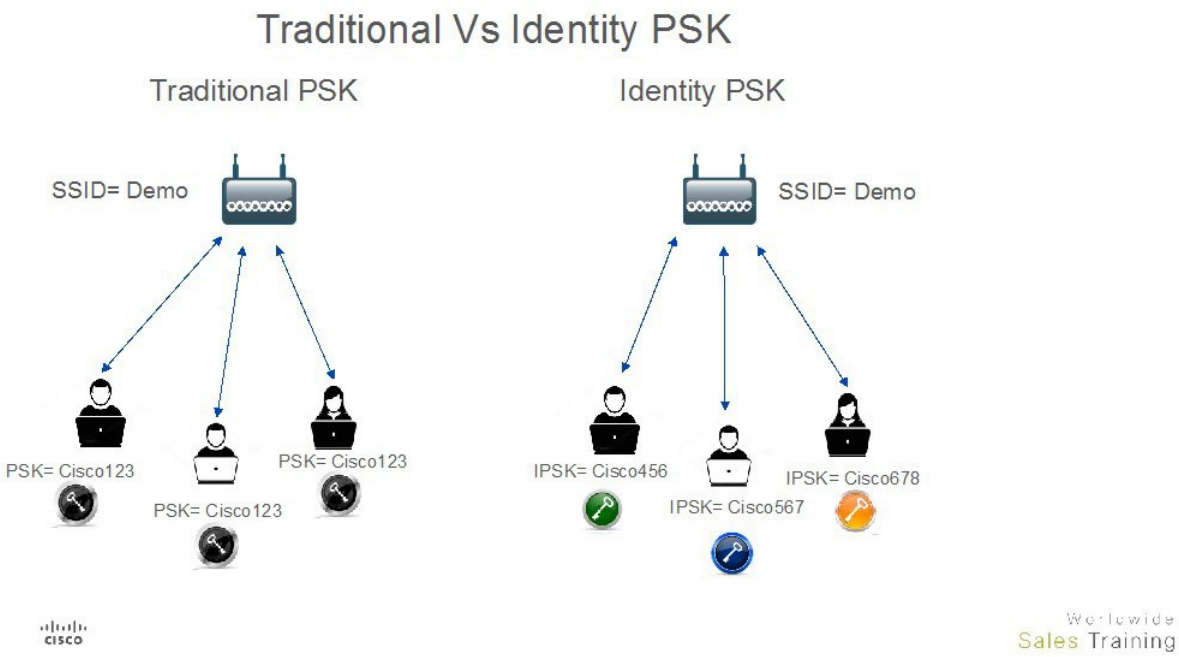
8.5 Identity PSK 機能導入ガイド

改訂：2018 年 11 月 28 日

製品や機能の概要

「IoT：Internet of Things（モノのインターネット）」の到来により、インターネットに接続されるデバイスの数は非常に増加しています。これらのすべてのデバイスが 802.1x サプリカントをサポートしているわけではなく、インターネットに接続するための代替メカニズムが必要です。セキュリティ メカニズムの 1 つである WPA-PSK が代替手段として考えられます。現在の設定では、事前共有キーは同じ WLAN に接続するすべてのクライアントで同じです。教育機関などの一部の設置環境では、これによりキーが不正ユーザに共有され、セキュリティ違反をもたらします。したがって、前述の内容やその他の要件により、大規模な環境ではクライアントごとに一意の事前共有キーを準備しておく必要が生じます。

- Identity PSK は、同じ SSID の個人またはユーザ グループのために作成された一意の事前共有キーです。
- クライアントに複雑な設定は必要ありません。PSK と同じシンプルさで、IoT、BYOD、ゲストに対して最適に展開できます。
- 802.1x 未対応のほとんどのデバイスでサポートされるため、より強力な IoT セキュリティを実現します。
- 他に影響を与えずに 1 つのデバイスまたは個人に対するアクセスを簡単に取り消せます。
- 何千ものキーを簡単に管理でき、AAA サーバを介して配布することができます。



上の図に示すように、従来の PSK では、特定の SSID に接続するすべてのクライアントのキーは同じなので、セキュリティ上の問題につながります。Identity PSK では、同じ SSID に接続するクライアントごとに別のキーを設定できます。

IPSK ソリューション

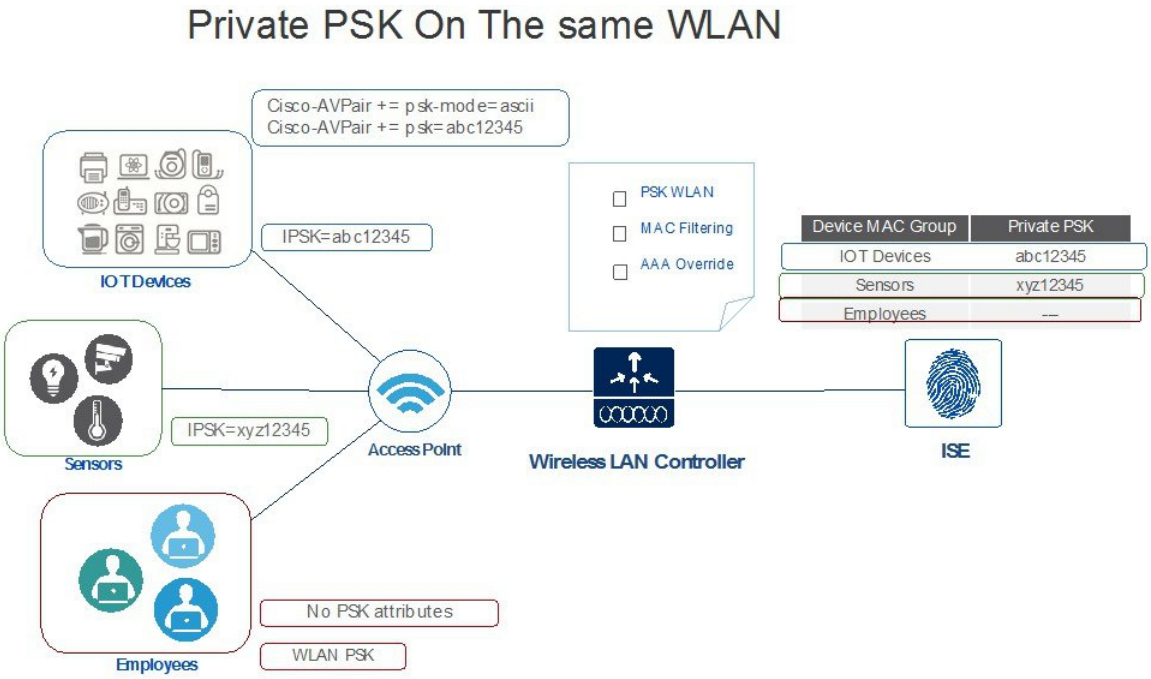
クライアントの認証時に、AAA サーバはクライアントの MAC アドレスを認証し、Cisco-AVPair リストの一部としてパスフレーズ（設定されている場合）を送信します。WLC は RADIUS 応答の一部としてこれを受信し、PSK の計算のため追加処理します。

クライアントがアクセス ポイントからブロードキャストされている SSID にアソシエーション要求を送信すると、ワイヤレス LAN コントローラはクライアントの特定の MAC アドレスを含む RADIUS 要求パケットを形成し、RADIUS サーバに中継します。

RADIUS サーバは認証を実行し、クライアントが許可されているかどうか、および WLC への応答として ACCESS-ACCEPT または ACCESS-REJECT のいずれかを送信するかどうかをチェックします。

Identity PSK をサポートするために、認証サーバは、認証応答を送信するだけでなく、この特定のクライアントに対して AV Pair パスフレーズを提供します。これは PSK の計算のためにさらに使用されます。

RADIUS サーバは、クライアントに特有のユーザ名、VLAN、QoS などの追加パラメータをこの応答で提供することもできます。単一ユーザが所有している複数のデバイスのためにパスフレーズを同一にしておくこともできます。

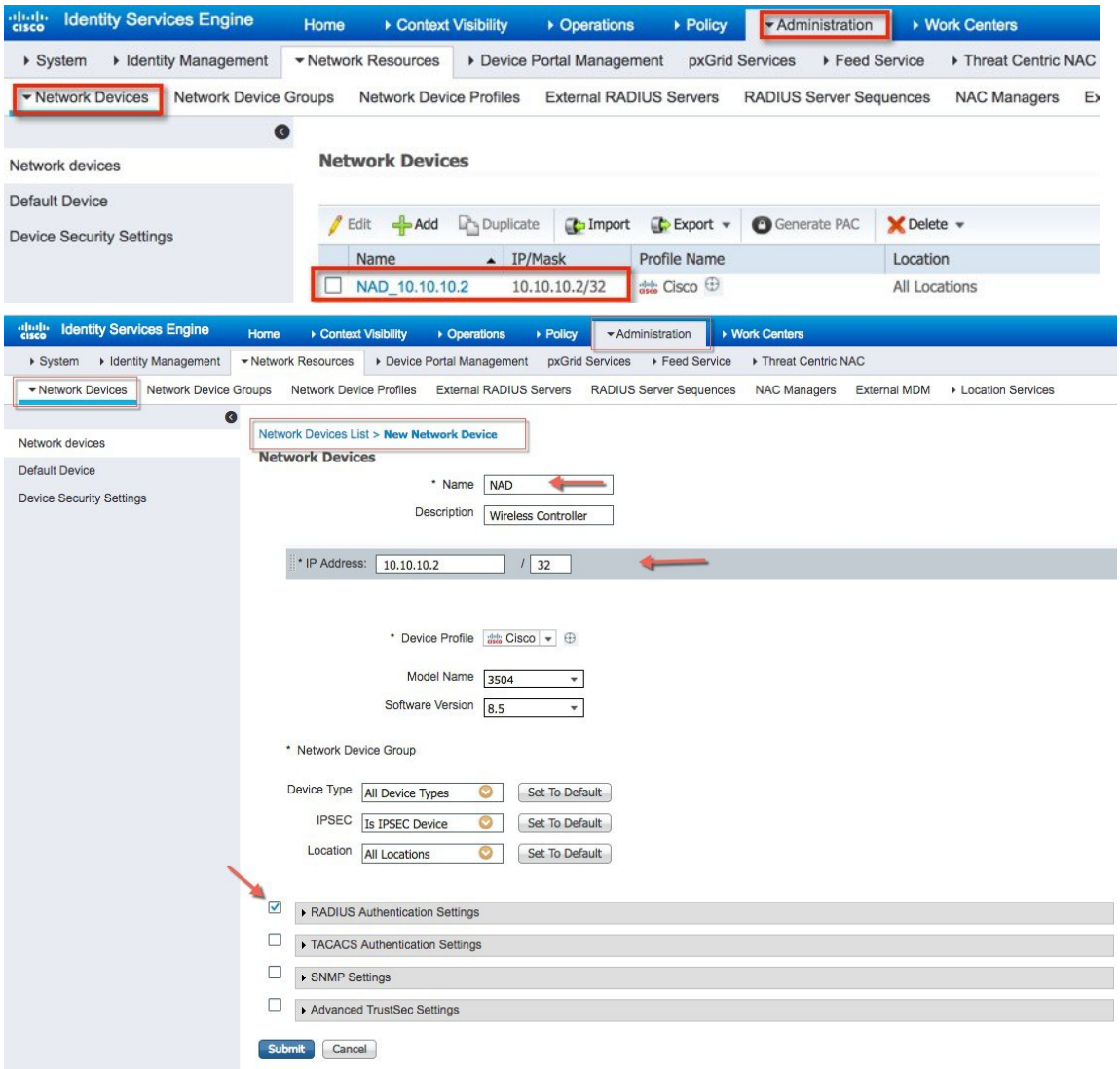


8.5 リリースでの IPSK の設定手順

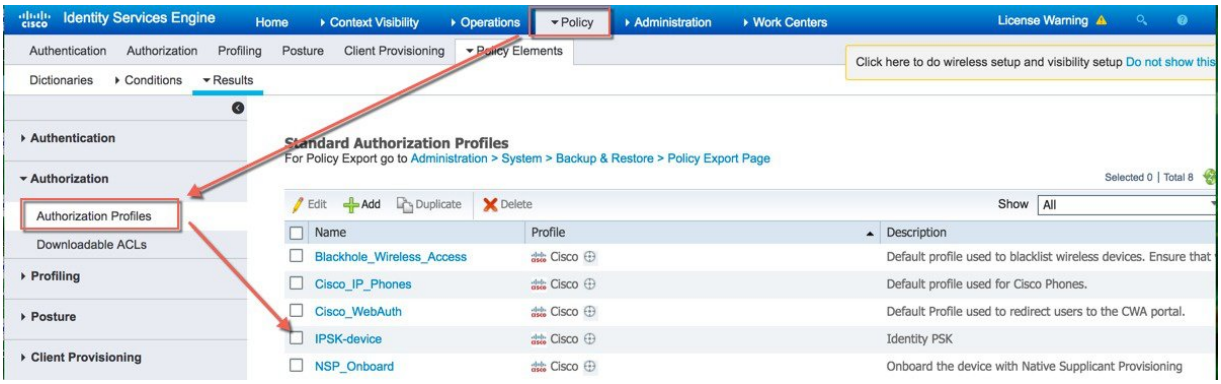
IPSK は、Cisco AV-pair をサポートする AAA サーバで設定できます。この導入ガイドでは、Cisco Identity Service Engine での設定に焦点を合わせます。ISE 2.2 構成手順

手順

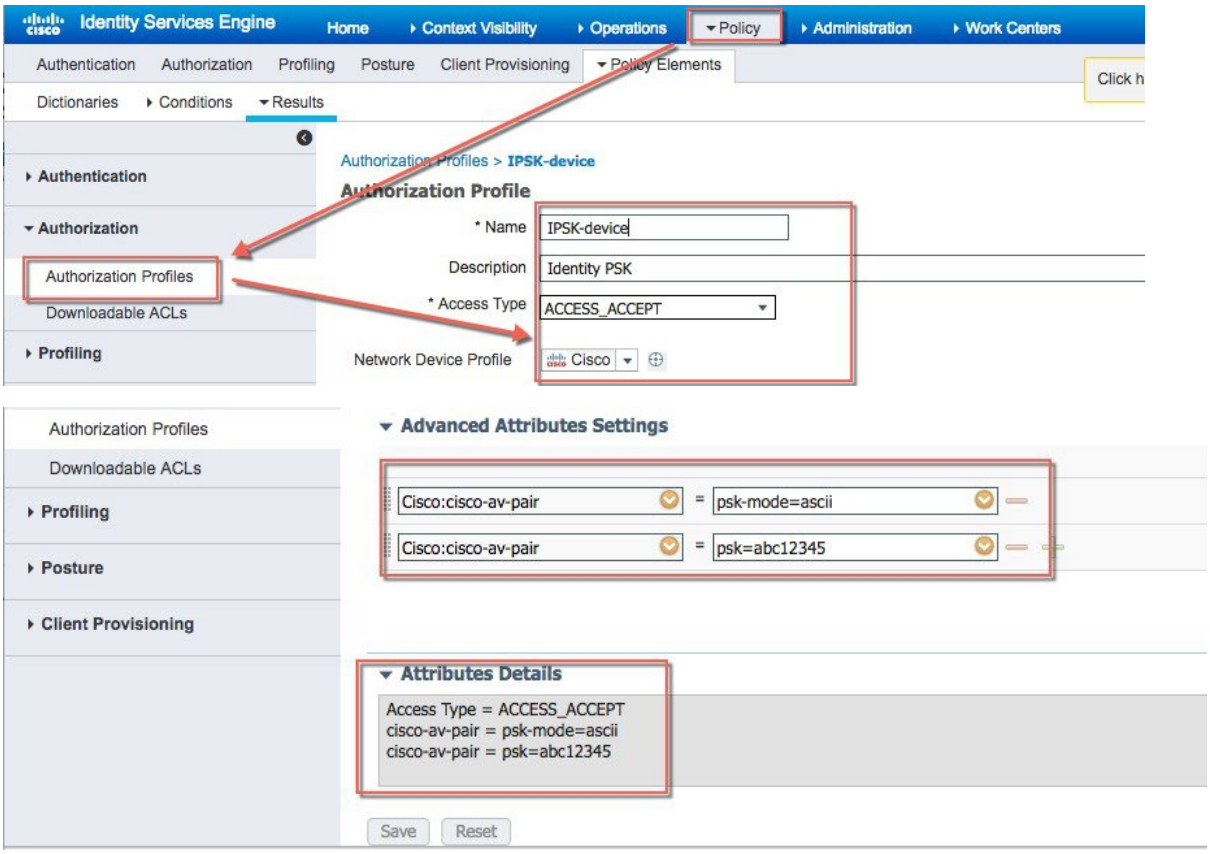
ステップ 1 次のように ISE でテスト対象のワイヤレスコントローラを追加し、[Radius Authentication Setting] で secret password を設定して [Submit] をクリックします。



ステップ 2 以下の例に示すように、[Policy] > [Results] > [Authorization] > [Authorization Profiles] > [IPSK-Device] で Authorization Profile を作成し、確認します。



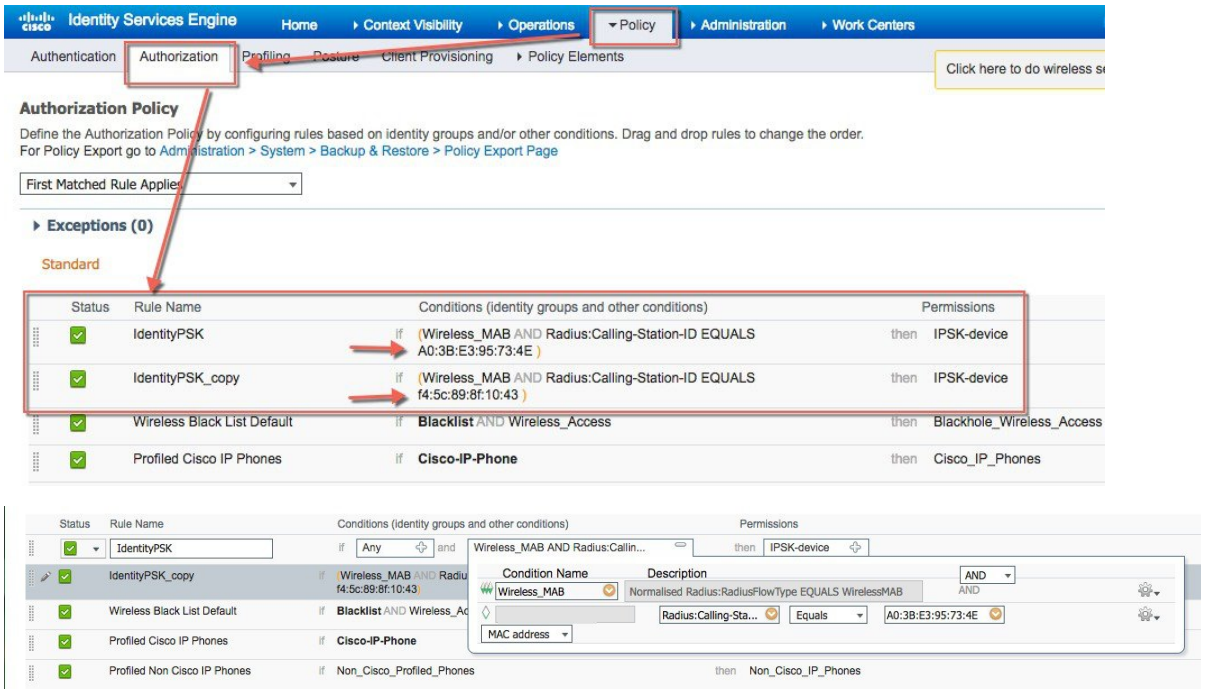
ステップ 3 以下の例に示すように、[Access Type] が [Access_Accept]、cisco-av-pair が psk-mode と psk password で設定した Authorization Profile を作成します。



ステップ 4 次の例に示すように、[Policy] > [Authorization] で IPSK で使用されるすべてのデバイスまたはユーザ MAC アドレスのルールを設定します。必要であれば、複数の MAC アドレス エントリを使用できます。

（注） ルールは、ステップ 3 で作成したプロファイルにリンクされます。

（注） デバイスの Mac アドレスが正しく設定されていることを確認してください。今回の例では、Apple 製 MacBook の Mac アドレスを設定しています。

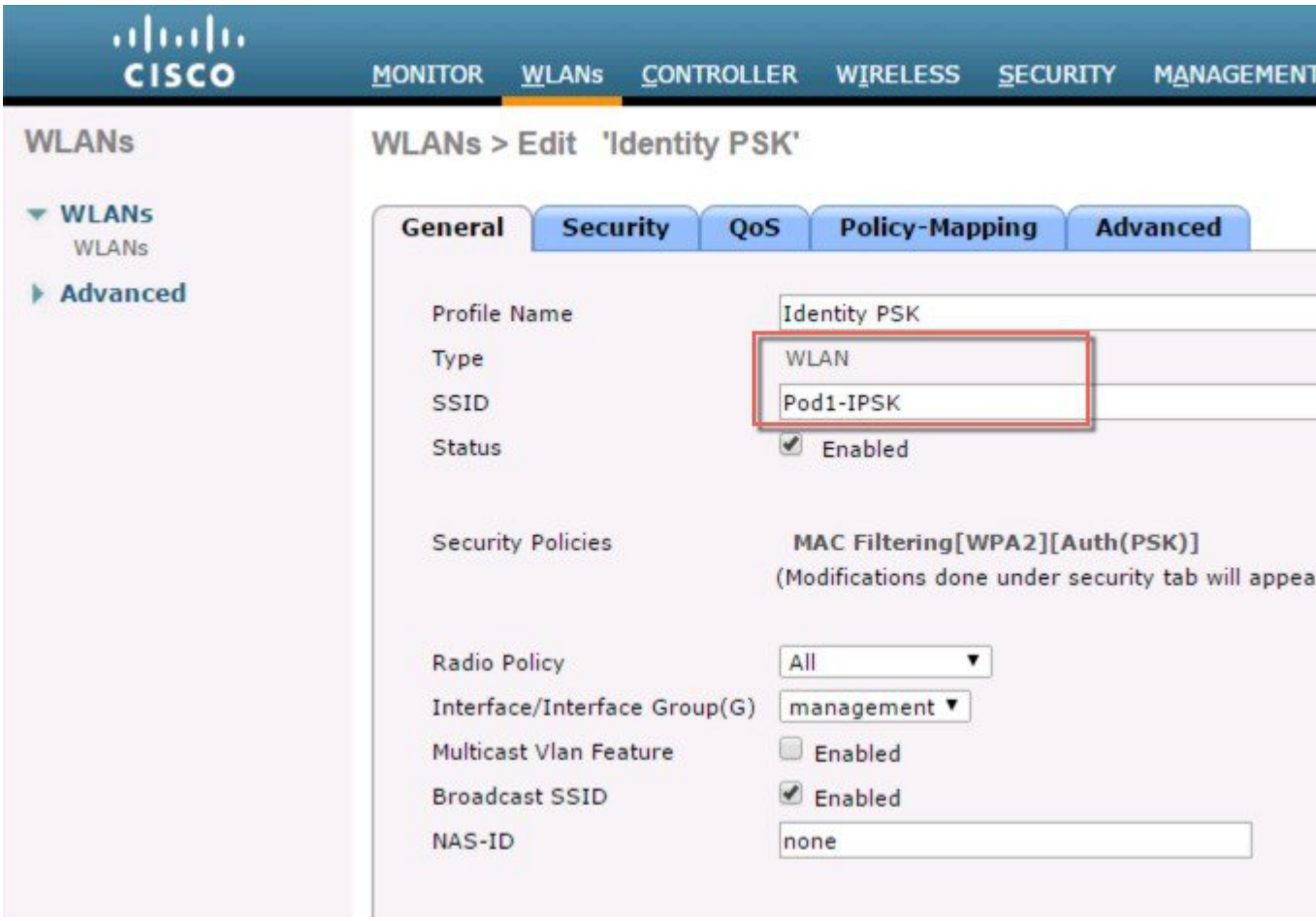


ステップ 5 上記のすべての手順が実行され、すべての設定が適用され保存されたことを確認します。

コントローラ設定の手順

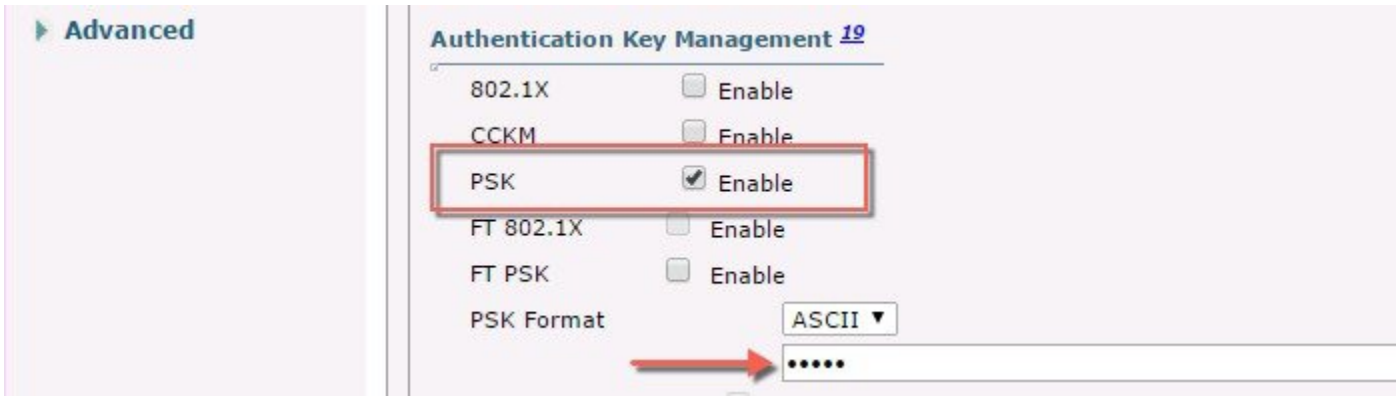
手順

ステップ 1 次の例の Pod1-IPSK に示すように、コントローラの WLAN を作成します。

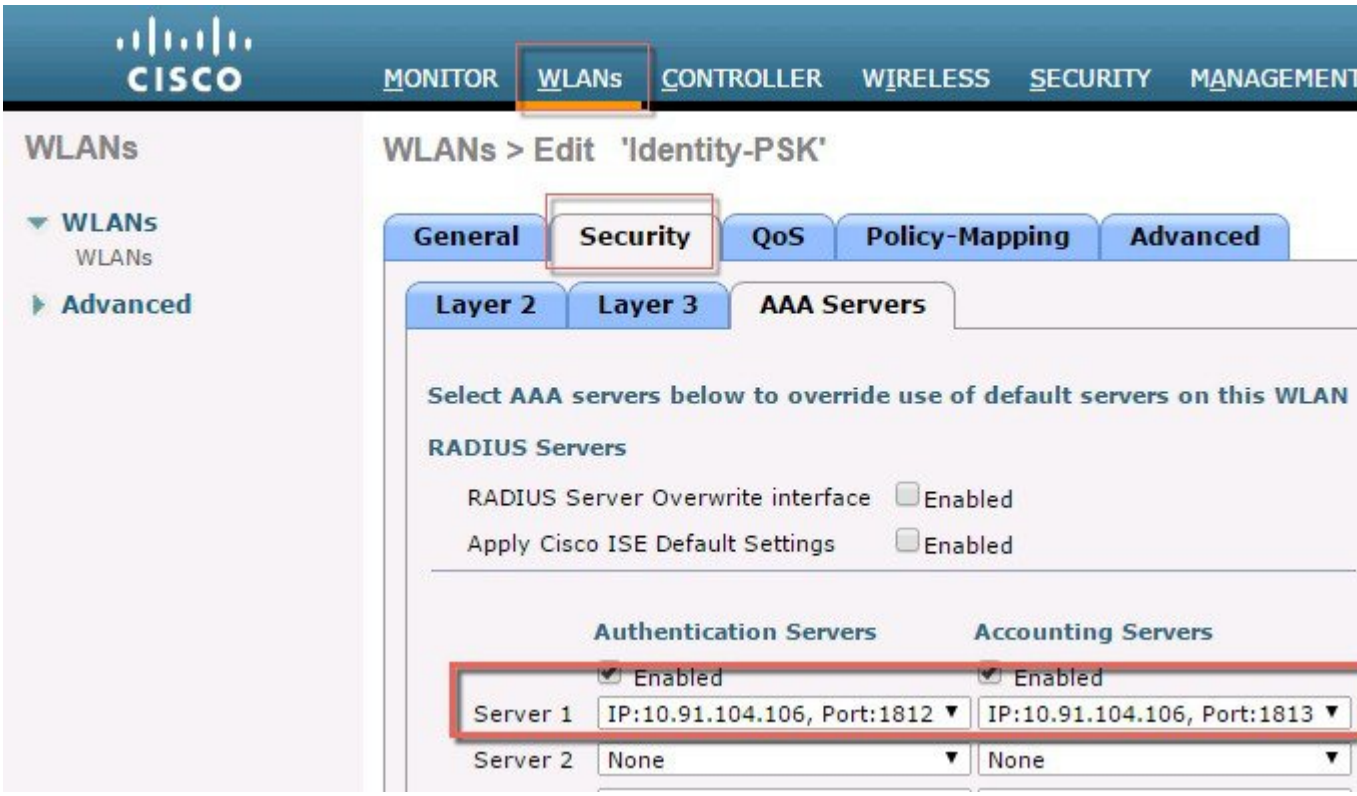


ステップ 2 WLAN でセキュリティとして WPA2/PSK に設定し、**MAC フィルタリング**を有効にします。以下の例では、PSK キーとして **PSK = 12345678** を使用しています。

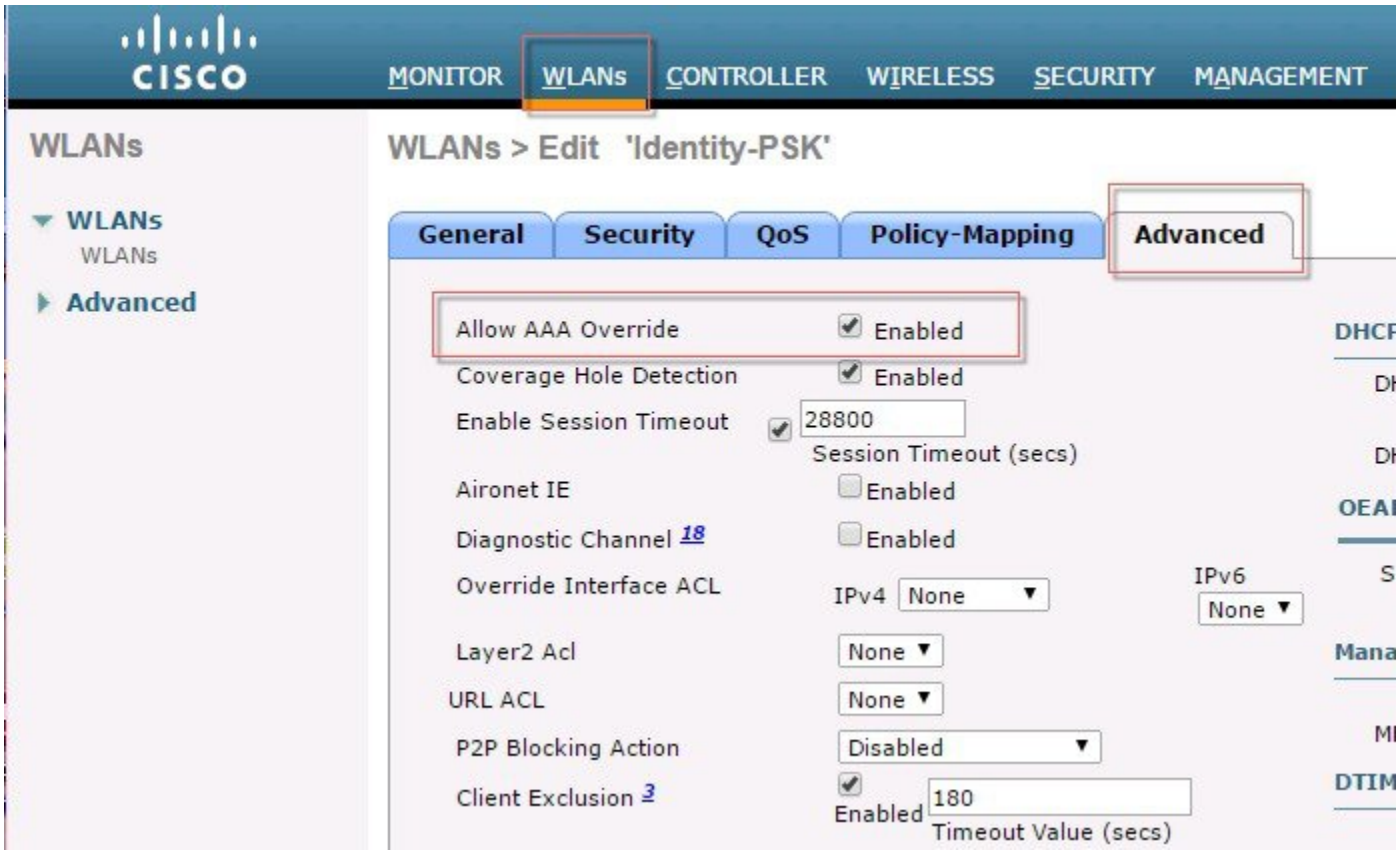
ステップ 3 WLAN でセキュリティとして WPA2/PSK に設定し、PSK を設定します。以下の例では、PSK キーとして **PSK = 12345678** を使用しています。



ステップ 4 WLC で認証サーバを ISE IP アドレスを使用して設定し、上記の手順で作成した WLAN Pod1-IPSK に適用します。この例では、ISE の IP アドレスは 10.91.104.106 です。



ステップ 5 最後に、[WLAN advanced settings] で AAA Override を有効にします。

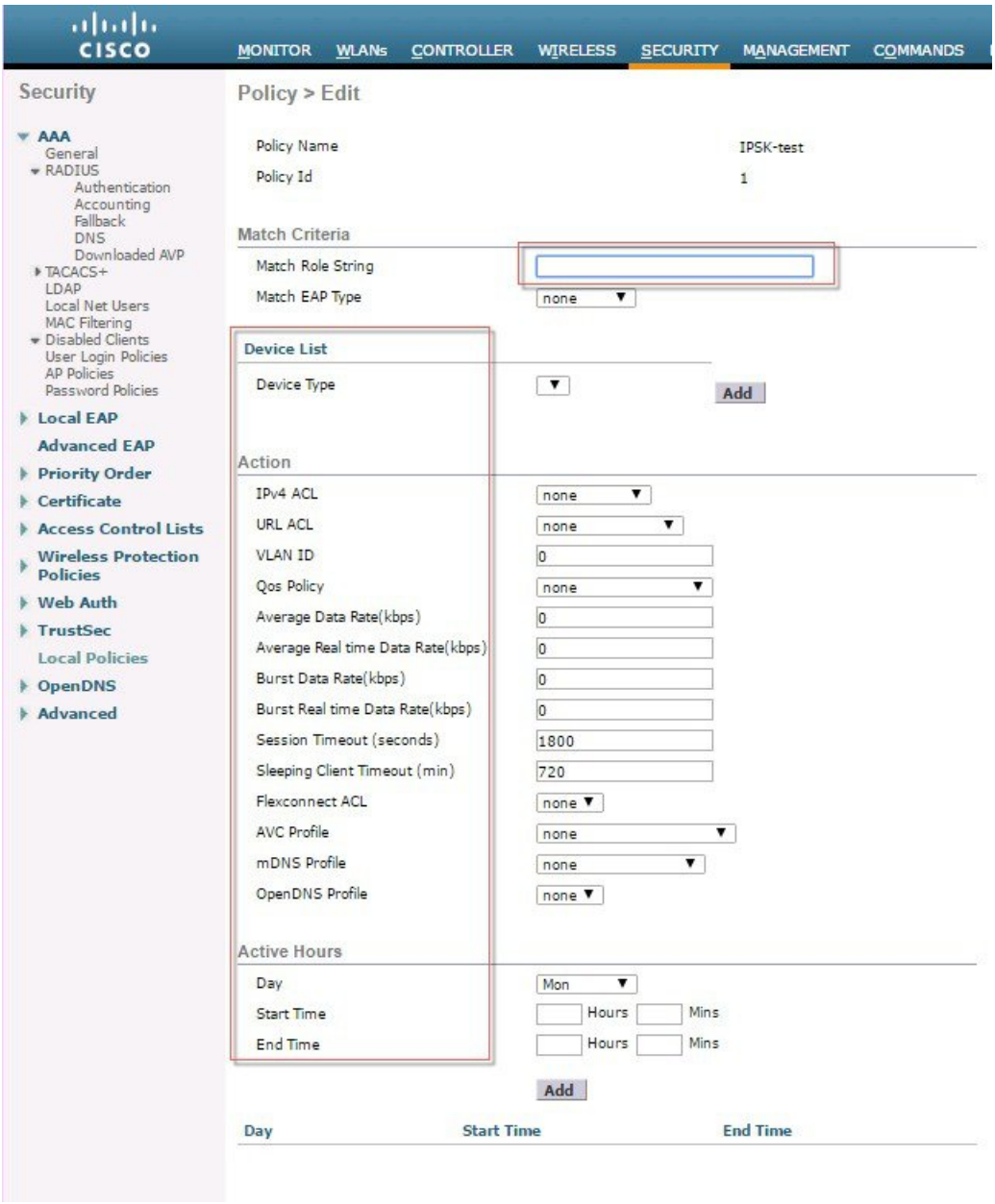


IPSK と組み合わせた WLC ローカル ポリシー

AVC と同じように、mDNS またはオープン DNS プロファイルは、特定のデバイス タイプのクライアントのためにローカル ポリシーにマップできます。IPSK は、コントローラのローカル ポリシーと組み合わせたり、特定の WLAN にマッピングしたりすることもできます。AV-pair=PSK-mode および PSK-password を ISE などの AAA サーバで設定する場合、管理者は、別の AV-pair=role を追加することで、たとえば、教師または学生のグループに対して、その特定のロールに対するローカル ポリシーを設定することもできます。各ローカル ポリシーは異なったプロファイル名、ACL、ロール、デバイス タイプ、および、同じ WLAN でプロファイルにより許可されていないサービスを利用/拒否することができることから、ポリシーを制限/許可する AAA オーバーライドに基づいて、アクティブ時間までも使用して設定できます。

同一の WLAN で IPSK とローカル ポリシーを組み合わせると、多くのさまざまな展開シナリオで制限なく使用できます。

たとえば、学内管理者は、学生が IPSK でログインし、グループ Students に属する学生のみ、特定のアプリケーションに特定の帯域幅と特定のデバイスで、特定の時間アクセスできるローカル ポリシーを適用するように設定できます。IPSK とローカル ポリシーを組み合わせることで、実質的に無制限の多様な機能を使用できます。



WLC のプロファイリングとポリシー エンジンの概要

Cisco では、ISE を介してデバイスの識別、オンボーディング、ポスチャ、およびポリシーを実行する、豊富な機能を提供しています。WLC では新たに、ネットワーク上のエンドデバイスを識別するために DHCP、HTTP などのプロトコルに基づくデバイスのプロファイリングを行います。ユーザは、デバイス ベースのポリシーを設定し、ネットワーク上のユーザごと、またはデバイスポリシーごとに適用できます。WLC では、ユーザごと、またはデバイスエンドポイントごとに基づく統計情報とデバイスごとの適切なポリシーも表示できます。

BYOD（Bring Your Own Device）では、この機能がネットワーク上のさまざまなデバイスの理解に影響します。この機能を使うことで、WLC 自身で小規模に BYOD を実装できます。

範囲と目的

このセクションでは、AireOS8.5 コードを動かしている Cisco WLC でプロファイリングとポリシーを設定して実行します。

プロファイリングとポリシーの適用は、2 つの異なるコンポーネントとして設定します。WLC での設定は、前のセクションで設定したように、IPSK セキュリティを使用してネットワークに参加するクライアントに特有な定義済みパラメータに基づきます。対象のポリシー属性は次のとおりです。

1. Role：ユーザが属するユーザ タイプまたはユーザ グループを定義
2. PSK-mode：ASCII

   PSK-password：特定の PSK パスワードとデバイスの MAC アドレスとの一致

   たとえば、学生、従業員など
3. Device：デバイスのタイプを定義

   たとえば、Windows マシン、スマートフォン、iPad や iPhone などの Apple デバイス
4. Time of day：設定で、エンドポイントがネットワーク上で許可される時間を定義

上記のパラメータはポリシー一致属性として設定できます。WLC では、上記のパラメータに（エンドポイントごとに）一致する通信を検出すると、ポリシーを適用します。ポリシーの適用は次のようなセッション属性に基づいています。

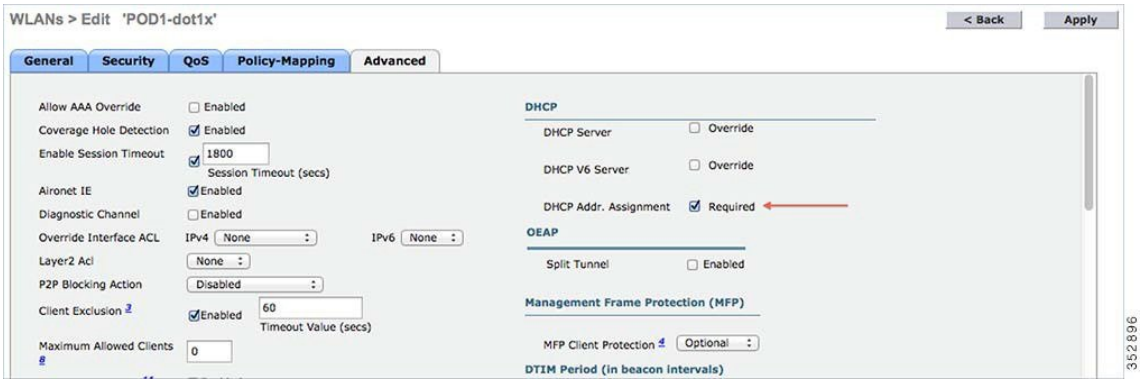
- VLAN
- ACL
- セッション タイムアウト
- QoS
- スリープ状態のクライアント
- FlexConnect ACL
- AVC プロファイル
- mDNS プロファイル
- オープン DNS プロファイル
- セキュリティ グループ タグ

ユーザは、これらのポリシーを設定し、指定したポリシーをエンドポイントに適用できます。ワイヤレス クライアントは、MAC アドレス、MAC OUI、DHCP、HTTP ユーザ エージェント（HTTP プロファイリングを成功させるためには、Internet へのアクセスが必要）に基づいて、プロファイリングされます。WLC はこれらの属性と定義済みの分類プロファイルを使用して、デバイスを識別します。

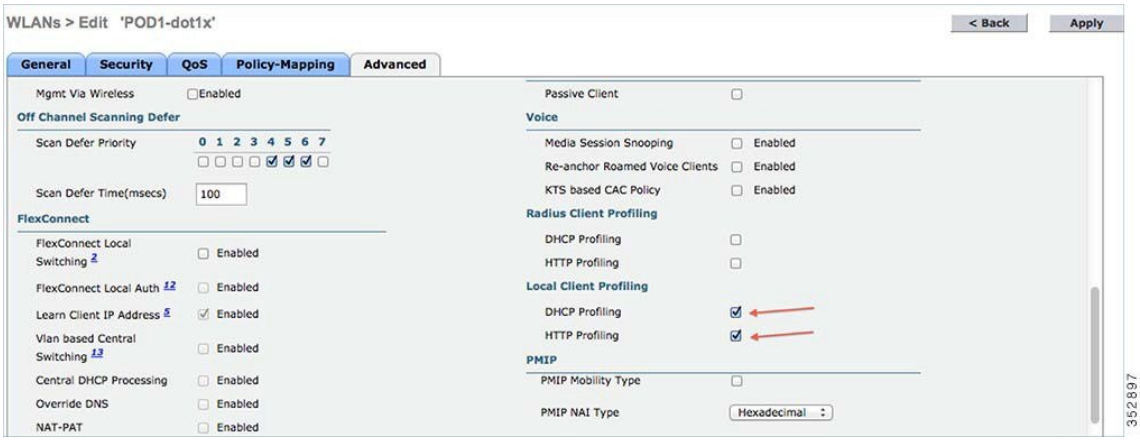
プロファイリングおよびポリシーの設定

手順

ステップ 1 WLAN でデバイス プロファイリングを設定するには、ネイティブ プロファイリングおよびポリシーを設定する対象となる特定の WLAN に移動して、[Advanced] をクリックします。[Allow AAA Override] が有効になっている場合は、無効にします。[DHCP] の [DHCP Addr. **Assignment**]。

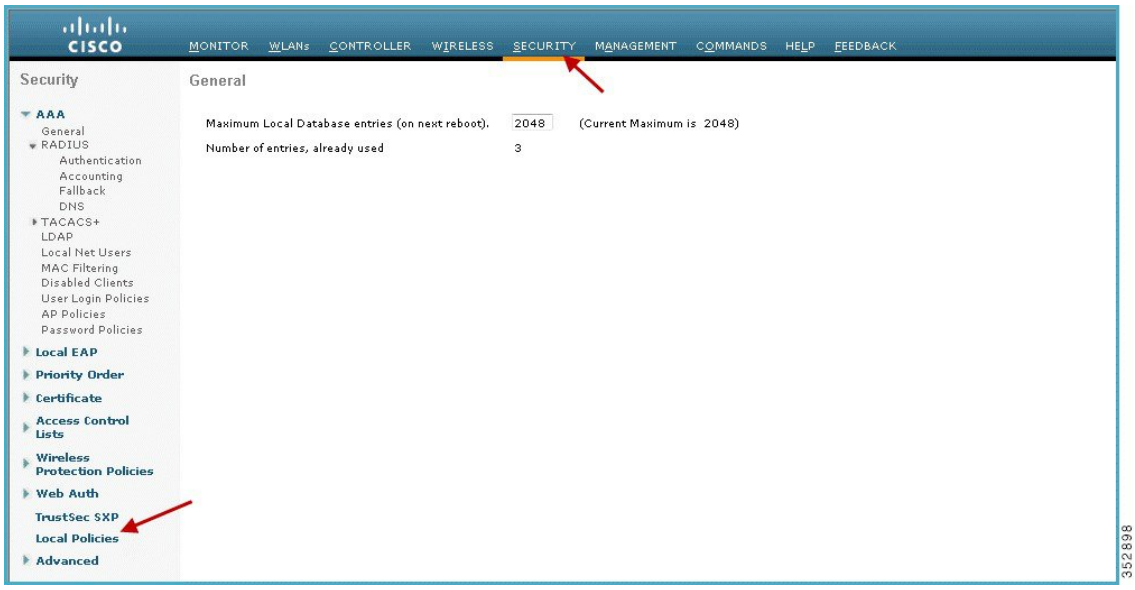


ステップ 2 [DHCP Required] オプションを有効にした後、スクロール ダウンし、[Local Client Profiling] で、[DHCP Profiling] と [HTTP Profiling] が有効でない場合は有効にして、[Apply] をクリックします。



WLC GUI から WLAN でポリシーを作成

ステップ 3 プロファイルを設定したら、ローカル ポリシーの作成と WLAN での適用に進みます。WLC メニュー バーで、[Security] > [Local Policies] に移動すると、ポリシー リストの作成画面が表示されます。



ステップ 4 [Local Policy List] で、[New] をクリックして、ポリシー名を作成します。この例では、**teacher-LP** をポリシー名として使用していますが、任意の名前を使用して独自のポリシーを定義することもできます。

ポリシー名を設定した後、[Role]、[EAP Type]、[DeviceType] が一致するようなポリシーを作成できます。また、一致条件に関連する必要なアクションを定義できます。

ここでは、[User Role] と [Device Type] を [Match Criteria] に使用していますが、必要に応じて任意のタイプを使用できます。

（注） [Match Role string] が AAA で定義されたロール名と同じであることを確認してください。この例では、「teacher」と定義されています。

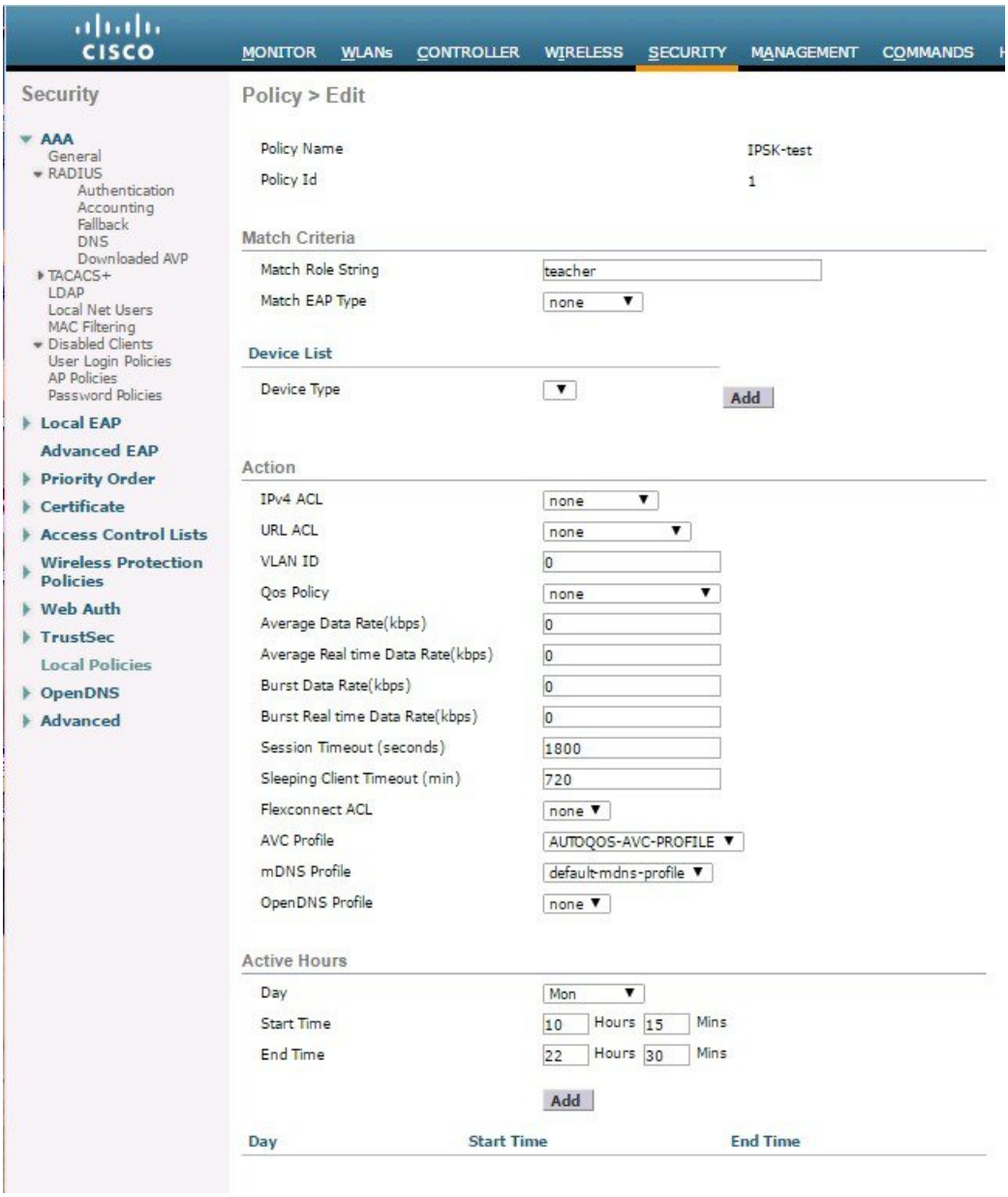
ステップ 5 [User Role] を入力し、[Apply] をクリックします。ここではロール名「teacher」が例として使用されています。

ステップ 6 ユーザ デバイスに基づいてポリシーを適用するには、[Device List] で、[Device Type] ドロップダウン リストから、ポリシーを適用する**デバイス タイプ**を選択し、[Add] をクリックします。

ここで、[Match Criteria] に対し、デバイス タイプとして [Apple-iPad] を使用しています。Apple-iPhone やその他の Apple デバイスも同様に [Device Type] ドロップ ダウン リストから追加できます。

（注） 任意のデバイス タイプと一致させない場合は、[Device Type] オプションを設定しないでください。

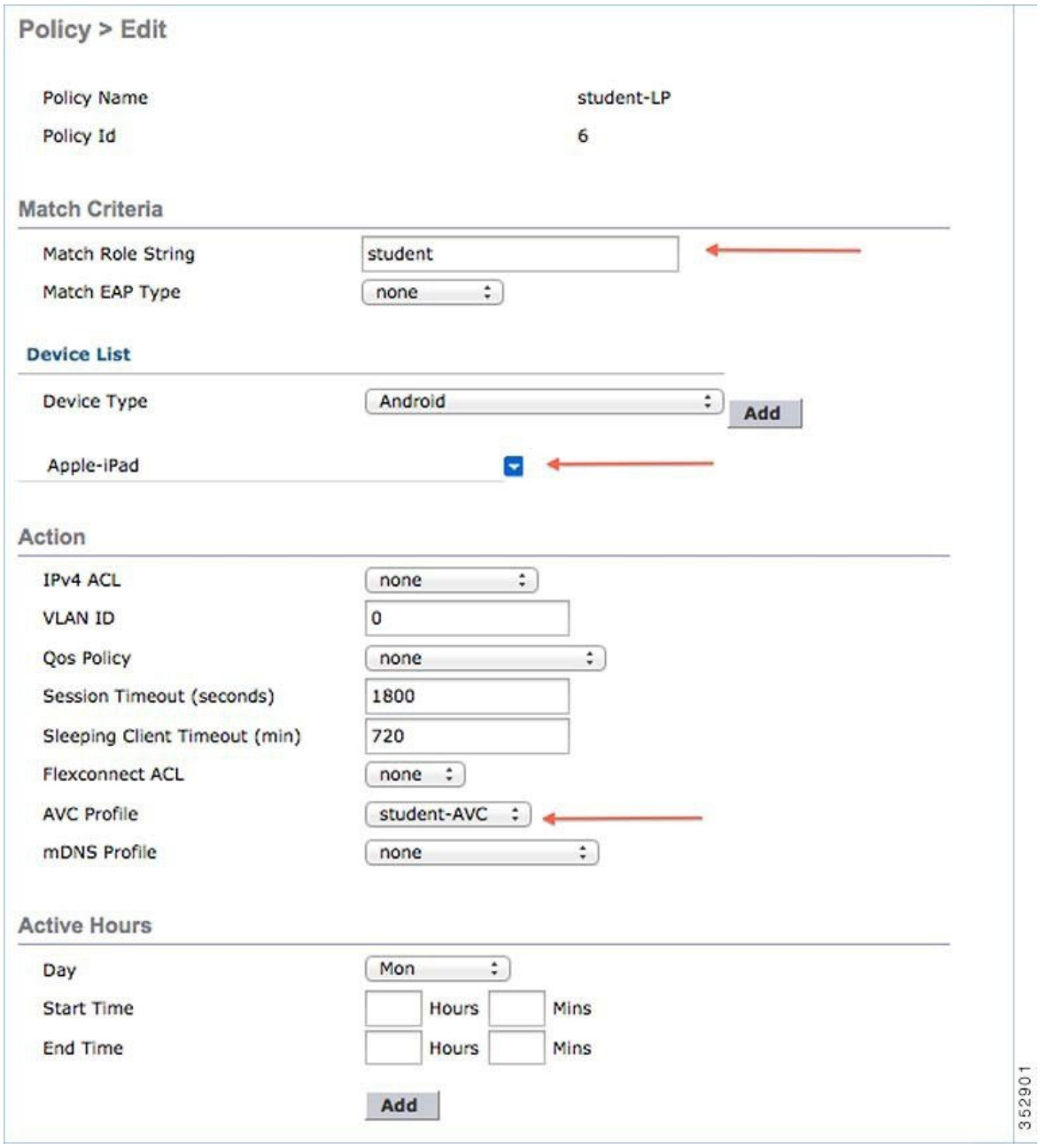
ステップ 7 適切なアクションを適用するには、[Action] のパラメータから選択して、ポリシーを適用します。最後のセクションで定義されている AVC プロファイルを選択します。



（注） ローカル ポリシーの設定の詳細についてはリンク先を参照してください http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-3/config-guide/b_cg83/b_cg83_chapter_01110.html

ステップ 8 ユーザは、1 つ以上のローカル ポリシーを作成し、「student-LP」の学生に適用できます。

（注） [Match Role string] が AAA/Radius サーバで定義されたロール名と同じであることを確認してください。

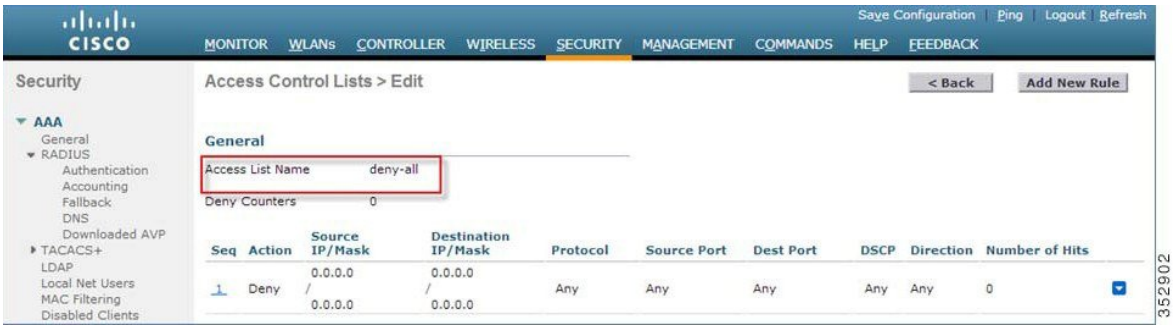


ステップ 9 その他のデバイスのデフォルトのローカル ポリシーを作成します。

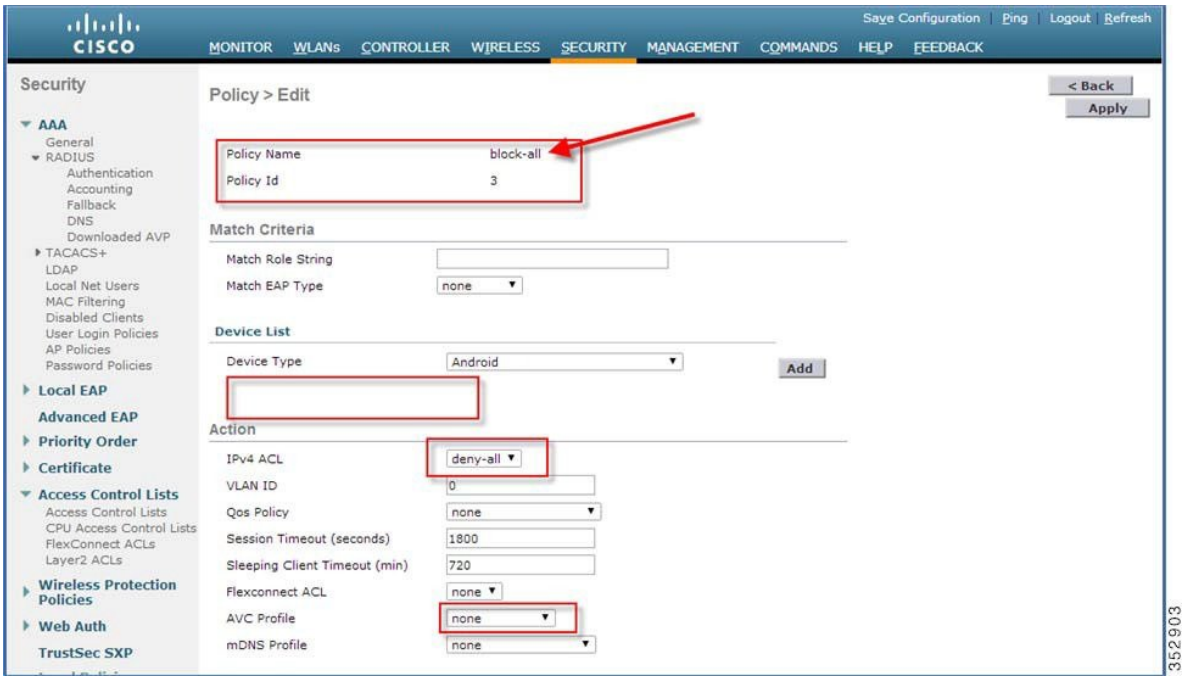
ローカル ポリシーに他の ACL が適用されていない場合、Apple-iPad 以外の他のデバイスは、すべてのポリシーの最終フィルタ機能が [Allow all] なので、アプリケーションにアクセスできます。

Apple-iPad を除くすべてのデバイスのすべてのアプリケーションをブロックするために、[deny all] ACL を作成してローカル ポリシーに適用し、その後、WLAN にそのポリシーを適用します。下記のスクリーンショットから設定例を参照してください。

すべての IPv4 フローをブロックする ACL を作成します。



ローカル ポリシー [Block-all] を作成し、[deny all] ACL をこれに適用し、デバイス ロールやプロファイルは選択しないでください。

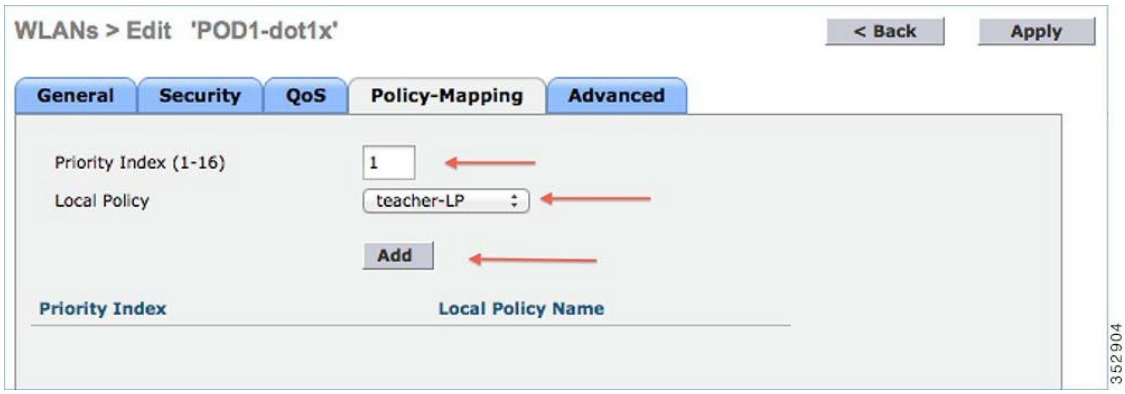


WLAN でのポリシーのマッピング

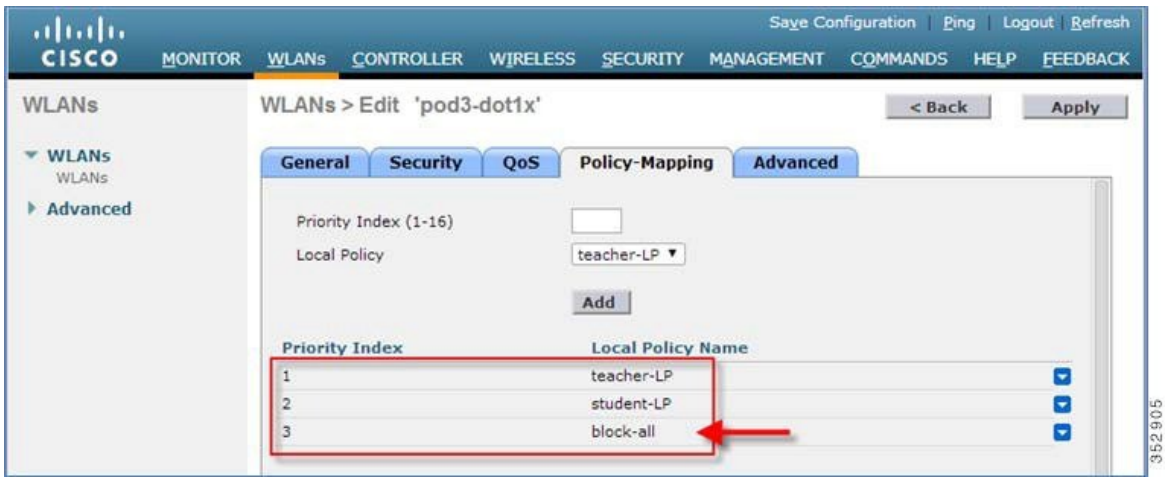
手順

ステップ 1 WLC メニューバーから [WLANs] に移動し、ポリシーを設定したい [WLAN ID] をクリックします。WLAN の [Edit] メニューから [Policy-Mapping] タブをクリックします。

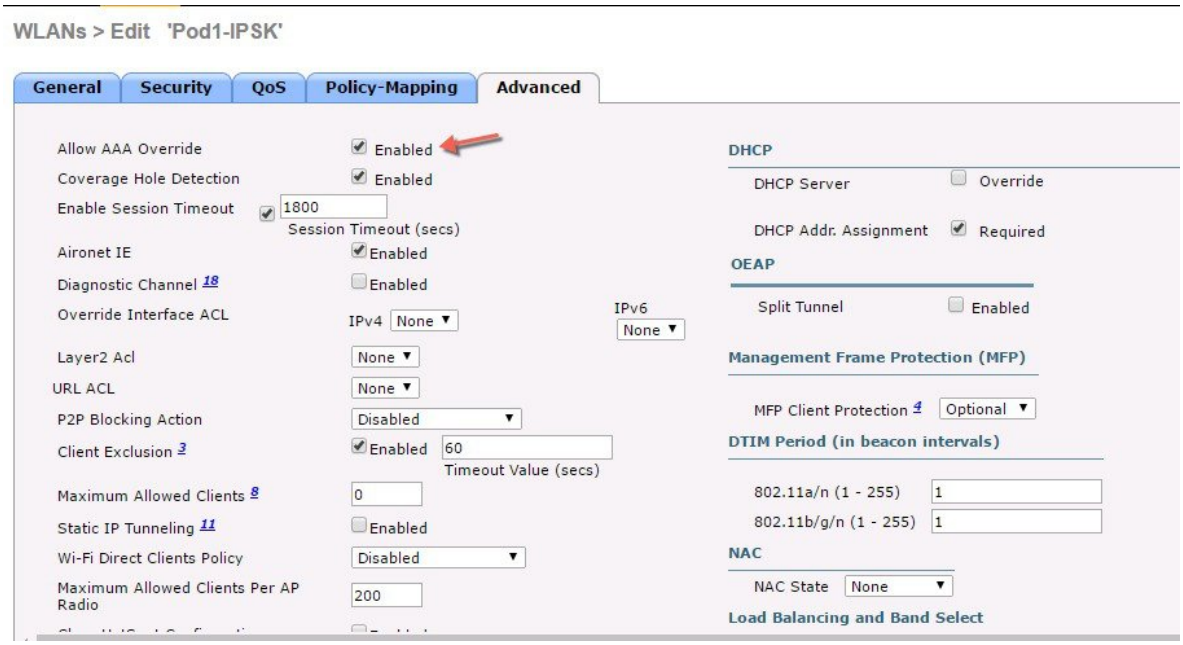
[Priority Index] で、1 ～ 16 から任意の値を設定します。[Local Policy] ドロップダウン リストから、すでに作成したポリシーを選択します。WLAN でポリシーを適用するには、[Add] をクリックします。ポリシーが追加されます。



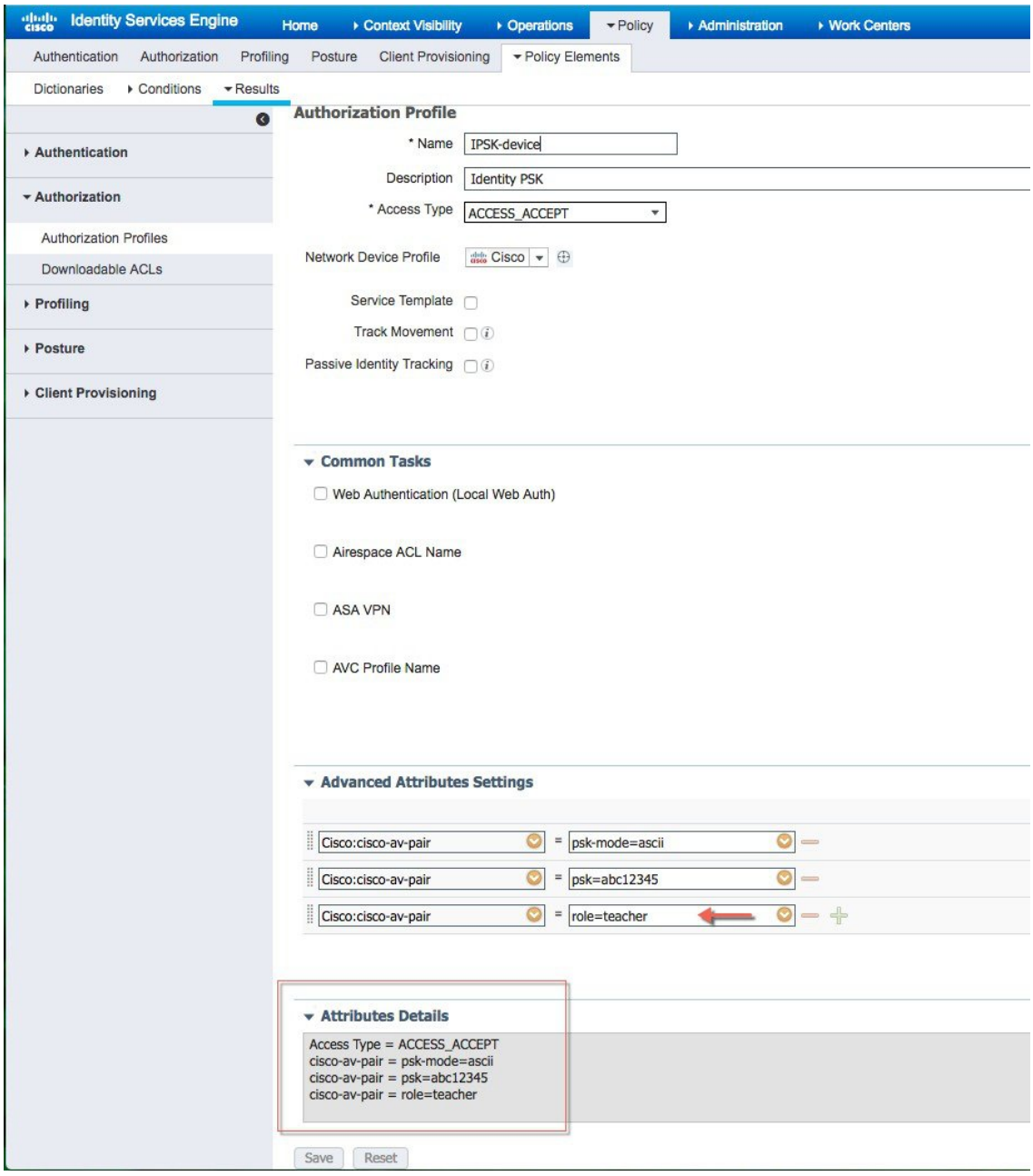
ステップ 2 適切なポリシーを WLAN の [Policy-Mapping] に追加します。



ステップ 3 [Advanced] タブで、[Allow AAA Override] が IPSK のために設定されていて有効な場合は、無効にします。



ステップ 4 AAA ロールが正しく設定されていることを確認します。つまり、AAA サーバでのロール名はローカル ポリシーで定義されている [Role String] と一致する必要があります。以下の例は、cisco-av-pair role=teacher で設定されている Cisco ISE サーバです。role=students に対しても同じ設定です。



エンド ユーザ デバイスの設定

手順

ステップ 1 MAC アドレスが ISE で設定されているエンド ユーザ デバイスで、WLAN Pod1-IPSK に接続し、そのデバイスの IPSK パスワード **abc12345** を入力するか、または ISE で設定されたようにします。

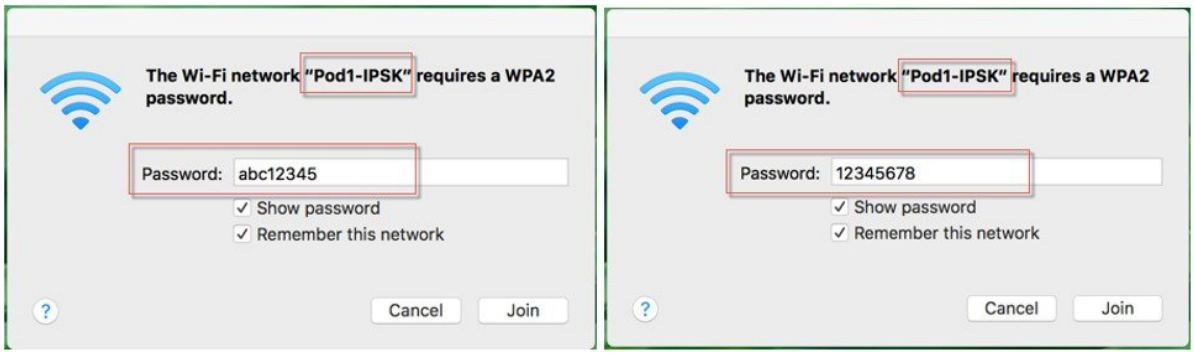
---接続に**成功**しました

ステップ 2 同じ WLAN に PSK **12345678** で接続します。

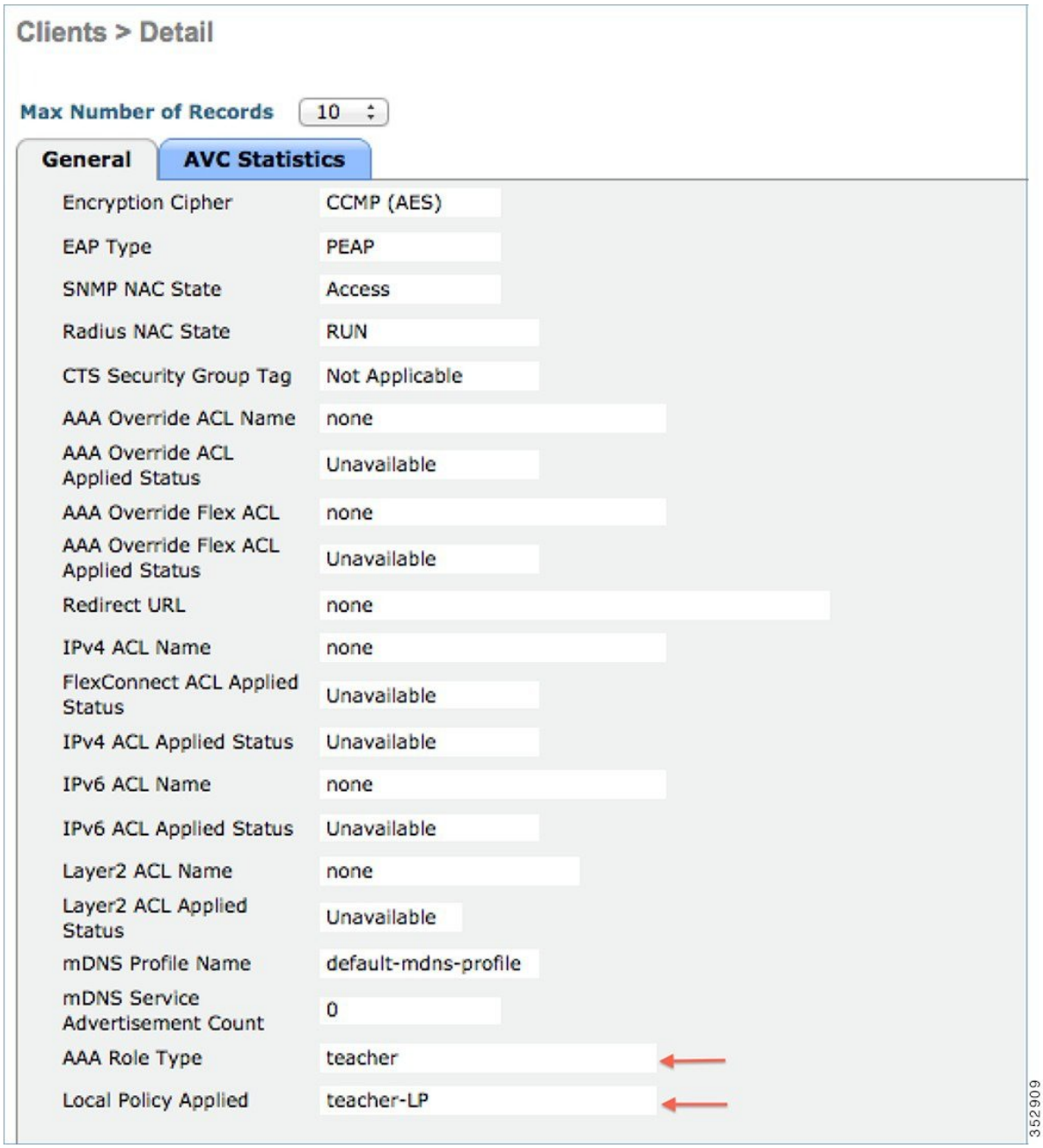
---接続に**失敗**します

ステップ 3 同じ WLAN に MAC アドレスが ISE に設定されていないデバイスと **PSK 12345678** で接続します。

----接続に**成功**しました



ステップ 4 WLC GUI から、ポリシーの適用を確認するために、[Monitor] > [Clients] に移動して [Client MAC address] をクリックします。



まとめ

- Mac フィルタリングおよび AAA Override が有効化され、ISE が設定されているコントローラは、IPSK を設定したデバイスが ISE で設定された MAC アドレスを使用して WLAN に接続することを許可します。

- ISE で設定された MAC アドレスを持つデバイスは、WLAN に通常の PSK で接続できず、そのデバイスのために設定された IPSK でのみ接続できます。
- ISE で設定された MAC アドレスを持たないデバイスは、通常の PSK のみで WLAN に接続できます。
- IPSK は、FlexConnect local switching ではサポートされません。AAA サーバで AV-Pair のサポートが必要です。
- IPSK は、FlexConnect Group ではサポートされません。
- IPSK は FSR をサポートし、高速ローミングの際に、ローミングごとの RADIUS 接続を避けるため、キーキャッシングを実行します。
- 特定のスケジュールされた時間に IPSK の設定を有効にするには、RADIUS 応答の radius session-timeout 属性を使用できます。

CLI コマンドを使用した IPSK の設定

次の既知の CLI は、この機能のために使用されます。

```
config wlan mac-filtering enable <wlanId>
config wlan aaa-override enable <wlanId>
config wlan security wpa akm psk enable <wlanId>
config wlan security wpa akm psk set-key <ascii/hex> <key> <wlanId>
```

既知の show コマンドは、WLAN およびクライアントの設定を表示します。

```
show wlan <wlanId>
show client detail <clientMac>
```

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/