アイデンティティ サービス エンジンのワイヤレス BYOD

内容

概要

Cisco Identity Services Engine（ISE）は、Cisco TrustSec ソリューションに認証と認可インフラストラクチャを提供する、Cisco の次世代のポリシー サーバです。この他に、次の 2 つの重要なサービスを提供します。

- 最初のサービスは、Cisco ISE がさまざまな情報ソースから受領した属性に基づいて、エンドポイントのデバイス タイプを自動的にプロファイリングする手段を提供することです。このサービス（プロファイラと呼ばれる）は、Cisco NAC Profiler アプライアンスが以前提供していたものに相当する機能を備えます。
- Cisco ISEが提供するもう1つの重要なサービスは、エンドポイントのコンプライアンスをスキャンすることです。たとえば、AV/ASソフトウェアのインストールとその定義ファイルの有効性（ポスチャと呼ばれます）をスキャンします。このポスチャ機能はこれまで、Cisco NAC アプライアンスでのみ提供されていました。

Cisco ISE は同等レベルの機能を提供し、これは 802.1X 認証メカニズムに統合されます。

ワイヤレス LAN コントローラ（WLC）が統合された Cisco ISE は、Appleの iDevice（iPhone、iPad、および iPod）、Android ベースのスマートフォンなどのようなモバイル デバイスのプロファイリング メカニズムを提供できます。802.1X のユーザ向けに、Cisco ISE はプロファイリングやポスチャ スキャンのような同等レベルのサービスを提供できます。Cisco ISE のゲスト サービスも、Web 認証要求を認証のために Cisco ISE へリダイレクトすることによって、Cisco WLC と統合できます。

このドキュメントでは、既知のエンドポイントとユーザ ポリシーに基づいて差別化アクセスを提供するといった、Bring Your Own Device（BYOD; 個人所有デバイスの持ち込み）向けのワイヤレス ソリューションを紹介します。本書は BYOD の完全なソリューションを提供するものではなく、ダイナミック アクセスの簡単なユース ケースを示す役割があります。その他の設定例では、ISE スポンサー ポータルを使用することなどが含まれます。このポータルでは、特権ユーザがワイヤレス ゲスト アクセスをプロビジョニングするためにゲストのスポンサーとなることができます。

前提条件

要件

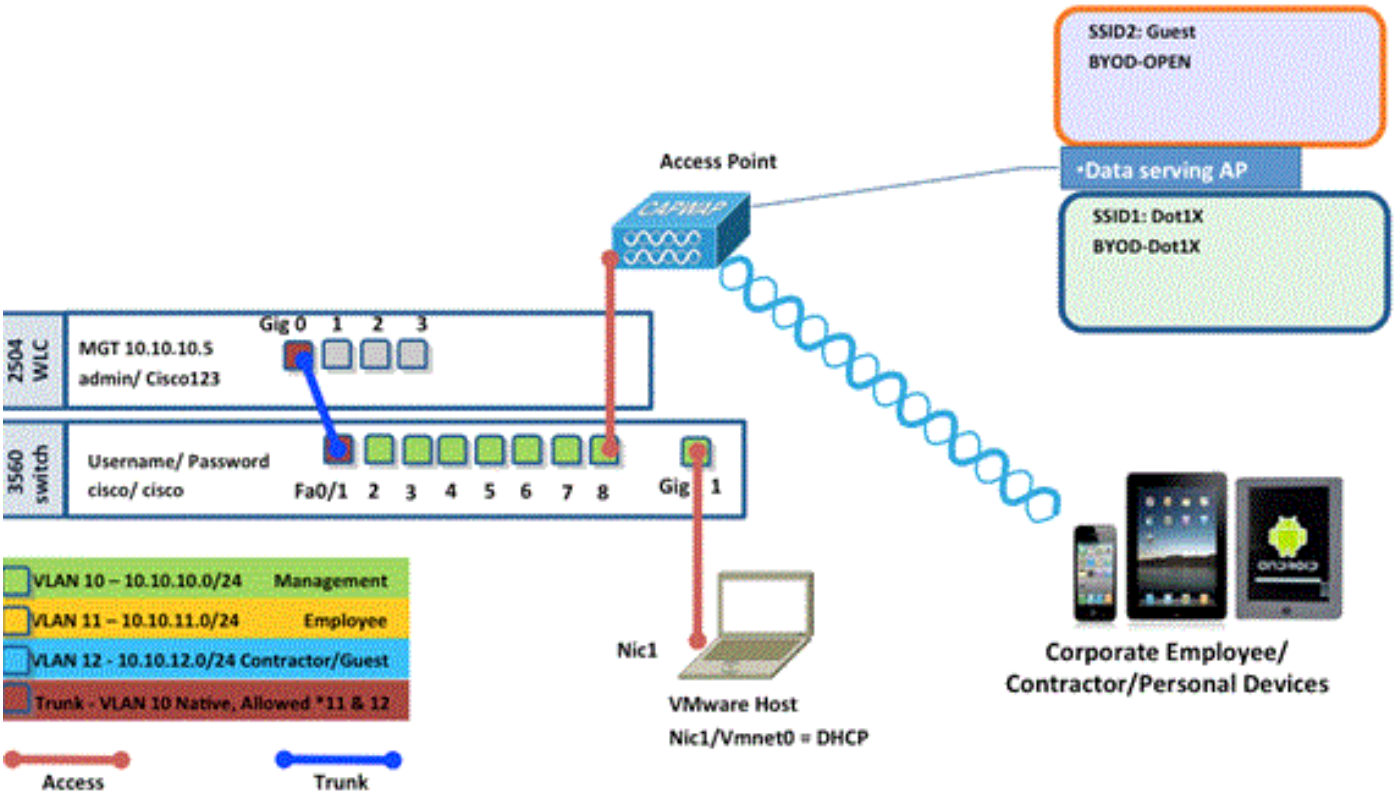
このドキュメントに特有の要件はありません。

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。

- ソフトウェア バージョン 7.2.103 のシスコ ワイヤレス LAN コントローラ 2504 または 2106
- Catalyst 3560：8 ポート
- WLC 2504
- Identity Services Engine 1.0MR（VMware サーバ イメージ バージョン）
- Windows 2008 Server（VMwareイメージ）:512 M、20 GBディスクActive DirectoryDNSDHCP証明書サービス

トポロジ



Name	IP Address	Credential
Vmware Host	10.10.10.2	*(Machine used to host the ISE 1.0 MR vmware server files)*
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	*(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)*

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ワイヤレス LAN コントローラの RADIUS NAC と CoA の概要

この設定により、WLC は ISE RADIUS サーバから到達する URL リダイレクションの AV ペアを見つけることができます。これは、RADIUS NAC 設定が有効になっているインターフェイスに接続されている WLAN のみが対象となります。URL リダイレクションのための Cisco AV ペアを受信すると、クライアントは POSTURE_REQD 状態に入ります。これは基本的に、コントローラ内部の WEBAUTH_REQD 状態と同じです。

ISE RADIUS サーバは、クライアントが Posture_Compliant であると判断した場合、CoA 再認証を発行します。Session_ID はそれらを結びつけるために使用されます。この新しい AuthC (再認証) があると、URL リダイレクト AV ペアは送信されません。URL リダイレクト AV ペアがないため、WLC はクライアントがもはやポスチャを必要としなくなったことを理解します。

RADIUS NAC 設定が有効でないと、WLC は URL リダイレクト VSA を無視します。

CoA-ReAuth:RFC 3576設定で有効になります。再認証機能は、以前にサポートされていた既存の CoA コマンドに追加されました。

RADIUS NAC 設定は CoA を機能させるために必要ですが、この機能からは相互に排他的です。

プレポスチャACL：クライアントがPOSTURE_REQ状態の場合、WLCのデフォルトの動作では、DHCP/DNSを除くすべてのトラフィックがブロックされます。プレポスチャ ACL (url-redirect-acl AV-Pair で呼び出される) がクライアントに適用され、ACL の許可対象にクライアントが到達できます。

事前認証ACLとVLANオーバーライド：隔離VLANまたはアクセスVLANと異なるAuthC VLANは、7.0MR1ではサポートされていません。ポリシー サーバから VLAN を設定すると、セッション全体の VLAN となります。最初の AuthZ の後、VLAN の変更は不要です。

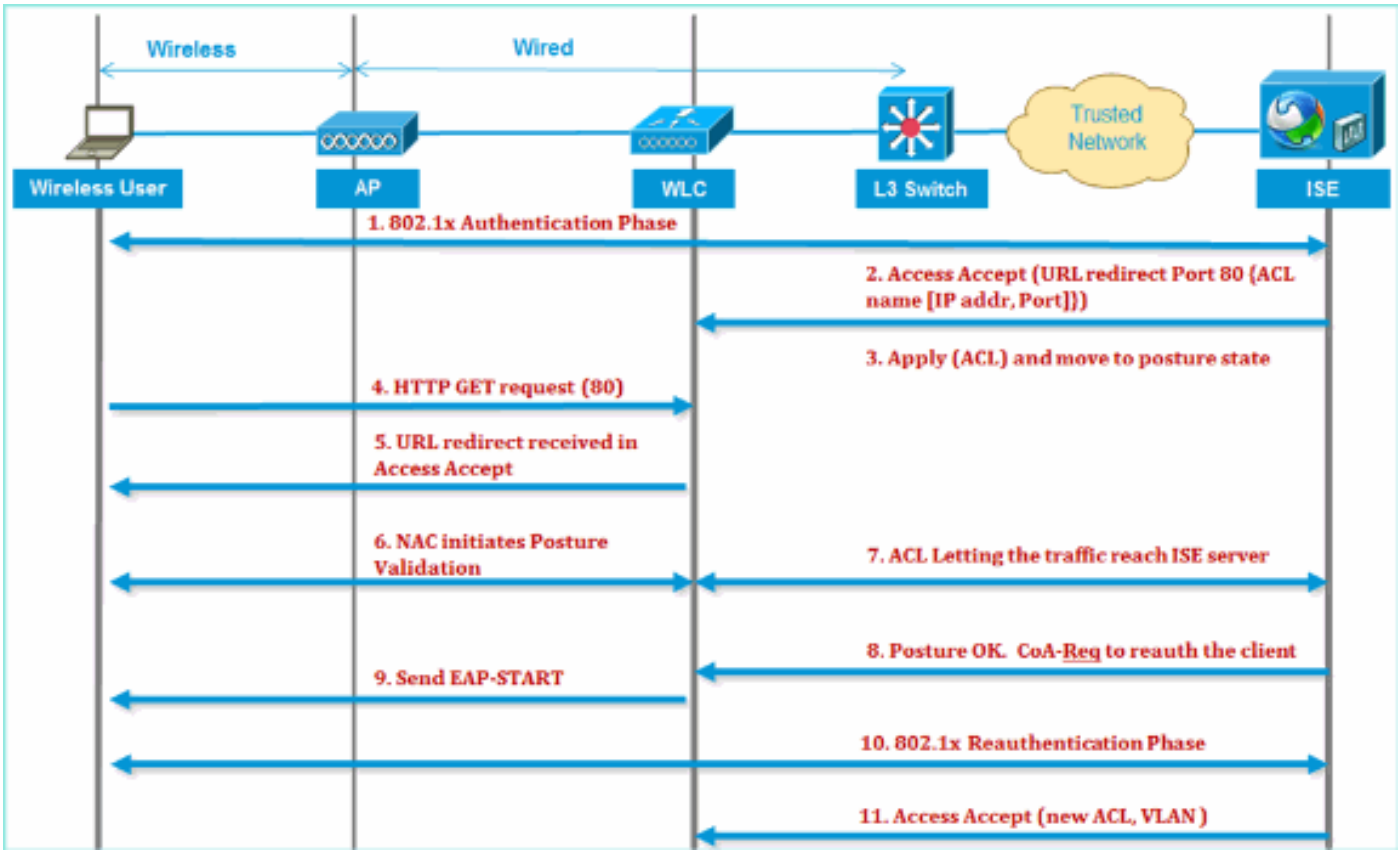
ワイヤレス LAN コントローラの RADIUS NAC と CoA の機能フロー

次の図は、クライアントがバックエンド サーバと NAC ポスチャ検証で認証されたときに交換されるメッセージの詳細を示します。

1. クライアントは dot1x 認証を使用して認証を行います。
2. RADIUS の Access Accept では、ポート 80 のリダイレクトされた URL と、許可される IP アドレスとポート、または隔離 VLAN を含むプレ認証 ACL が伝達されます。
3. クライアントは Access Accept で提供された URL にリダイレクトされ、ポスチャ検証が実施されるまで、新しい状態に入ります。この状態のクライアントが ISE サーバと通信し、ISE NAC サーバで設定されたポリシーに対して自身を検証します。
4. クライアント上のNACエージェントがポスチャ検証 (ポート80へのトラフィック) を開始：エージェントがHTTPディスカバリ要求をポート80に送信し、コントローラがアクセスアクセプトで提供されたURLにリダイレクトします。ISE は、クライアントが到達しようと試みていることを認識し、クライアントに直接応答します。このようにして、クライアントは ISE サーバ IP について学習し、その後はクライアントが ISE サーバと直接通信します。
5. ACL がこのトラフィックを許可するように設定されているため、WLC はこのトラフィックを許可します。VLAN のオーバーライド時には、ISE サーバに到達できるようにトラフィックはブリッジされます。
6. ISE クライアントが評価を完了すると、再認証サービスを持つ RADIUS CoA-Req が WLC に送信されます。これによってクライアントの再認証が始まります (EAP-START を送信することにより)。再認証が成功すると、ISE は新しい ACL (あれば) を使用して Access Accept を送信し、URL リダイレクトまたはアクセス VLAN は行われません。
7. WLC は RFC 3576 に従って CoA-Req と Disconnect-Req をサポートします。WLC は RFC 5176 に従って再認証サービスの CoA-Req をサポートする必要があります。
8. ダウンロード可能な ACL の代わりに、事前設定された ACL が WLC で使用されます。ISE サーバは、コントローラですでに設定されている ACL 名のみを送信します。

9. この設計は、VLAN と ACL の両方のケースで機能します。VLAN のオーバーライドの場合、ポート 80 のみをリダイレクトし、隔離 VLAN の残りのトラフィックを許可（ブリッジ）します。ACL では、Access Accept で受信したプレ認証 ACL が適用されます。

次の図は、この機能フローを視覚的に表したものです。



ISE プロファイリングの概要

Cisco ISE プロファイラ サービスは、企業ネットワークへの適切なアクセスを確保および維持するために、デバイス タイプにかかわらず、ネットワーク上のすべての接続されたエンドポイントの機能を、検出、検索、および決定するための機能を提供します。主にネットワーク上のすべてのエンドポイントの属性を収集し、エンドポイントをそのプロファイルに従って分類します。

プロファイラは、ここに示されているコンポーネントで構成されています。

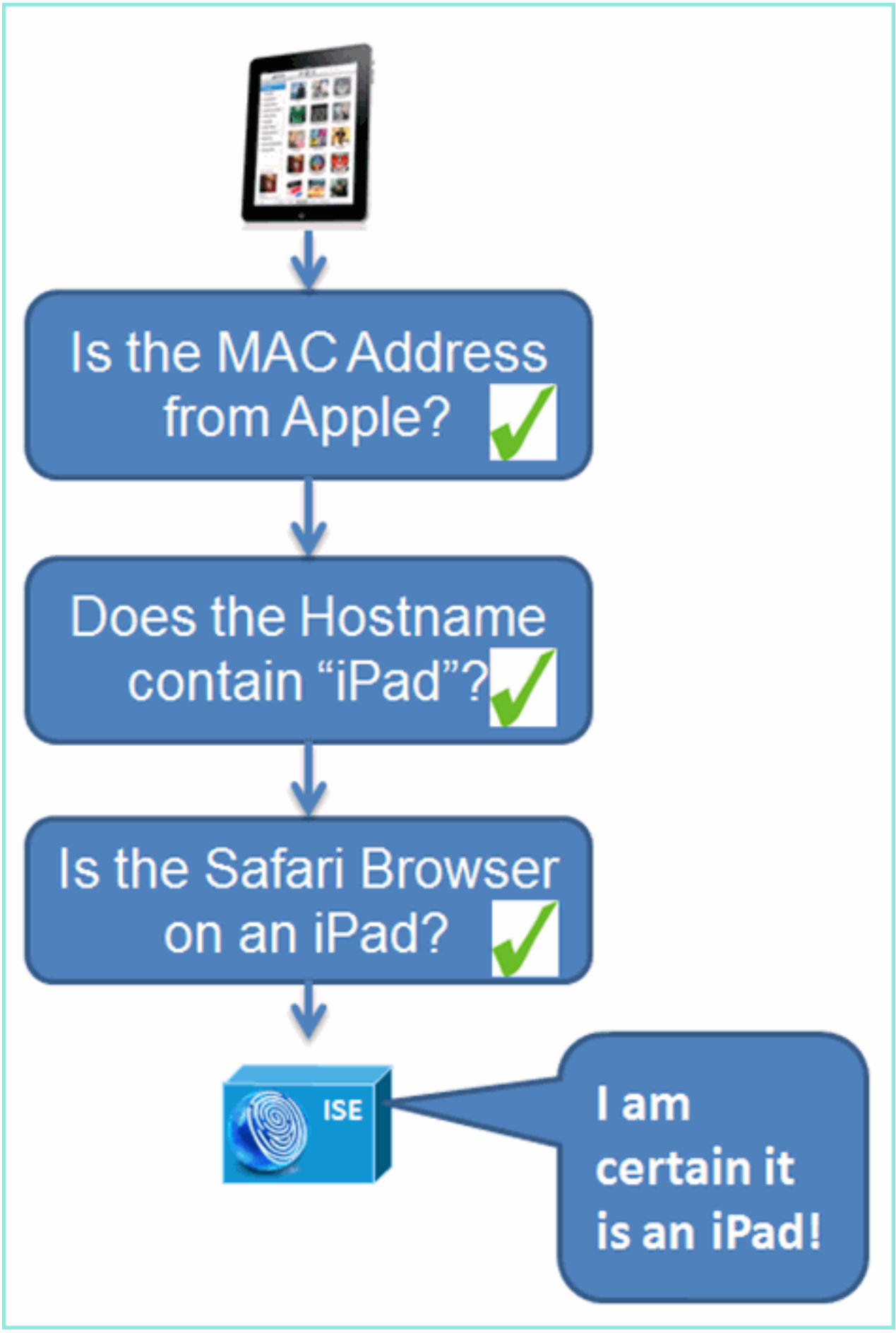
- センサーには、さまざまなプローブが含まれています。プローブはネットワーク アクセス デバイスに対してクエリを実行することでネットワーク パケットをキャプチャし、エンドポイントから収集された属性と属性値をアナライザに転送します。
- アナライザは、設定済みのポリシーと ID グループを使用してエンドポイントを評価し、収集された属性と属性値を照合します。これにより、エンドポイントを指定されたグループに分類し、一致したプロファイルを持つエンドポイントを Cisco ISE データベースに保存します。

モバイル デバイスの検出では、デバイスの適切な識別のため、これらのプローブの組み合わせを使用することが推奨されます。

- RADIUS(Calling-Station-ID):MACアドレス(OUI)を提供します
- DHCP（ホスト名）：ホスト名 – デフォルトのホスト名にはデバイスタイプを含めることができます。例：jsmith-ipad

- DNS（逆IPルックアップ）:FQDN：デフォルトのホスト名にデバイスタイプを含めることができる
- HTTP(User-Agent)：特定のモバイルデバイスタイプの詳細

この iPad の例では、プロファイラは Web ブラウザ情報を User-Agent 属性および要求メッセージの他の HTTP 属性から取得し、エンドポイント属性のリストに追加します。



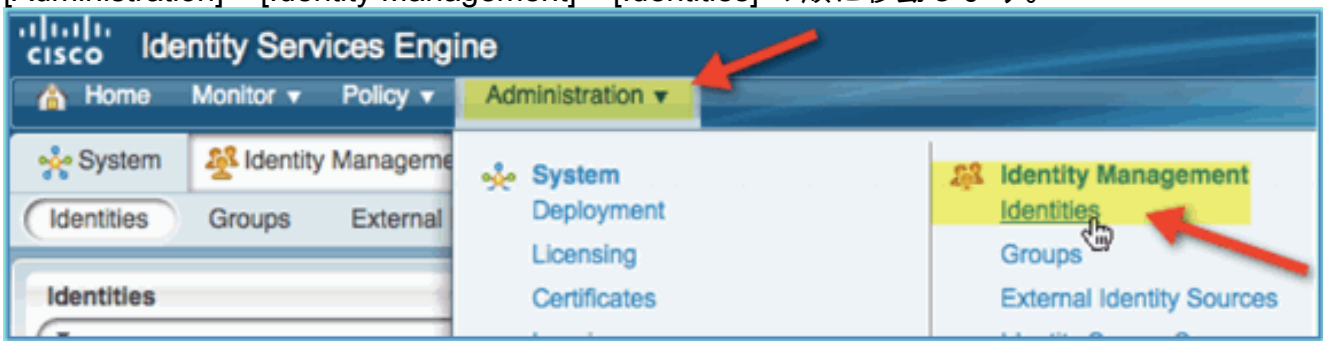
[内部アイデンティティ ユーザの作成]

MS の Active Directory（AD）は簡単な概念実証では必要ありません。ISE は、アクセス制御およびきめ細かいポリシー制御のためのユーザ アクセスの差別化を含む、唯一の ID ストアとして使用できます。

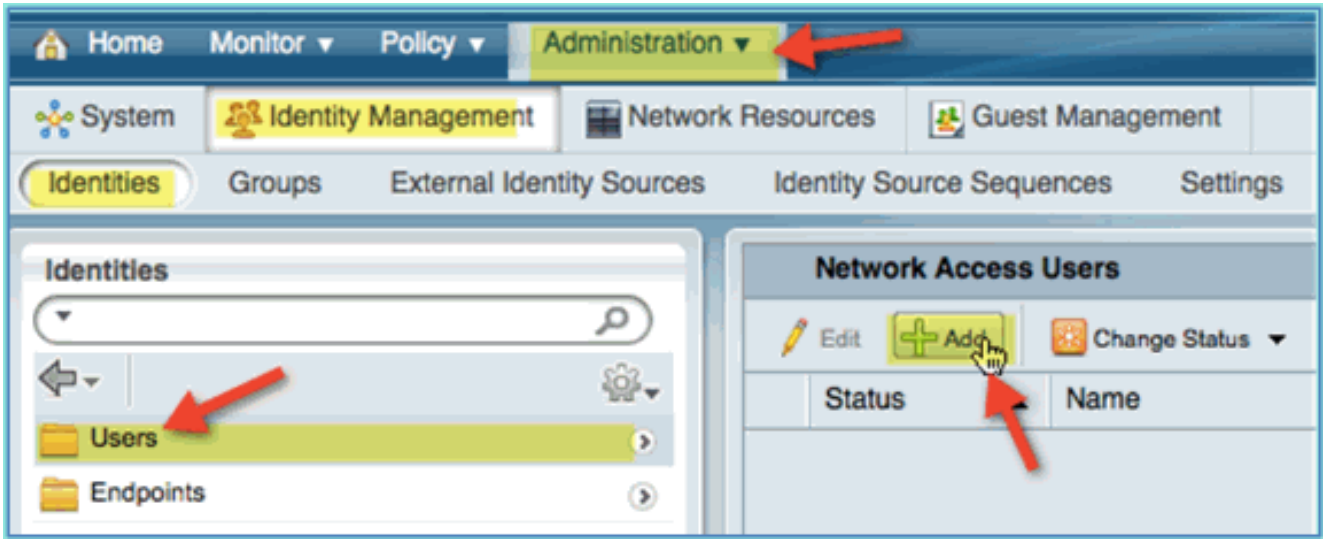
AD 統合を使用する ISE 1.0 のリリースにより、ISE は認証ポリシーで AD グループを使用できるようになりました。ISE の内部ユーザ ストアを使用すると（AD 統合を使用せず）、グループをデバイスの ID グループと一緒にポリシーで使用することができません（特定されたバグであり、ISE 1.1 で解決予定）。そのため、デバイス ID グループに加えて使用する場合は、従業員や請負業者といった個々のユーザのみを区別することができます。

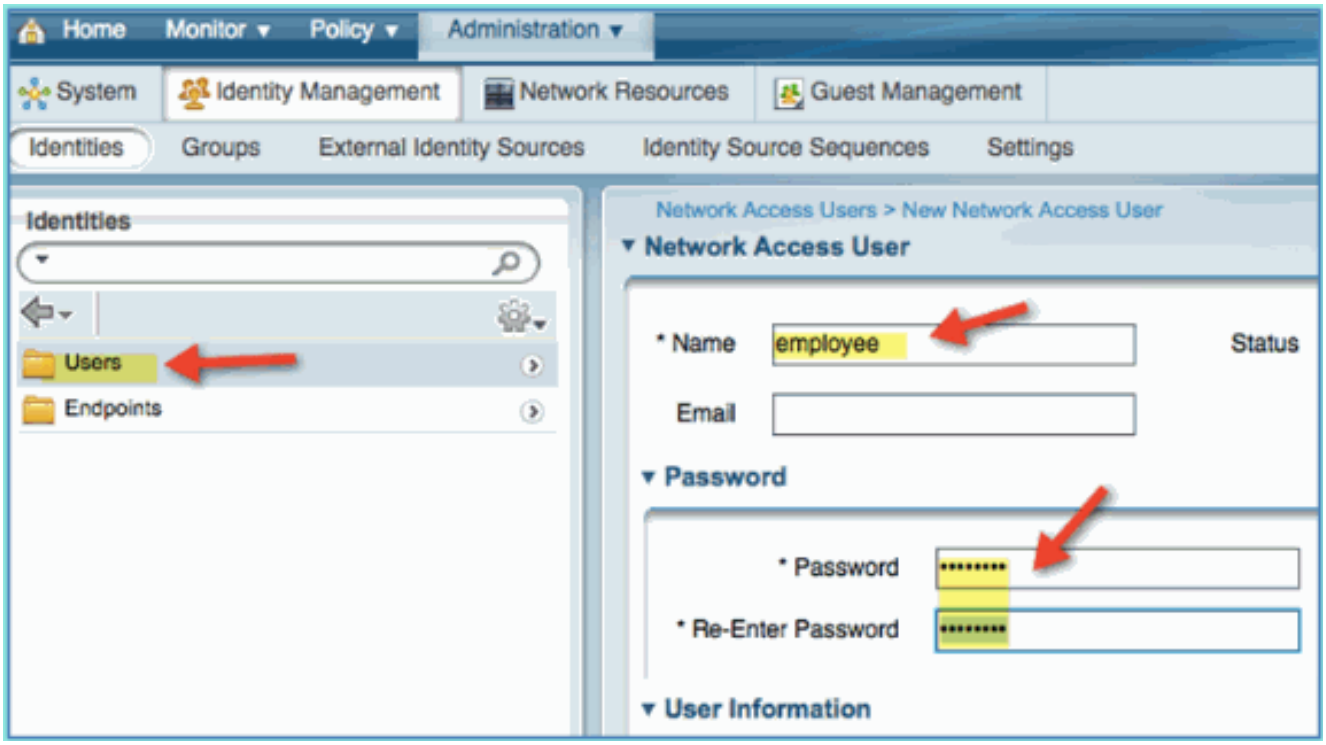
次のステップを実行します。

1. ブラウザウィンドウを開き、https://ISE の IP アドレスに移動します。
2. [Administration] > [Identity Management] > [Identities] の順に移動します。

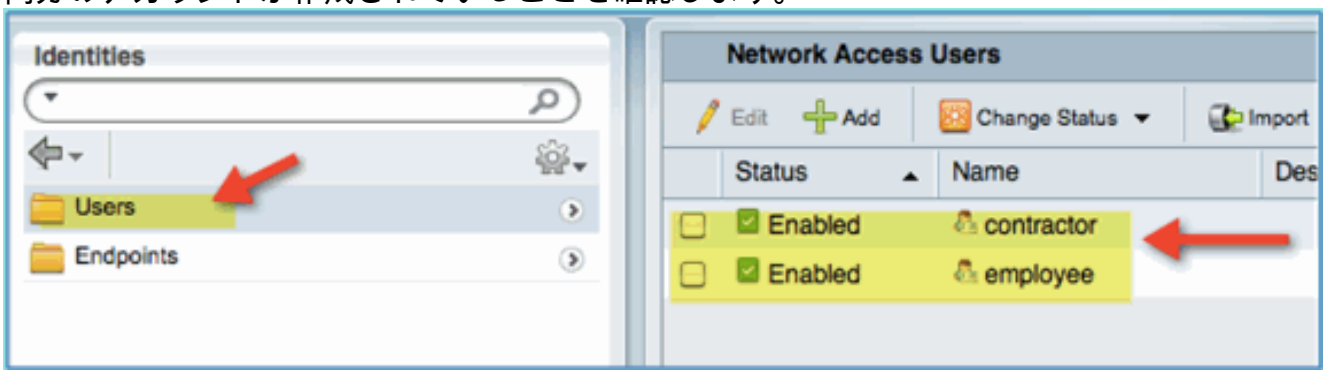


3. [Users]、[Add]（Network Access User）をクリックします。これらのユーザ値を入力し、Employee グループに割り当てます。[Name（名前）]:employeeパスワード：XXXX





4. [Submit] をクリックします。[Name (名前)]:contractorパスワード：XXXX
5. 両方のアカウントが作成されていることを確認します。



ISE へのワイヤレス LAN コントローラの追加

ISE への RADIUS 要求を開始するすべてのデバイスが、ISE で定義されている必要があります。これらのネットワーク デバイスは、IP アドレスに基づいて定義されます。ISE のネットワーク デバイスの定義では IP アドレスの範囲を指定できるため、複数の実際のデバイスを表すように定義できます。

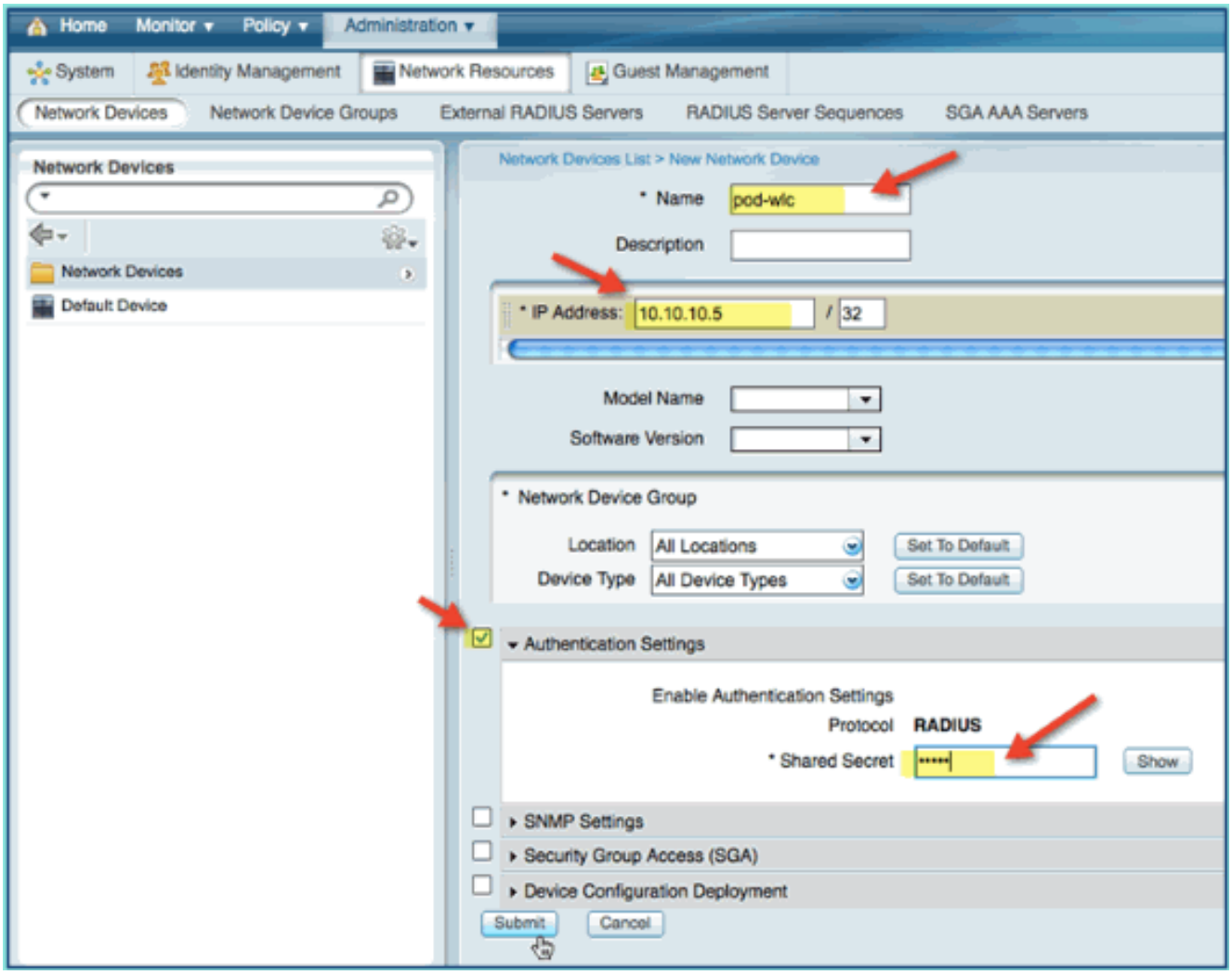
RADIUS の通信に必要なものに限らず、ISE のネットワーク デバイスの定義は、SNMP および SSH などの他の ISE/デバイス通信の設定が含まれます。

ネットワーク デバイスの定義の別の重要な側面は、デバイスの適切なグループ化によってこのグループ化をネットワーク アクセス ポリシーで利用できるようにすることです。

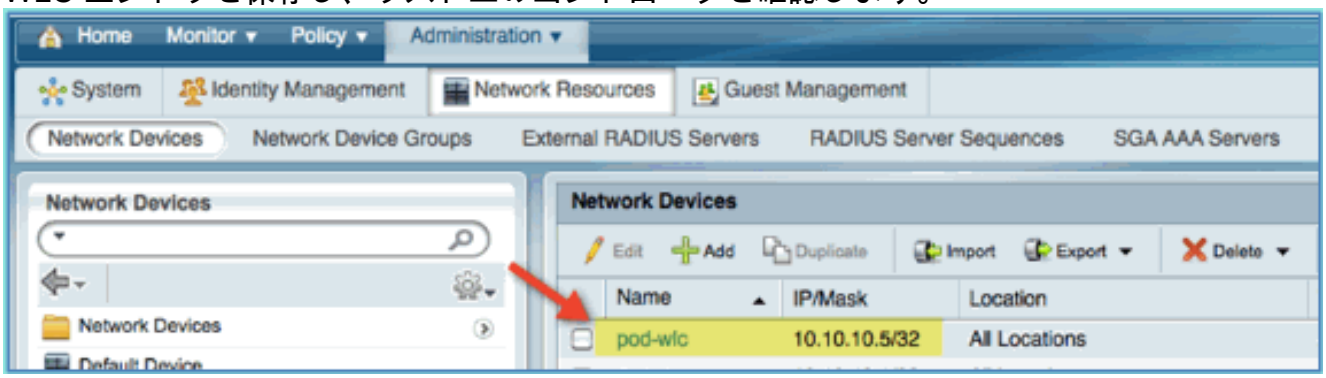
この演習では、ラボで必要なデバイスの定義が設定されています。

次のステップを実行します。

1. ISE から、[Administration] > [Network Resources] > [Network Devices] に移動します。



2. [Network Devices]から、[Add] をクリックします。IP アドレスを入力し、[Authentication Setting] にチェックを入れ、[Shared Secret] に ‘cisco’ と入力します。
3. WLC エントリを保存し、リスト上のコントローラを確認します。

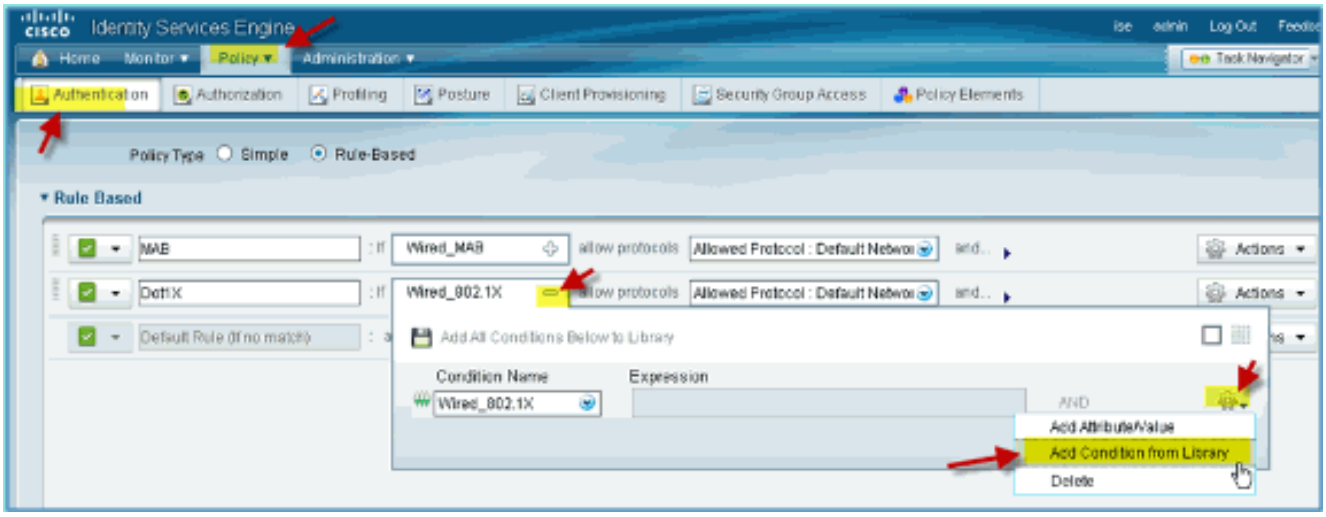


ワイヤレス認証のための ISE の設定

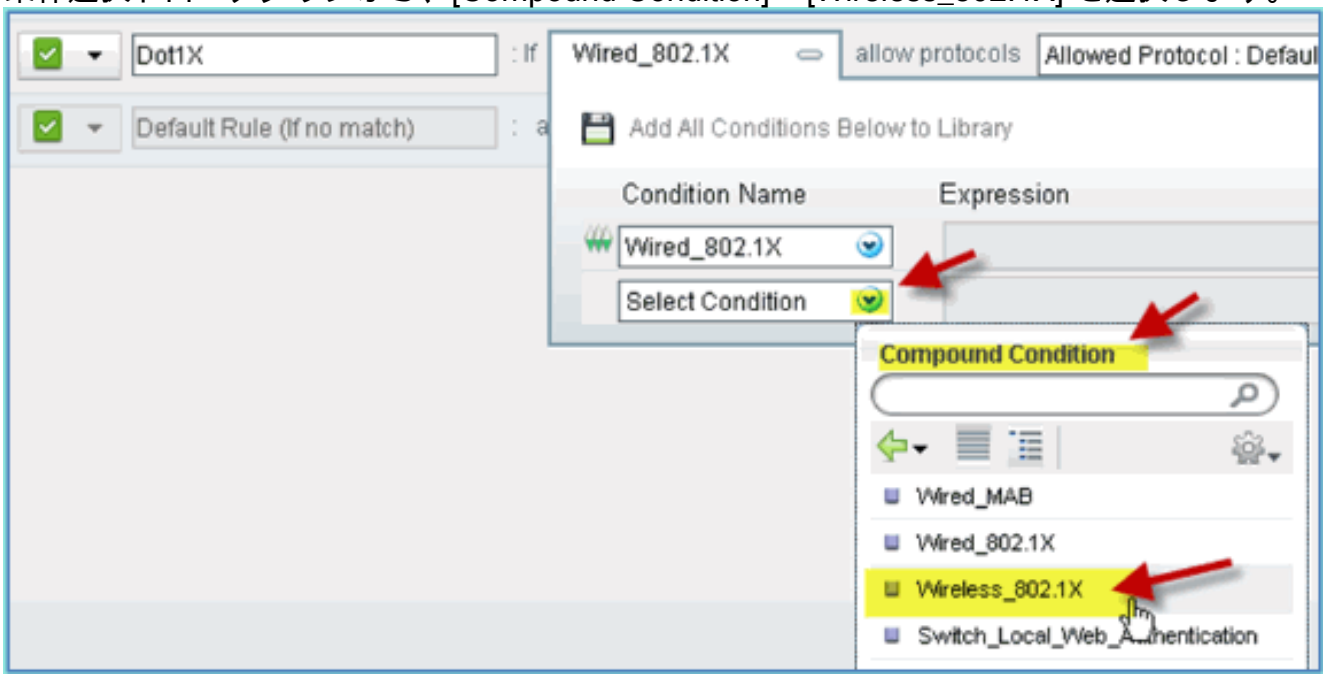
ISE は、802.1x ワイヤレス クライアントを認証するように設定し、ID ストアとして Active Directory を使用する必要があります。

次のステップを実行します。

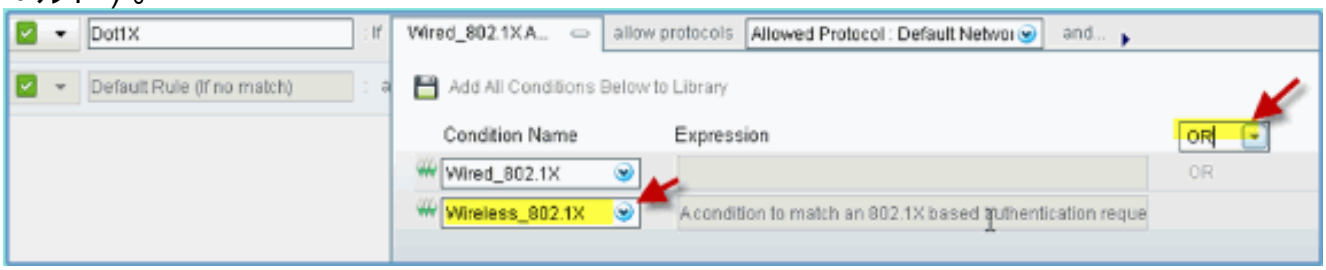
1. ISE から、[Policy] > [Authentication] に移動します。
2. [Dot1x] > [Wired_802.1X] (-) をクリックして展開します。
3. 歯車アイコンをクリックして、[Add Condition from Library] (ライブラリから条件を追加) します。

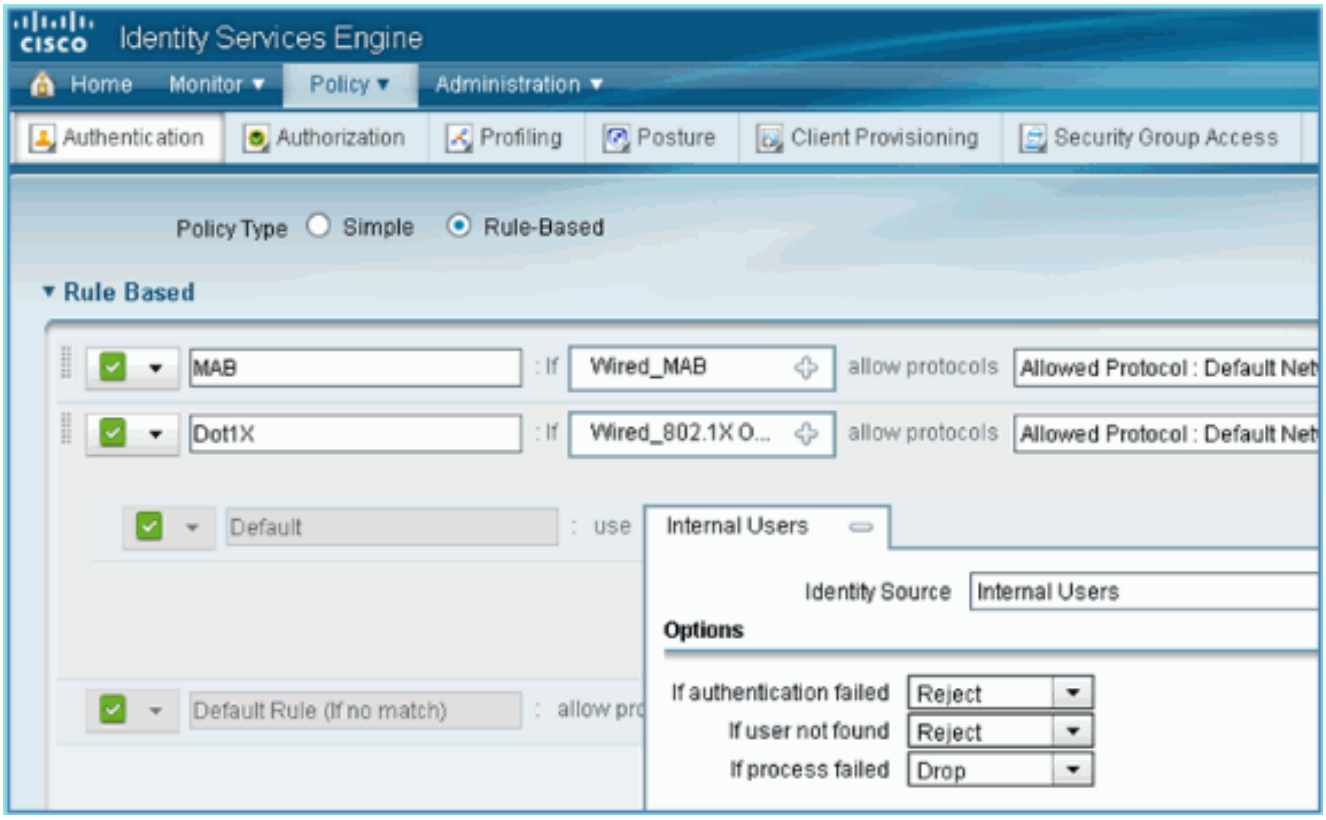


4. 条件選択ドロップダウンから、[Compound Condition] > [Wireless_802.1X] を選択します。



5. [Express] 条件を [OR] に設定します。
6. allow protocol オプションの後を展開し、デフォルトの [Internal Users] を承認します（デフォルト）。





7. 他はすべてデフォルトのままとします。[Save] をクリックして更新を完了します。

ワイヤレス LAN コントローラのブートストラップ

WLC のネットワークへの接続

Cisco 2500 ワイヤレス LAN コントローラの導入ガイドは、Cisco 2500 シリーズ ワイヤレス コントローラ導入ガイド [英語] でも入手できます。

スタートアップ ウィザードを使用したコントローラの設定

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
 Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
```

```
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

ネイバー スイッチの設定

コントローラは、ネイバー スイッチ上のイーサネット ポート（Fast Ethernet 1）に接続されます。ネイバー スイッチ ポートは 802.1Q トランクとして設定され、トランク上のすべての VLAN を許可します。ネイティブ VLAN 10 では、WLC の管理インターフェイスが接続できます。

802.1Q スイッチ ポートの設定は次のとおりです。

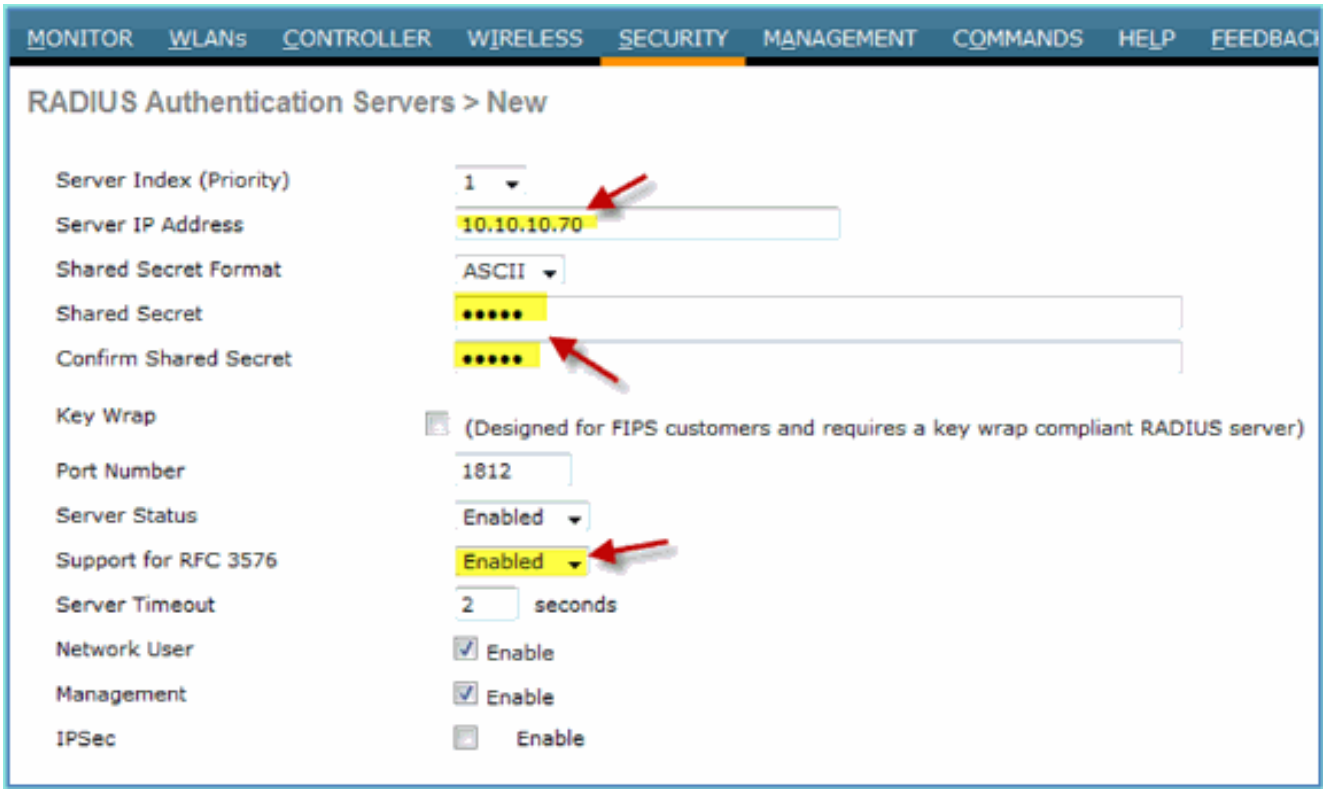
```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

WLC への認証サーバ（ISE）の追加

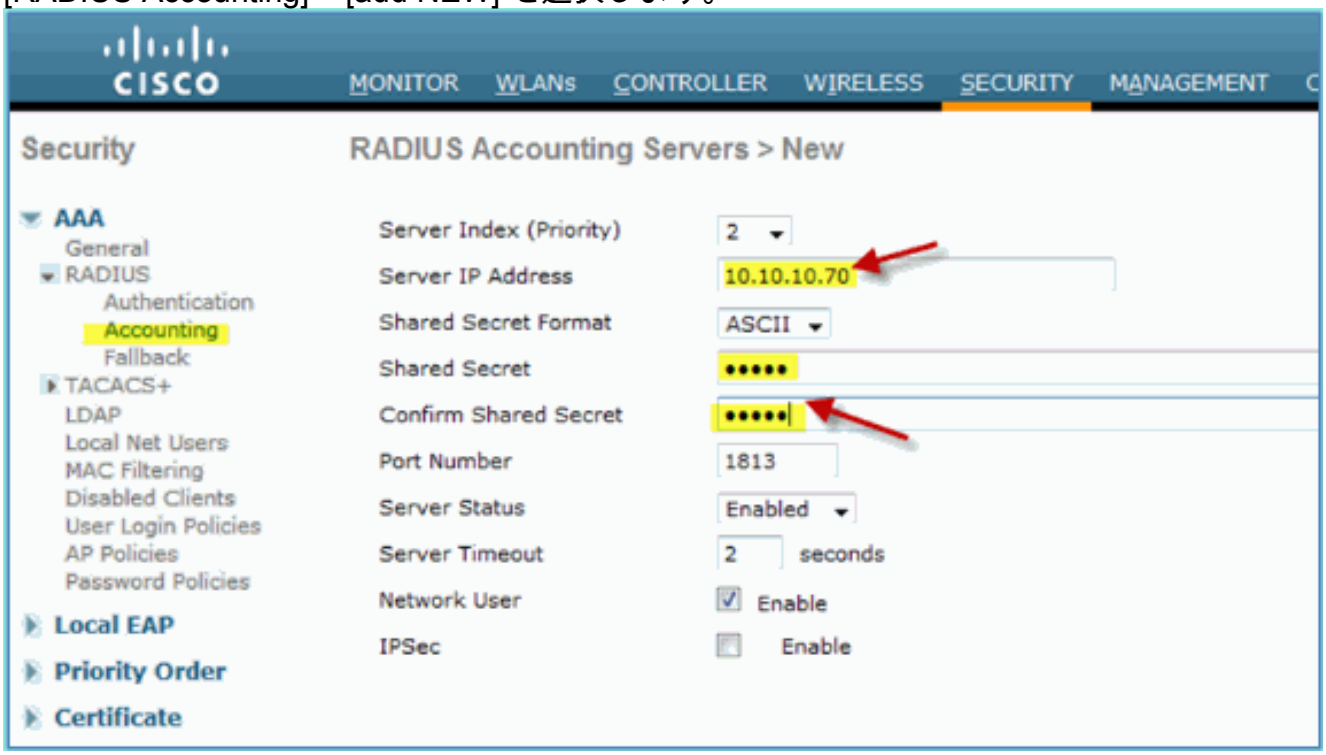
ワイヤレス エンドポイントの 802.1X と CoA 機能を有効にするため、ISE を WLC に追加する必要があります。

次のステップを実行します。

1. ブラウザを開き、（セキュア HTTP を使用して）[pod WLC] > [https://wlc] に接続します。
2. [Security] > [Authentication] > [New] の順に移動します。



3. 次の値を入力してください。[Server IP Address（サーバIPアドレス）]:10.10.10.70（割り当てを確認）共有秘密：ciscoRFC 3576(CoA)のサポート：有効（デフォルト）その他すべて：デフォルト
4. [Apply] をクリックして、次に進みます。
5. [RADIUS Accounting] > [add NEW] を選択します。



6. 次の値を入力してください。[Server IP Address]:10.10.10.70共有秘密：ciscoその他すべて：デフォルト
7. [Apply] をクリックして、WLC の設定を保存します。

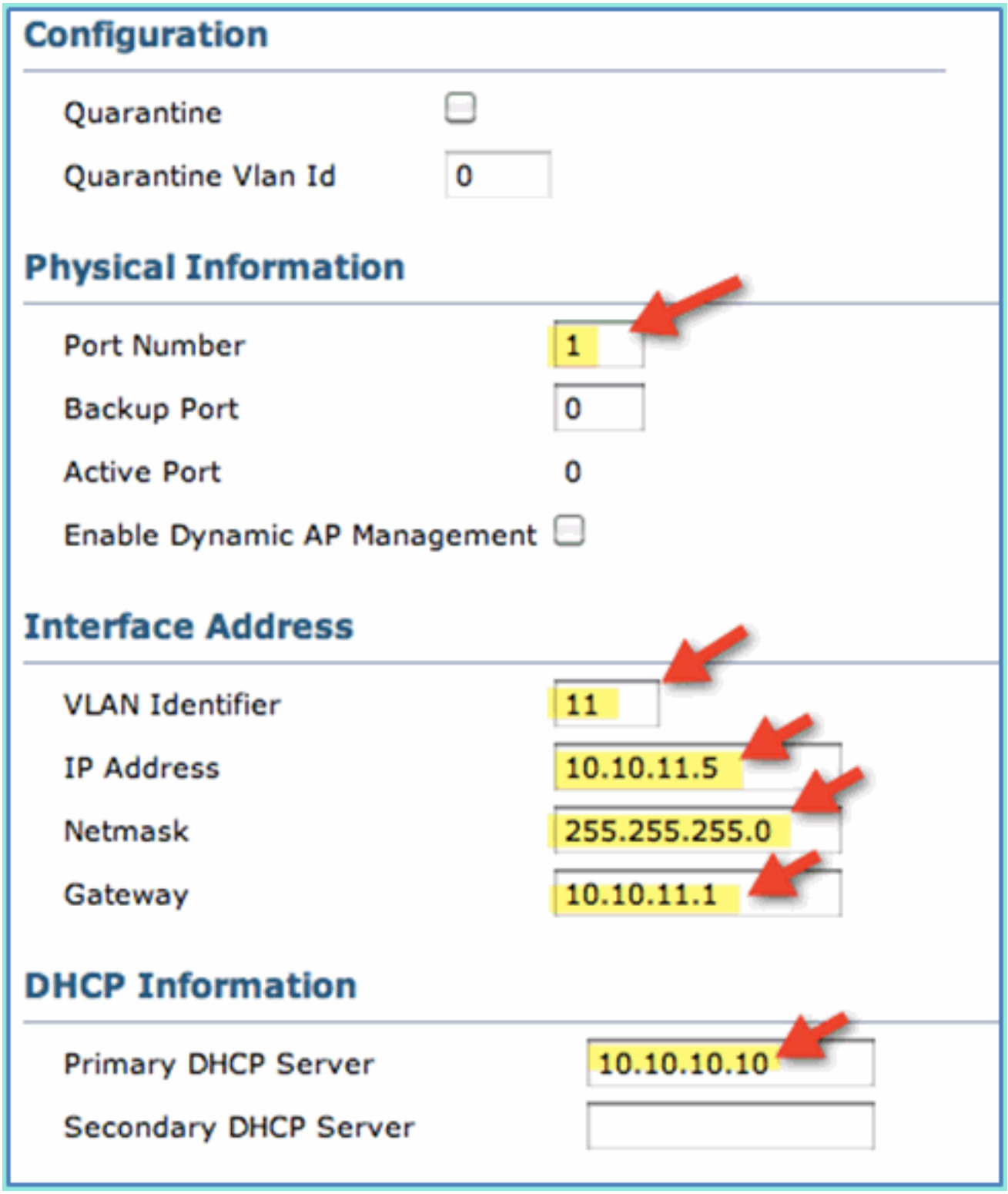
WLC 従業員ダイナミック インターフェイスの作成

WLC の新しいダイナミック インターフェイスを追加し、従業員 VLAN にそれをマッピングするには、次の手順を実行します。

1. WLC から、[Controller] > [Interfaces] に移動します。次に、[New] をクリックします。

2. WLC から、[Controller] > [Interfaces] に移動します。次の内容を入力します。[Interface Name]:EmployeeVLAN
ID:11

3. 従業員インターフェイスに次を入力します。ポート番号：1[VLAN Identifier]:11IPアドレス：10.10.11.5ネットマスク：255.255.255.0ゲートウェイ：10.10.11.1DHCP:10.10.10.10

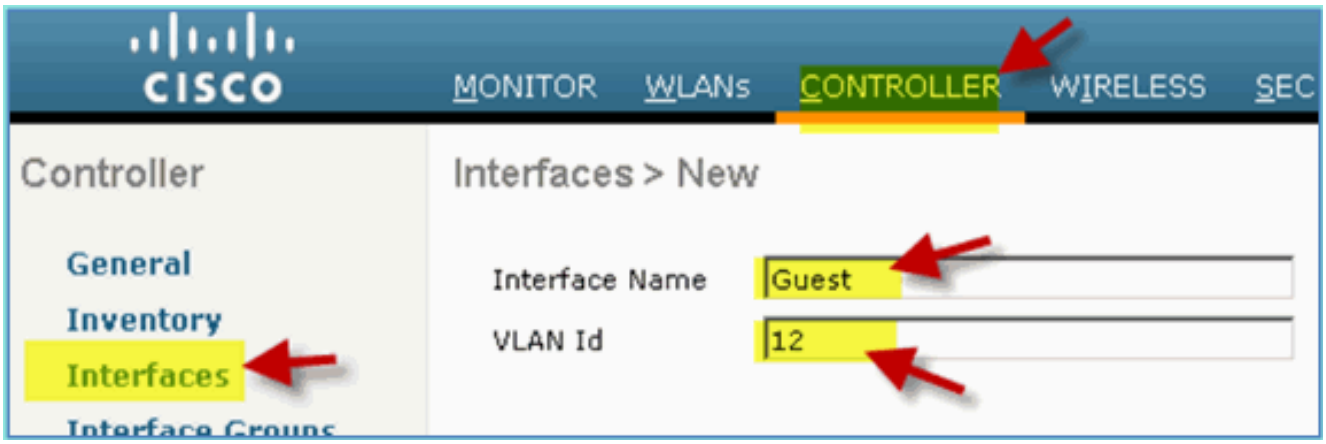


4. 従業員の動的なインターフェイスが新たに作成されたことを確認します。

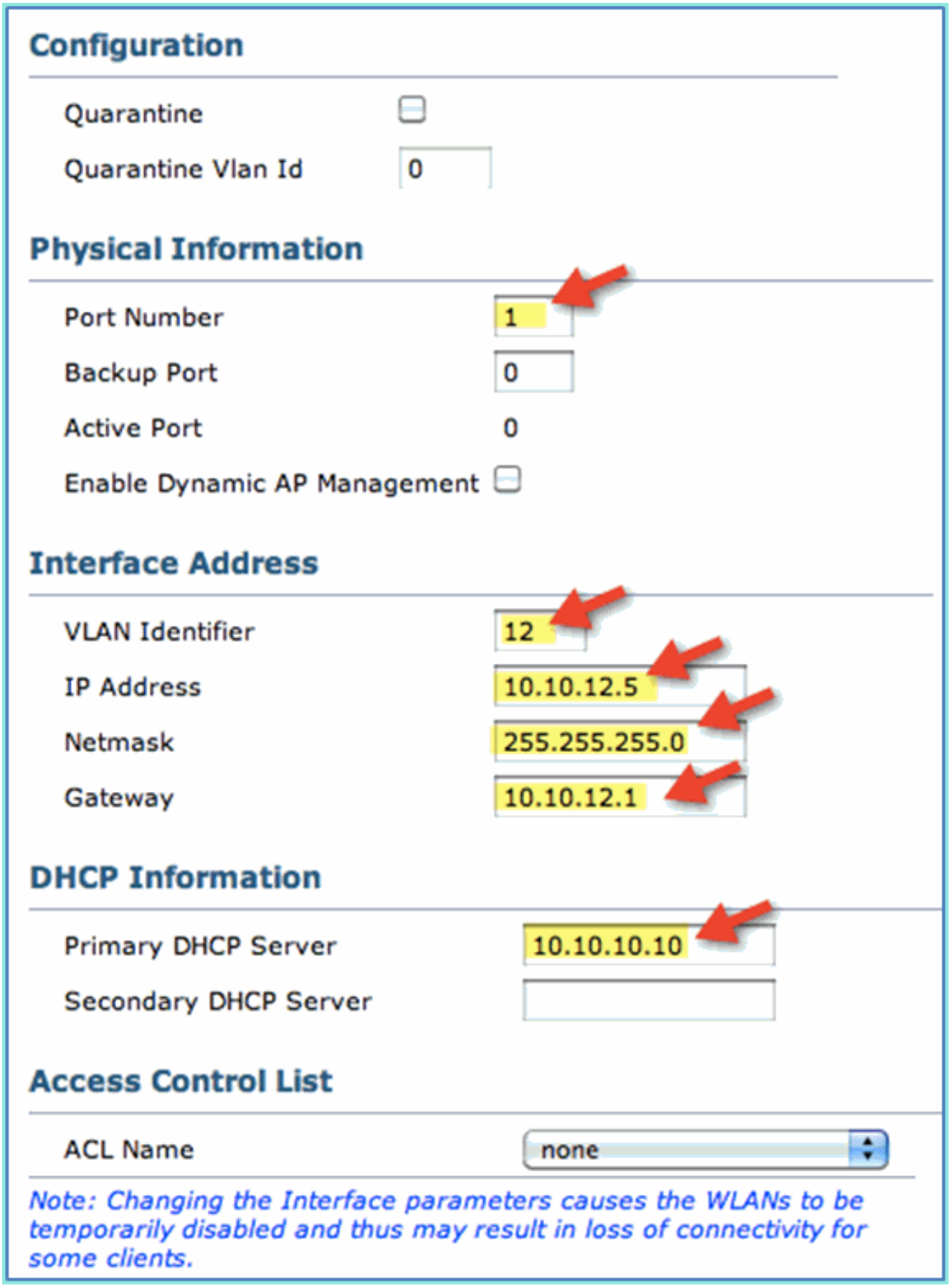
WLC ゲスト ダイナミック インターフェイスの作成

WLC の新しいダイナミック インターフェイスを追加し、ゲスト VLAN にそれをマッピングするには、次の手順を実行します。

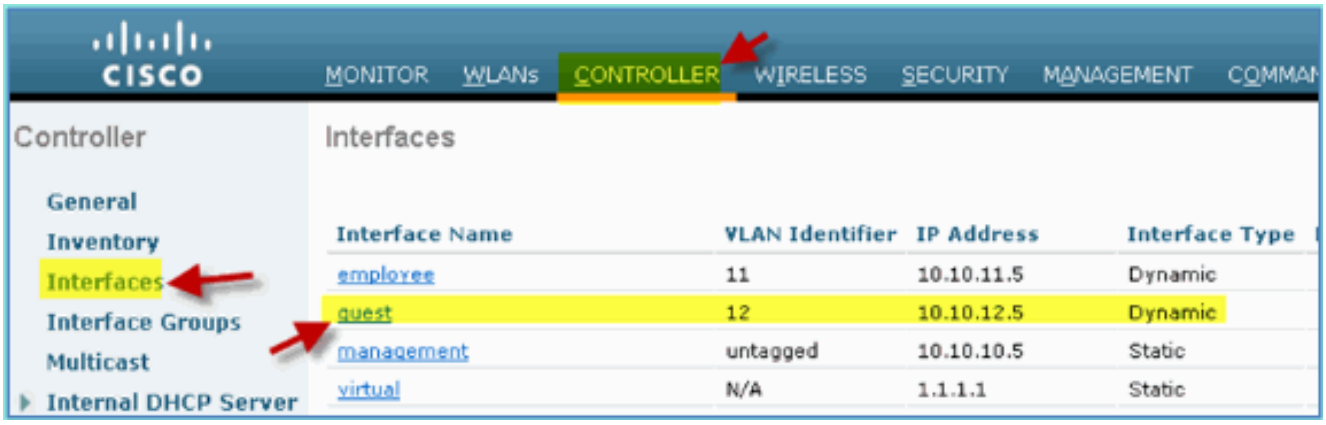
1. WLC から、[Controller] > [Interfaces] に移動します。次に、[New] をクリックします。
2. WLC から、[Controller] > [Interfaces] に移動します。次の内容を入力します。[Interface Name]:GuestVLAN
   ID:12



3. ゲスト インターフェイスに次を入力します。ポート番号：1[VLAN Identifier]:12IPアドレス：10.10.12.5ネットマスク：255.255.255.0ゲートウェイ：10.10.12.1DHCP:10.10.10.10



4. ゲスト インターフェイスが追加されたことを確認します。



802.1x WLAN の追加

WLC の最初のブートストラップからデフォルト WLAN が作成される場合があります。その場合、それを変更するか、ガイドの指示どおりにワイヤレス 802.1X 認証をサポートする新しい WLAN を作成します。

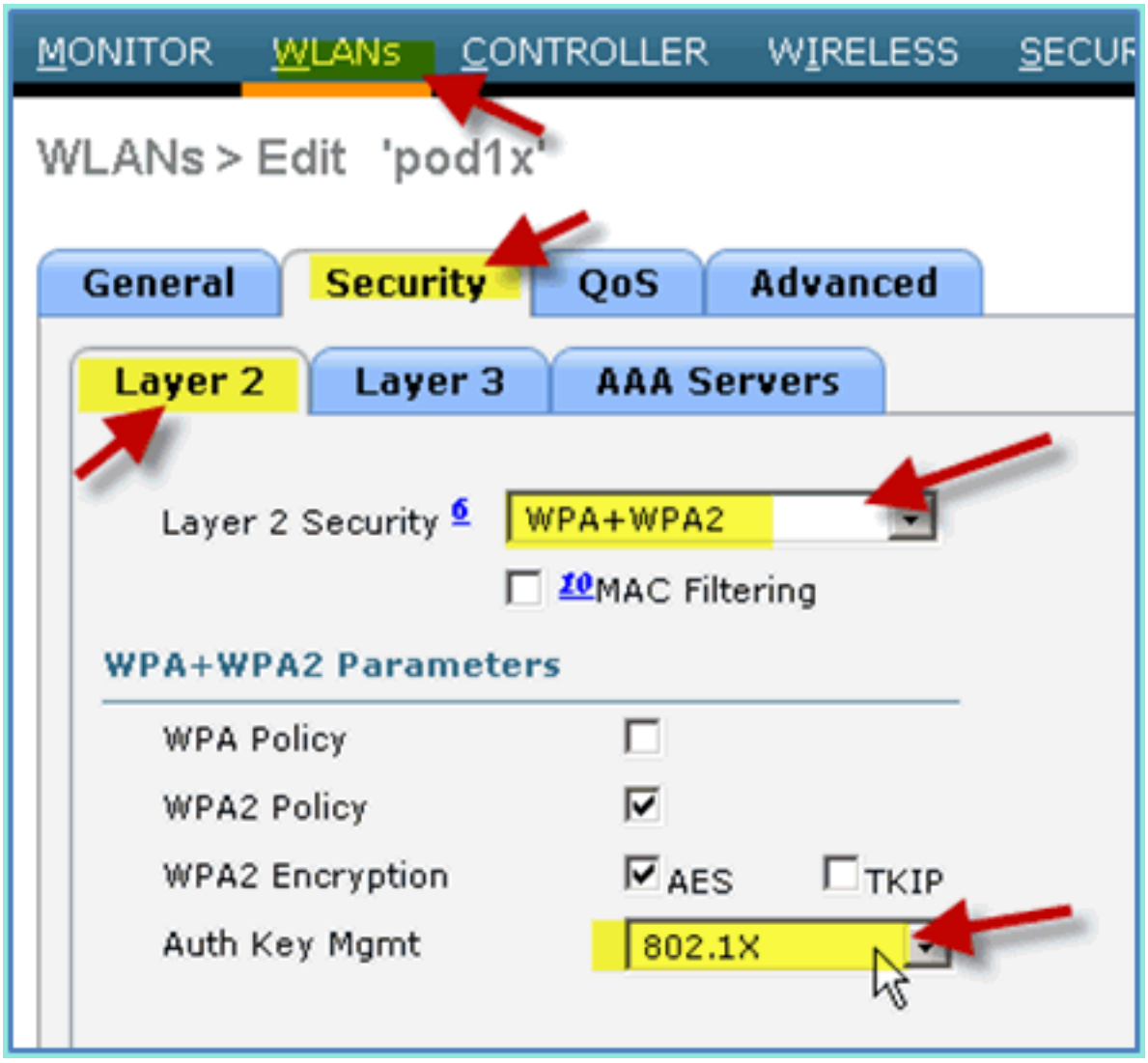
次のステップを実行します。

1. WLC から [WLAN] > [Create New] に移動します。

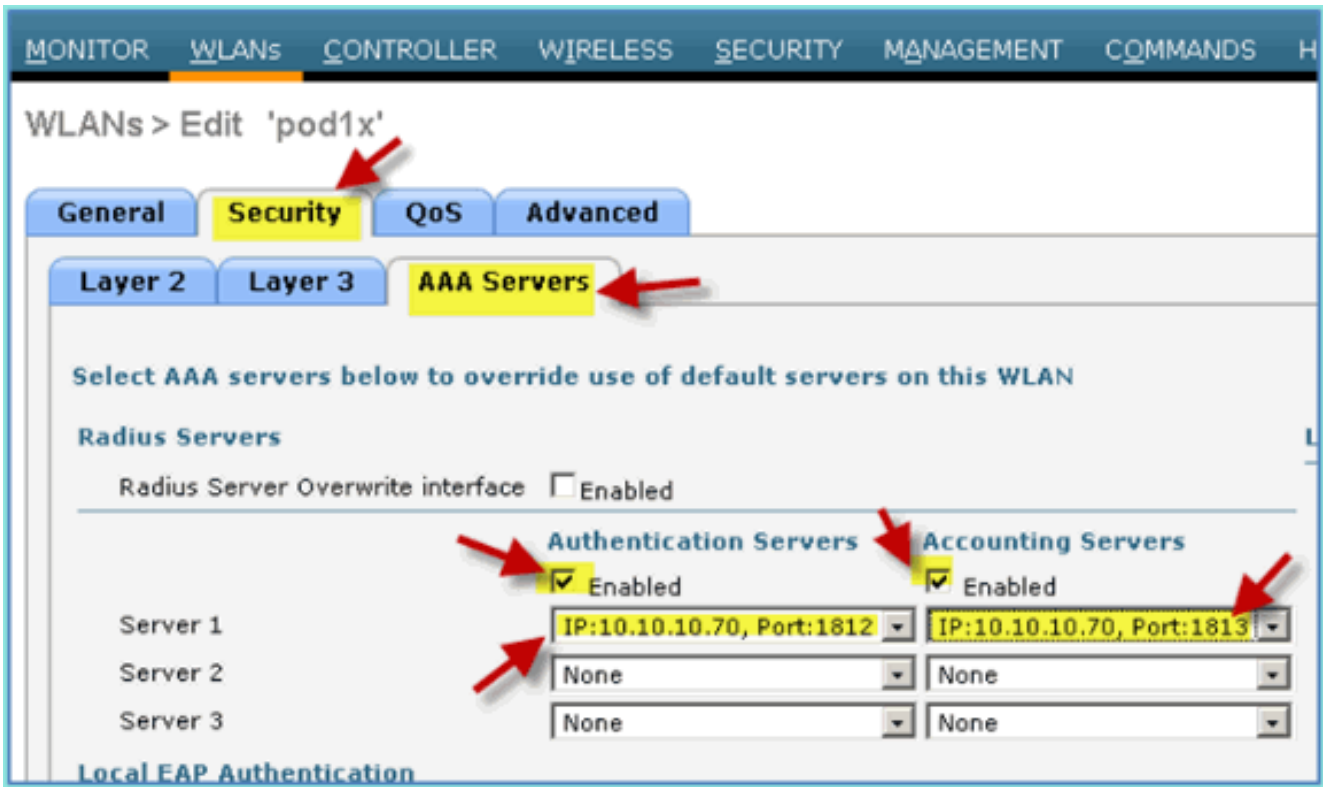
2. WLAN で以下を入力します。[Profile Name (プロファイル名)]:pod1xSSID：同じ

3. WLAN の設定 > [General] タブでは、次の手順を使用します。[Radio Policy]:Allインターフェイス/グループ：管理その他すべて：デフォルト

4. [WLAN] > [Security] タブ > [Layer 2] では、次を設定します。Layer 2 Security：WPA+WPA2WPA2ポリシー/暗号化：有効/AES[Auth Key Mgmt]:802.1X

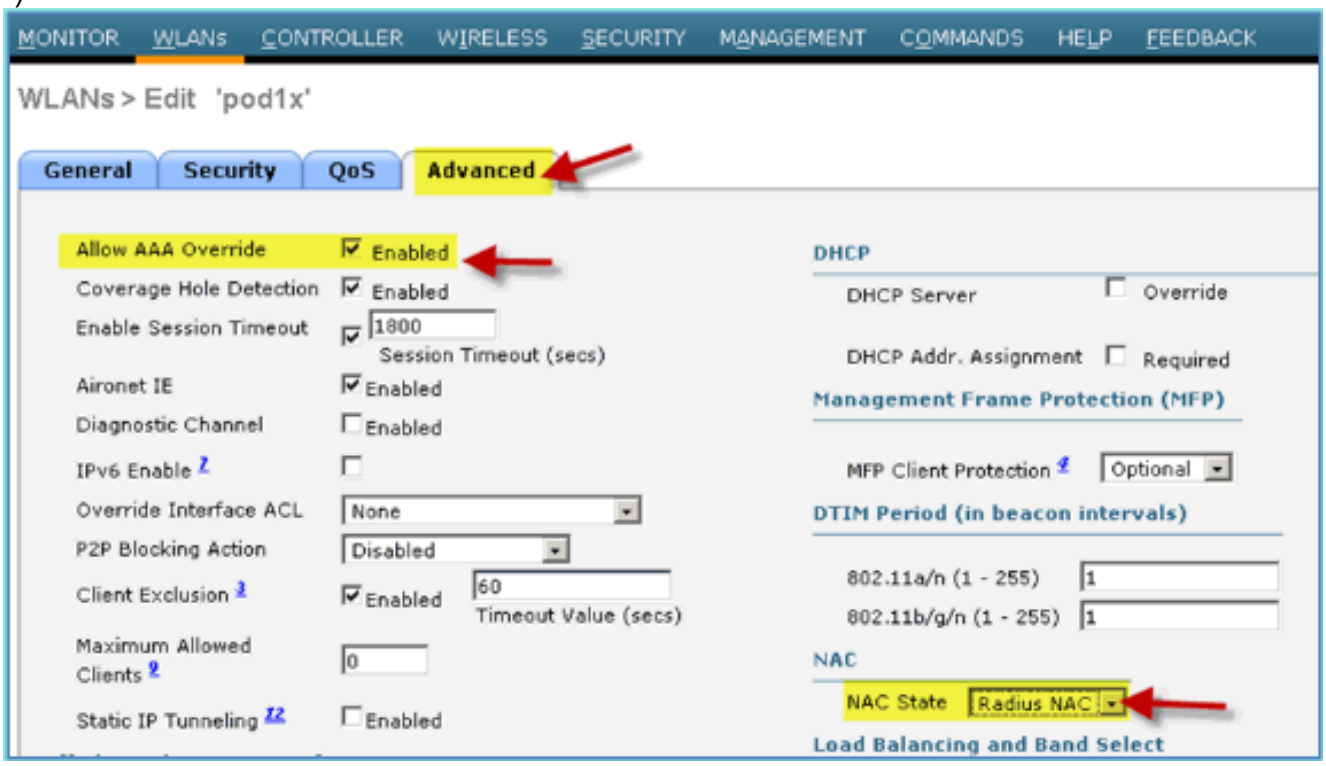


5. [WLAN] > [Security] タブ > [AAA Servers] では、次を設定します。Radio Server Overwrite Interface: Disabled認証/アカウンティングサーバ：有効サーバ 1:10.10.10.70

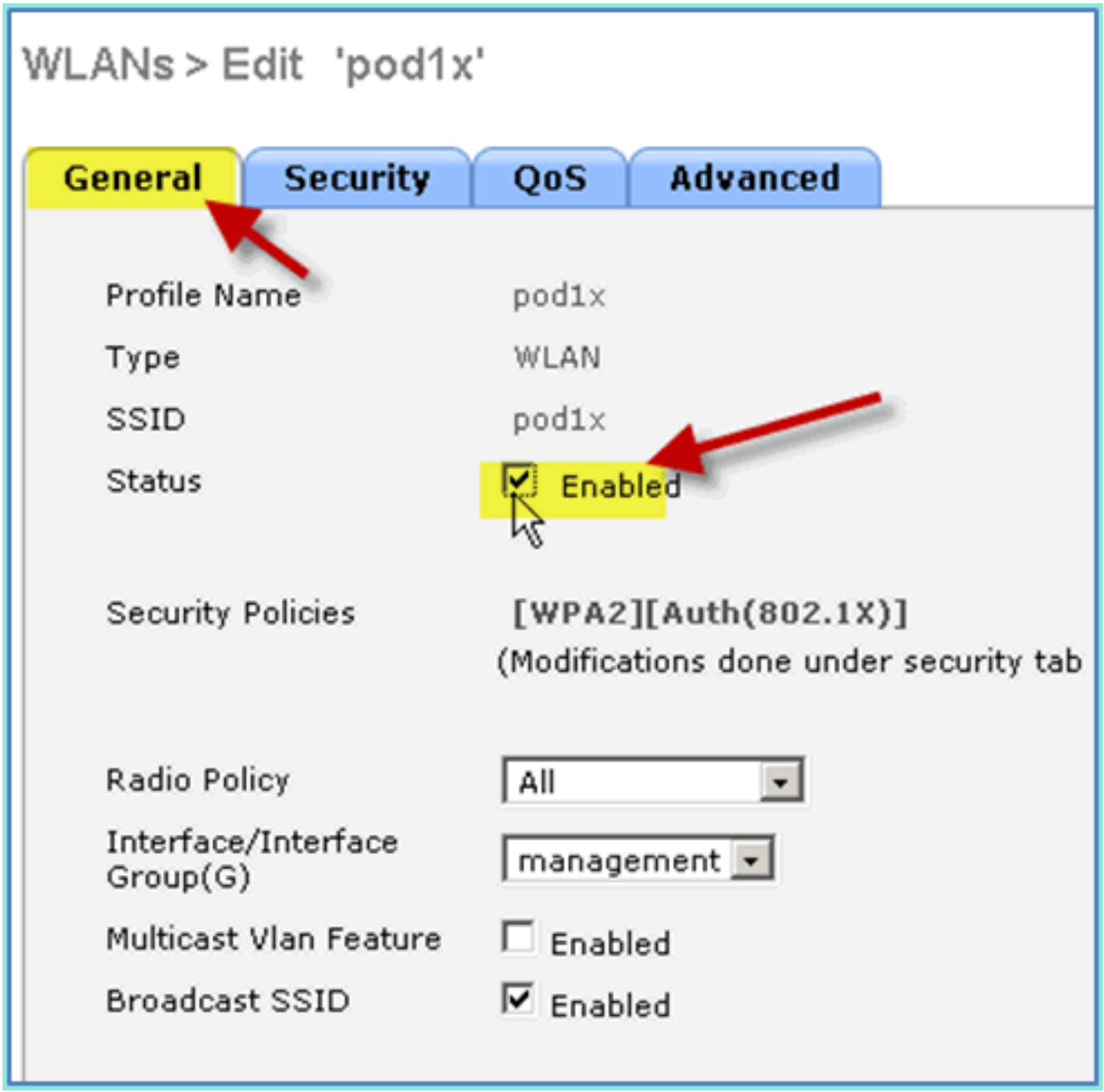


6. [WLAN] > [Advanced] タブでは、次を設定します。[Allow AAA Override]:[Enabled][NAC

State（NAC状態）]:[Radius NAC（半径NAC）]（選択済み
）



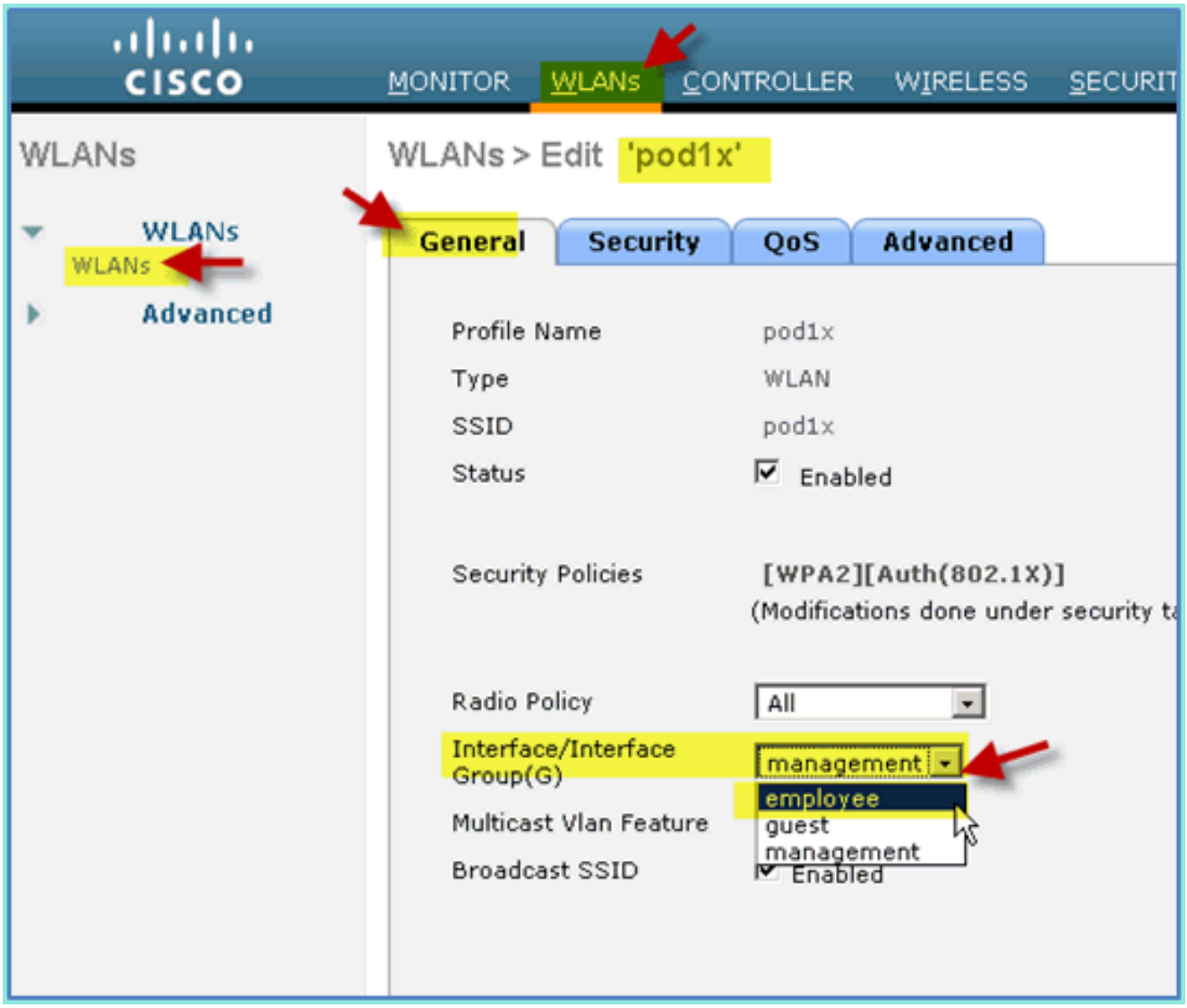
7. [WLAN] > [General] タブ > [Enable WLAN]（チェックボックス）に戻ります。



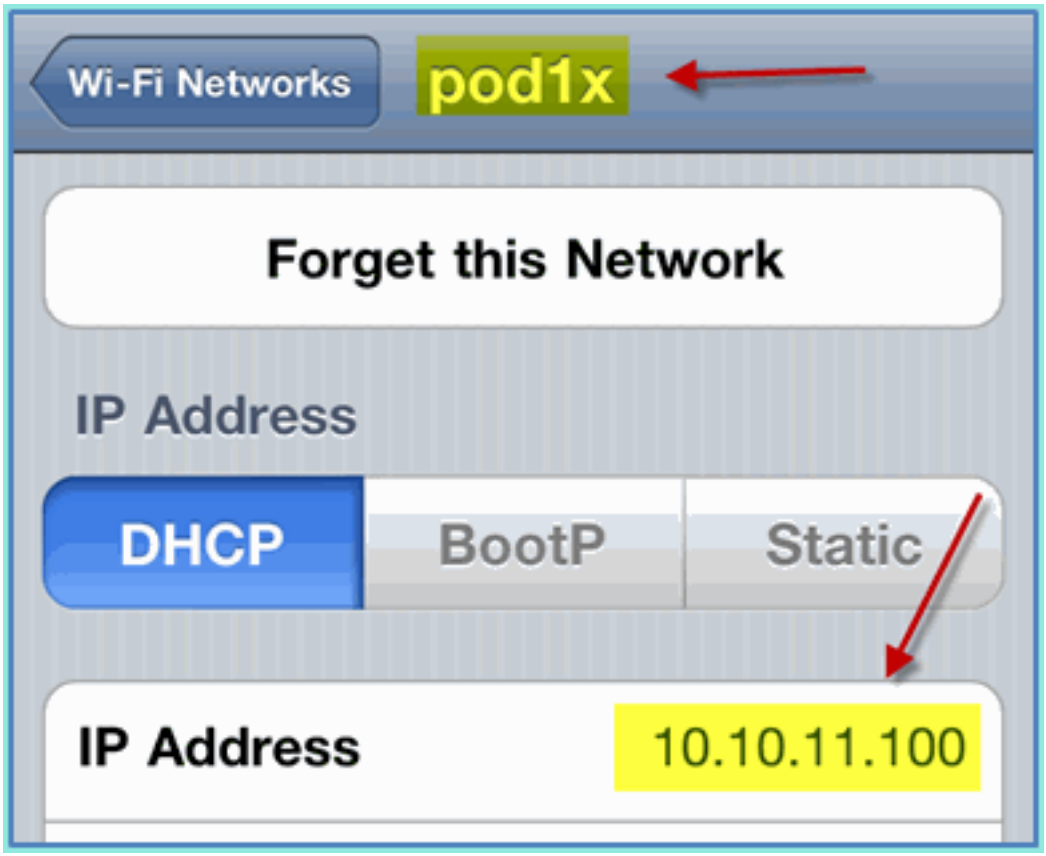
WLC ダイナミック インターフェイスのテスト

従業員とゲストのインターフェイスが有効か、簡単にチェックする必要があります。WLAN に関連付ける任意のデバイスを使用して、WLAN インターフェイスの割り当てを変更します。

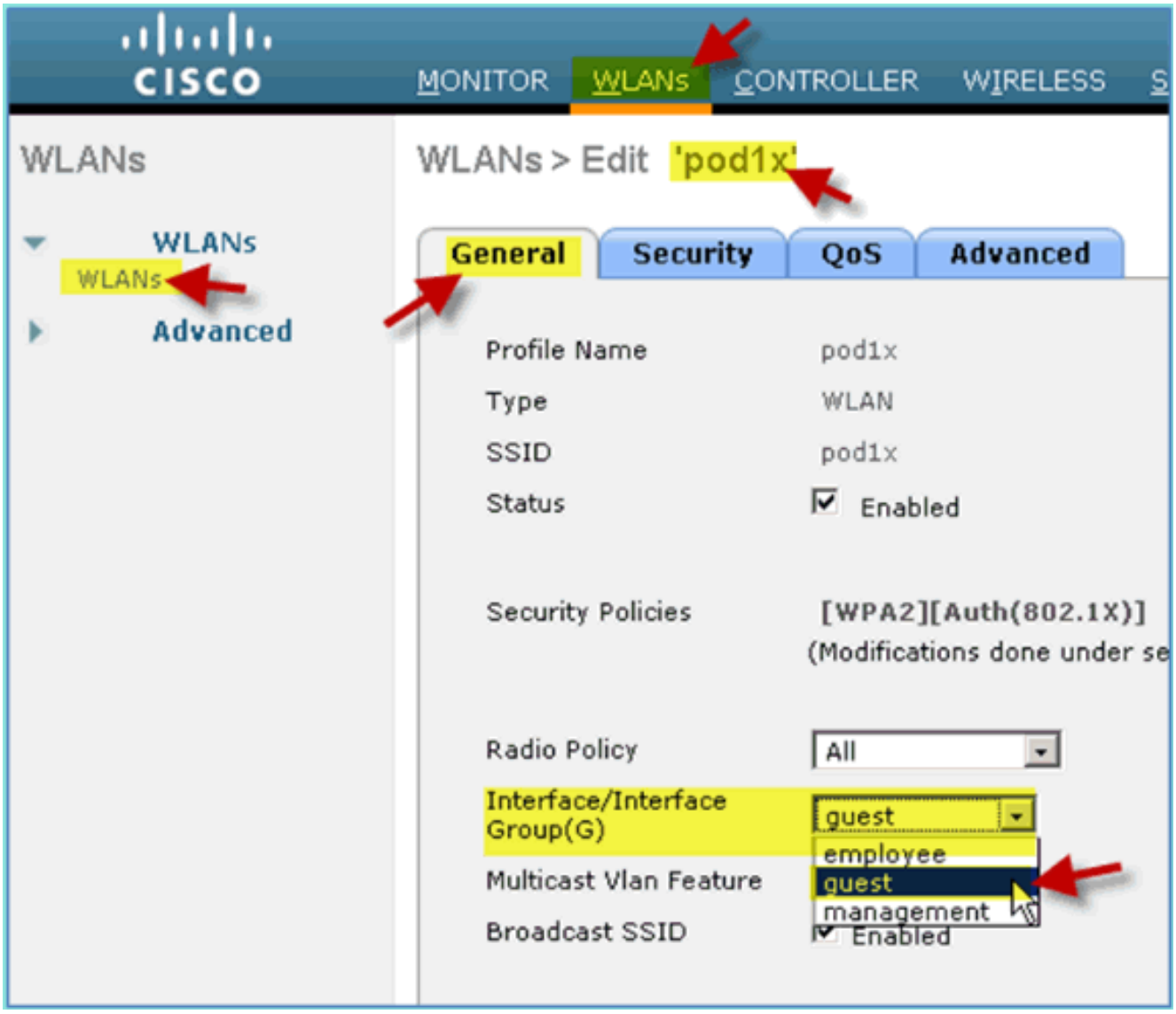
1. WLC から [WLAN] > [WLANs] に移動します。クリックして、先ほどの作業で作成された安全な SSID を編集します。
2. [Interface/Interface Group] を [Employee] に変更し、[Apply] をクリックします。



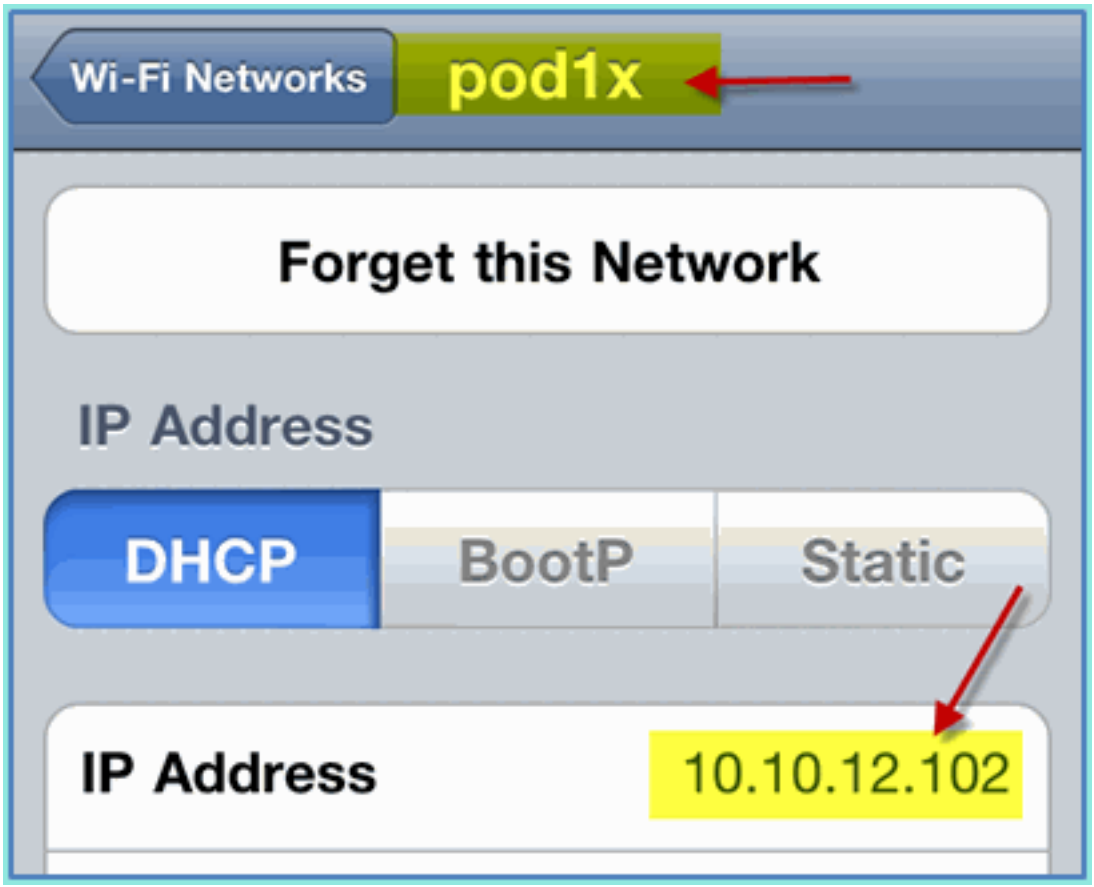
3. 適切に設定されていると、デバイスは従業員 VLAN（10.10.11.0/24）から IP アドレスを受信します。この例では、新しい IP アドレスを取得する iOS デバイスを示しています。



4. 先ほどのインターフェイスを確認したら、WLAN のインターフェイスの割り当てを [Guest] に変更し、[Apply] をクリックします。



5. 適切に設定されていると、デバイスはゲスト VLAN（10.10.12.0/24）から IP アドレスを受信します。この例では、新しい IP アドレスを取得する iOS デバイスを示しています。



6. **重要：インターフェイスの割り当てを元の管理に戻します。**
7. [Apply] をクリックして、WLC の設定を保存します。

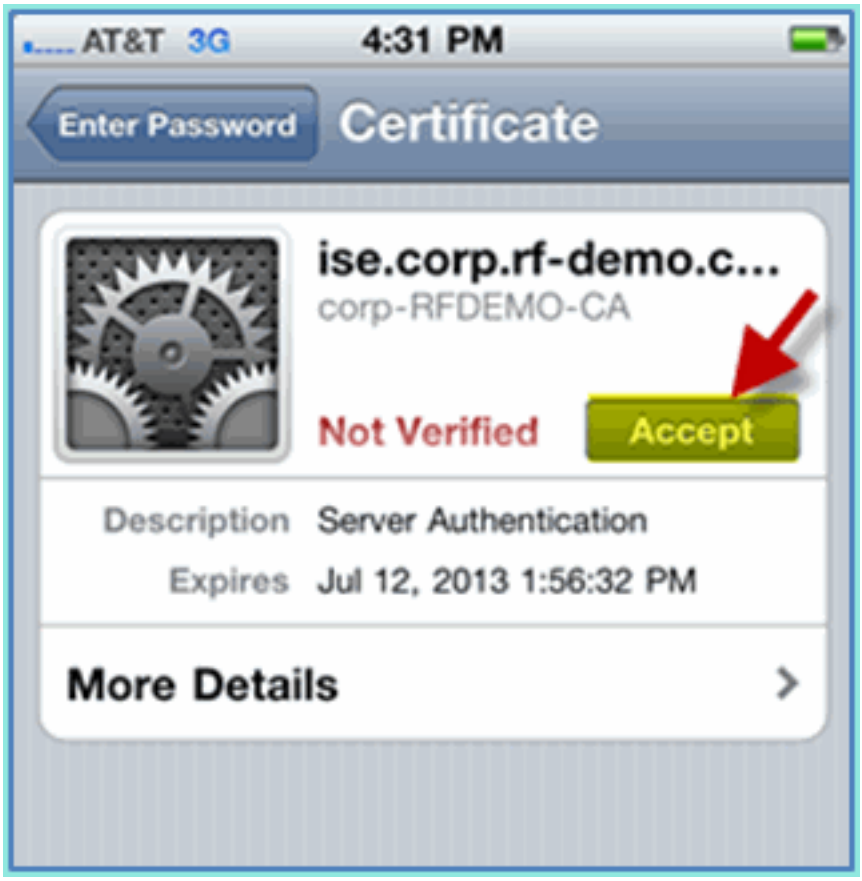
iOS（iPhone/iPad）のワイヤレス認証

iPhone、iPad、または iPod などの iOS デバイスを使用して認証された SSID 経由で、WLC に社内ユーザ（または統合された AD ユーザ）を関連付けます。該当しない手順は飛ばしてください。

1. iOS デバイスで、WLAN の設定に移動します。Wi-Fi を有効にし、前のセクションで作成された 802.1X 対応の SSID を選択します。
2. 次の情報を入力して接続します。ユーザ名：従業員（社内 – 従業員）または請負業者（社内 – 請負業者）パスワード

: XXXX

3. クリックして ISE 証明書を受け入れます。

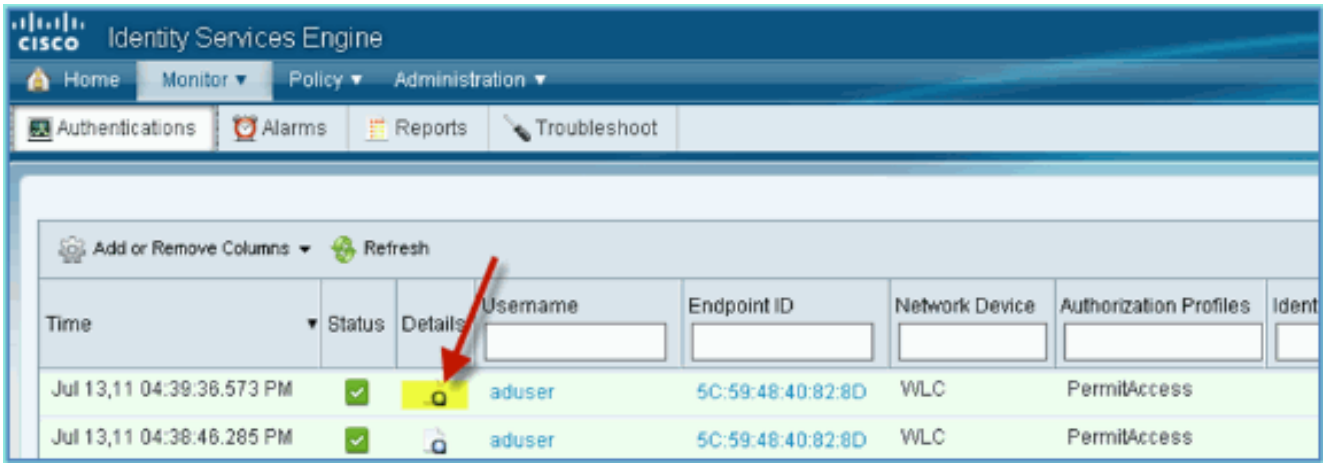


4. iOS デバイスが管理（VLAN10）インターフェイスから IP アドレスを取得していることを確

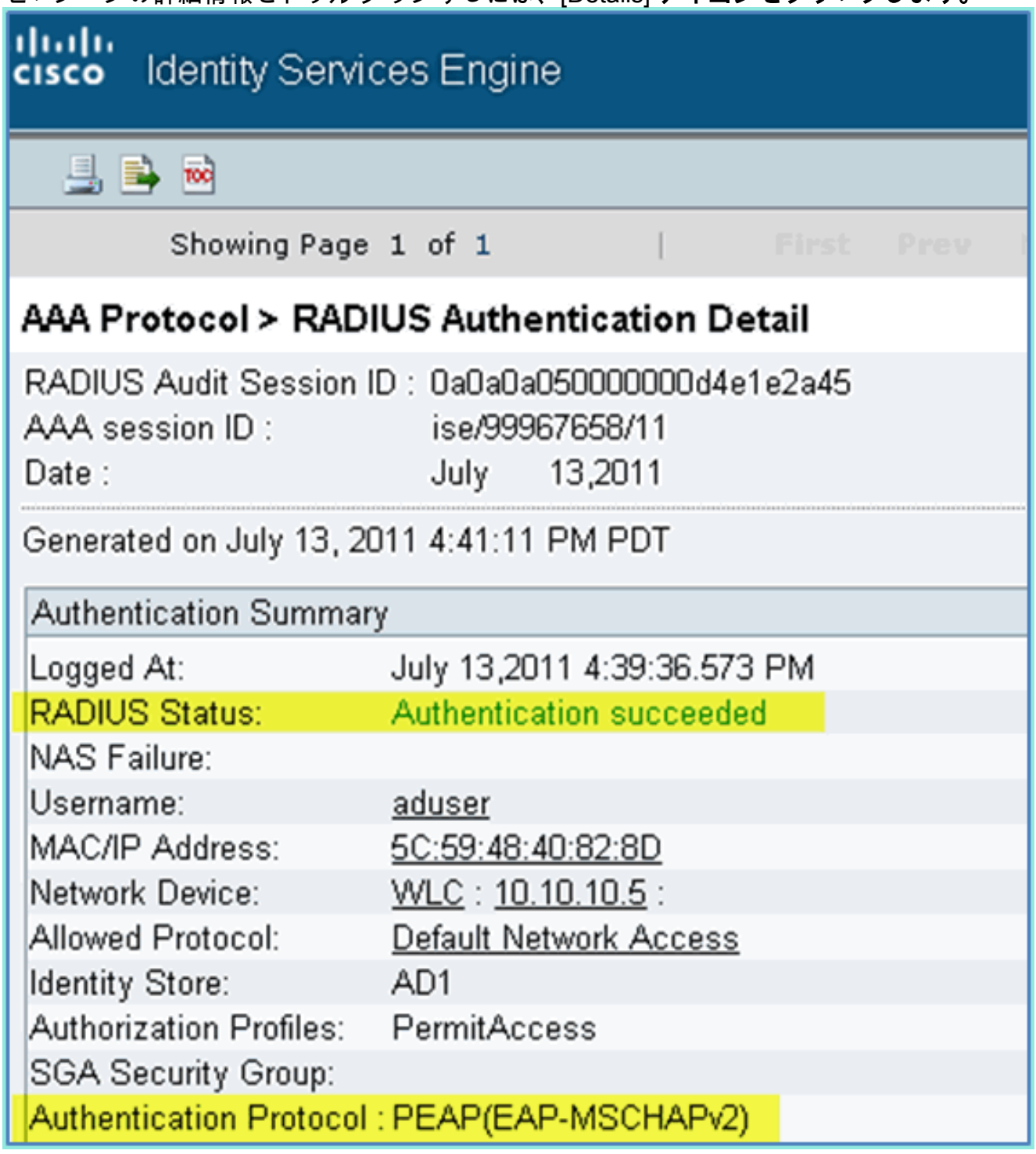
認します。

5. [WLC] > [Monitor] > [Clients] で、使用状況、状態および EAP のタイプを含むエンドポイント情報を確認します。

6. 同様に、クライアント情報が [ISE] > [Monitor] > [Authentication] で提供されます。



7. セッションの詳細情報をドリル ダウンするには、[Details] **アイコンをクリックします。**

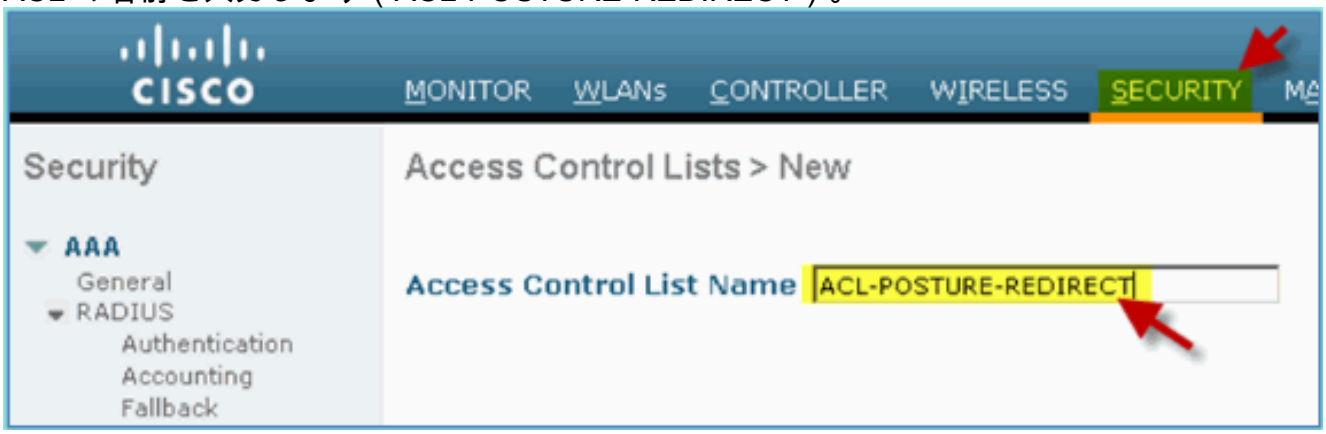


WLC へのポスチャ リダイレクト ACL の追加

ポスチャ リダイレクト ACL は WLC で設定されます。ここで ISE を使用してポスチャのためにクライアントが制限されます。実際には、ACL は最低でも ISE 間のトラフィックを許可します。必要に応じてこの ACL にオプション ルールを追加できます。

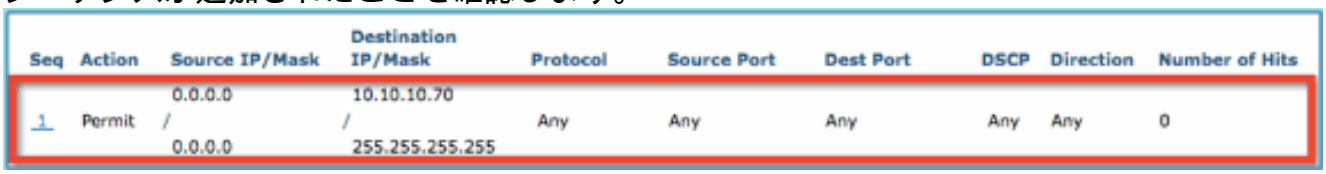
1. [WLC] > [Security] > [Access Control Lists] > [Access Control Lists] の順に移動します。[New] をクリックします。

2. ACL の名前を入力します（ACL-POSTURE-REDIRECT）。



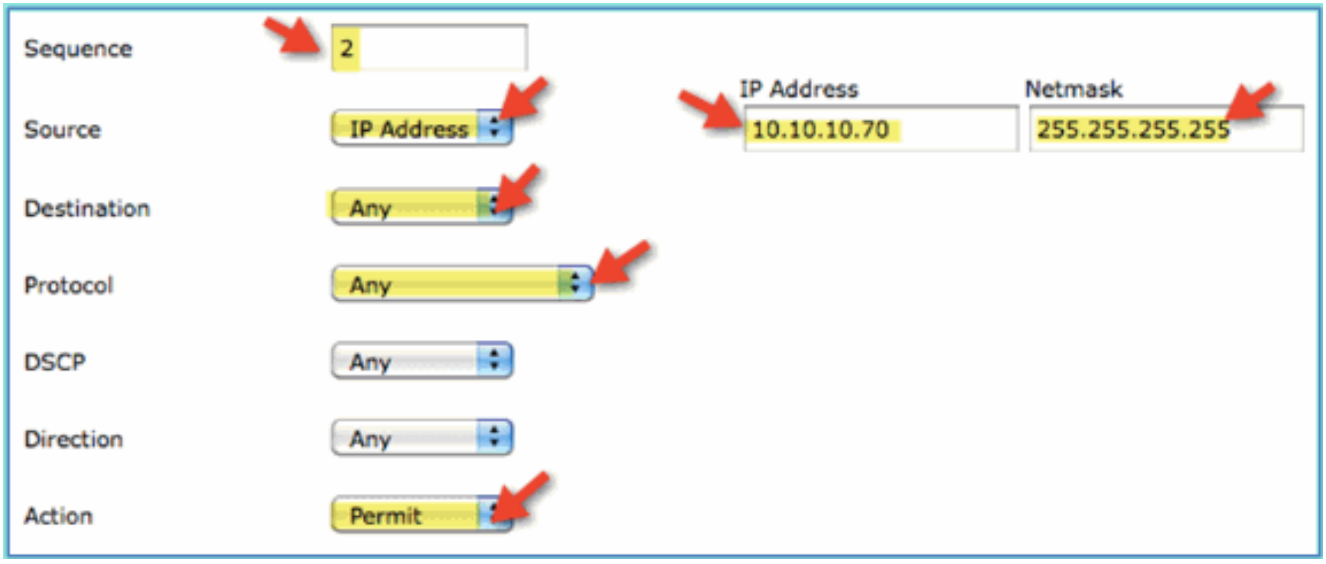
3. 新しい ACL で [Add New Rule] をクリックします。ACL シーケンス #1 に次の値を設定します。最後に、[Apply] をクリックします出典：Any宛先：IPアドレス10.10.10.70、255.255.255.255プロトコル：任意アクション：許可

4. シーケンスが追加されたことを確認します。

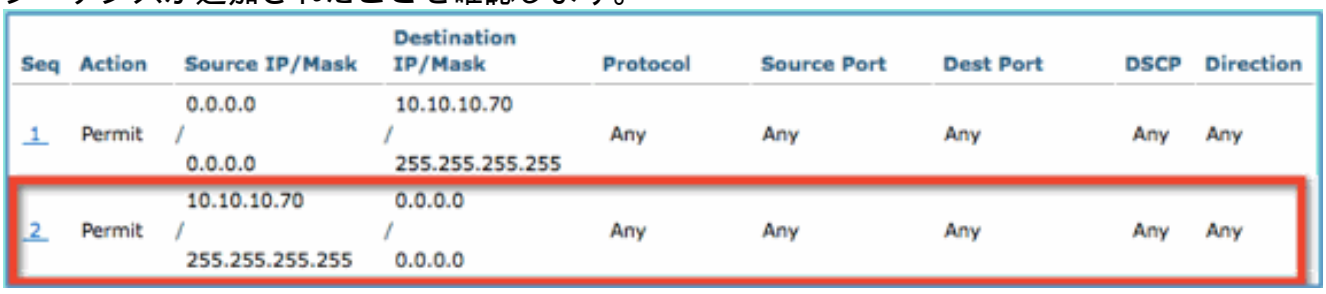


Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

5. [Add New Rule] をクリックします。ACL シーケンス #2 に次の値を設定します。最後に、[Apply] をクリックします送信元：IPアドレス10.10.10.70、255.255.255.255宛先：任意プロトコル：任意アクション：許可

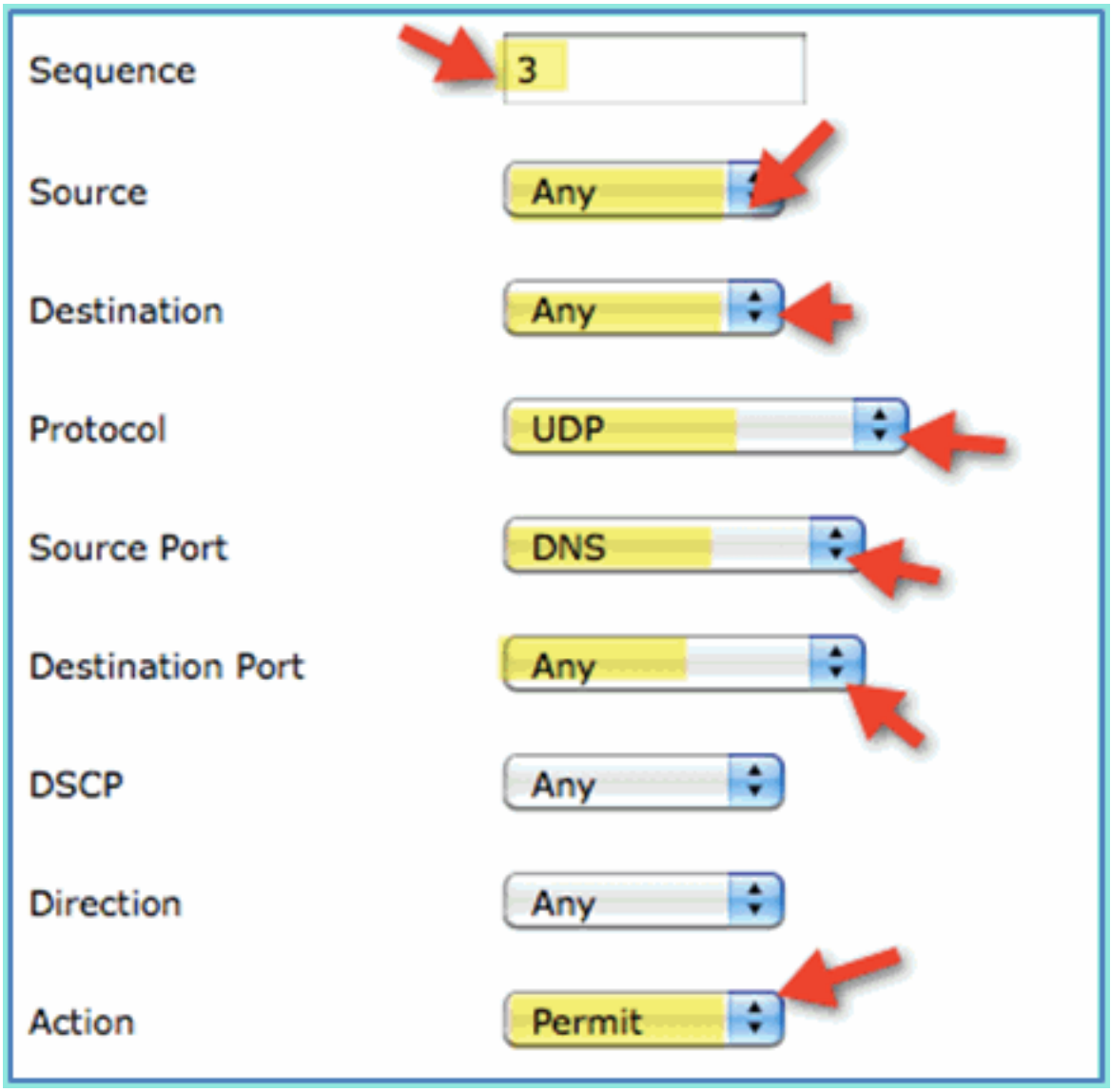


6. シーケンスが追加されたことを確認します。



Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any

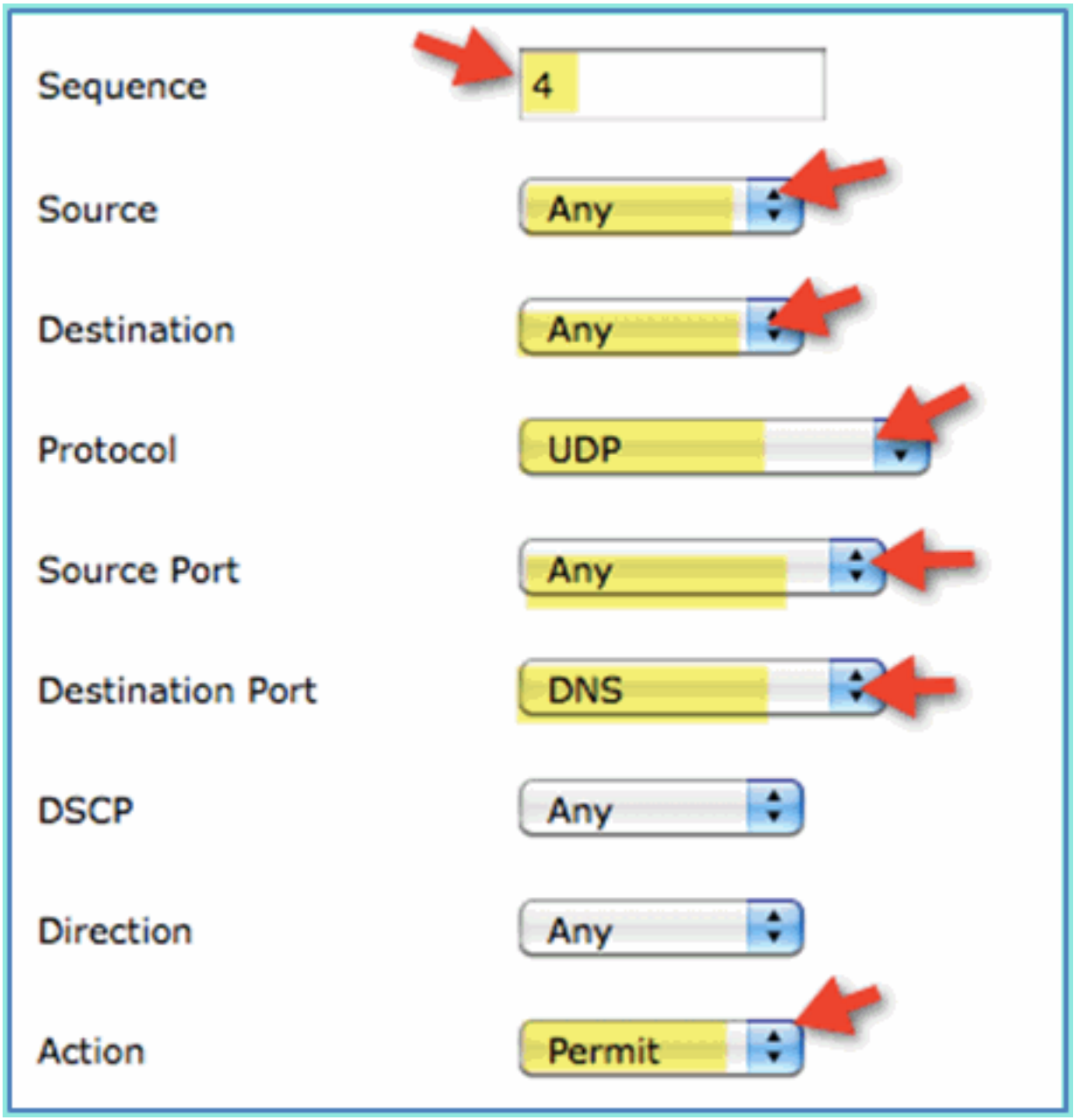
7. ACL シーケンス #3 に次の値を設定します。最後に、[Apply] をクリックします出典：Any宛先：任意プロトコル：UDP送信元ポート：DNS宛先ポート：任意アクション：許可



8. シーケンスが追加されたことを確認します。

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any

9. [Add New Rule] をクリックします。ACL シーケンス #4 に次の値を設定します。最後に、[Apply] をクリックします出典：Any宛先：任意プロトコル：UDP送信元ポート：任意宛先ポート：DNSアクション：許可



10. シーケンスが追加されたことを確認します。

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any

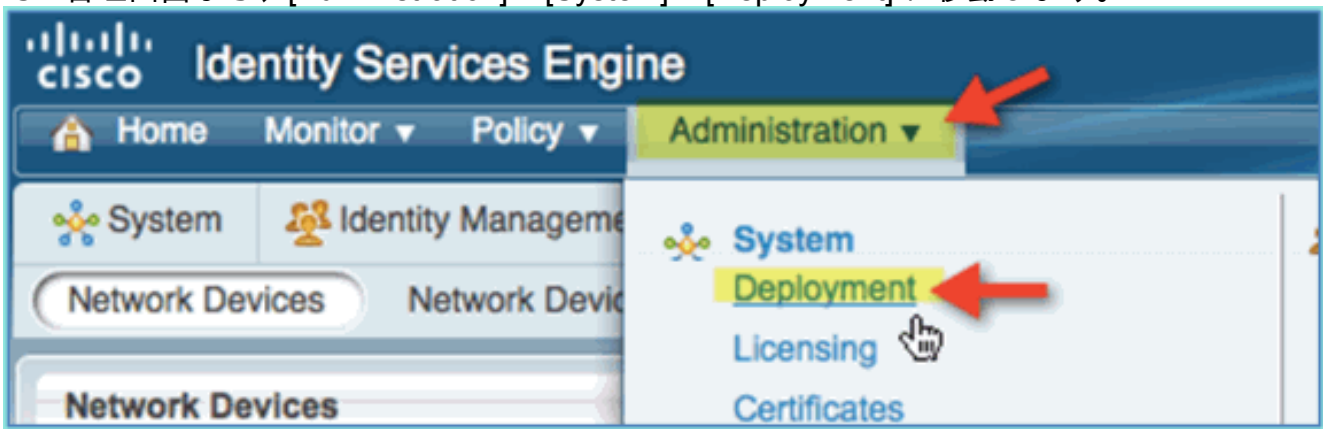
11. 現在の WLC 設定を保存します。

ISE のプローブのプロファイリングの有効化

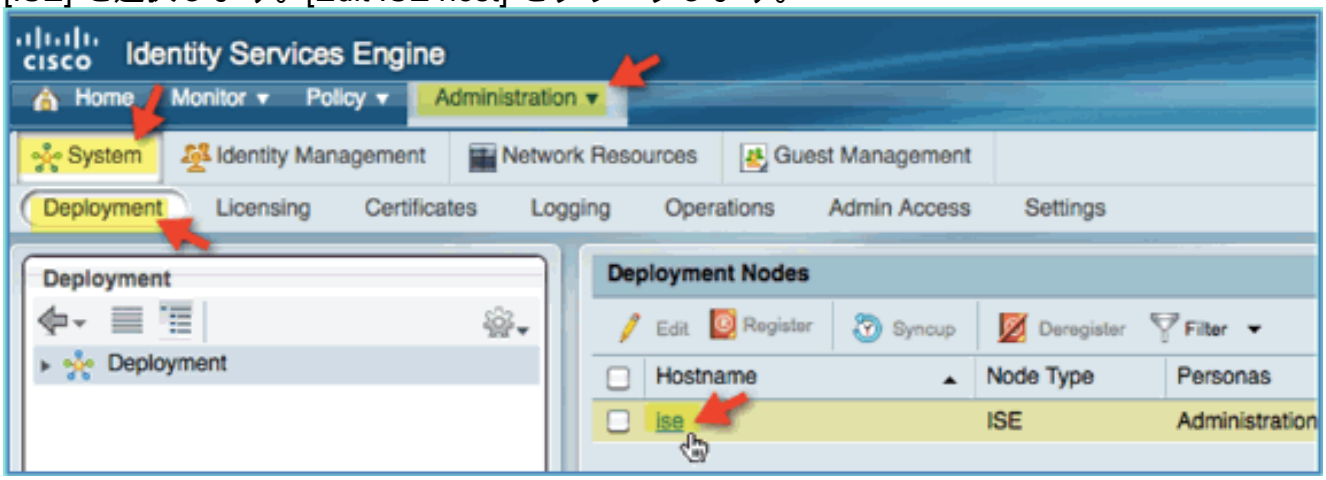
エンドポイントを効果的にプロファイルするには、ISE をプローブとして設定する必要があります。デフォルトでは、これらのオプションはディセーブルです。このセクションでは、ISE をプ

ロープとして設定する方法を示します。

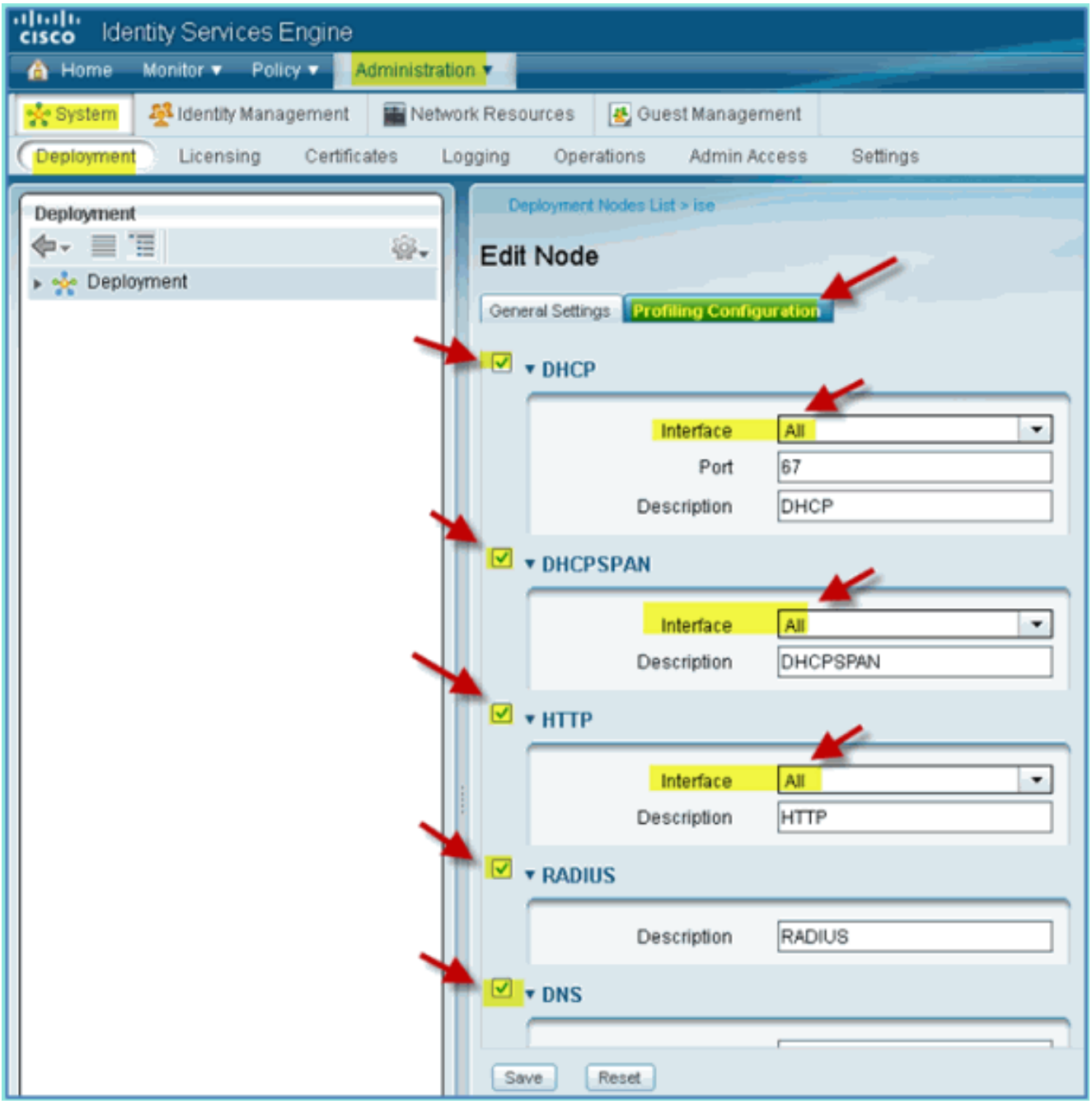
1. ISE 管理画面から、[Administration] > [System] > [Deployment] に移動します。



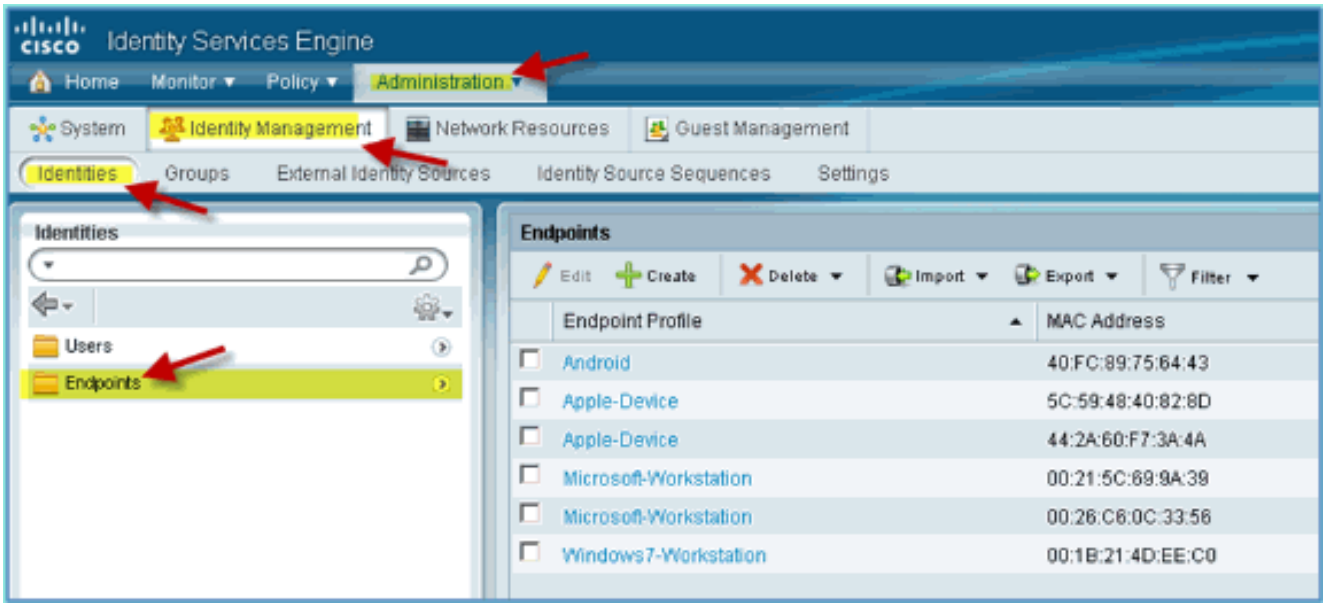
2. [ISE] を選択します。[Edit ISE host] をクリックします。



3. [Edit Node] ページから、[Profiling Configuration] を選択して次を設定します。
DHCP:Enabled、All（またはdefault）DHCPSPAN：有効、すべて（またはデフォルト）HTTP：有効、すべて（またはデフォルト）RADIUS:Enabled、N/ADNS：有効、該当なし



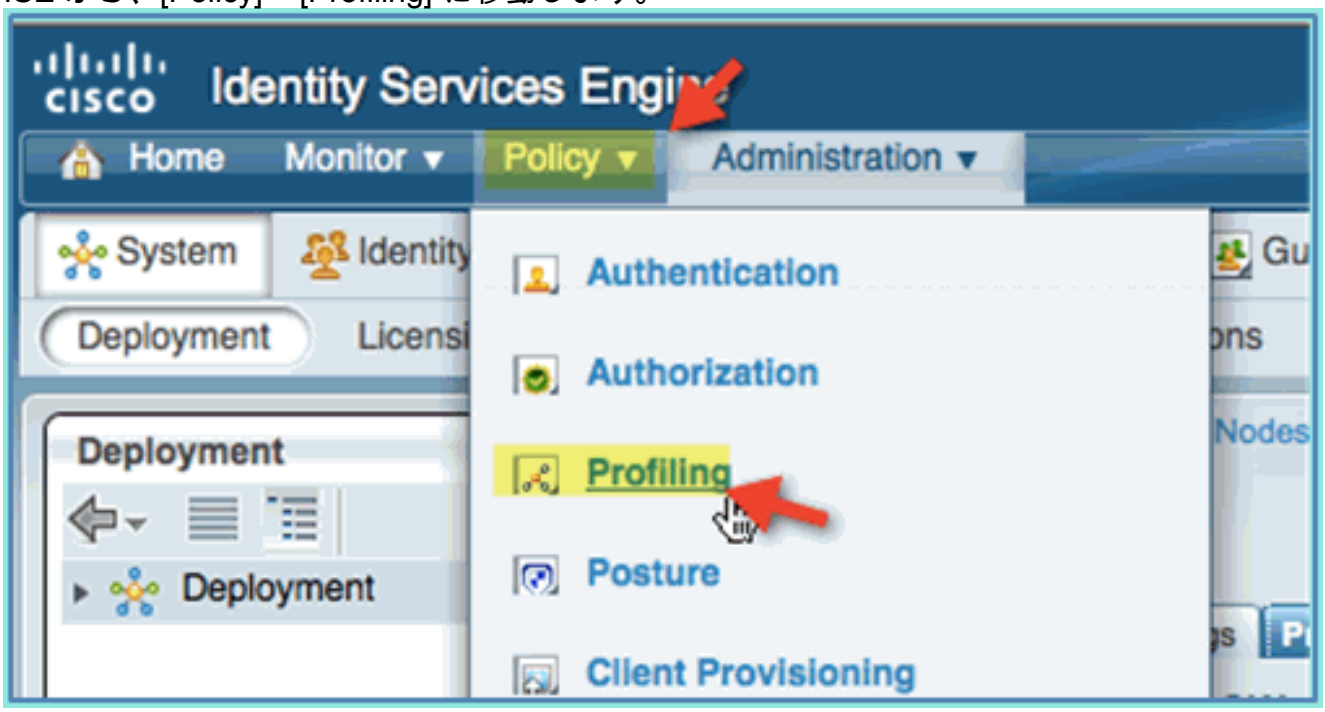
4. デバイス（iPhone/iPad/Droid/Mac など）を再び関連付けます。
5. ISE のエンドポイントの ID を確認します。[Administration] > [Identity Management] > [Identities] の順に移動します。[Endpoints] をクリックし、プロファイリングされたものを一覧表示します。**注：最初のプ**ロファイルはRADIUSプローブからのものです。



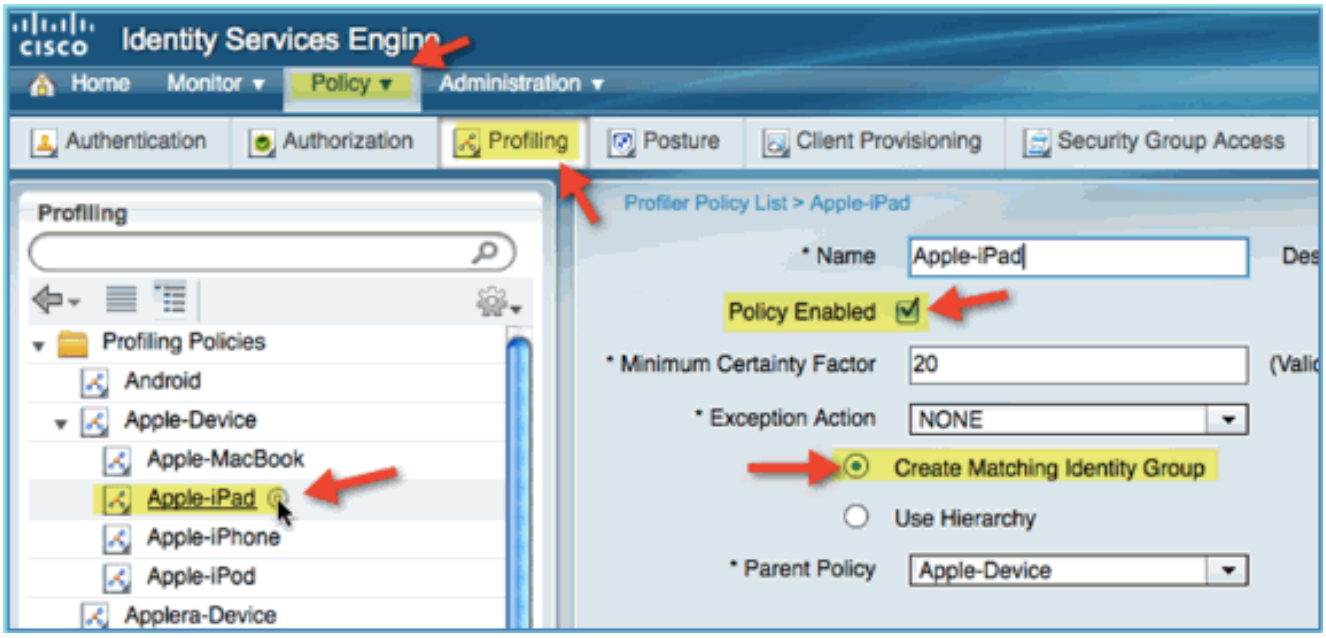
デバイスの ISE プロファイル ポリシーの有効化

ISE はそのままの状態でもさまざまなエンドポイント プロファイルのライブラリを提供します。複数のデバイスのプロファイルを有効にするには、次の手順を実行します。

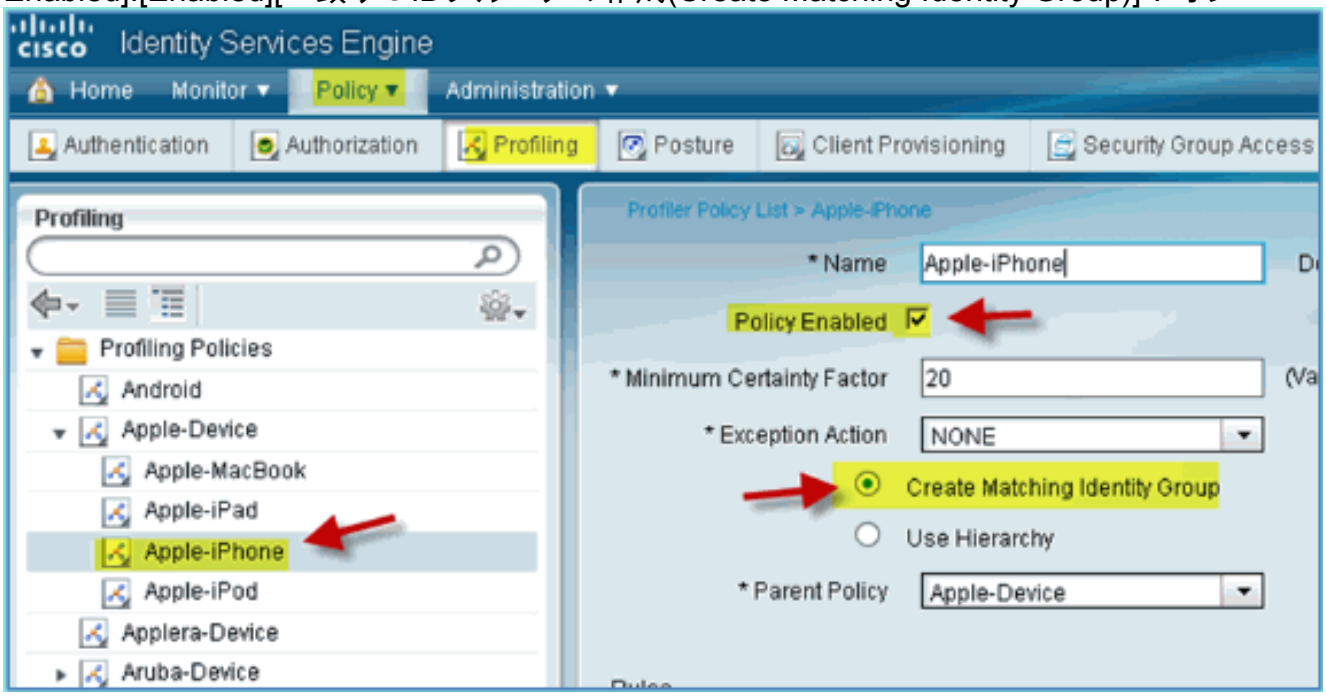
1. ISE から、[Policy] > [Profiling] に移動します。



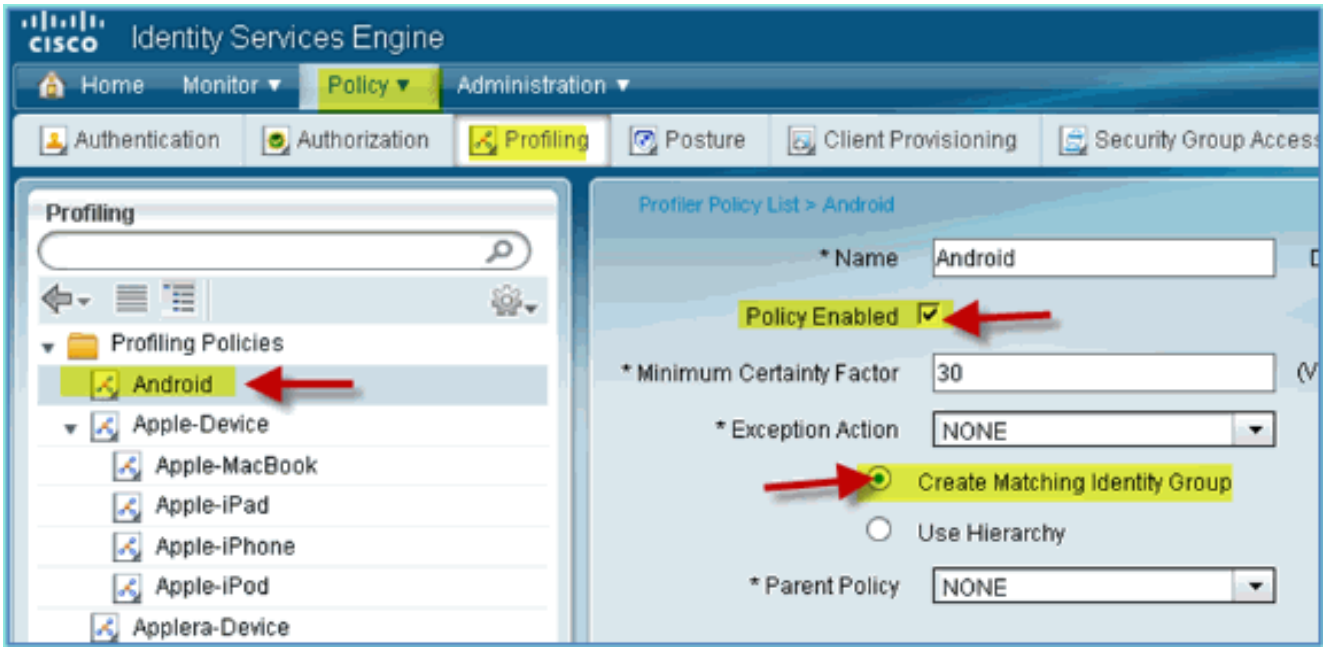
2. 左ペインから、[Profiling Policies] を展開します。
3. [Apple Device] > [Apple iPad] をクリックし、次のように設定します。[Policy Enabled]:[Enabled][一致するIDグループの作成(Create Matching Identity Group)]：オン



4. [Apple Device] > [Apple iPhone] をクリックし、次のように設定します。[Policy Enabled]:[Enabled][一致するIDグループの作成(Create Matching Identity Group)]：オン



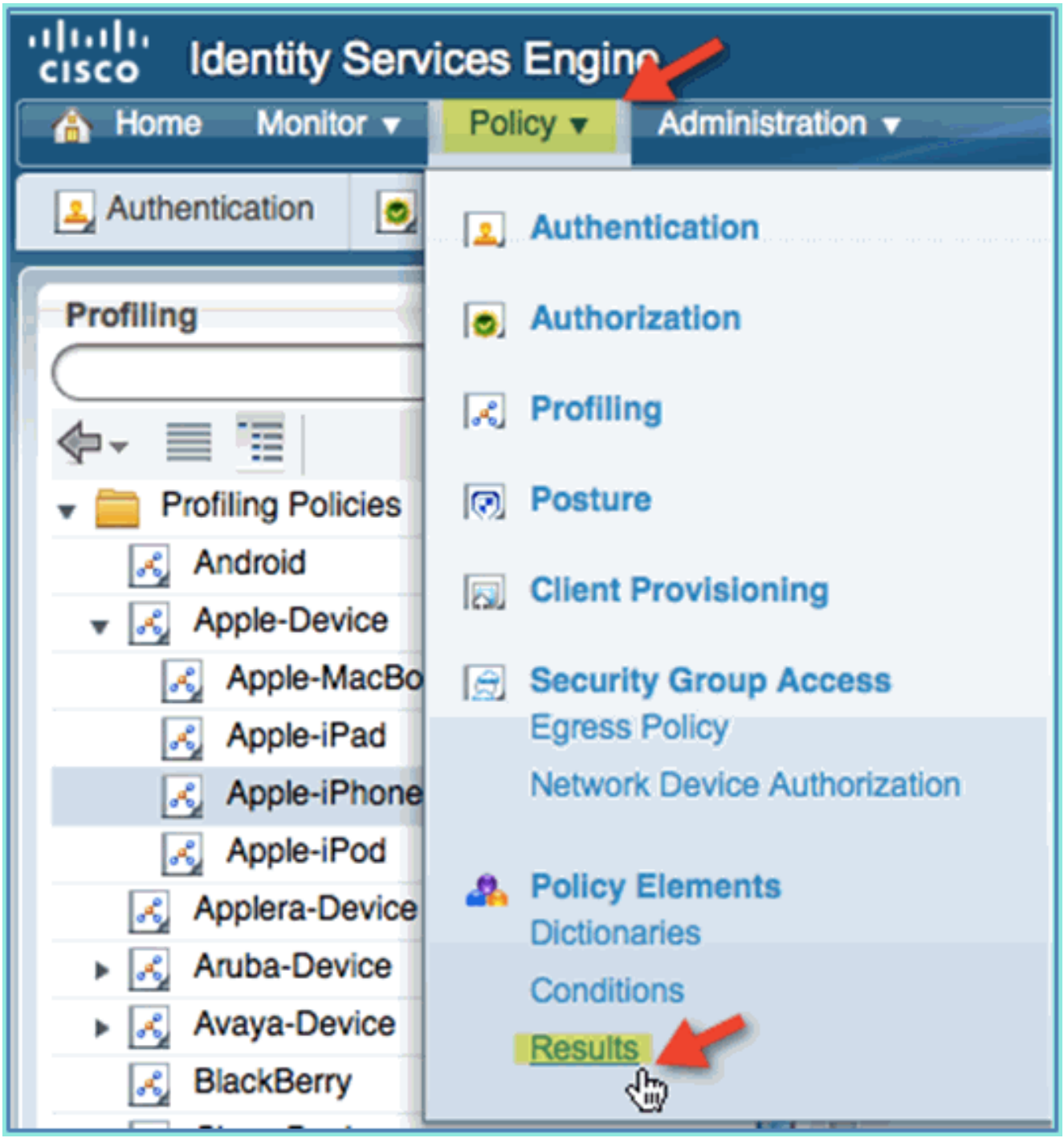
5. [Android] をクリックし、次のように設定します。[Policy Enabled]:[Enabled][一致するIDグループの作成(Create Matching Identity Group)]：オン



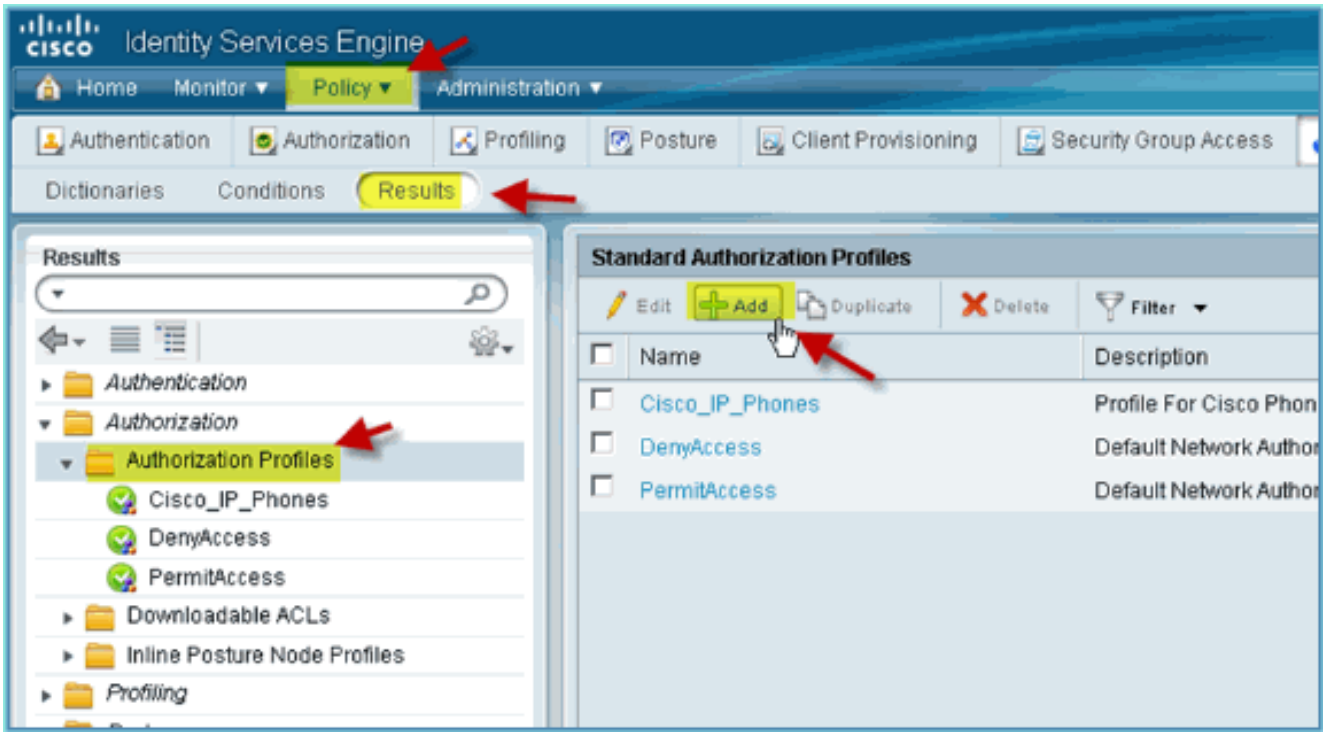
ポスチャ検出リダイレクト用の ISE 認証プロファイル

ポスチャ リダイレクトの認証ポリシーを設定し、新しいデバイスが ISE にリダイレクトされて適切な検出およびプロファイリングを行えるようにするには、次の手順を実行します。

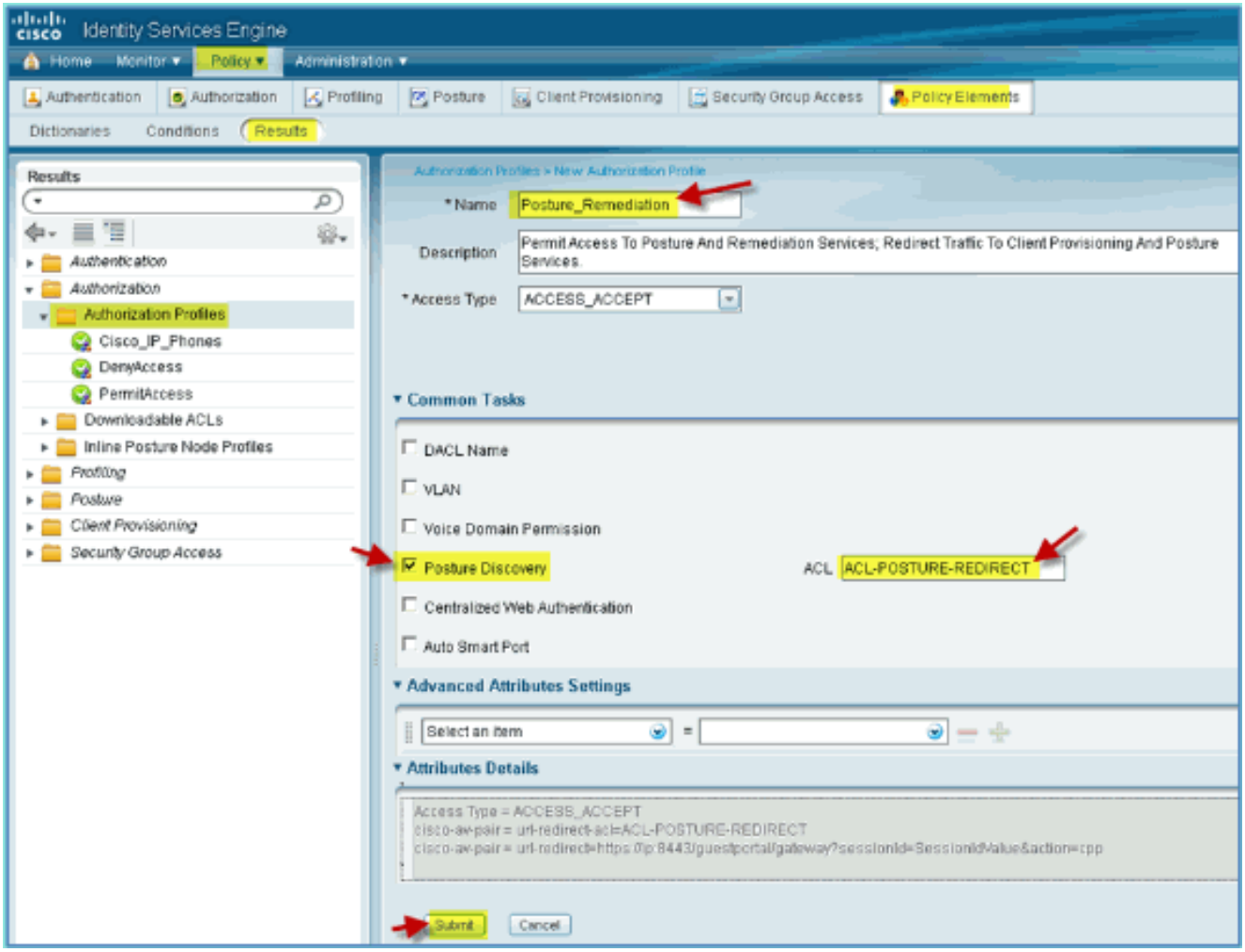
1. ISE から、[Policy] > [Policy Elements] > [Results] に移動します。



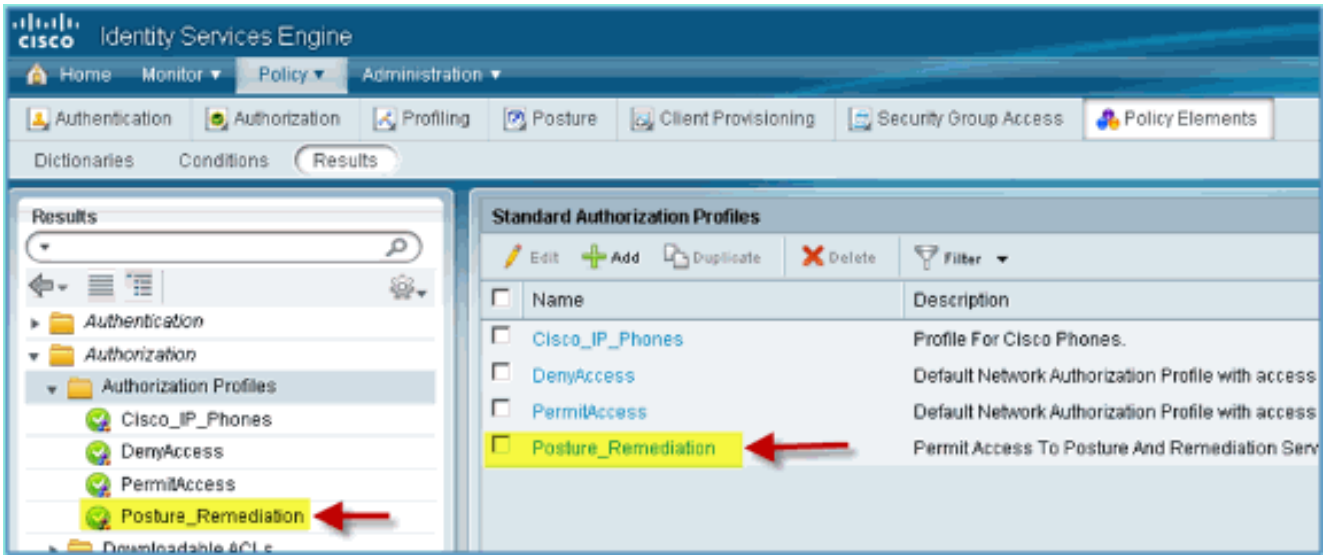
2. [Authorization] を展開します。[Authorization **Profiles] (左ペイン) をクリックし、[Add] をクリックします。**



3. 以下のように認証ポリシーを作成します。[Name]:Posture_Remediation[Access Type]:Access_Accept共通ツール：Posture Discovery、有効化Posture Discovery、ACL ACL-POSTURE-REDIRECT



4. [Submit] をクリックして、この作業を完了します。
5. 新しい認証プロファイルを追加されたことを確認します。

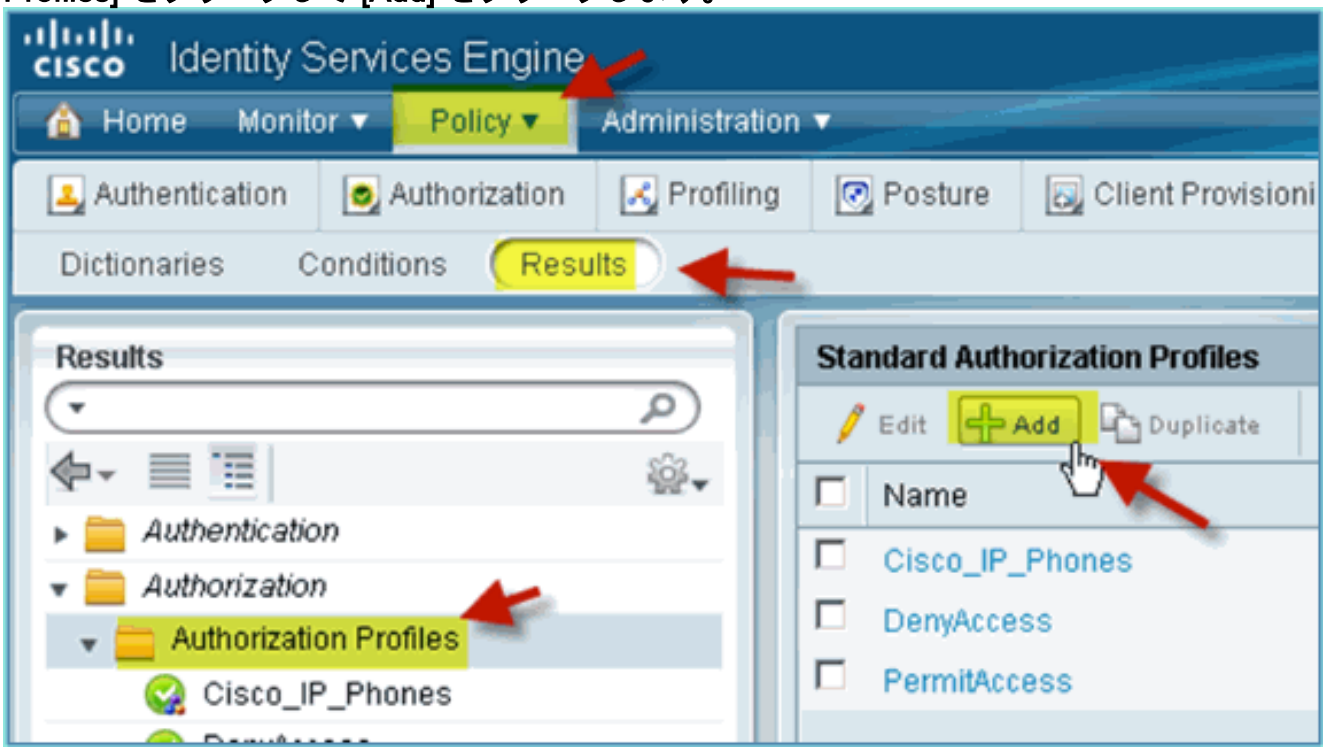


従業員用の ISE 認証プロファイルの作成

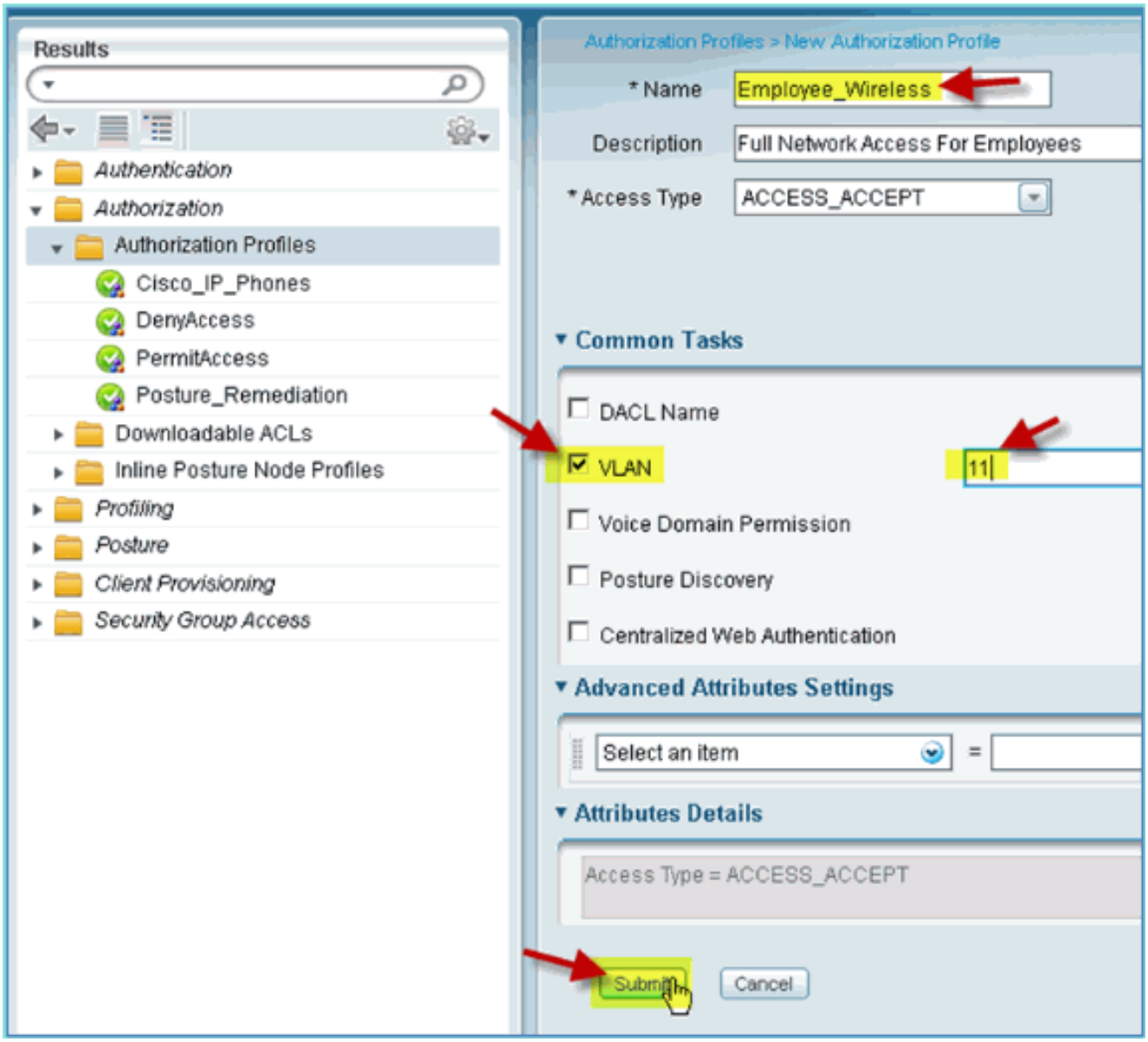
従業員用の認証プロファイルを追加すると、ISE は割り当てられた属性を持つアクセスを認証し、許可できるようになります。この場合は従業員 VLAN 11 が割り当てられます。

次のステップを実行します。

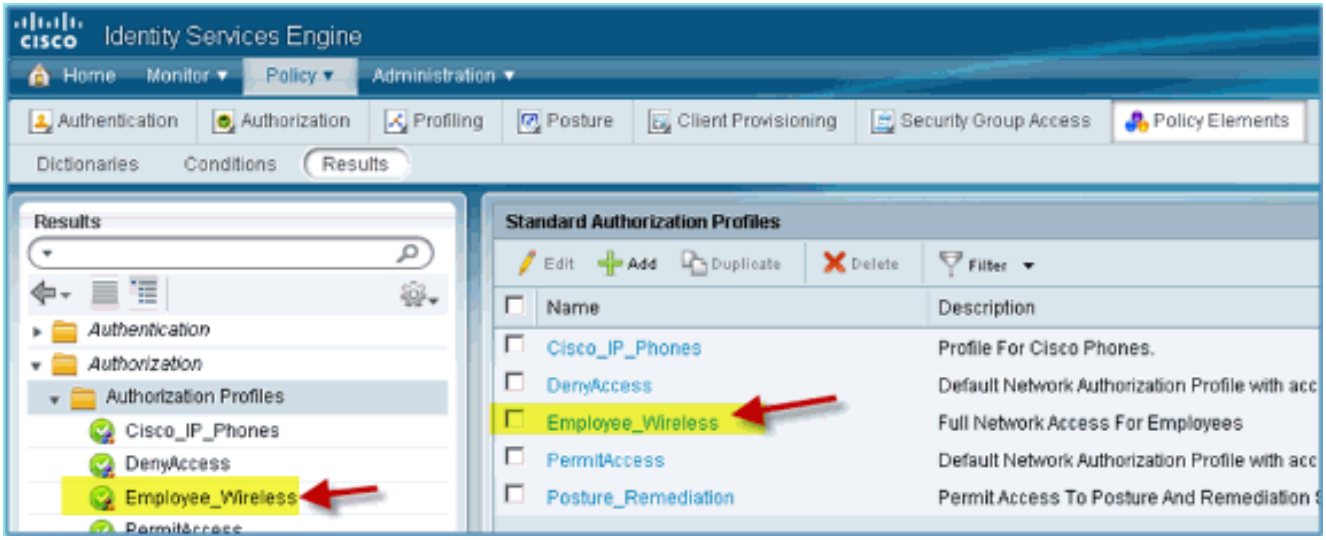
1. ISE から、[Policy] > [Results] に移動します。**[Authorization] を展開し、[Authorization Profiles] をクリックして [Add] をクリックします。**



2. 従業員認証プロファイルに次を入力します。[Name（名前）]:Employee_Wireless共通タスク：VLAN、有効VLAN、サブ値 11
3. [Submit] をクリックして、この作業を完了します。



4. 従業員の認証プロファイルが新たに作成されたことを確認します。

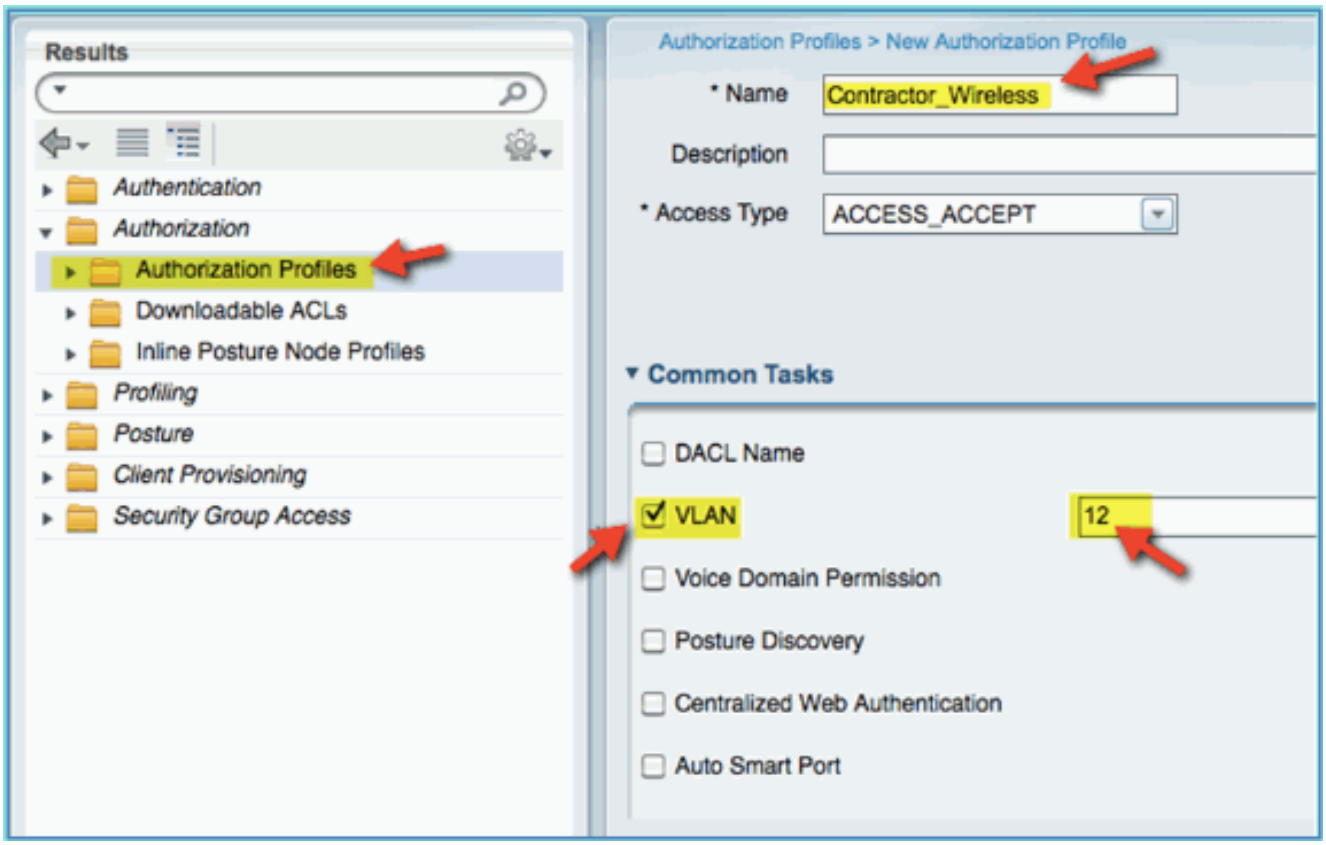


請負業者用の ISE 認証プロファイルの作成

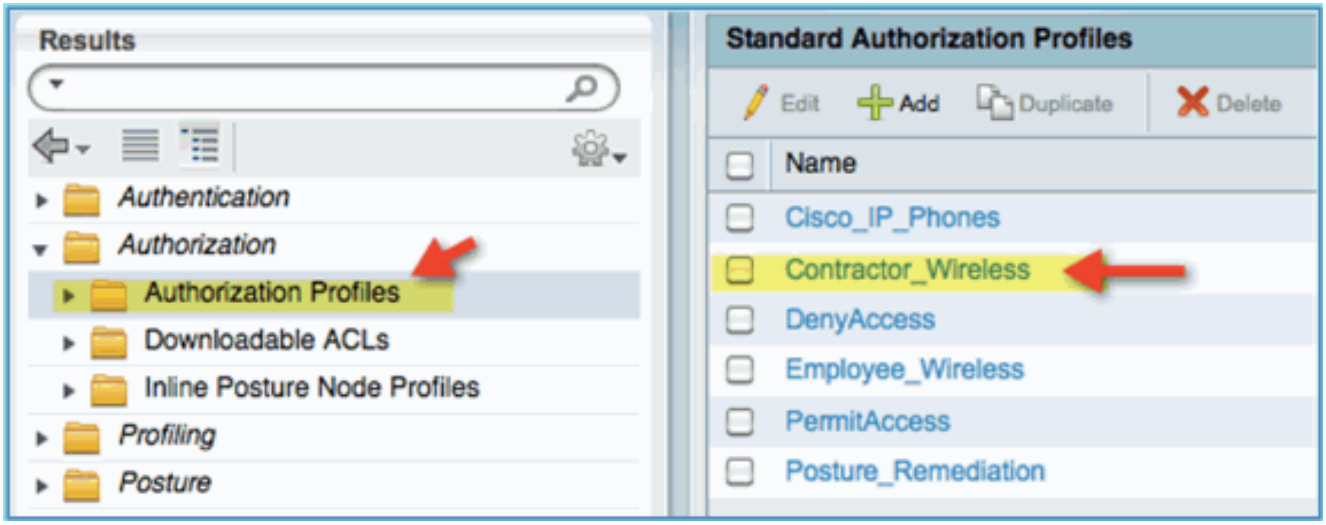
請負業者用の認証プロファイルを追加すると、ISE は割り当てられた属性を持つアクセスを認証し、許可できるようになります。この場合は請負業者 VLAN 12 が割り当てられます。

次のステップを実行します。

1. ISE から、[Policy] > [Results] に移動します。**[Authorization] を展開し、[Authorization Profiles] をクリックして [Add] をクリックします。**
2. 従業員認証プロファイルに次を入力します。[Name（名前）]:Employee_Wireless共通タスク：VLAN、有効VLAN、サブ値
   12



3. [Submit] をクリックして、この作業を完了します。
4. 請負業者の認証プロファイルが新たに作成されたことを確認します。



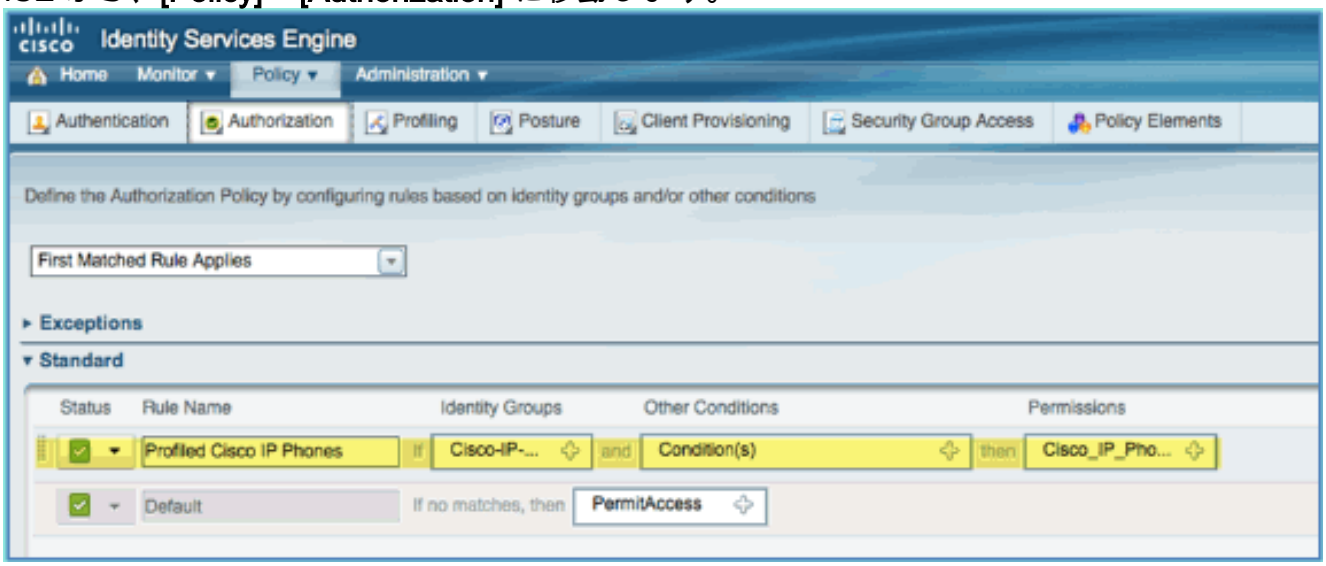
デバイス ポスチャ/プロファイリングの認証ポリシー

新しいデバイスが最初にネットワークに参加すると、そのデバイスに関する情報はほとんどありません。そのため、アクセスを許可する前に不明なエンドポイントを特定できるように、管理者は適切なポリシーを作成することになります。この演習では、ポスチャ評価のために新しいデバイスがISEにリダイレクトされ（モバイルデバイスはエージェントレスであるため、プロファイ

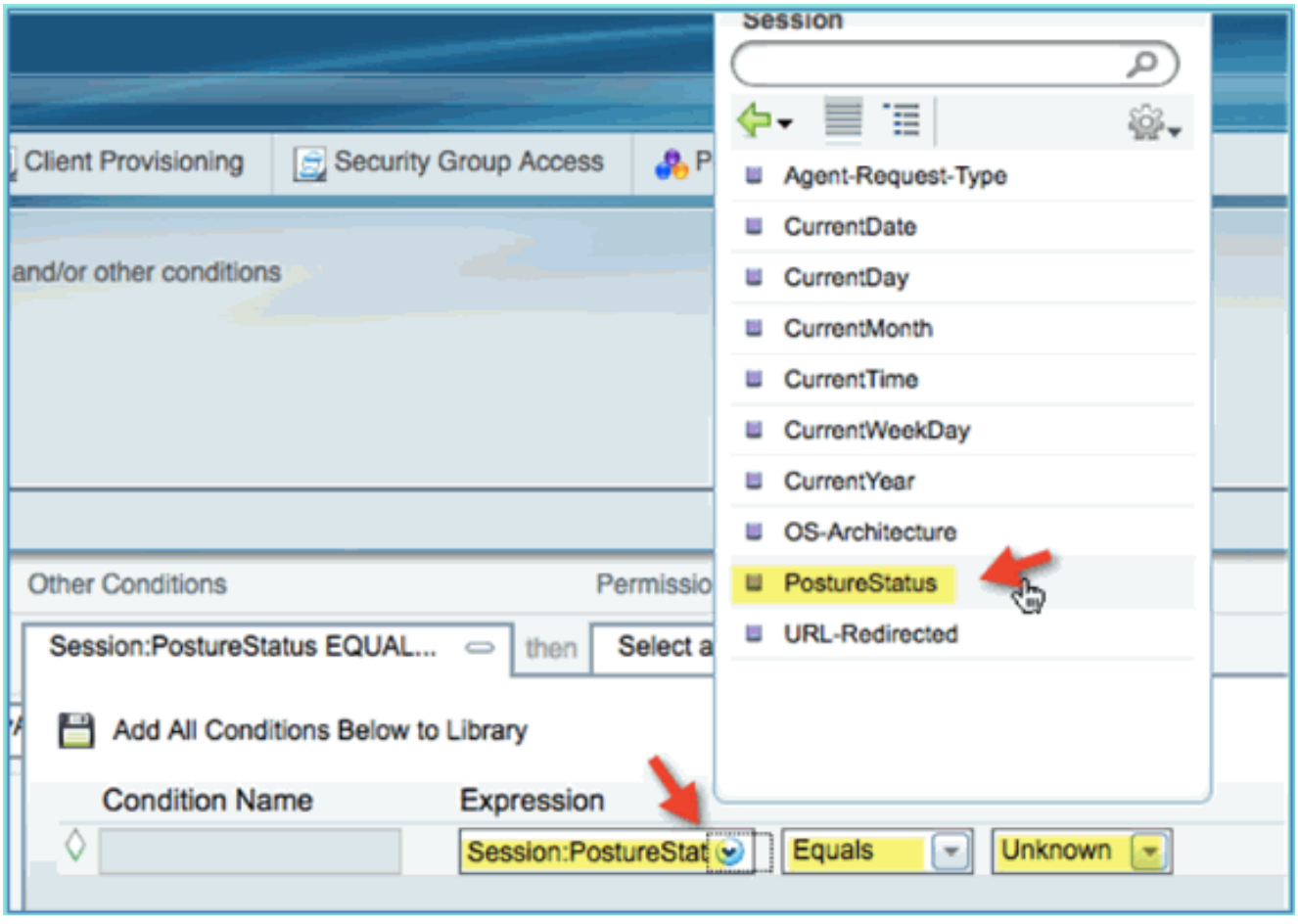
リングだけが関連します）、エンドポイントがISEキャプティブポータルにリダイレクトされて識別されるように、認証ポリシーが作成されます。

次のステップを実行します。

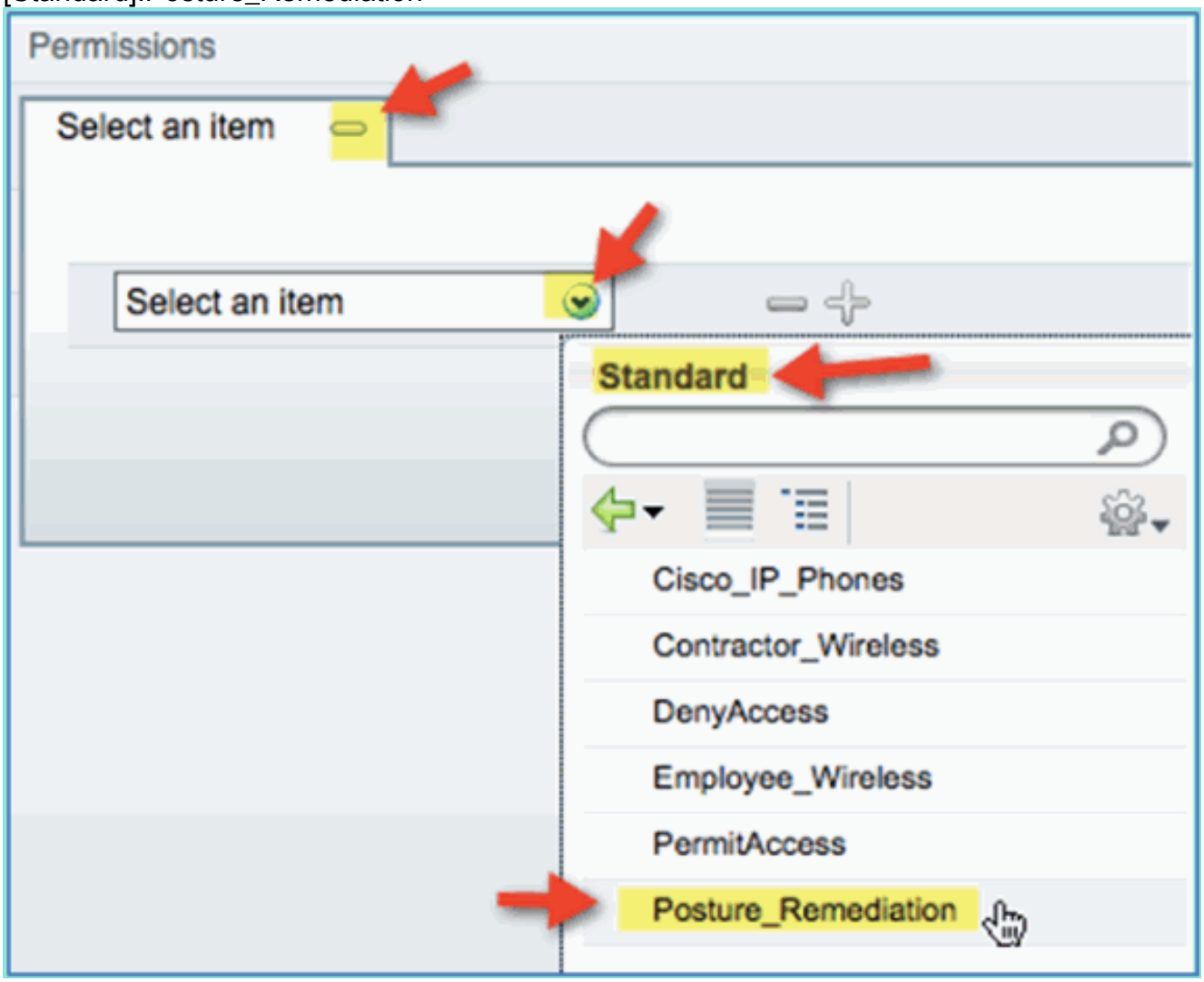
1. ISE から、**[Policy] > [Authorization]** に移動します。



2. プロファイリング済みの Cisco IP Phone のポリシーがあります。これはカスタマイズ前の状態です。これをポスチャ ポリシーとして編集します。
3. このポリシーに次の値を入力します。[Rule Name（ルール名）]:Posture_Remediation[Identity Groups]：任意[その他の条件(Other Conditions)] > [新規作成(Create New)]:（詳細）セッション> [ポスチャステータス(PostureStatus)]PostureStatus > Equals:
Unknown



4. アクセス許可を次のように設定します。[Permissions] > [Standard]:Posture_Remediation

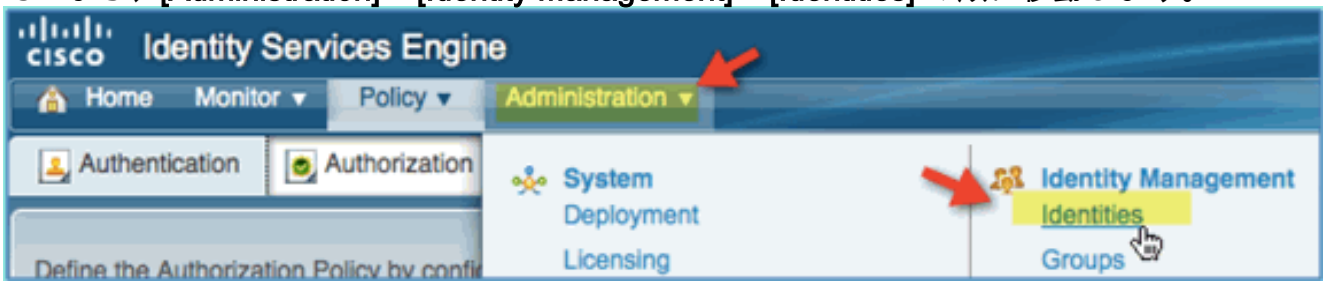


5. [Save] をクリックします。**注：**また、使いやすさを向上させるために、カスタムポリシー要素を作成することもできます。

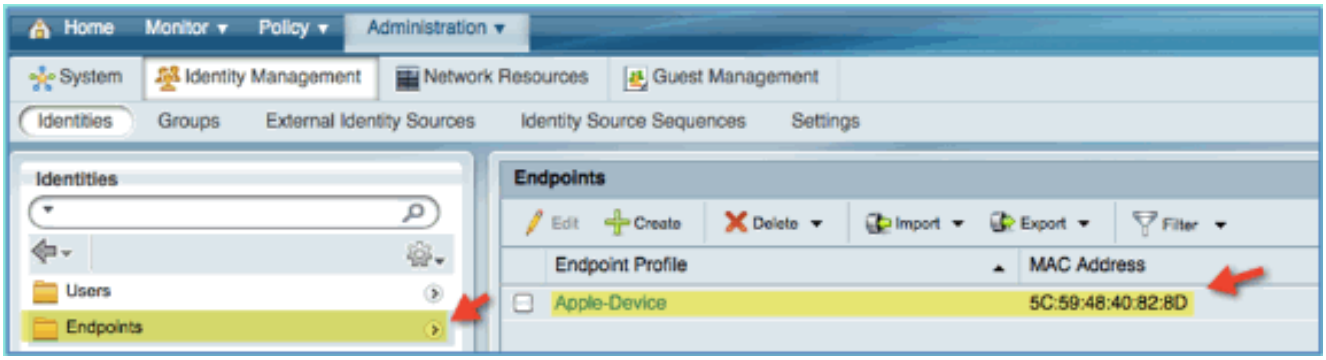
ポスチャ修復ポリシーのテスト

ISE がポスチャ ポリシーに基づいて新しいデバイスを正常にプロファイリングしていることを示すため、簡単なデモを実施できます。

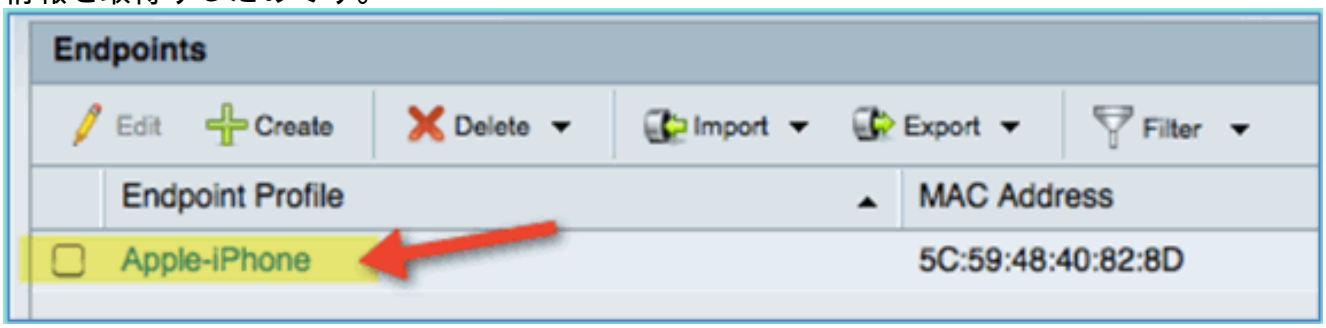
1. ISE から、**[Administration] > [Identity Management] > [Identities]** の順に移動します。



2. **[Endpoints]** をクリックします。デバイス（この例では iPhone）を関連付けて、接続します。



3. エンドポイントのリストを更新します。どの情報が入力されるか確認します。
4. エンドポイント デバイスから、次を参照してください。URL:http://www（または 10.10.10.10）デバイスがリダイレクトされます。証明書のプロンプトが表示されたら、承認します。
5. モバイル デバイスが完全にリダイレクトされたら、ISE からエンドポイント リストを再度更新します。変更内容を観察します。先ほどのエンドポイント（たとえば、Apple-Device）が 'Apple-iPhone' などに変更しているはずです。この理由は、キャプティブ ポータルにリダイレクトされるプロセスの一環として、HTTP プローブが効果的に User-Agent 情報を取得するためです。

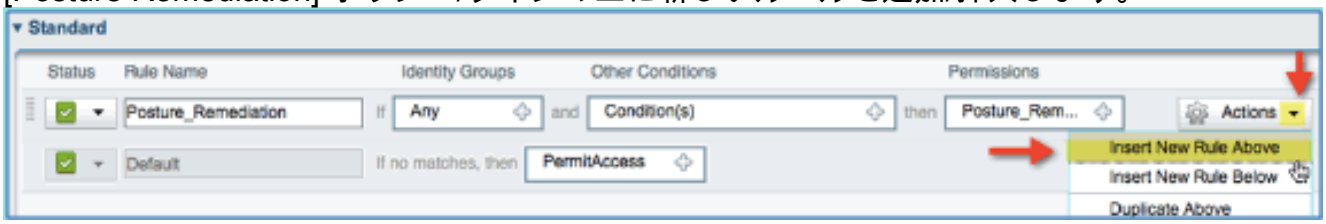


差別化アクセスの認証ポリシー

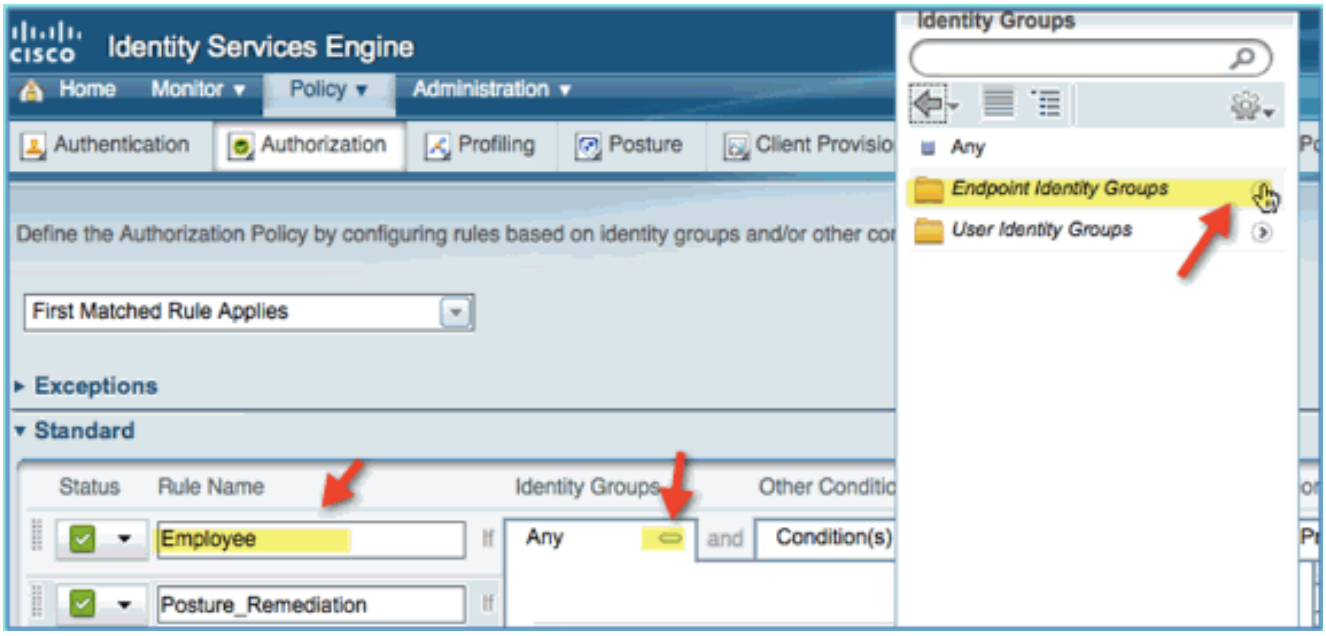
ポスチャ認証のテストが正常に終了したら、既知のデバイスおよびユーザ ロール（このシナリオでは従業員と請負業者）別の異なる VLAN の割り当てによる、従業員と請負業者の差別化アクセスをサポートするポリシーの作成を続行します。

次のステップを実行します。

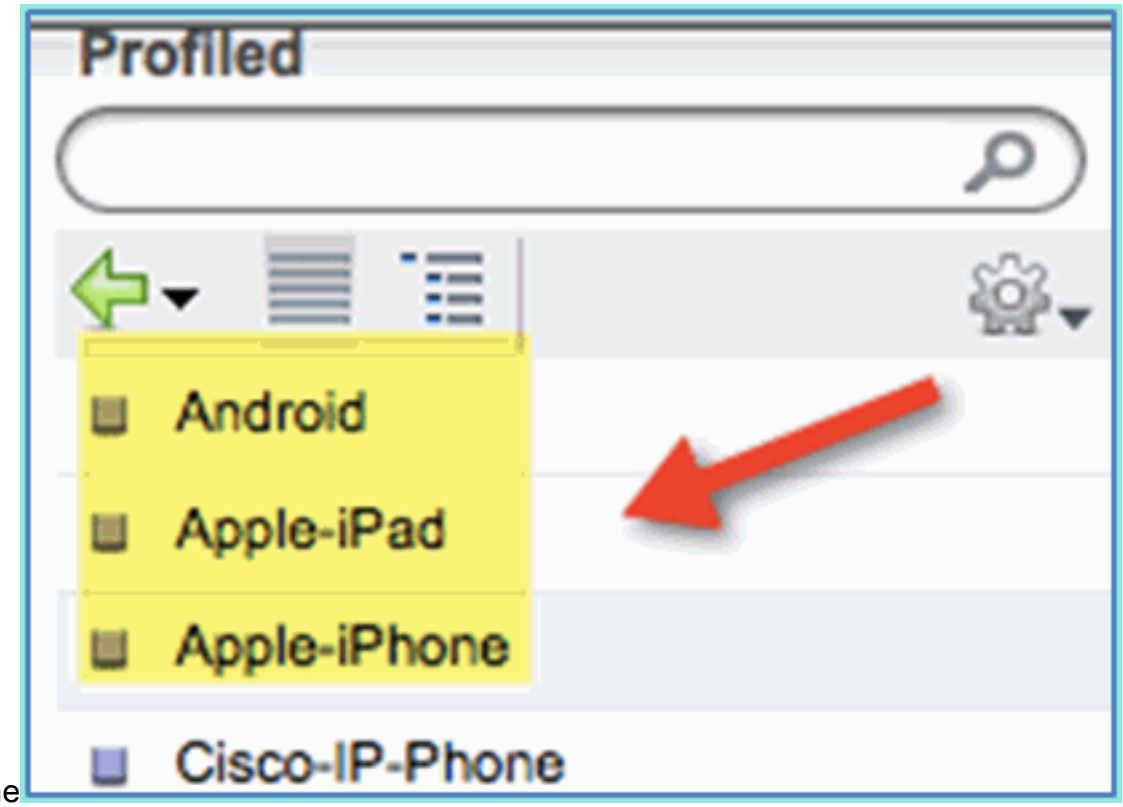
1. **[ISE] > [Policy] > [Authorization]** に移動します。
2. [Posture Remediation] ポリシー/ラインの上に新しいルールを追加/挿入します。



3. このポリシーに次の値を入力します。[Rule Name]:Employee[IDグループ(Identity Groups)]（展開）:[エンドポイントIDグループ(Endpoint Identity Groups)]

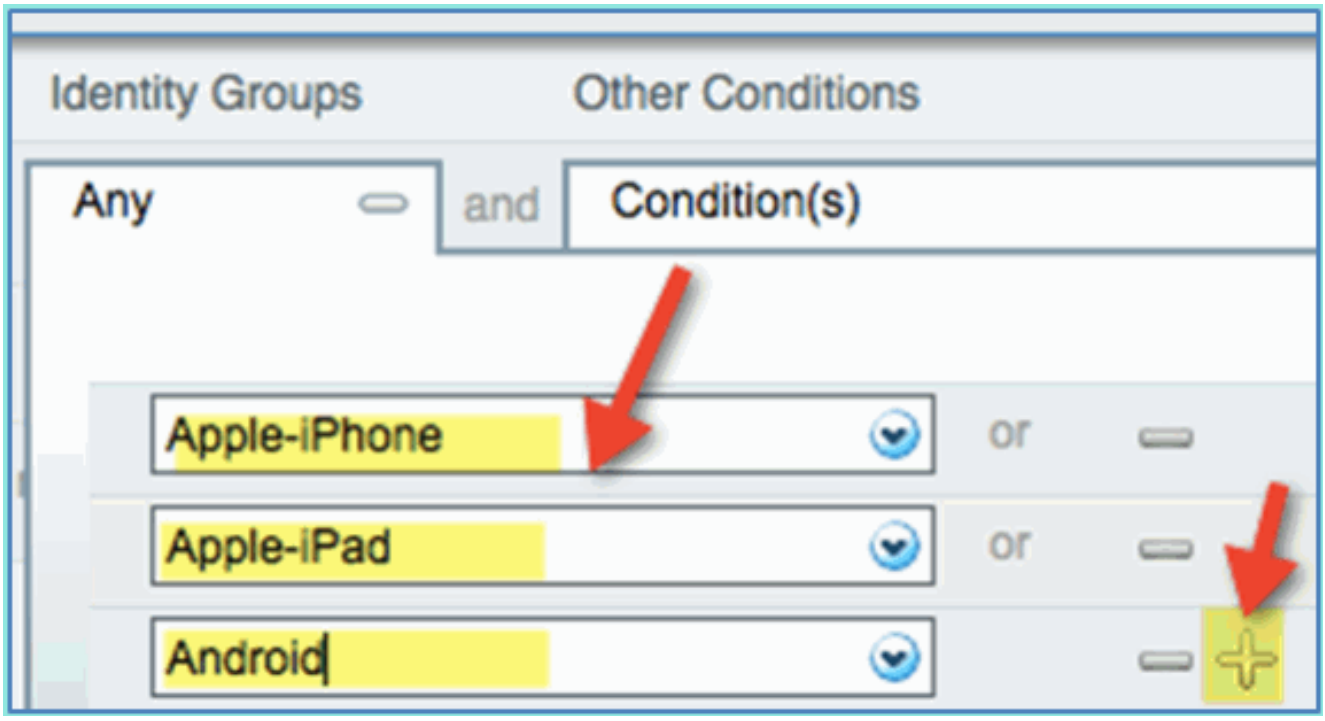


エンドポイントIDグループ：プロファイル済みプロファイル：Android、Apple-iPad、またはApple-

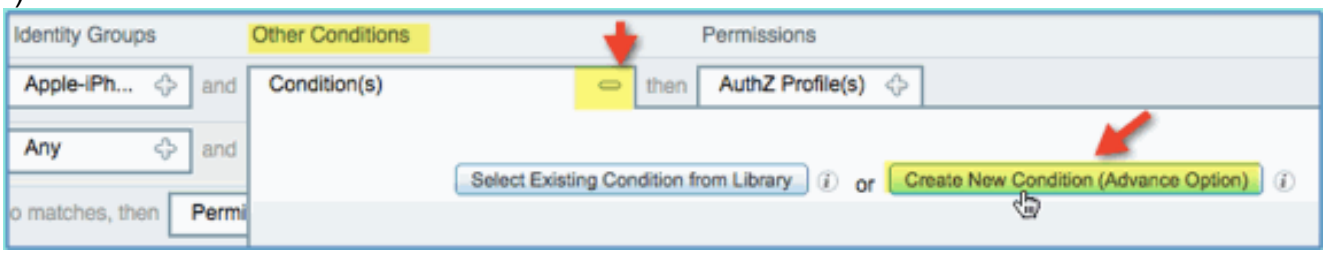


iPhone

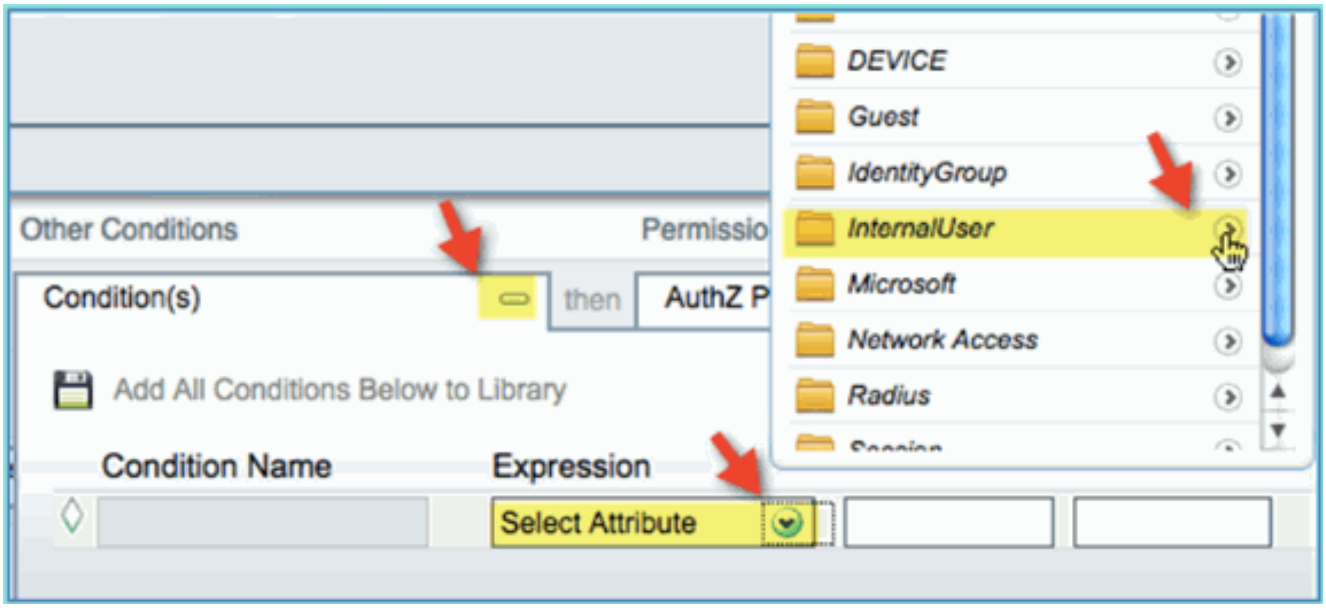
4. 追加のデバイス タイプを指定するには、**[+] をクリックしてより多くのデバイスを追加します（必要に応じて）。**エンドポイントIDグループ：プロファイル済みプロファイル：Android、Apple-iPad、またはApple-iPhone



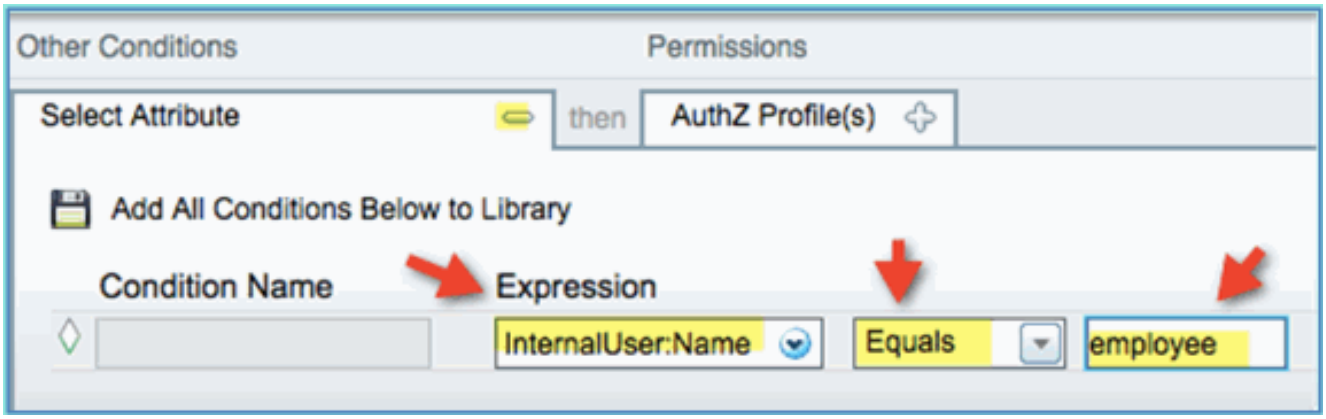
5. このポリシーの次のアクセス許可の値を入力します。その他の条件（展開）：新しい条件の作成（詳細オプション
）



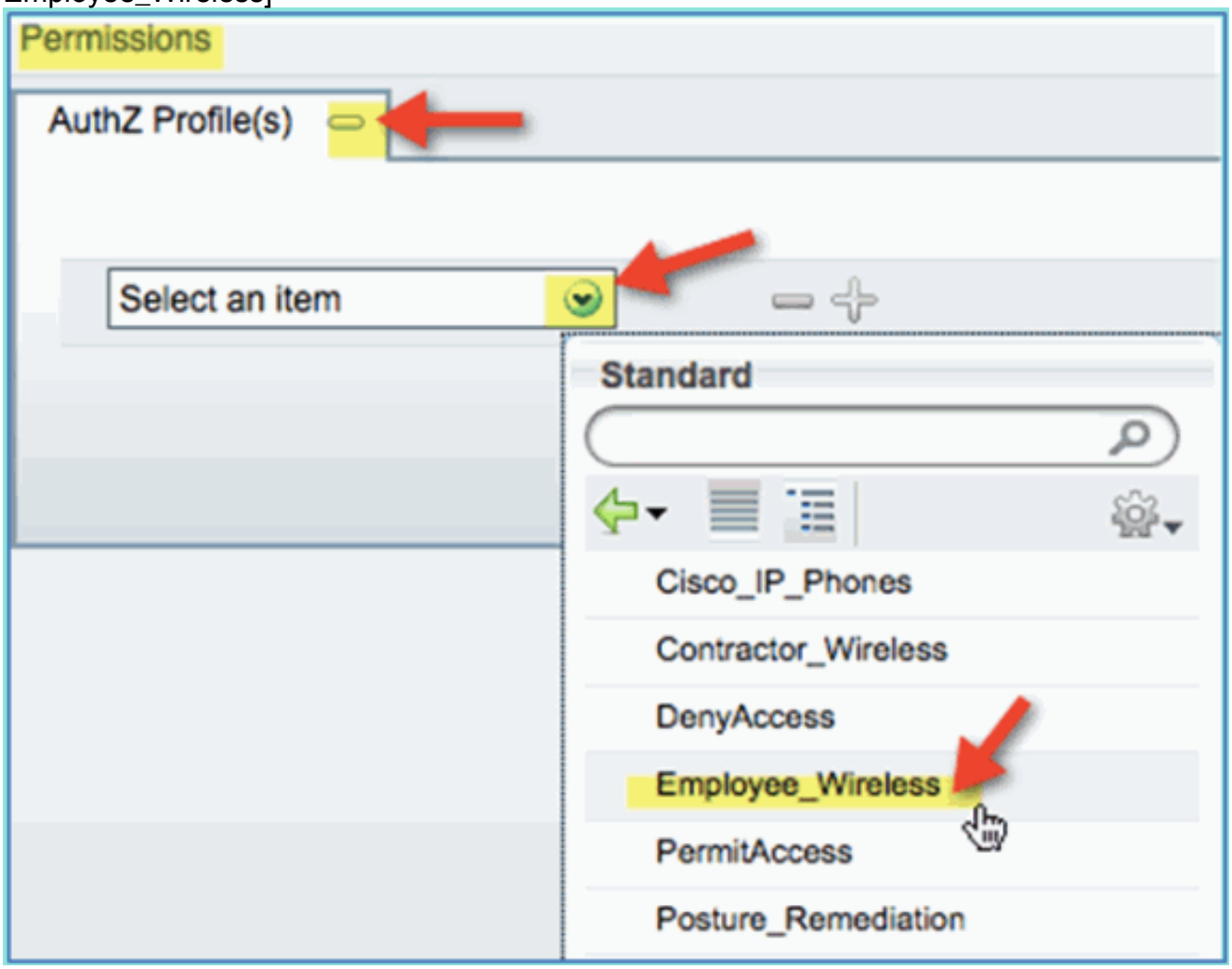
条件>式（リストから）: InternalUser >
Name



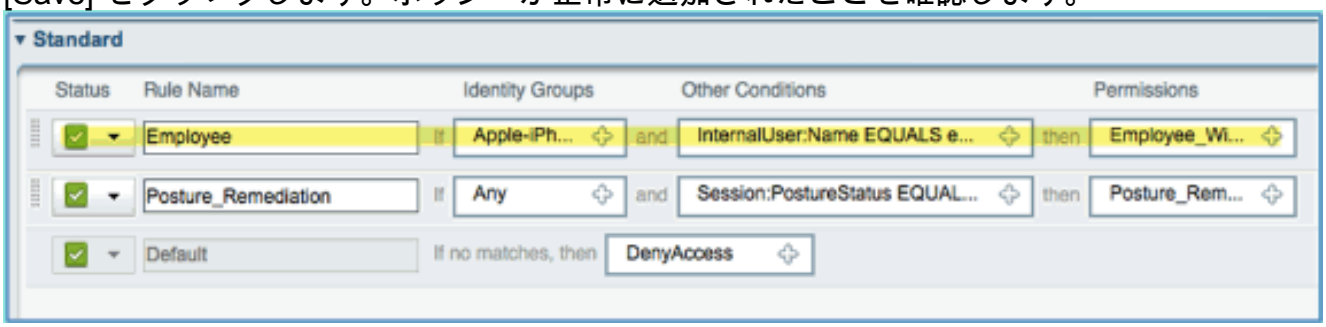
InternalUser > Name:
employee



6. ポスチャ セッションのコンプライアンス条件を追加する：[Permissions] > [Profiles] > [Standard:
Employee_Wireless]

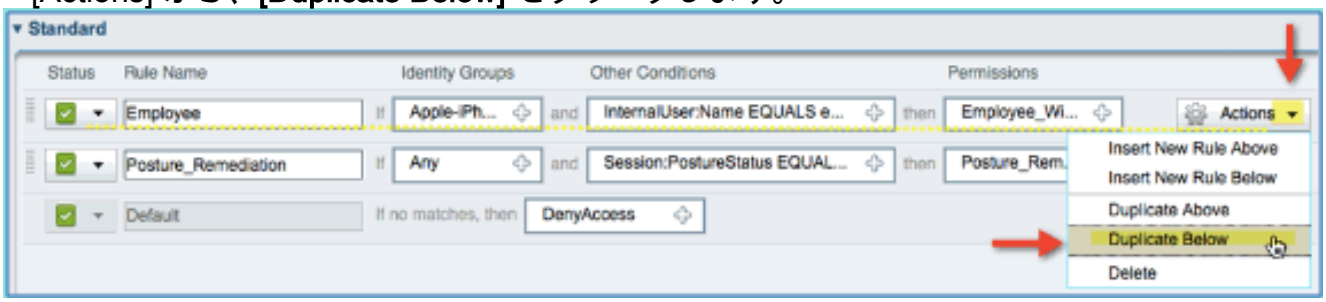


7. [Save] をクリックします。ポリシーが正常に追加されたことを確認します。

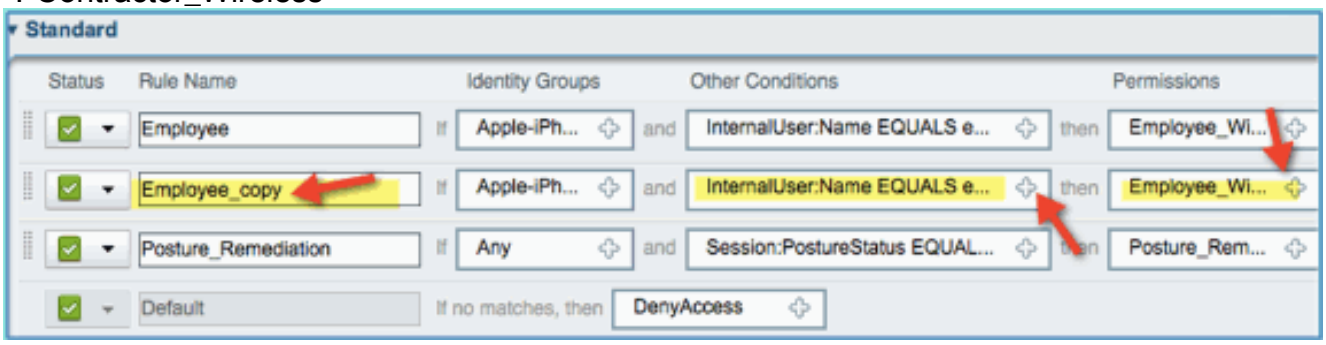


8. 引き続き請負業者ポリシーを追加します。このドキュメントでは、プロセスを迅速に進めるため、ポリシーを複製します（または手動で設定することもできます）。[Employee policy]

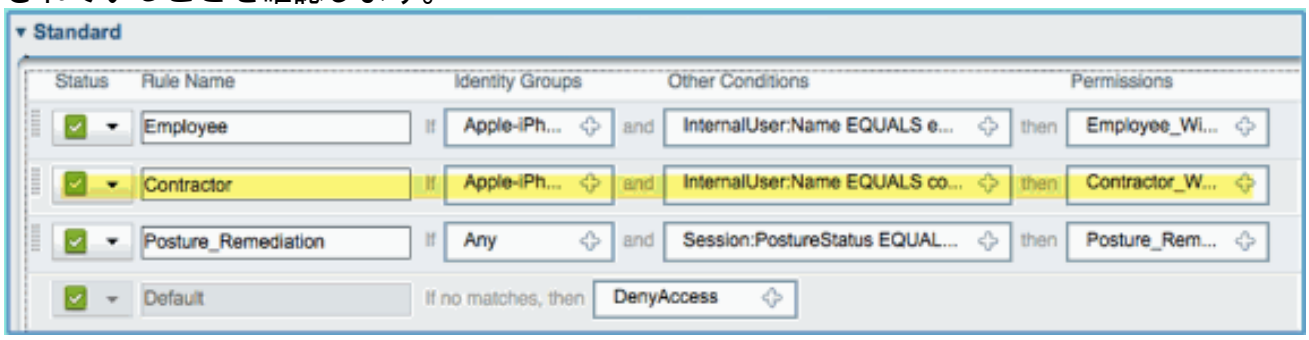
> [Actions] から、**[Duplicate Below]** をクリックします。



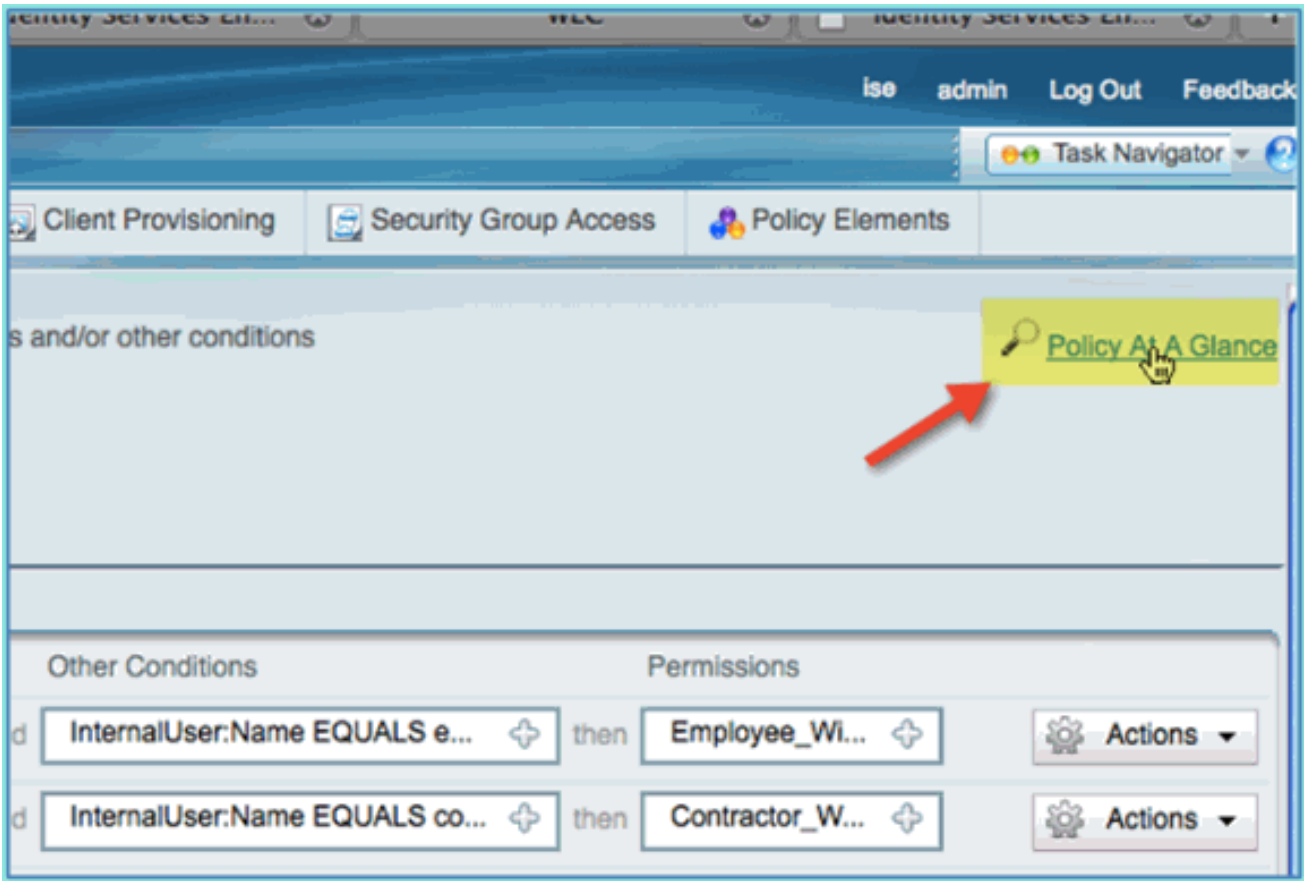
9. このポリシー（複製コピー）の次のフィールドを編集します。[Rule Name（ルール名）]:Contractor[その他の条件(Other Conditions)] > [内部ユーザ(InternalUser)] > [名前(Name)]:contractor権限
：Contractor_Wireless



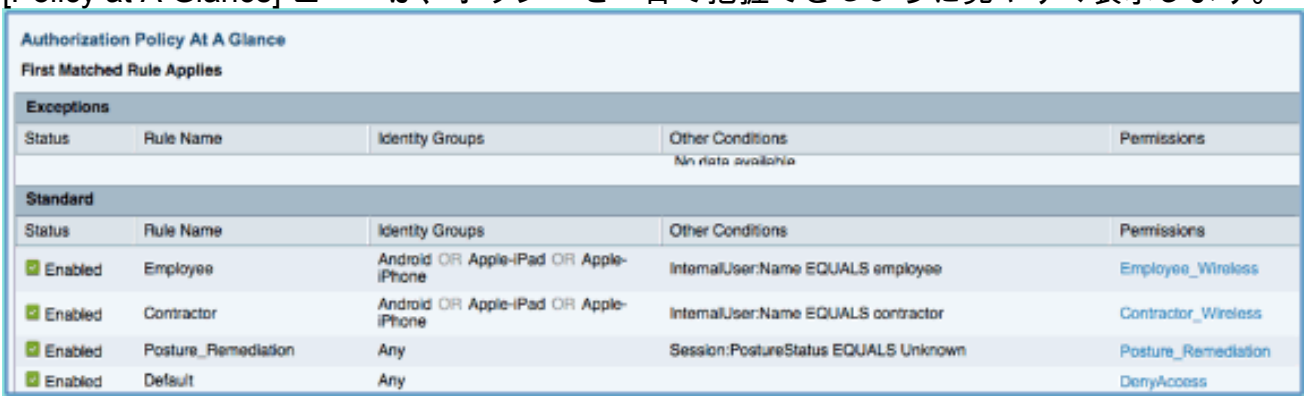
10. [Save] をクリックします。先ほどの複製したコピー（または新規ポリシー）が正しく設定されていることを確認します。



11. ポリシーをプレビューするには、[Policy-at-a-Glance] をクリックします。



[Policy at A Glance] ビューは、ポリシーを一目で把握できるように見やすく表示します。



Authorization Policy At A Glance

First Matched Rule Applies

Exceptions

Status	Rule Name	Identity Groups	Other Conditions	Permissions
			No data available	

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Employee	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS employee	Employee_Wireless
Enabled	Contractor	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS contractor	Contractor_Wireless
Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
Enabled	Default	Any		DenyAccess

差別化アクセスのための CoA のテスト

認証プロファイルおよびポリシーで差別化アクセスの準備ができたら、テストを行います。単一の保護された WLAN では、従業員には従業員 VLAN が割り当てられ、請負業者には請負業者 VLAN が割り当てられます。次の例では 1 台の Apple iPhone/iPad を使用します。

次のステップを実行します。

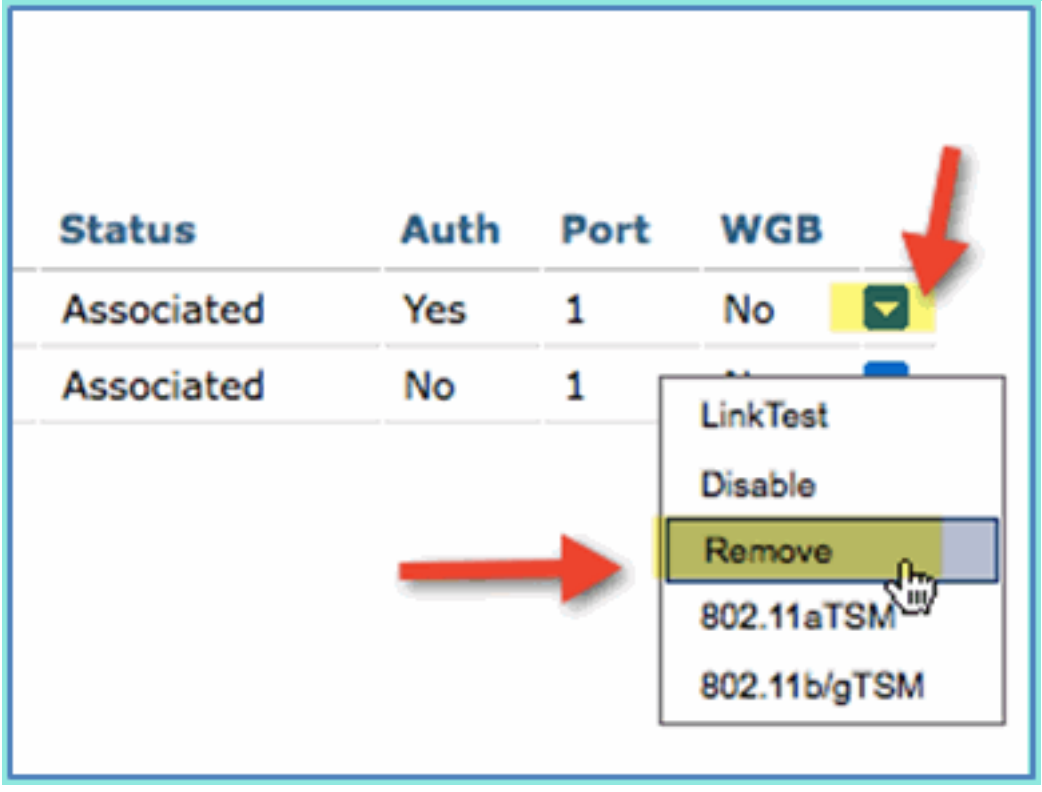
1. 保護された WLAN（POD1x）にモバイル デバイスを接続し、次のクレデンシャルを使用します。ユーザ名：employeeパスワード
   ：XXXXX

2. [Join] をクリックします。従業員に VLAN 11（従業員 VLAN）が割り当てられたことを確認します。

3. [Forget this Network] をクリックします。[Forget] をクリックして確定します。

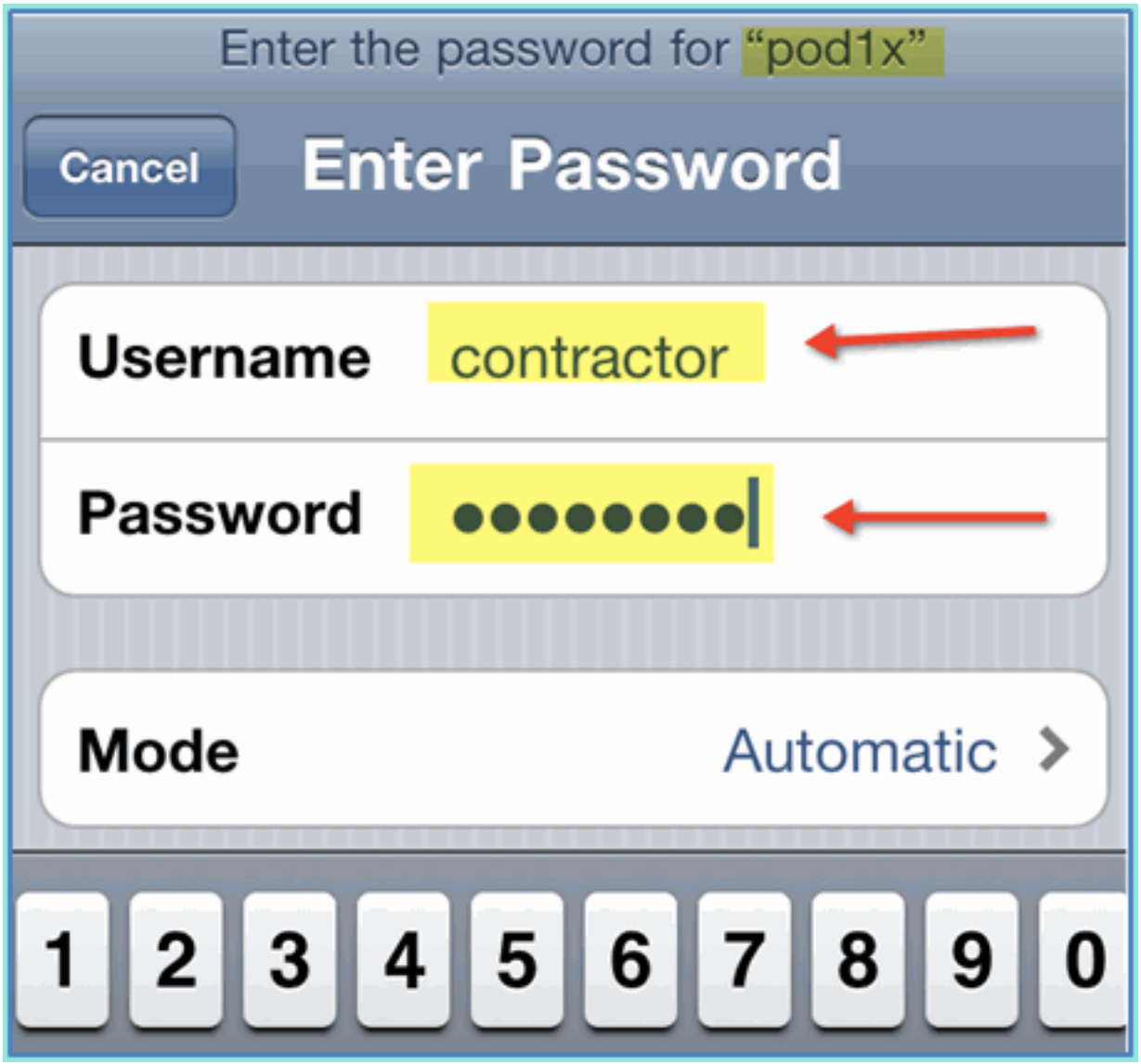
4. WLC に移動し、既存のクライアント接続を削除します（前の手順で同じものが使用されている場合）。[Monitor] > [Clients] > [MAC address] に移動し、[Remove] をクリックします。


CISCO
MONITOR
WLANs
Monitor
Clients
Summary
Current Filter
Access Points
Cisco CleanAir
Client MAC Addr
Statistics
44:2a:60:f7:3a:4a
CDP
5c:59:48:40:82:8d
Rogues
Clients
Multicast


Status
Auth
Port
WGB
Associated
Yes
1
No
Associated
No
1
LinkTest
Disable
Remove
802.11aTSM
802.11b/gTSM

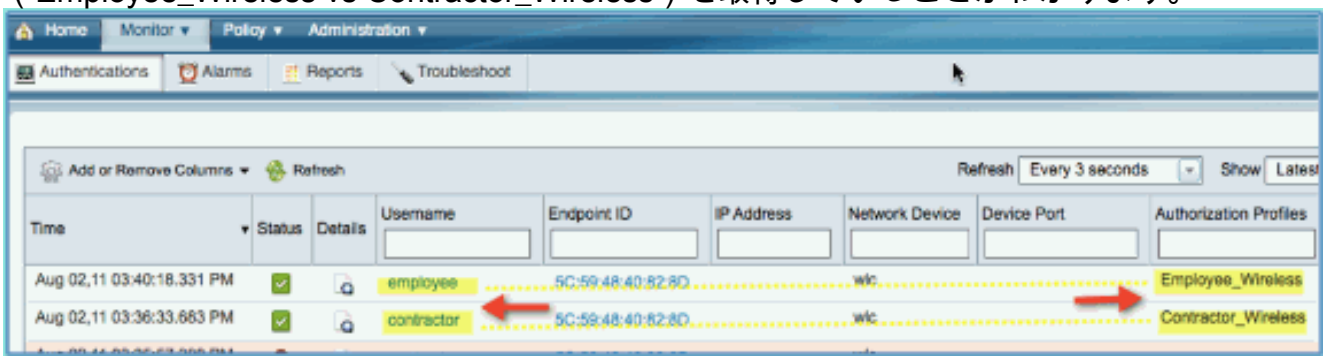
5. 前のクライアント セッションをクリアするもう 1 つの確実な方法は、WLAN を無効化してから有効にすることです。[WLC] > [WLANs] > [WLAN] に移動し、編集する WLAN をクリックします。[Enabled] > [Apply] **のチェックを外します（無効化する）。**[Enabled] > [Apply] **のチェックボックスをオンにします（再度有効化する）。**

6. モバイル デバイスに戻ります。次のクレデンシャルを使用して、同じ WLAN に再度接続します。ユーザ名：contractorパスワード
：XXXX



7. [Join] をクリックします。請負業者のユーザに VLAN 12 (請負業者/ゲスト VLAN) が割り当てられたことを確認します。

8. ISE のリアルタイムのログ ビューは [ISE] > [Monitor] > [Authorizations] で確認できます。個々のユーザ（従業員、請負業者）が、異なる VLAN で差別化された認証プロファイル（Employee_Wireless vs Contractor_Wireless）を取得していることがわかります。



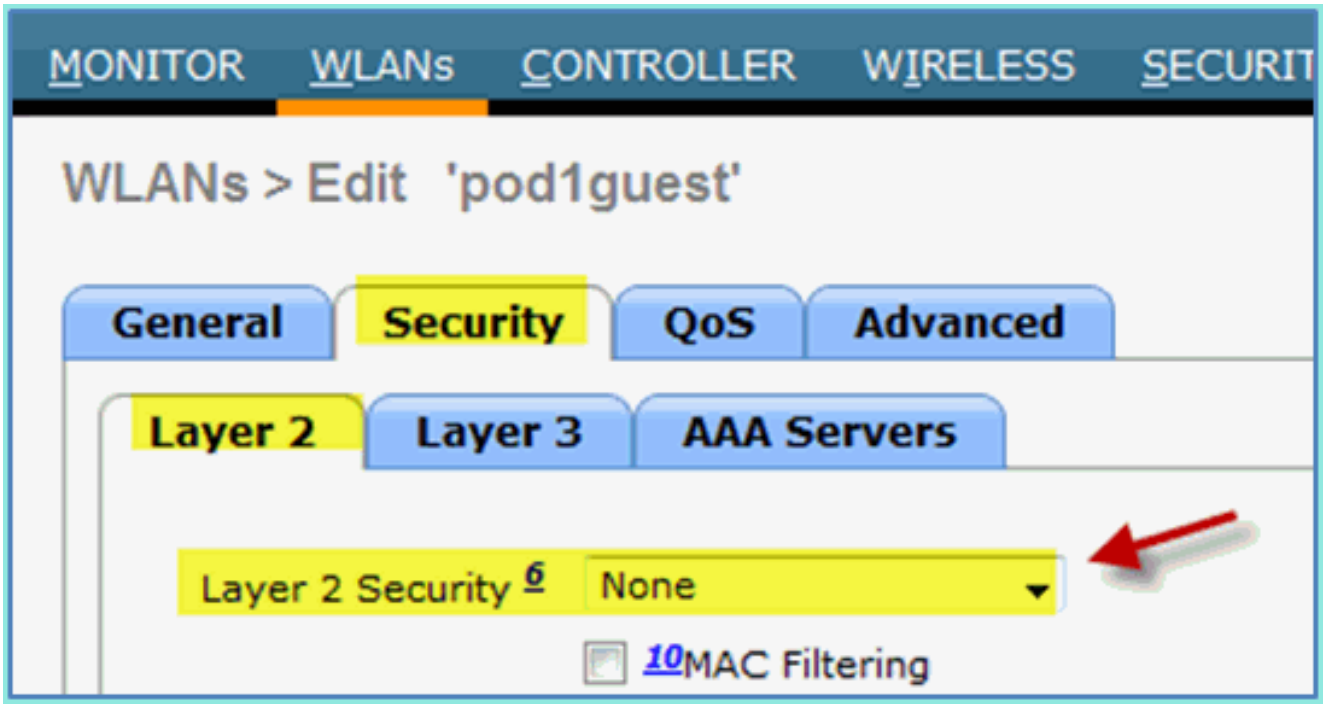
WLC のゲスト WLAN

ゲスト WLAN を追加し、ゲストが ISE スポンサー ゲスト ポータルにアクセスできるようにするには、次の手順を実行します。

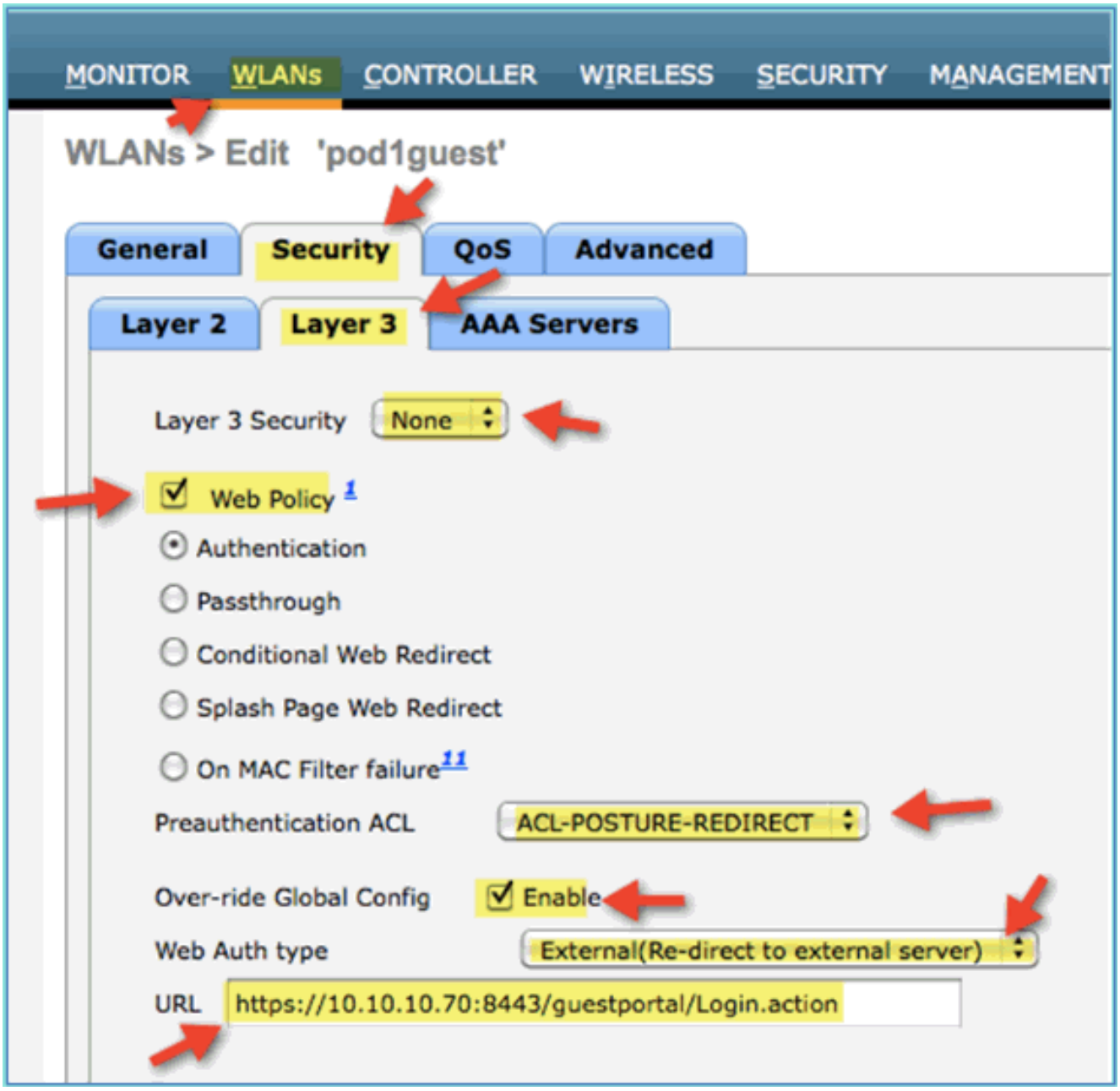
1. WLC から [WLANs] > [WLANs] > [Add New] に移動します。
2. 新しいゲスト WLAN に次を入力します。[Profile Name (プロファイル名)]:pod1guestSSID:pod1guest

3. [Apply] をクリックします。
4. ゲスト WLAN > [General] タブに次を入力します。ステータス：無効[Interface/Interface Group]:Guest

5. [WLAN] > [Security] > [Layer2] **に移動し、次を入力します。**レイヤ2セキュリティ：なし



6. [WLAN] > [Security] > [Layer3] **タブに移動し、次を入力します。**レイヤ3セキュリティ：なしWebポリシー：有効[Web Policy]サブ値：認証事前認証ACL:ACL-POSTURE-REDIRECTWeb認証タイプ：外部（外部サーバにリダイレクト）URL:https://10.10.10.70:8443/guestportal/Login.action



7. [Apply] をクリックします。
8. WLC 設定を保存したことを確認します。

ゲスト WLAN とゲスト ポータルのテスト

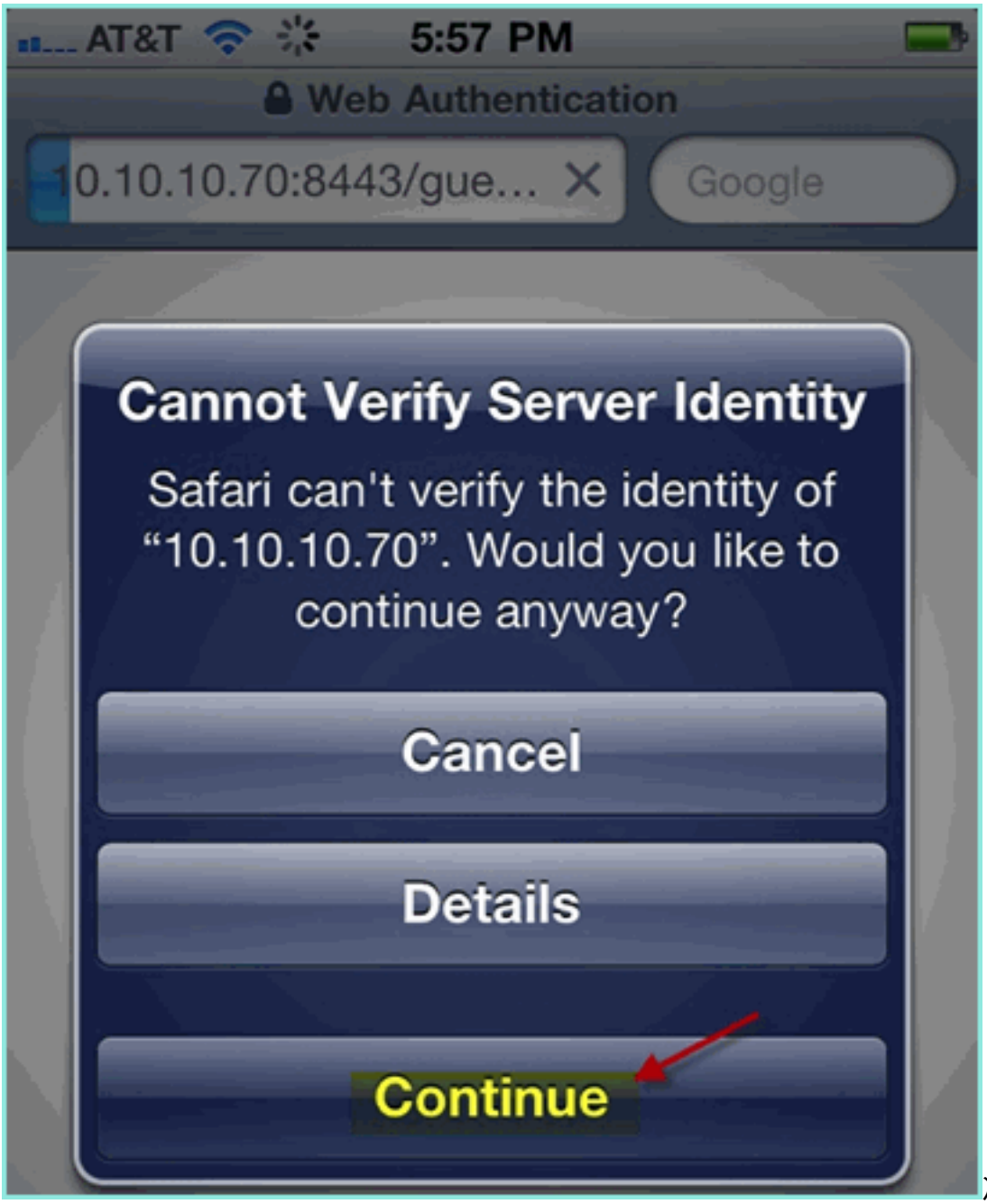
これで、ゲスト WLAN の設定をテストできるようになりました。ゲストは ISE のゲスト ポータルにリダイレクトされるはずです。

次のステップを実行します。

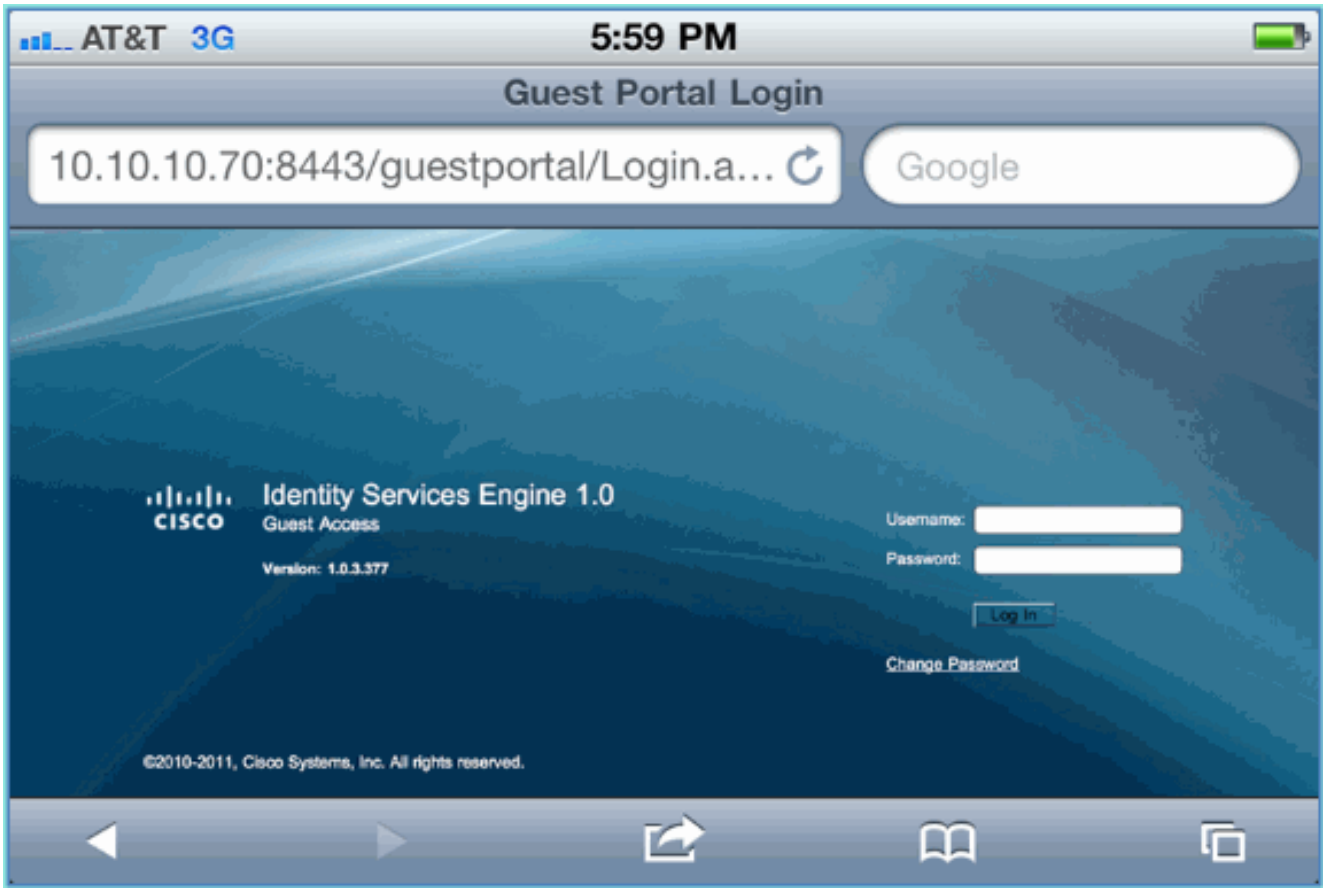
1. iPhone などの iOS デバイスから、[Wi-Fi Networks] > [Enable] に移動します。次に、POD ゲスト ネットワークを選択します。

2. iOS デバイスは、ゲスト VLAN（10.10.12.0/24）からの有効な IP アドレスを示している必要があります。

3. Safari ブラウザを開いて次の URL に接続します。URL:http://10.10.10.10Web 認証のリダイレクトが表示されます。
4. ISE ゲスト ポータル ページに到達するまで、[Continue] をクリックします。



次のサンプル スクリーンショットは、[Guest Portal Login] での iOS デバイスを示します。ここから、WLAN と ISE のゲスト ポータルの正しい設定が有効であることが確認できます。

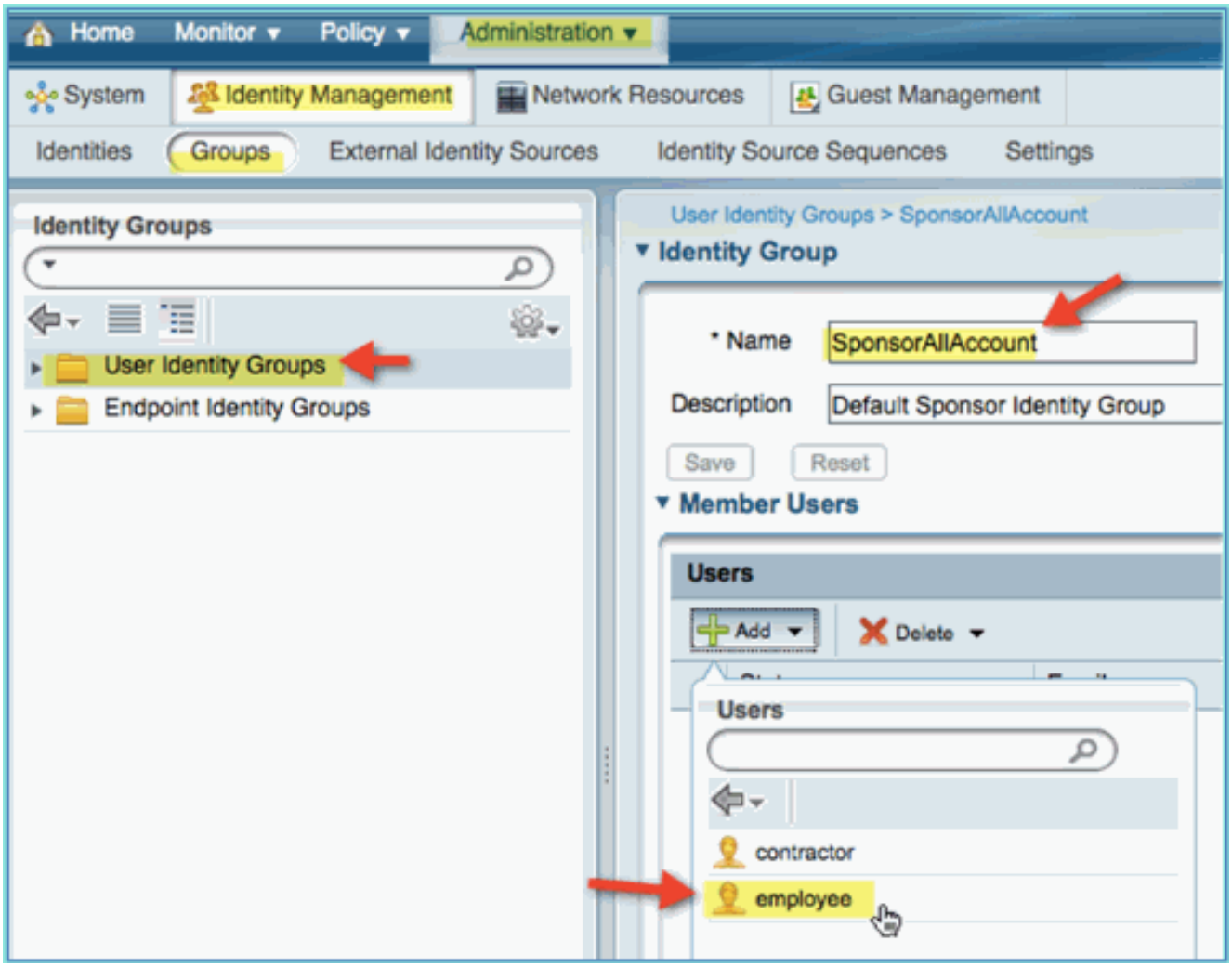


ISE ワイヤレス スポンサード ゲスト アクセス

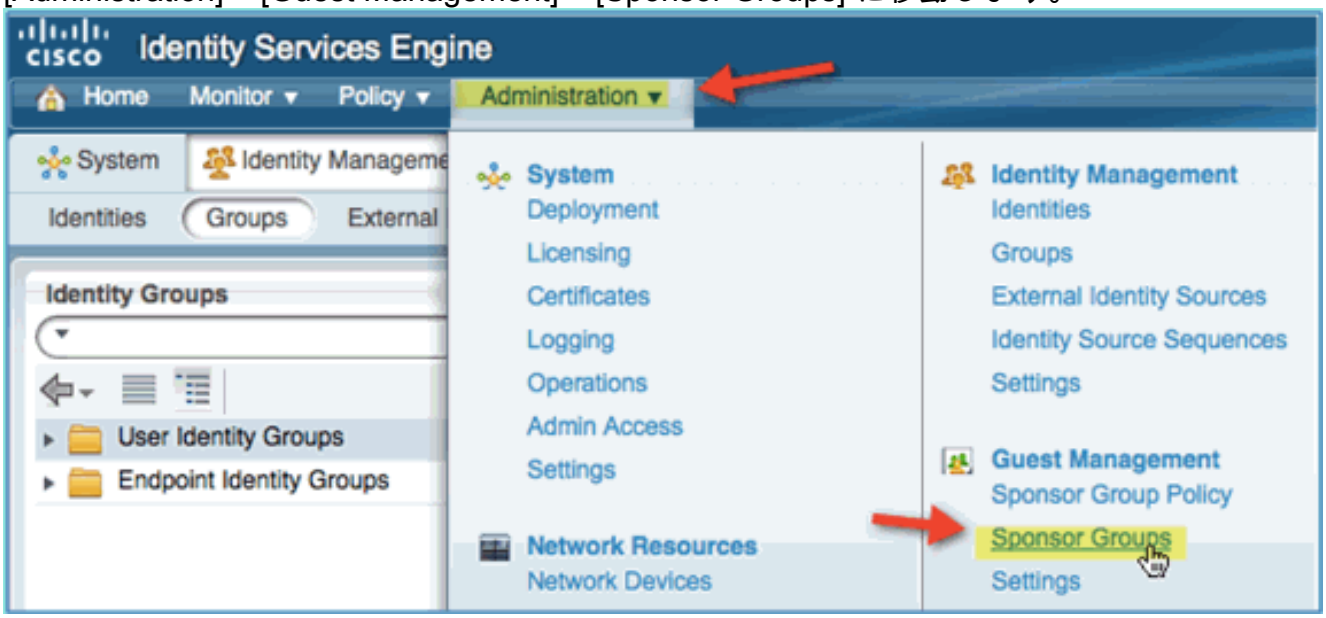
ISE はゲストのスポンサーとなることができるように設定できます。この場合、内部または AD ドメイン（統合されている場合）ユーザがゲスト アクセスのスポンサーとなれるように、ISE ゲスト ポリシーを設定することになります。また、スポンサーがゲスト パスワードを閲覧（オプション、このラボで有益）できるように ISE を設定することもできます。

次のステップを実行します。

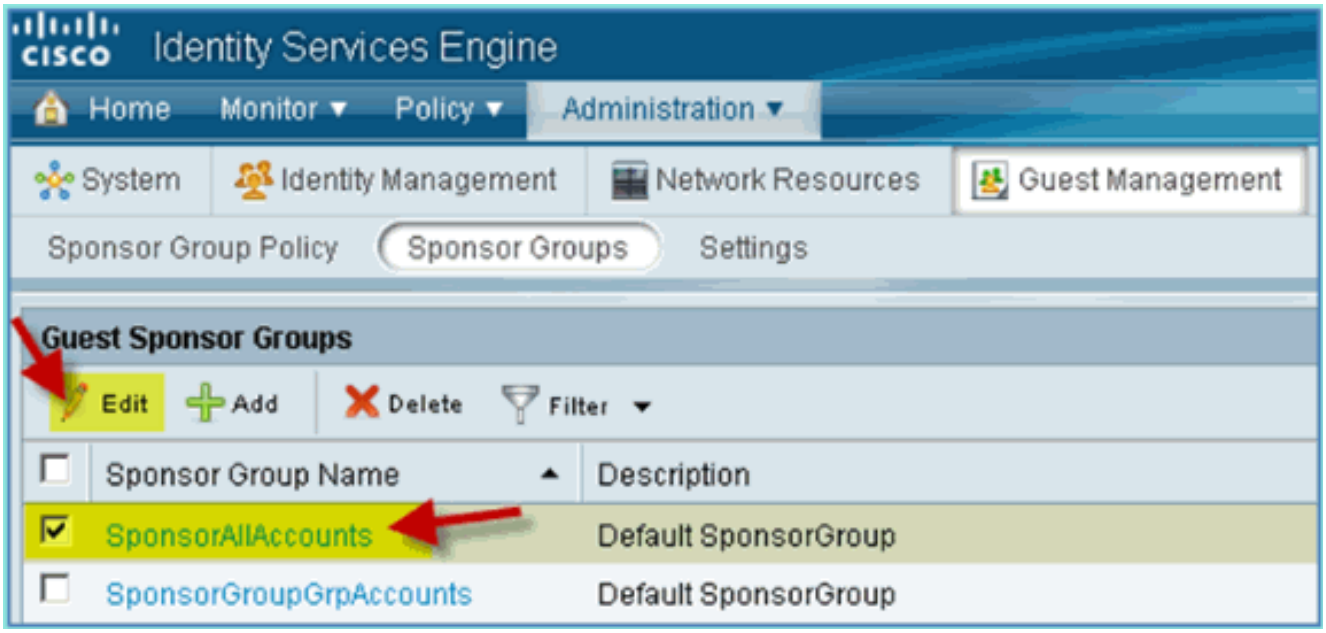
1. 従業員ユーザを SponsorAllAccount グループに追加します。これを行うには、グループに直接移動する方法と、ユーザを編集してグループを割り当てる方法とがあります。この例では、[Administration] > [Identity Management] > [Groups] > [User Identity Groups] に移動します。次に、[SponsorAllAccount] **をクリックして従業員ユーザを追加します。**



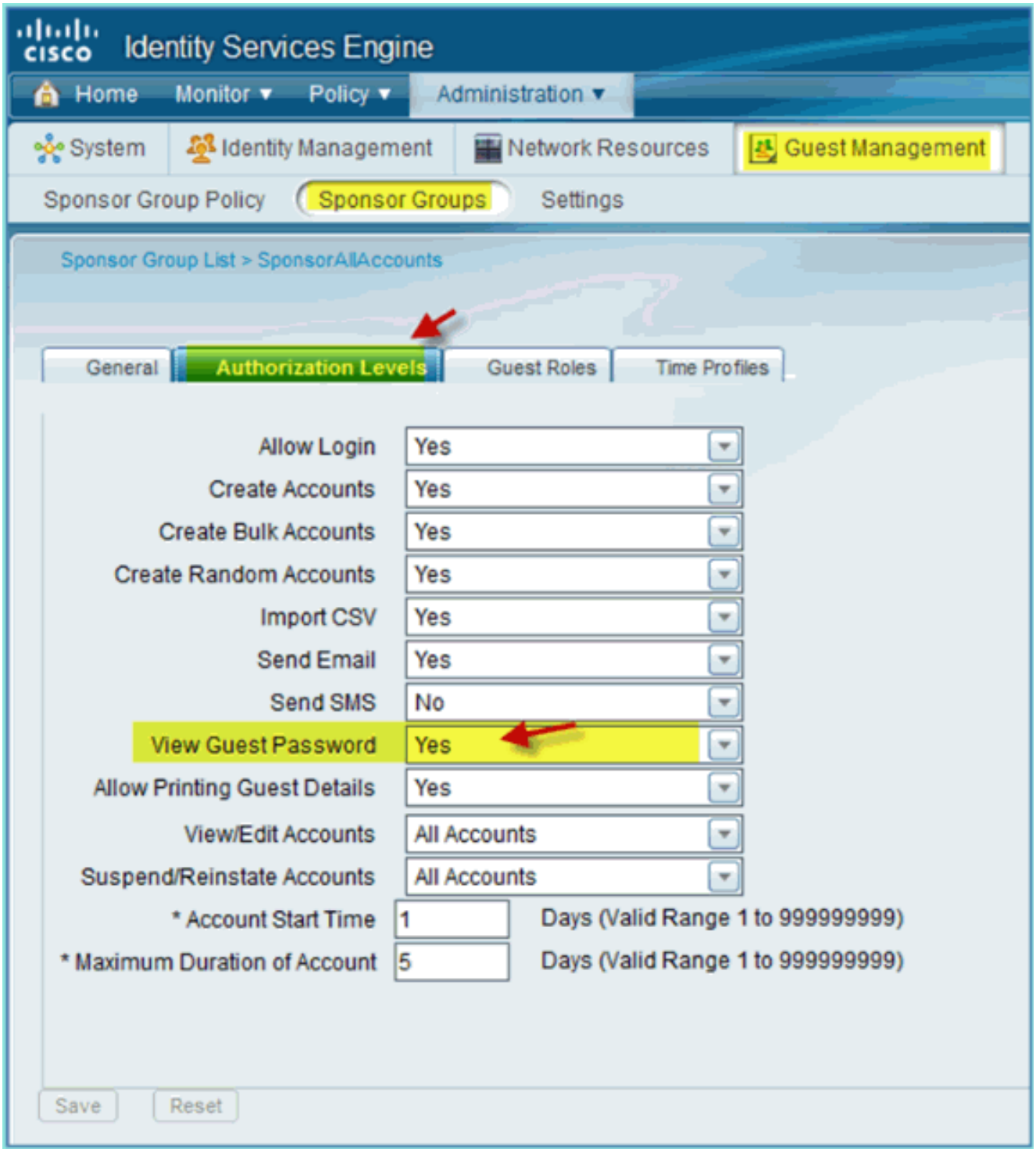
2. [Administration] > [Guest Management] > [Sponsor Groups] に移動します。



3. [Edit] をクリックして、[SponsorAllAccounts] を選択します。



4. [Authorization Levels] を選択し、次のように設定します。ゲストパスワードの表示：はい



5. [Save] をクリックして、この作業を完了します。

ゲストのスポンサー

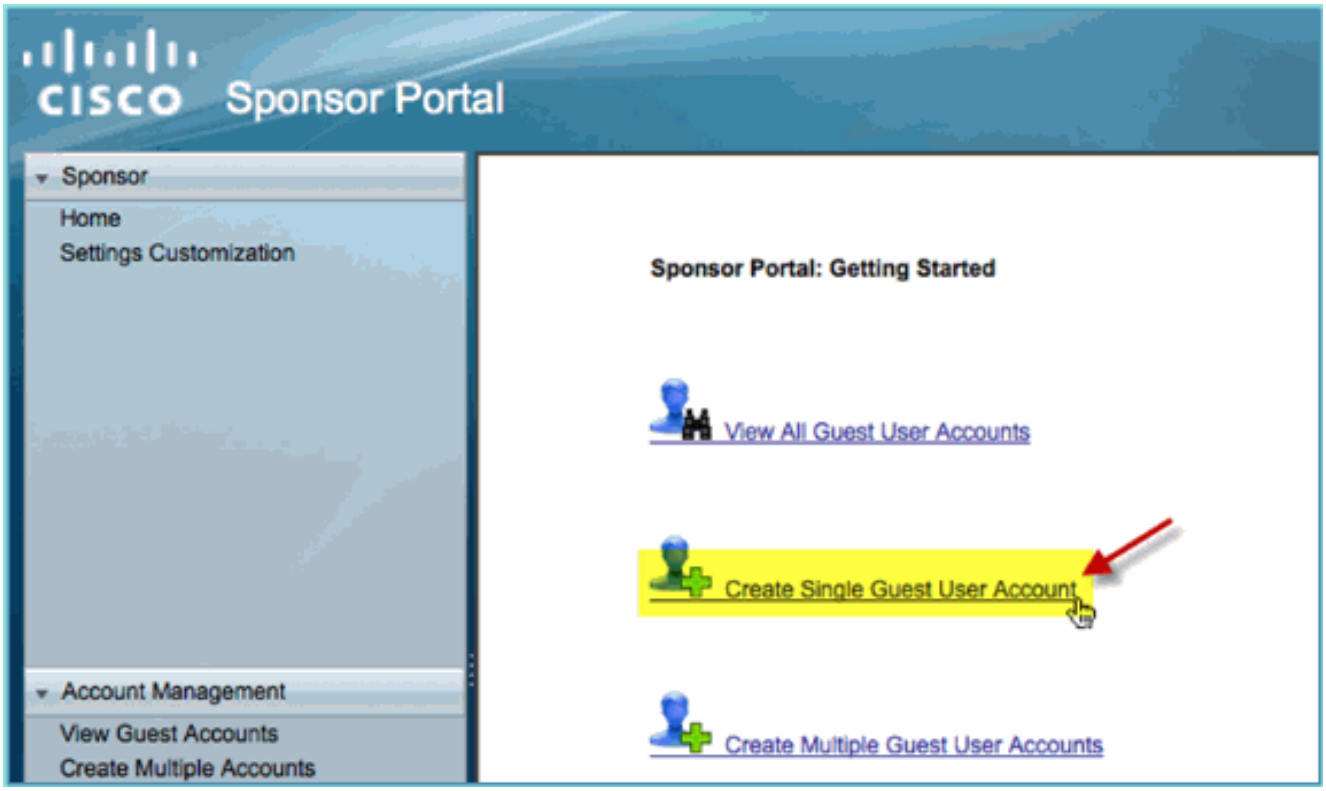
先ほど、適切なゲスト ポリシーとグループを設定して AD ドメインのユーザが一時的なゲストのスポンサーとなることを許可しました。次に、スポンサー ポータルにアクセスし、一時的なゲスト アクセスを作成します。

次のステップを実行します。

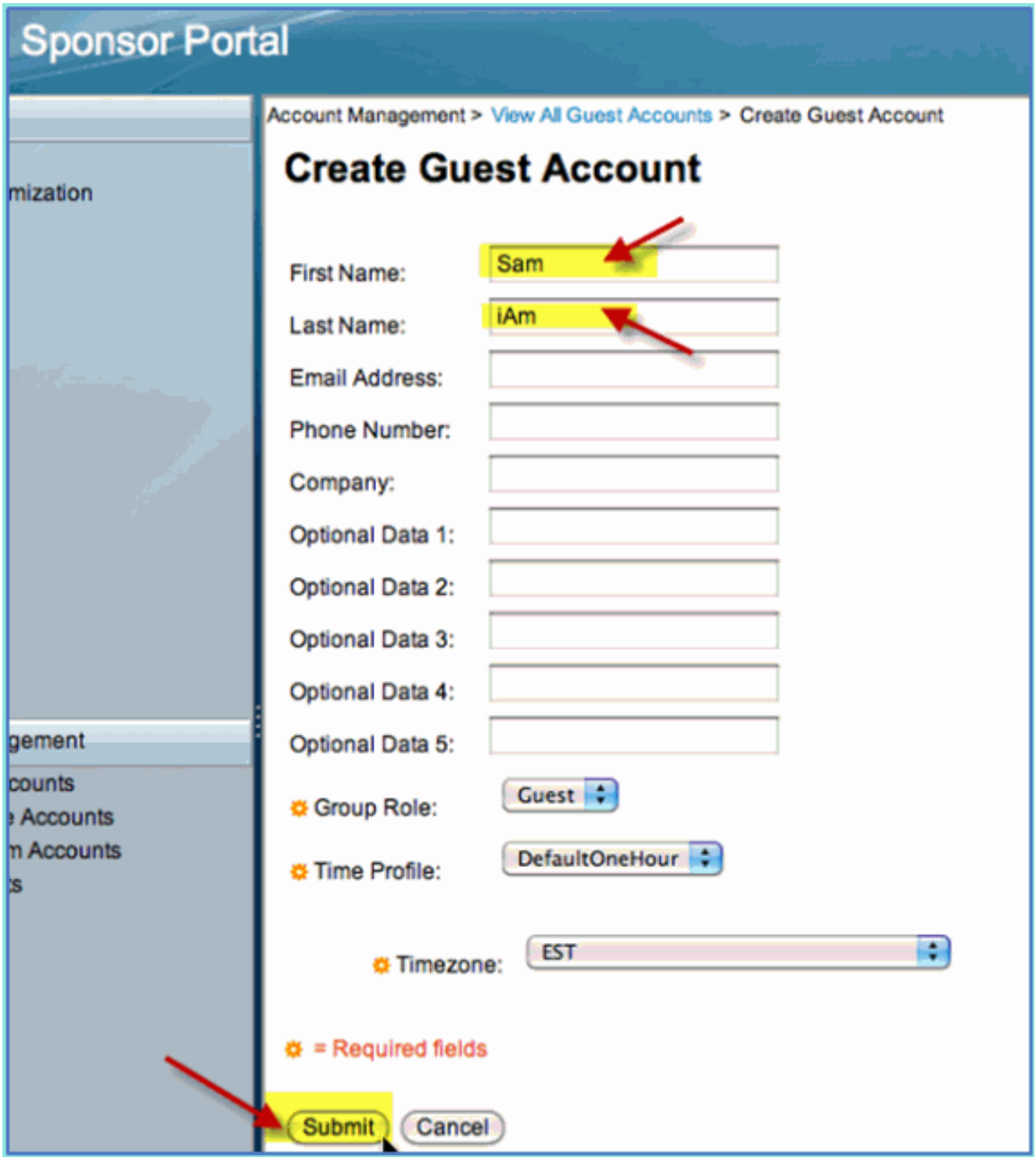
1. ブラウザから、http://<ise ip>:8080/sponsorportal/**または**https://<ise ip>:8443/sponsorportal/のいずれかのURLに移動します。その後、次の情報を使用してログインします。ユーザ名：aduser(Active Directory)、employee（内部ユーザ）パスワード

: XXXX

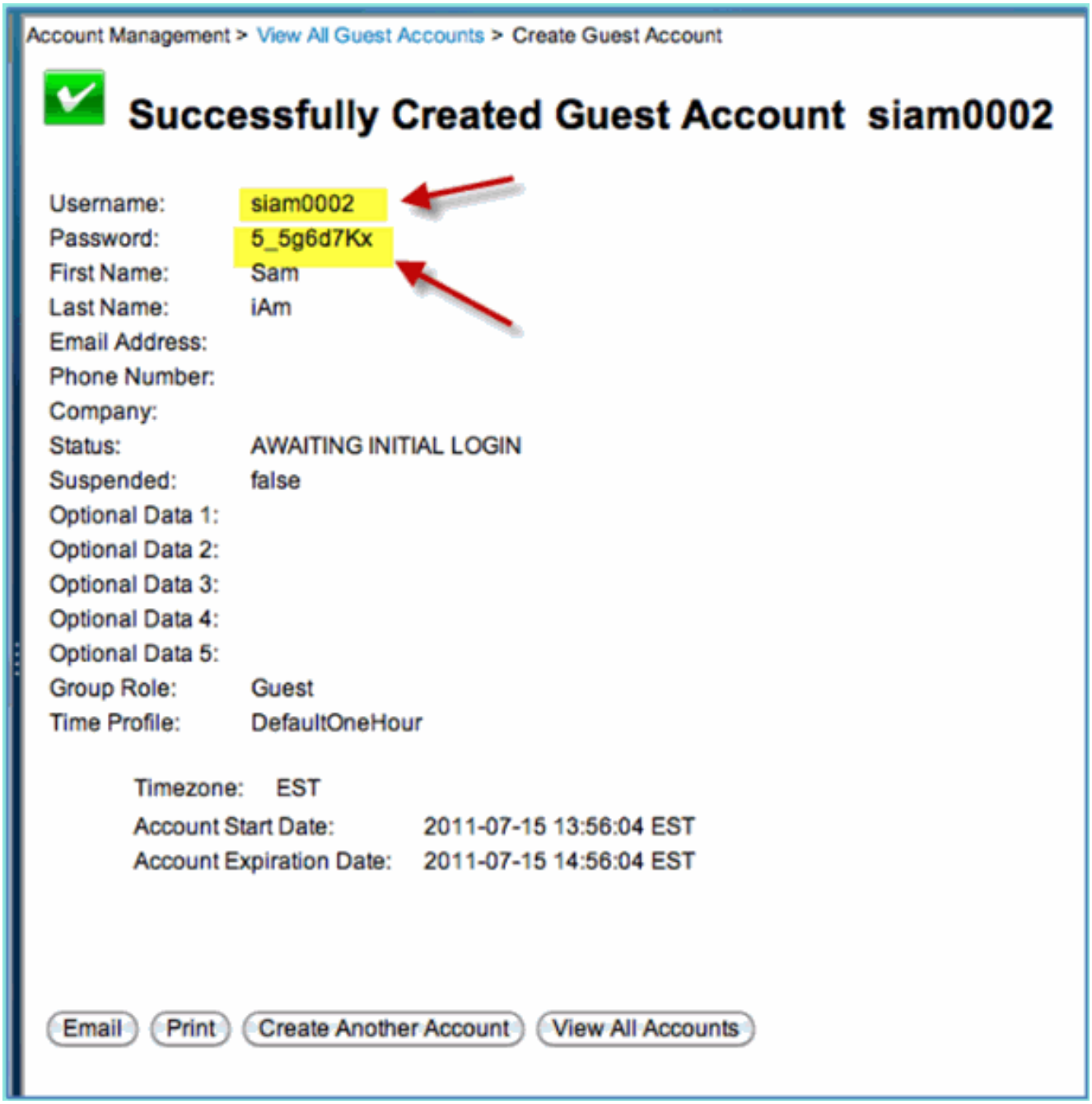
2. [Sponsor] ページから、[Create Single Guest User Account] をクリックします。



3. 一時的なゲストに、次の情報を追加します。名：必須（Samなど）姓：必須（例：Jones）[Group Role]:Guest時間プロファイル： DefaultOneHour[Time Zone（タイムゾーン）]:Any/Default



4. [Submit] をクリックします。
5. ゲスト アカウントが先ほどのエントリに基づいて作成されます。パスワードはハッシュ *** ではなく表示される（先ほどの演習から）ことに注意してください。
6. このウィンドウは閉じず、ゲストのユーザ名とパスワードを表示させておきます。このページはゲスト ポータルへのログインをテストするために使用します（次へ）。



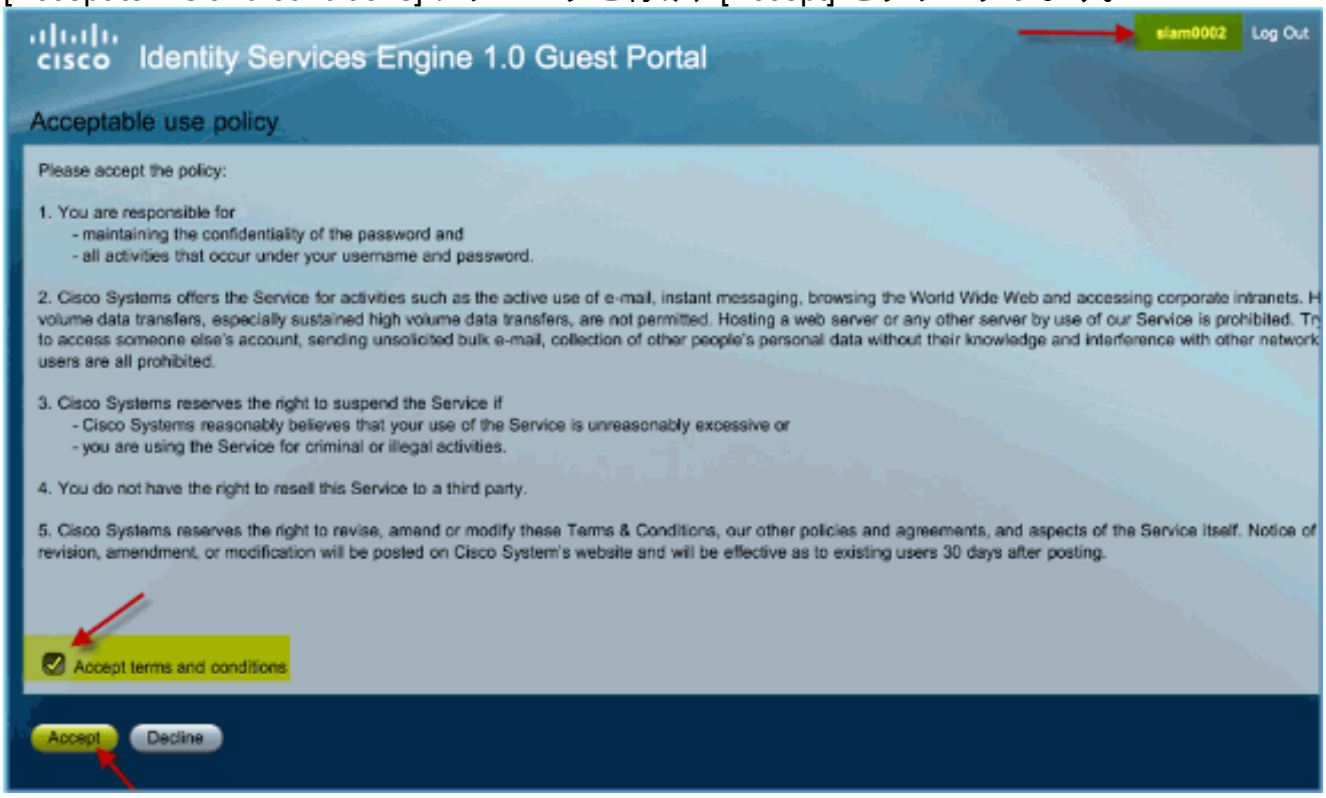
ゲスト ポータル アクセスのテスト

AD ユーザ/スポンサーによって新しいゲスト アカウントが作成されたら、ゲスト ポータルとアクセスをテストできます。

次のステップを実行します。

1. 優先デバイス (この場合は Apple iOS/iPad) で、ポッド ゲスト SSID に接続し、IP アドレス/接続製を確認します。
2. ブラウザを使用して、http://www への移動を試みます。ゲスト ポータルのログイン ページにリダイレクトされます。

3. 先ほどの演習で作成したゲスト アカウントを使用してログインします。成功すると、アクセプタブル ユース ポリシー ページが表示されます。
4. [Accept terms and conditions] にチェックを付け、[Accept] をクリックします。



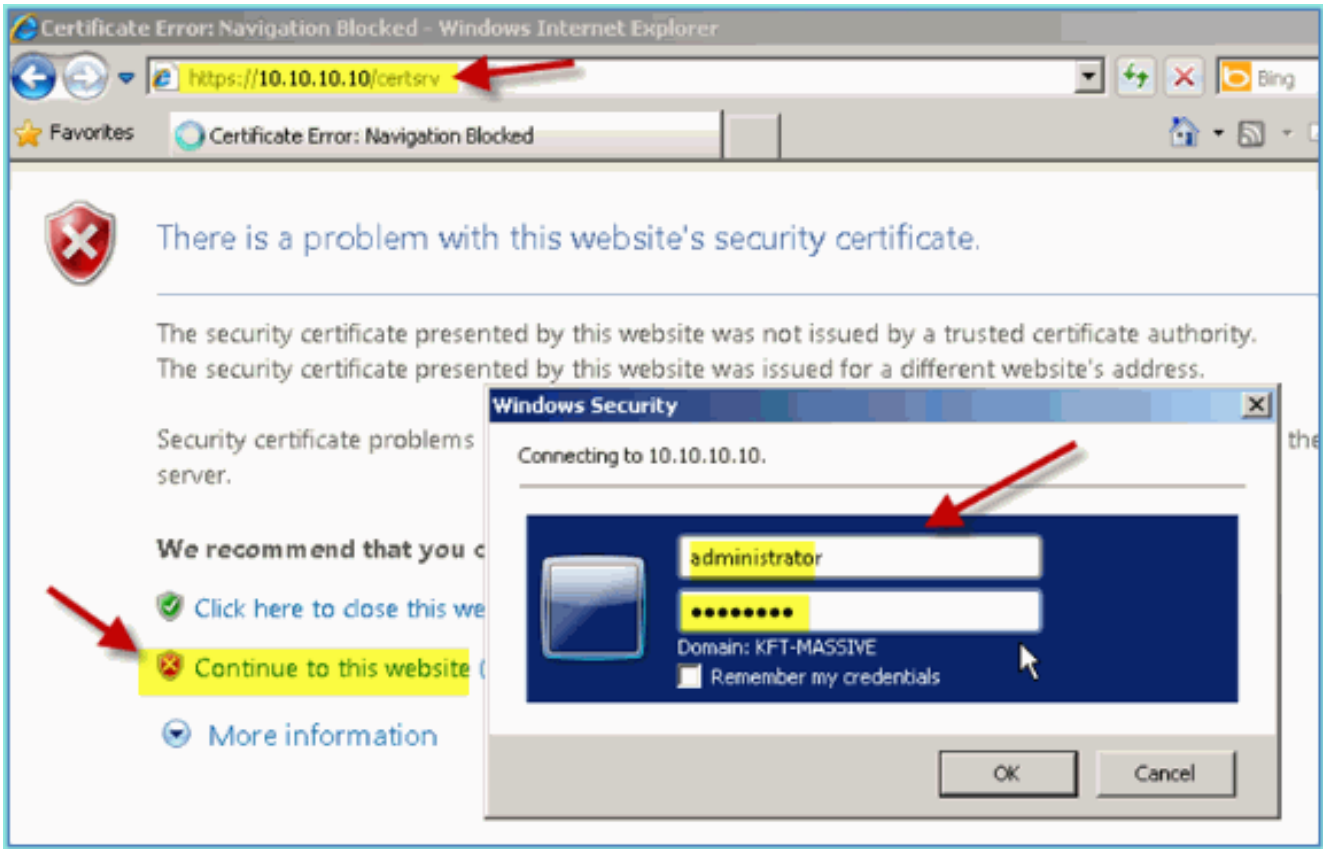
元の URL が入力され、エンドポイントがゲストとしてアクセスが許可されます。

証明書の設定

ISE との安全な通信のため、通信が認証関係か、ISE 管理に関するものかどうかを決定します。たとえば、ISE Web UI を使用する設定では、X.509 証明書と証明書信頼チェーンを設定して、非対称暗号化を有効にする必要があります。

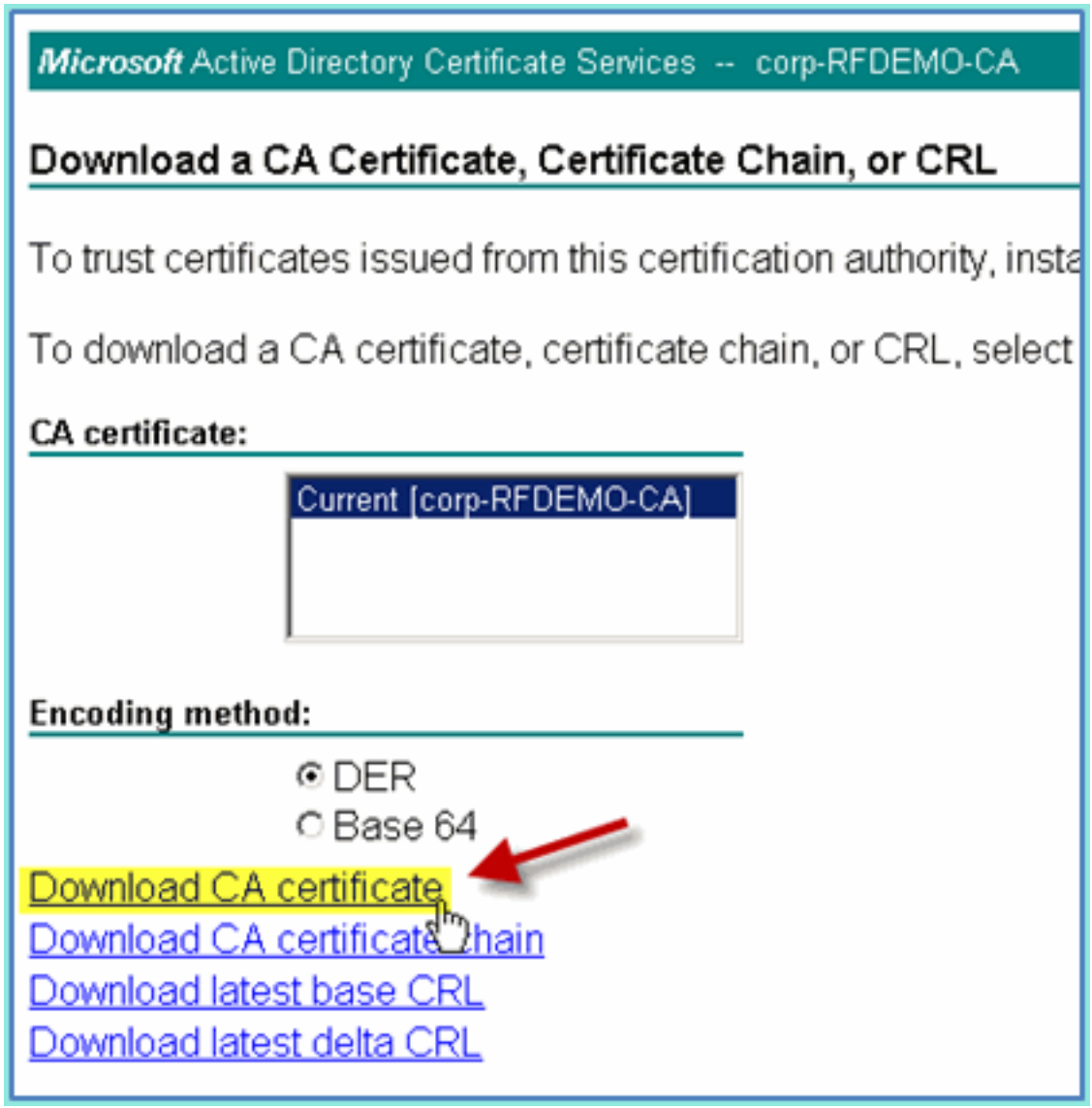
次のステップを実行します。

1. 有線接続された PC から、https://AD/certsrv にブラウザ ウィンドウを開きます。**注：セキュ**アHTTPを使用します。**注：**ISEにアクセスするには、Mozilla FirefoxまたはMS Internet Explorerを使用します。
2. administrator/Cisco123 としてログインします。



3. [Download a CA certificate, certificate chain, or CRL] をクリックします。

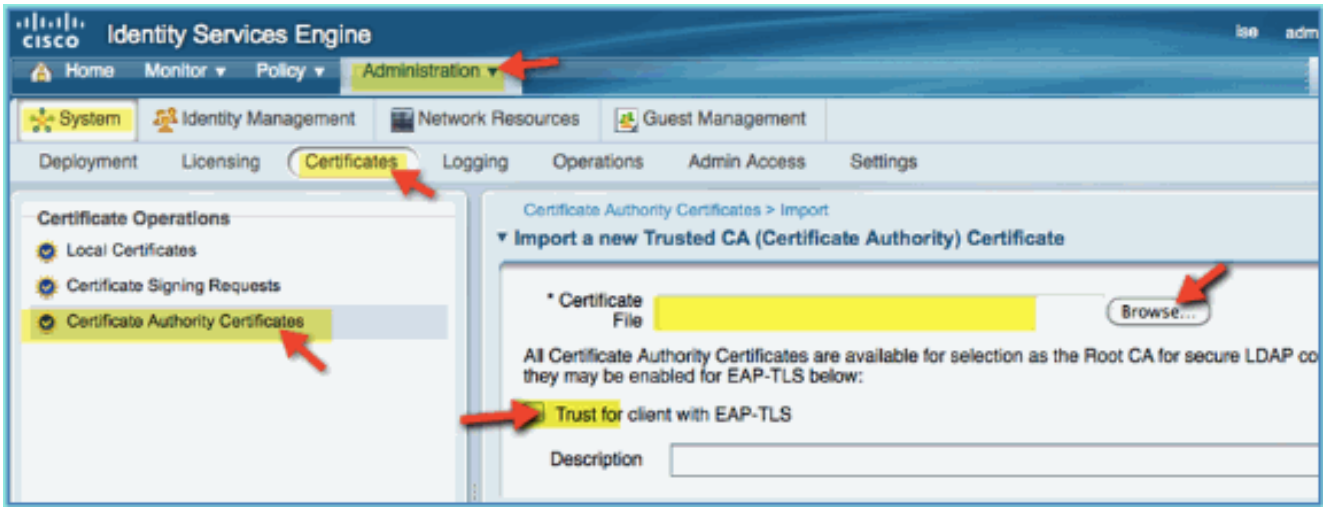
4. [Download CA certificate] をクリックし、保存します (保存した場所をメモしておきます



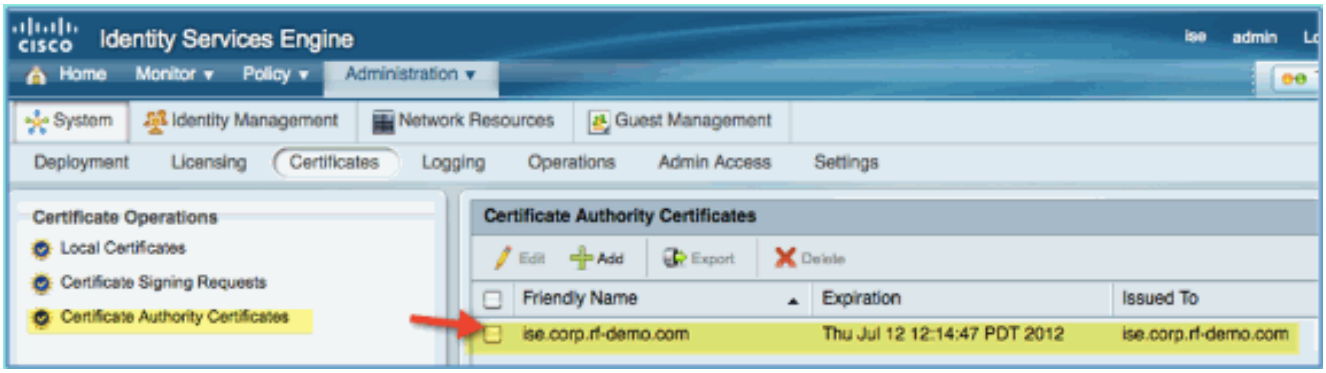
）。

5. ブラウザ ウィンドウで https://<Pod-ISE> を開きます。
6. [Administration] > [System] > [Certificates] > [Certificates Authority Certificates] に移動します。

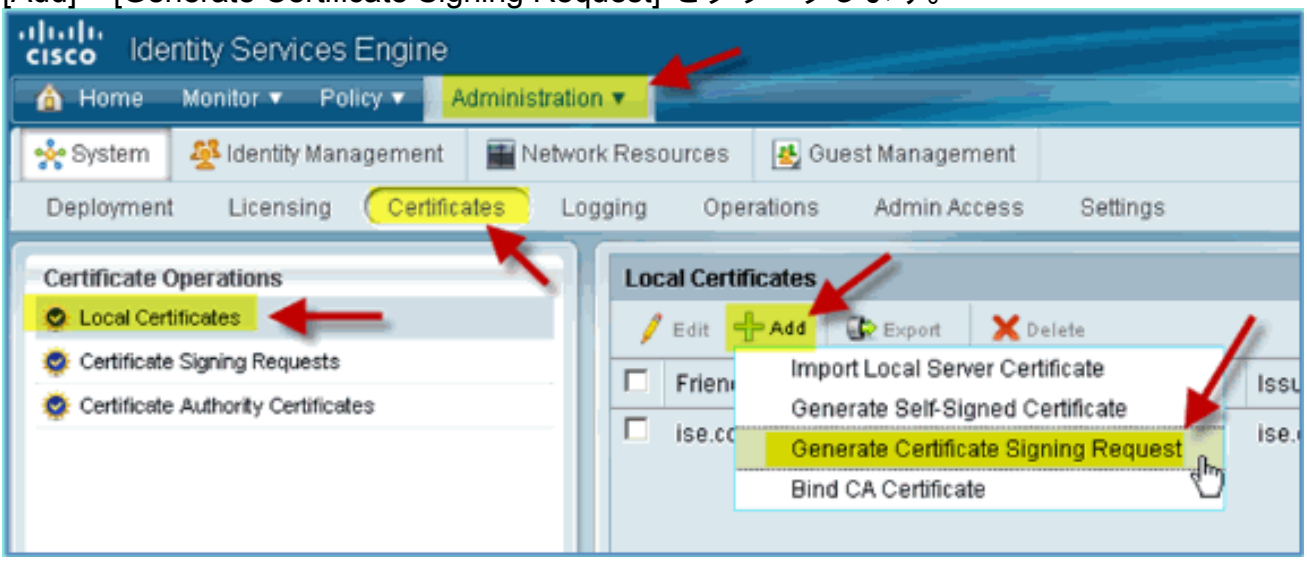
7. [Certificate Authority Certificates] **操作を選択し、先ほどダウンロードした CA 証明書を参照します。**
8. [Trust for client with EAP-TLS] を選択し、送信します。



9. CA がルート CA として追加され、信頼されていることを確認します。



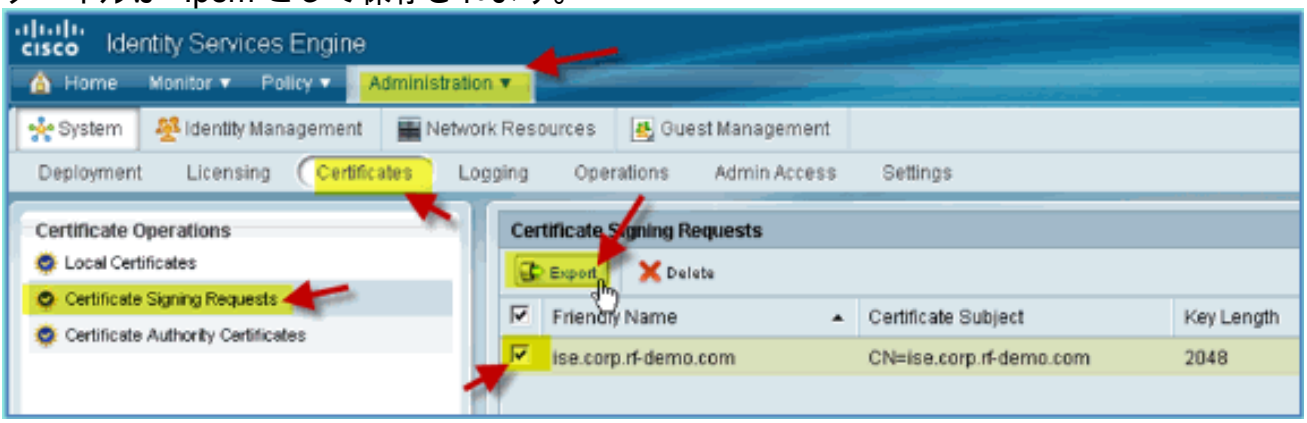
10. ブラウザから、[Administration] > [System] > [Certificates] > [Certificates Authority Certificates] に移動します。
11. [Add] > [Generate Certificate Signing Request] をクリックします。



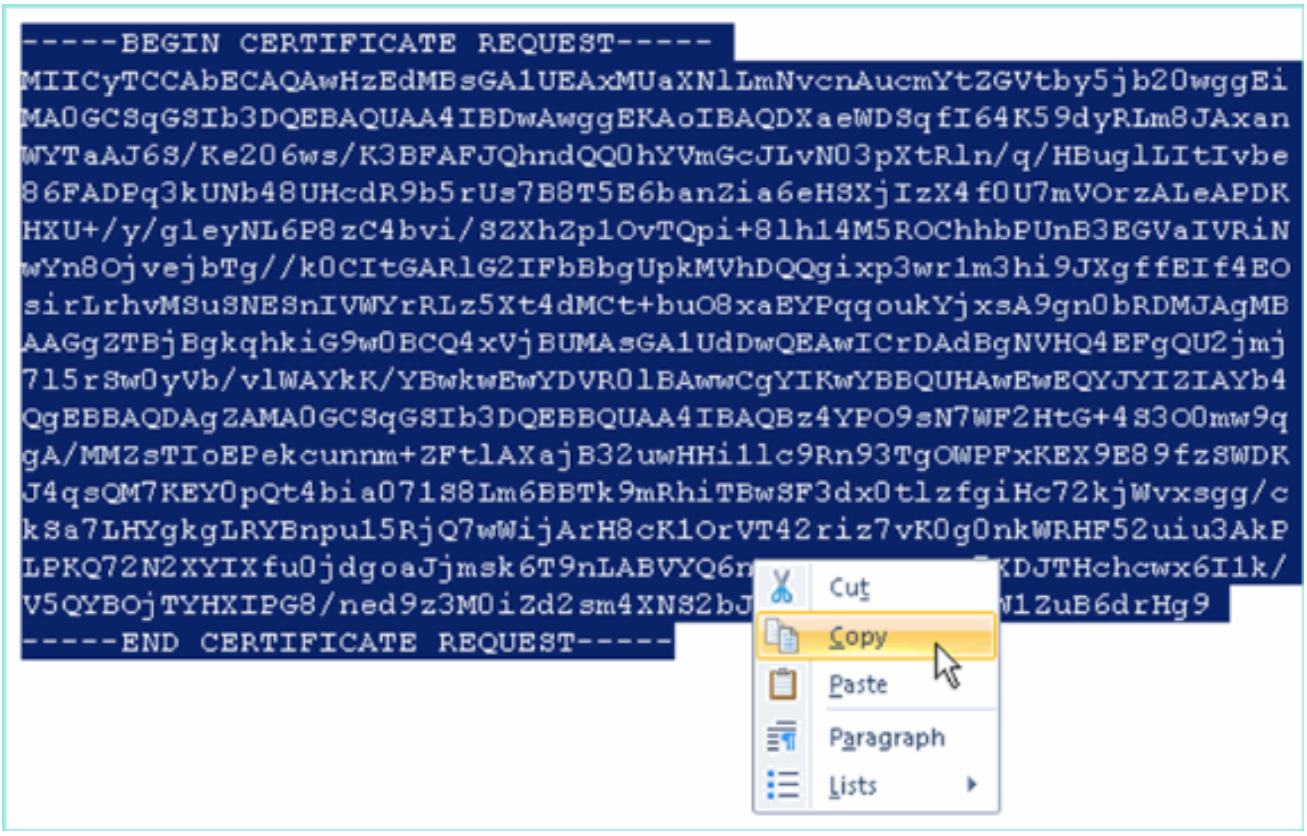
12. 次の値を送信します。[Certificate Subject]:CN=ise.corp.rf-demo.comキーの長さ：2048

13. ISE のプロンプトで、CSR ページで CSR を使用できることが表示されます。[OK] をクリックします。

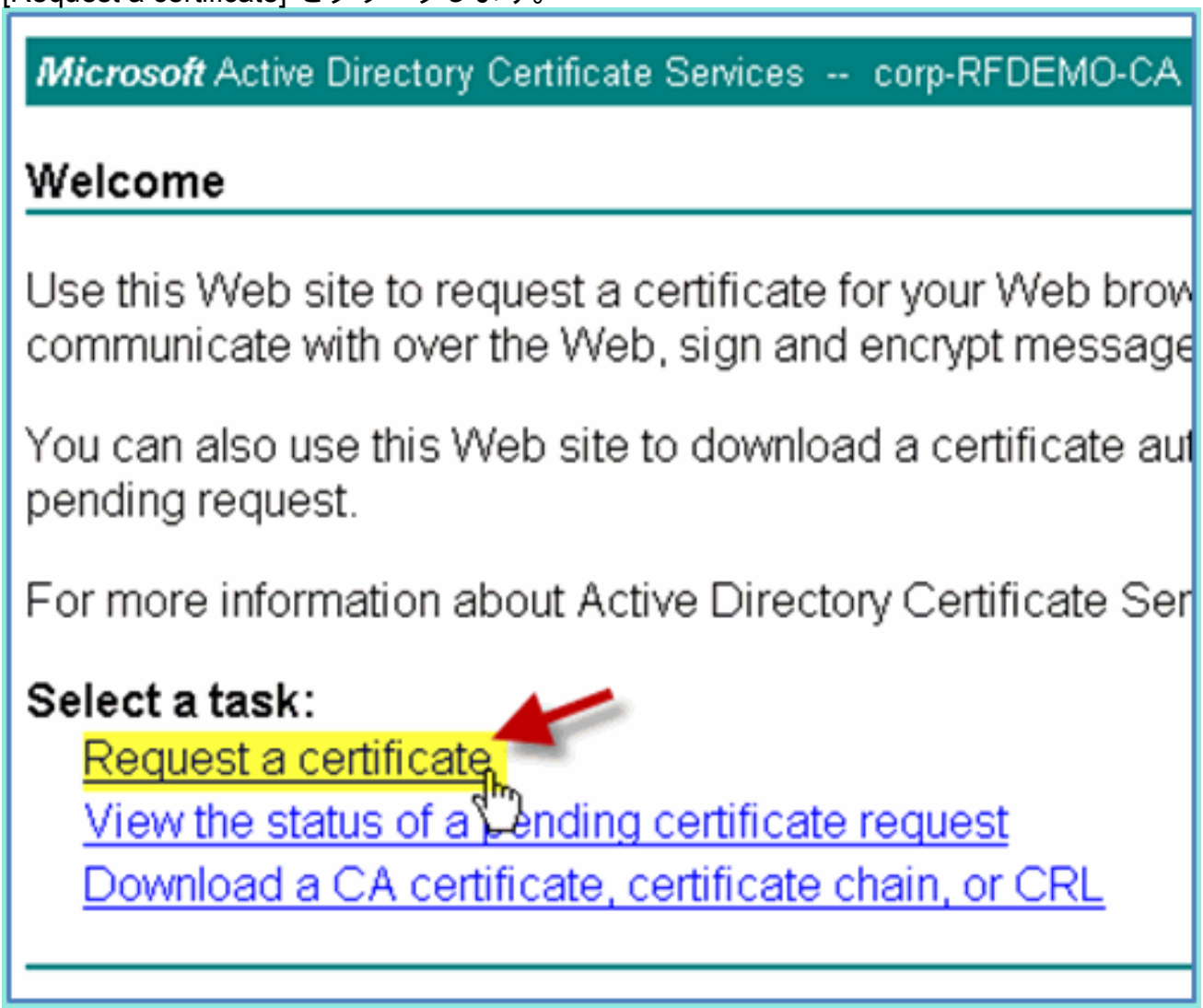
14. ISE CSR ページから CSR を選択し、[Export] をクリックします。
15. 任意の場所にファイルを保存します（たとえば、[Downloads] など）。
16. ファイルは *.pem として保存されます。



17. CSR ファイルを探し、メモ帳/ワードパッド/TextEdit のいずれかを使用して編集します。
18. コンテンツをコピーします（[all] > [Copy] を選択）。

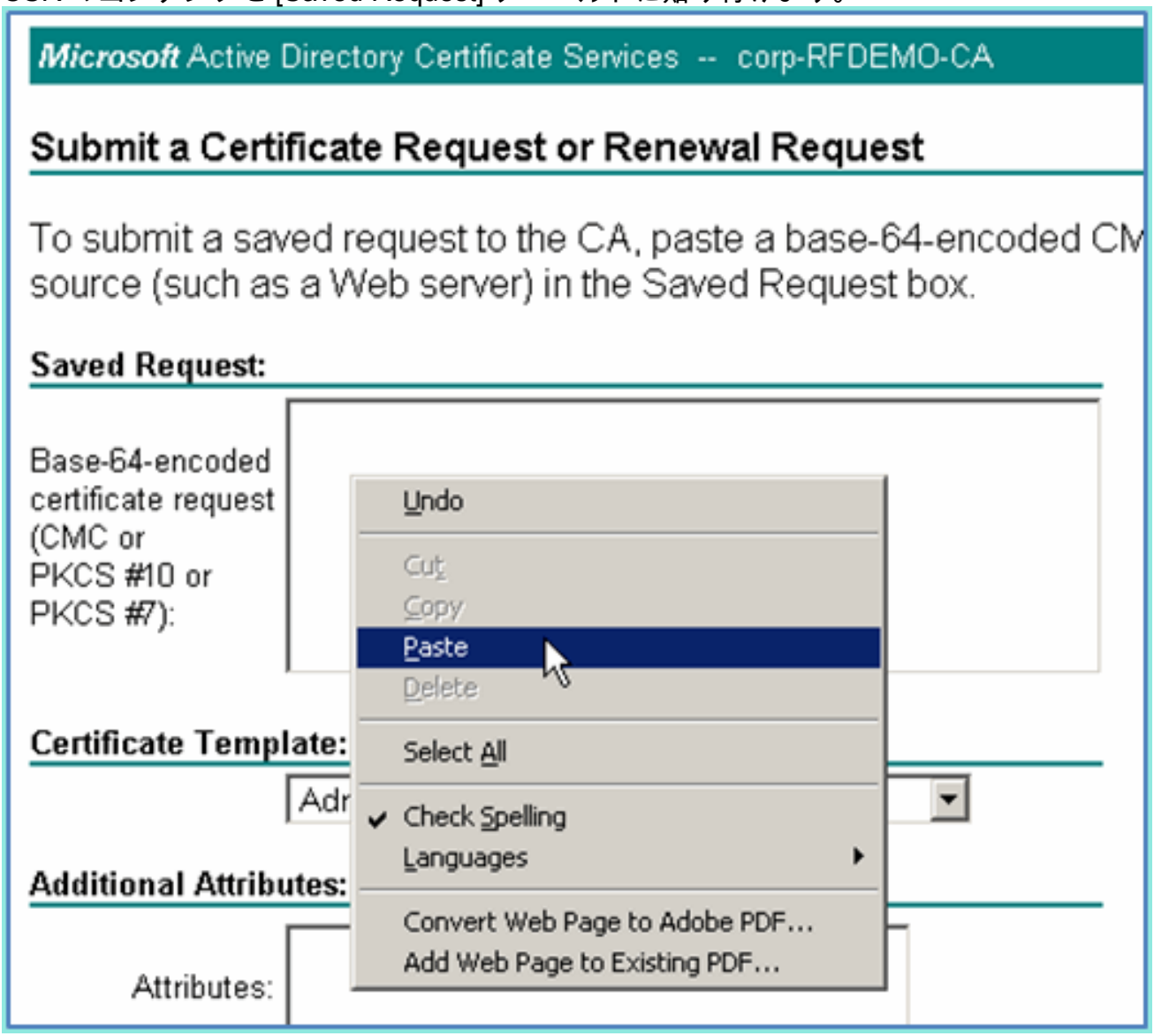


19. ブラウザ ウィンドウで https://<Pod-AD>/certsrv を開きます。
20. [Request a certificate] をクリックします。

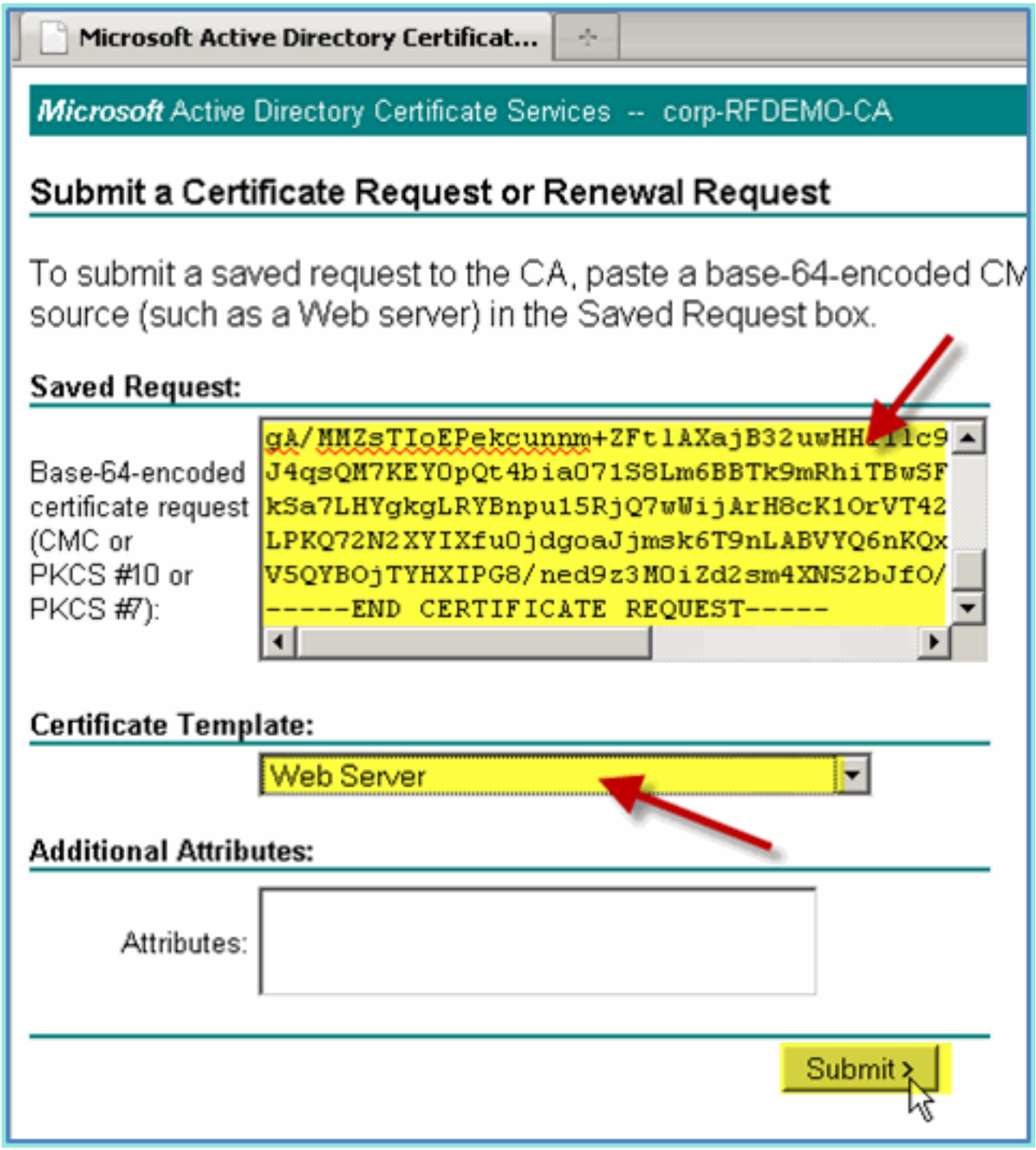


21. クリックして [Advanced certificate request] を送信します。

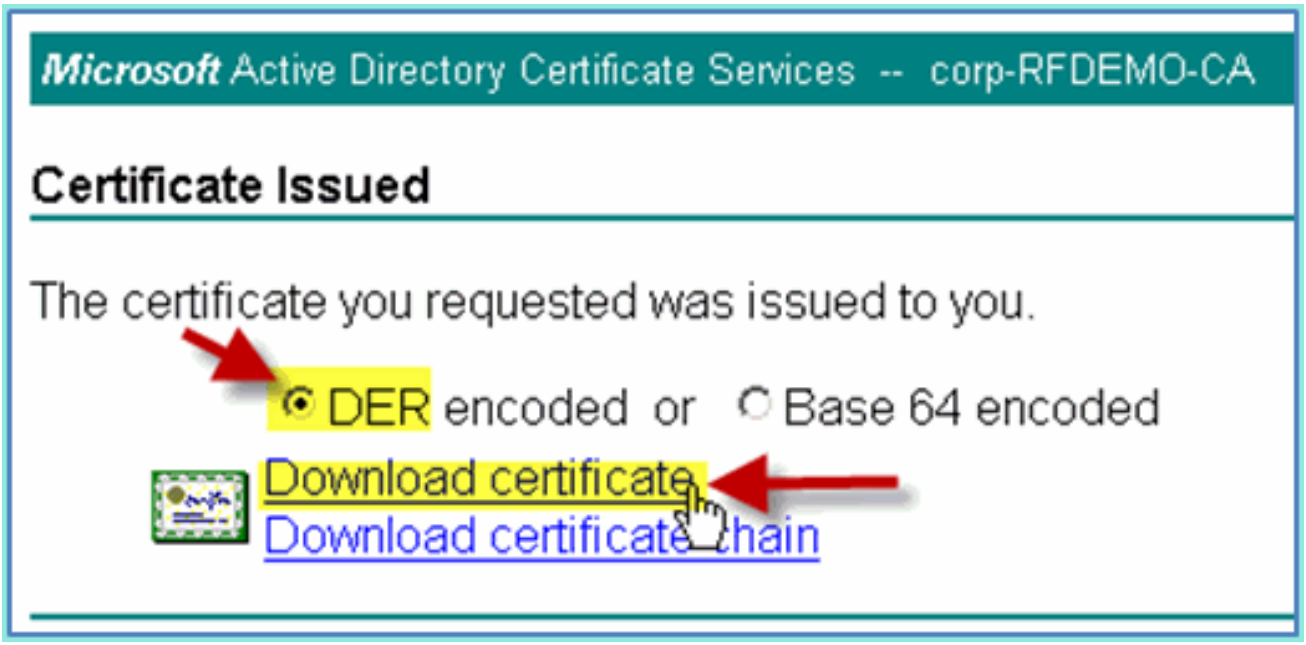
22. CSR のコンテンツを [Saved Request] フィールドに貼り付けます。



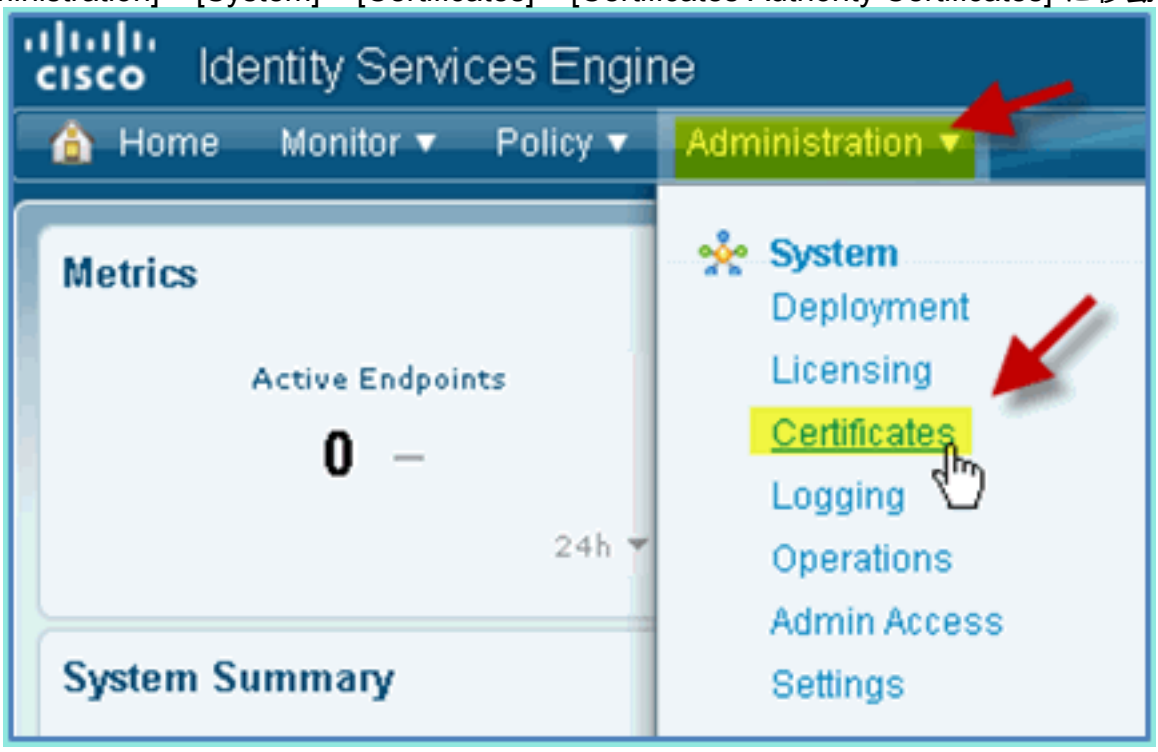
23. 証明書テンプレートとして [Web Server] サーバを選択し、[Submit] をクリックします。



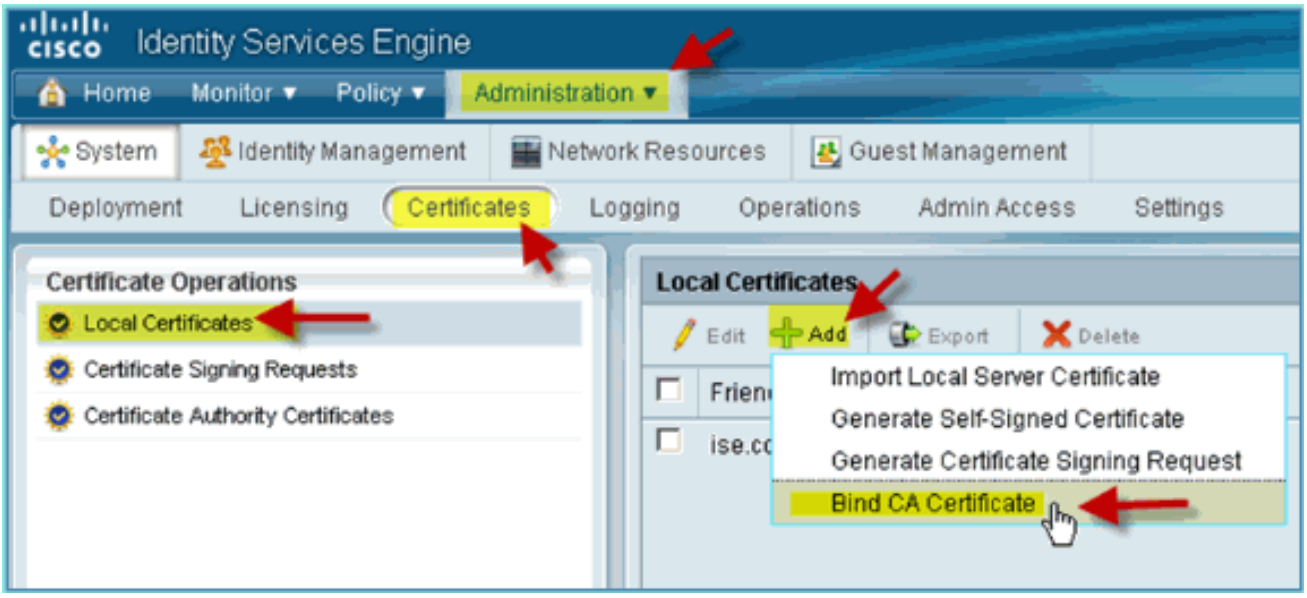
24. [DER encoded] を選択し、[Download certificate] をクリックします。



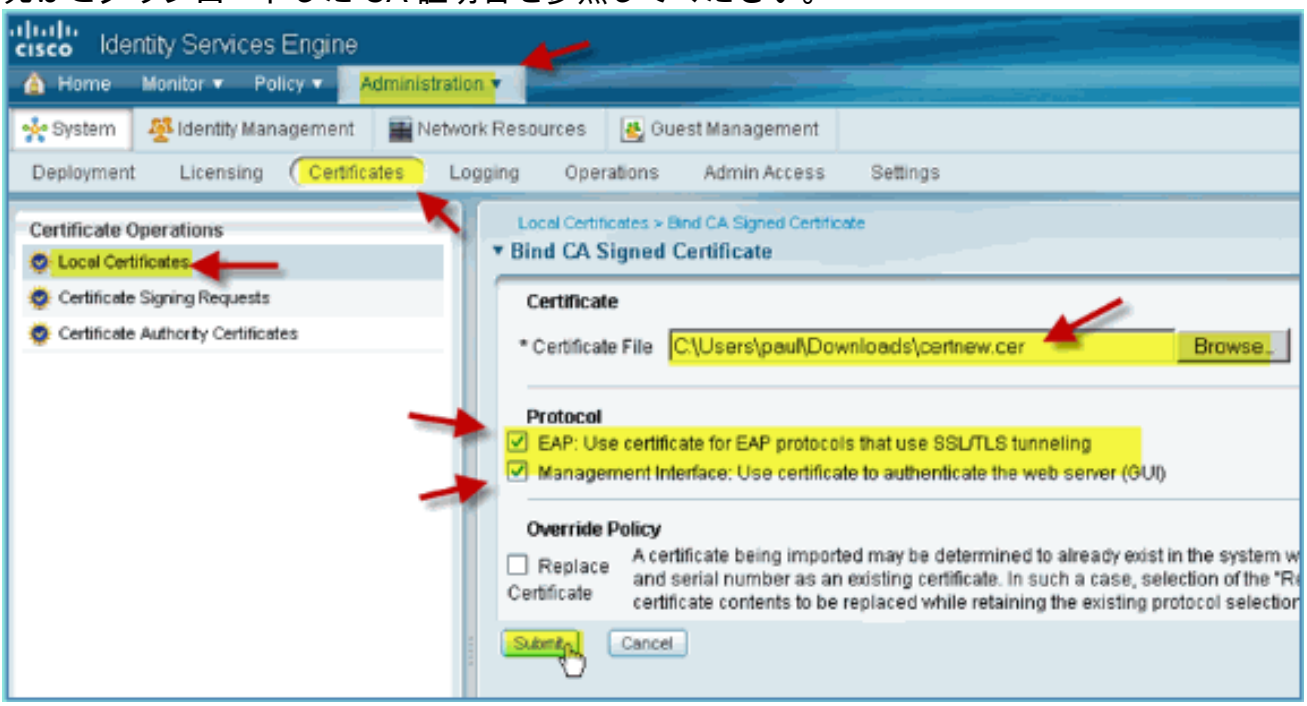
25. 既知の場所にファイルを保存します（ たとえば、[Downloads] ）。
26. [Administration] > [System] > [Certificates] > [Certificates Authority Certificates] に移動します。



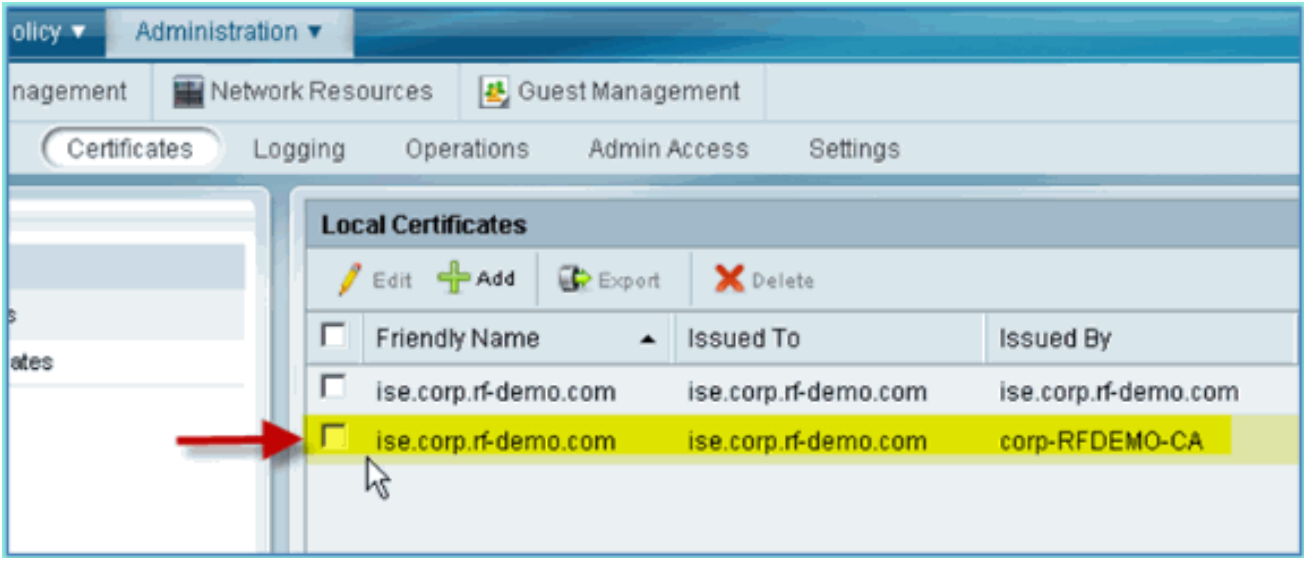
27. [Add] > [Bind CA signed Certificate] をクリックします。



28. 先ほどダウンロードした CA 証明書を参照してください。



29. [Protocol EAP] と **[Management Interface]** の両方を選択し、[Submit] をクリックします。
30. CA がルート CA として追加され、信頼されていることを確認します。

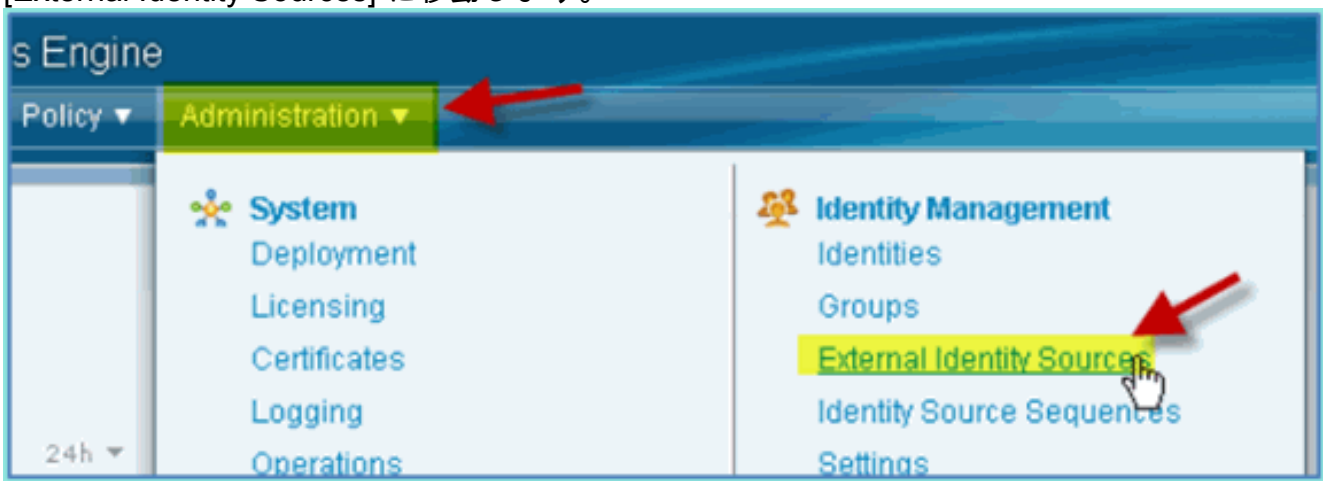


Windows 2008 の Active Directory Integration

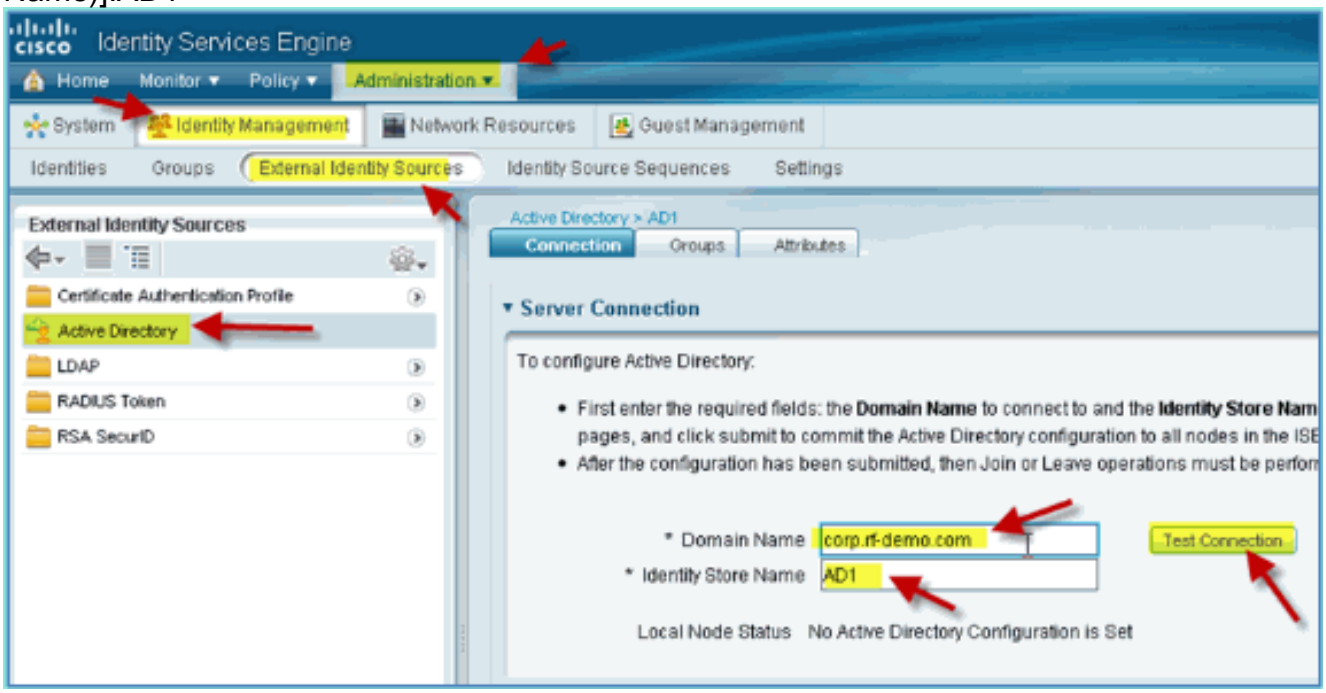
ISE はユーザ/マシンの認証のため、または認証情報やユーザ属性を取得するために Active Directory（AD）と直接通信できます。AD と通信するには、ISE は AD ドメインに「参加」する必要があります。この演習では、ISE を AD ドメインに参加させ、AD との通信が正しく動作していることを確認します。

次のステップを実行します。

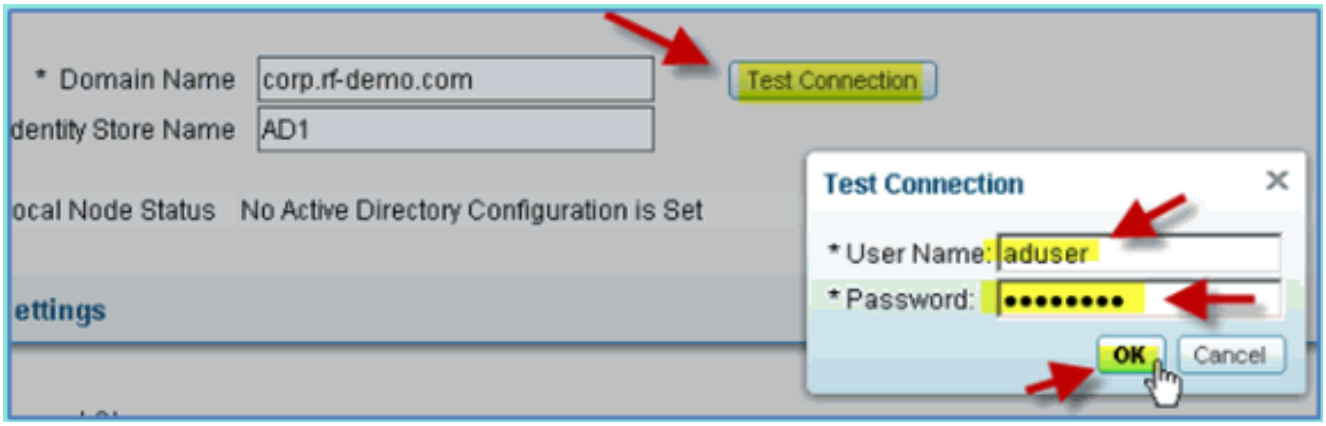
1. ISE を AD ドメインに参加させるには、ISE から [Administration] > [Identity Management] > [External Identity Sources] に移動します。



2. 左ペイン（External Identity Sources）から、[Active Directory] を選択します。
3. 右側で [Connection] **タブを選択し、次を入力します。**ドメイン名：corp.rf-demo.com[IDストア名(Identity Store Name)]:AD1

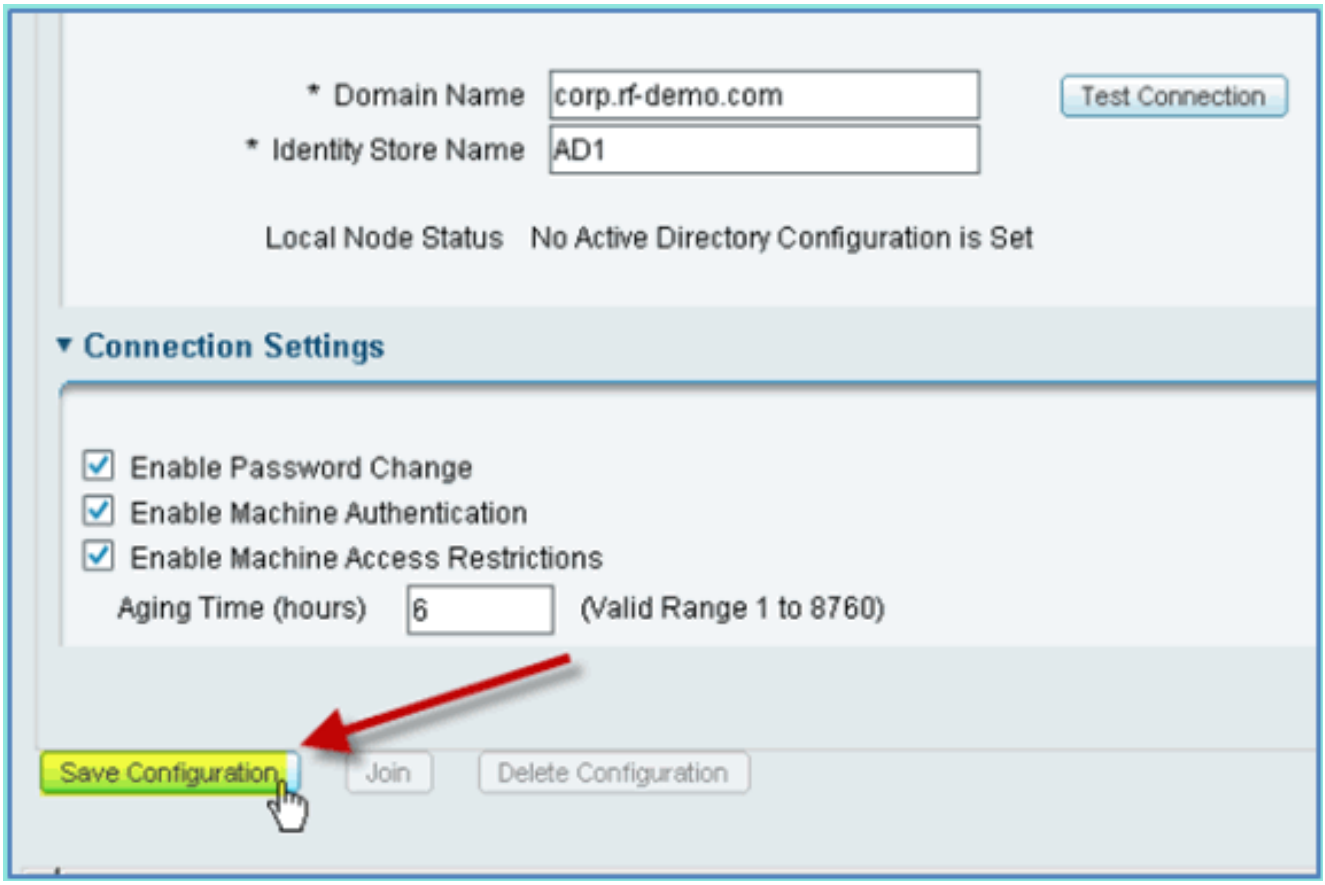


4. [Test Connection] をクリックします。AD ユーザ名（aduser/Cisco123）を入力し、[OK] をクリックします。

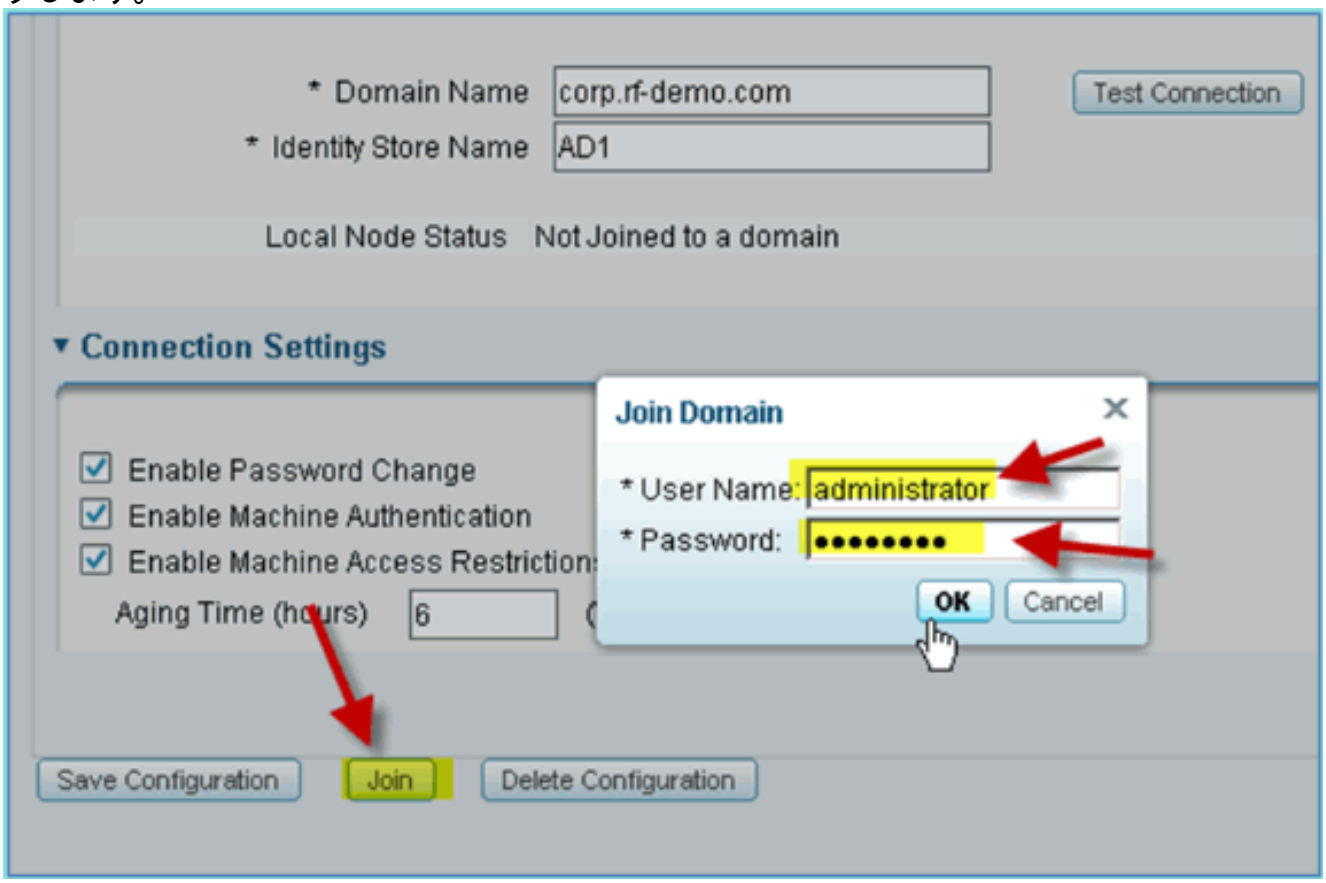


5. [Test Status] が [Test Succeeded] を示していることを確認します。
6. [Show Detailed Log] を選択し、トラブルシューティングに役立つ詳細情報を確認します。[OK] をクリックして、次に進みます。

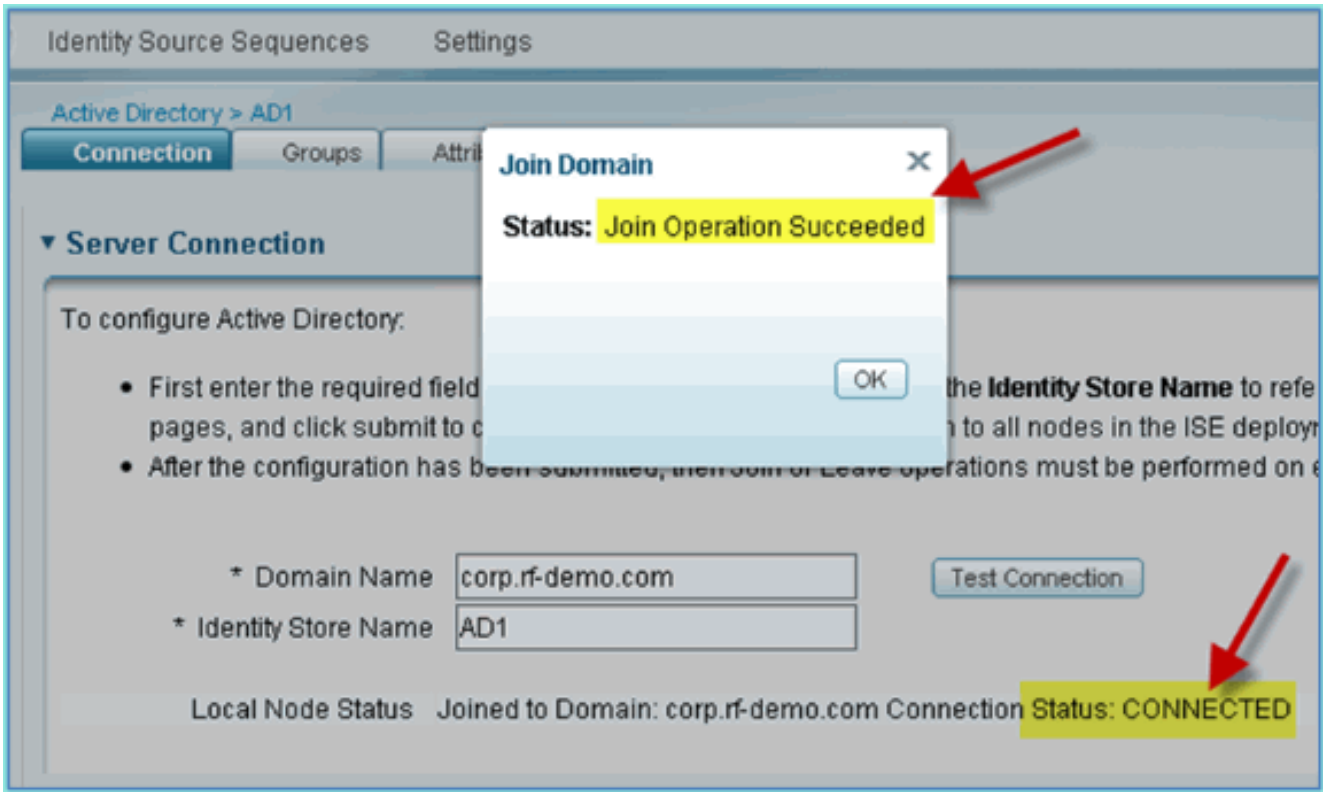
7. [Save Configuration] をクリックします。



8. [Join] をクリックします。AD ユーザ名（administrator/Cisco123）を入力し、[OK] をクリックします。



9. [Join Operation] ステータスが [Succeeded] と表示されていることを確認したら、[OK] をクリックして続行します。[Server Connection] ステータスは [CONNECTED] と表示されます。このステータスが変更されたらいつでも、[Test Connection] をクリックすることで AD の動作に関する問題をトラブルシューティングすることができます。



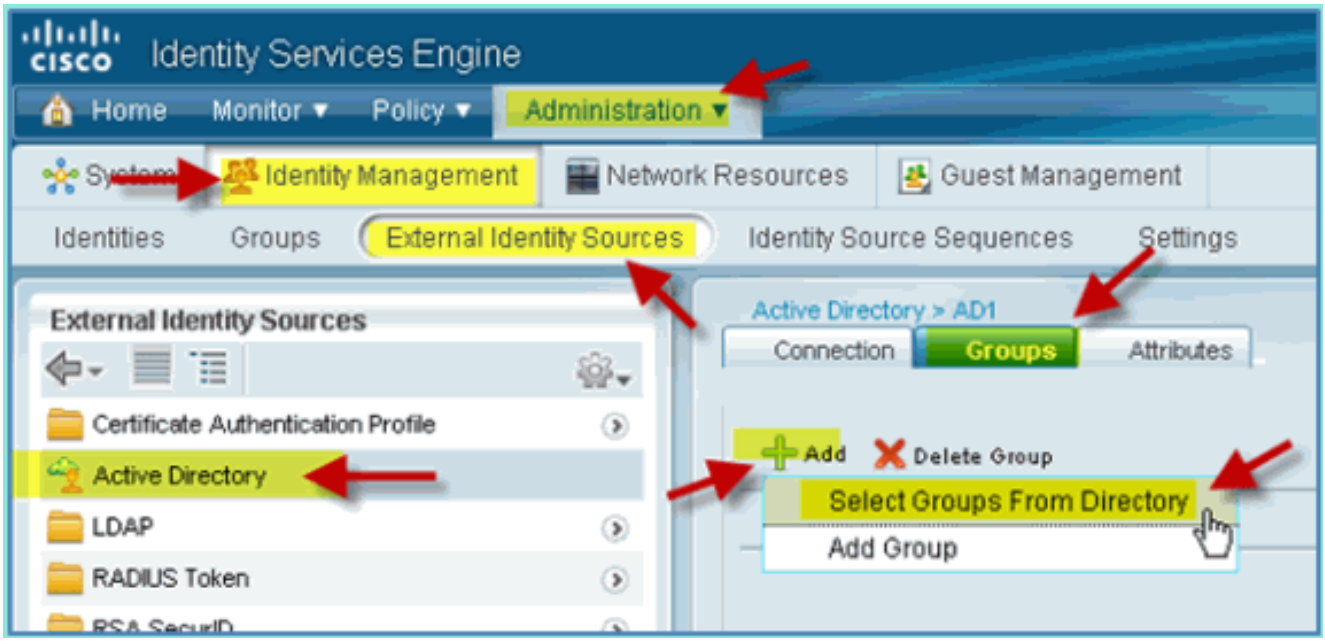
Active Directory グループの追加

AD グループを追加すると、ISE ポリシーに対してよりきめ細かい制御を行えるようになります。たとえば、AD グループを、従業員や請負業者のグループなどの機能的役割別に差別化することができます。ポリシーがユーザにのみ限定されていた以前の ISE 1.0 の演習では、これに関連するバグは発生していません。

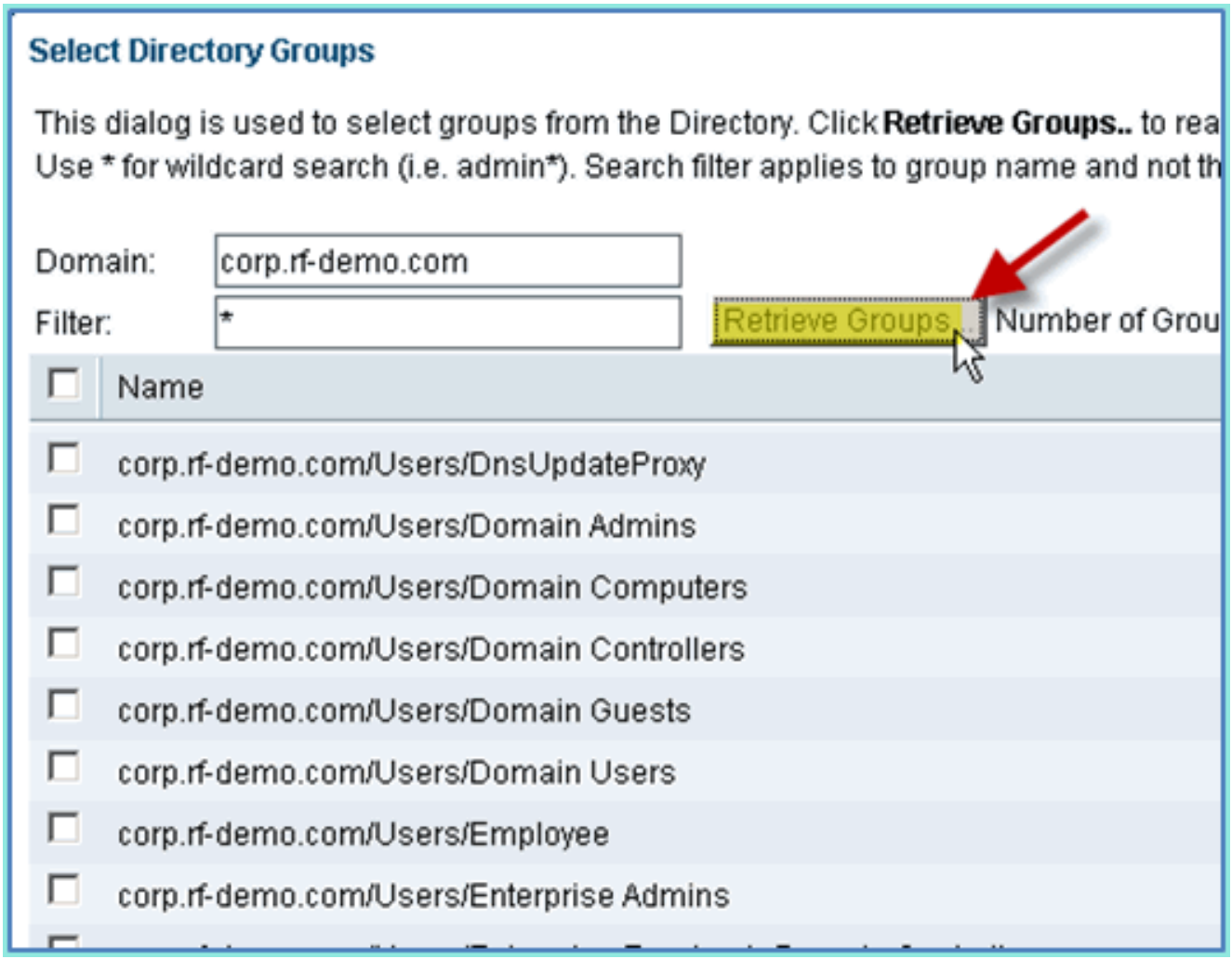
このラボでは、ドメイン ユーザや従業員のグループのみを使用します。

次のステップを実行します。

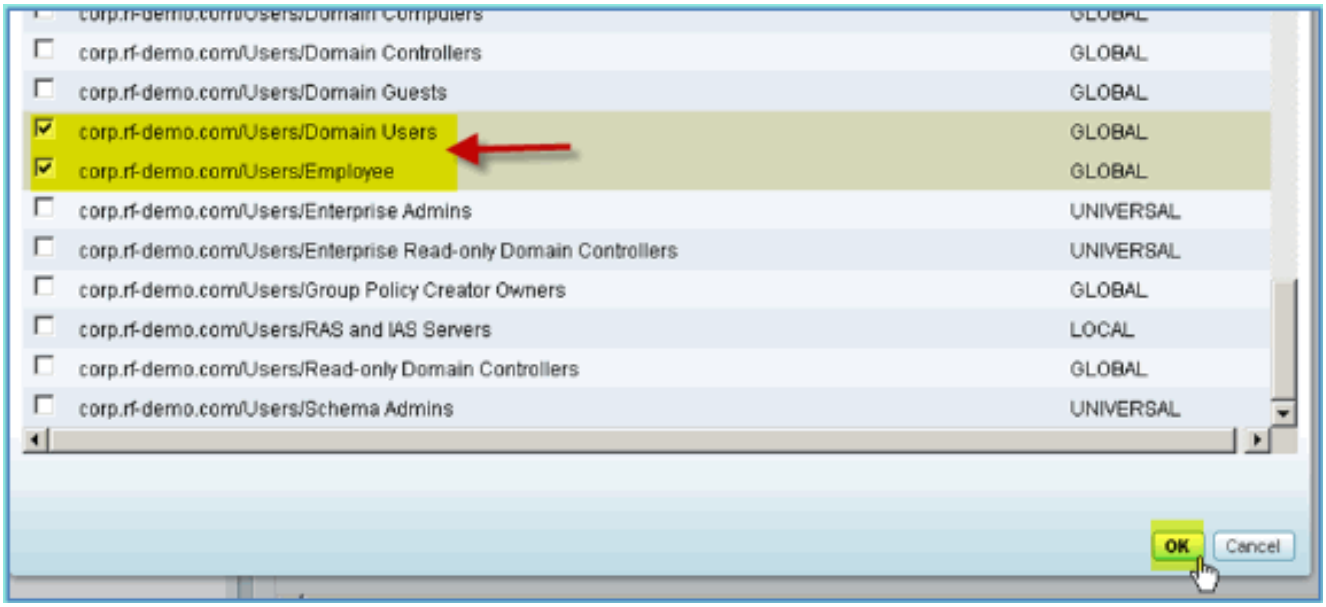
1. ISE から、[Administration] > [Identity Management] > [External Identity Sources] の順に移動します。
2. [Active Directory] > [Groups] **タブを選択します。**
3. [+Add] をクリックし、[Select Groups From Directory] を選択します。



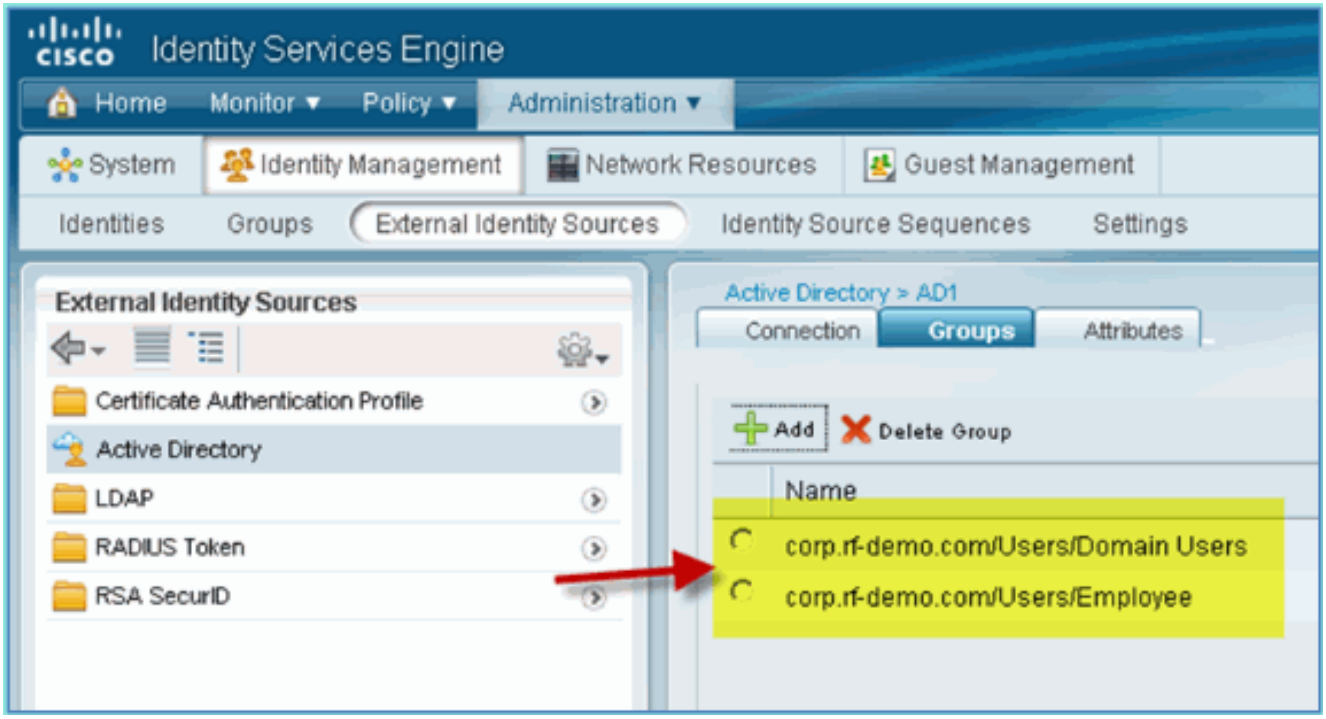
4. 次に表示されるウィンドウ（Select Directory Groups）で、ドメイン（corp rf demo.com）およびフィルタ（*）のデフォルトを承認します。次に、[Retrieve Groups] をクリックします。



5. [Domain Users] と **[Employee] グループのチェックボックスを選択します。**完了したら、[OK] をクリックします。



6. グループがリストに追加されたことを確認します。

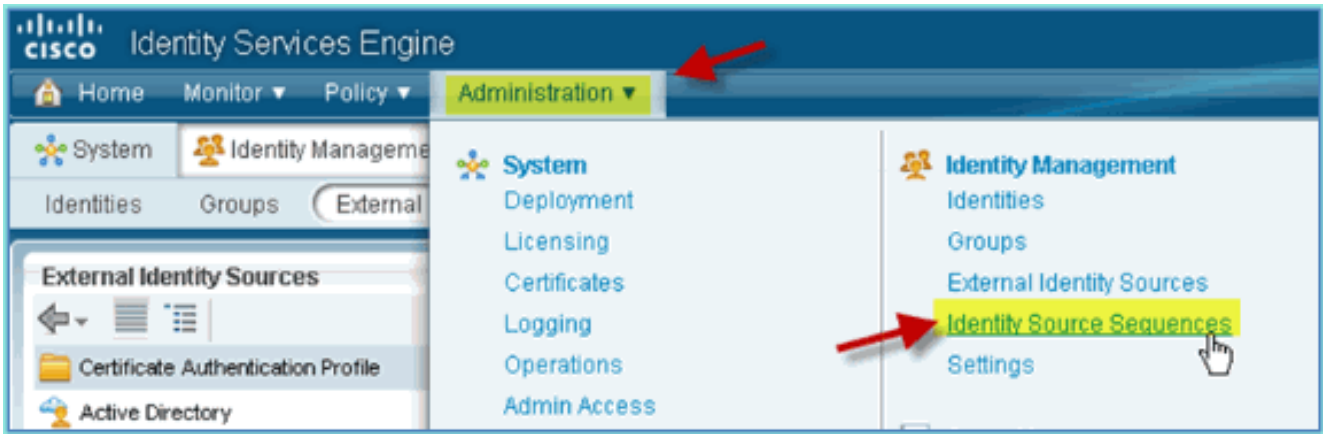


ID ソース順序の追加

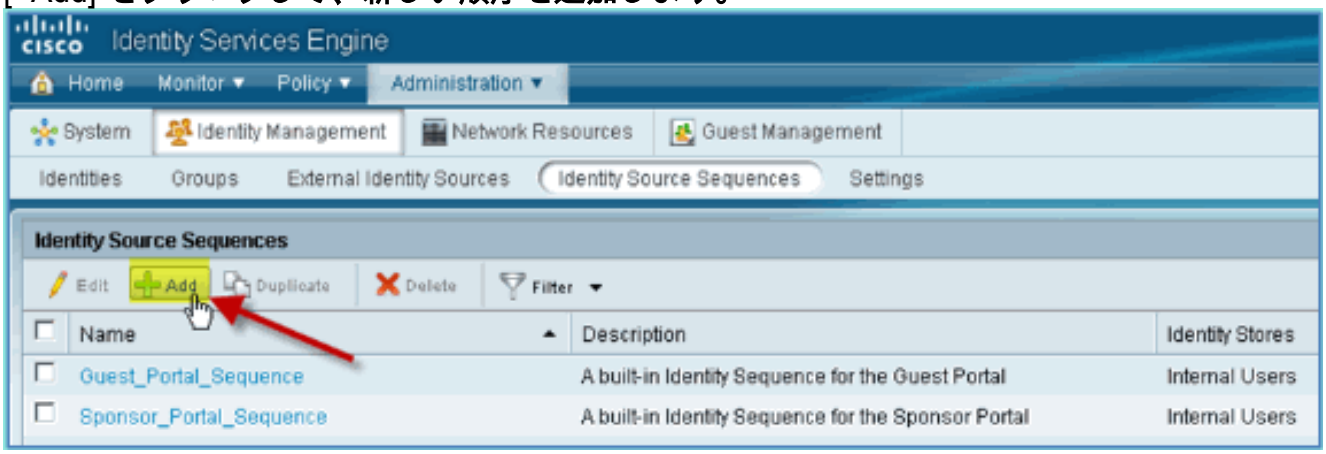
デフォルトでは、ISE は認証ストアに内部ユーザを使用するように設定されています。AD が追加されると、ISE が認証を確認するために使用する AD を含めるように、優先順位別の順序を作成することができます。

次のステップを実行します。

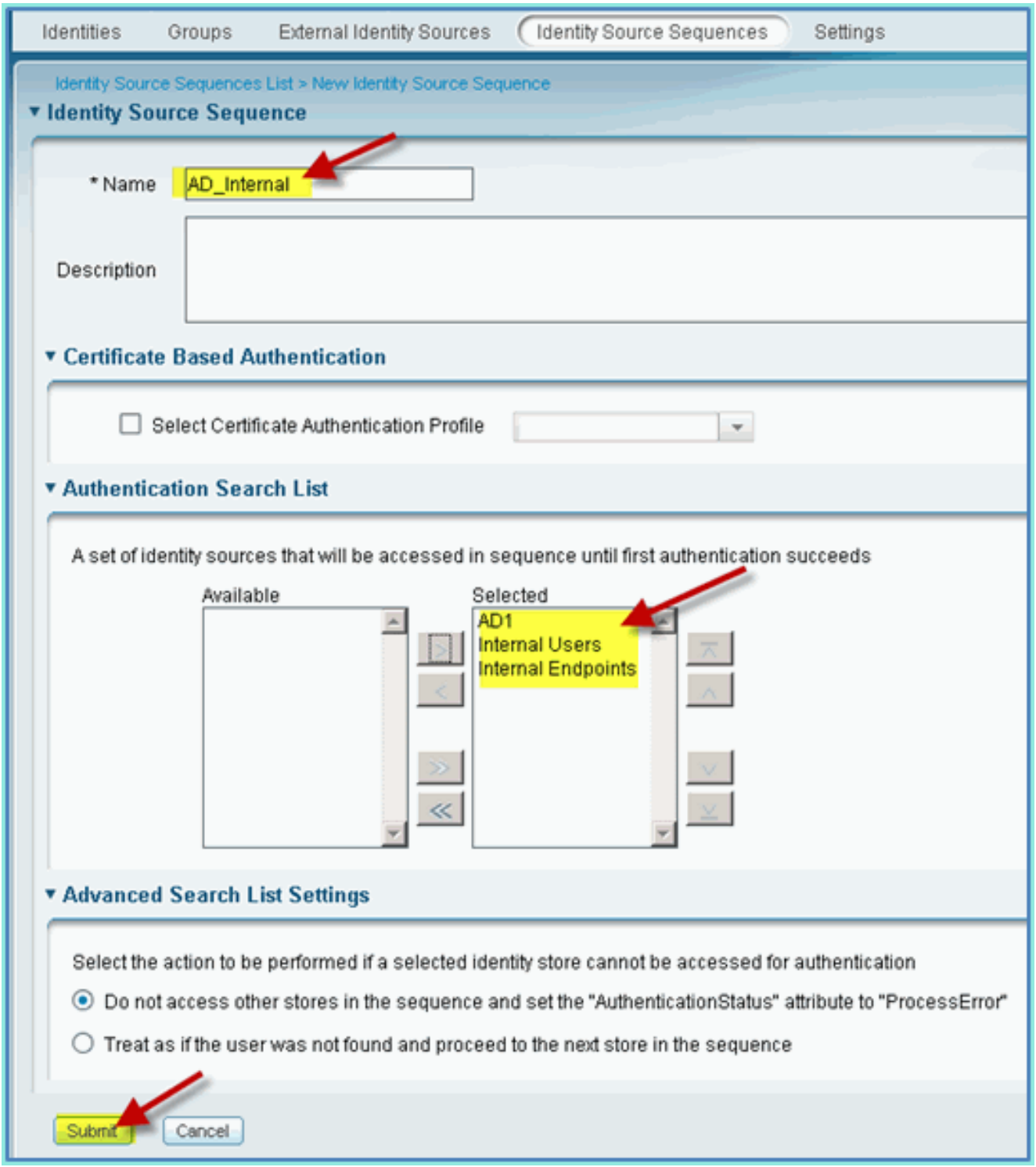
1. ISE から、[Administration] > [Identity Management] > [Identity Source Sequences] の順に移動します。



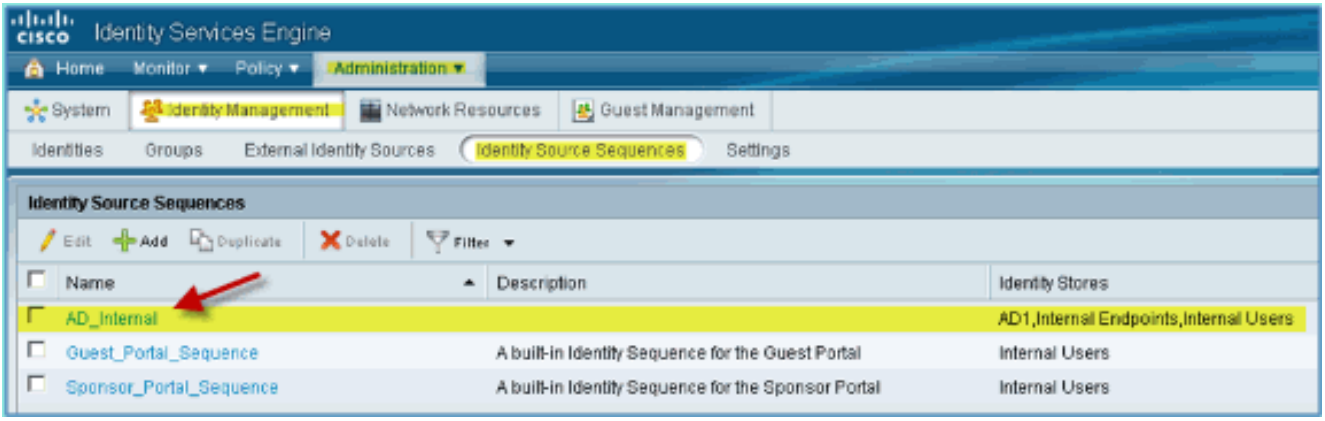
2. [+Add] をクリックして、新しい順序を追加します。



3. 新しい名前**AD_Internal**を入力します。[Selected] フィールドに使用可能なすべてのソースを追加します。次に、AD1 がリストの先頭に移動するように、必要に応じて順序を並べ替えます。[Submit] をクリックします。



4. 順序がリストに追加されたことを確認します。



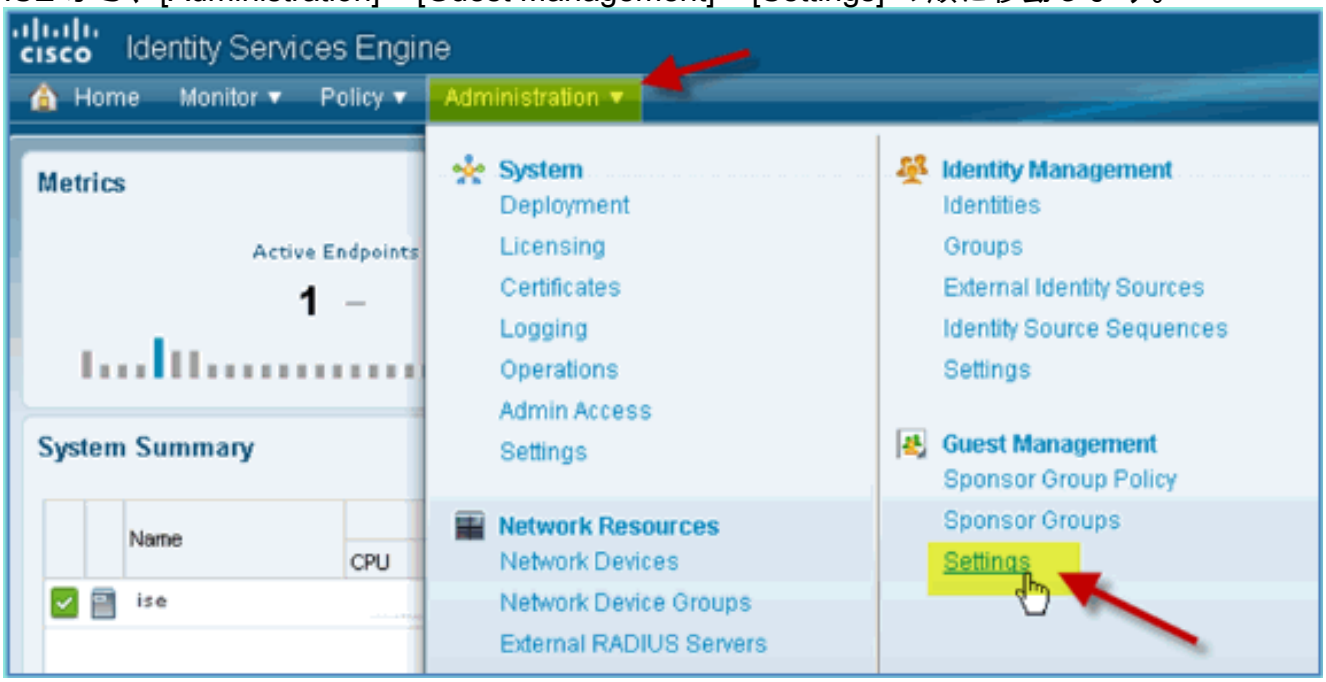
統合された AD による ISE のワイヤレス スポンサード ゲスト ア

クセス

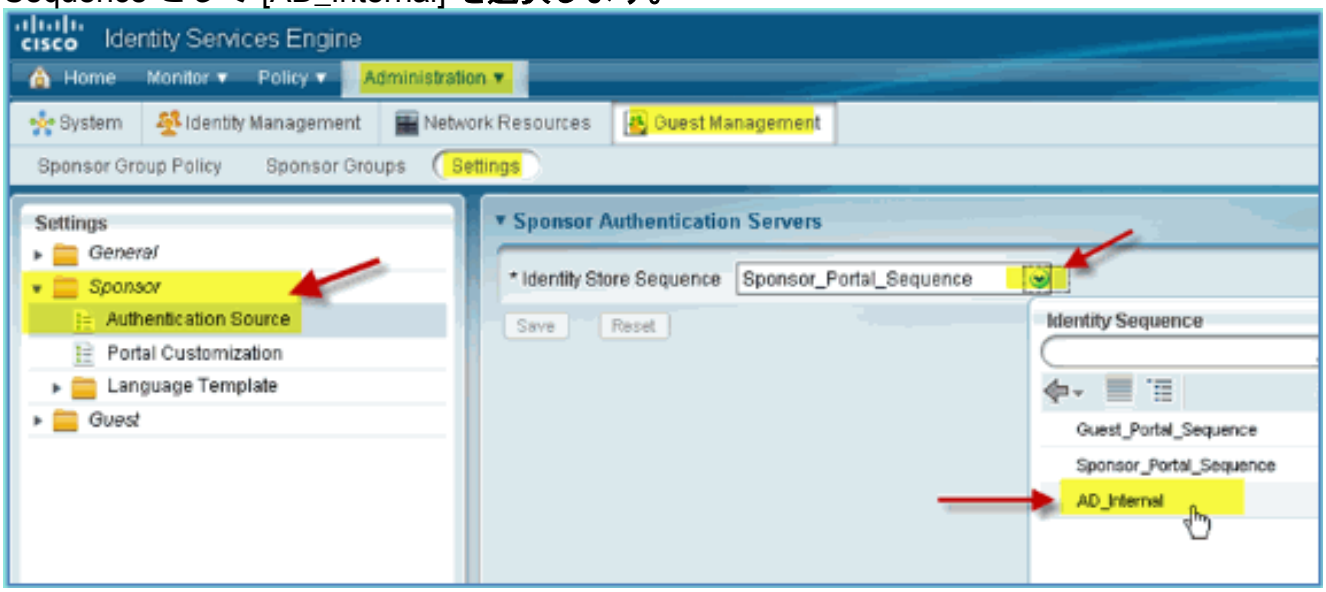
ISE は、AD ドメイン ユーザがゲスト アクセスのスポンサーとなることができるように、ゲストがポリシーのスポンサーとなるように設定できます。

次のステップを実行します。

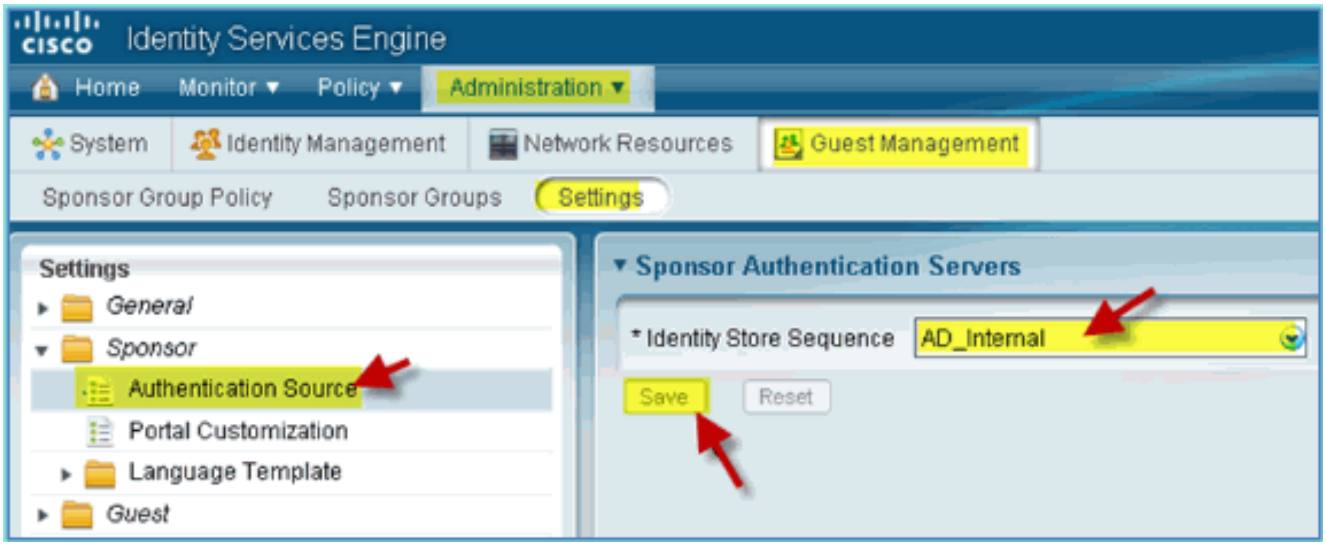
1. ISE から、[Administration] > [Guest Management] > [Settings] の順に移動します。



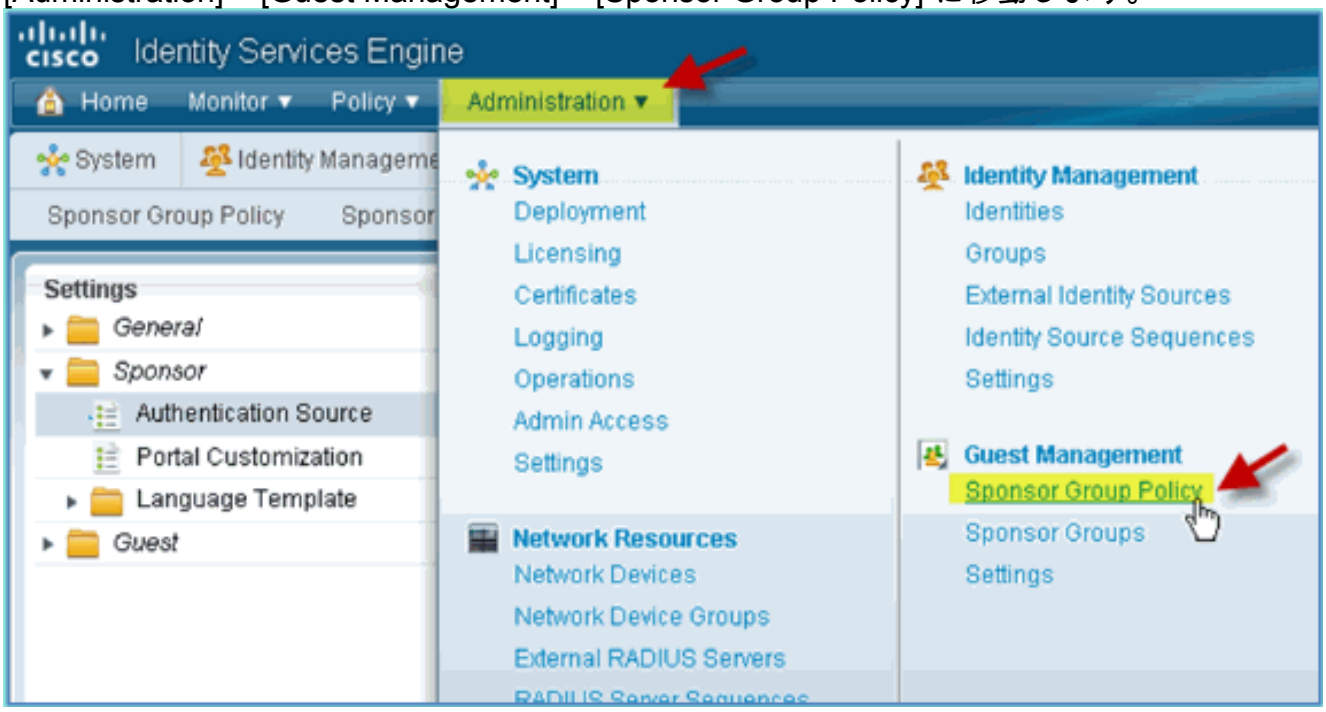
2. [Sponsor] を展開し、[Authentication Source] をクリックします。次に、Identity Store Sequence として [AD_Internal] **を選択します。**



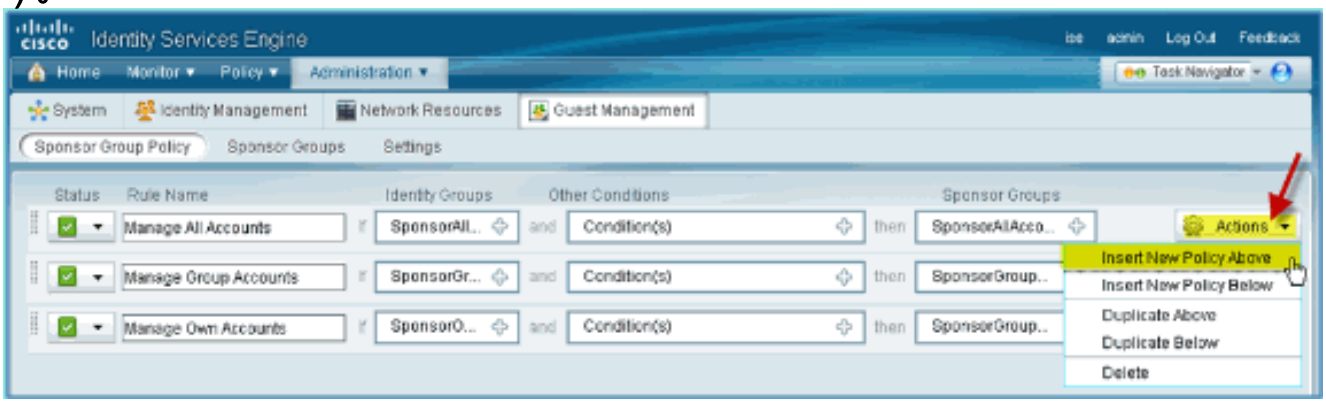
3. AD_Internal を Identity Store Sequence として確定します。[Save] をクリックします。



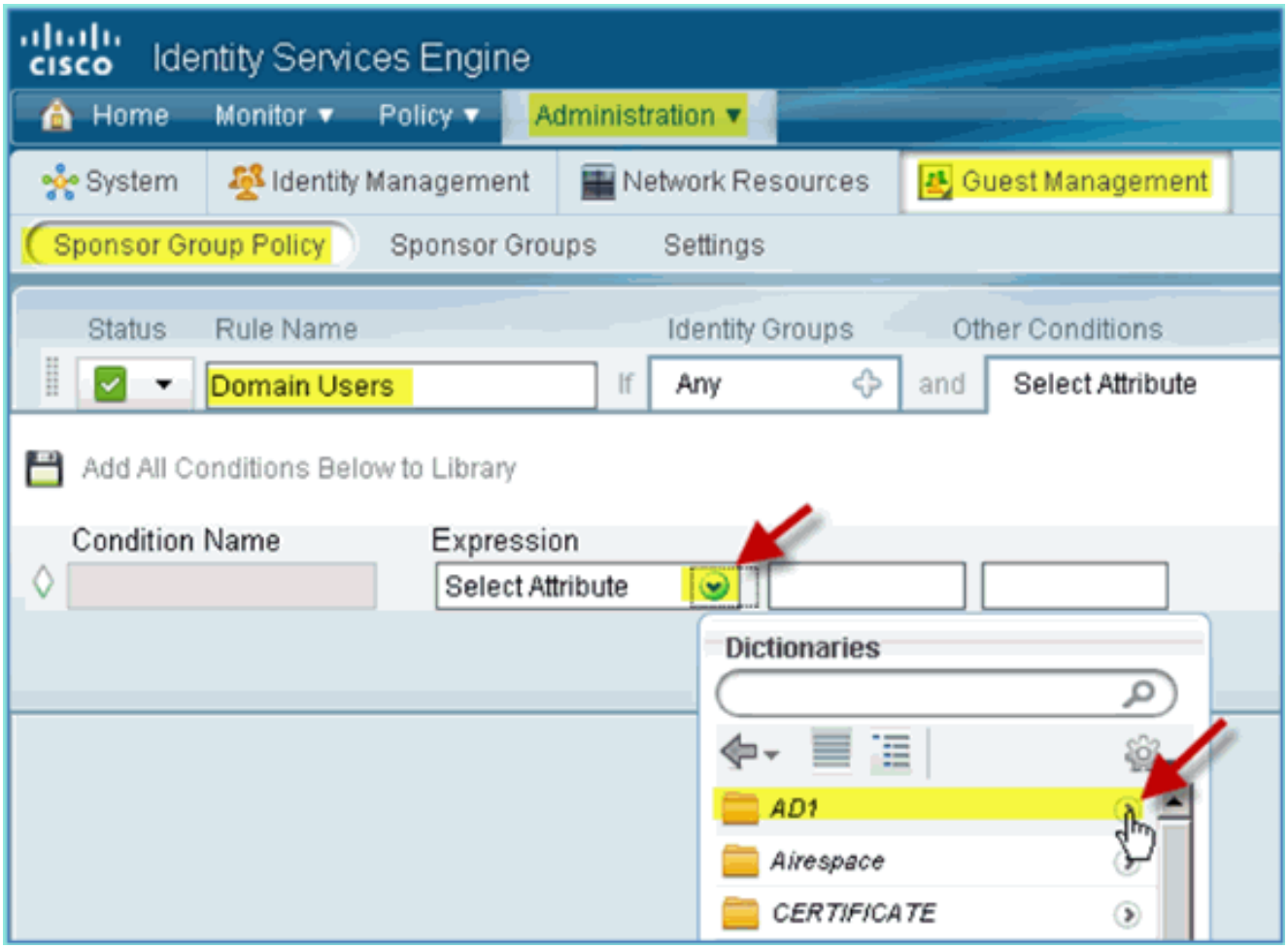
4. [Administration] > [Guest Management] > [Sponsor Group Policy] に移動します。



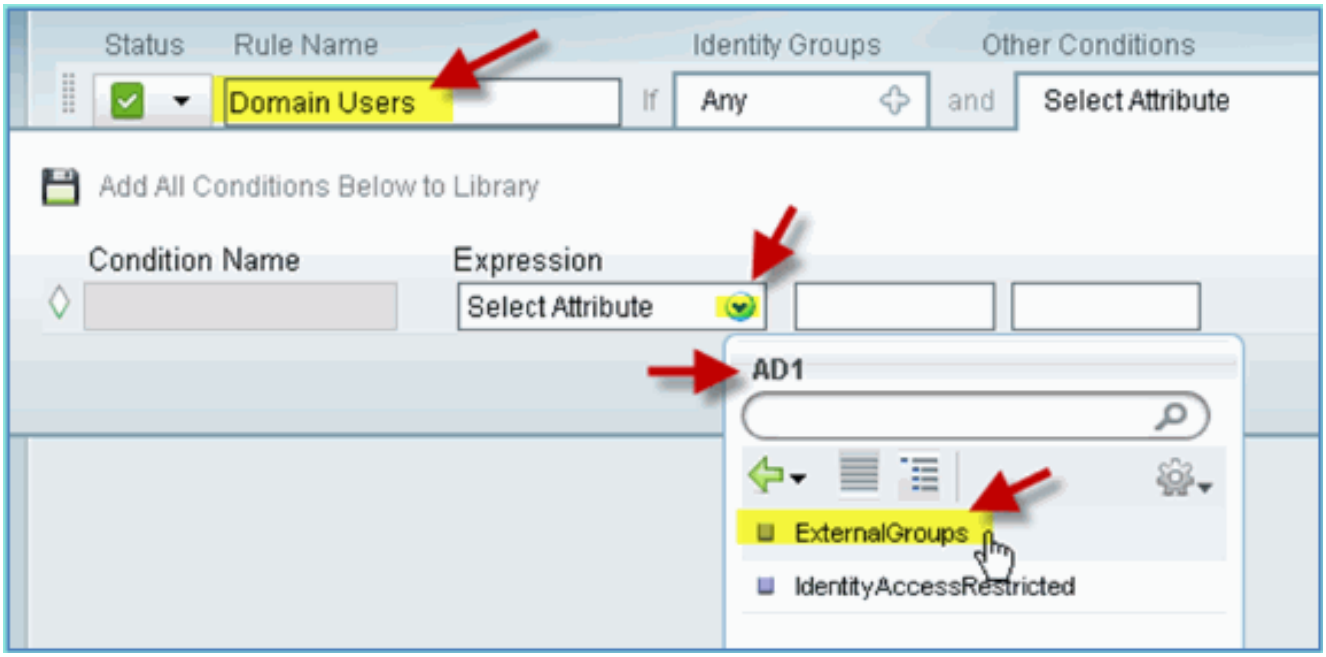
5. 最初のルールの上部に新しいポリシーを挿入します（右側の [Actions] アイコンをクリック）。



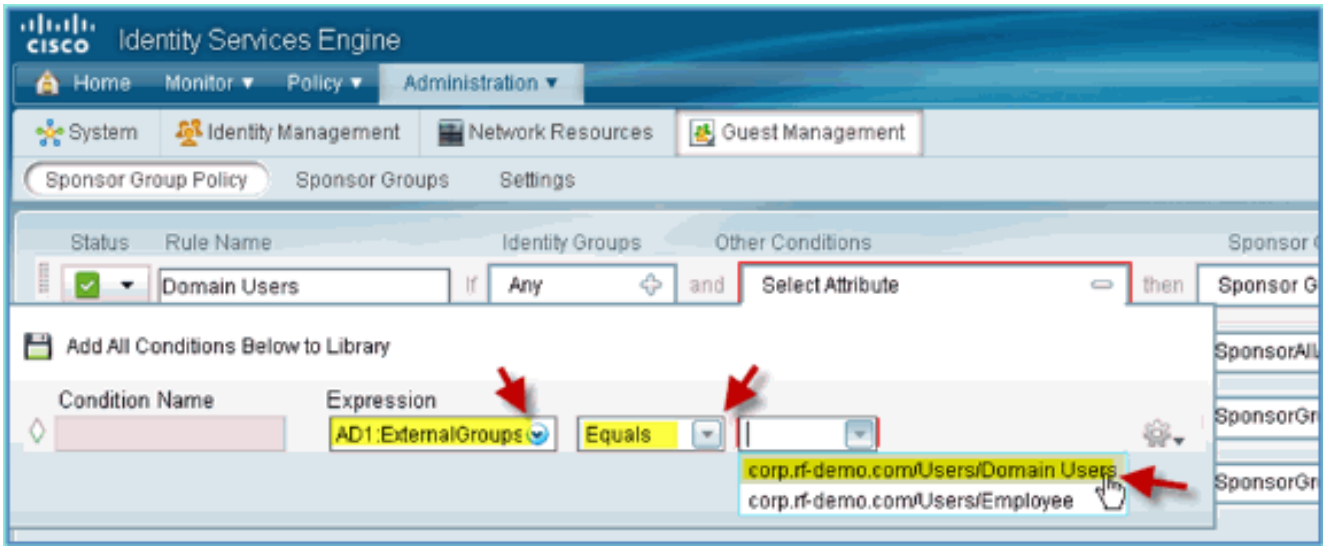
6. 新しいスポンサー グループ ポリシーに対して、次を作成します。[Rule Name（ルール名）]:Domain Users[Identity Groups]：任意その他の条件：（新規作成/詳細）> AD1



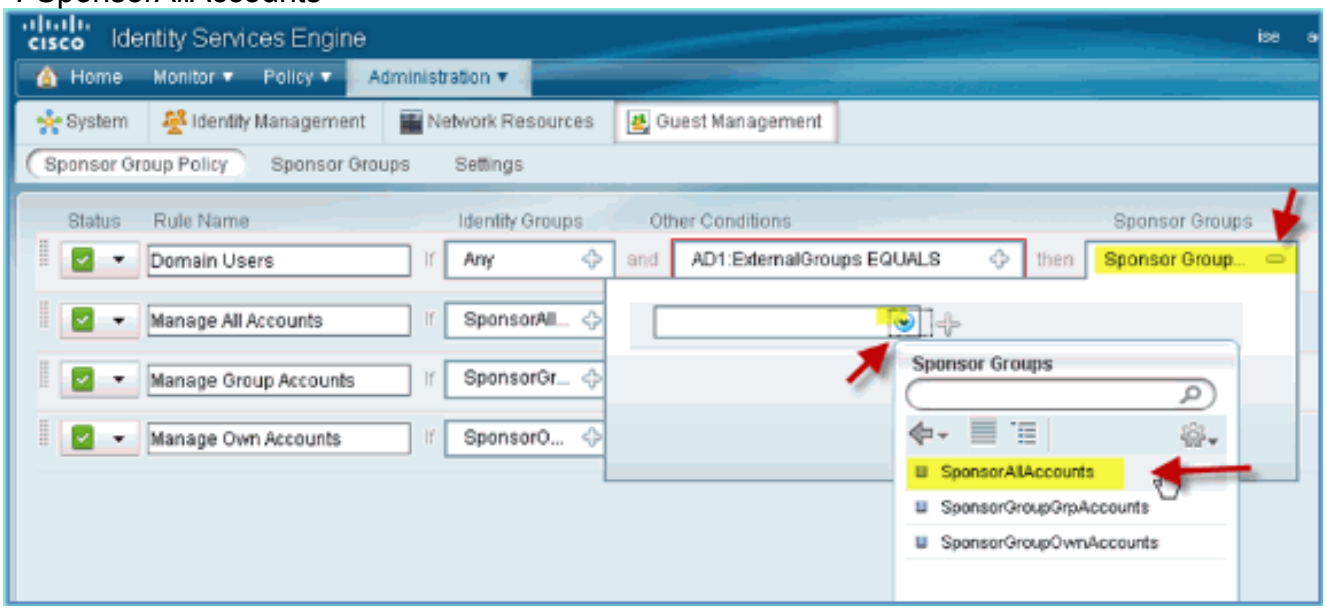
AD1：外部グループ



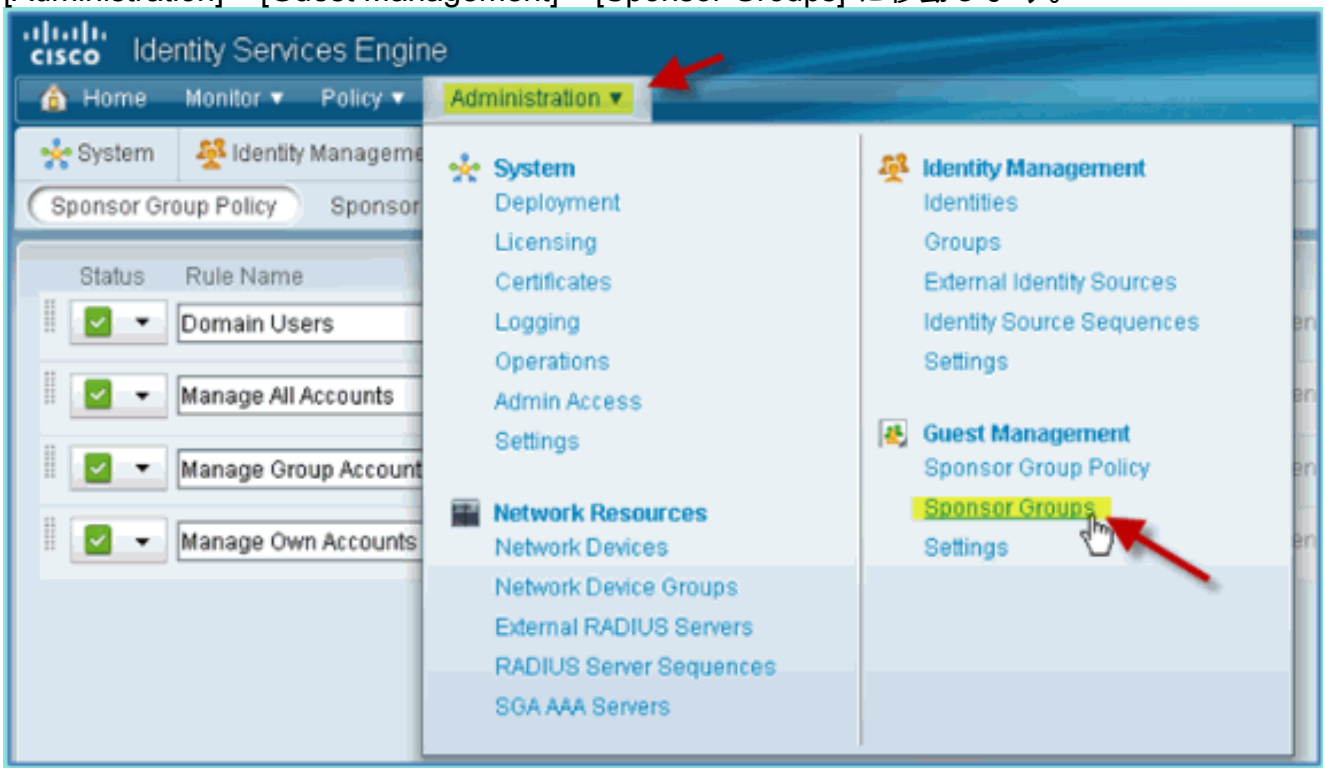
[AD1 External Groups] > [Equals] > corp.rf-demo.com/Users/Domain Users



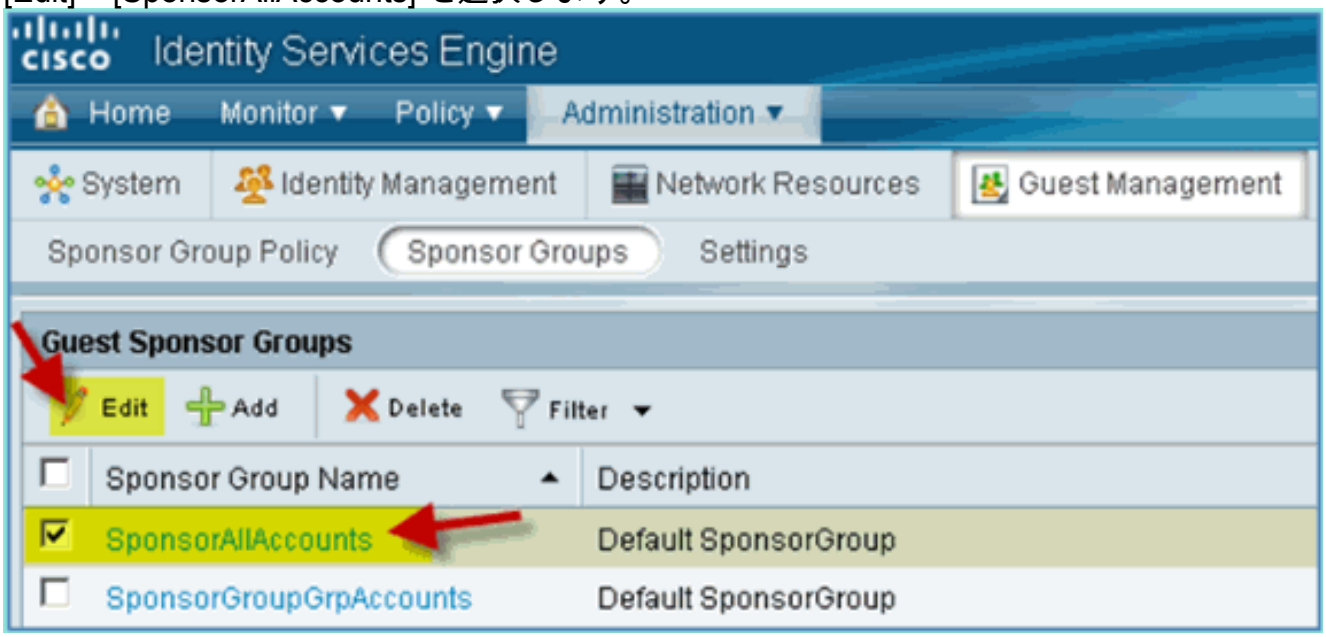
7. スポンサー グループでは、次のように設定します。スポンサーグループ
：SponsorAllAccounts



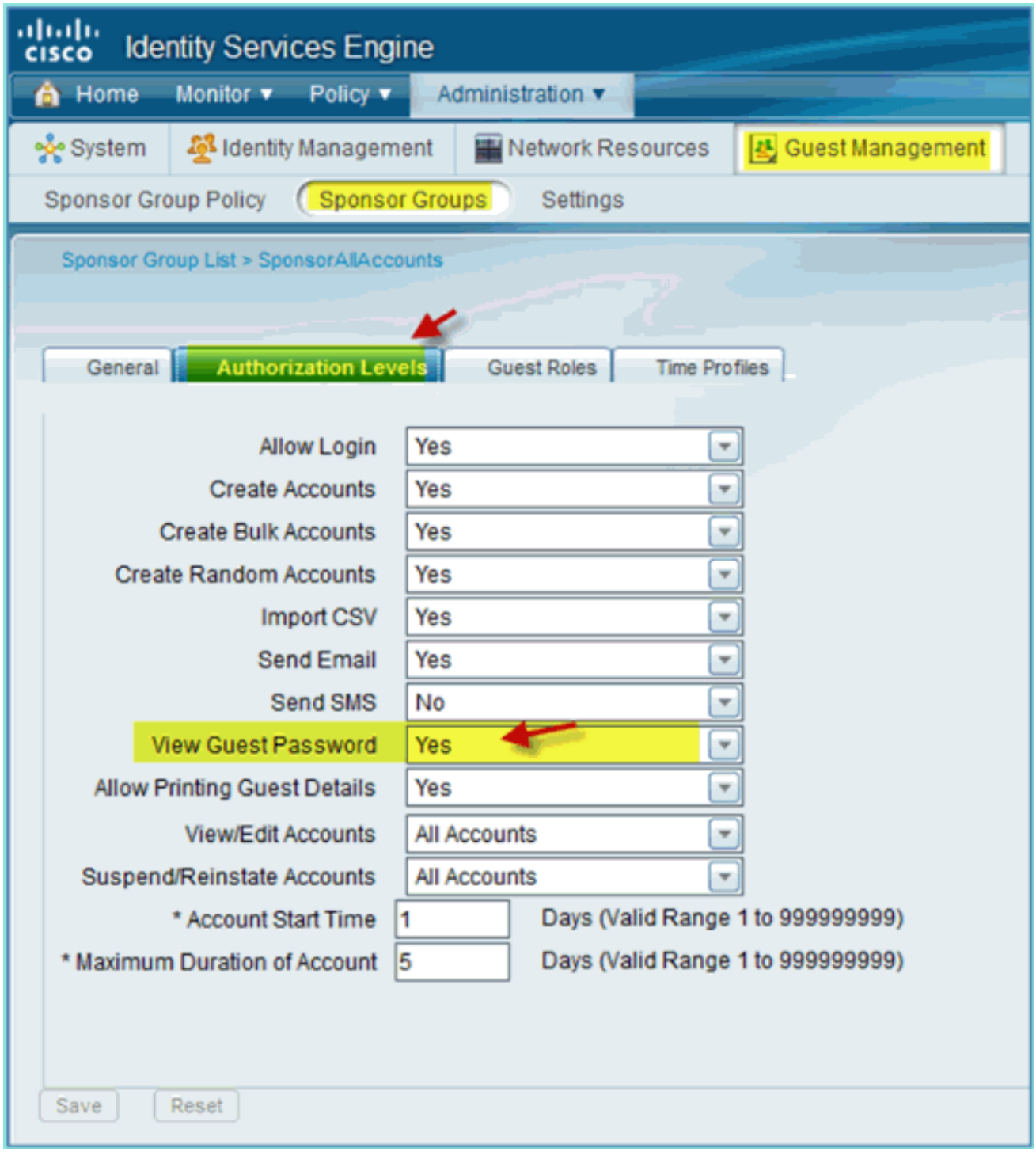
8. [Administration] > [Guest Management] > [Sponsor Groups] に移動します。



9. [Edit] > [SponsorAllAccounts] を選択します。



10. [Authorization Levels] を選択し、次のように設定します。ゲストパスワードの表示：はい



スイッチ上での SPAN の設定

SPAN の設定：ISE の管理/プローブ インターフェイスは、WLC 管理インターフェイスに隣接する L2 です。スイッチは、SPAN、および従業員やゲスト インターフェイス VLAN などの他のインターフェイス向けに設定できます。

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

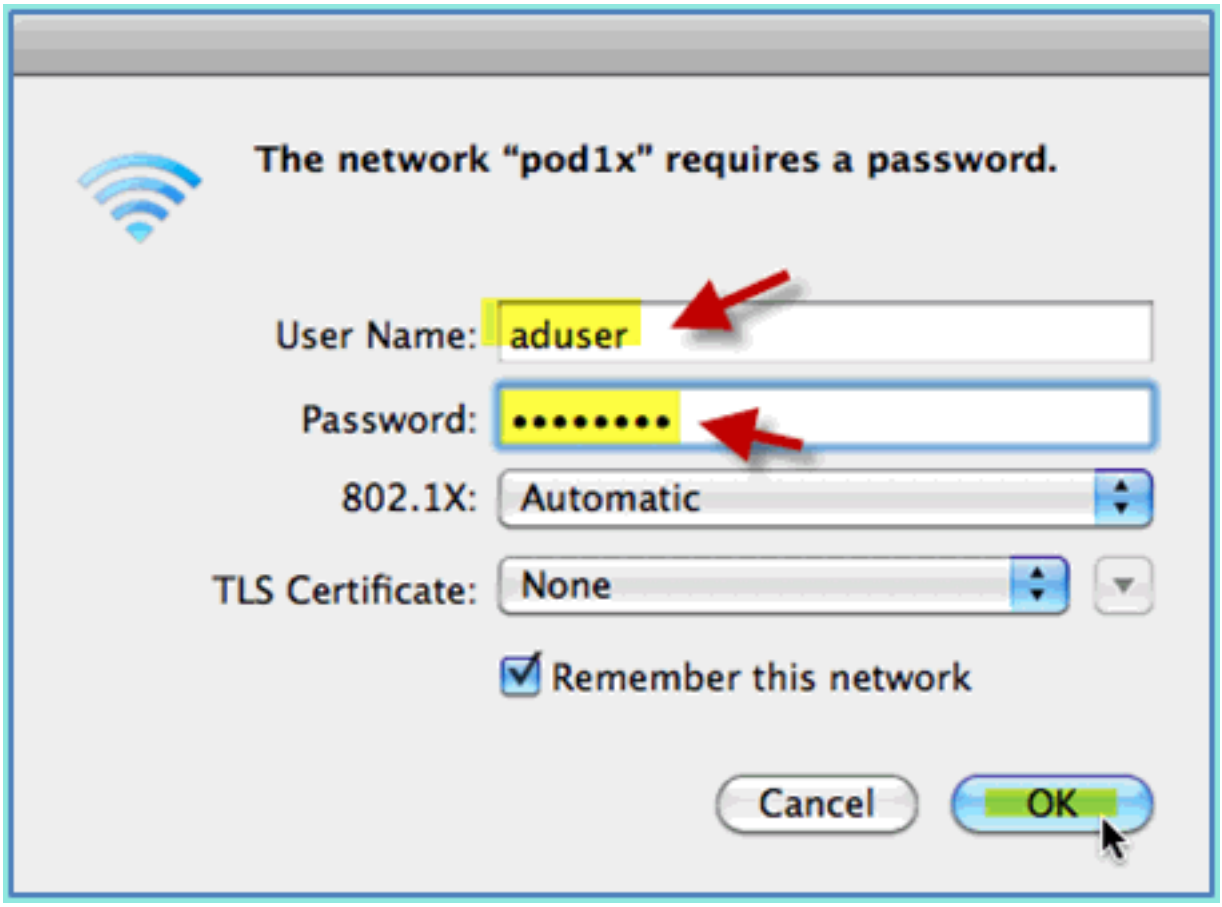
リファレンス：Apple MAC OS Xのワイヤレス認証

Apple Mac OS X ワイヤレス ラップトップを使用して、内部ユーザ（または統合された AD ユー

ザ）として認証された SSID 経由で WLC に関連付けます。該当しない手順は飛ばしてください。

1. Mac で、WLAN の設定に移動します。Wi-Fi を有効にし、前の演習で作成した 802.1X 対応の POD SSID を選択し、接続します。

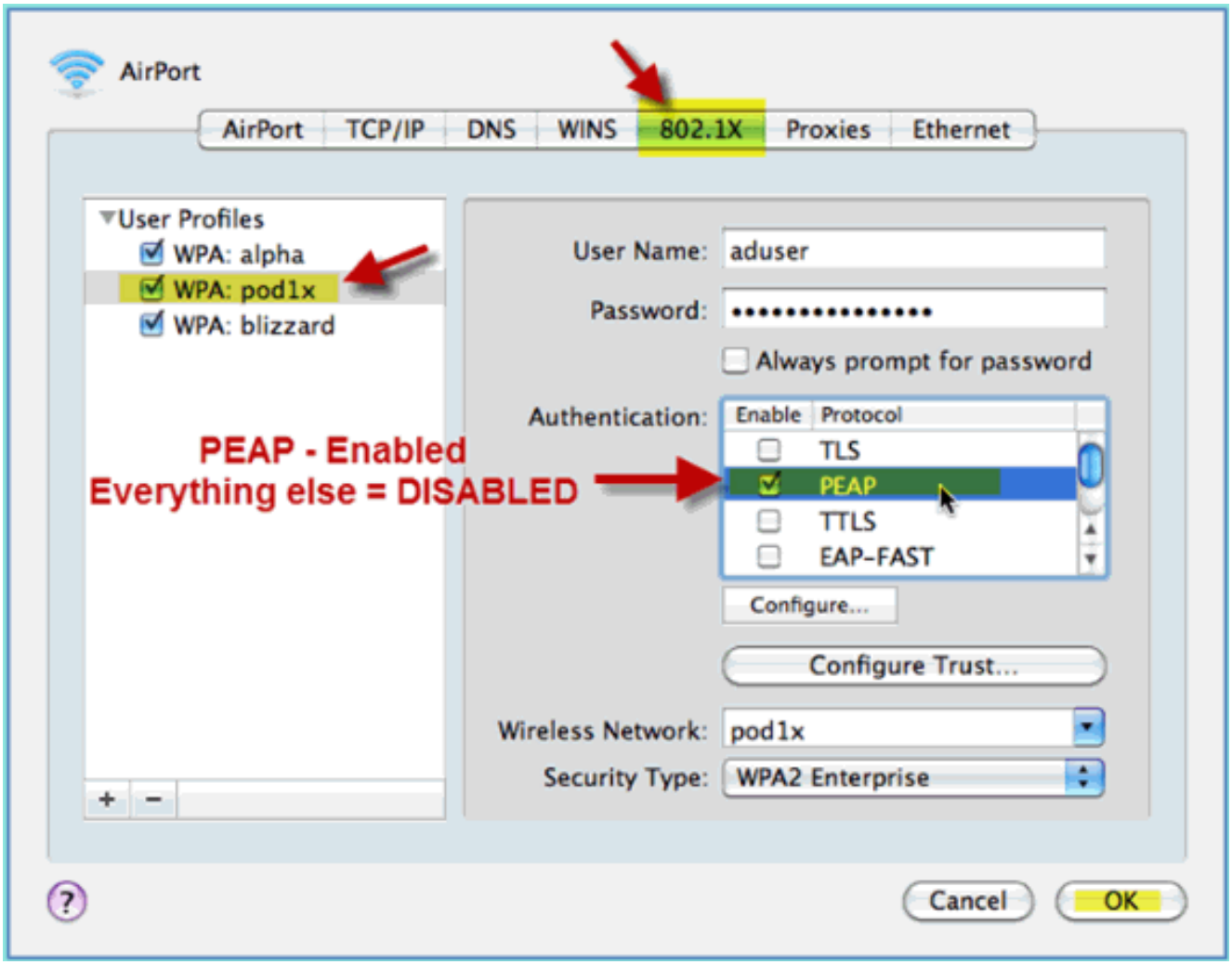
2. 接続するには、次の情報を入力します。ユーザ名：aduser（ADを使用している場合）、employee（内部 – 従業員）、contractor（内部 – 請負業者）パスワード：XXXX802.1X：自動TLS証明書：なし



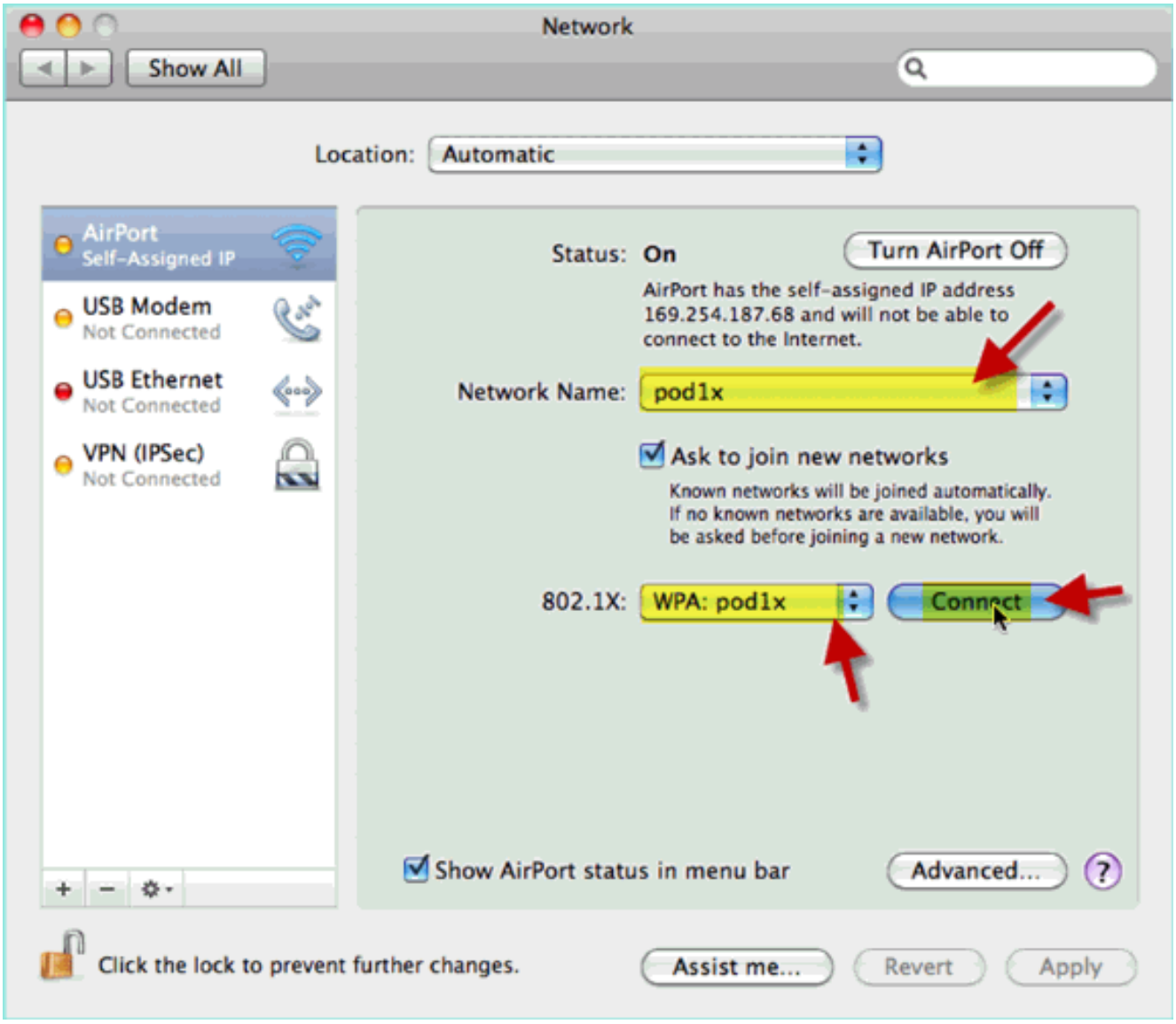
この時点では、ラップトップが接続されないことがあります。加えて、ISE は次のように失敗したイベントをスローできます。

```
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of
an unknown CA in the client certificates chain
```

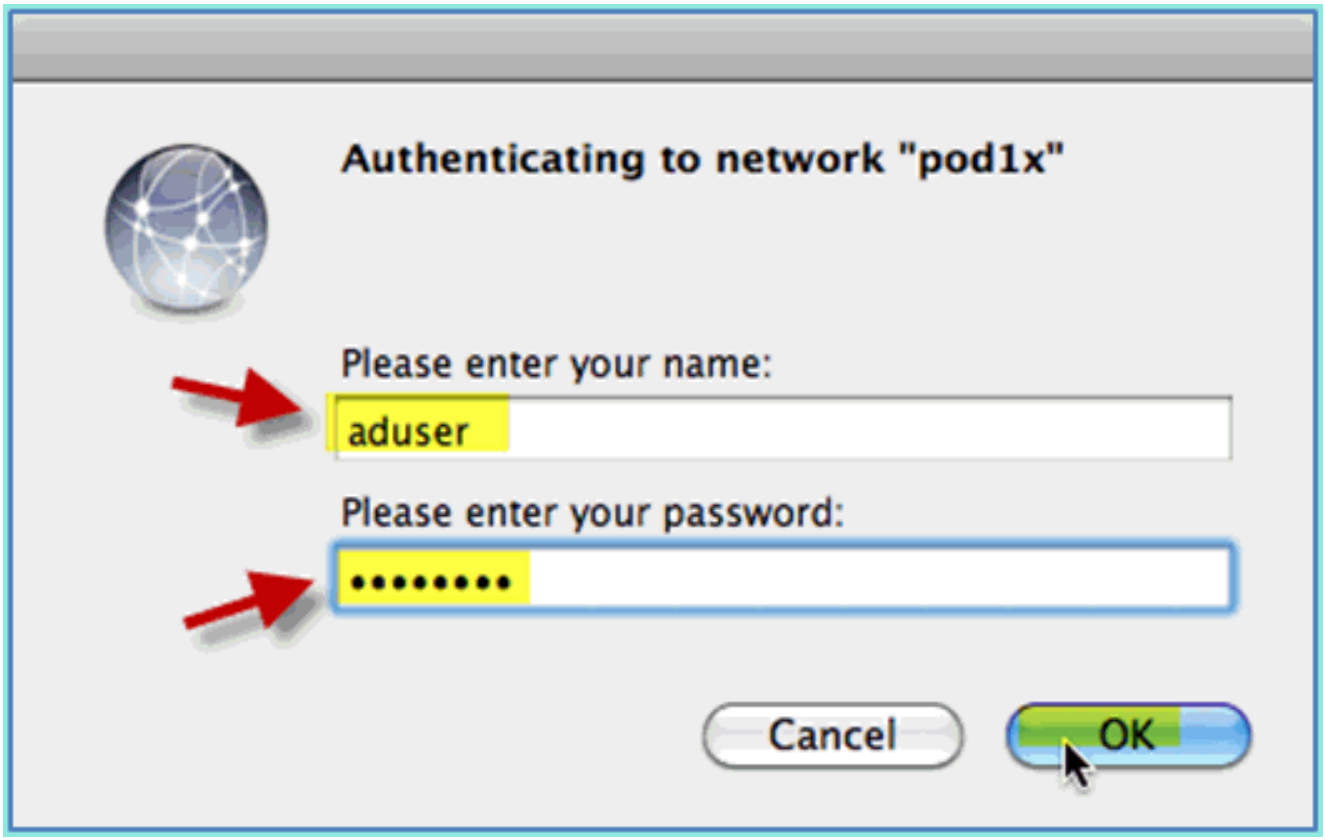
3. [System Preference] > [Network] > [Airport] > [802.1X] **設定に移動し、新しい POD SSID/WPA プロファイル認証を次のように設定します。**TLS：無効 PEAP:EnabledTTLS:DisabledEAP-FAST：無効



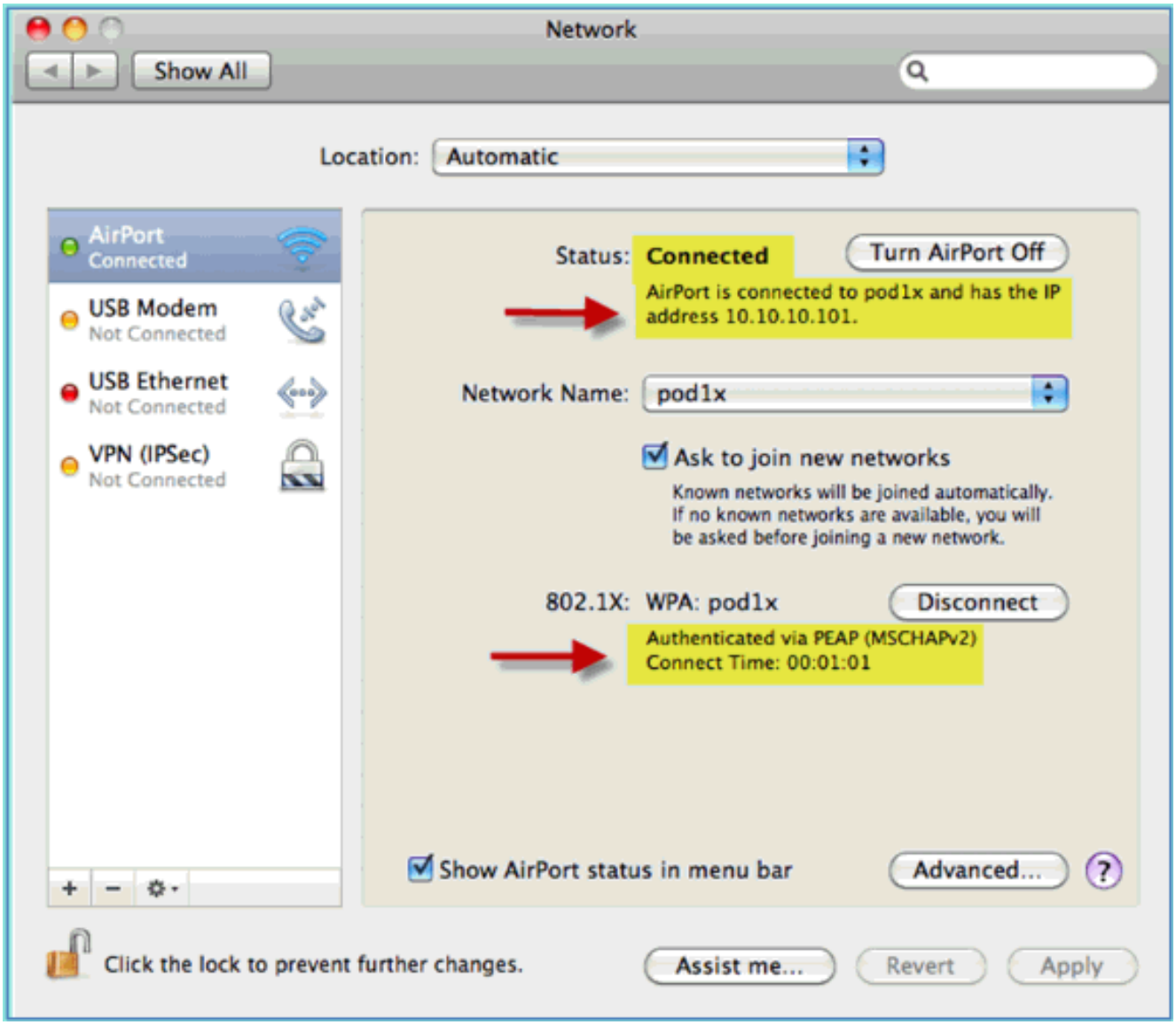
4. [OK] をクリックして続行し、設定を保存します。
5. [ネットワーク] 画面で、適切な SSID + 802.1X WPA プロファイルを選択し、[Connect] をクリックします。



6. ユーザ名およびパスワードを入力するように要求される場合があります。AD ユーザとパスワード（aduser/XXXX）を入力し、[OK] をクリックします。



クライアントは、有効な IP アドレスを持つ PEAP 経由で [Connected] **と示されているはずです。**

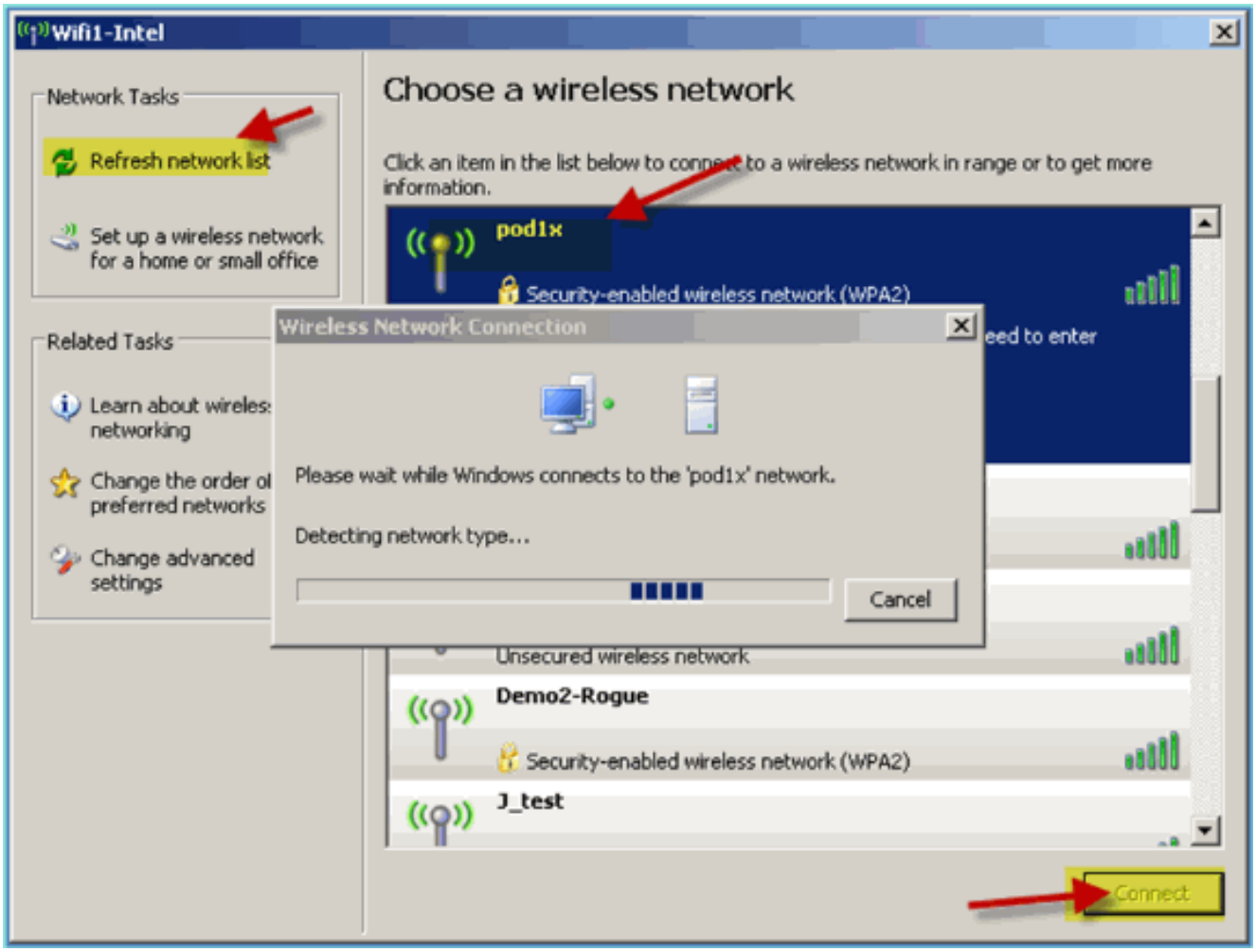


リファレンス：Microsoft Windows XPのワイヤレス認証

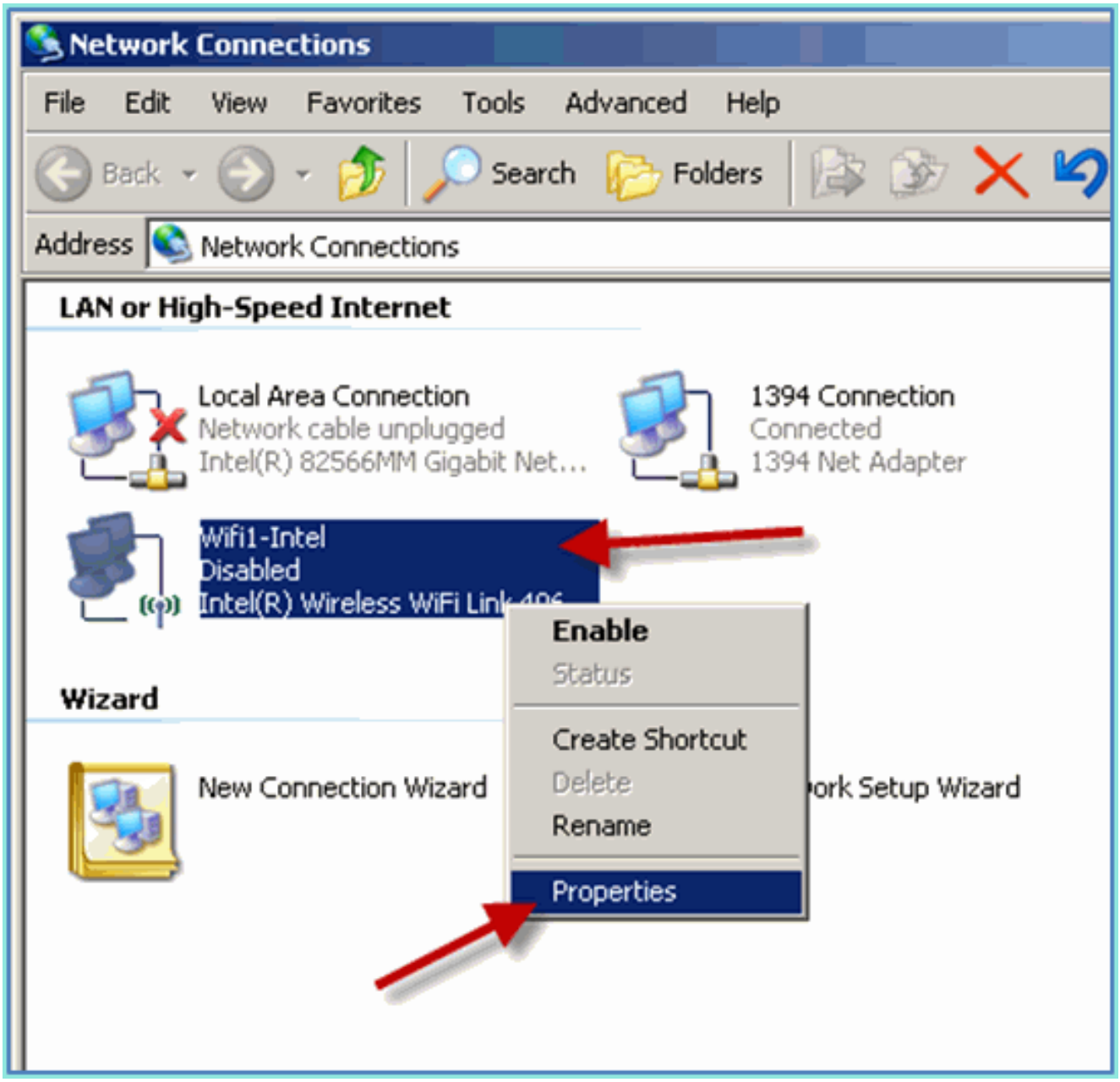
Windows XP ワイヤレス ラップトップを使用して、内部ユーザ (または統合された AD ユーザ) として認証された SSID 経由で WLC に関連付けます。該当しない手順は飛ばしてください。

次のステップを実行します。

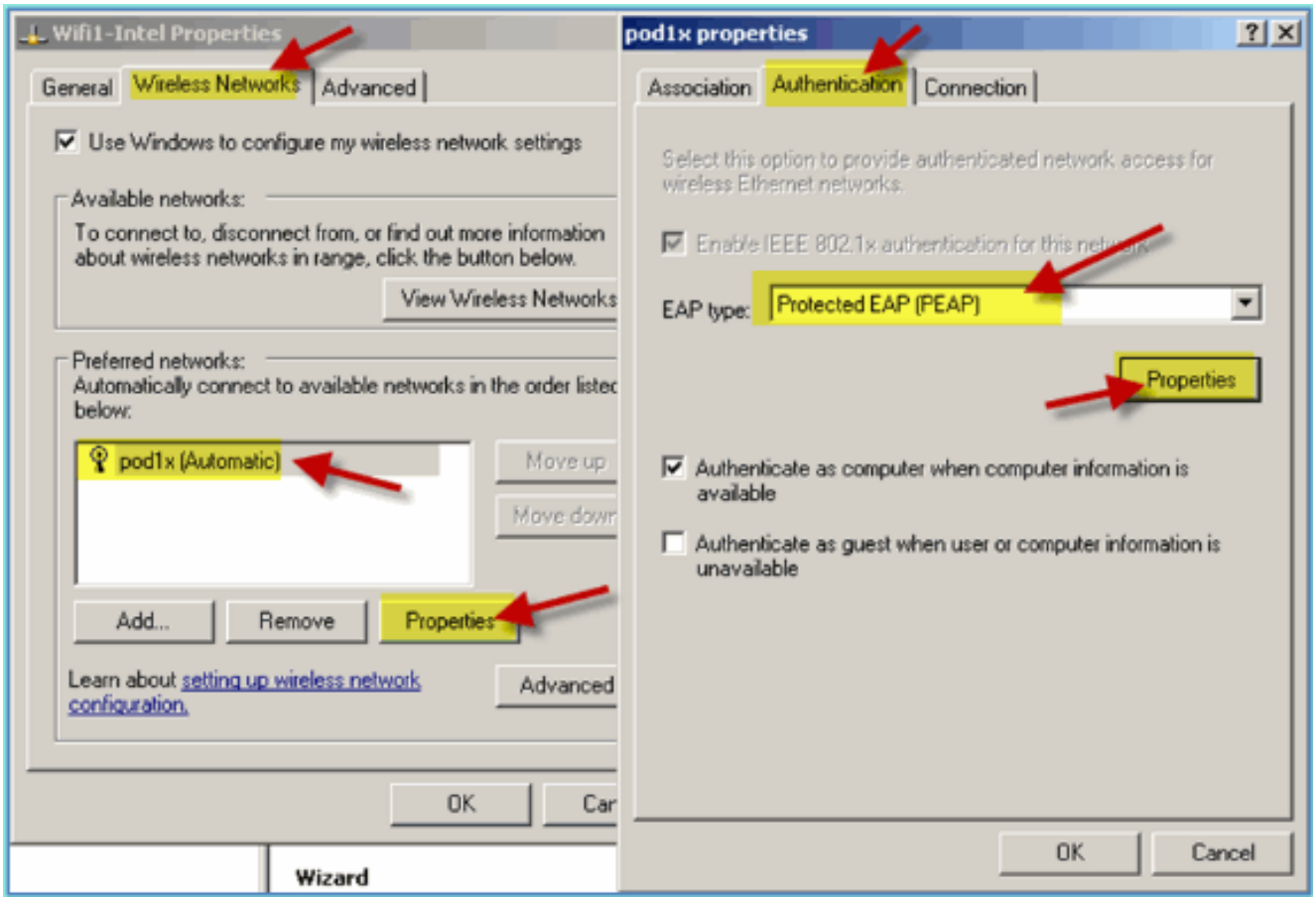
1. ラップトップで、WLAN の設定に移動します。Wi-Fi を有効にし、前の演習で作成した 802.1X 対応の POD SSID に接続します。



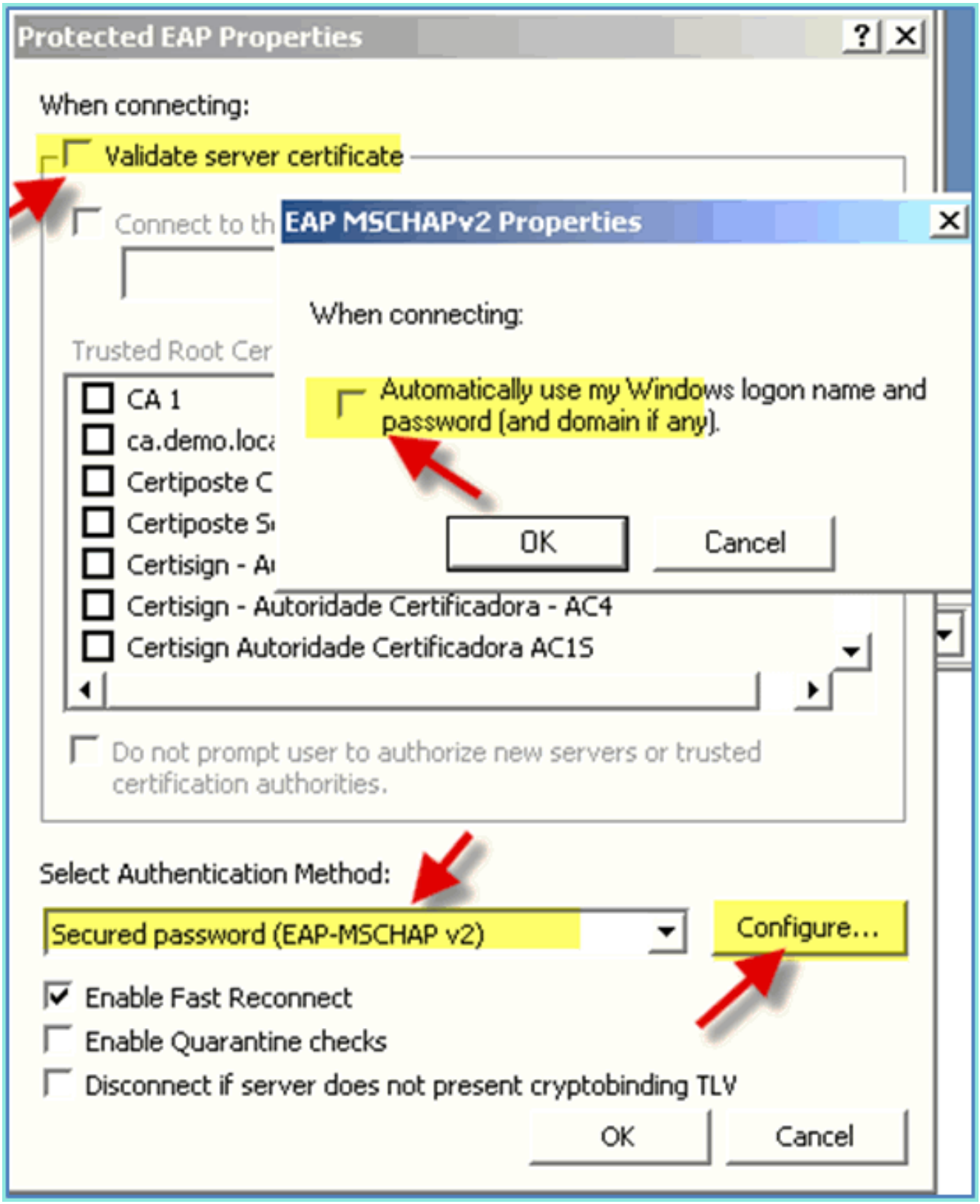
2. Wi-Fi インターフェイスのネットワーク プロパティにアクセスします。



3. [Wireless Networks] **タブに移動します。**ポッド SSID ネットワーク プロパティ > [Authentication] タブ > [EAP] タイプ = [Protected EAP（PEAP）] を選択します。



4. [EAP Properties] をクリックします。
5. 次の設定を行います。サーバー証明書の検証：無効[Authentication Method]:Secured password(EAP-MSCHAP
   v2)

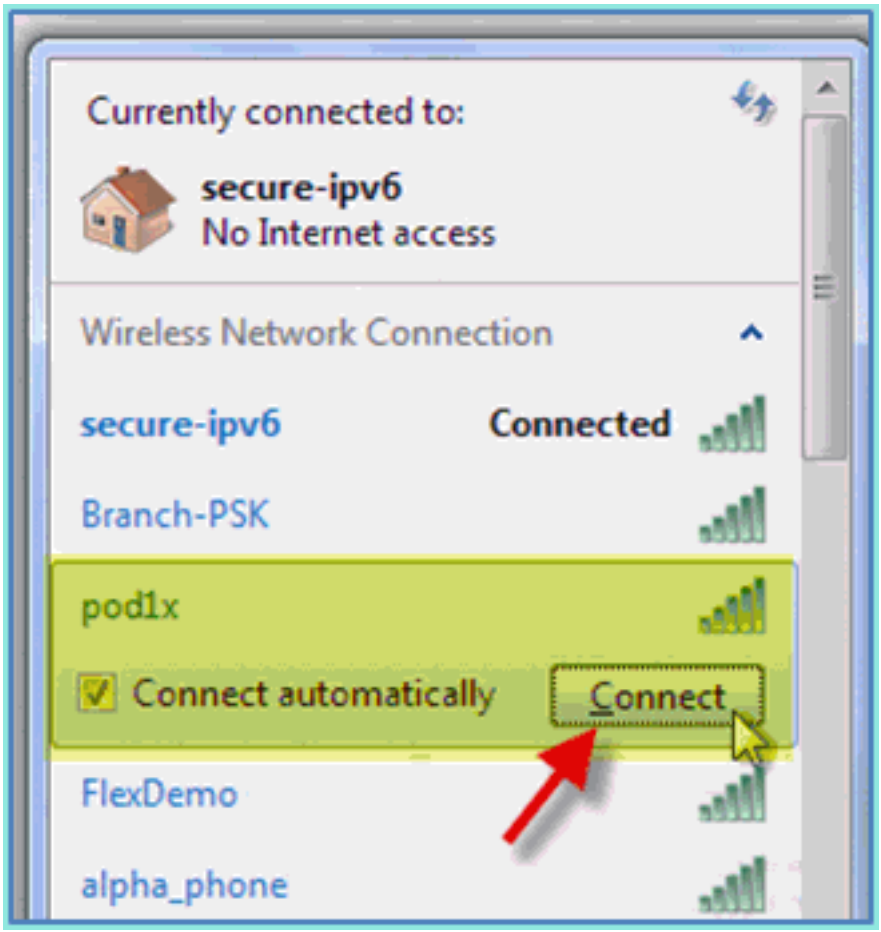


6. すべてのウィンドウで[OK] をクリックし、この設定タスクを完了します。
7. Windows XP クライアントから、ユーザ名とパスワードの入力が求められます。この例では、aduser/XXXX です。
8. ネットワーク接続、IP アドレスの割り当て（v4）を確認します。

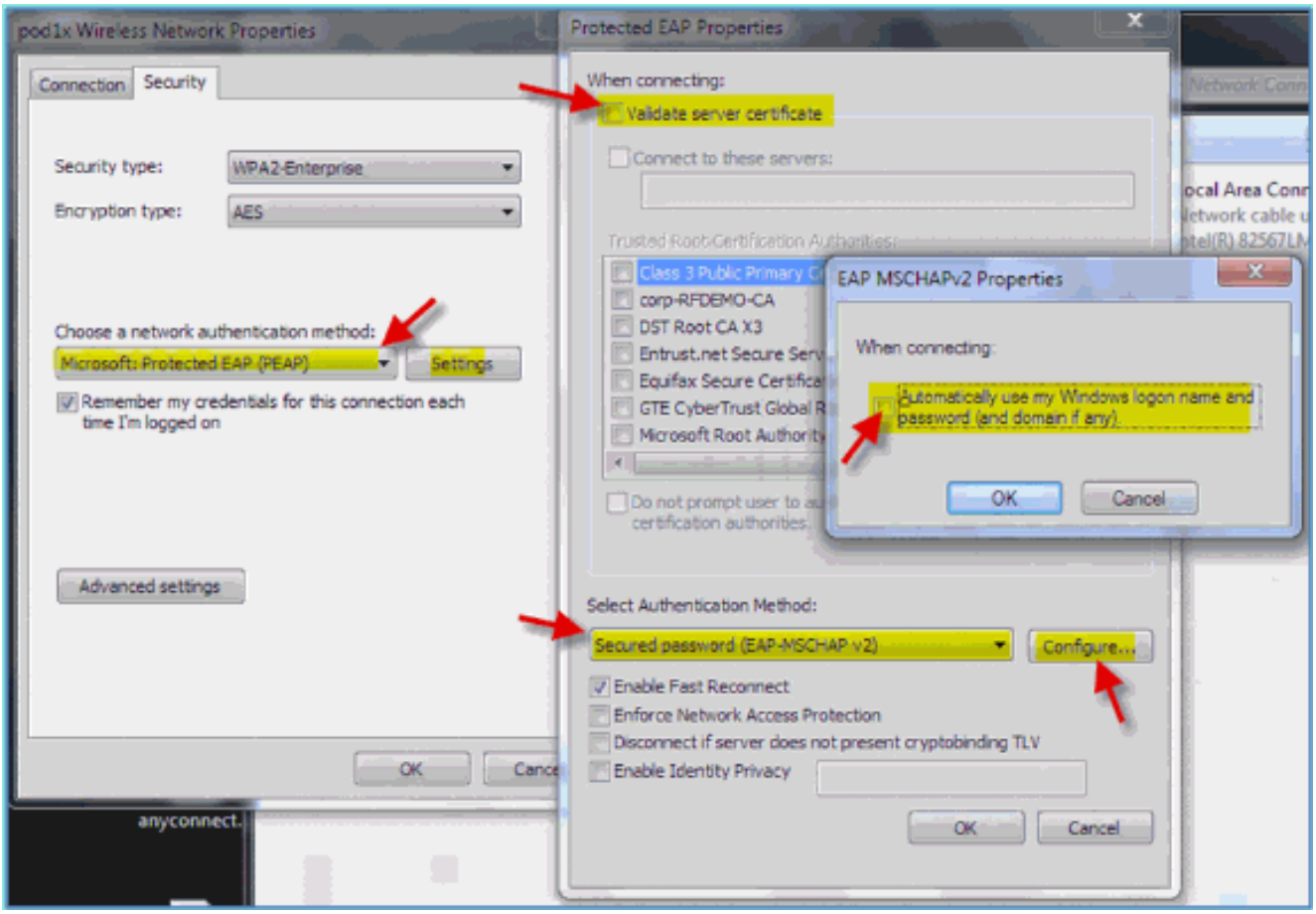
参考：Microsoft Windows 7のワイヤレス認証

Windows 7 ワイヤレス ラップトップを使用して、内部ユーザ（または統合された AD ユーザ）として認証された SSID 経由で WLC に関連付けます。

1. ラップトップで、WLAN の設定に移動します。Wi-Fi を有効にし、前の演習で作成した 802.1X 対応の POD SSID に接続します。



2. ワイヤレス マネージャにアクセスし、新しい POD ワイヤレス プロファイルを編集します。
3. 次の設定を行います。[Authentication Method]:PEAP資格情報を記憶する…：無効サーバー証明書の検証（詳細設定）：無効[Authentication Method (adv. Setting)]:EAP-MSCHAP v2[Automatically use my Windows logon...]：無効



関連情報

- 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。