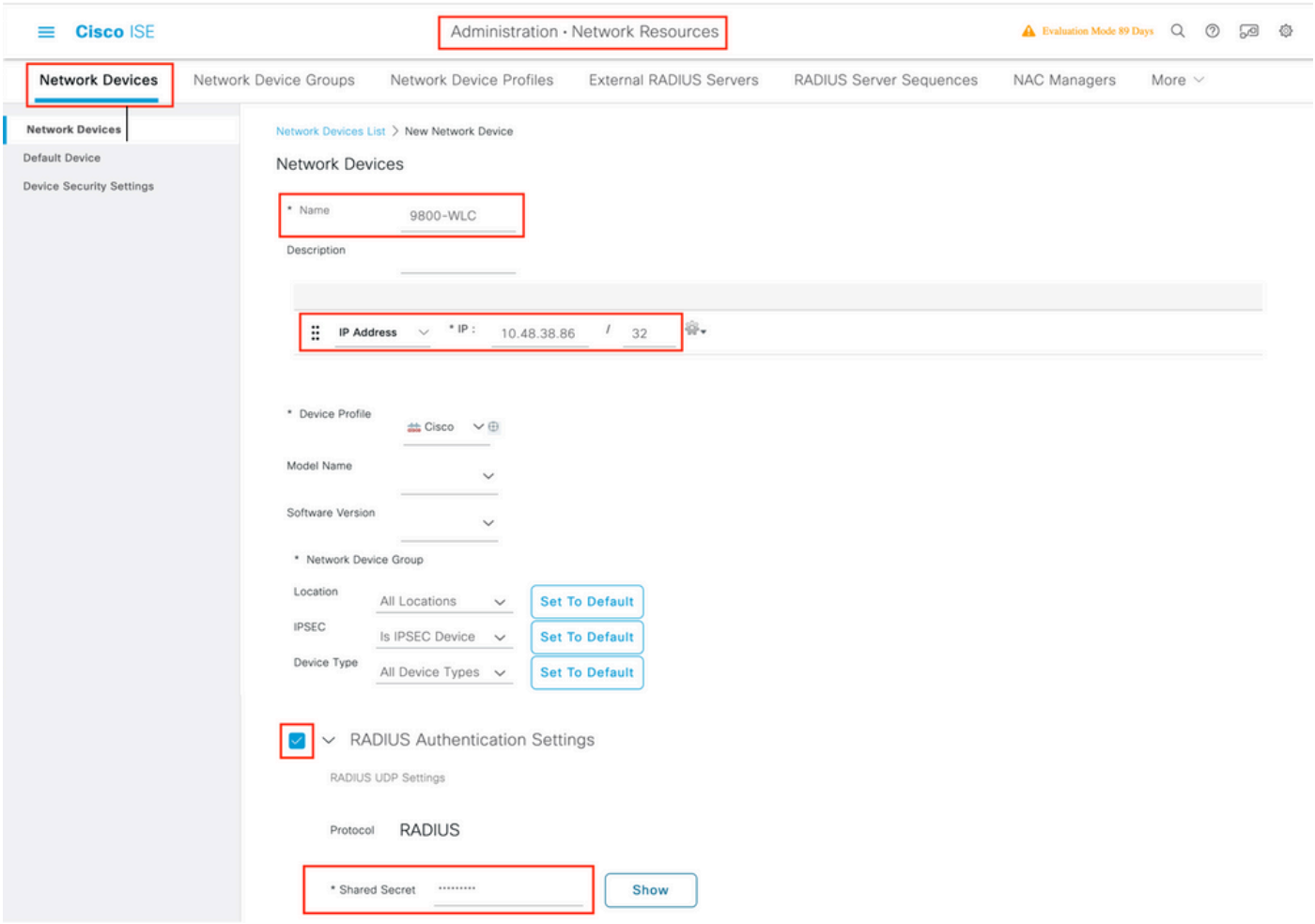
```
wlan
```

[Configuration] > [Wireless] > [Access Points] で、WLANをブロードキャストする必要があるアクセスポイントに次のタグが適用されていることを確認します。

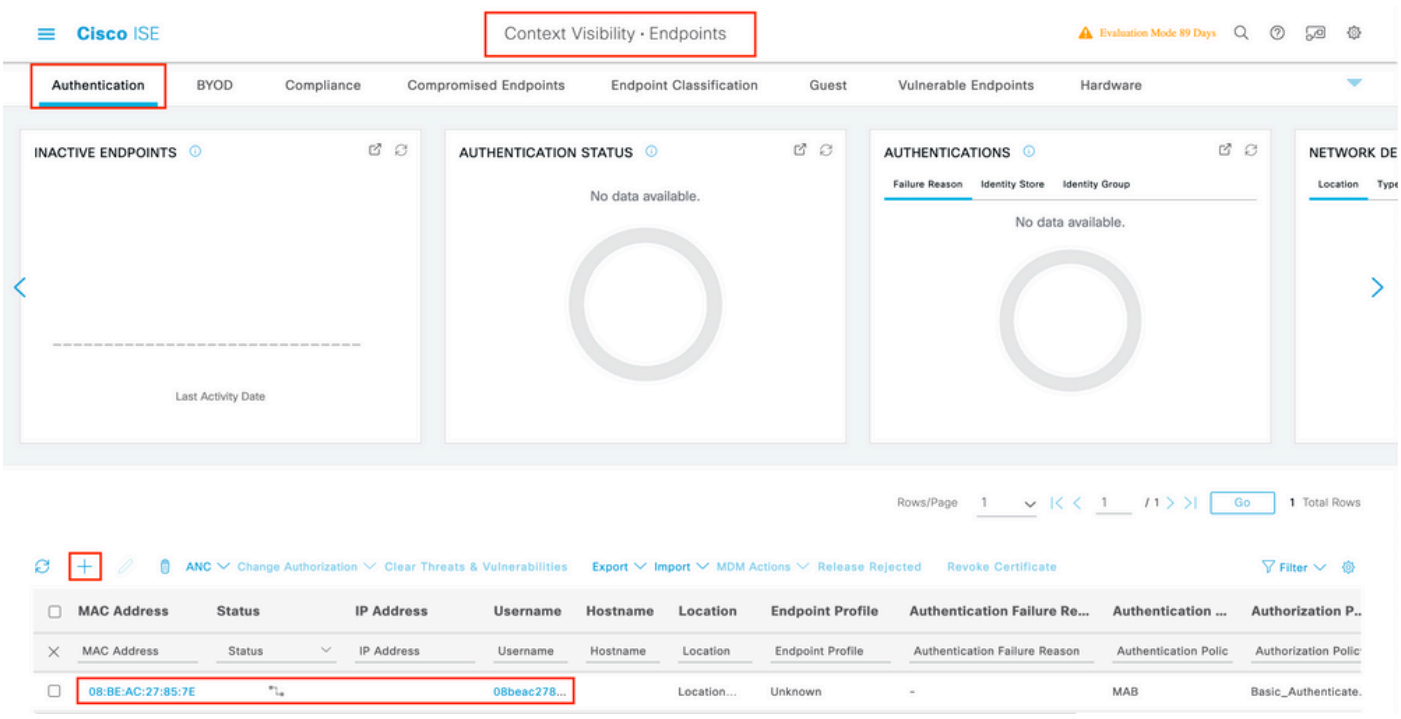


ISE の設定

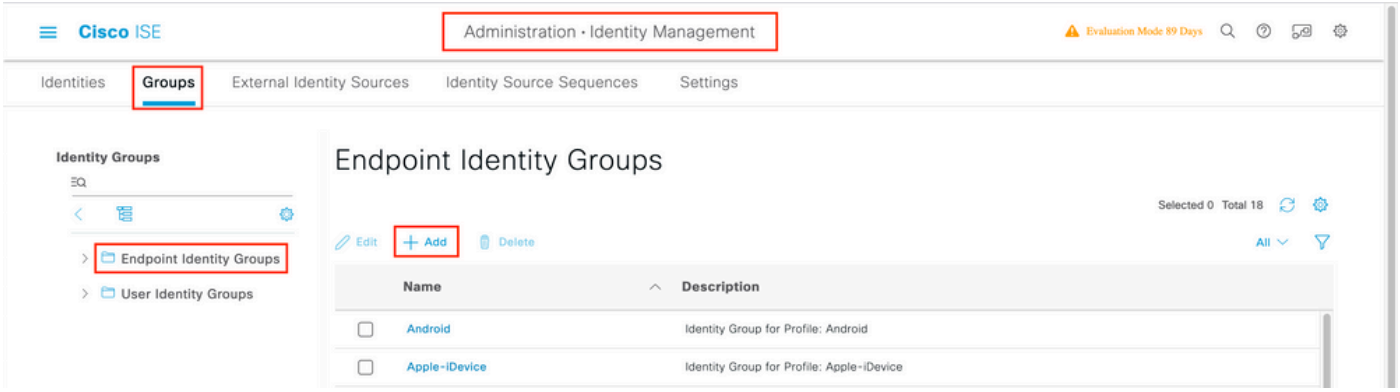
この設定ガイドでは、クライアントのMACアドレスに基づいてデバイスのPSKが決定されるシナリオについて説明します。[Administration] > [Network Resources] > [Network Devices] で、新しいデバイスを追加し、IPアドレスを指定し、RADIUS認証設定を有効にし、RADIUS共有秘密を指定します。

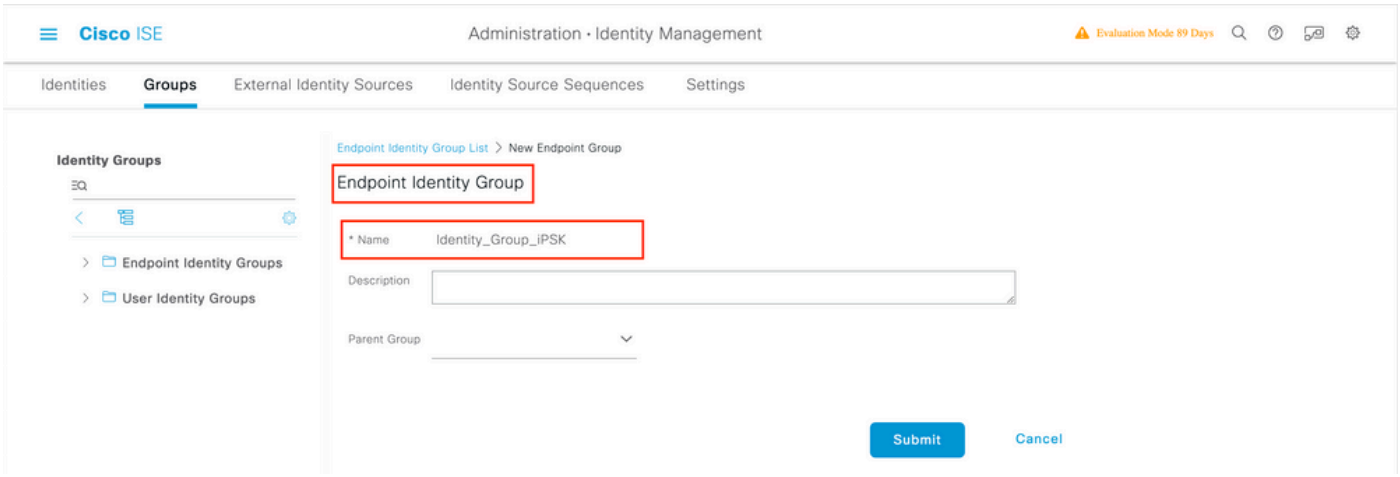


[Context Visibility] > [Endpoints] > [Authentication] で、iPSKネットワークに接続しているすべてのデバイス（クライアント）のMACアドレスを追加します。

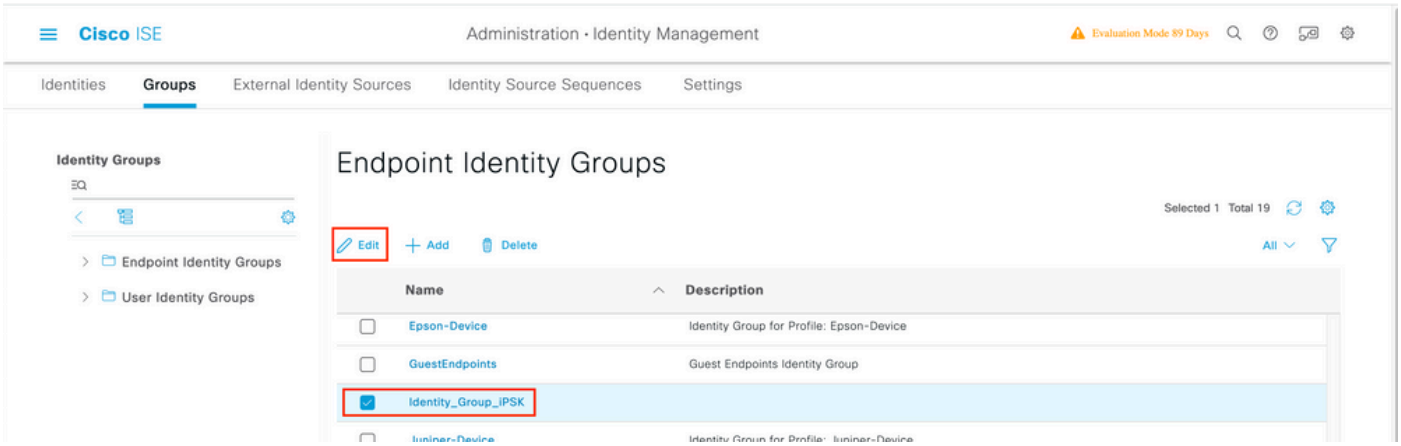


[Administration] > [Identity Management] > [Groups] > [Endpoint Identity Groups] で、1つ以上のグループを作成し、それらにユーザを割り当てます。各グループは、後でネットワークに接続するために異なるPSKを使用するように設定できます。

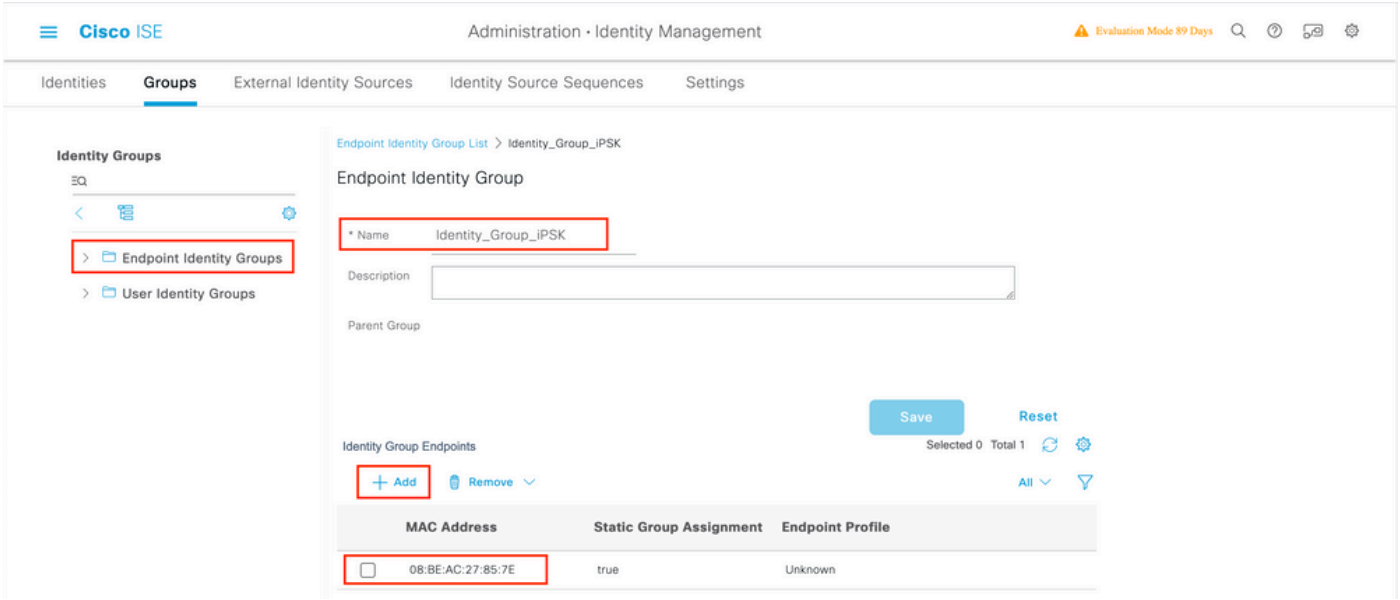




グループが作成されたら、ユーザをグループに割り当てることができます。作成したグループを選択し、[Edit]をクリックします。



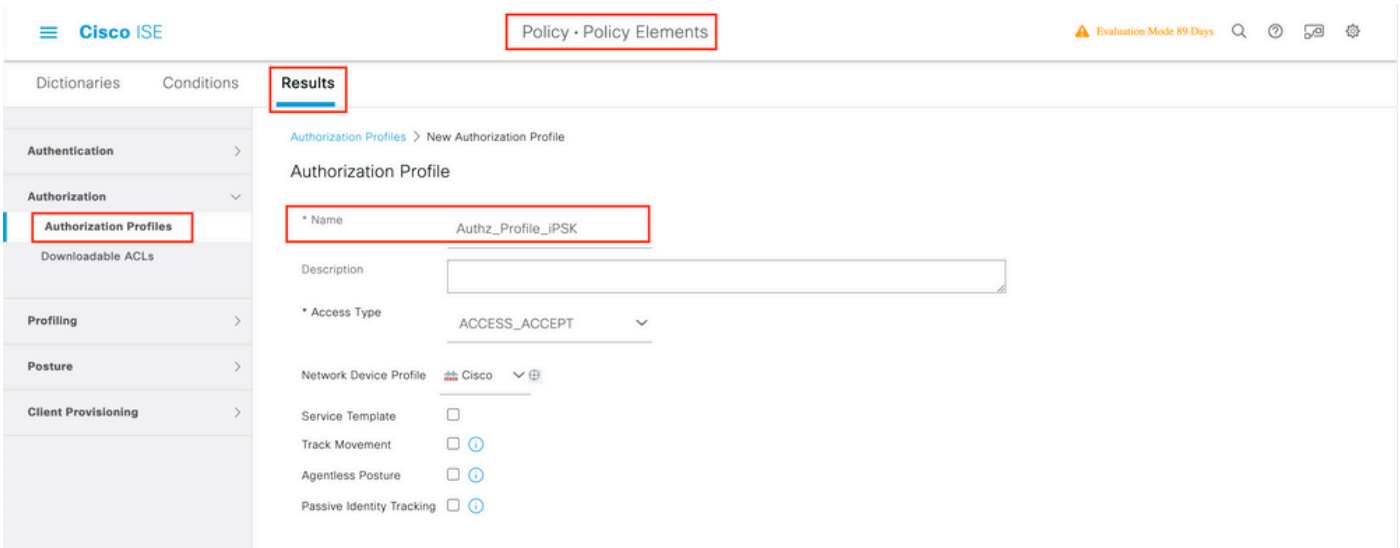
グループ設定で、[Add]ボタンをクリックして、このグループに割り当てるクライアントのMACアドレスを追加します。

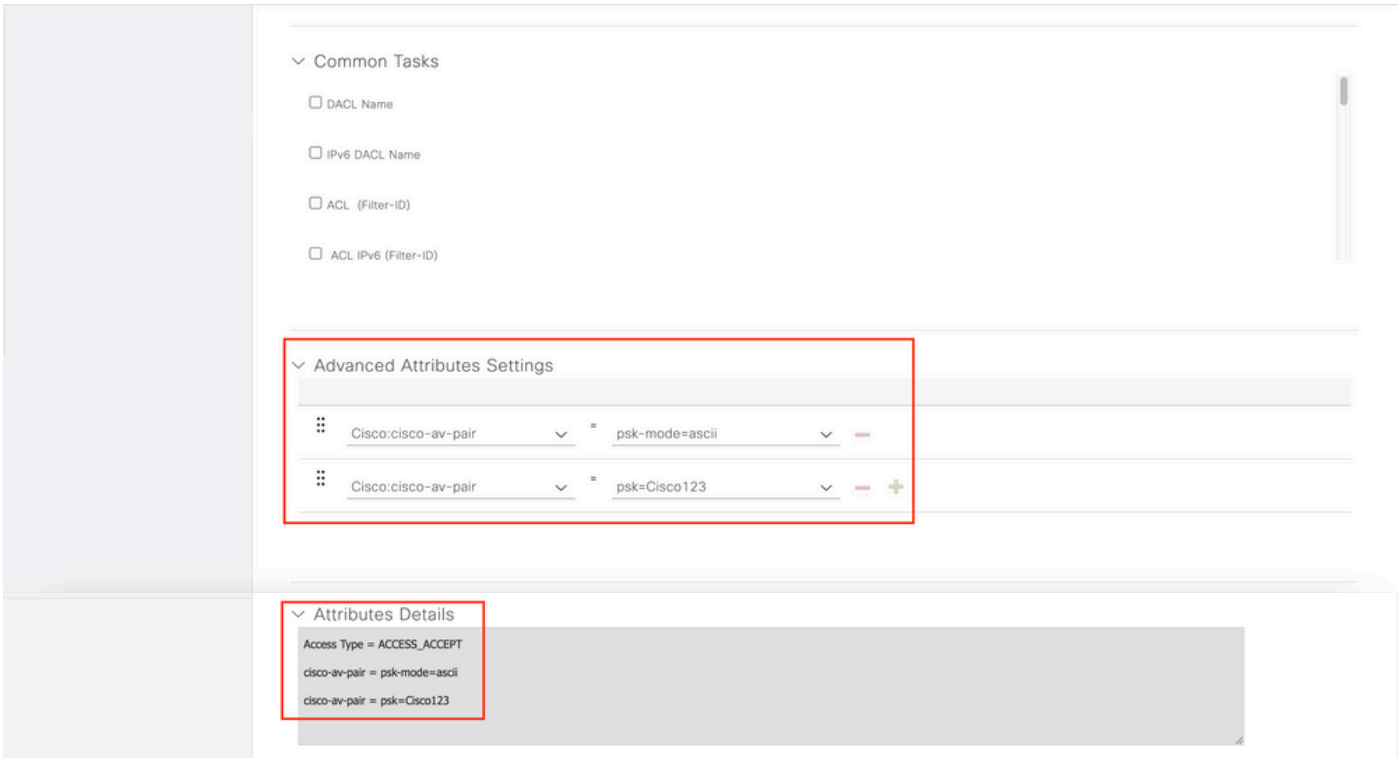


[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] で、新しい認可プロファイルを作成します。属性を次のように設定します。

```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=
```

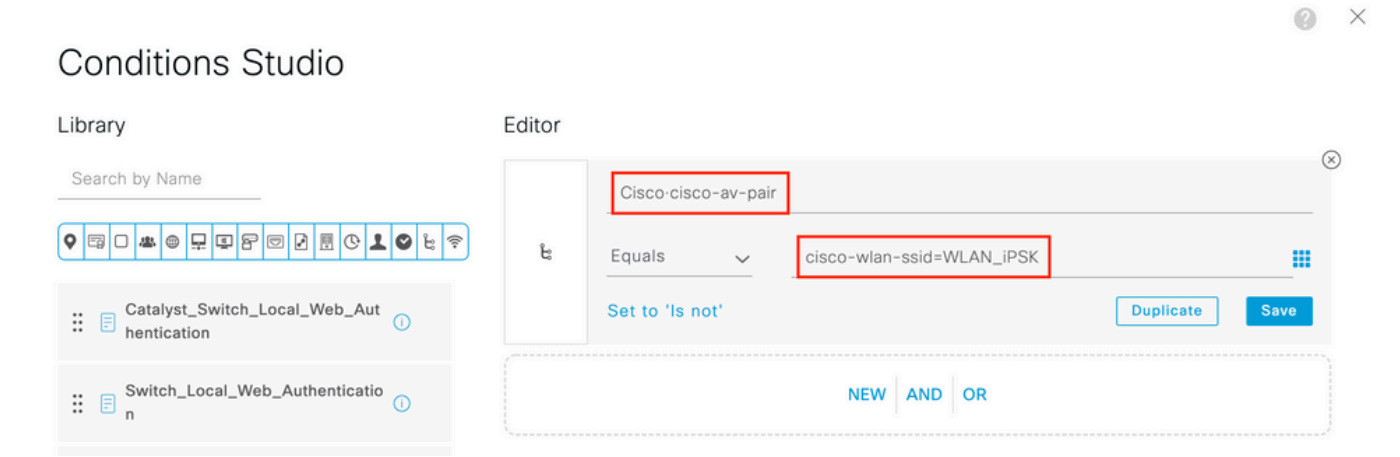
異なるPSKを使用する必要があるユーザグループごとに、異なるpsk avペアを使用して追加の結果を作成します。ACLやVLANオーバーライドなどの追加パラメータもここで設定できます。



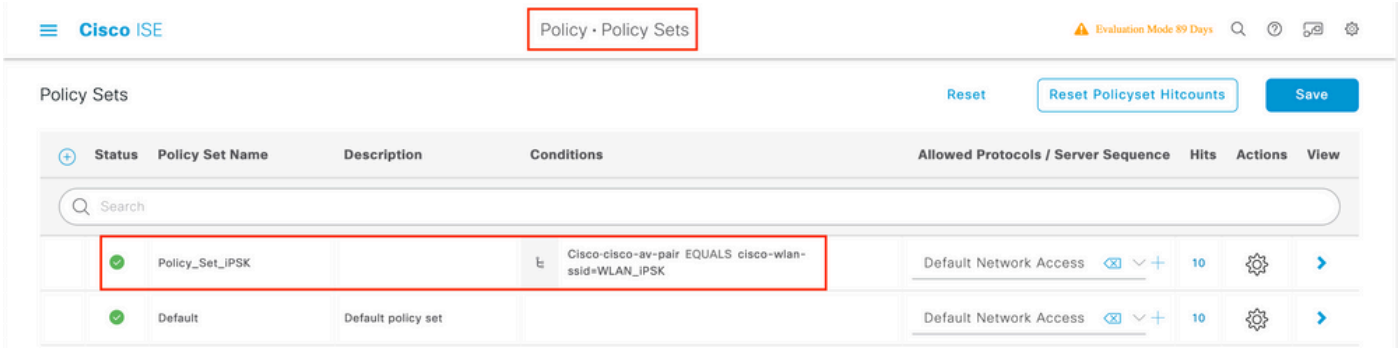


[Policy] > [Policy Sets] で、新しいポリシーを作成します。クライアントがポリシーセットに一致していることを確認するために、次の条件が使用されます。

```
Cisco:cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_iPSK    // "WLAN_iPSK" is WLAN name
```

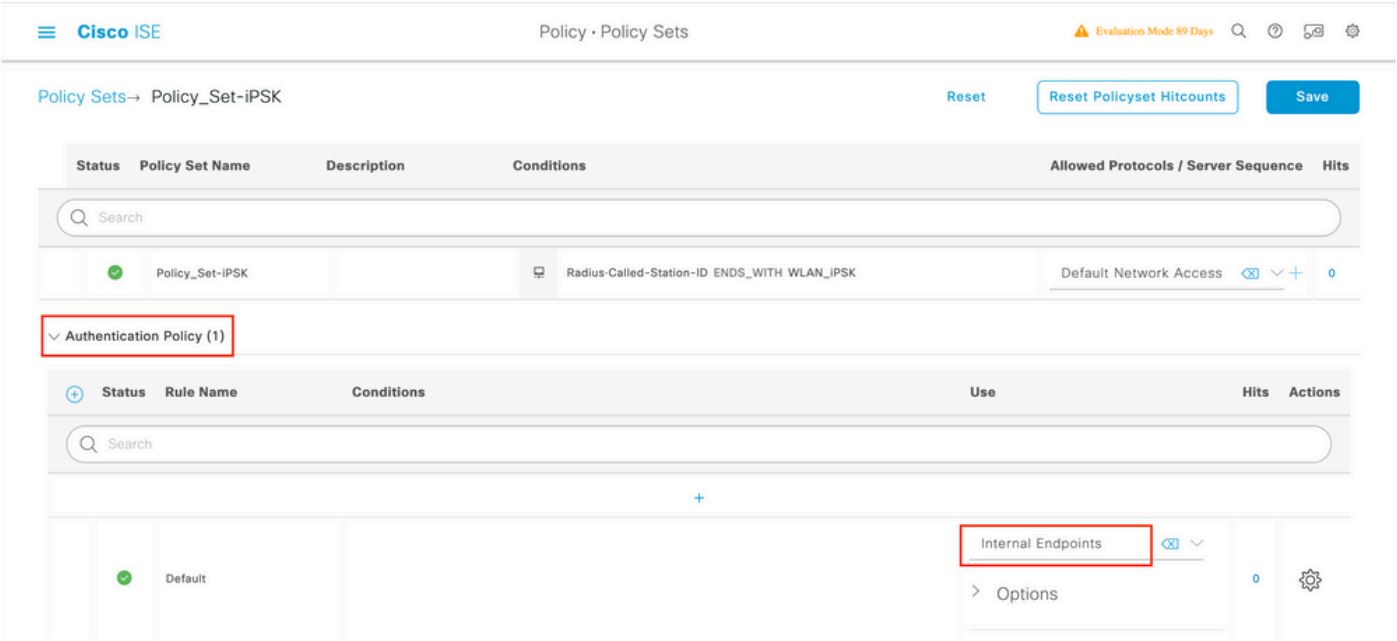


ポリシー照合をより安全にするために、条件を追加できます。



[Policy Set]行の右側にある青い矢印をクリックして、新しく作成したiPSKポリシーセット設定に移動します。

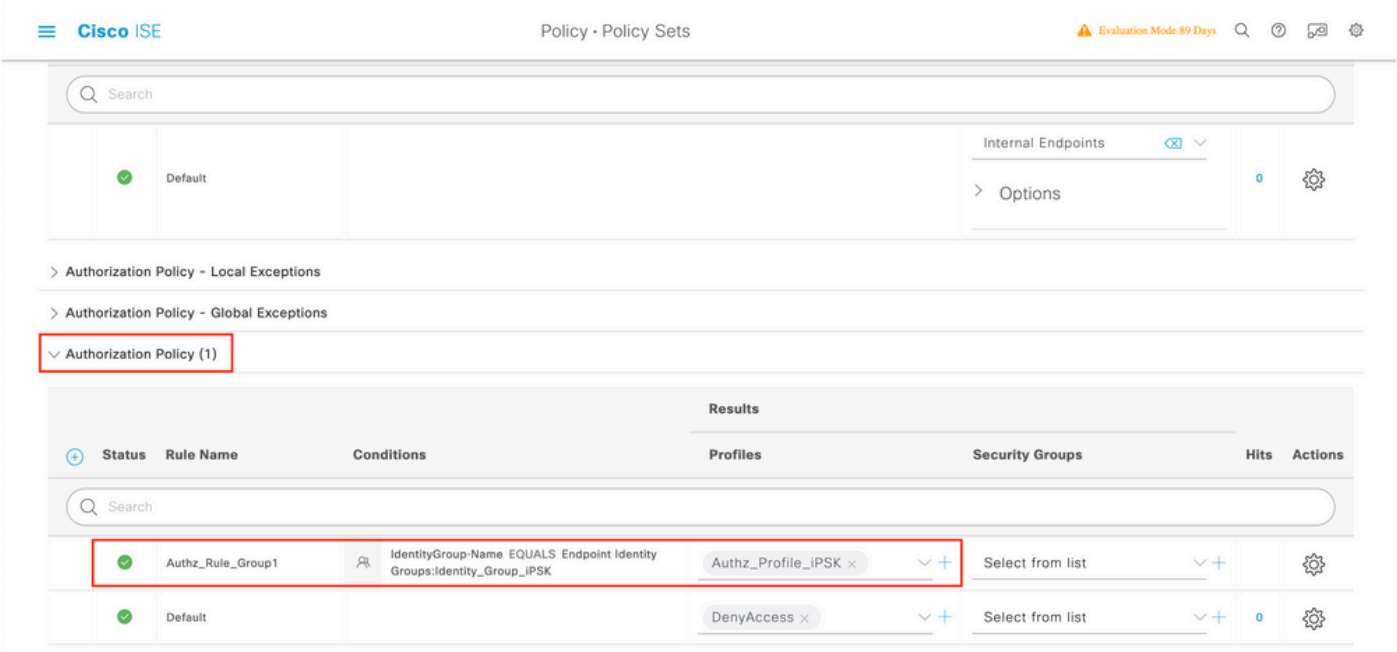
[Authentication Policy] が[Internal Endpoints]に設定されていることを確認します。



[Authorization Policy] で、ユーザグループごとに新しいルールを作成します。条件として、次を使用します。

```
IdentityGroup-Name EQUALS Endpoint Identity Group:Identity_Group_iPSK      //
"Identity_Group_iPSK" is name of the created endpoint group
```

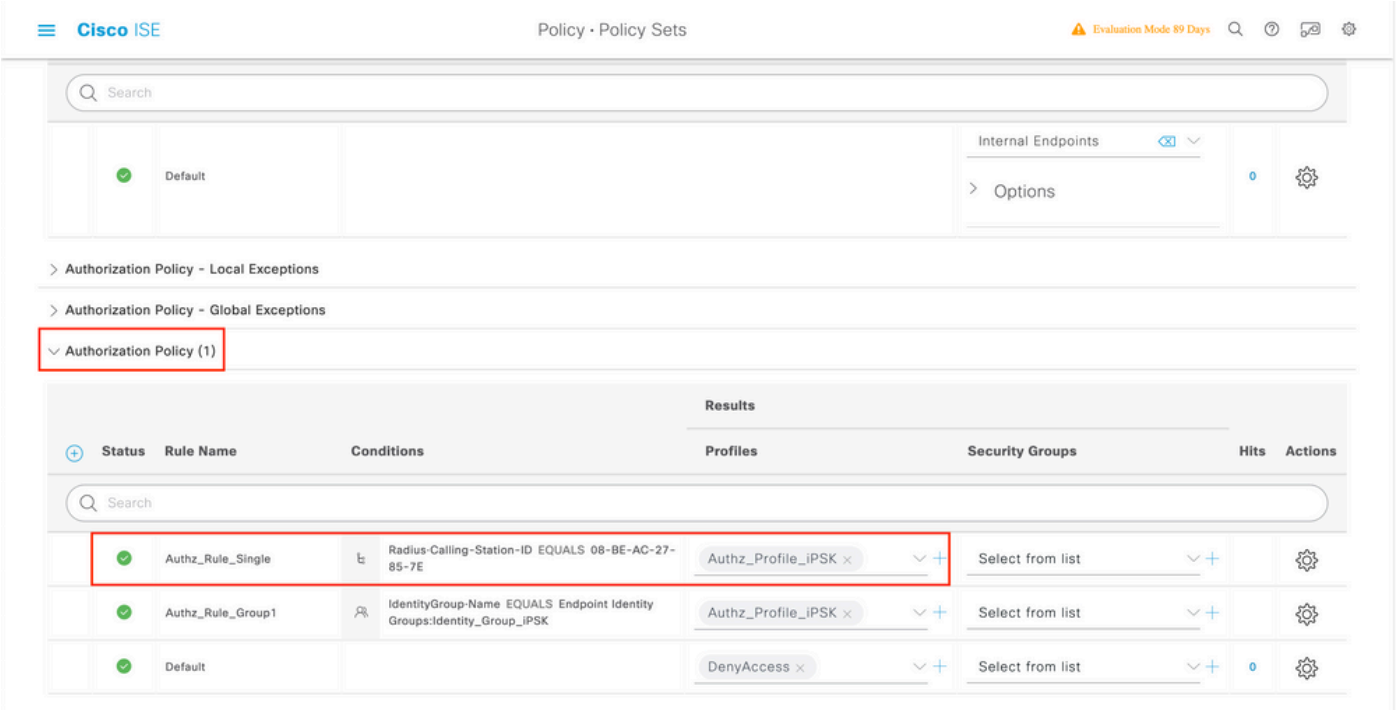
Resultは、以前に作成した認可プロファイルです。[Default] ルールが一番下に残り、[DenyAccess] をポイントしていることを確認します。



すべてのユーザが異なるパスワードを使用する場合、エンドポイントグループとそのエンドポイントグループに一致するルールを作成する代わりに、次の条件を持つルールを作成できます。

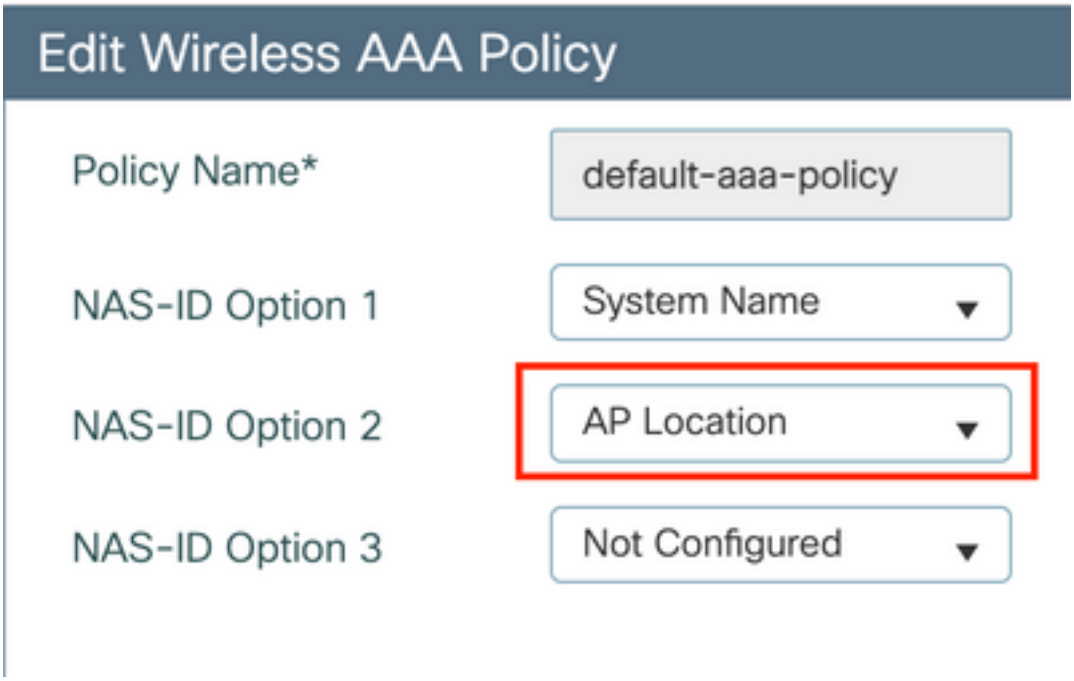
```
Radius-Calling-Station-ID EQUALS <client_mac_addr>
```

注： MACアドレスデリミタは、WLCの**[AAA] > [AAA Advanced] > [Global Config] > [Advanced Settings]で設定できます。**この例では、文字「 – 」が使用されています。



認可ポリシーのルールでは、ユーザが使用しているパスワードを指定するために、他の多くのパラメータを使用できます。最も一般的に使用されるルールは次のとおりです。

1. **ユーザの場所に基づく照合**
   このシナリオでは、WLCはAPロケーション情報をISEに送信する必要があります。これにより、ある場所のユーザは1つのパスワードを使用し、別の場所のユーザは別のパスワードを使用できます。これは、[Configuration] > [Security] > [Wireless AAA Policy] で設定できます。



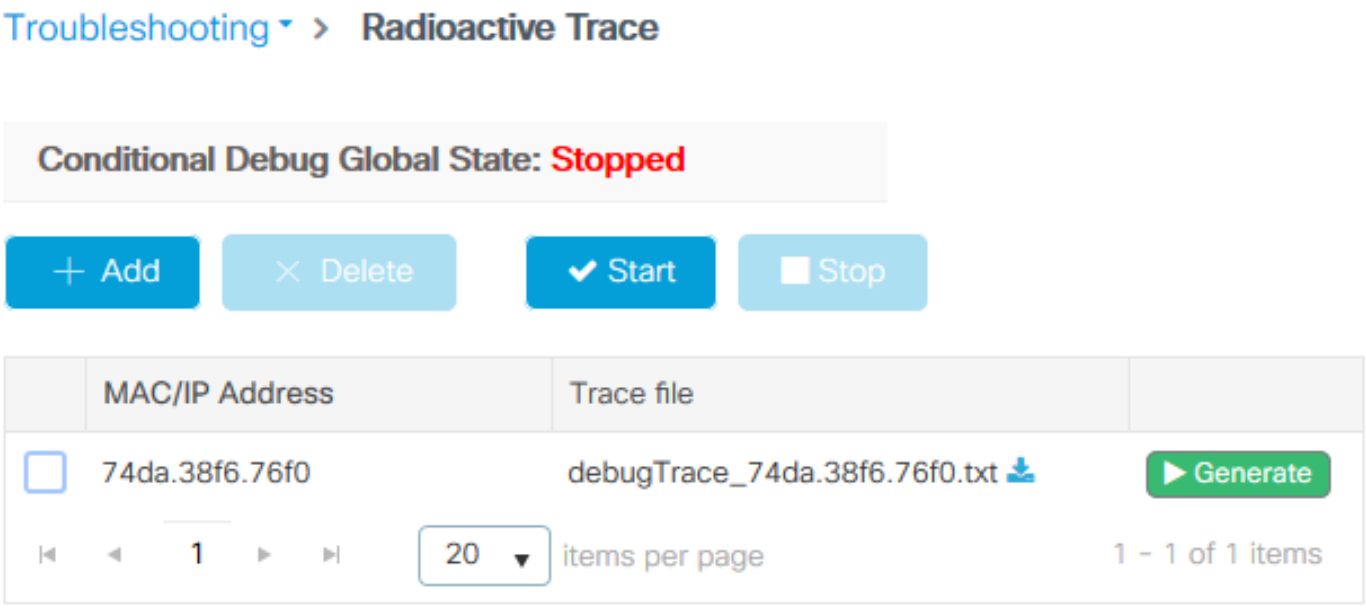
2. **デバイスのプロファイリングに基づく照合**
   このシナリオでは、デバイスをグローバルにプロファイルするようにWLCを設定する必要があります。これにより、管理者はラップトップデバイスと電話デバイスに異なるパスワードを設定できます。グローバルデバイス分類は、[Configuration] > [Wireless] > [Wireless Global] で有効にできます。ISEでのデバイスプロファイリングの設定については、『ISEプロファイリング設計ガイド』を参照してください。

暗号化キーを返すだけでなく、この認可は802.11アソシエーションフェーズで発生するため、ACLやVLAN IDなど、他のAAA属性をISEから返すことも完全に可能です。

トラブルシュート

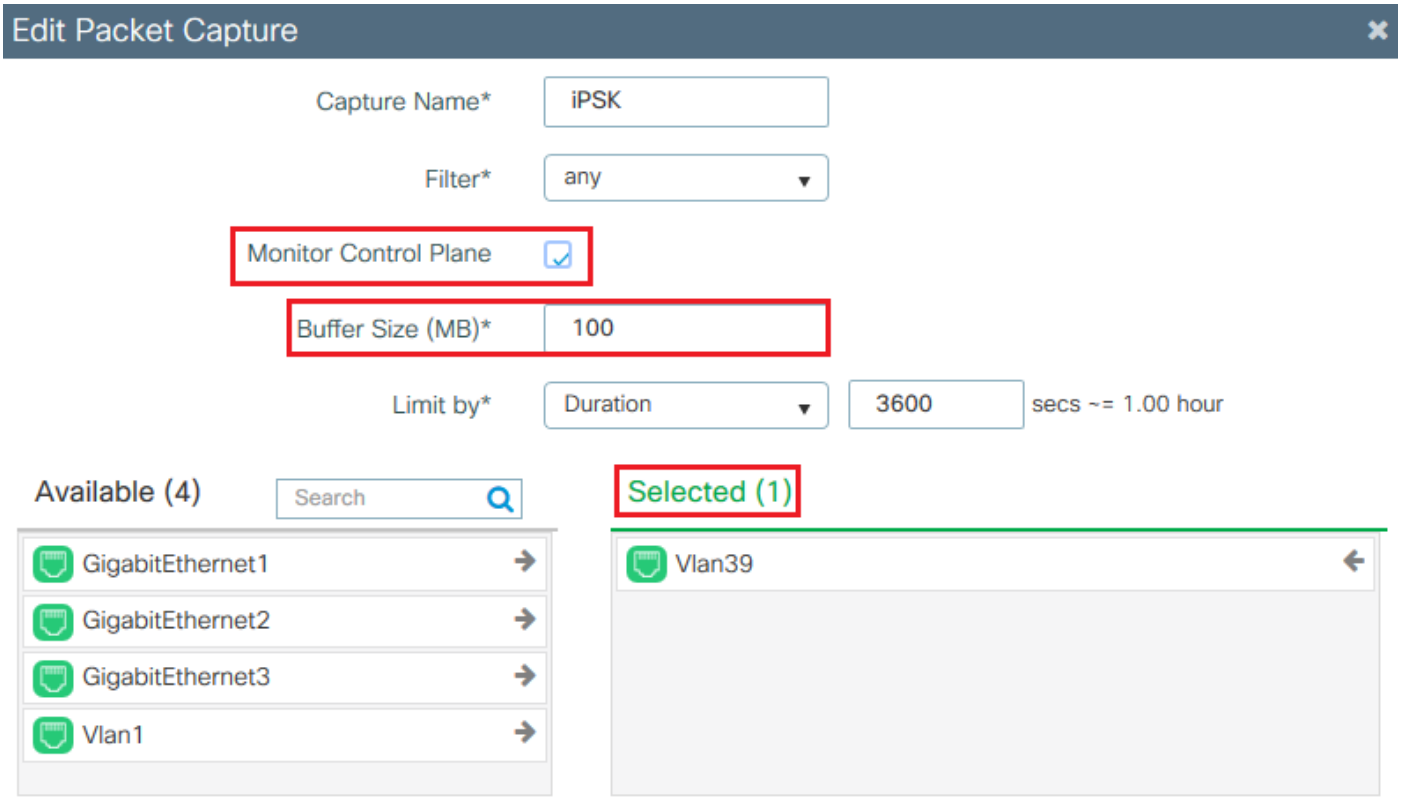
9800 WLCのトラブルシューティング

WLCでは、放射性トレースの収集は、問題の大部分を特定するのに十分な量である必要があります。これは、WLC Webインターフェイスの[Troubleshooting] > [Radioactive Trace] で実行できます。クライアントのMACアドレスを追加し、**Start**を押して問題の再現を試みます。 [Generate] をクリックしてファイルを作成し、ダウンロードします。



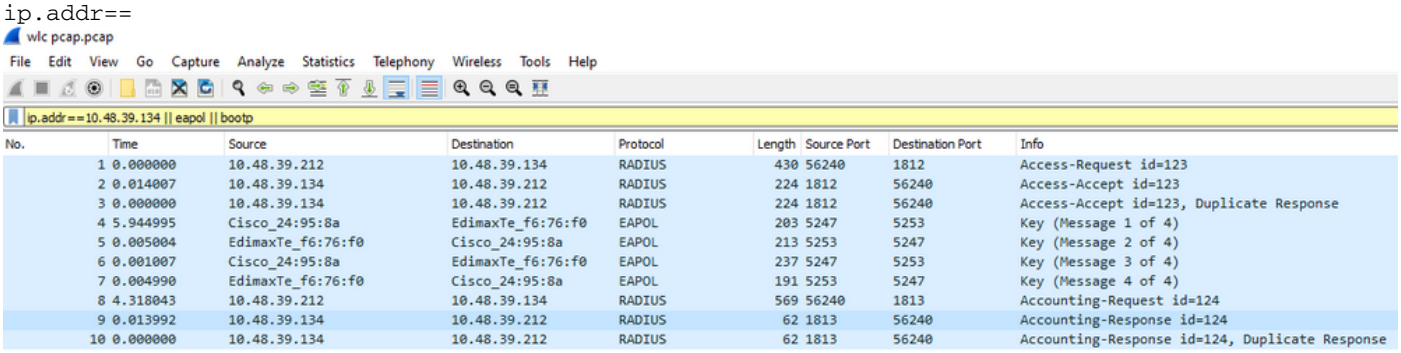
重要：IOS 14およびAndroid 10スマートフォンのiPhoneは、ネットワークへの関連付けにランダム化されたMACアドレスを使用します。この機能により、iPSK設定が完全に壊れる可能性があります。この機能が無効になっていることを確認してください。

放射性トレースでは問題を特定するのに十分でない場合は、パケットキャプチャをWLCで直接収集できます。[Troubleshooting] > [Packet Capture] で、キャプチャポイントを追加します。デフォルトでは、WLCはすべてのRADIUS AAA通信にワイヤレス管理インターフェイスを使用します。WLCのクライアント数が多い場合は、バッファサイズを100 MBに増やします。



次の図に、認証とアカウンティングの試行が成功したときのパケットキャプチャを示します。このクライアントに関連するすべてのパケットをフィルタリングするには、次のWiresharkフィルタを使用します。

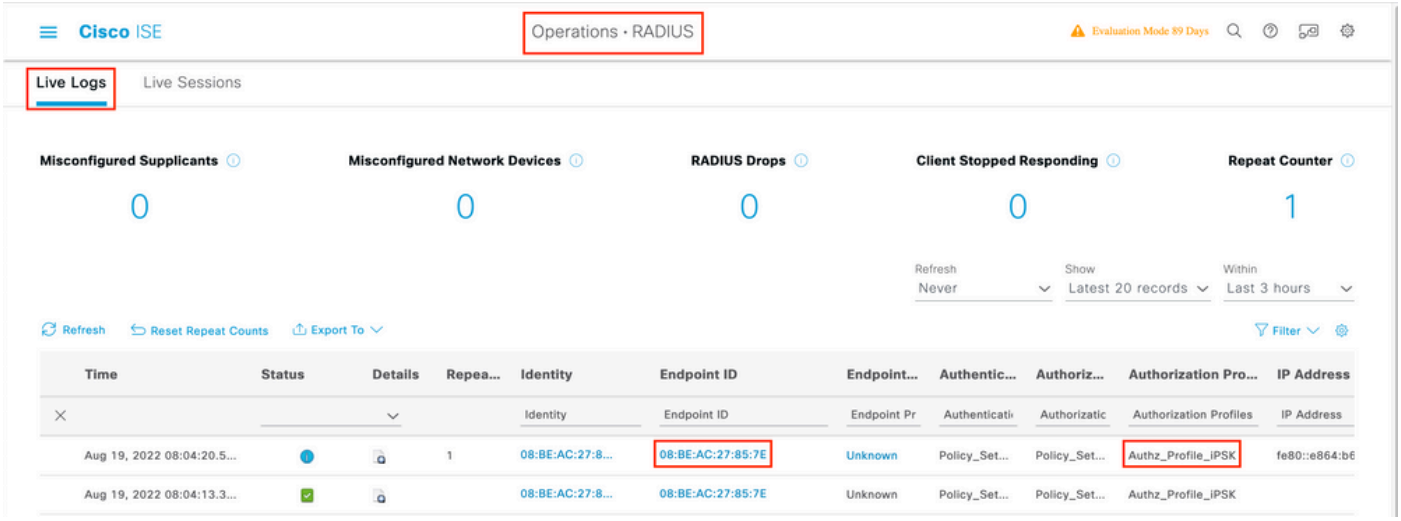
ip.addr==



No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	0.000000	10.48.39.212	10.48.39.134	RADIUS	430	56240	1812	Access-Request id=123
2	0.014007	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123
3	0.000000	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123, Duplicate Response
4	5.944995	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	203	5247	5253	Key (Message 1 of 4)
5	0.005004	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	213	5253	5247	Key (Message 2 of 4)
6	0.001007	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	237	5247	5253	Key (Message 3 of 4)
7	0.004990	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	191	5253	5247	Key (Message 4 of 4)
8	4.318043	10.48.39.212	10.48.39.134	RADIUS	569	56240	1813	Accounting-Request id=124
9	0.013992	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124
10	0.000000	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124, Duplicate Response

ISEのトラブルシューティング

Cisco ISEの主なトラブルシューティングテクニックは、[Operations] > [RADIUS] > [Live Logs] にある[Live Logs] ページです。これらは、クライアントのMACアドレスを[Endpoint ID]フィールドに入力することでフィルタリングできます。 完全なISEレポートを開くと、障害の原因に関する詳細が表示されます。クライアントが正しいISEポリシーにヒットしていることを確認します。



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。