FlexConnect 向けワイヤレス BYOD 導入ガイド

内容

概要

モバイル デバイスは、徐々にコンピュータに近づいて強力になり、消費者間での人気が増しています。何百万ものデバイスが、ユーザのコミュニケーションとコラボレーションを可能にするために、高速 Wi-Fi を搭載して消費者に販売されます。消費者は、これらのモバイル デバイスがもたらす生産性の向上に慣れて、個人的経験を作業空間に持ち込もうとしています。これにより、職場への個人所有デバイス持ち込み（BYOD）ソリューションの機能的な必要が生じています。

このドキュメントでは、BYOD ソリューションのブランチ導入について説明します。従業員は、自分の新しい iPad を使用して企業のサービス セット識別子（SSID）に接続し、自己登録ポータルにリダイレクトされます。Cisco Identity Services Engine（ISE）は、ユーザを企業の Active Directory（AD）に対して認証し、組み込みの iPad MAC アドレスとユーザ名が含まれた証明書を

、dot1x 接続の方法として Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）の使用を強制するサプリカント プロファイルとともに iPad にダウンロードします。ISE での許可ポリシーに基づいて、ユーザは dot1x を使用して接続し、適切なリソースへのアクセスを取得します。

ソフトウェア リリース 7.2.110.0 より前までは、シスコ ワイヤレス LAN コントローラの ISE 機能は FlexConnect アクセス ポイント（AP）を介して関連付けるローカル スイッチング クライアントをサポートしていませんでした。リリース 7.2.110.0 で導入されたこれらの ISE 機能は、ローカル スイッチングと中央で認証されたクライアントのために FlexConnect AP でサポートされるようになりました。さらに、ISE 1.1.1 と統合されたリリース 7.2.110.0 では、次のワイヤレス用（次のものに限定されません）の BYOD ソリューション機能が提供されます。

- デバイスのプロファイリングとポスチャ
- デバイスの登録とサプリカントのプロビジョニング
- 個人用デバイスのオンボーディング（iOS または Android デバイスのプロビジョニング）

注：PCまたはMacワイヤレスラップトップやワークステーションなどの他のデバイスはサポートされていますが、このガイドには含まれていません。

前提条件

要件

このドキュメントに特有の要件はありません。

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。

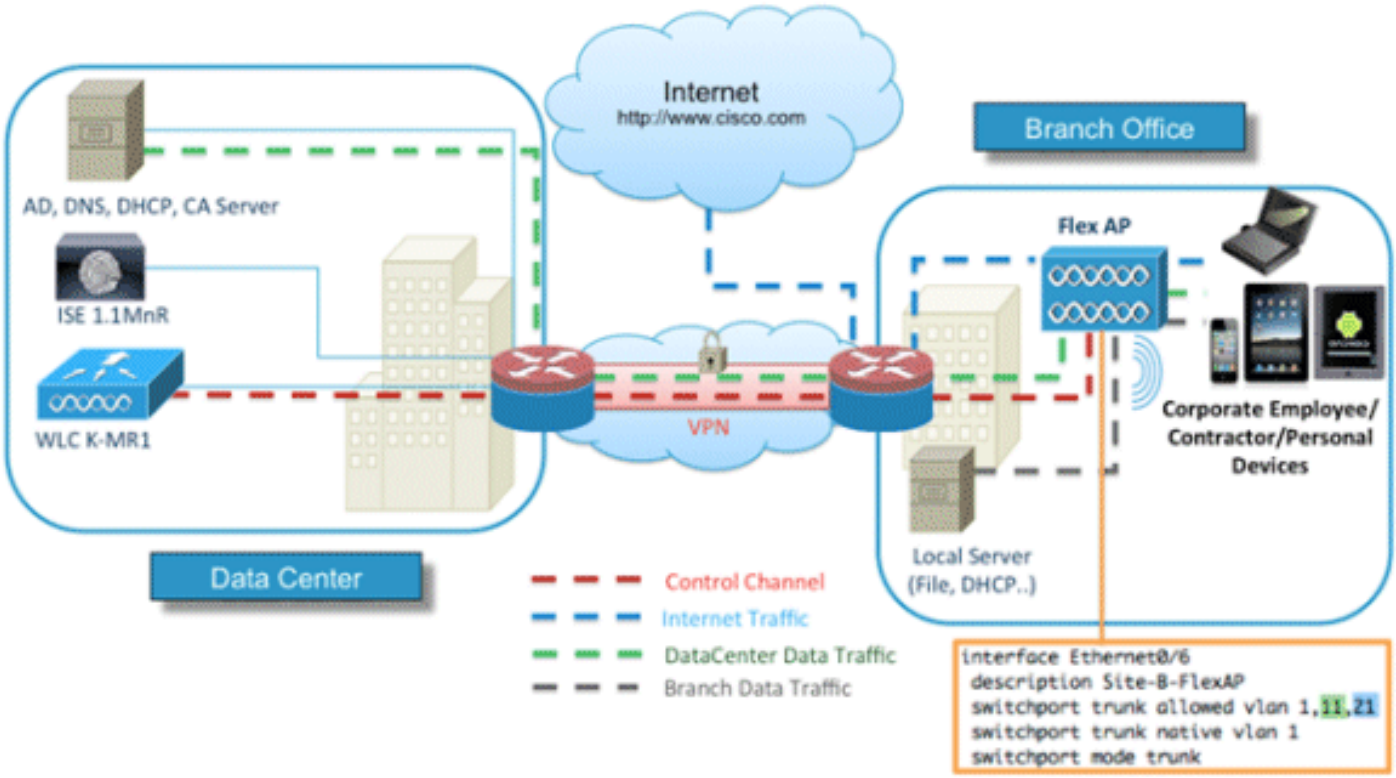
- Cisco Catalyst スイッチ
- Cisco ワイヤレス LAN（WLAN）コントローラ
- Cisco WLAN コントローラ（WLC）ソフトウェア リリース 7.2.110.0 以降
- FlexConnect モードの 802.11n AP
- Cisco ISE ソフトウェア リリース 1.1.1 以降
- Windows 2008 AD。認証局（CA）のインストール済み
- DHCP サーバ
- ドメイン ネーム システム（DNS）サーバ
- Network Time Protocol（NTP）
- ワイヤレス クライアント ラップトップ、スマートフォン、タブレット（Apple iOS、Android、Windows、Mac）

注：このソフトウェアリリースに関する重要な情報については、『Cisco Wireless LAN ControllerとLightweightアクセスポイントリリース7.2.110.0のリリースノート』を参照してください。ソフトウェアをロードしてテストする前に、Cisco.com のサイトにログインして最新のリリース ノートを参照してください。

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

トポロジ

これらの機能を正しく実装してテストするには、次の図に示すような最小限のネットワーク設定が必要です。



このシミュレーションでは、FlexConnect AP を備えたネットワーク、ローカル DHCP、DNS、WLC、および ISE を含むローカル サイトまたはリモート サイトが必要です。FlexConnect AP は、複数の VLAN を使用したローカル スイッチングをテストするためにトランクに接続されています。

デバイスの登録とサプリカントのプロビジョニング

dot1x 認証用にネイティブ サプリカントをプロビジョニングするには、デバイスを登録する必要があります。正しい認証ポリシーに基づいて、ユーザはゲスト ページにリダイレクトされ、そのユーザの従業員クレデンシャルを使用して認証されます。ユーザにはデバイス登録ページが表示され、デバイス情報を入力するよう求められます。デバイスのプロビジョニング プロセスが開始します。オペレーティング システム（OS）がプロビジョニングでサポートされていない場合、そのデバイスを MAC Authentication Bypass（MAB）アクセス用にマークするために、ユーザは資産登録ポータルにリダイレクトされます。OS がサポートされている場合、登録プロセスが開始され、dot1x 認証のためにデバイスのネイティブ サプリカントが設定されます。

資産登録ポータル

資産登録ポータルは、従業員が認証と登録プロセスによってエンドポイントのオンボーディングを開始できるようにする ISE プラットフォームの要素です。

管理者は、[endpoints identities] ページから資産を削除できます。それぞれの従業員は、登録した資産の編集、削除、およびブラックリストへの登録を行うことができます。ブラックリストに登録されたエンドポイントはブラックリスト ID グループに割り当てられ、ブラックリストに登録されたエンドポイントによるネットワークへのアクセスを防止するために許可ポリシーが作成されます。

自己登録ポータル

中央 Web 認証（CWA）フローでは、従業員は、クレデンシャルを入力し、認証してから、登録する特定の資産の特性の入力に進むことができるポータルにリダイレクトされます。このポータルは、自己プロビジョニング ポータルと呼ばれ、デバイス登録ポータルと似ています。ここでは、従業員は MAC アドレスと、エンドポイントのわかりやすい説明を入力できます。

認証とプロビジョニング

従業員が自己登録ポータルを選択すると、プロビジョニング フェーズに進むために、有効な一連の従業員クレデンシャルを指定するよう求められます。正常に認証されると、エンドポイントをエンドポイント データベースにプロビジョニングでき、エンドポイントの証明書が生成されます。ページ上のリンクを使用して、従業員は Supplicant Pilot Wizard（SPW）をダウンロードできます。

> **注**:BYODの最新のFlexConnect機能マトリックスを確認するには、シスコの記事「FlexConnect機能マトリックス」を参照してください。

iOS（iPhone/iPad/iPod）のプロビジョニング

EAP-TLS 設定の場合、ISE は Apple の Over-the-Air（OTA）登録プロセスに従います。

- 正常に認証されると、評価エンジンが、サプリカント プロファイルになるクライアントのプロビジョニング ポリシーを評価します。
- サプリカント プロファイルが EAP-TLS 設定用である場合、OTA プロセスは、ISE が自己署名を使用しているかまたは不明な CA によって署名されたかを判別します。いずれかの条件に当てはまる場合、登録プロセスを開始する前に、ユーザは ISE または CA のいずれかの証明書をダウンロードするよう求められます。
- その他の EAP 方法の場合、ISE は単に認証の成功時に最終プロファイルを適用します。

Android のプロビジョニング

セキュリティ上の考慮事項により、Android エージェントは Android マーケットプレイス サイトからダウンロードする必要があり、ISE からはプロビジョニングできません。シスコでは、Cisco Android マーケットプレイス パブリッシャ アカウントを使用して、ウィザードのリリース候補バージョンを Android マーケットプレイスにアップロードします。

Android プロビジョニング プロセスは次のとおりです。

1. シスコは、ソフトウェア開発キット（SDK）を使用して、拡張子 .apk の付いた Android パッケージを作成します。
2. 次に、パッケージを Android マーケットプレイスにアップロードします。
3. ユーザは、適切なパラメータを使用してクライアント プロビジョニングでポリシーを設定します。
4. デバイスの登録後、dot1x 認証が失敗すると、エンド ユーザはクライアント プロビジョニング サービスにリダイレクトされます。
5. プロビジョニングのポータル ページには、SPW をダウンロードできる Android マーケットプレイス ポータルにユーザをリダイレクトするためのボタンがあります。
6. サプリカントのプロビジョニングを実行するために Cisco SPW が起動します。 SPW によって ISE が検出され、ISE からプロファイルがダウンロードされます。SPW が EAP TLS の証明書およびキー ペアを作成します。SPW は、ISE に対して Simple Certificate Enrollment Protocol（SCEP）プロキシ要求呼び出しを行い、証明書を取得します。SPW はワイヤレス プロファイルを適用します。プロファイルが正常に適用されると、SPW は再認証を要求します。SPW は終了します。

デュアル SSID ワイヤレス BYOD 自己登録

これは、デュアル SSID ワイヤレス BYOD 自己登録の場合のプロセスです。

1. ユーザはゲスト SSID に関連付けられます。
2. ユーザはブラウザを開き、ISE CWA ゲスト ポータルにリダイレクトされます。
3. ユーザは従業員ユーザ名とパスワードをゲスト ポータルに入力します。
4. ISE がユーザを認証し、ユーザは従業員でありゲストではないという事実に基づいて [Employee Device Registration] ゲスト ページにリダイレクトされます。
5. MAC アドレスが DeviceID の [Device Registration] ゲスト ページに事前に入力されています。ユーザは説明を入力して（必要に応じて）アクセプタブル ユース ポリシー（AUP）を受け入れます。
6. ユーザは [Accept] を選択して、SPW のダウンロードとインストールを開始します。
7. ユーザのデバイスのサプリカントが証明書とともにプロビジョニングされます。
8. CoA が発生し、デバイスが企業の SSID の（CORP）に再度関連付けられ、EAP-TLS（またはそのサプリカントに使用されている任意の認証方式）によって認証が行われます。

シングル SSID ワイヤレス BYOD 自己登録

このシナリオには、Protected Extensible Authentication Protocol（PEAP）と EAP-TLS の両方がサポートされる、企業アクセス（CORP）のためのシングル SSID があります。ゲスト SSID はありません。

これは、シングル SSID ワイヤレス BYOD 自己登録の場合のプロセスです。

1. ユーザは CORP に関連付けられます。
2. ユーザは PEAP 認証のために従業員ユーザ名とパスワードをサプリカントに入力します。
3. ISE がユーザを認証し、PEAP 方法に基づいて同意の許可ポリシーを提供し、[Employee Device Registration] ゲスト ページにリダイレクトします。

4. ユーザはブラウザを開き、[Employee Device Registration] ゲスト ページにリダイレクトされます。
5. MAC アドレスが DeviceID の [Device Registration] ゲスト ページに事前に入力されています。ユーザは説明を入力して、AUP を受け入れます。
6. ユーザは [Accept] を選択して、SPW のダウンロードとインストールを開始します。
7. ユーザのデバイスのサプリカントが証明書とともにプロビジョニングされます。
8. CoA が発生し、デバイスは CORP SSID に再度関連付けられ、EAP-TLS によって認証が行われます。

機能の設定

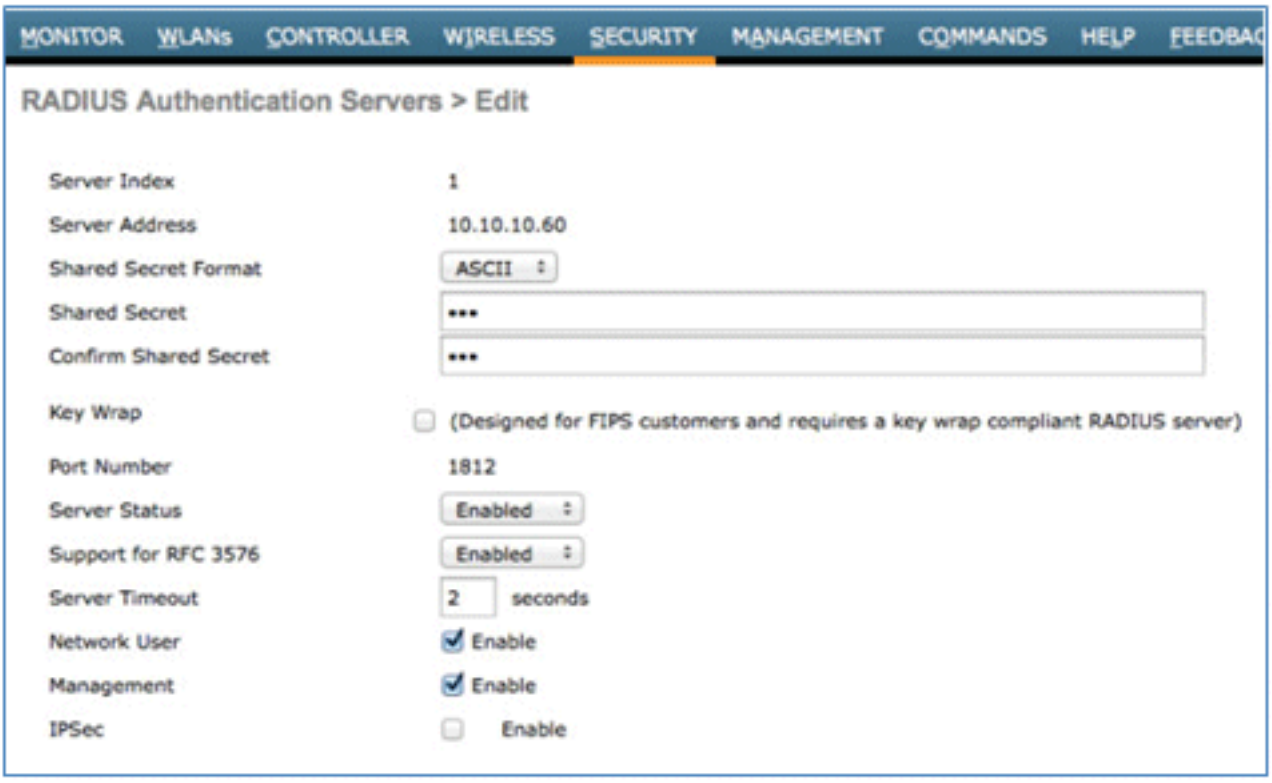
設定を開始するには、次の手順を実行します。

1. このガイドでは、WLC バージョンは 7.2.110.0 以降でなければなりません。

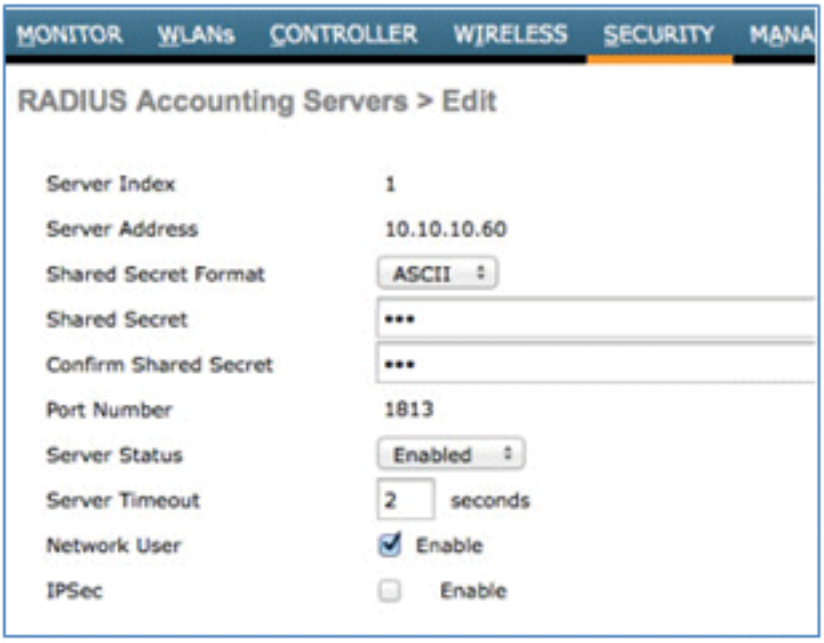
2. [Security] **> [RADIUS] > [Authentication] に移動して、RADIUS サーバを WLC に追加します。**

3. ISE 1.1.1 を WLC に追加します。

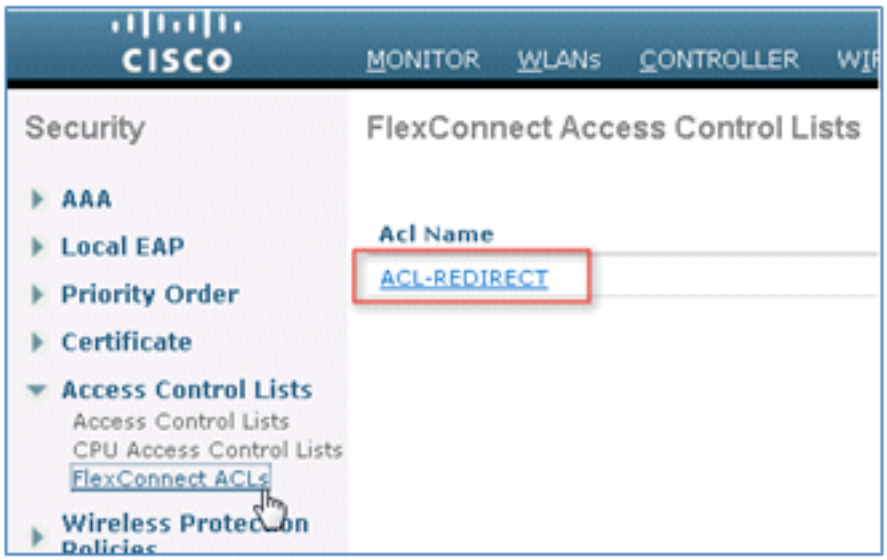
   共有秘密を入力します。RFC 3576 のサポートを [Enabled] に設定します。



4. RADIUS アカウンティング サーバと同じ ISE サーバを追加します。



5. 後で ISE ポリシーで使用される WLC 事前認証 ACL を作成します。[WLC] **> [Security] >** [Access Control Lists] **> [FlexConnect ACLs] に移動し、新しい FlexConnect ACL（この例では、ACL-REDIRECT**）を作成します。

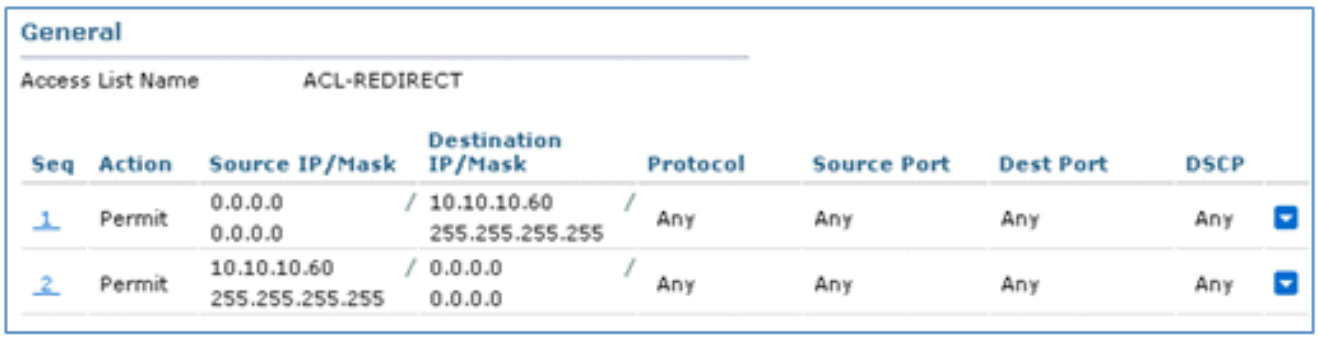


6. ACL ルールでは、ISE との間のすべてのトラフィックを許可し、サプリカント プロビジョニング中のクライアント トラフィックを許可します。

   最初のルール（シーケンス 1）の場合：

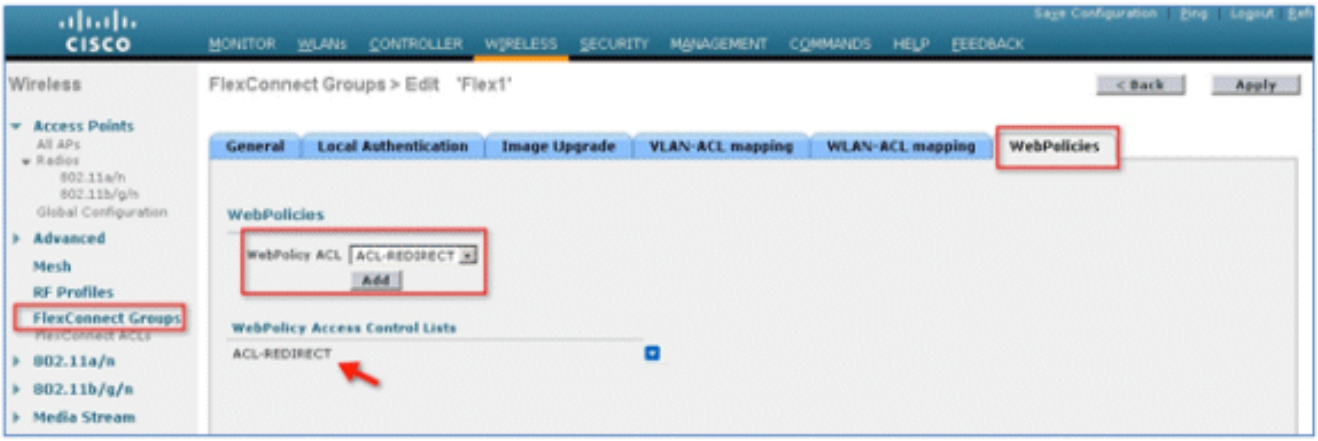
   [Source] を [Any] に設定します。[IP (ISE address)]/[Netmask] **255.255.255.255** を設定します。[Action] を [Permit] に設定します。

   2 番目のルール（シーケンス 2）の場合、[source IP (ISE address)/ mask 255.255.255.255] を [Any] **に設定し、[Action] を [Permit]** に設定します。



7. FlexConnect グループを作成します（この例では、Flex1）。

   [FlexConnect Group] **> [WebPolicies] タブに移動します。**[WebPolicy ACL] フィールドで、[Add] をクリックして [ACL-REDIRECT] または以前に作成した FlexConnect ACL を選択します。[WebPolicy Access Control Lists] フィールドが入力されていることを確認します。



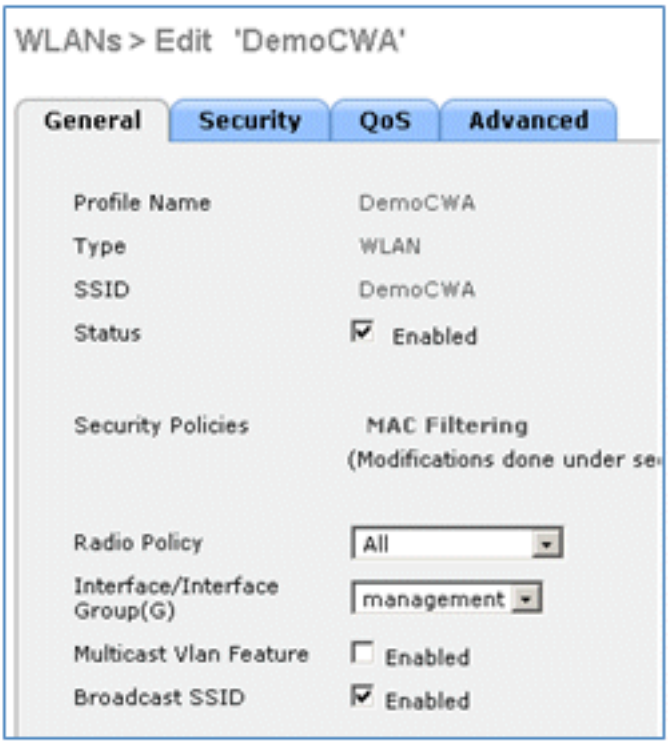
8. [Apply] をクリックし、[Save Configuration] をクリックします。

WLAN 設定

WLAN を設定するには、次の手順を実行します。

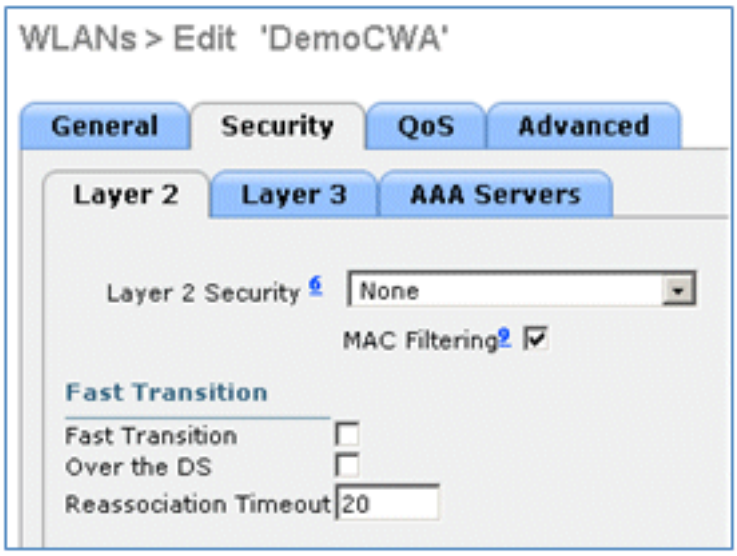
1. オープン WLAN SSID（デュアル SSID の例の場合）を作成します。

   WLAN名として**DemoCWA**を入力します（この例では）。[Status] で [Enabled] オプションを選択します。



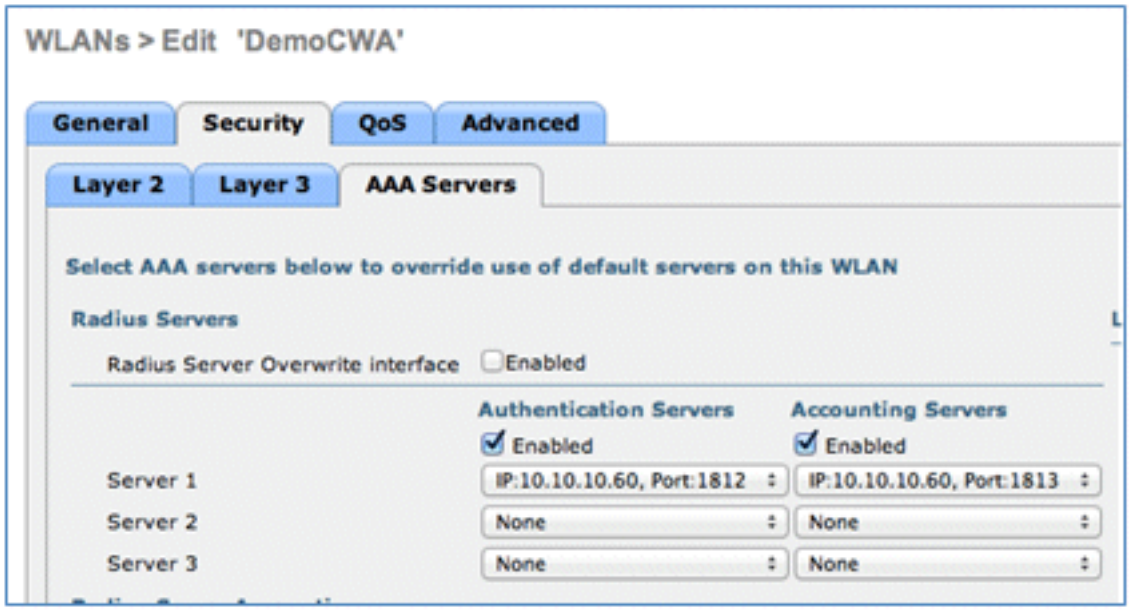
2. [Security] **タブ > [Layer 2] タブに移動して、次の属性を設定します。**

レイヤ2セキュリティ：**なし**[MAC Filtering]:[Enabled]（ボックスがオンになっている）[Fast Transition]:[Disabled]（ボックスはオンになっていない）



3. [AAA Servers] タブに移動し、次の属性を選択します。

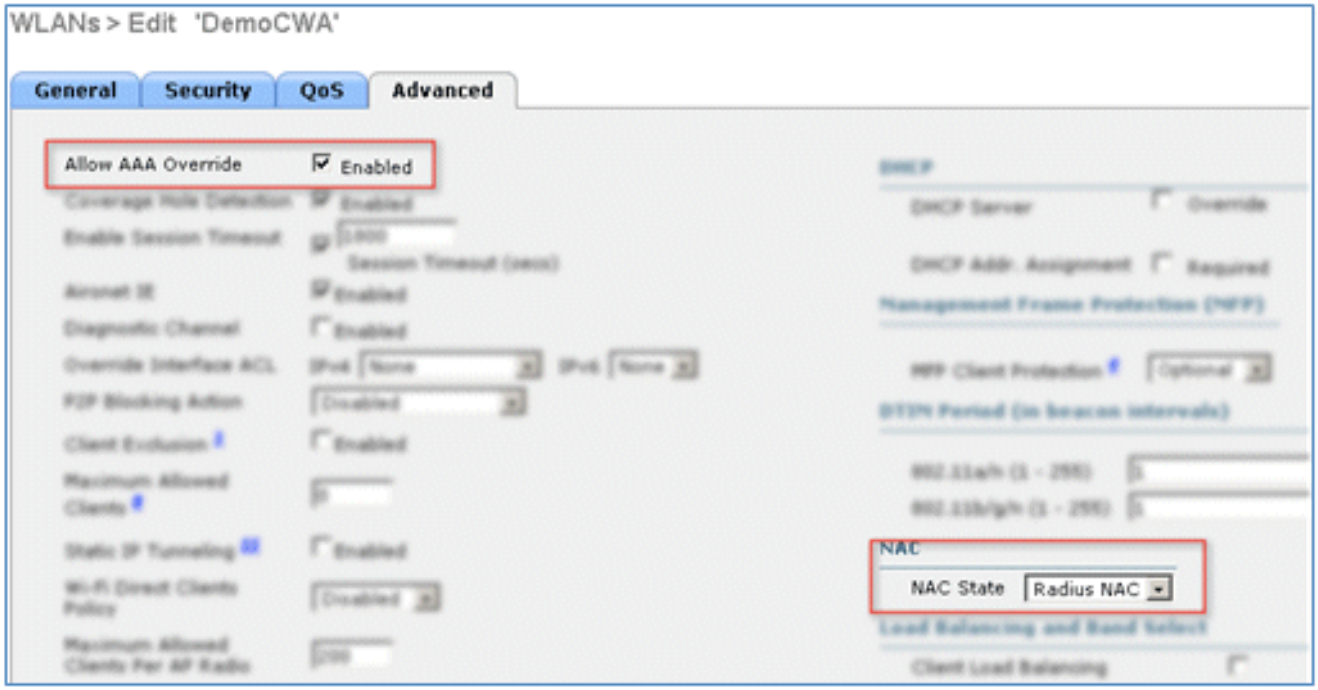
   認証およびアカウントサーバ：**有効**サーバ1:*<ISE IPアドレス>*



4. [AAA Servers] タブからスクロールダウンします。[Authentication priority order for web-auth user] で、[RADIUS] **が認証に使用され、その他のものは使用されていないことを確認します。**

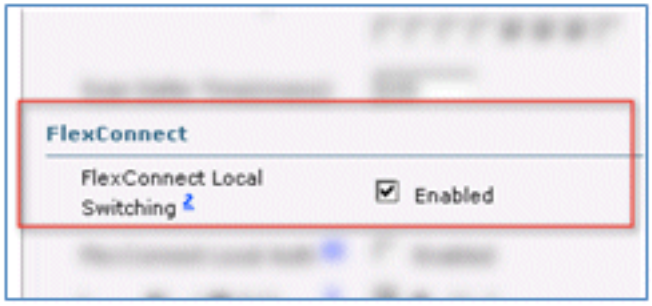
5. [Advanced] タブに移動し、次の属性を選択します。

   [Allow AAA Override]:**Enabled**NAC状態：**Radius NAC**



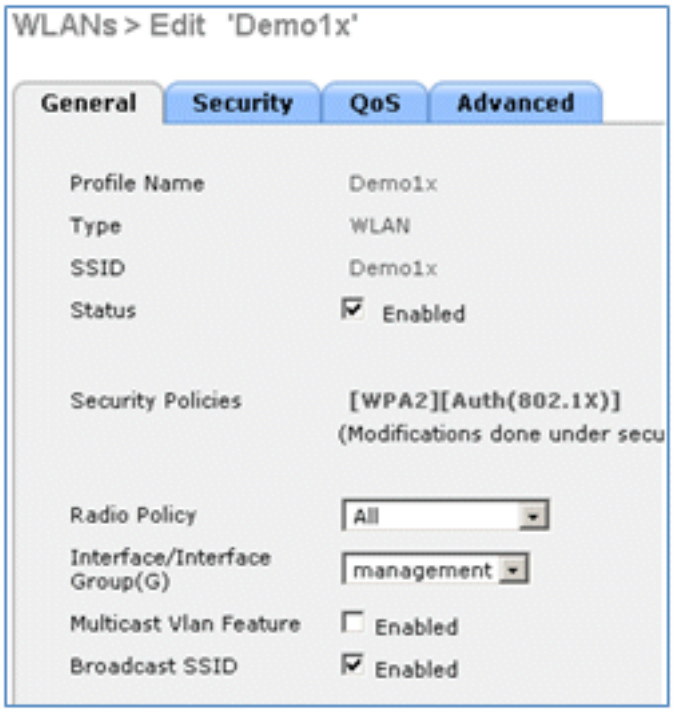
   注:FlexConnect APが切断モードの場合、RADIUS Network Admission Control(NAC)はサポートされません。そのため、FlexConnect AP がスタンドアロン モードで、WLC への接続を失う場合、すべてのクライアントは切断され、SSID はアドバタイズされなくなります。

6. [Advanced] タブでスクロールダウンして、[FlexConnect Local Switching] を [Enabled] に設定します。



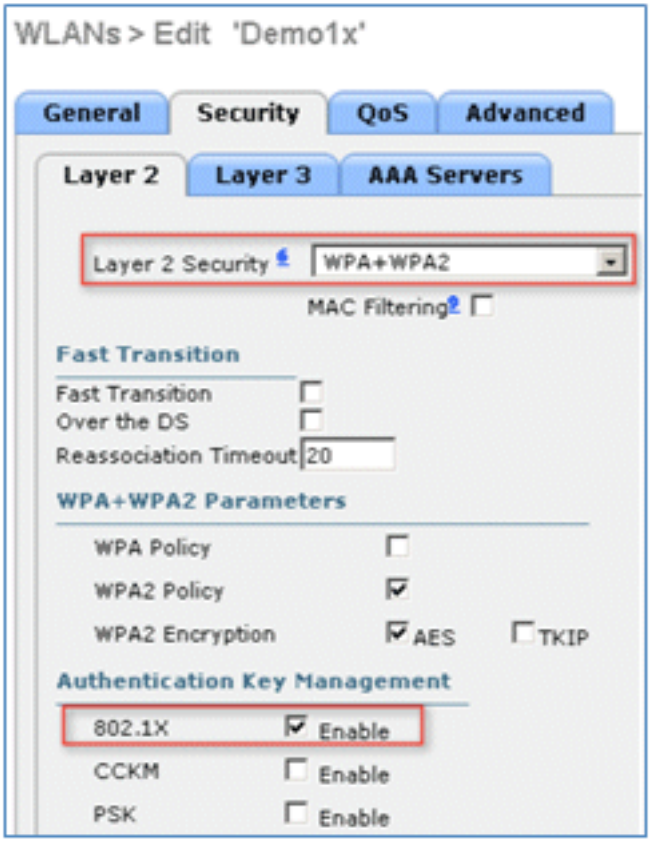
7. [Apply] をクリックし、[Save Configuration] をクリックします。

8. シングルおよびデュアル SSID のシナリオ用の 802.1X WLAN SSID (この例では、**Demo1x) を作成します。**



9. [Security] **タブ > [Layer 2] タブに移動して、次の属性を設定します。**

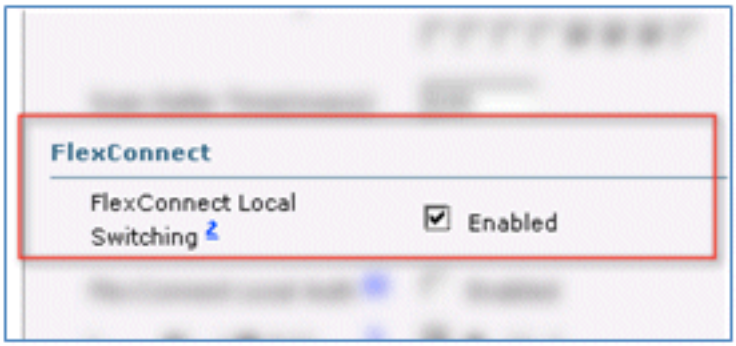
   レイヤ2セキュリティ：**WPA+WPA2**[Fast Transition]:[Disabled]（ボックスはオンになっていない）[Authentication Key Management]:802.IX:**Enable**



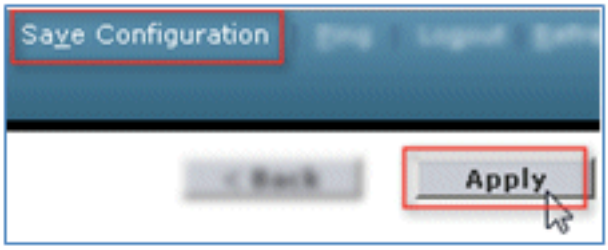
10. [Advanced] タブに移動し、次の属性を選択します。

    [Allow AAA Override]:**Enabled**NAC状態：**Radius NAC**

11. [Advanced] タブでスクロールダウンして、[FlexConnect Local Switching] を [Enabled] に設定します。



12. [Apply] をクリックし、[Save Configuration] をクリックします。



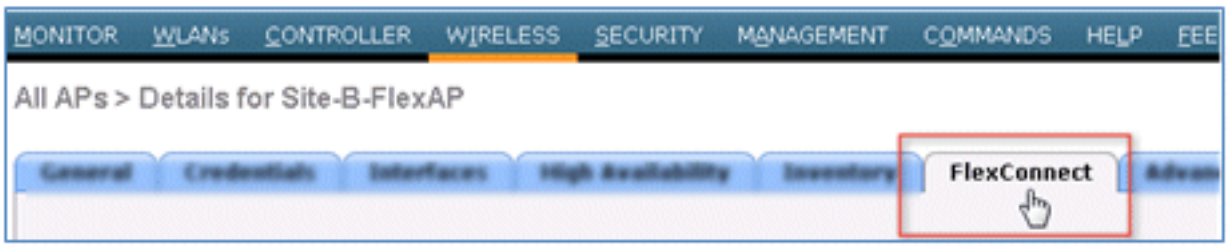
13. 新しい WLAN が両方とも作成されたことを確認します。

FlexConnect AP 設定

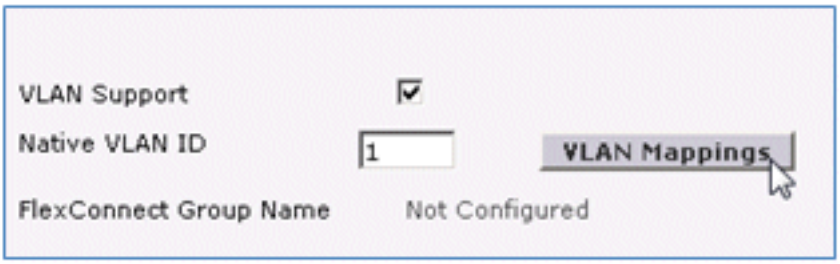
FlexConnect AP を設定するには、次の手順を実行します。

1. [WLC] **> [Wireless]** に移動して、ターゲット FlexConnect AP をクリックします。

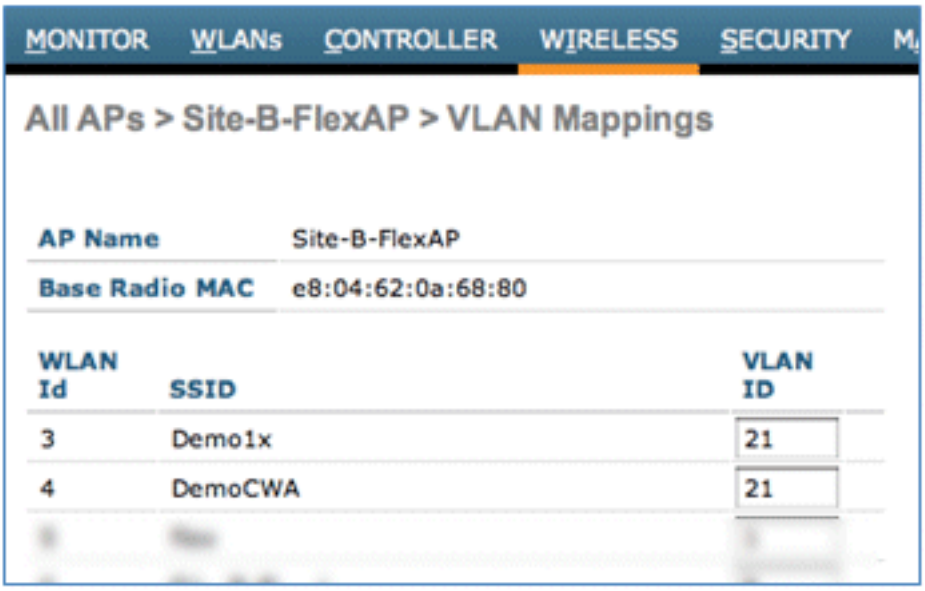
2. [FlexConnect] タブをクリックします。



3. [VLAN Support] を有効にします（ボックスをチェック）。[Native VLAN ID] を設定し、[VLAN Mappings] をクリックします。



4. ローカル スイッチング用に SSID の VLAN ID を設定します（この例では、21 **です**）。



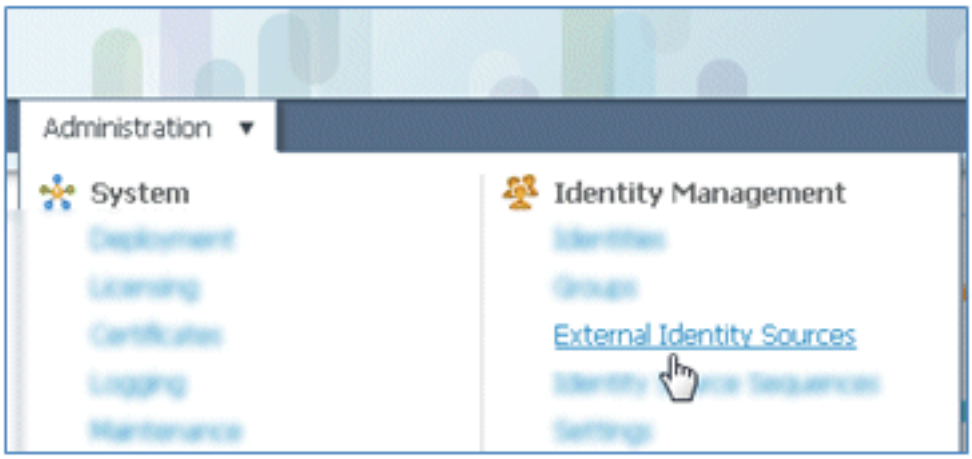
5. [Apply] をクリックし、[Save Configuration] をクリックします。

ISE の設定

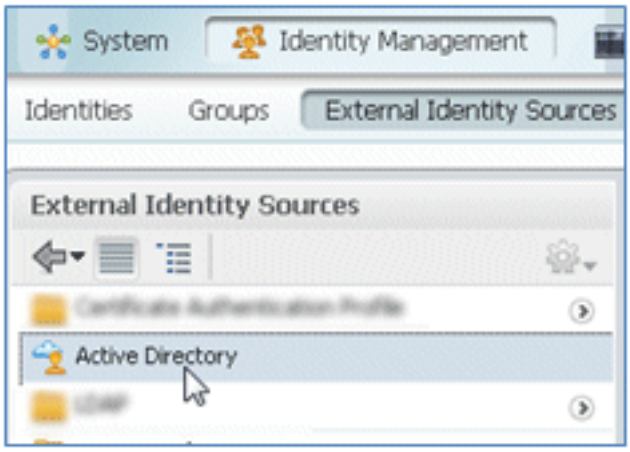
ISE を設定するには、次の手順を実行します。

1. ISEサーバ<https://ise>にログインします。

2. [Administration] **> [Identity Management] > [External Identity Sources]** に移動します。

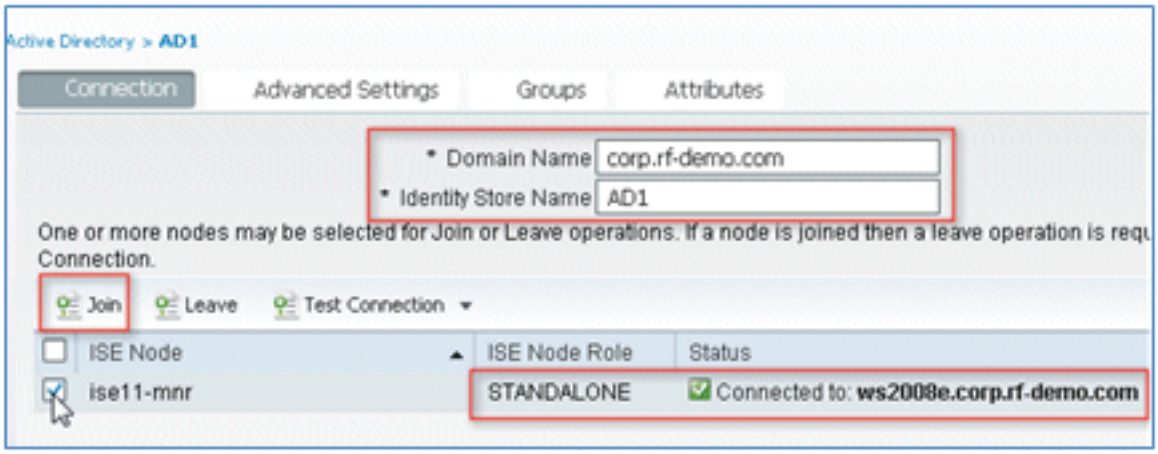


3. [Active Directory] をクリックします。

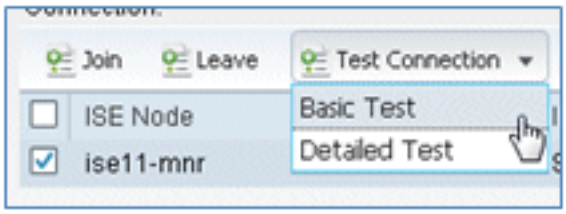


4. [Connection] タブで次のようにします。

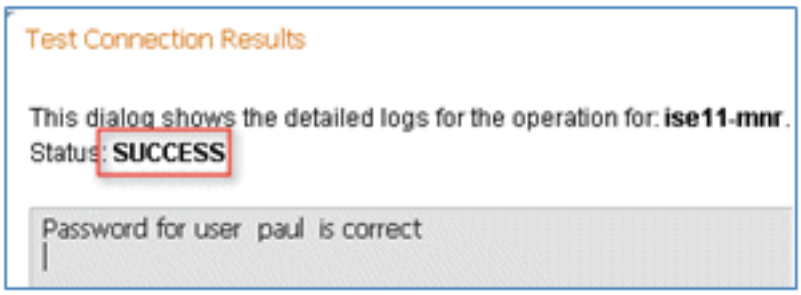
   [Domain Name]（この例では、**corp.rf-demo.com**）**を追加して、[Identity Store Name] のデフォルトを [AD1]** に変更します。[Save Configuration] をクリックします。[Join] をクリックして、加入するために必要な AD 管理者アカウントのユーザ名とパスワードを指定します。[Status] は緑色で表示されます。[Connected to:] を有効にします（チェックボックスがオンになっています）。



5. 現在のドメイン ユーザを使用して AD への基本的な接続テストを実行します。

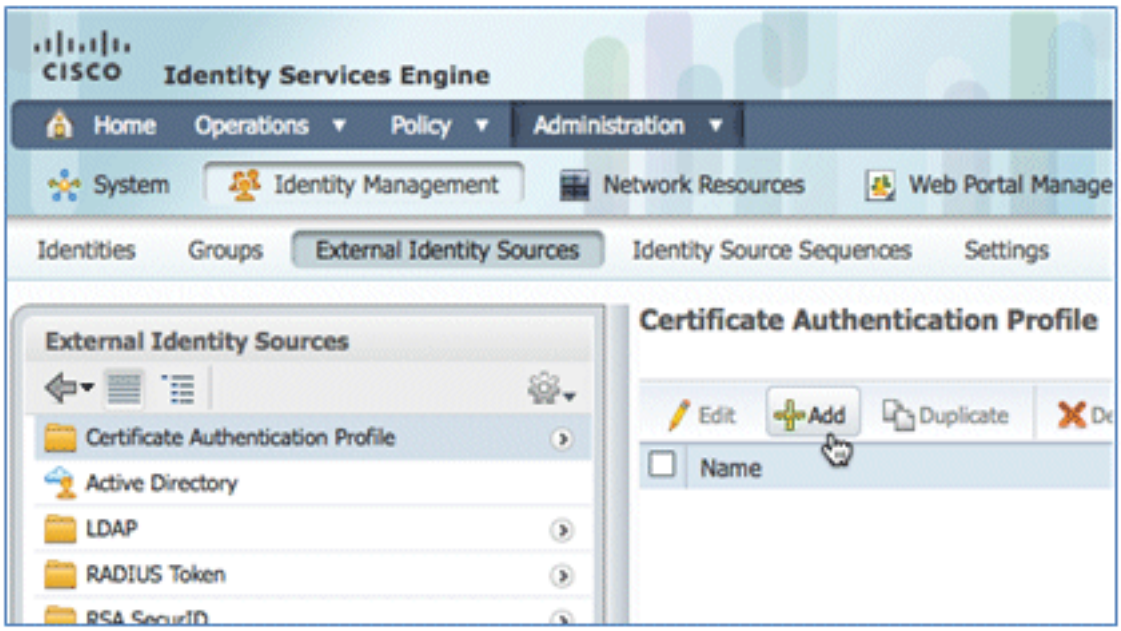


6. AD への接続が正常に行われた場合、パスワードが正しいことを確認するダイアログが表示されます。

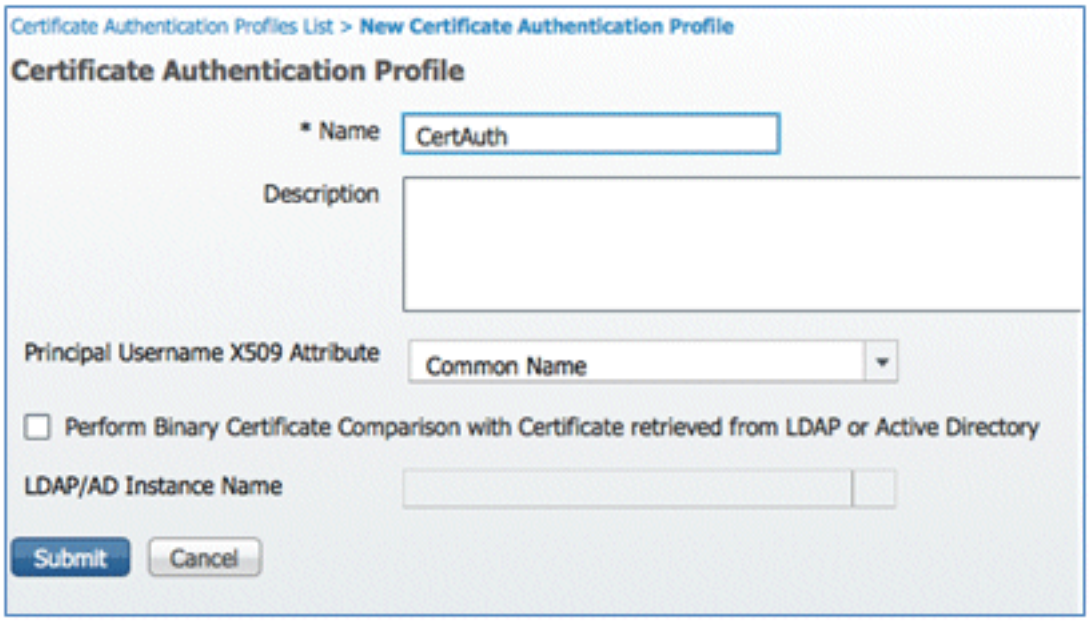


7. [Administration] **> [Identity Management] > [External Identity Sources]** に移動します。

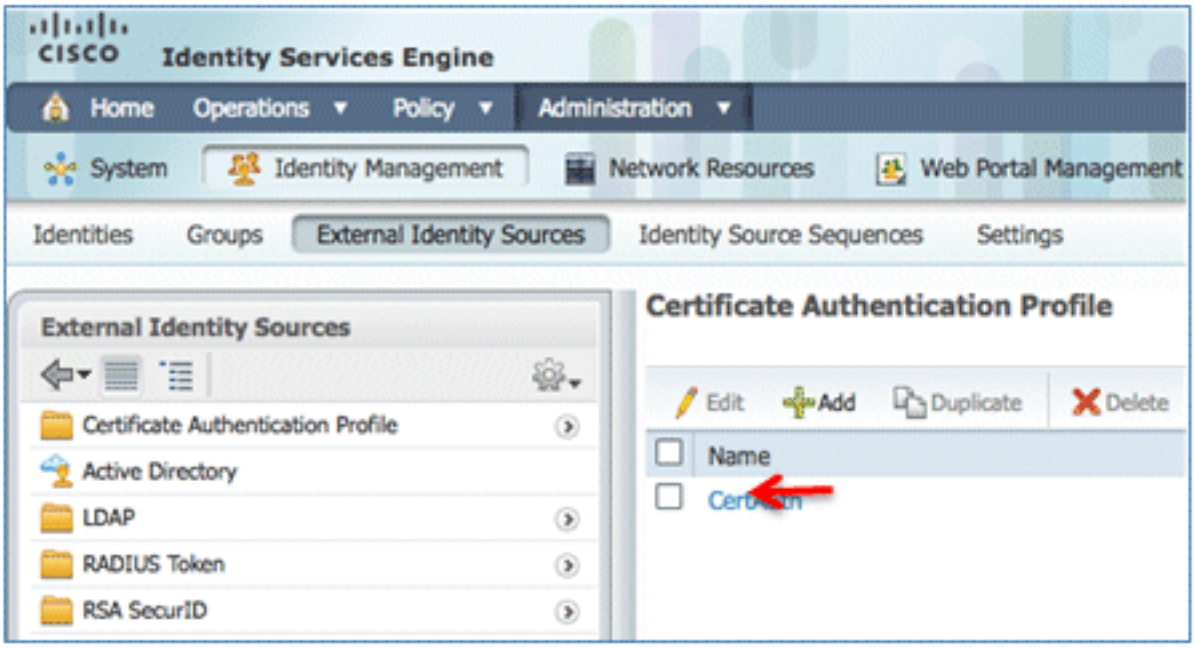
   [Certificate Authentication Profile] をクリックします。新しい [Certificate Authentication Profile（CAP）] で [Add] をクリックします。



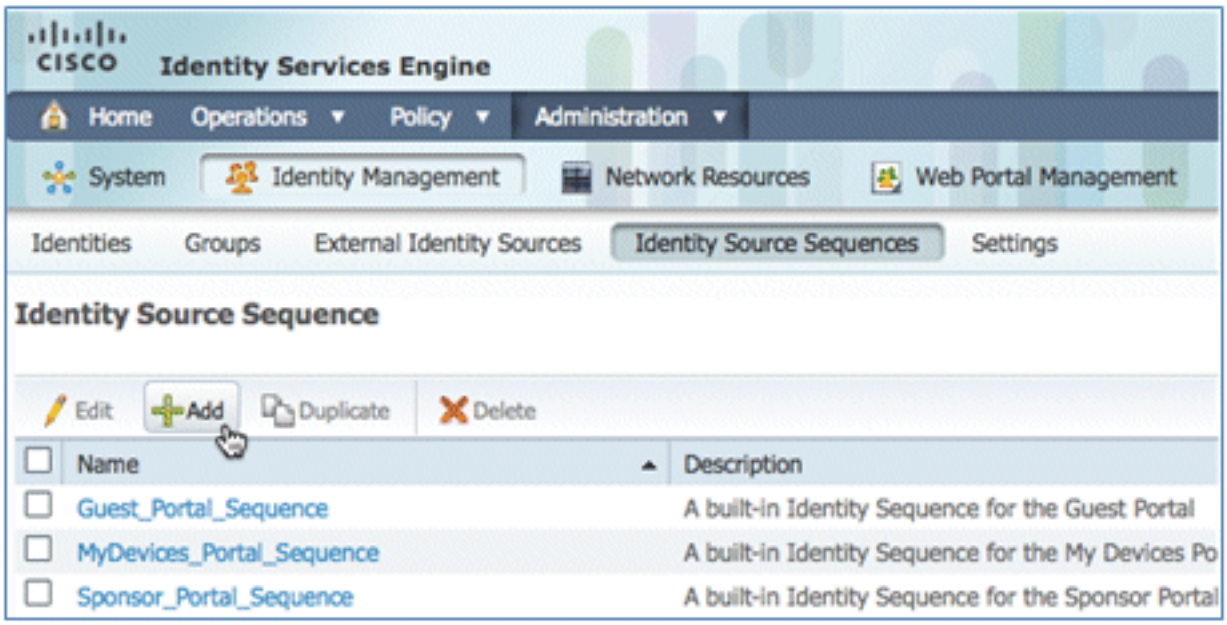
8. CAPの名前として**CertAuth**（この例の場合）を入力し、[Principal Username X509 Attribute]で[Common Name] を選択し、[Submit] をクリックします。



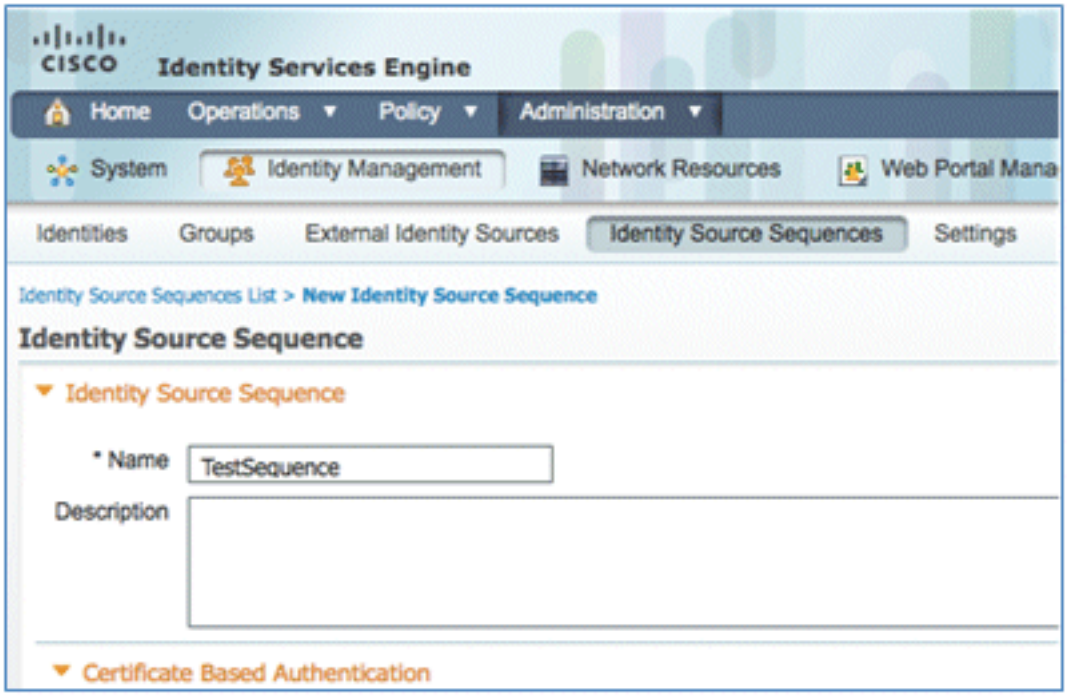
9. 新しい CAP が追加されたことを確認します。



10. [Administration] > **[Identity Management] > [Identity Source Sequences]** に移動して、[Add] をクリックします。

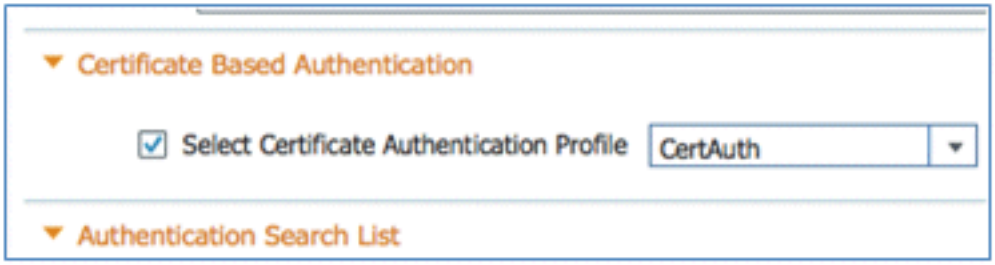


11. シーケンスに名前を付けます（この例では、**TestSequence**）。



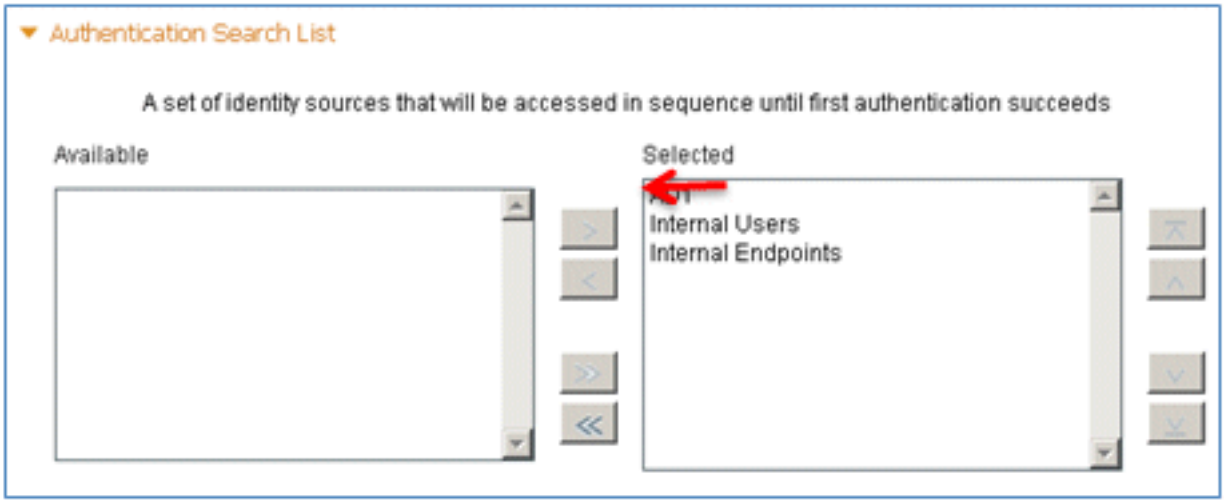
12. [Certificate Based Authentication] までスクロールダウンします。

    [Select Certificate Authentication Profile] **を有効にします（ボックスをチェック）。**
    [CertAuth]（または前の手順で作成した別の **CAP プロファイル**）**を選択します。**

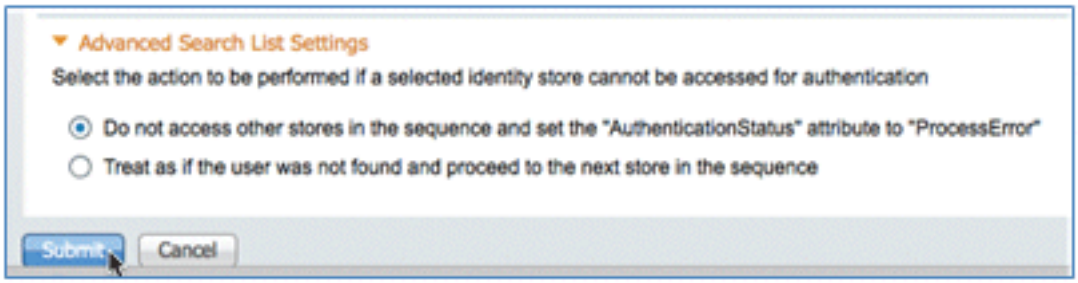


13. [Authentication Search List] までスクロールダウンします。

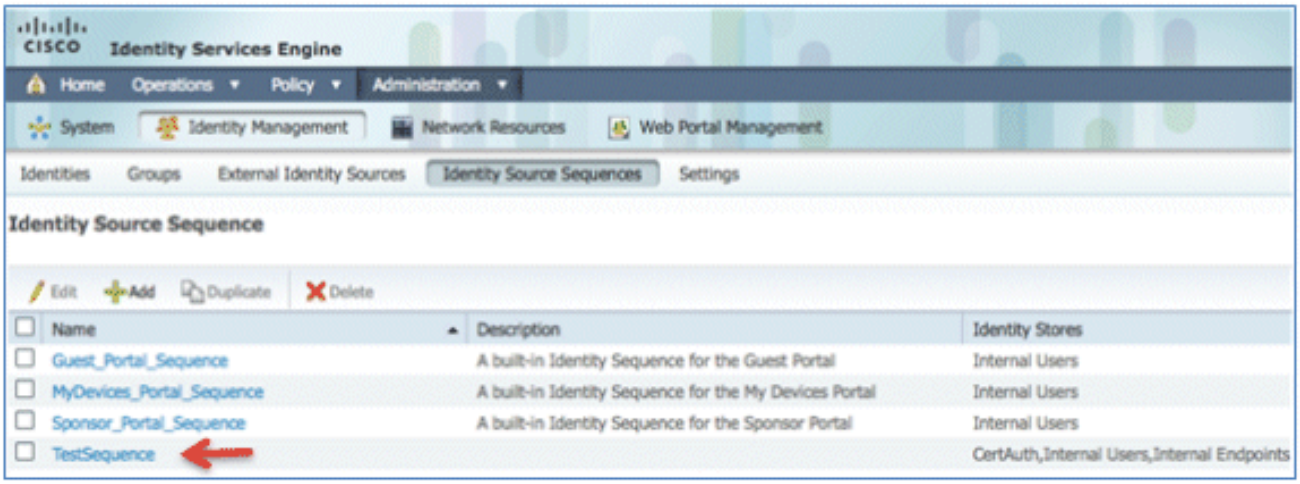
AD1 を [Available] から [Selected] に移動します。AD1 を最高の優先度に移動するには、[Up] ボタンをクリックします。



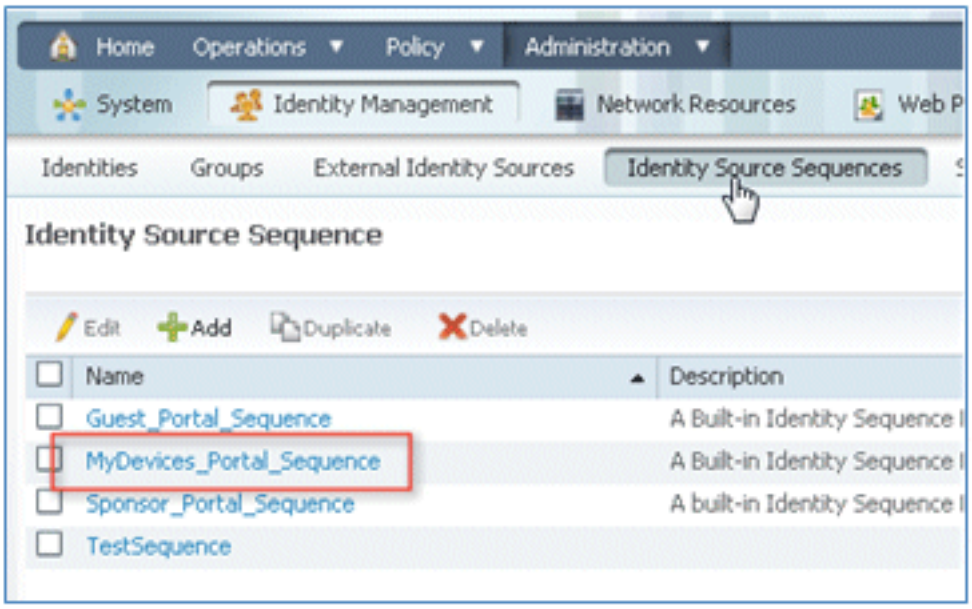
14. 保存するには [Submit] をクリックします。



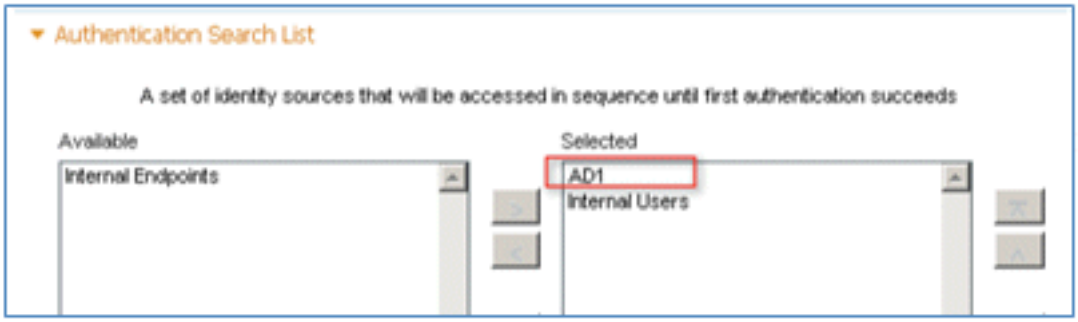
15. 新しい ID ソース シーケンスが追加されたことを確認します。



16. AD を使用して、デバイス ポータルを認証します。[ISE] > **[Administration] > Identity Management[] > [Identity Source Sequence]** に移動して、[MyDevices_Portal_Sequence] を編集します。



17. [AD1] を [Selected] リストに追加し、AD1 を最高の優先度に移動するには、[Up] ボタンをクリックします。

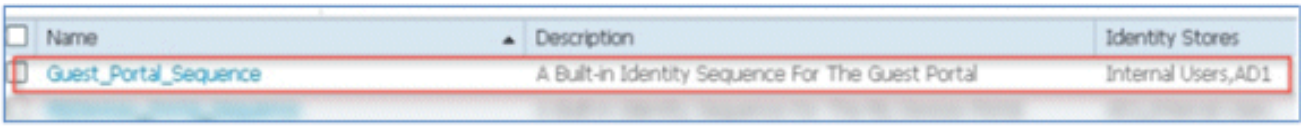


18. [Save] をクリックします。

19. MyDevices_Portal_Sequence の Identity Store sequence に [AD1] が含まれていることを確認します。

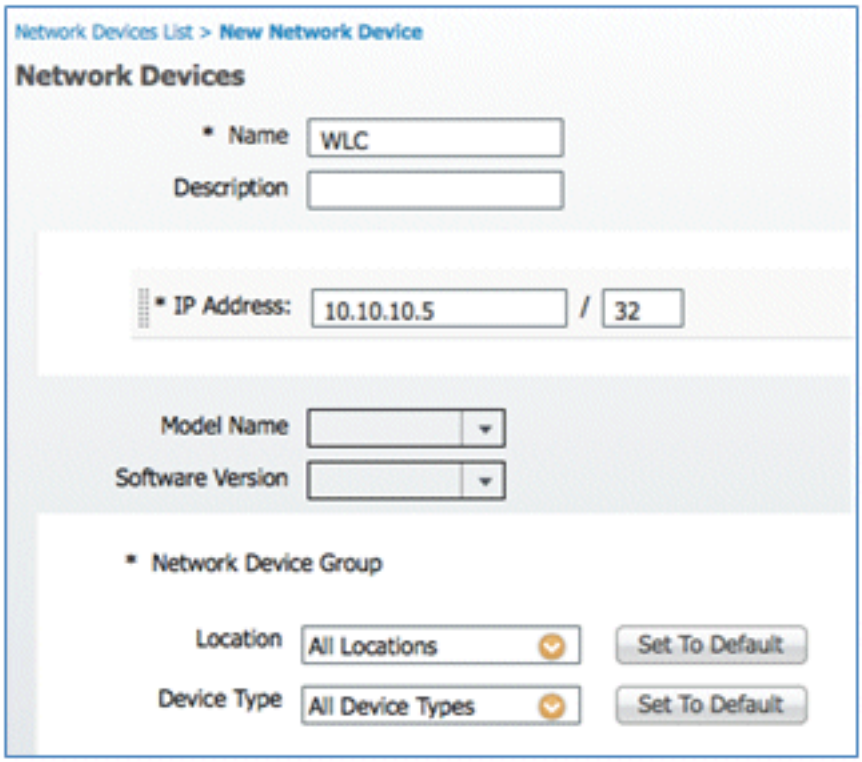
20. Guest_Portal_Sequence で AD1 を追加するには、手順 16 ~ 19 を繰り返して、[Save] をクリックします。

21. Guest_Portal_Sequence に [AD1] が含まれていることを確認します。

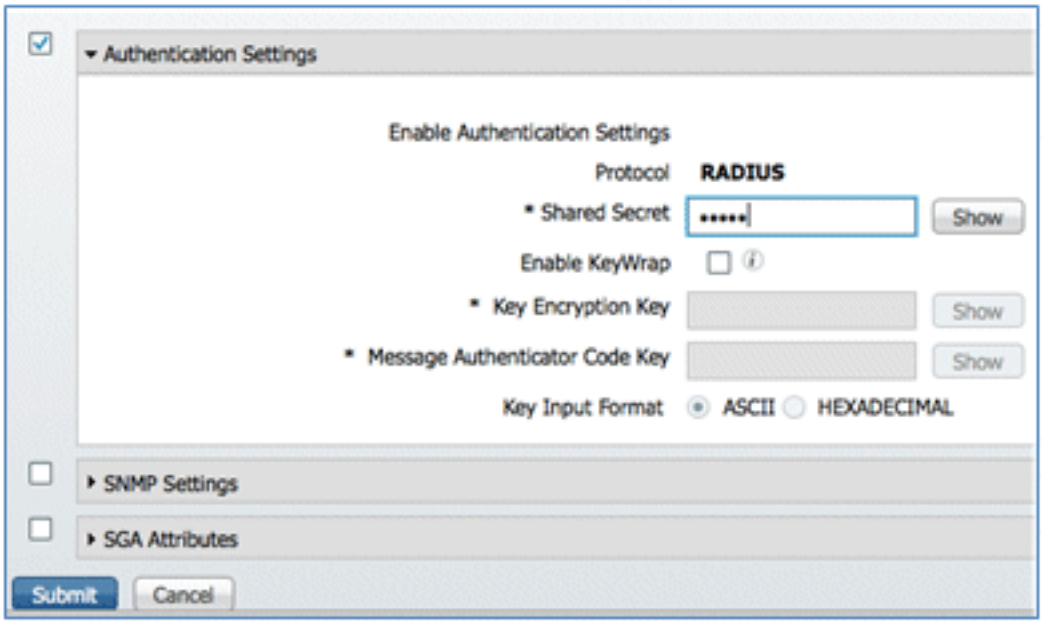


22. WLC をネットワーク アクセス デバイス (WLC) に追加するには、[Administration] > **[Network Resources] > [Network Devices]** に移動して、[Add] をクリックします。

23. WLC の名前、IP アドレス、サブネット マスクなどを追加します。

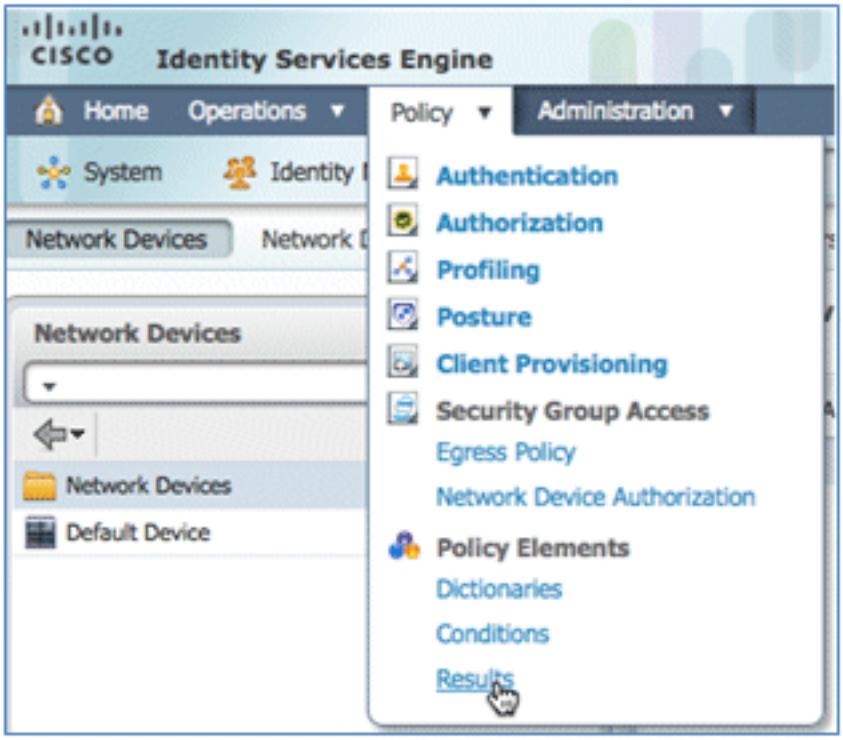


24. [Authentication Settings] までスクロールダウンして、[Shared Secret] に入力します。これは WLC RADIUS の共有秘密と一致する必要があります。

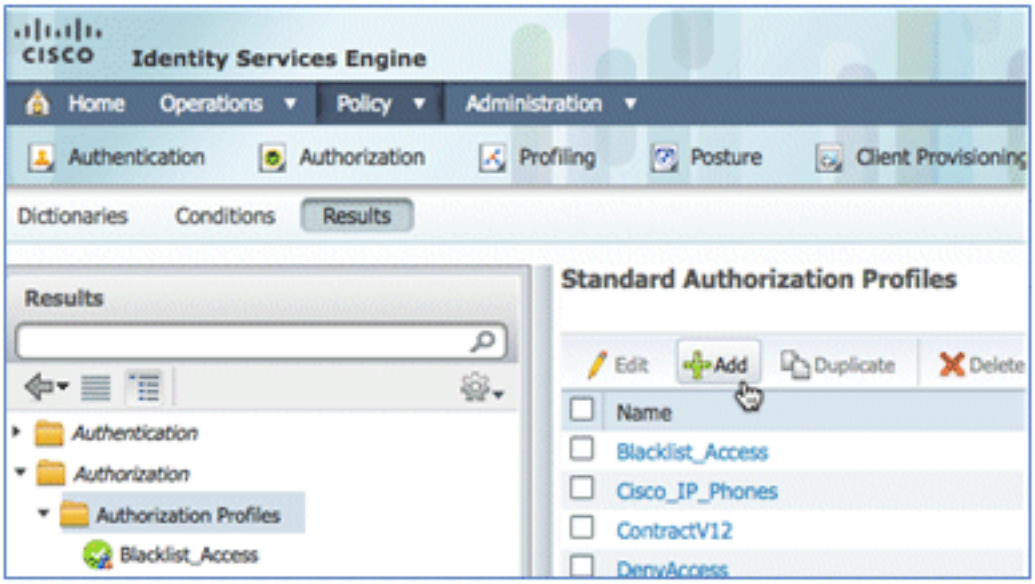


25. [Submit] をクリックします。

26. [ISE] **> [Policy] > [Policy Elements] > [Results]** に移動します。

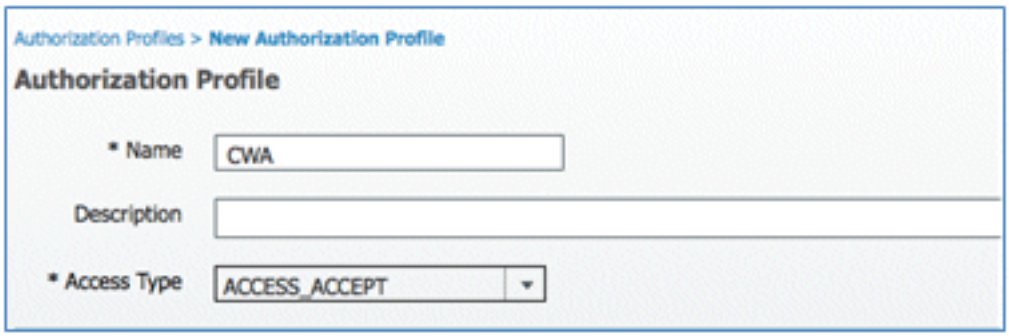


27. [Results] **および [Authorization]** を展開し、[Authorization Profiles] をクリックして、新しいプロファイルのために [Add] をクリックします。



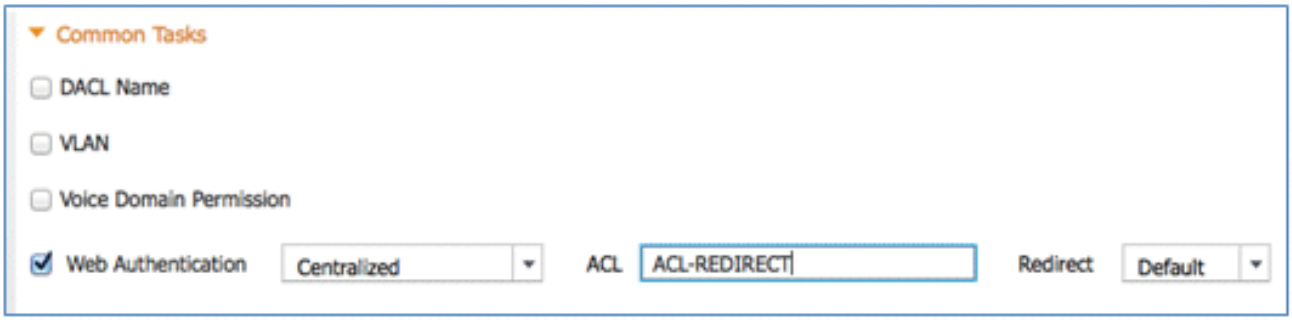
28. このプロファイルに次の値を指定します。

名前：**CWA**

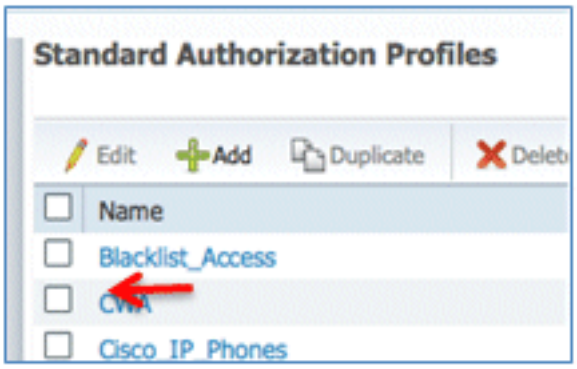


[Web Authentication] を有効にします（ボックスをチェック）。

Web認証：集中型**認証**ACL:**ACL-REDIRECT**（WLC事前認証ACL名と一致する必要があります）リダイレクト：デフォルト



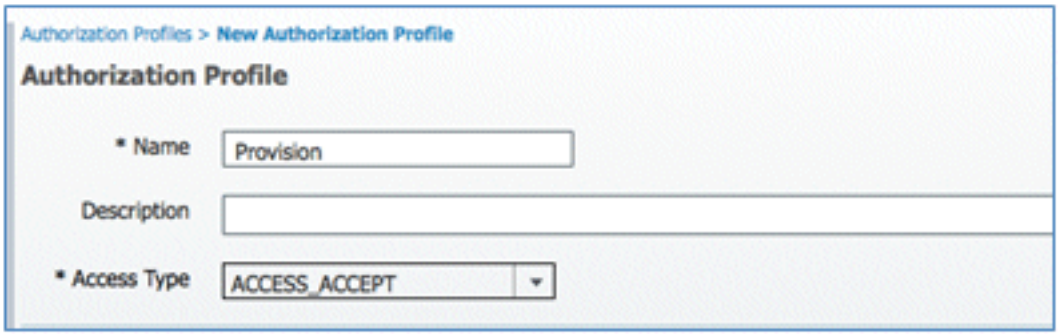
29. [Submit] をクリックして、新しい許可プロファイルが追加されたことを確認します。



30. [Add] をクリックして新しい許可プロファイルを作成します。

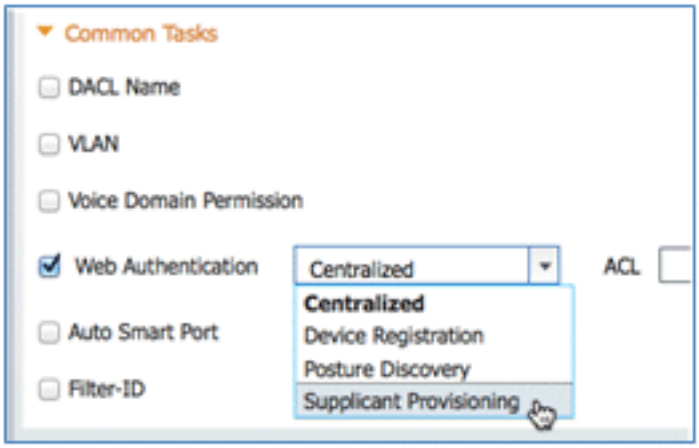
31. このプロファイルに次の値を指定します。

    名前：プロビジョニング

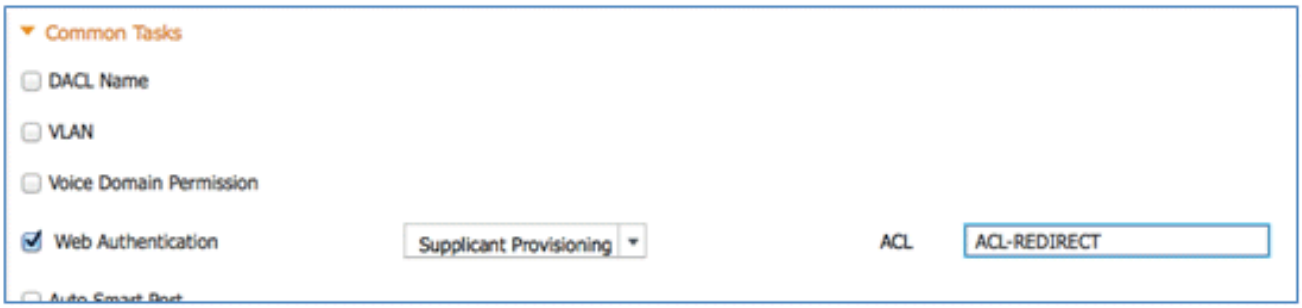


    [Web Authentication] を有効にします（ボックスをチェック）。

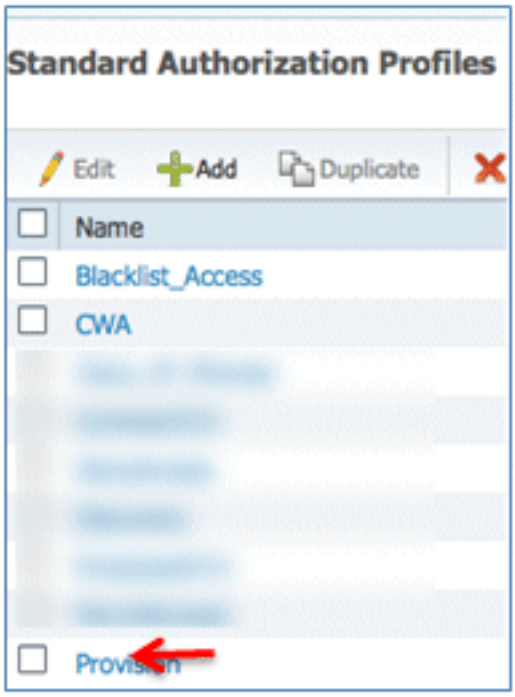
    Web認証値：サプリカントプロビジョニング



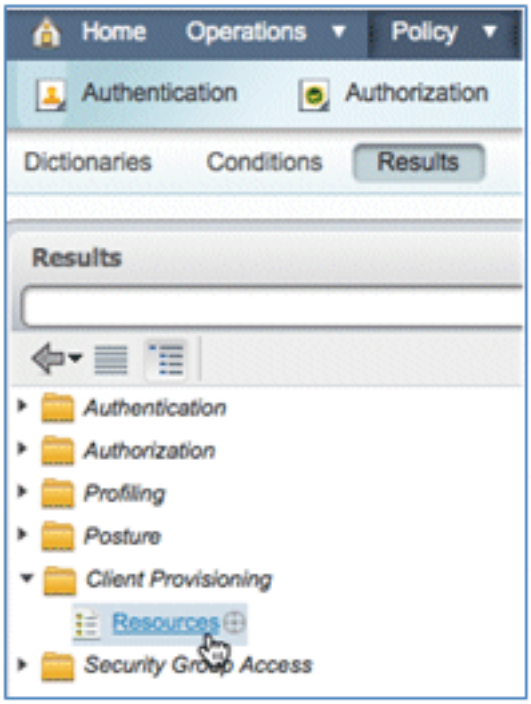
    ACL:ACL-REDIRECT（WLC事前認証ACL名と一致する必要があります）



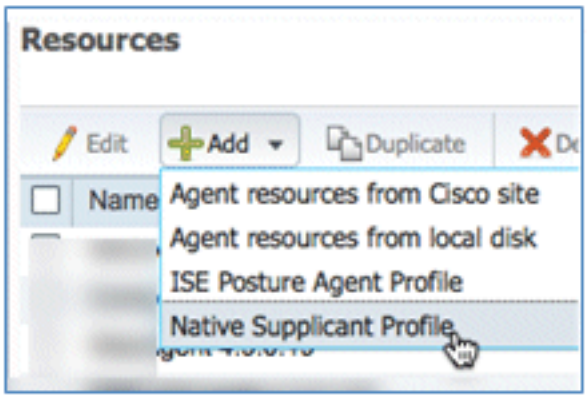
32. [Submit] をクリックして、プロビジョニング許可プロファイルが追加されたことを確認します。



33. [Results] までスクロールダウンして、[Client Provisioning] を展開して [Resources] をクリックします。



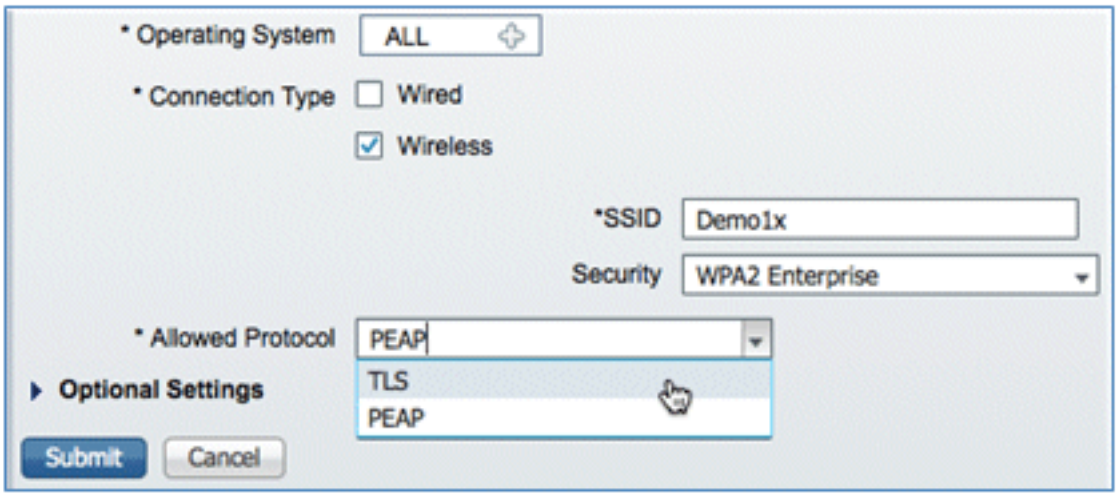
34. [Native Supplicant Profile] を選択します。



35. プロファイルに名前を付けます（この例では、[WirelessSP]）。

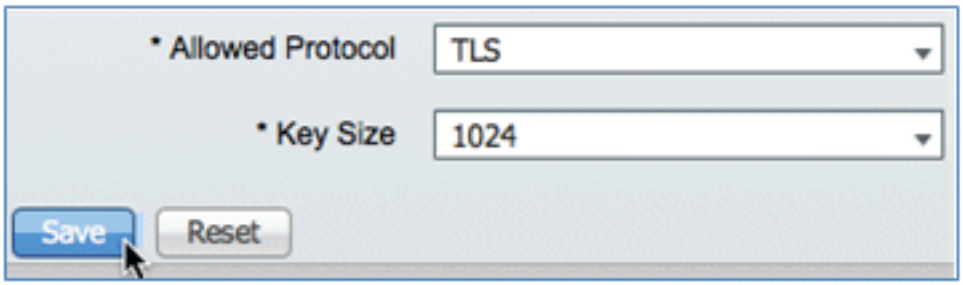
36. 次の値を入力してください。

[Connection Type]:**Wireless**SSID:**Demo1x**（この値はWLC 802.1x WLAN設定のものです）[Allowed Protocol]:**TLS**キーサイズ：**1024**

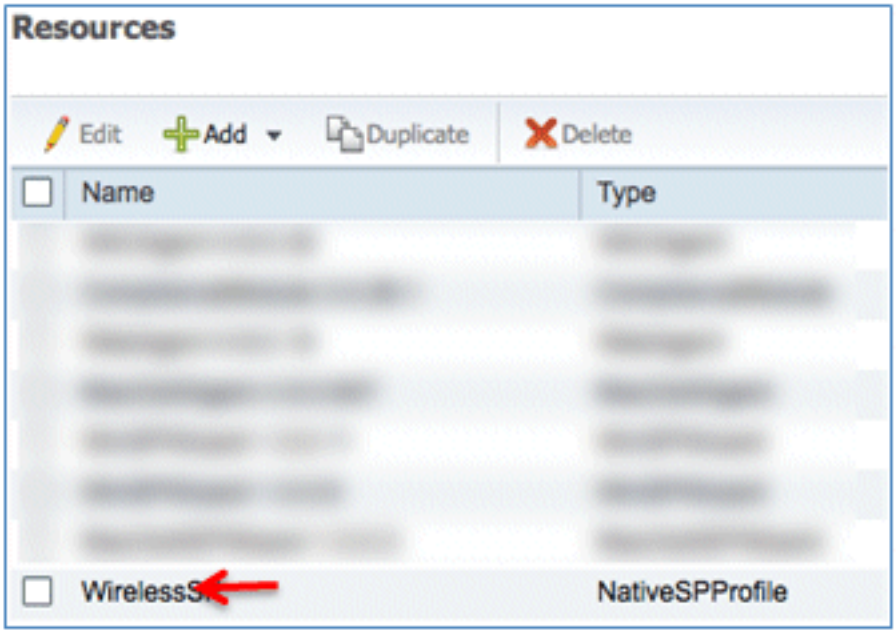


37. [Submit] をクリックします。

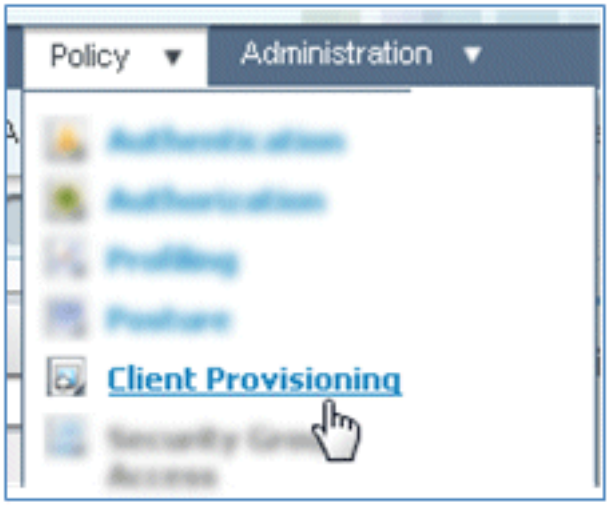
38. [Save] をクリックします。



39. 新しいプロファイルが追加されたことを確認します。

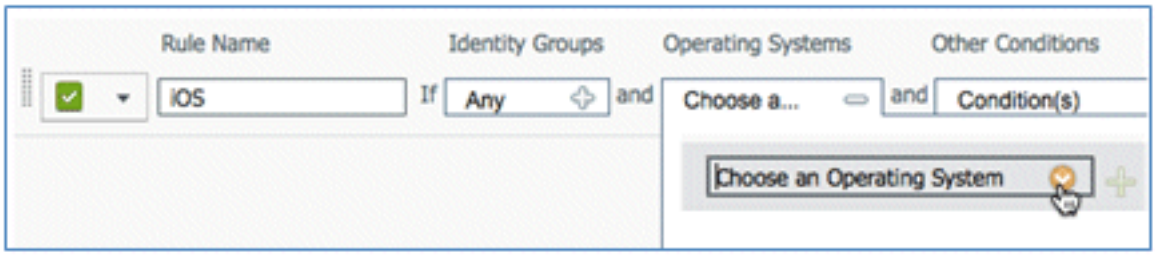


40. [Policy] > [Client Provisioning] に移動します。

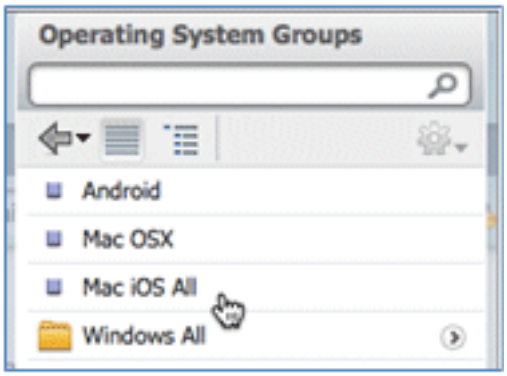


41. iOS デバイスのプロビジョニング ルールについて次の値を入力します。

[Rule Name（ルール名）]:**iOS**IDグループ：**任意**

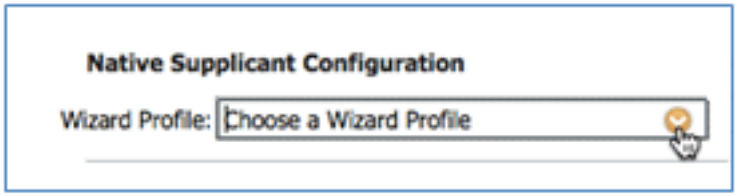


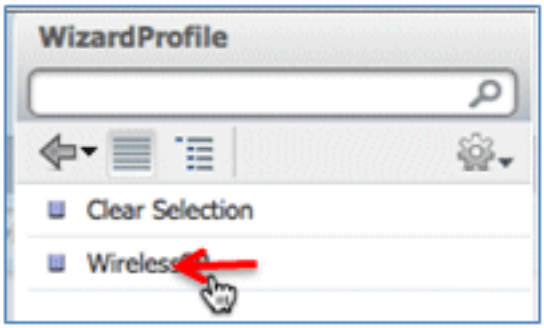
オペレーティングシステム：Mac iOS All



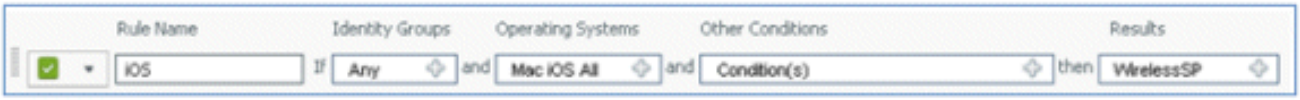
結果：**WirelessSP**（以前に作成されたネイティブサプリカントプロファイル）

[Results] **> [Wizard Profile]（ドロップダウン リスト） > [WirelessSP] に移動します。**

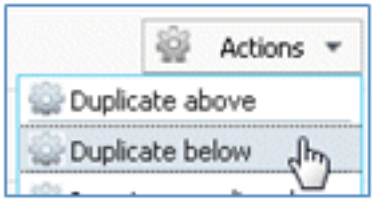




42. iOS プロビジョニング プロファイルが追加されたことを確認します。

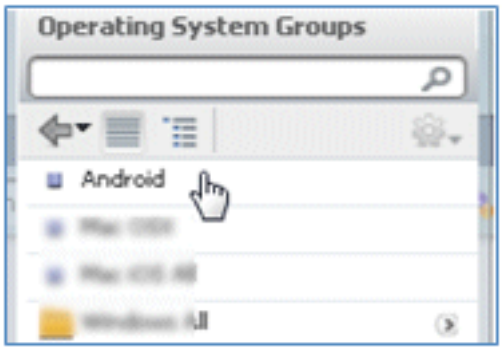


43. 最初のルールの右側で、[Actions] ドロップダウン リストを見つけて、[Duplicate below] **または [Duplicate above] を選択します。**



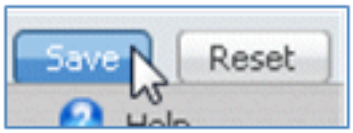
44. 新しいルールの名前を [Android] に変更します。

45. オペレーティング システムを [Android] に変更します。

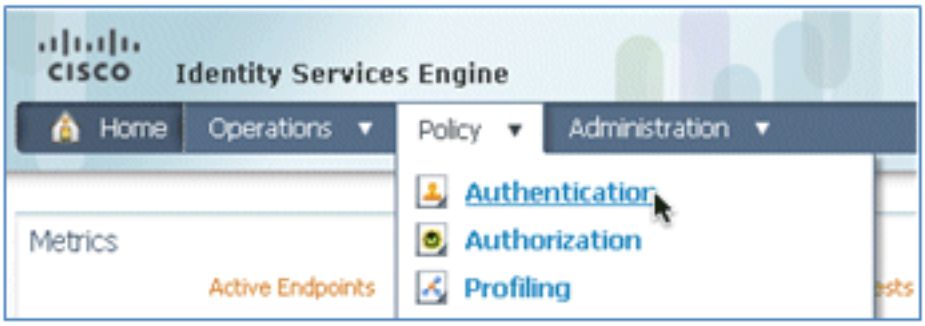


46. 他の値は未変更のままにします。

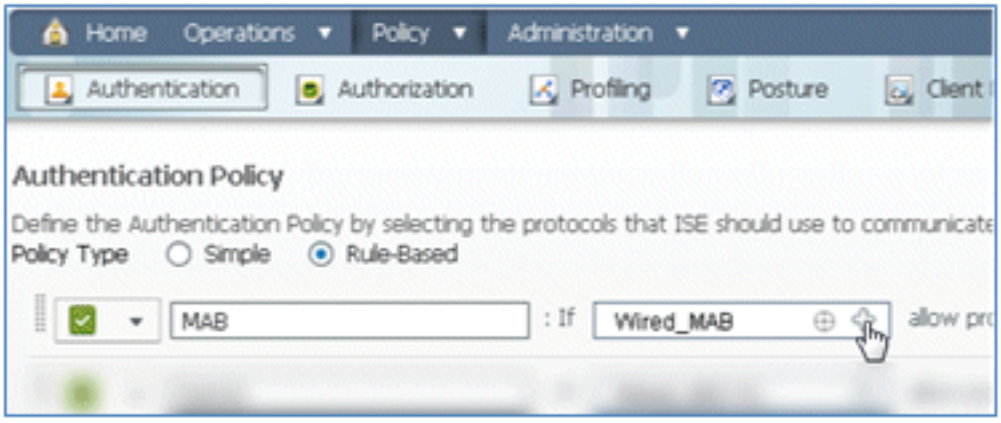
47. [Save]（画面左下）をクリックします。



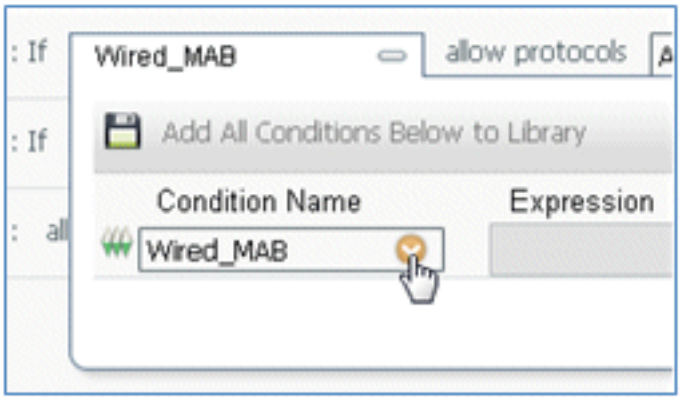
48. [ISE] **> [Policy] > [Authentication]** に移動します。



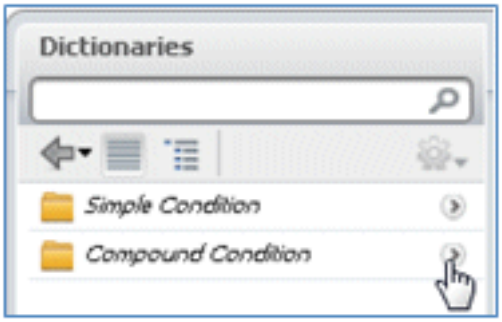
49. Wireless_MAB を含めるよう条件を変更して、[Wired_MAB] を展開します。



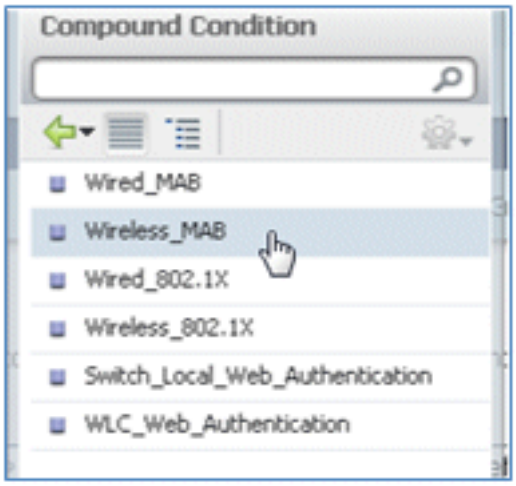
50. [Condition Name] **ドロップダウン リストをクリックします。**



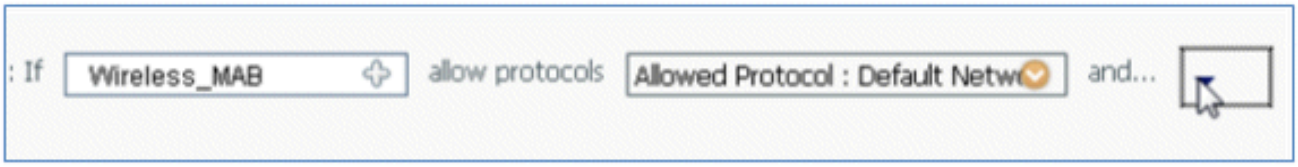
51. [Dictionaries] [Compound Condition] を選択します。



52. [Wireless_MAB] を選択します。

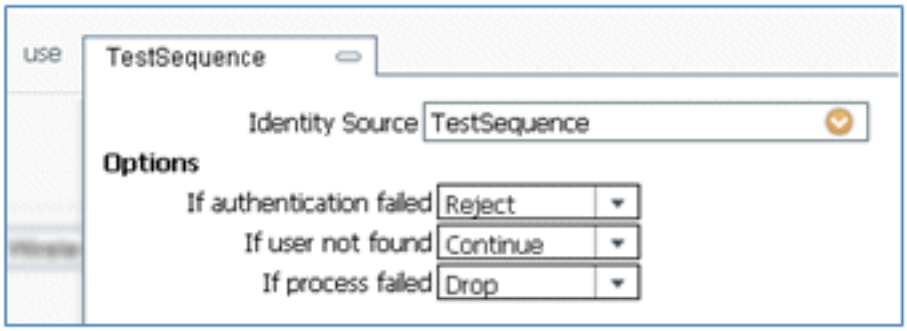


53. ルールの右側で、矢印を選択して展開します。

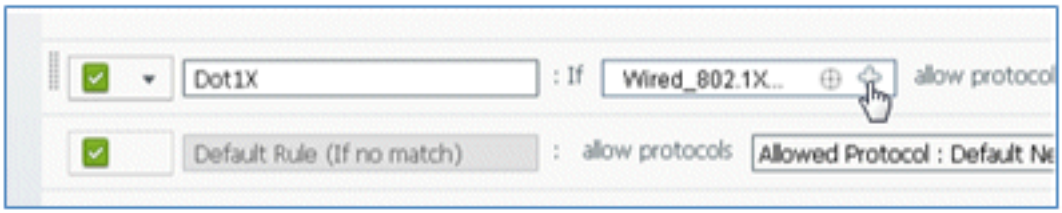


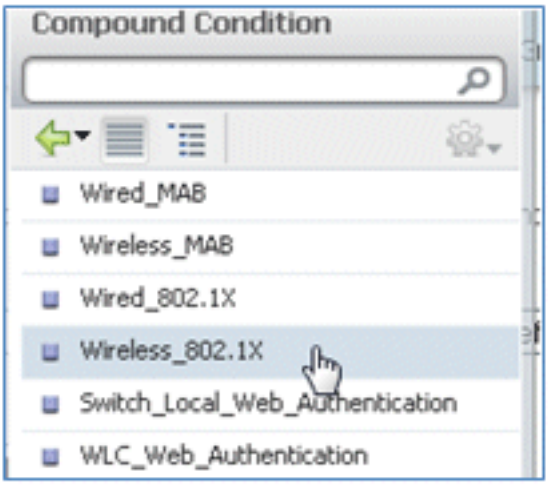
54. ドロップダウン リストから次の値を選択します。

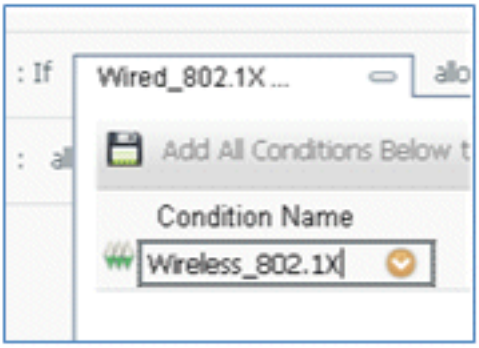
[Identity Source]:**TestSequence**（以前に作成された値）認証に失敗した場合：**Reject**ユーザが見つからない場合：**Continue**プロセスが失敗した場合：**Drop**



55. [Dot1X] **ルールにアクセスして、次の値を変更します。**

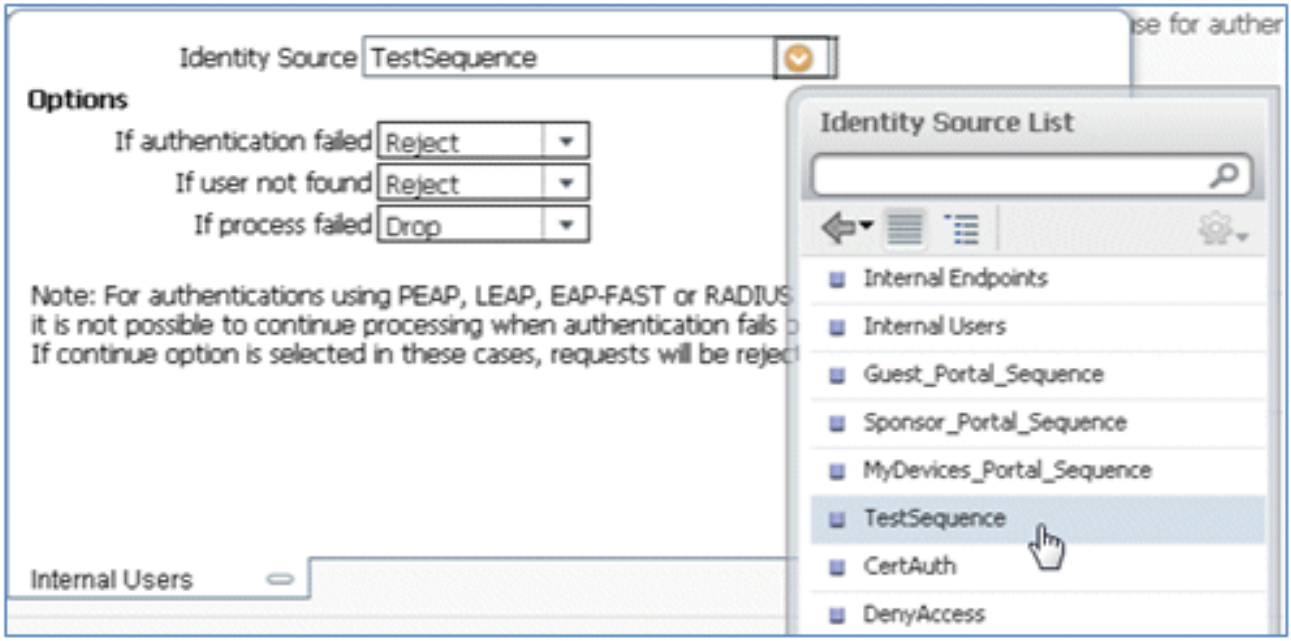






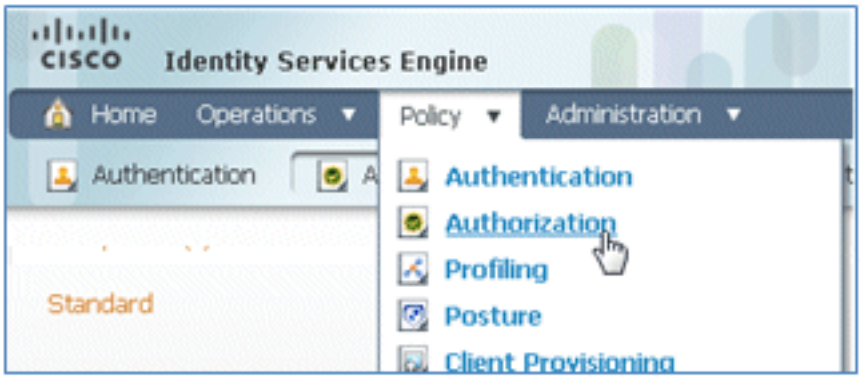
条件：**Wireless_802.1X**

[Identity Source]:**TestSequence**

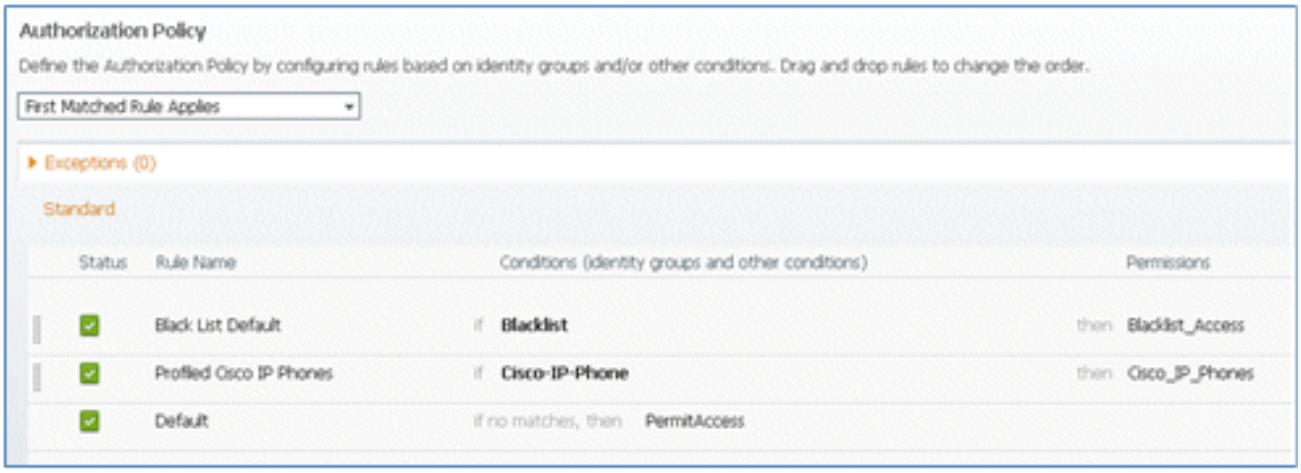


56. [Save] をクリックします。

57. **[ISE] > [Policy] > [Authorization]** に移動します。



58. デフォルトのルール([ブラックリストデフォルト(Black List Default)]、[プロファイル済み(Profiled)]、[デフォルト(Default)]など)は、インストールからすでに設定されています。最初の2つは無視できます。デフォルトのルールは後で編集されます。

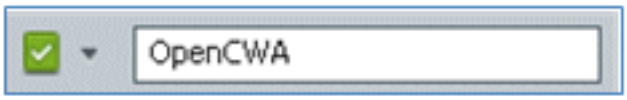


59. 2 番目のルール（ [Profiled Cisco IP Phones] ）の右側で、[Edit] の横にある下矢印をクリックして、[Insert New Rule Below] を選択します。

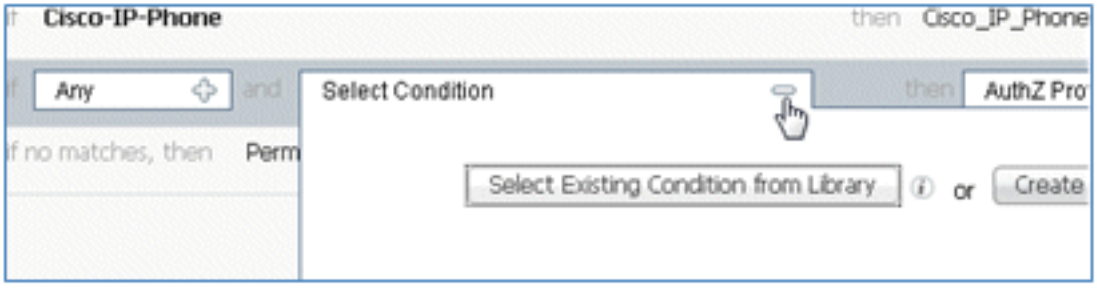
新しく [Standard Rule #] が追加されます。

60. ルール名を [Standard Rule #] から [OpenCWA] に変更します。このルールは、デバイスを

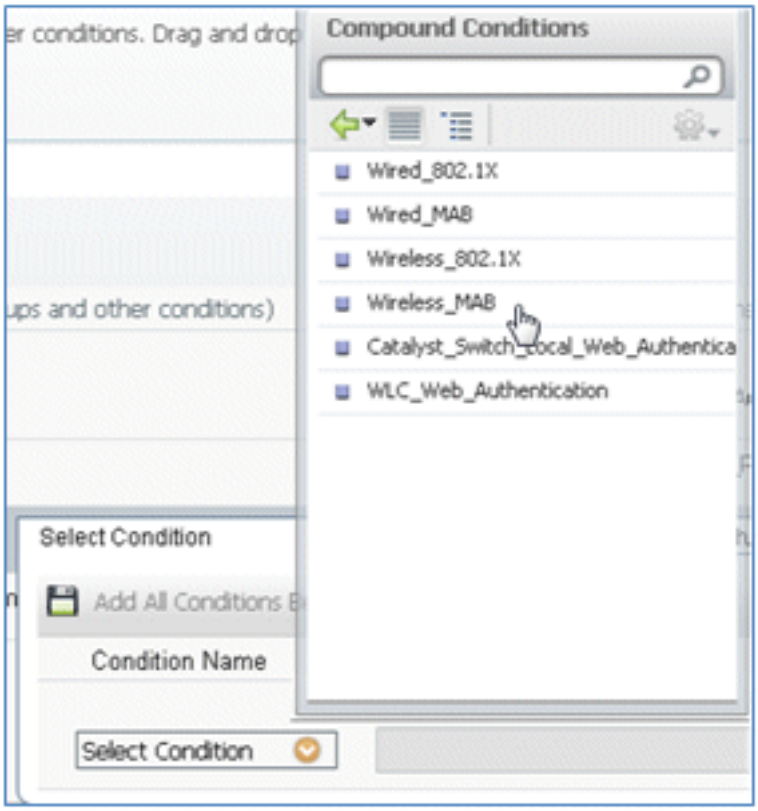
プロビジョニングするために、ゲスト ネットワークへの着信時にオープン WLAN（デュアル SSID）で登録プロセスを開始します。



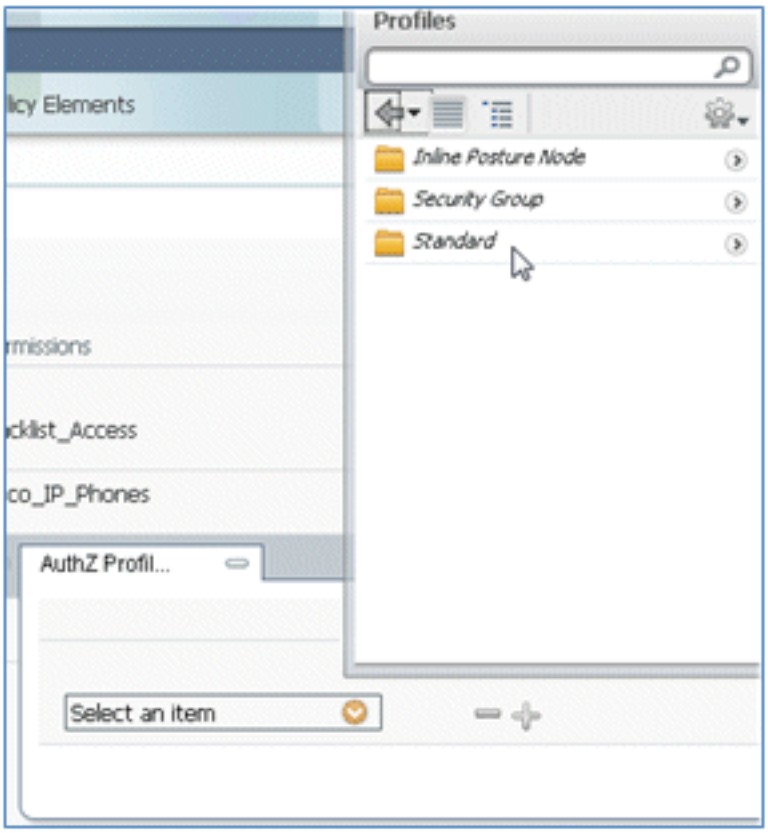
61. [Condition(s)] のプラス記号（[+]）をクリックして、条件のプラス記号（+）をクリックして、[Existing Condition from Library] を選択します。



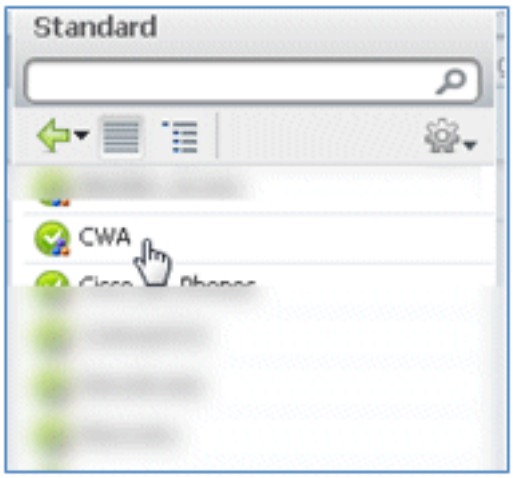
62. [Compound Conditions] [Wireless_MAB] を選択します。



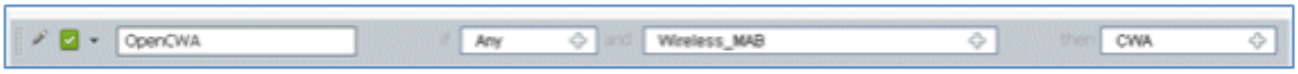
63. [AuthZ Profile] でプラス記号（[+]）をクリックして、[Standard] を選択します。



64. 標準の [CWA]（以前に作成した許可プロファイル）を選択します。



65. 正しい条件と許可とともにルールが追加されたことを確認します。

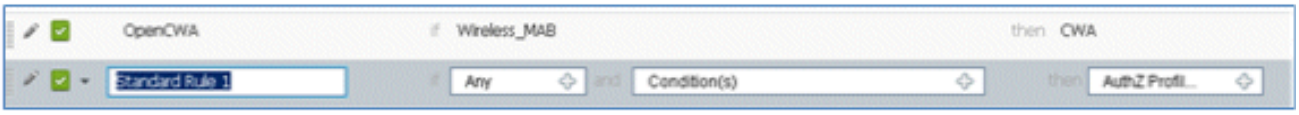


66.（ルールの右側にある）[Done] をクリックします。

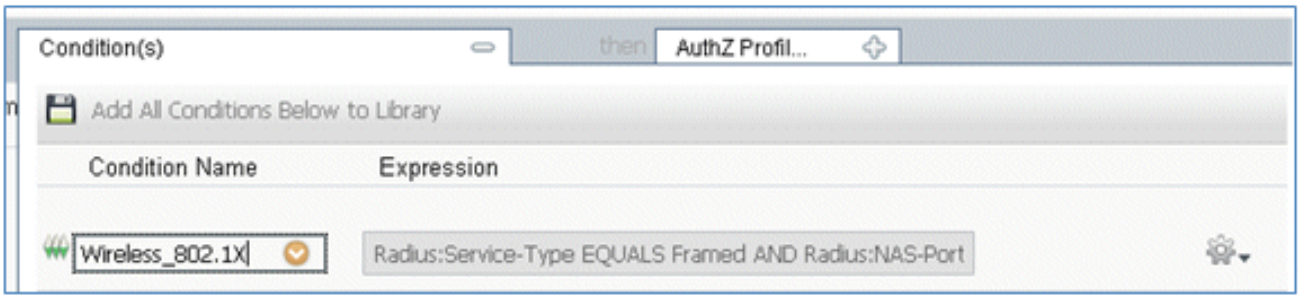
67. 同じルールの右側で、[Edit] の横にある下矢印をクリックして、[Insert New Rule Below] を

選択します。

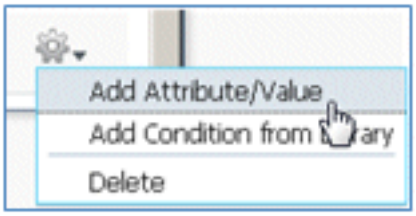
68. ルール名を [Standard Rule #] から [PEAPrule] **に変更します（この例の場合）。**このルールは PEAP 用です（シングル SSID のシナリオでも使用されます）。Transport Layer Security（TLS）なしで 802.1X を認証したかどうか、およびネットワーク サプリカントのプロビジョニングが以前に作成した「Provision」許可プロファイルを使用して開始されたかどうかを確認します。



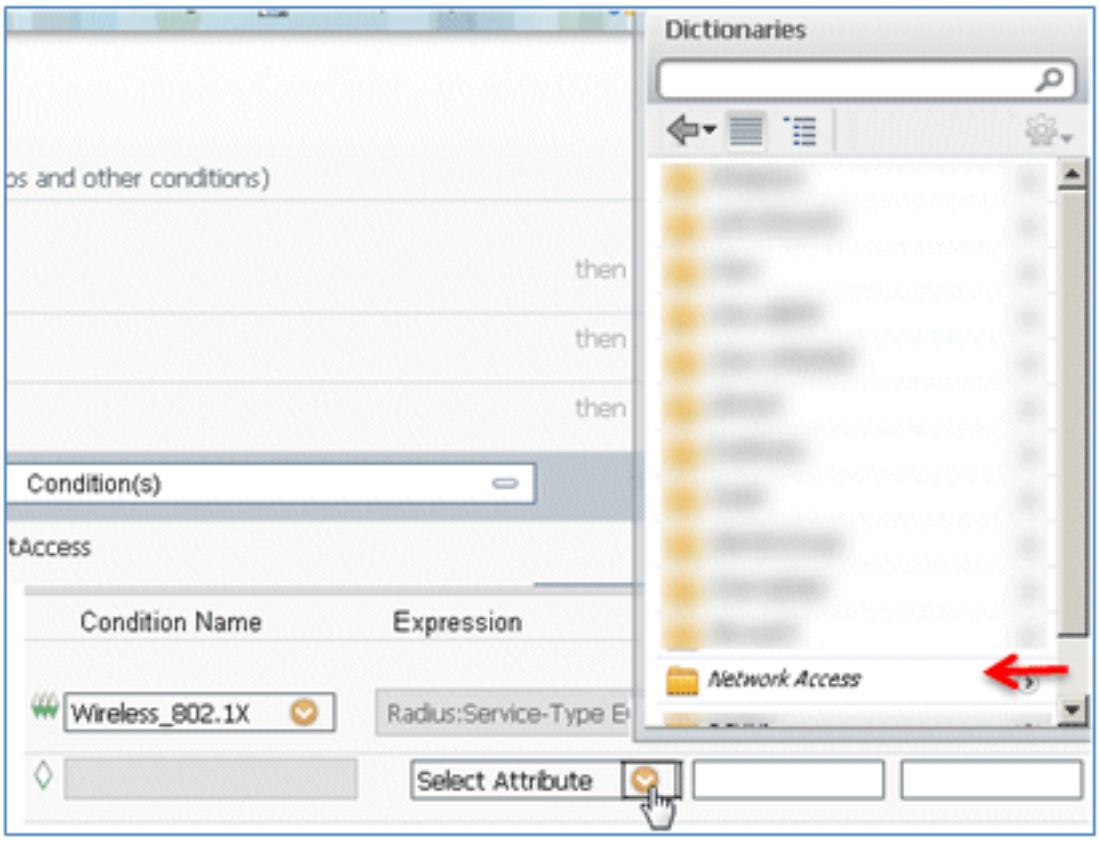
69. 条件を [Wireless_802.1X] に変更します。



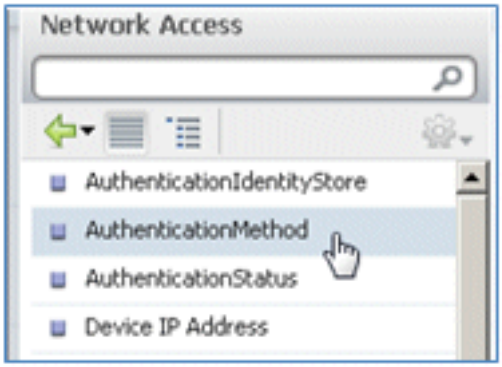
70. 条件の右側にある歯車アイコンをクリックし、[Add Attribute/Value] を選択します。これは、OR 条件ではなく AND 条件です。



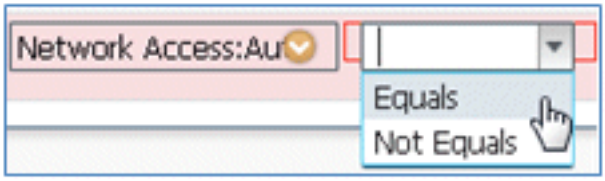
71. [Network Access] を見つけて選択します。



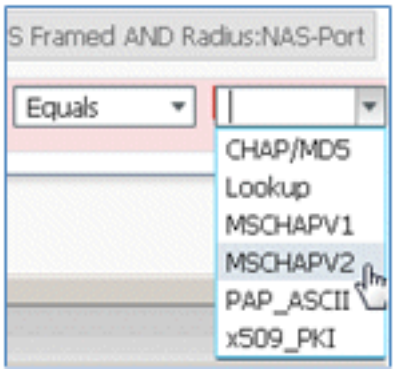
72. [AuthenticationMethod] を選択して、次の値を入力します。



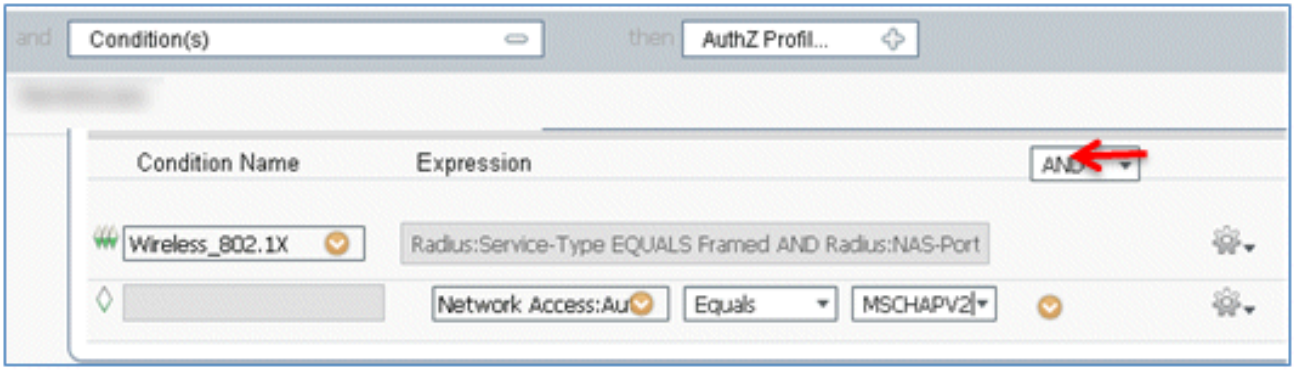
AuthenticationMethod:**Equals**



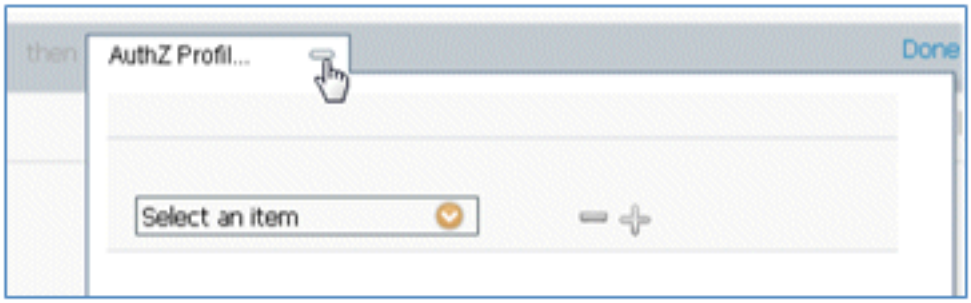
[MSCHAPV2] を選択します。

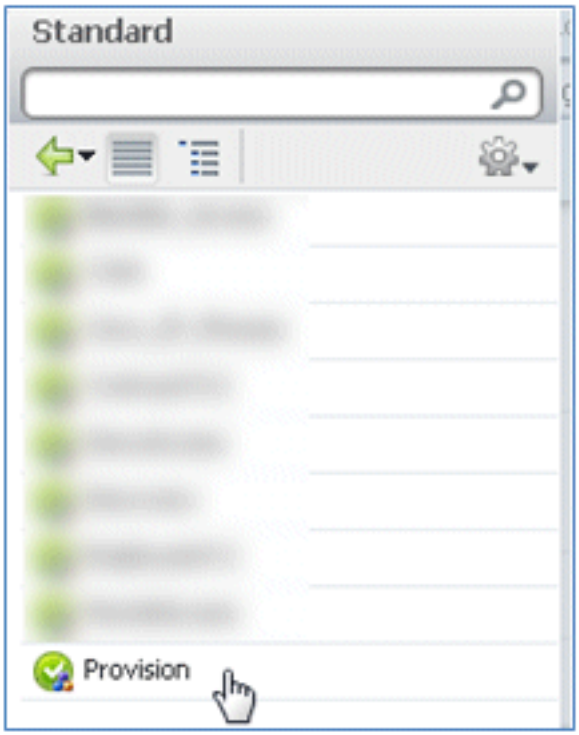


これはルールの例です。条件がANDであることを確認してください。



73. [AuthZ Profile] で、[Standard] **> [Provision]（以前に作成した許可プロファイル）を選択します。**

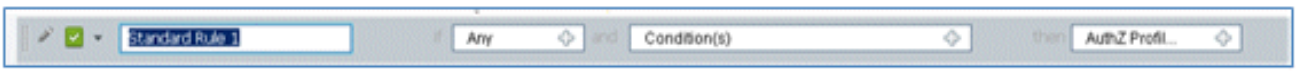




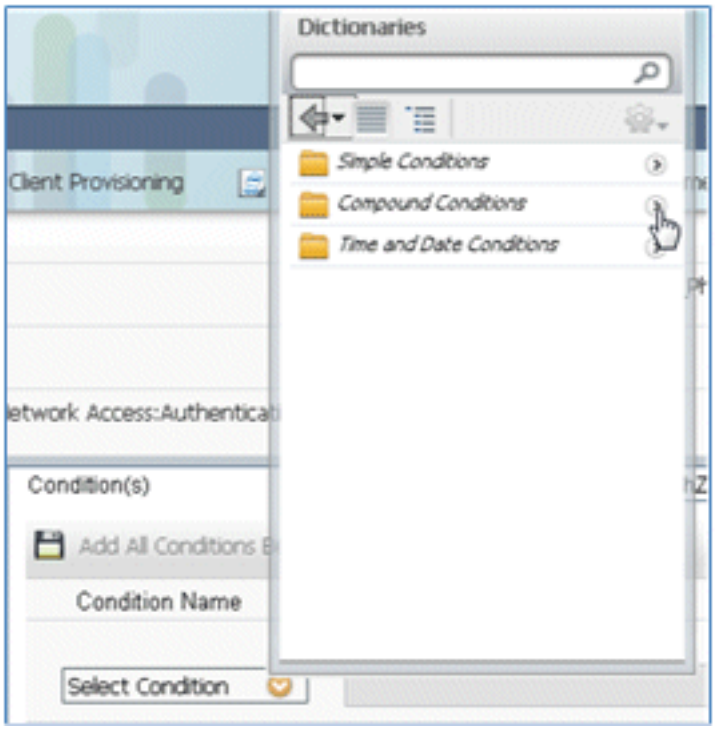
74. [Done] をクリックします。

75. PEAPrule の右側で、[Edit] の横にある下矢印をクリックして、[Insert New Rule Below] を選択します。

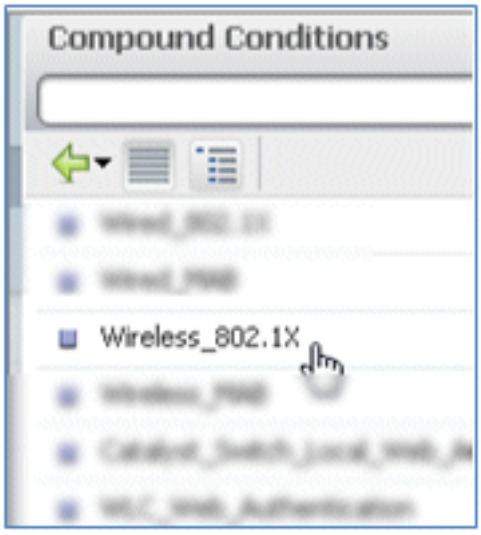
76. ルール名を [Standard Rule #] から [AllowRule] **に変更します (この例の場合) 。**このルールは、証明書がインストールされた登録済みデバイスへのアクセスを許可するために使用されます。



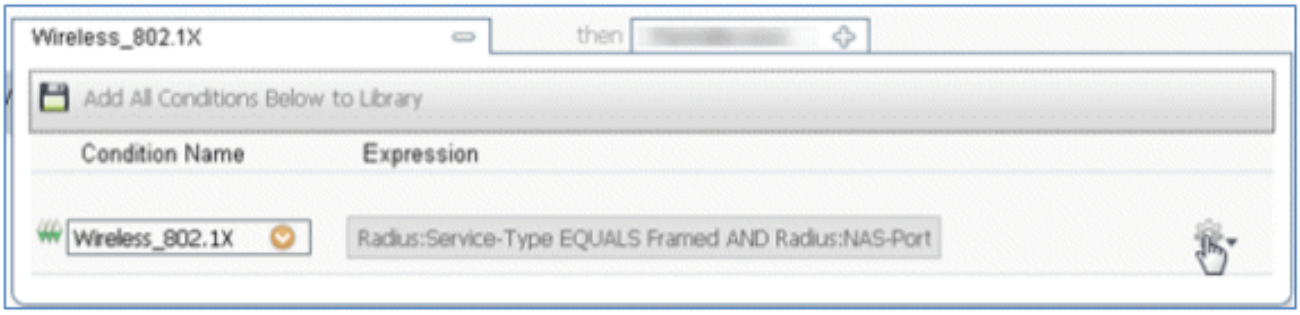
77. [Condition(s)] で [Compound Conditions] を選択します。



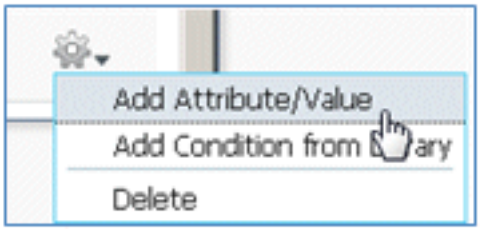
78. [Wireless_802.1X] を選択します。



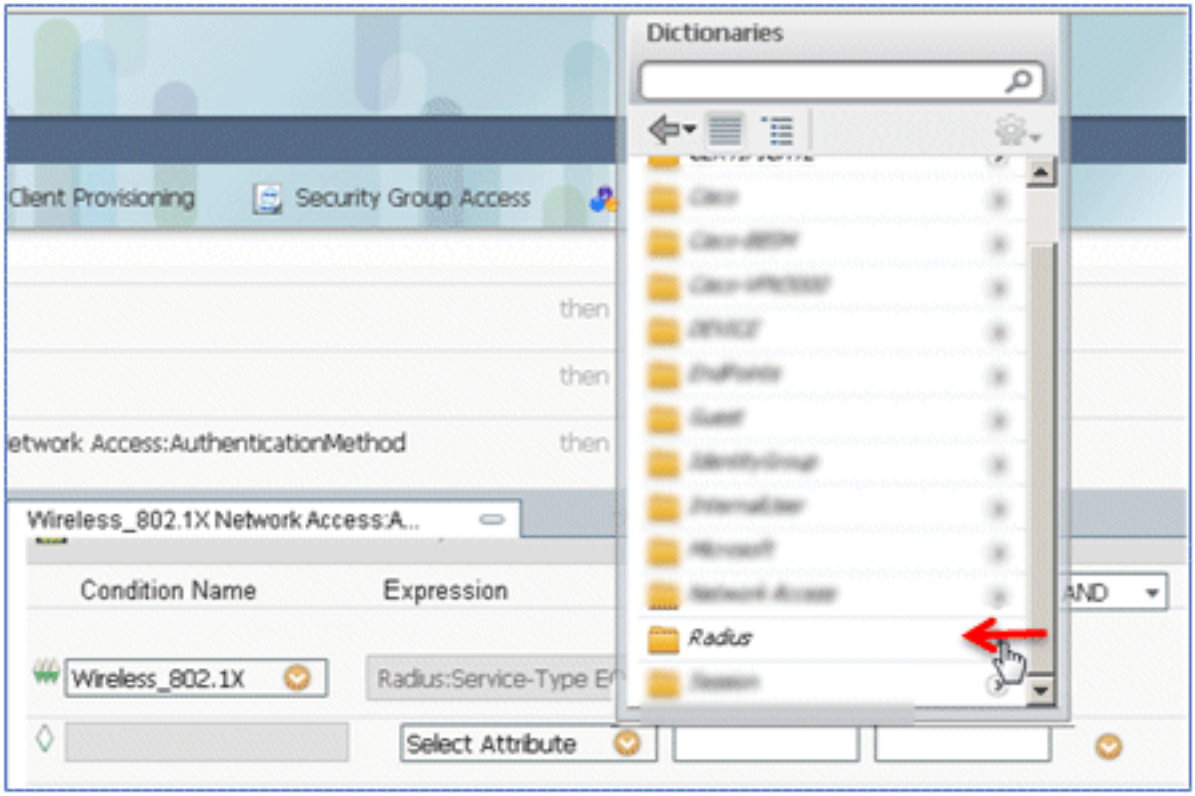
79. AND 属性を追加します。



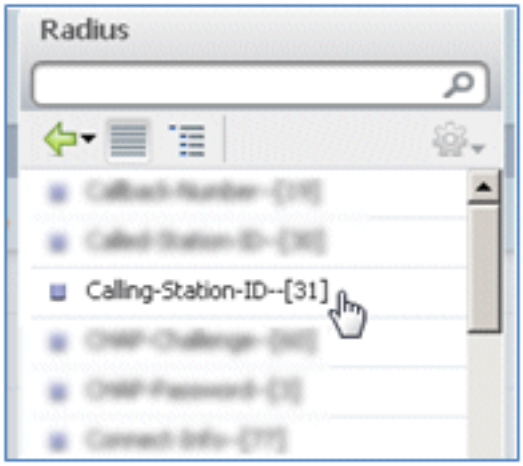
80. 条件の右側にある歯車アイコンをクリックし、[Add Attribute/Value] を選択します。



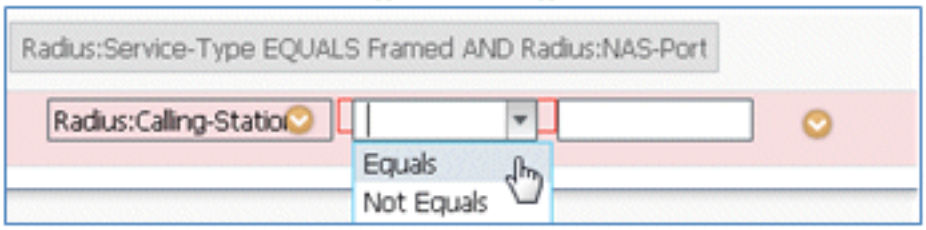
81. [Radius] を見つけて選択します。



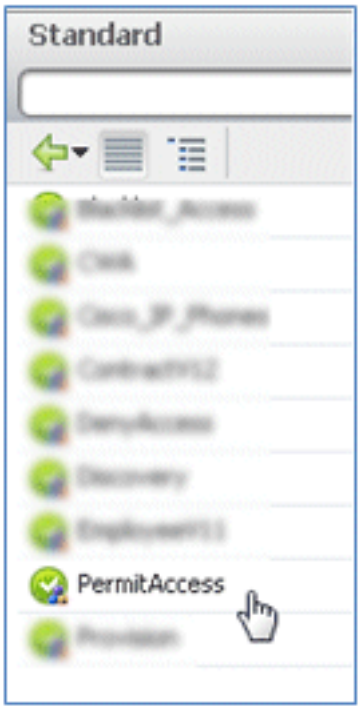
82. [Calling-Station-ID--[31]] を選択します。



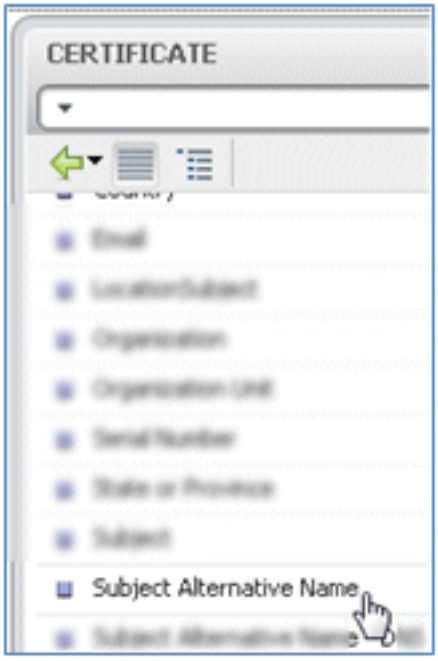
83. [Equals] を選択します。



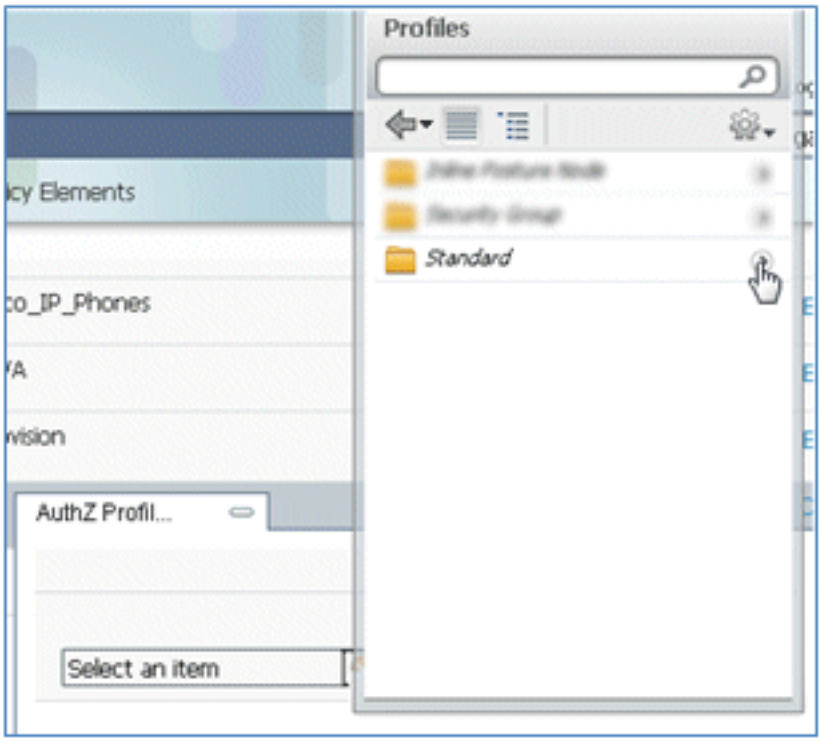
84. [CERTIFICATE] に移動して、右矢印をクリックします。



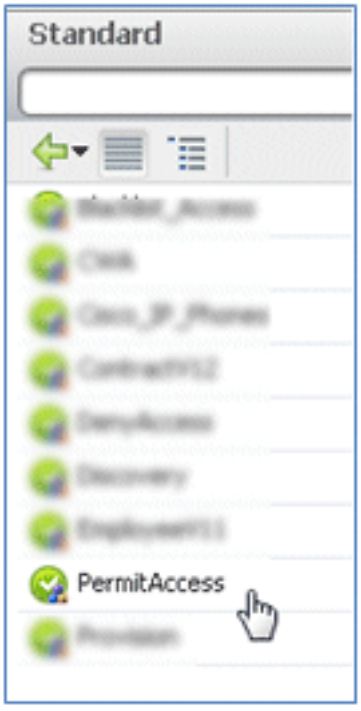
85. [Subject Alternative Name] を選択します。



86. [AuthZ Profile] で [Standard] を選択します。



87. [Permit Access] を選択します。

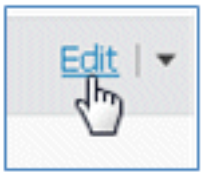


88. [Done] をクリックします。

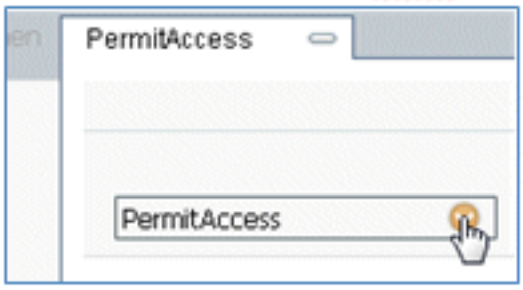
これはルールの例です。

89. [Default] ルールを見つけて、[PermitAccess] を [Deny Access] に変更します。

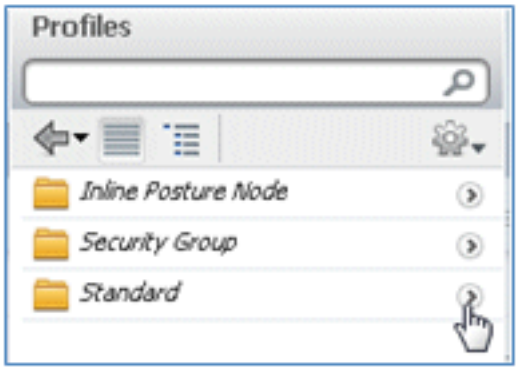
90. [Default] ルールを編集するには、[Edit] をクリックします。



91. PermitAccess の既存の AuthZ プロファイルに移動します。



92. [Standard] を選択します。



93. [DenyAccess] を選択します。

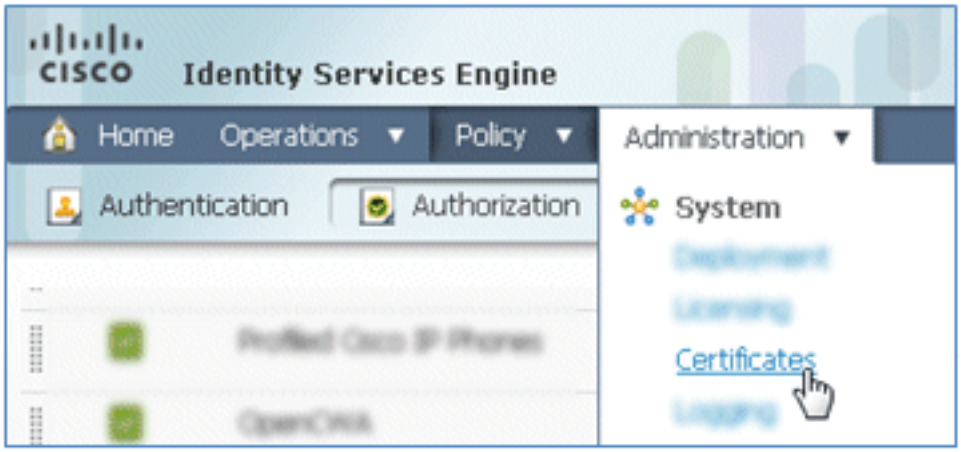
94. 一致が見つからない場合は、[Default] ルールに [DenyAccess] が指定されていることを確認します。

95. [Done] をクリックします。

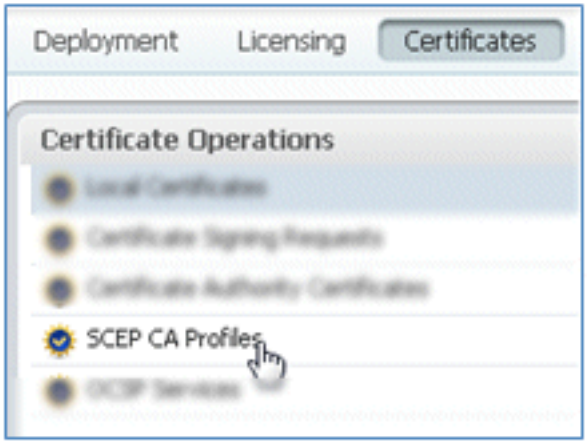
次に、このテストに必要な主なルールの例を示します。これらはシングルSSIDまたはデュアルSSIDのシナリオに適用できます。

96. [Save] をクリックします。

97. [ISE] > **[Administration] > [System] > [Certificates] に移動して、SCEP プロファイルで ISE サーバを設定します。**



98. [Certificate Operations] で [SCEP CA Profiles] をクリックします。



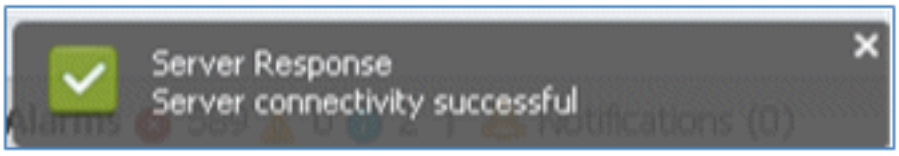
99. [Add] をクリックします。

100. このプロファイルについて次の値を入力します。

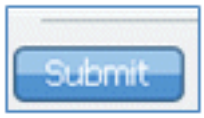
名前：**mySCEP**（この例では）URL:**https://**<ca-server>**/CertSrv/mscep/**（CAサーバの設定で正しいアドレスを確認します）

101. SCEP 接続をテストするには、[Test Connectivity] をクリックします。

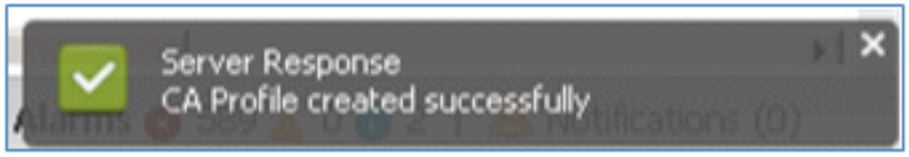
102. この応答は、サーバ接続が正常であることを示しています。



103. [Submit] をクリックします。



104. サーバ応答により、CA プロファイルが正常に作成されたことが示されます。



105. SCEP CA プロファイルが追加されたことを確認します。

ユーザ エクスペリエンス：iOS のプロビジョニング

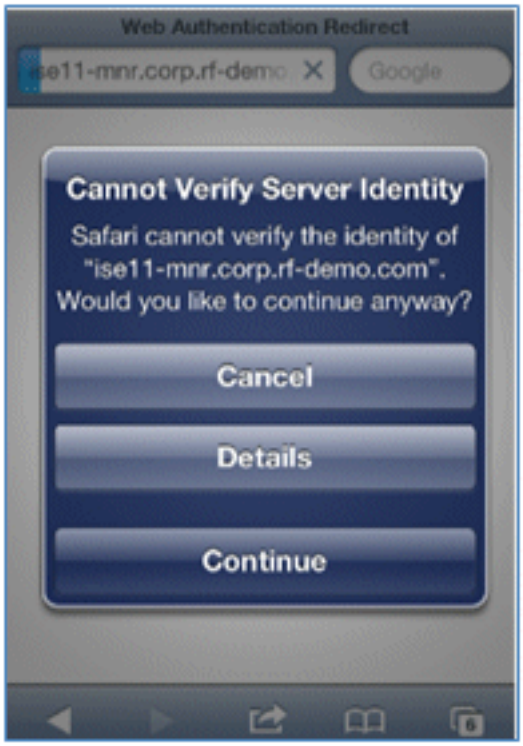
デュアル SSID

このセクションでは、デュアル SSID について扱われ、ビジョニングするゲストへの接続方法と 802.1x WLAN への接続方法が説明されます。

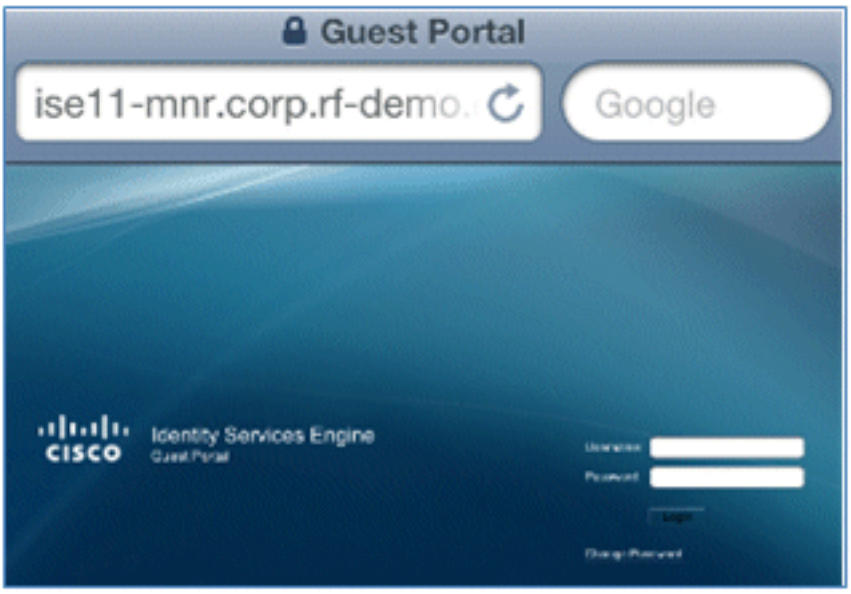
デュアル SSID のシナリオで iOS をプロビジョニングするには、次の手順を実行します。

1. iOS デバイスで、[Wi-Fi Networks] に移動して、[DemoCWA]（WLC で設定済みのオープン WLAN）を選択します。

2. iOS デバイスで Safari ブラウザを開き、到達可能な URL (たとえば、内部または外部 Web サーバ) にアクセスします。ISE がポータルにリダイレクトされます。[Continue] をクリックします。



3. ログインのためにゲスト ポータルにリダイレクトされます。



4. AD ユーザ アカウントとパスワードを使用してログインします。プロンプトが表示されたら CA プロファイルをインストールします。

5. CA サーバの信頼できる証明書の [Install] をクリックします。

6. プロファイルが完全にインストールされたら [Done] をクリックします。

7. ブラウザに戻って、[Register].をクリックします。デバイスの MAC アドレスが含まれているデバイス ID をメモします。

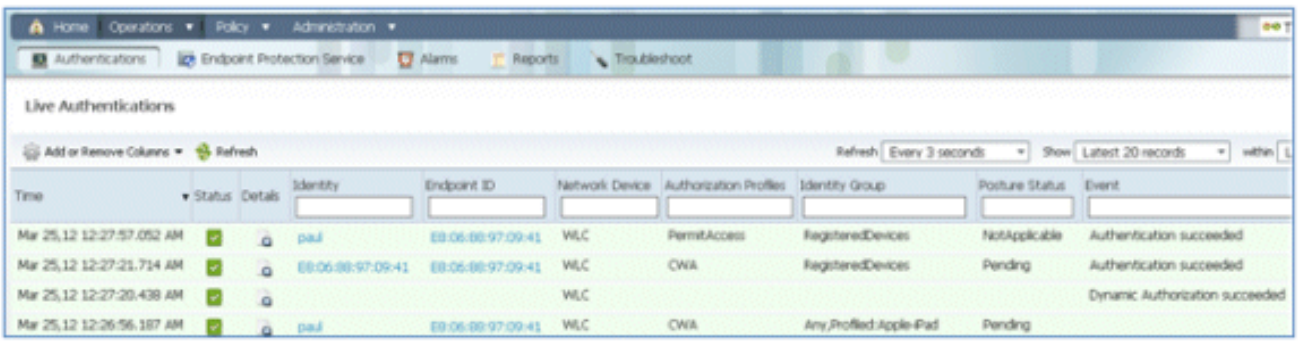
8. 確認したプロファイルをインストールするには、[Install] をクリックします。

9. [Install Now] をクリックします。

10. プロセスの完了後に、WirelessSP プロファイルがインストールされたことを確認します。[Done] をクリックします。

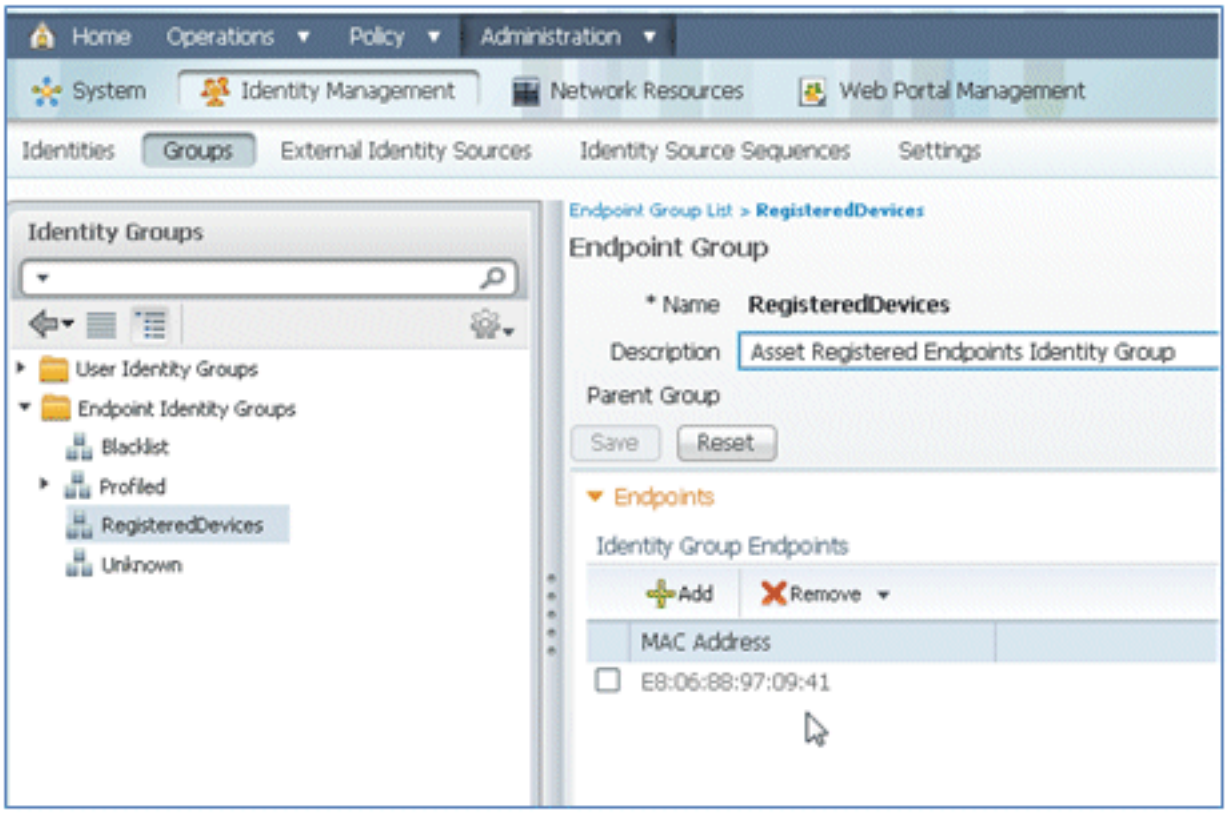
11. [Wi-Fi Networks] に移動して、ネットワークを [Demo1x] に変更します。これで、TLS を使用してデバイスが接続されます。

12. ISE で、[Operations] > **[Authentications]** に移動します。イベントに、デバイスがオープンなゲスト ネットワークに接続されるプロセスが表示され、サプリカント プロビジョニングを使用して登録プロセスが行われて、登録後にアクセスが許可されます。



13. [ISE] > **[Administration] > [Identity Management] > [Groups]** > [Endpoint Identity Groups] >

[RegisteredDevices] に移動します。MAC アドレスがデータベースに追加されます。

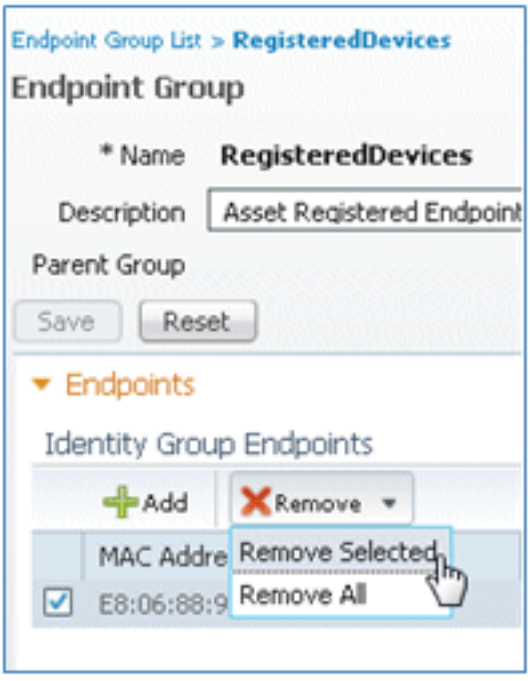


シングル SSID

これはシングル SSID に関するセクションであり、802.1x WLAN に直接接続する方法、PEAP を使用して認証するための AD ユーザ名/パスワードを指定する方法、およびゲストを介したプロビジョニングと TLS との再接続を行う方法について説明されています。

シングル SSID のシナリオで iOS をプロビジョニングするには、次の手順を実行します。

1. 同じ iOS デバイスを使用する場合、登録済みデバイスからエンドポイントを削除します。



2. iOS デバイスで、[Settings] **> [Generals] > [Profiles]** に移動します。この例でインストールされたプロファイルを削除します。

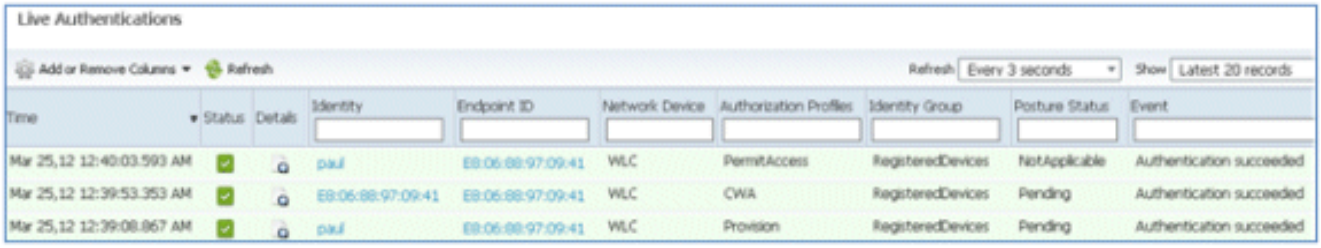
3. 前のプロファイルを削除するには、[Remove] をクリックします。

4. 既存の（クリアされた）デバイスを使用するか、新しい iOS デバイスを使用する場合は 802.1x に直接接続します。

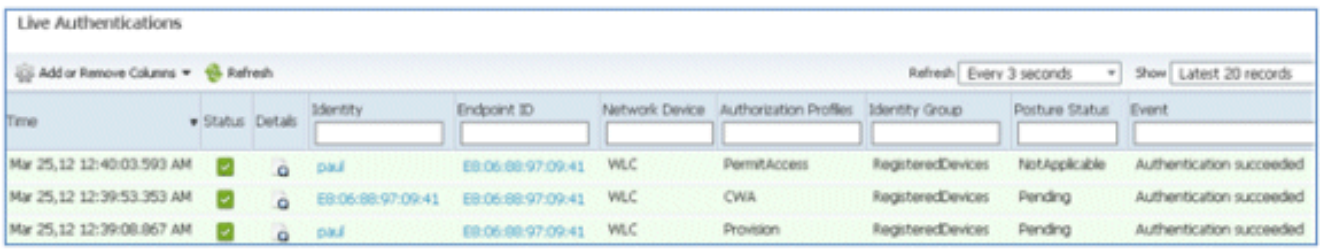
5. **Dot1x** に接続して、[Username] と [Password] に入力して、[Join] をクリックします。

6. 適切なプロファイルが完全にインストールされるまで、「ISE の設定」セクションのステップ 90 以降を繰り返します。

7. プロセスをモニタするには、[ISE] > **[Operations] > [Authentications] に移動します。**ここでは、802.1X WLAN に直接接続されたクライアントがプロビジョニングされ、切断されてから、TLS を使用して同じ WLAN に再接続する例を示します。



8. [WLC] > **[Monitor] > [Client MAC]** に移動します。クライアントの詳細から、クライアントが RUN 状態になっていて、その [Data Switching] は [local] に設定され、[Authentication] が [Central] になっていることがわかります。これは、FlexConnect AP に接続されているクライアントに当てはまります。



ユーザ エクスペリエンス：Android のプロビジョニング

デュアル SSID

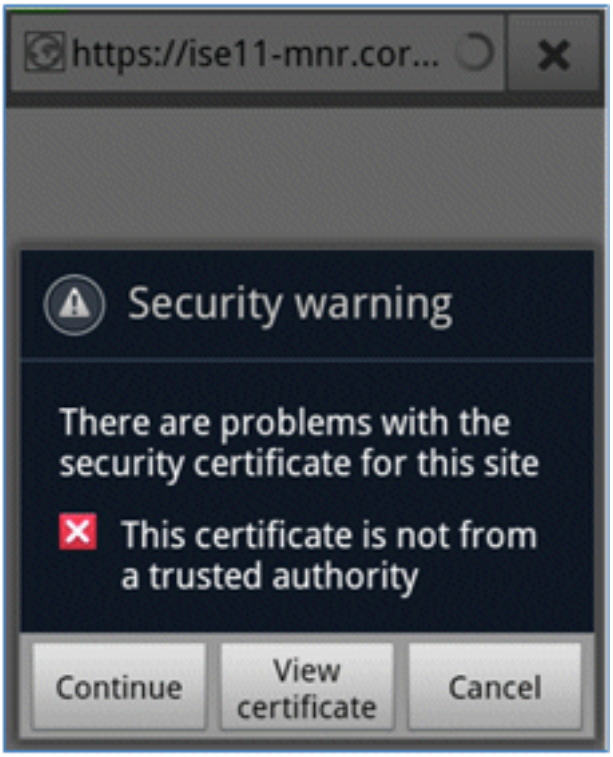
このデュアル SSID に関するセクションでは、プロビジョニングするゲストへの接続方法と 802.1x WLAN への接続方法を説明します。

Android デバイスへの接続プロセスは、iOS デバイス (シングルまたはデュアル SSID) への接続プロセスと非常によく似ています。違いは、Android デバイスでは、Google マーケットプレイス (現在では Google Play) にアクセスし、サプリカント エージェントをダウンロードするには、インターネットへのアクセスが必要であるという点です。

デュアル SSID のシナリオで Android デバイス (この例で Samsung Galaxy など) をプロビジョニングするには、次の手順を実行します。

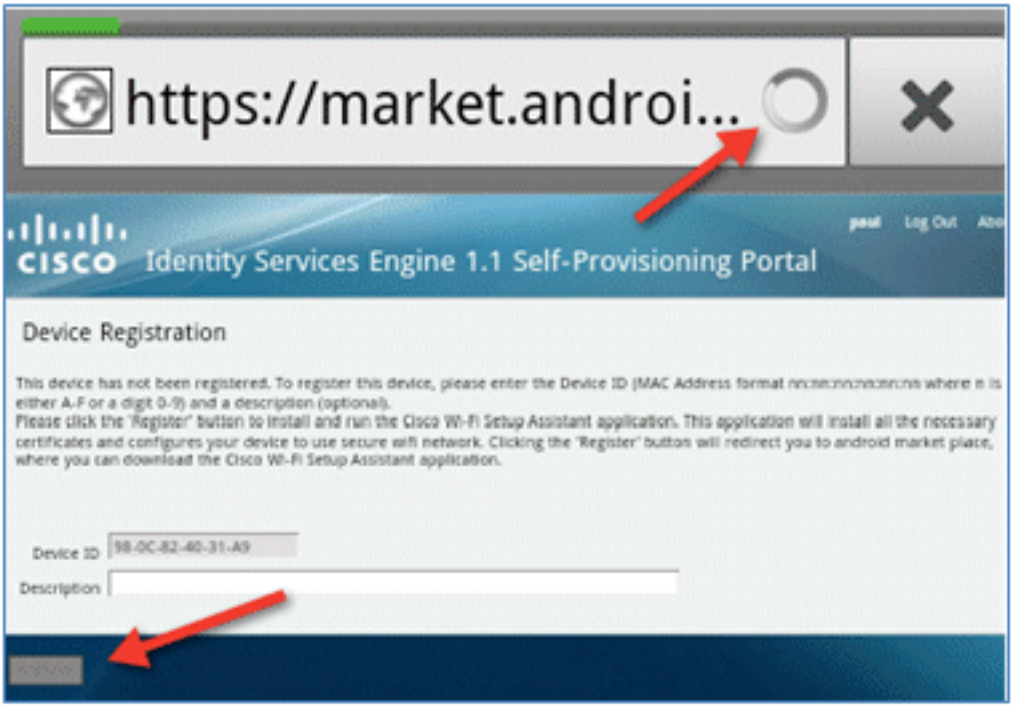
1. Android デバイスで、Wi-Fi 経由で [DemoCWA] に接続して、ゲスト WLAN を開きます。

2. ISE に接続するには、証明書を受け入れます。

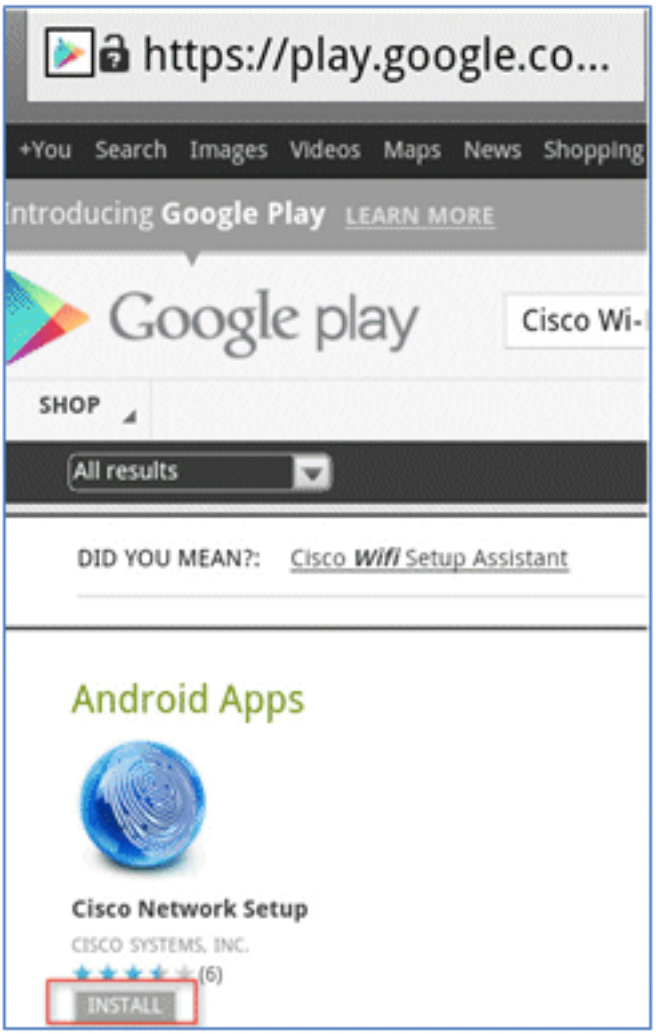


3. ログインするには、ゲスト ポータルで [Username] と [Password] に入力します。

4. [Register] をクリックします。デバイスは Google マーケットプレイスにアクセスするためにインターネットに到達しようとします。インターネットへのアクセスを許可するには、コントローラで追加のルールを事前認証 ACL（ACL-REDIRECT など）に追加します。

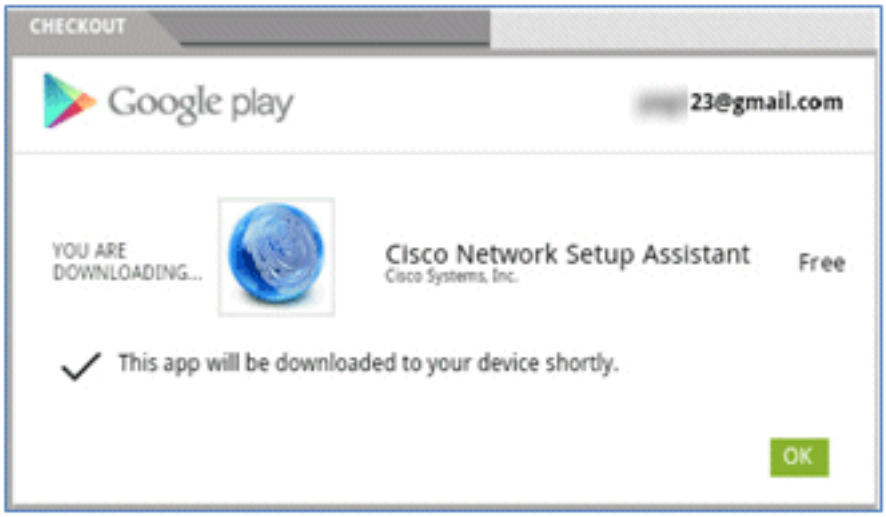


5. Google には [Android App] に [Cisco Network Setup] がリストされます。[INSTALL] をクリックします。

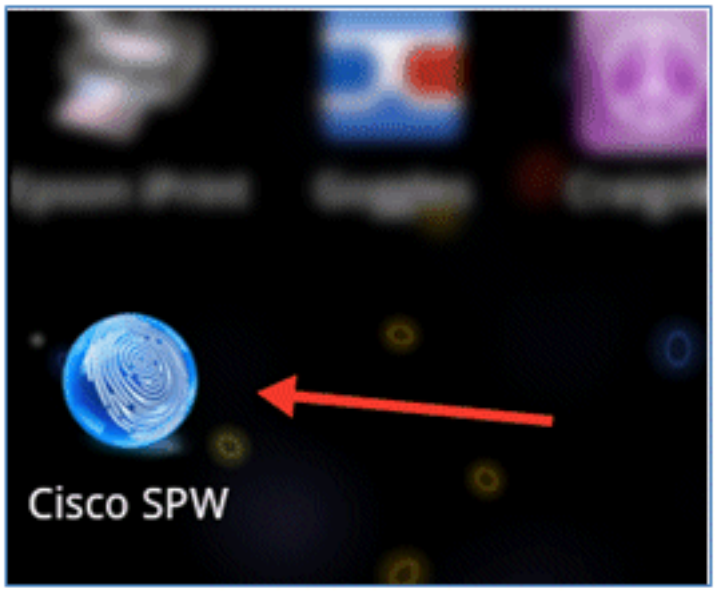


6. Google にサインインして、[INSTALL] をクリックします。

7. [OK] をクリックします。



8. Android デバイスで、インストールされた **Cisco SPW アプリを見つけて開きます。**



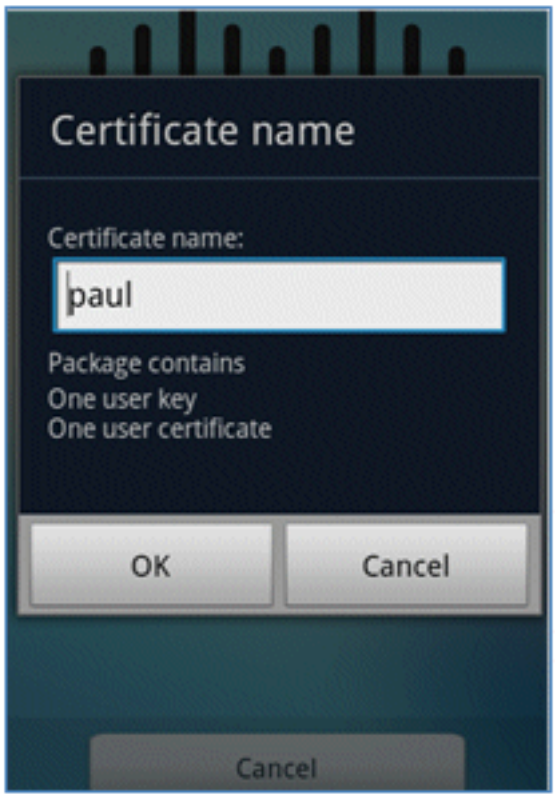
9. Android デバイスからまだゲスト ポータルにログインしたままにしてください。

10. Wi-Fi Setup Assistant を開始するには、[Start] をクリックします。

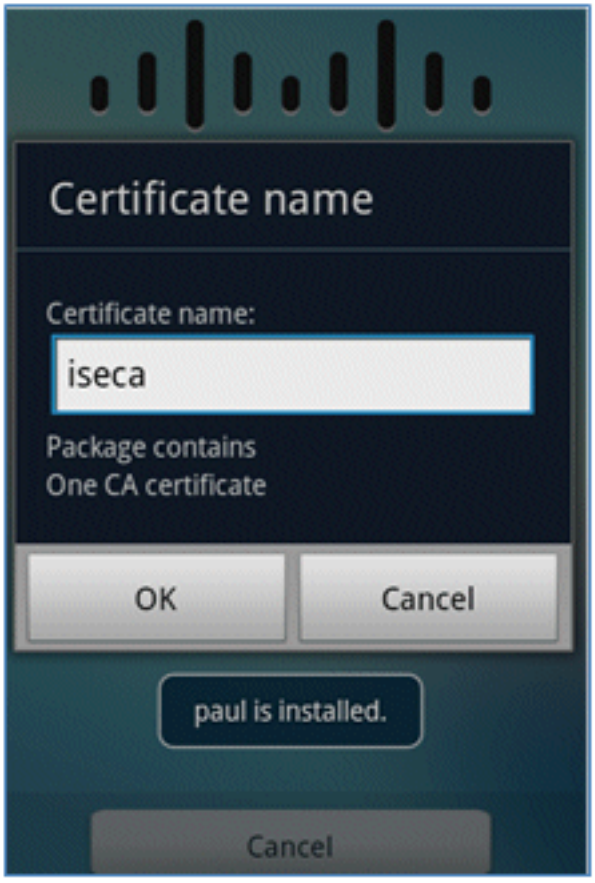
11. Cisco SPW が証明書のインストールを開始します。

12. プロンプトが表示されたら、クレデンシャルを保存するためのパスワードを設定します。

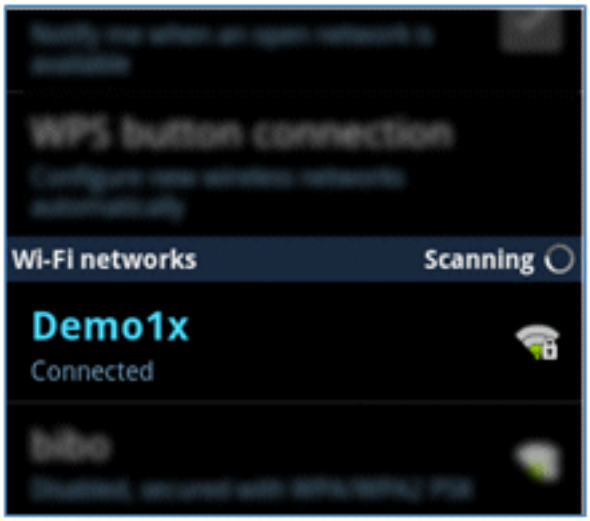
13. ユーザ キーと証明書が含まれている証明書名が示された Cisco SPW に戻ります。[OK] をクリックして確認します。



14. Cisco SPW はプロセスを続行して、CA 証明書が含まれている別の証明書名のプロンプトを表示します。名前（この例では **iseca** ）**を入力し、[OK]** をクリックして続行します。



15. Android デバイスが接続されます。

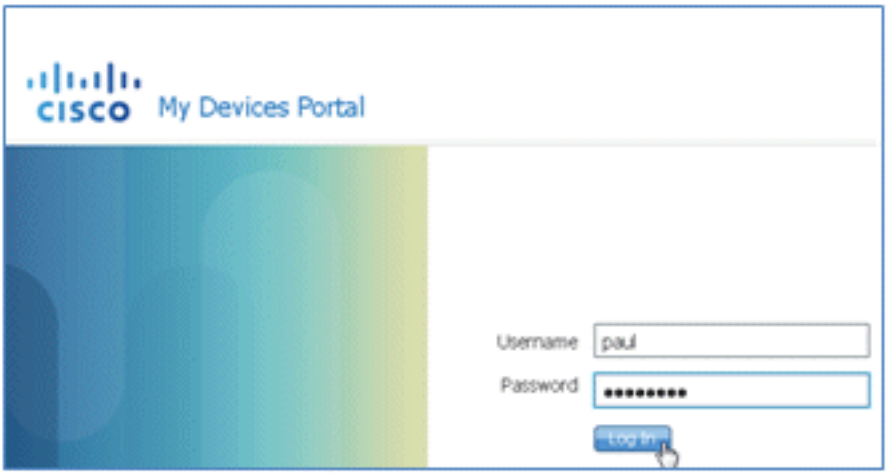


デバイス ポータル

My Devices ポータルでは、ユーザは、デバイスの損失/盗難の場合に以前に登録したデバイスをブラックリストに登録できます。また、ユーザは必要に応じて再度リストに入れることもできます。

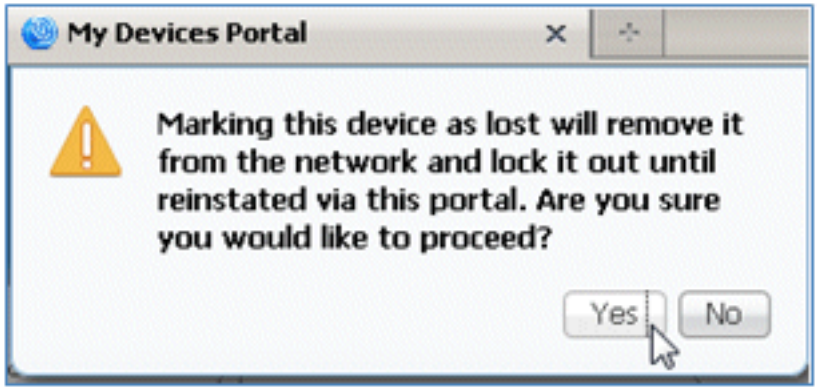
デバイスをブラックリストに登録するには、次の手順を実行します。

1. My Devices ポータルにログインするには、ブラウザを開き、https://ise-server:8443/mydevices（ポート番号は 8443 であることに注意してください）に接続して、AD アカウントを使用してログインします。



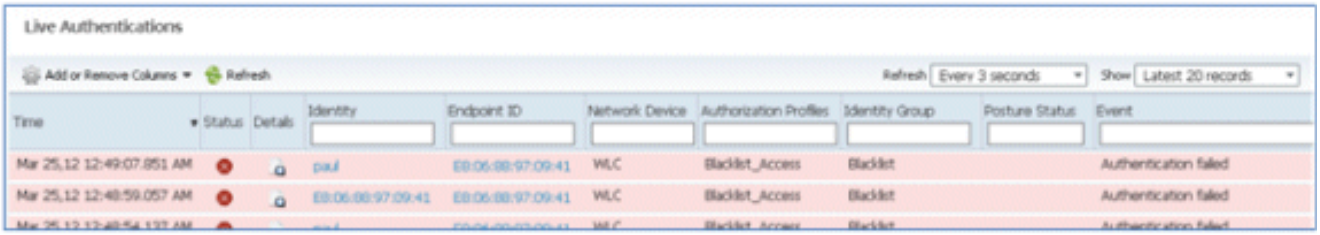
2. [Device ID] でデバイスを見つけて、[Lost?] をクリックしてデバイスのブラックリストへの登録を開始します。

3. ISE が警告を表示したら、[Yes] をクリックして続行します。



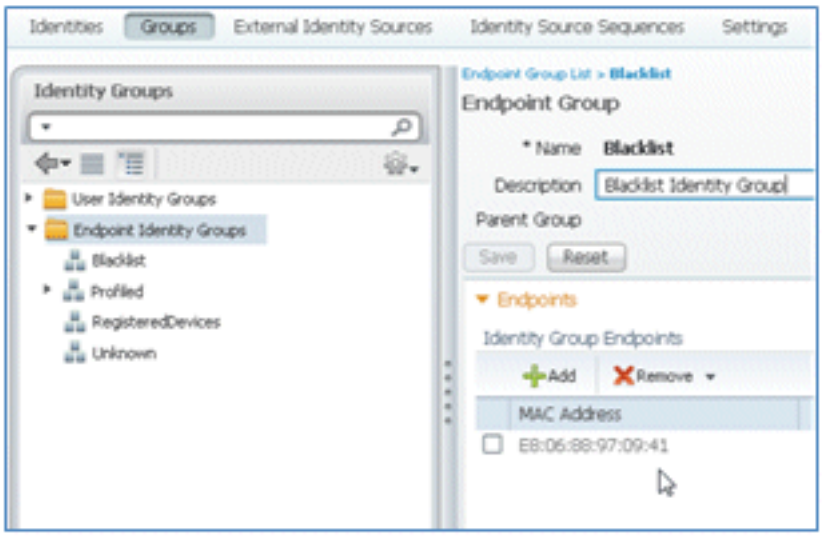
4. ISE は、デバイスを [lost] として正常にマークしたことを確認します。

5. 以前に登録されたデバイスを使用してネットワークに接続しようとすると、有効な証明書がインストールされている場合でもブロックされます。次に、認証に失敗する、ブラックリストに登録されたデバイスの例を示します。



6. 管理者は、[ISE] > **[Administration] > [Identity Management] > [Groups] に移動し、[Endpoint Identity Groups] > [Blacklist]** をクリックして、ブラックリストに登録されたデバイスを確認

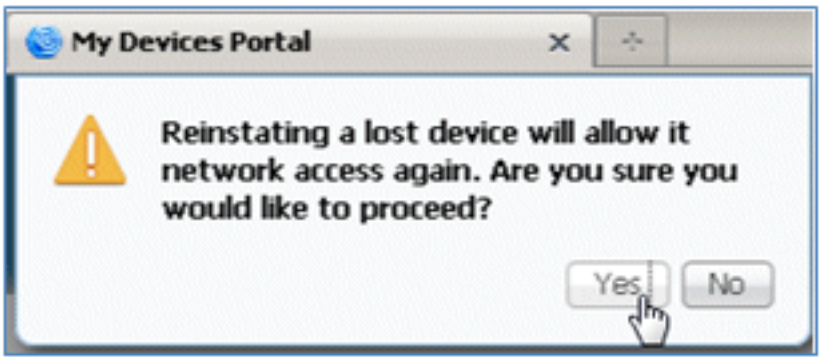
できます。



ブラックリストに登録したデバイスを復元するには、次の手順を実行します。

1. My Devices ポータルから、そのデバイスの [Reinstate] **をクリックします。**

2. ISE が警告を表示したら、続行するには [Yes] をクリックします。



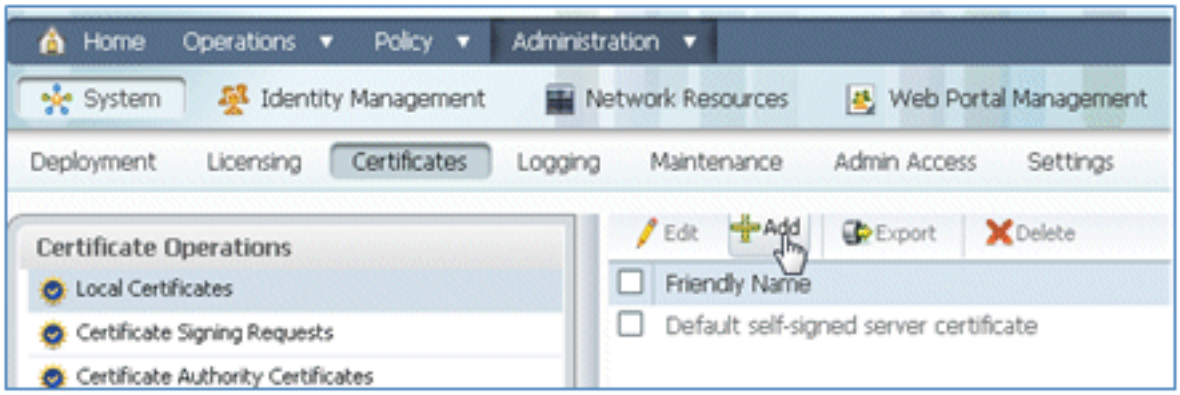
3. ISE は、デバイスが正常に復元されたことを確認します。復元したデバイスをネットワークに接続して、デバイスが許可されていることをテストできます。

参考：証明書

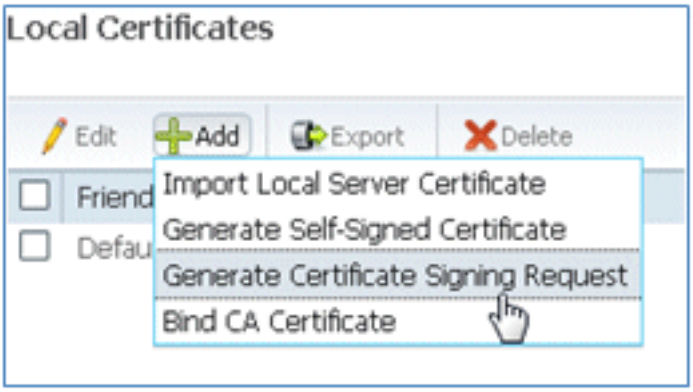
ISE では、有効な CA ルート証明書のみでなく、CA によって署名された有効な証明書が必要です。

新しい信頼できる CA 証明書を追加、バインド、およびインポートするには、次の手順を実行します。

1. [ISE] > **[Administration] > [System] > [Certificates]** に移動し、[Local Certificates] をクリックして、[Add] をクリックします。



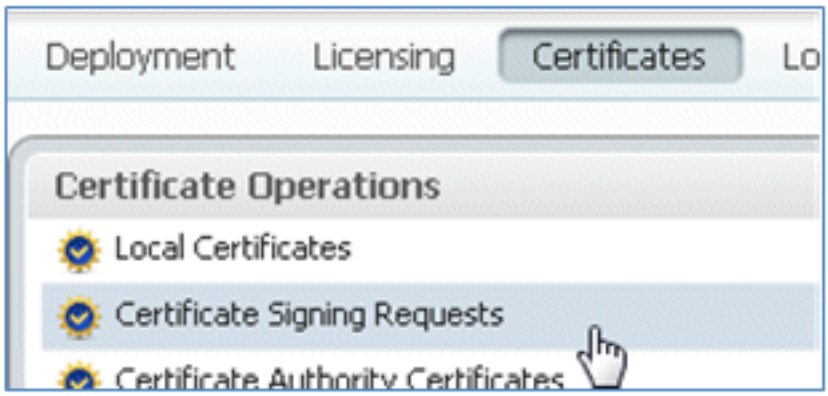
2. [Generate Certificate Signing Request]（CSR）を選択します。



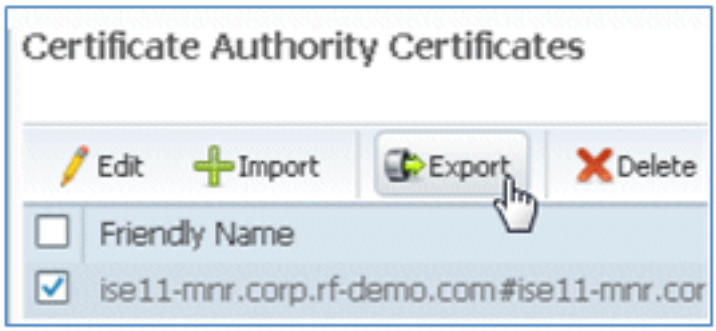
3. [Certificate Subject] に [CN=<ISE-SERVER hostname.FQDN>] を入力します。他のフィールドには、デフォルトまたは CA の設定で必要な値を使用できます。[Submit] をクリックします。

4. ISE は、CSR が生成されたことを確認します。

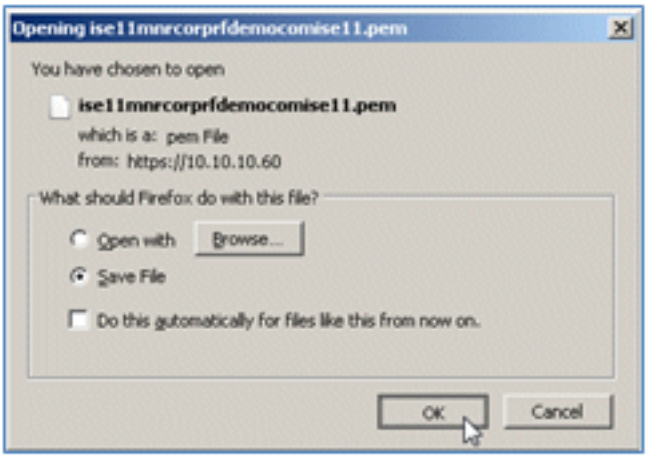
5. CSR にアクセスするには、[Certificate Signing Requests] 操作をクリックします。



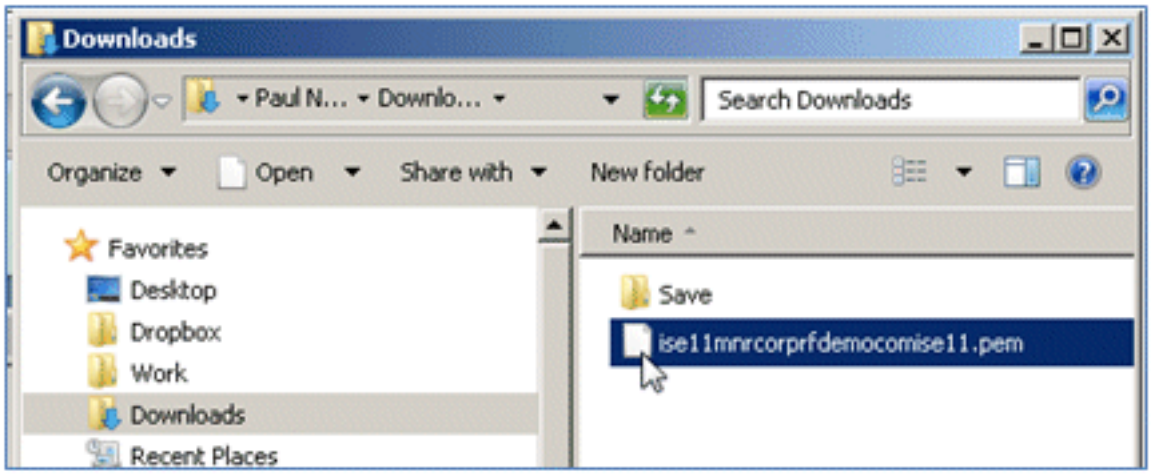
6. 新しく作成した CSR を選択して、[Export].をクリックします。



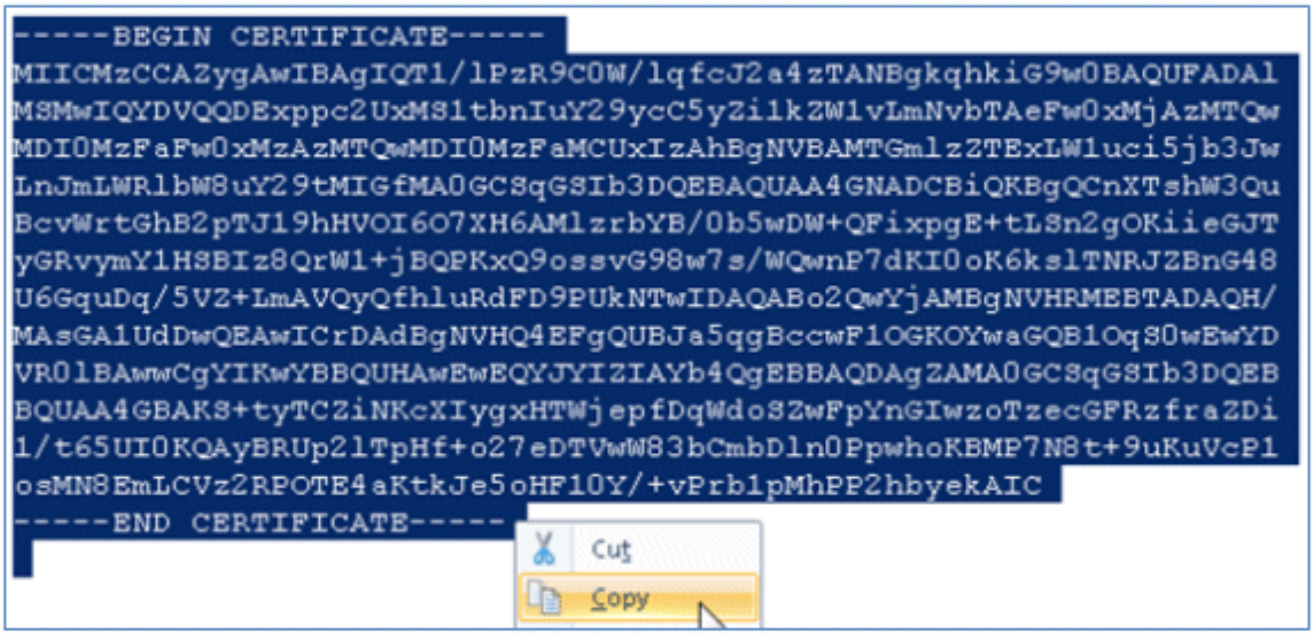
7. ISE は CSR を .pem ファイルにエクスポートします。[Save File] をクリックして、[OK] をクリックし、ファイルをローカル マシンに保存します。



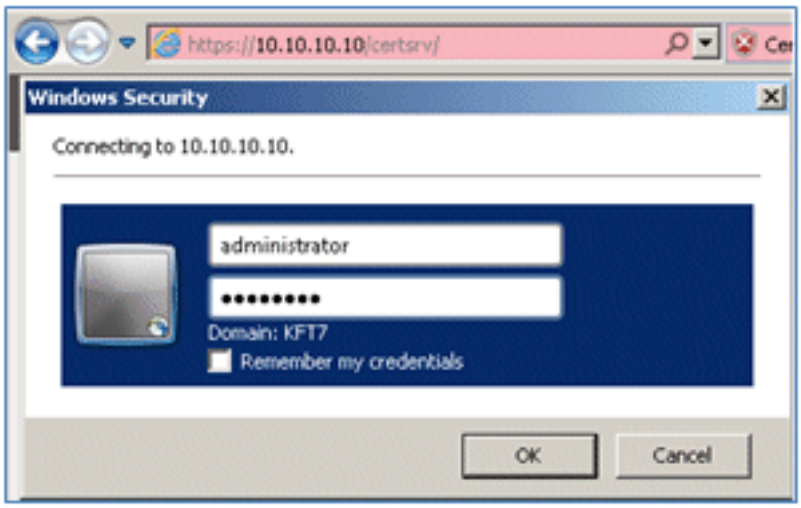
8. ISE 証明書ファイルを見つけて、テキスト エディタで開きます。



9. 証明書の内容全体をコピーします。

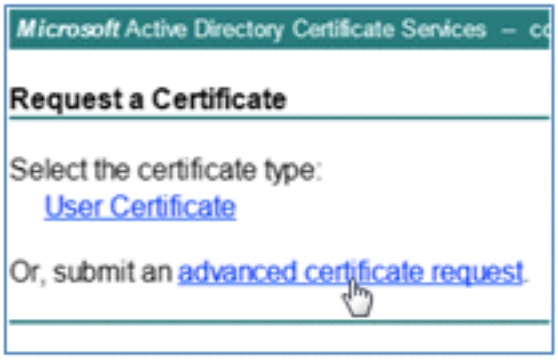


10. CA サーバに接続して、管理者アカウントを使用してログインします。サーバは、https://10.10.10.10/certsrv の Microsoft 2008 CA です（この例の場合）。

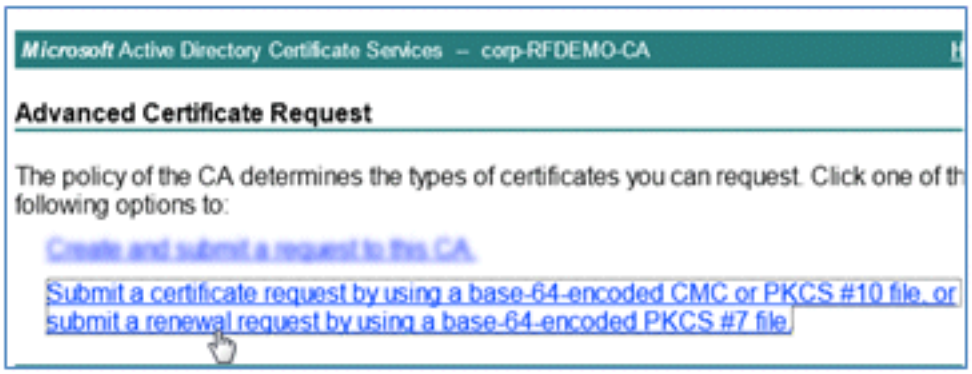


11. [Request a certificate] をクリックします。

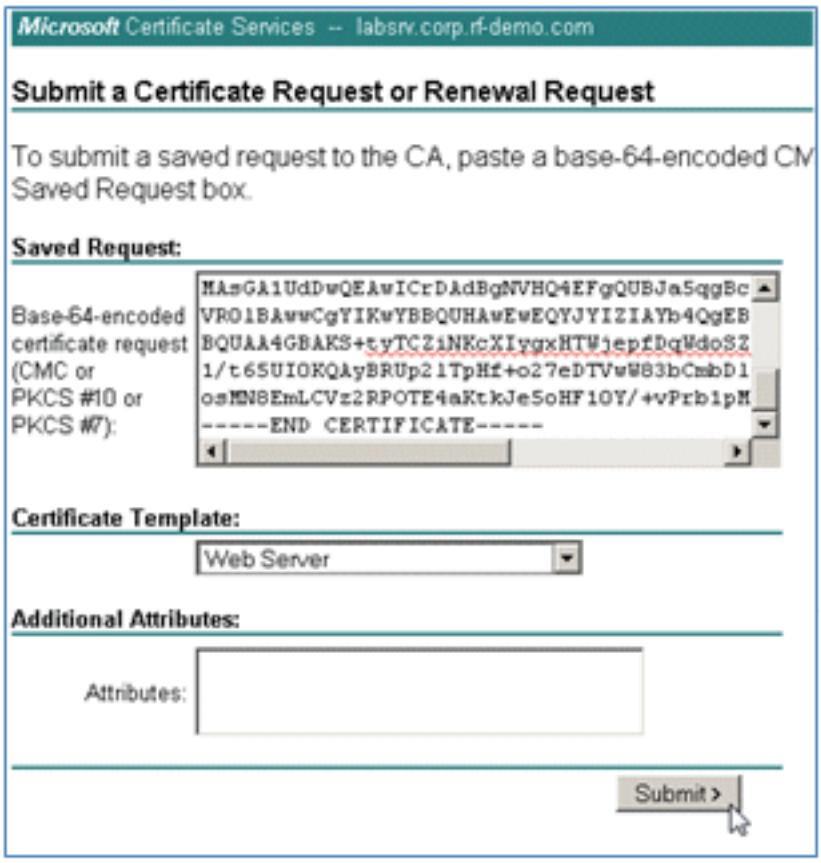
12. [advanced certificate request] をクリックします。



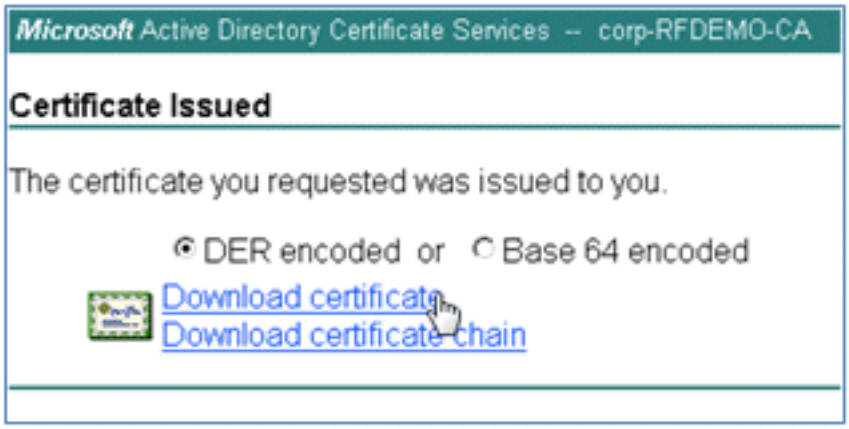
13. 2番目のオプションをクリックして、**Submit a certificate request by using a base-64-encoded CMC or ....**



14. ISE 証明書ファイル（.pem）の内容を [Saved Request] フィールドに貼り付けて、[Certificate Template] が [Web Server] であることを確認し、[Submit] をクリックします。

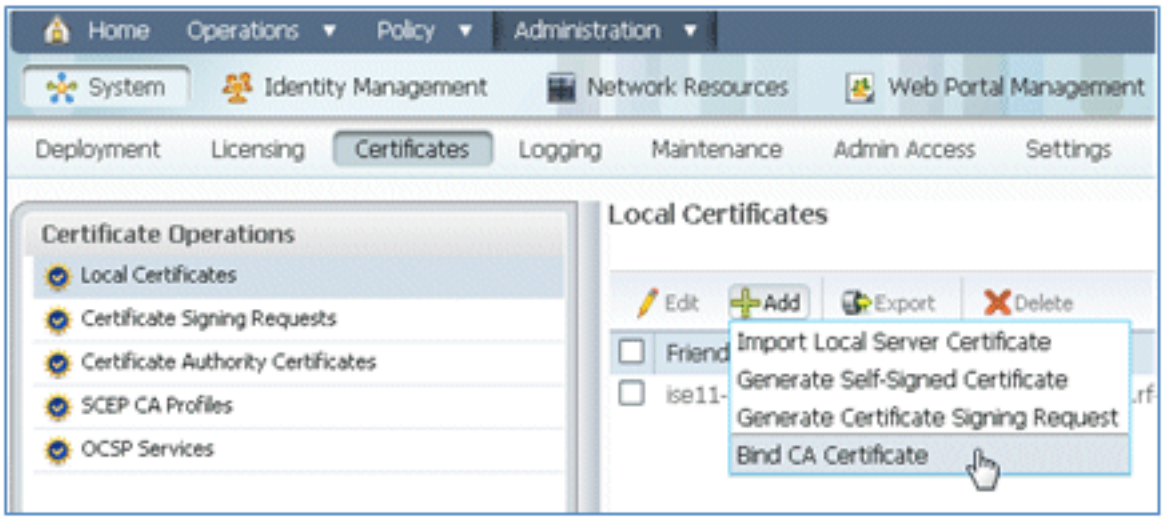


15. [Download certificate] をクリックします。

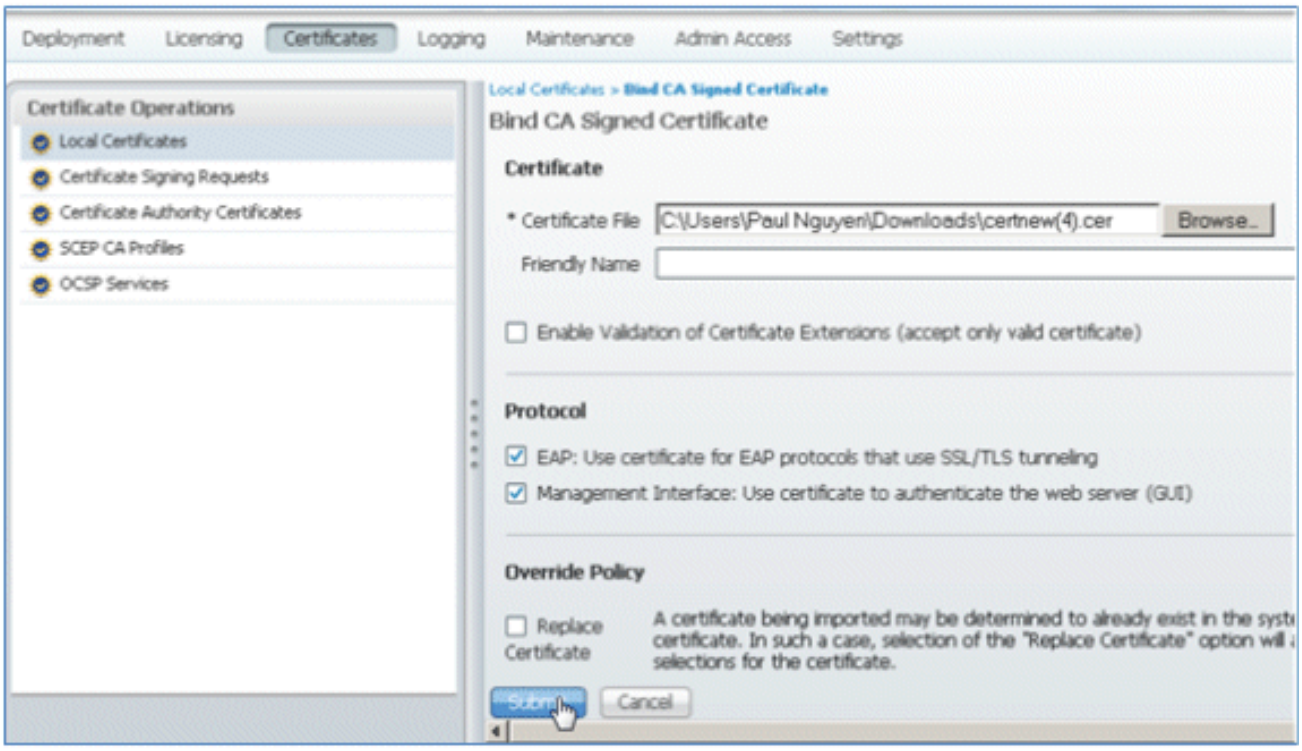


16. certnew.cerファイルを保存します。このファイルは、後でISEとのバインドに使用されます。

17. ISE の [Certificates] から、[Local Certificates] に移動し、[Add] > [Bind CA Certificate] をクリックします。



18. 前の手順でローカル マシンに保存した証明書を参照して、[EAP] と **[Management Interface] の両方のプロトコルを有効にします（ボックスをチェック）。その後、[Submit].をクリックします。**ISE がサービスを再起動するのに数分以上かかる場合があります。

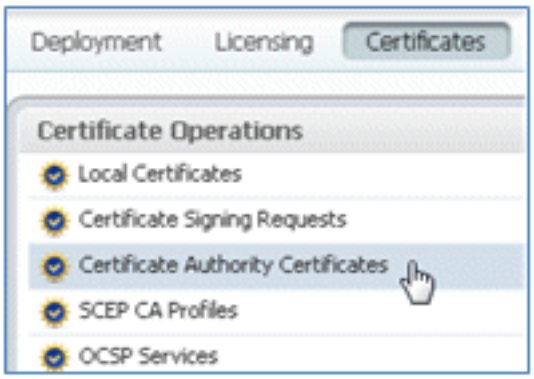


19. CA のランディング ページ（https://CA/certsrv/）に戻り、[Download a CA certificate, certificate chain, or CRL] をクリックします。

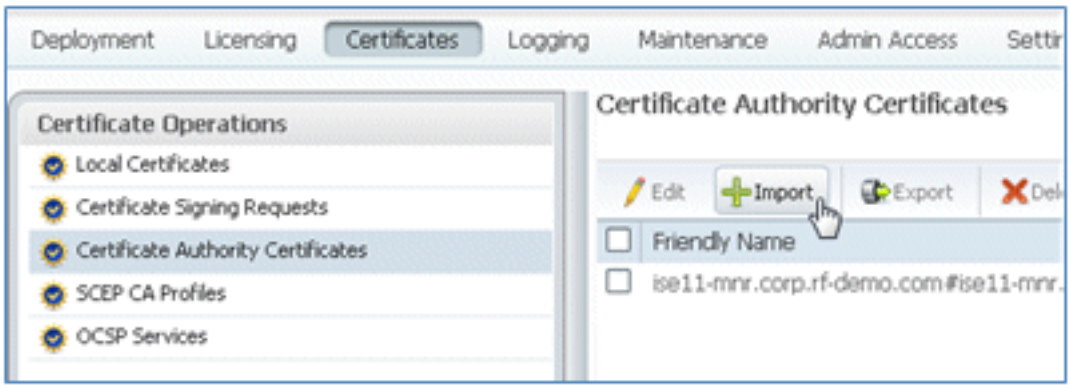
20. [Download CA certificate] をクリックします。

21. **[Save] をクリックして、ファイルをローカル マシンに保存します。**

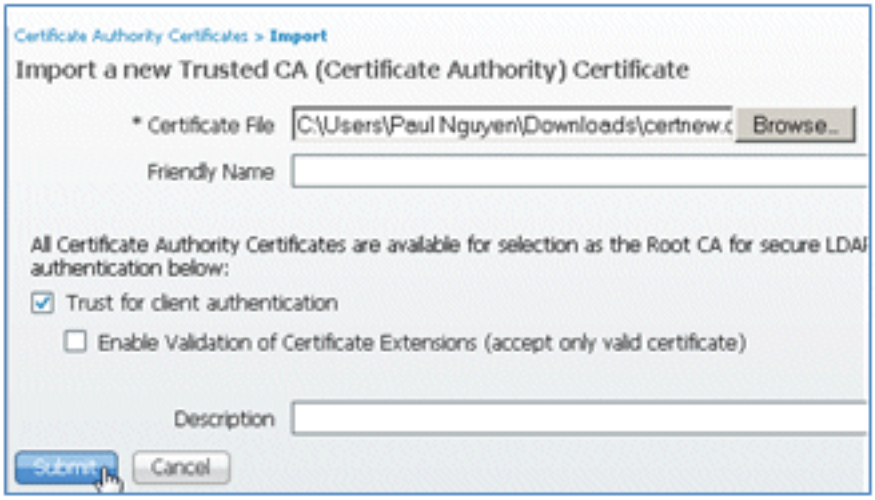
22. ISE サーバがオンラインの状態で、[Certificates] に移動して、[Certificate Authority Certificates] をクリックします。



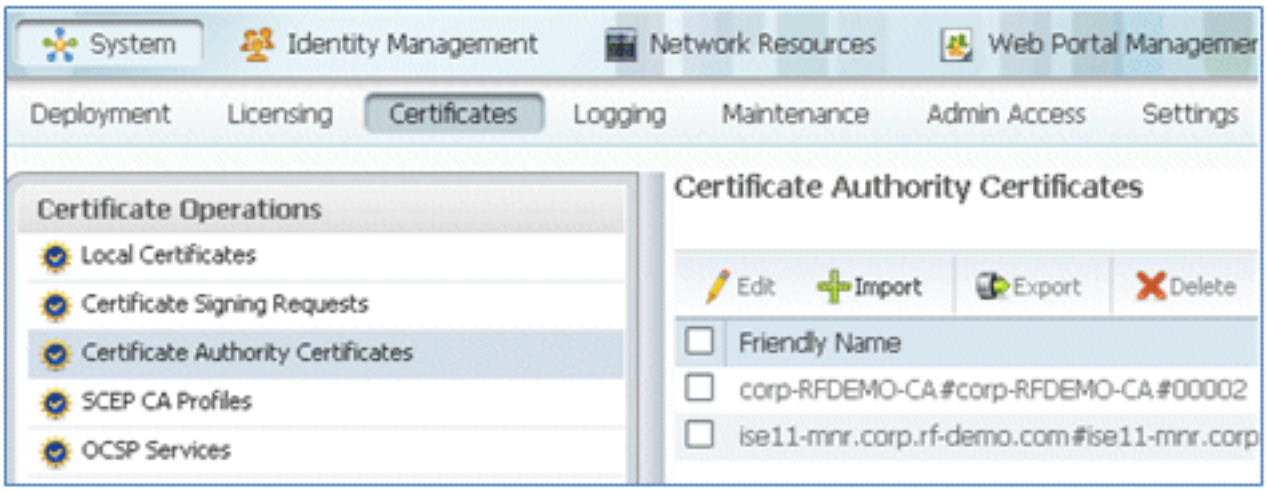
23. [Import] をクリックします。



24. CA 証明書を参照して、[Trust for client authentication] **を有効にし (ボックスをチェック) 、[Submit] をクリックします。**



25. 信頼できる新しい CA 証明書が追加されたことを確認します。



関連情報

- Cisco Identity Services Engine のハードウェア インストール ガイド、リリース 1.0.4
- Cisco 2000 シリーズ ワイアレス LAN コントローラ
- Cisco 4400 シリーズ ワイアレス LAN コントローラ
- Cisco Aironet 3500 シリーズ
- Flex 7500 ワイヤレス ブランチ コントローラ導入ガイド
- 個人所有デバイスの持ち込み（BYOD）：ユニファイド デバイス認証と一貫したアクセス経験
- アイデンティティ サービス エンジンのワイヤレス BYOD
- テクニカル サポートとドキュメント – Cisco Systems

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。