WLAN ごとの認証用 ACS バージョン 5.2 および WLC の設定例

内容

概要

このドキュメントでは、サービス セット識別子（SSID）に基づいてワイヤレス LAN（WLAN）へのユーザ別アクセスを制限するための設定例について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ワイヤレス LAN コントローラ（WLC）と Lightweight アクセス ポイント（LAP）の基本動作のための設定方法
- Cisco Secure Access Control Server(ACS)の設定方法
- Lightweight アクセス ポイント プロトコル（LWAPP）とワイヤレスのセキュリティ方式

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。

- ファームウェアバージョン7.4.110が稼働するCisco 5500シリーズWLC
- Cisco 1142 シリーズ LAP
- Cisco Secure ACSサーババージョン5.2.0.26.11

設定

この設定用にデバイスを設定するには、次の手順を実行します。

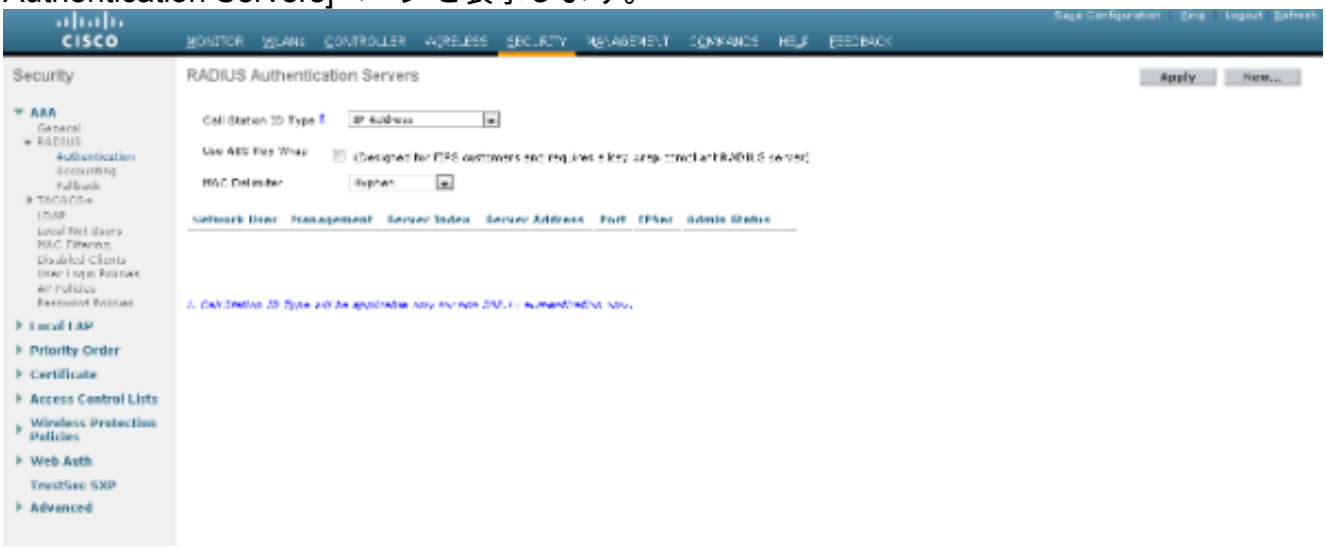
1. 2 つの WLAN と RADIUS サーバ用の WLC を設定します。

2. Cisco Secure ACS を設定します。
3. ワイヤレスクライアントを設定し、設定を確認します。

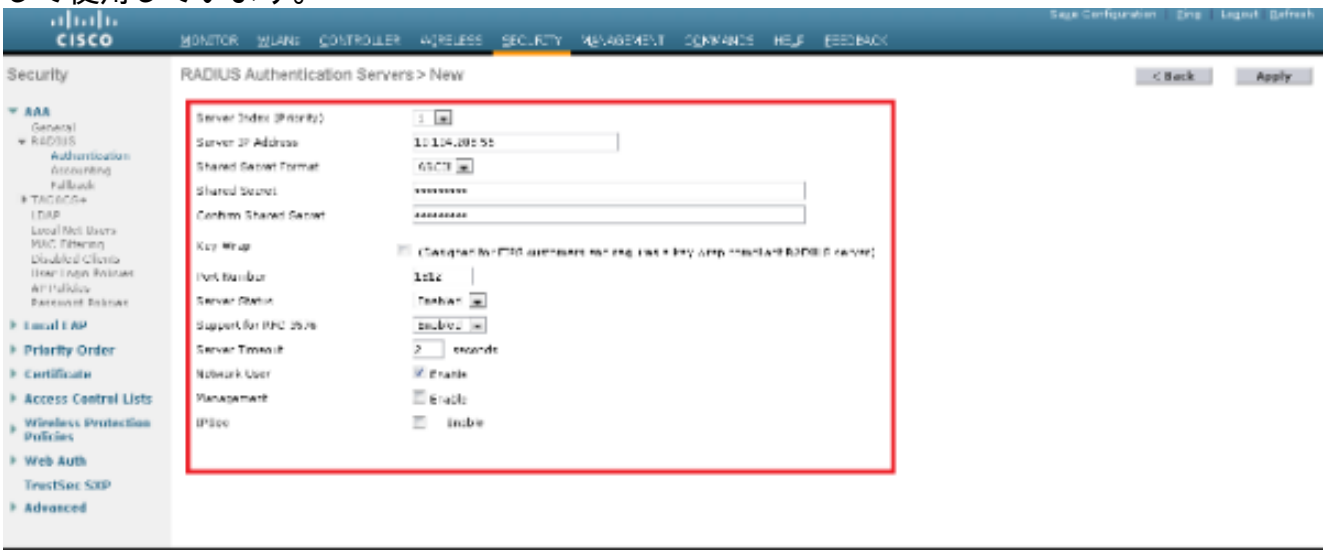
WLC の設定

このセットアップのために WLC を設定するには、次の手順を実行します。

1. ユーザクレデンシャルを外部RADIUSサーバに転送するようにWLCを設定します。設定すると、外部 RADIUS サーバ（この場合は Cisco Secure ACS）は、ユーザ クレデンシャルを検証し、ワイヤレス クライアントにアクセス権を付与します。次のステップを実行します。コントローラのGUIから**[Security] > [RADIUS Authentication]**の順に選択して、[RADIUS Authentication Servers]ページを表示します。



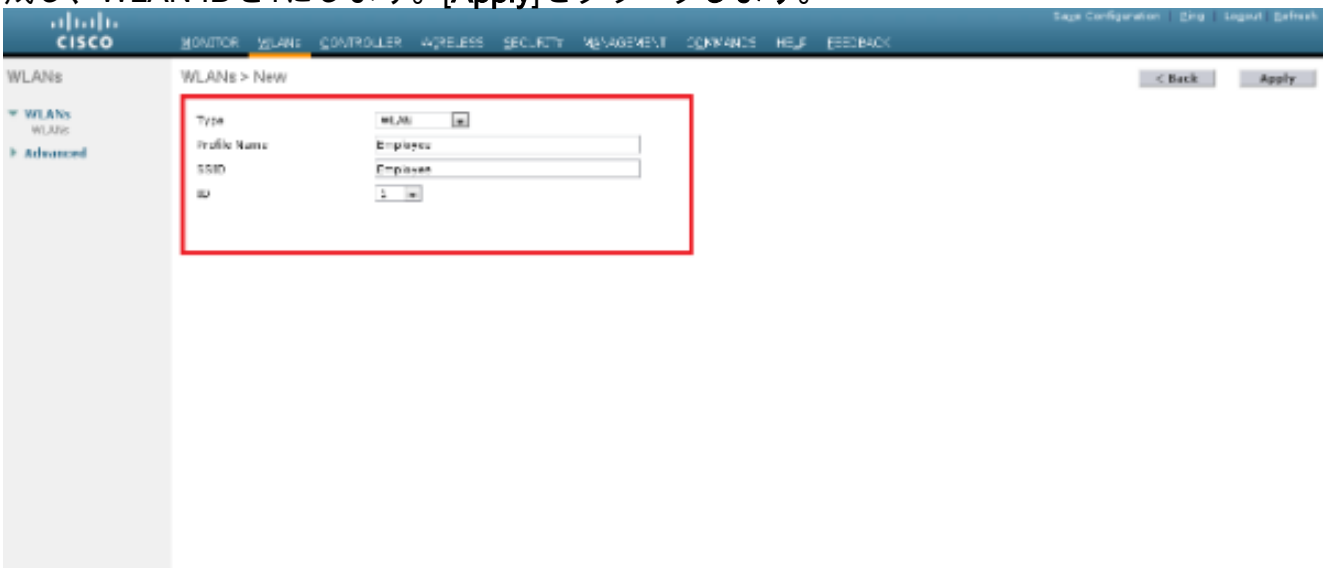
RADIUS サーバ パラメータを定義するには、[New] をクリックします。 RADIUS サーバ IP アドレス、共有秘密、ポート番号、サーバ ステータスなどのパラメータがあります。[Network User]チェックボックスと[Management]チェックボックスでは、RADIUSベースの認証が管理ユーザとネットワークユーザに適用されるかどうかが決まります。この例では、次のように、Cisco Secure ACS を IP アドレスが 10.104.208.56 である RADIUS サーバとして使用しています。



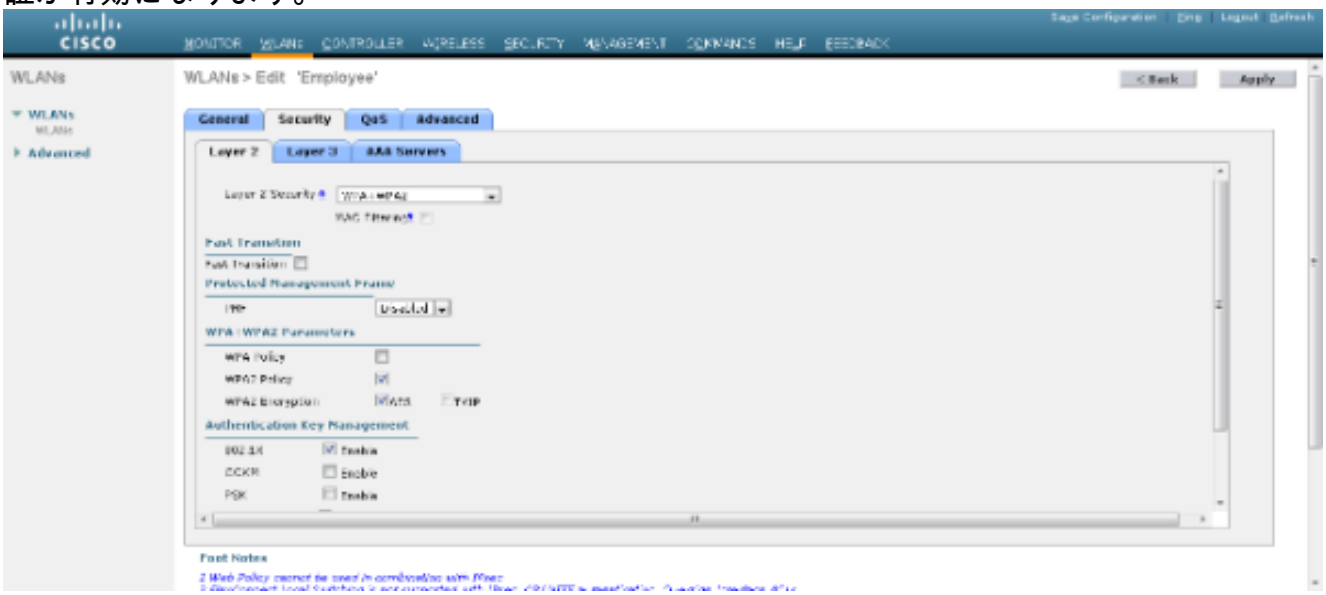
[Apply] をクリックします。

2. SSID **Employee**の従業員に1つのWLANを設定し、SSID Contractorの請負業者用にもう1つのWLANを設定するには、次の手順を実**行します**。 WLAN を作成するために、コントローラの GUI で [WLANs] をクリックします。WLANs ウィンドウが表示されます。このウィン

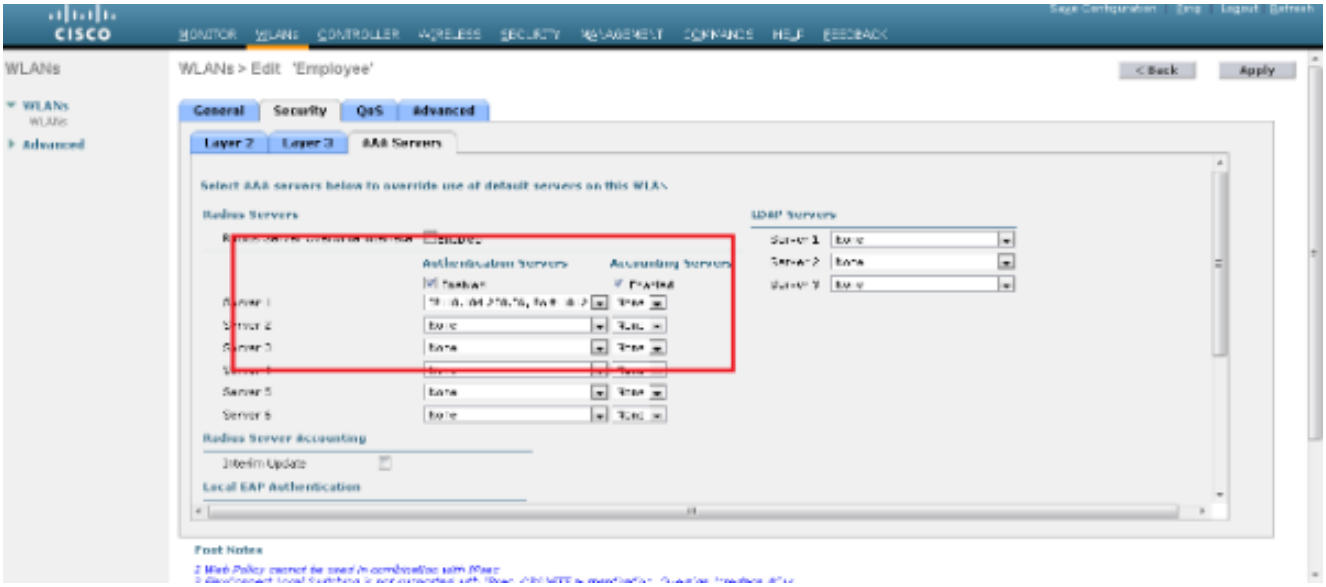
ドウには、コントローラに設定されている WLAN の一覧が表示されます。新しい WLAN を設定するために [New] をクリックします。この例では、Employeeという名前のWLANを作成し、WLAN IDを1にします。[Apply]をクリックします。



[WLAN] > [Edit]ウィンドウを選択し、WLAN固有のパラメータを定義します。 [Layer 2 Security]タブで、[802.1x]を選択します。デフォルトでは、レイヤ 2 セキュリティ オプションは 802.1x です。これにより、WLANの802.1 x/Extensible Authentication Protocol(EAP)認証が有効になります。



[AAA servers]タブで、[RADIUS Servers]のドロップダウンリストから適切なRADIUSサーバを選択します。WLAN ネットワークの要件に基づいて、その他のパラメータを変更できます。[Apply] をクリックします。



同様に、請負業者のWLANを作成するには、手順b ~ dを繰り返します。

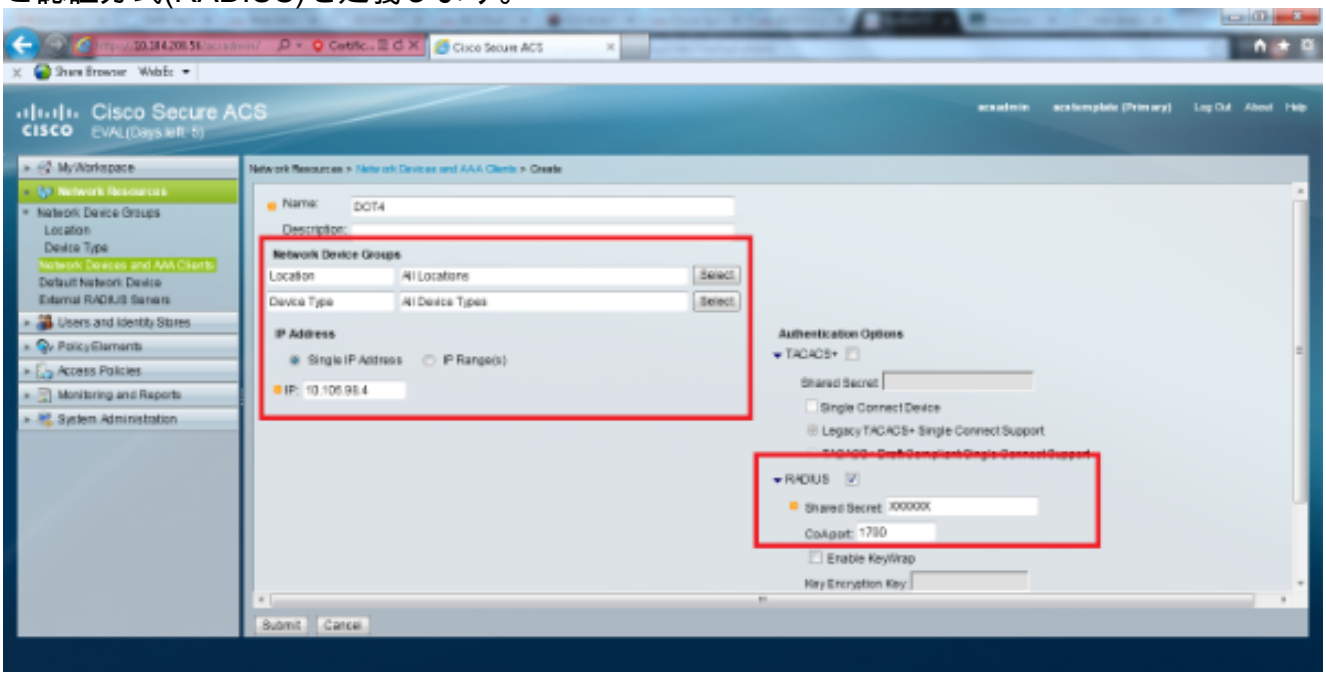
Cisco Secure ACS の設定

Cisco Secure ACS サーバで、次の操作を実行します。

1. WLC を AAA クライアントとして設定します。
2. SSIDベース認証のユーザデータベース (クレデンシャル) を作成します。
3. EAP 認証をイネーブルにします。

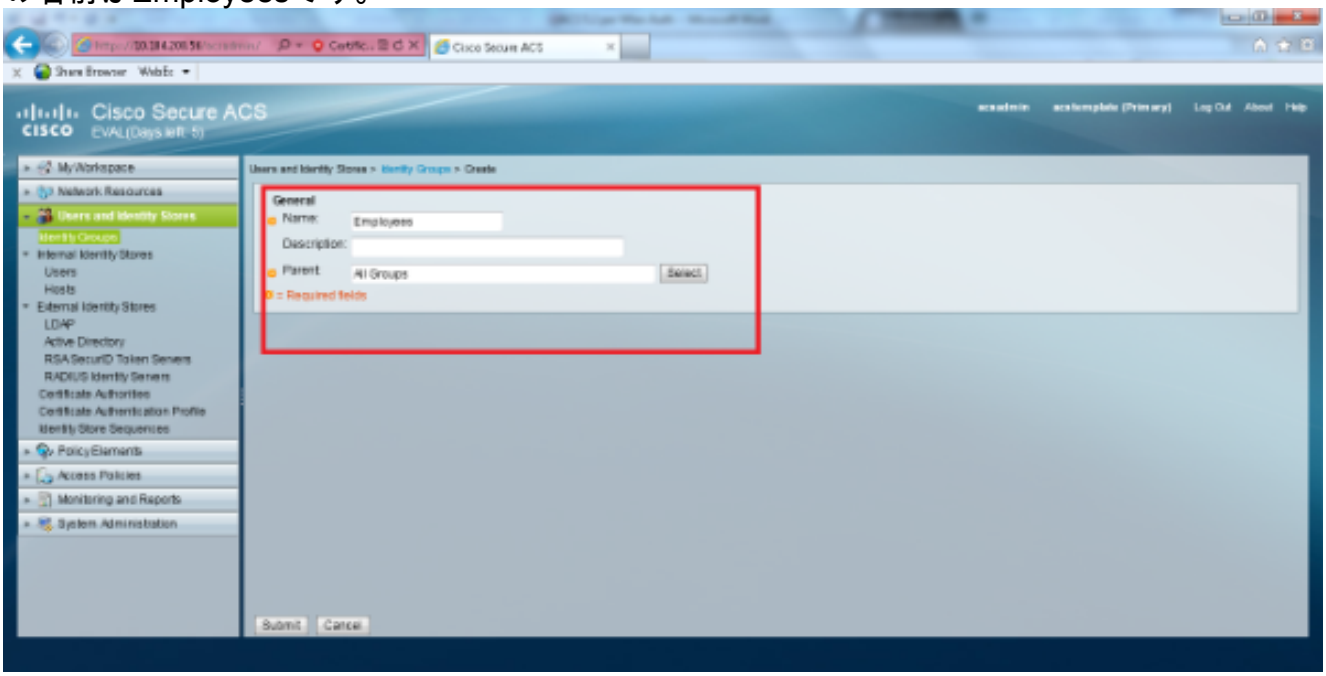
Cisco Secure ACS で次の手順を実行します。

1. コントローラをACSサーバ上のAAAクライアントとして定義するには、ACS GUIから**[Network Resources] > [Network Devices and AAA Clients]**を選択します。[Network Devices and AAA Clients]で**[Create]をクリックします。**
2. [Network Configuration]ページが表示されたら、WLCの名前、IPアドレス、および共有秘密と認証方式(RADIUS)を定義します。

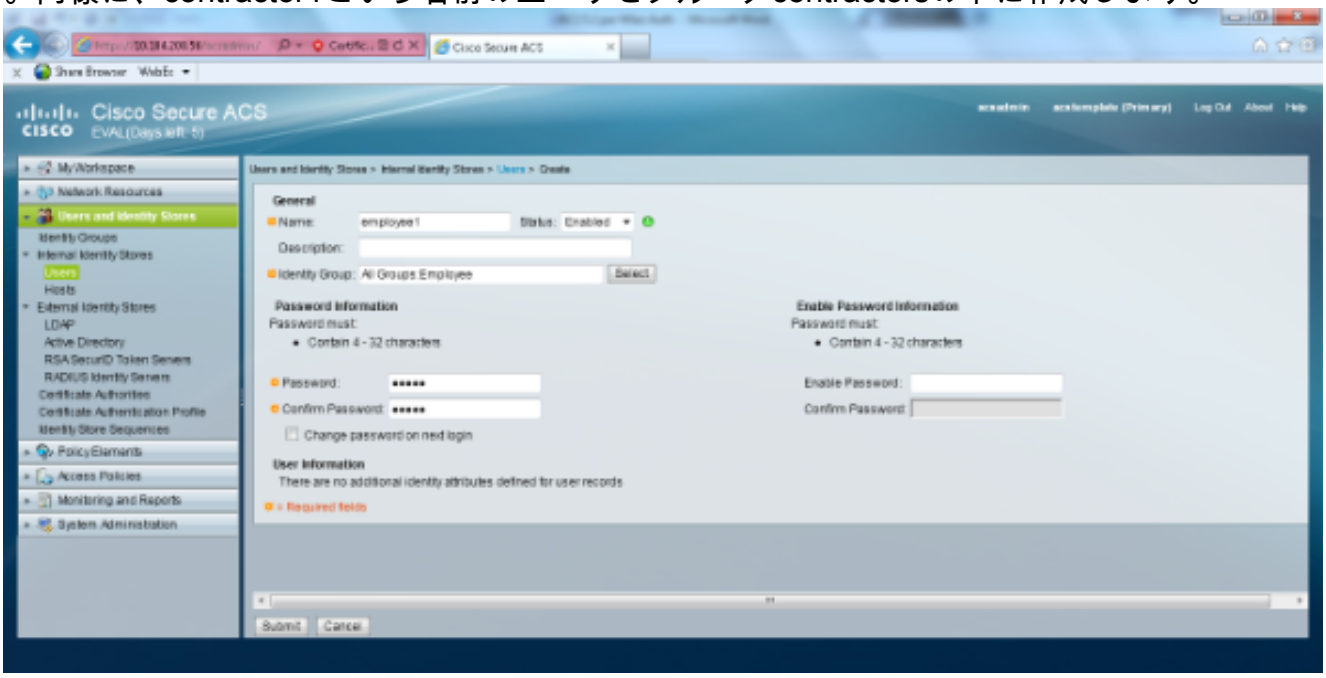


3. ACS GUIから**[Users and Identity Stores] > [Identity Groups]**を選択します。従業員および請負業者の各グループを作成し、「作成」をクリ**ックします。**この例では、作成したグループ

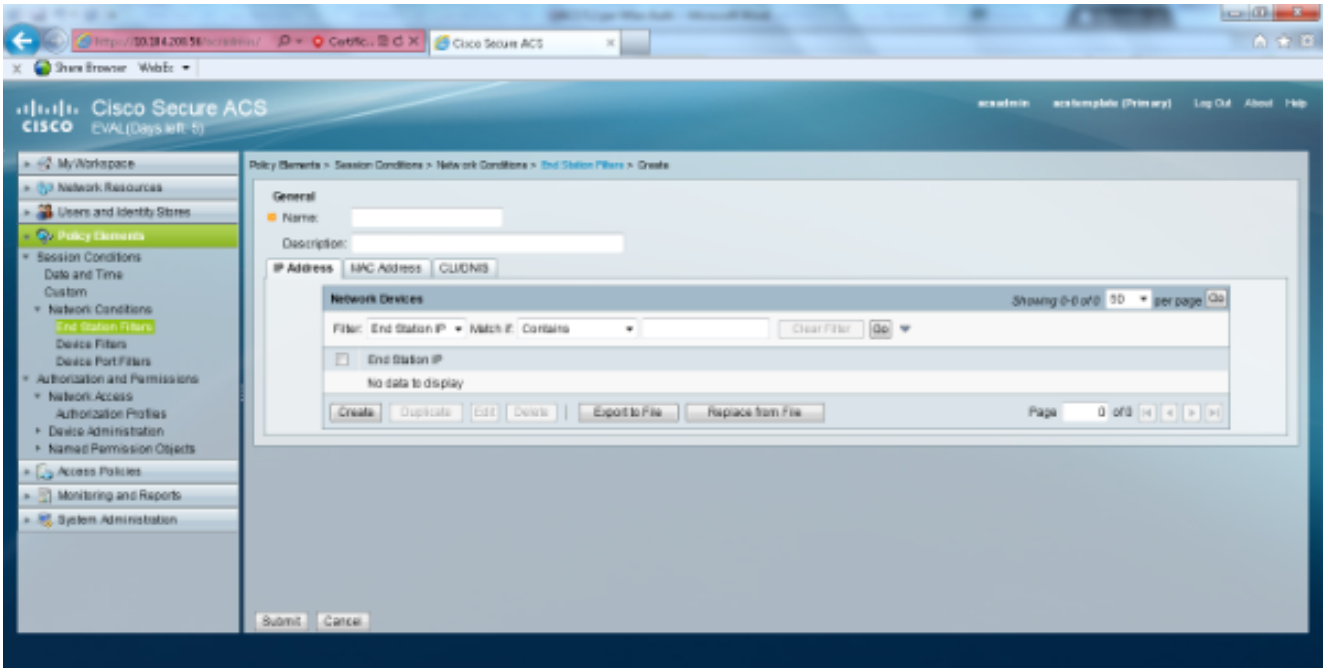
の名前はEmployeesです。



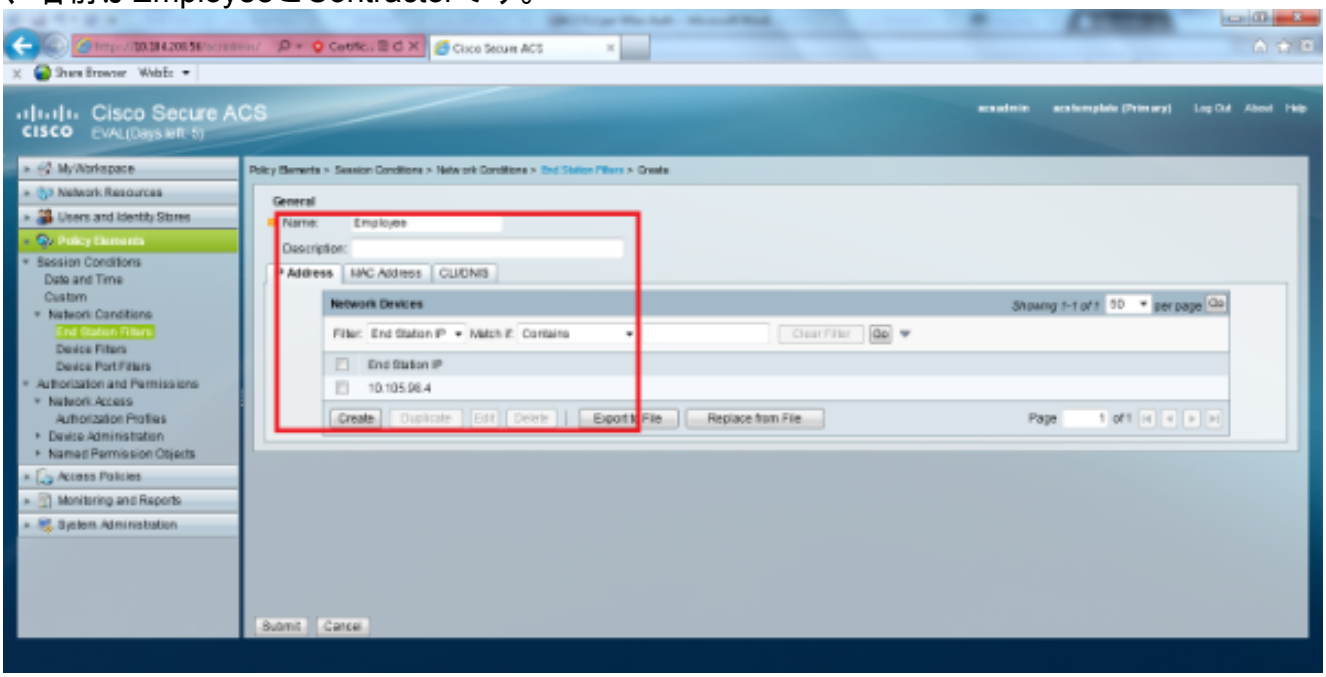
4. 「ユーザーとIDストア」>「内部IDストア」を選択します。[Create]をクリックし、ユーザ名を入力します。これらを正しいグループに配置し、パスワードを定義し、[送信]をクリックします。この例では、グループEmployeeのemployee1という名前のユーザが作成されます。同様に、contractor1という名前のユーザをグループcontractorsの下に作成します。



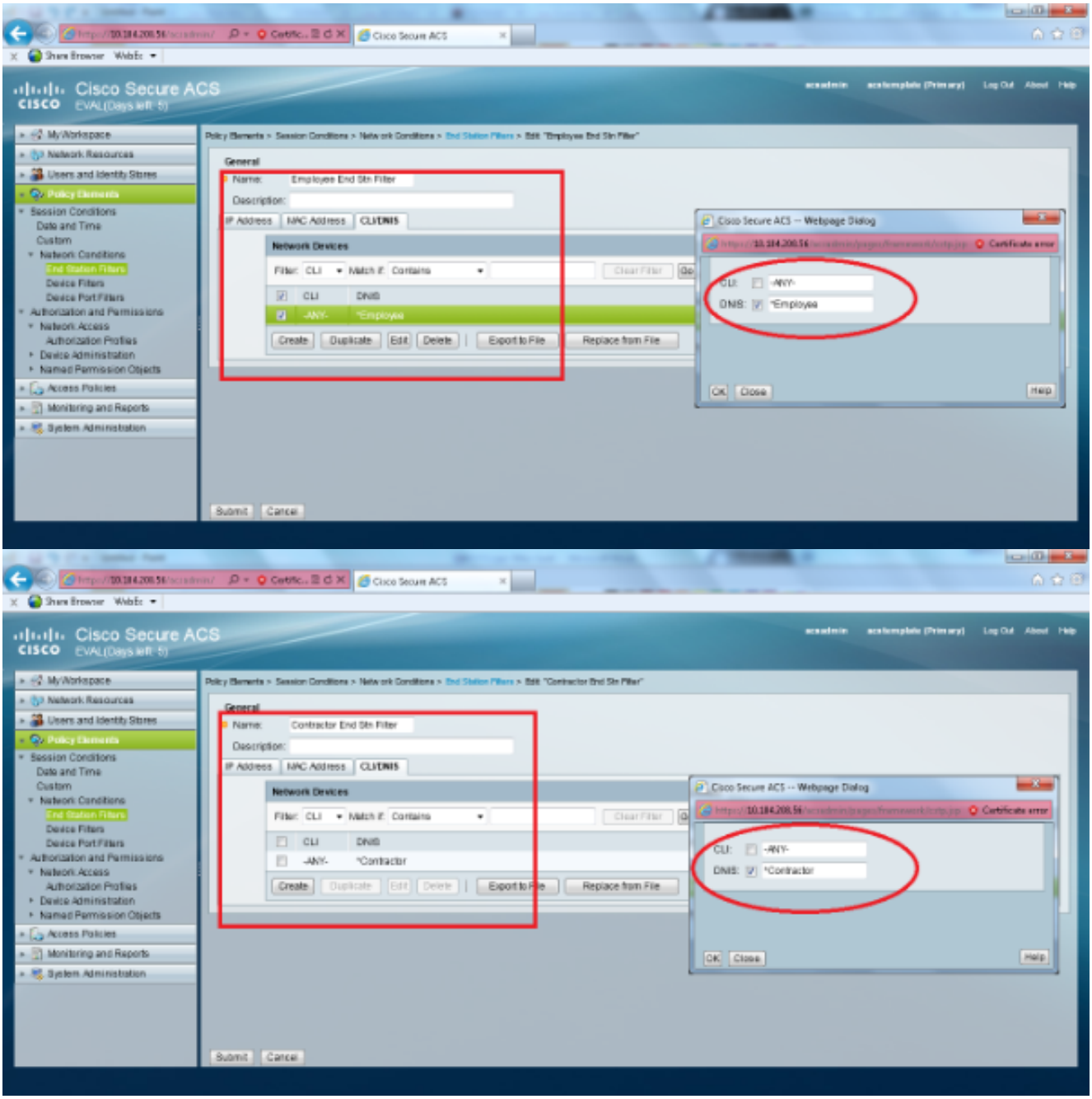
5. [Policy Elements] > [Network Conditions] > [End Station Filters]を選択します。[作成（Create）] をクリックします。



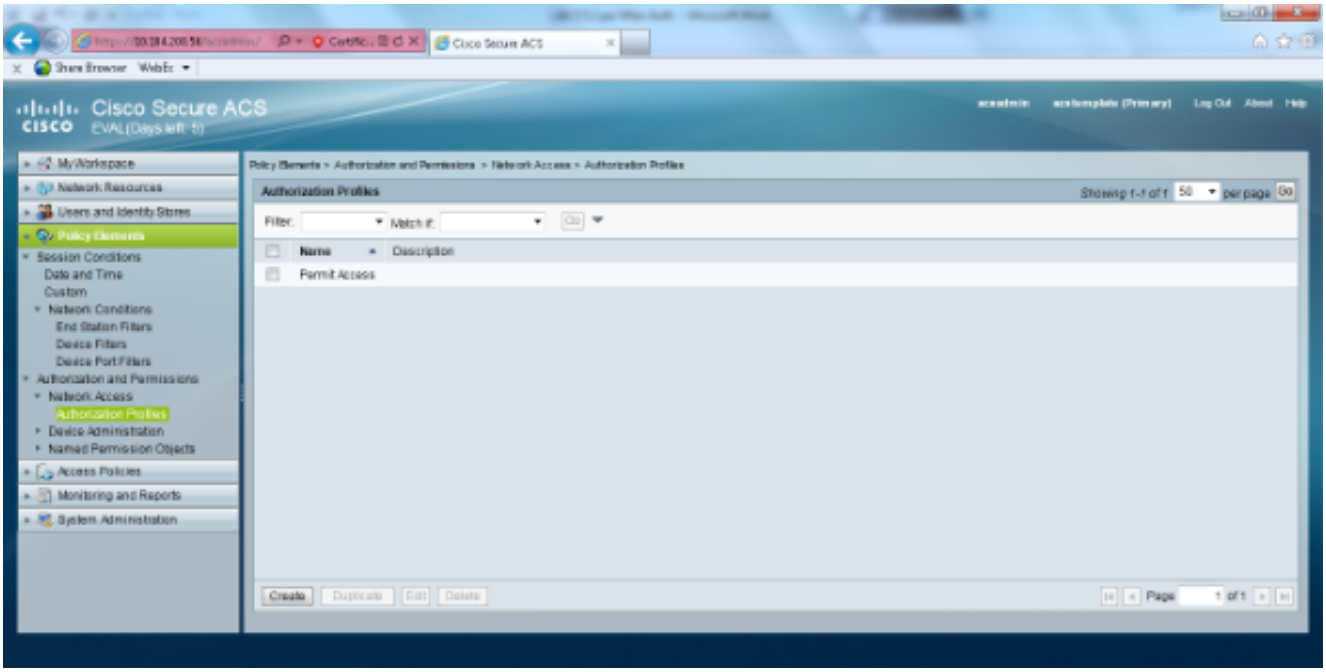
意味のある名前を入力し、[**IP address**]タブでWLCのIPアドレスを入力します。この例では、名前はEmployeeとContractorです。



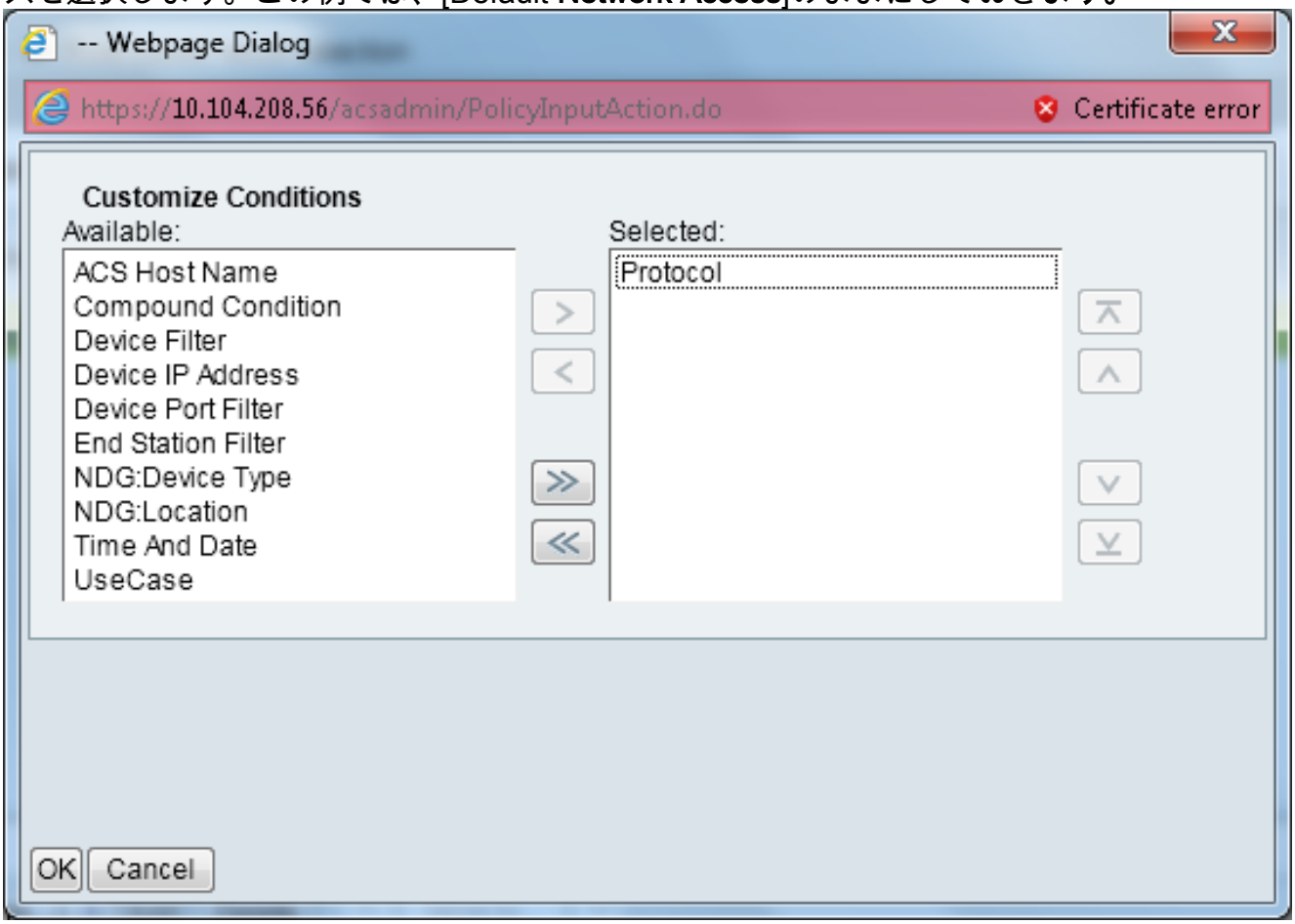
[CLI/DNIS]タブで、[CLI]を – ANY – のままにし、「DNIS」を*<SSID>として入力します。この例では、DNISフィールドに「*Employee」と入力します。このエンドステーションフィルタは、従業員WLANへのアクセスのみを制限するために使用されます。DNIS 属性は、ユーザがアクセスを許可される SSID を定義します。WLC は SSID を DNIS 属性で RADIUS サーバに送信します。Contractorエンドステーションフィルタについても同じ手順を繰り返します。

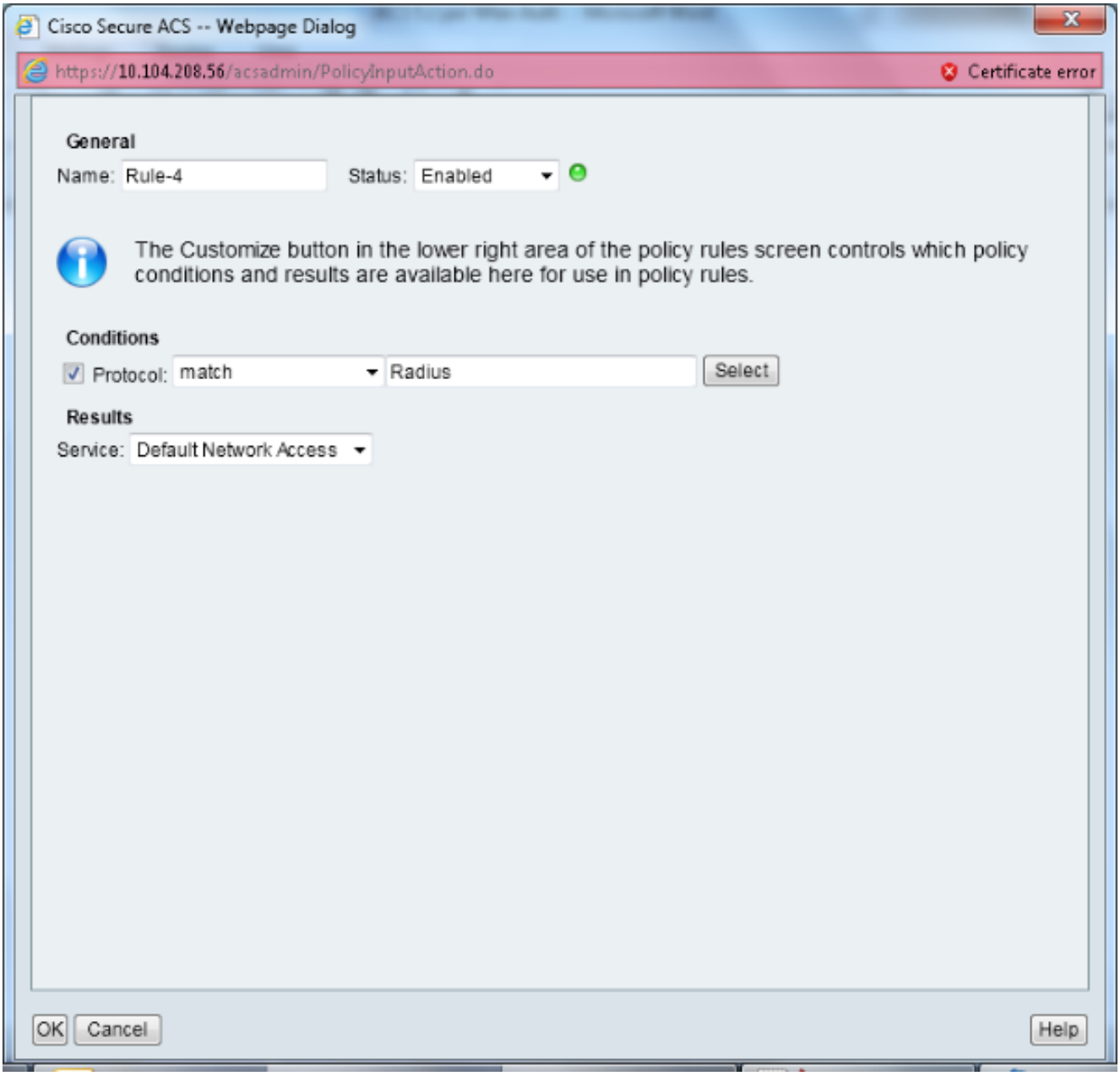


6. [Policy Elements] > [**Authorization and Permissions] > [Network Access] > [Authorization Profiles]を選択します。**[Permit Access]にはデフォルトプロファイルが必要です。

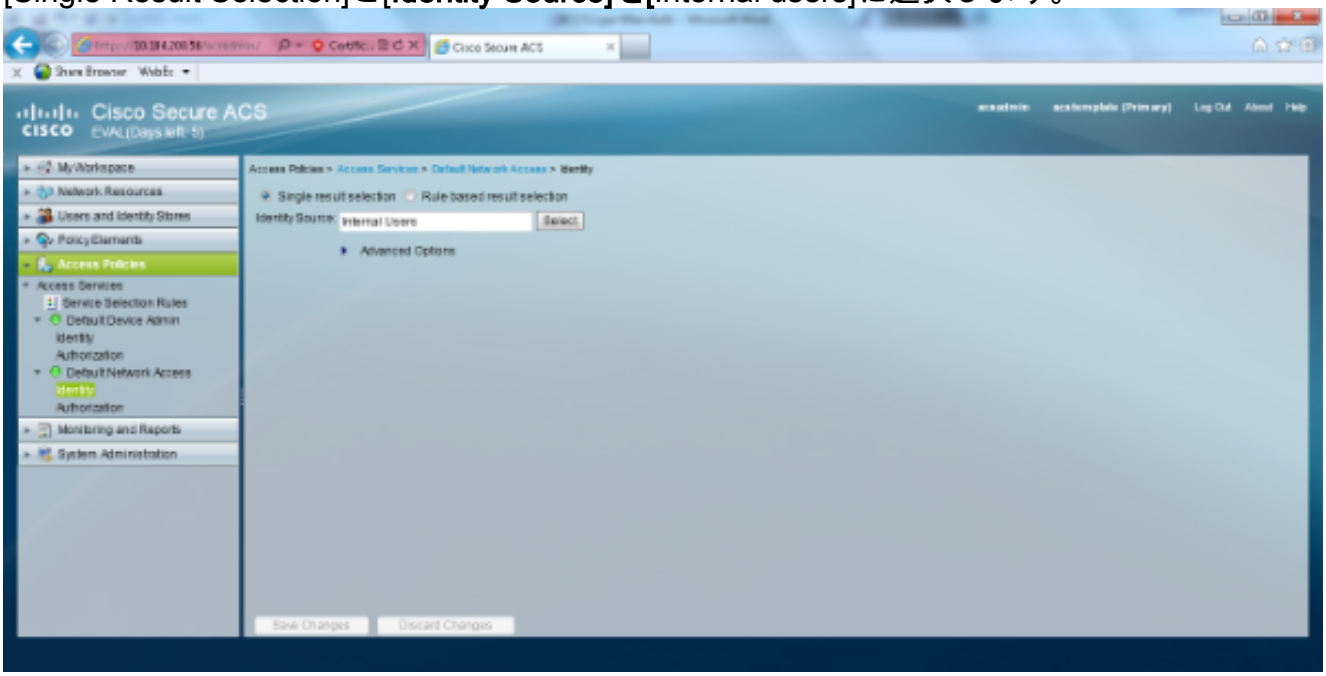


7. [Access Policies] > [Access Services] > [Service Selection Rules]を選択します。[Customize] をクリックします。 適切な条件を追加します。この例では、照合条件としてProtocol as Radiusを使用しています。[作成（Create）] をクリックします。ルールに名前を付けます。「プロトコル」を選択し、「Radius」を選択します。[Results] で、適切なアクセスサービスを選択します。この例では、[Default Network Access]のままにしておきます。

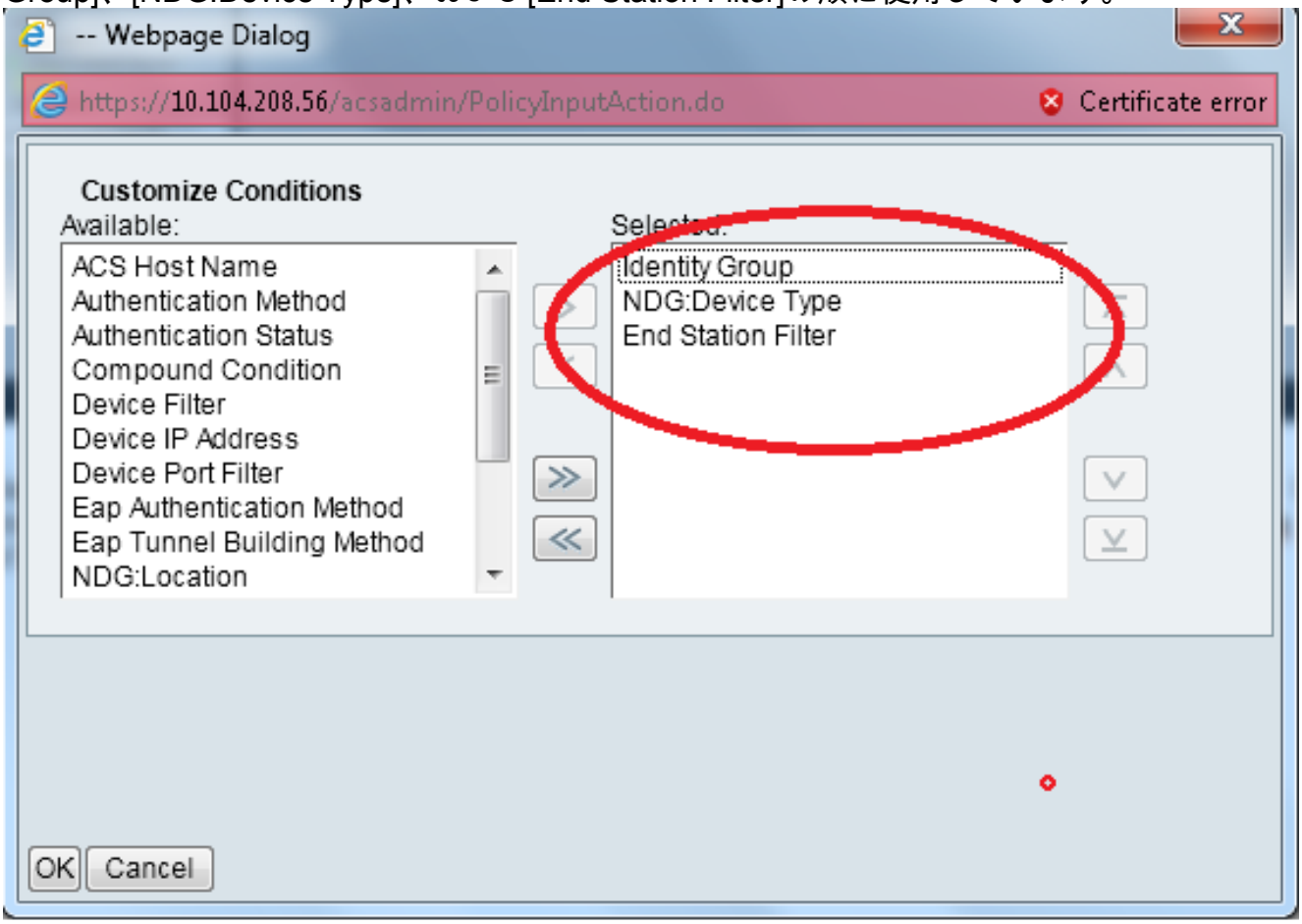




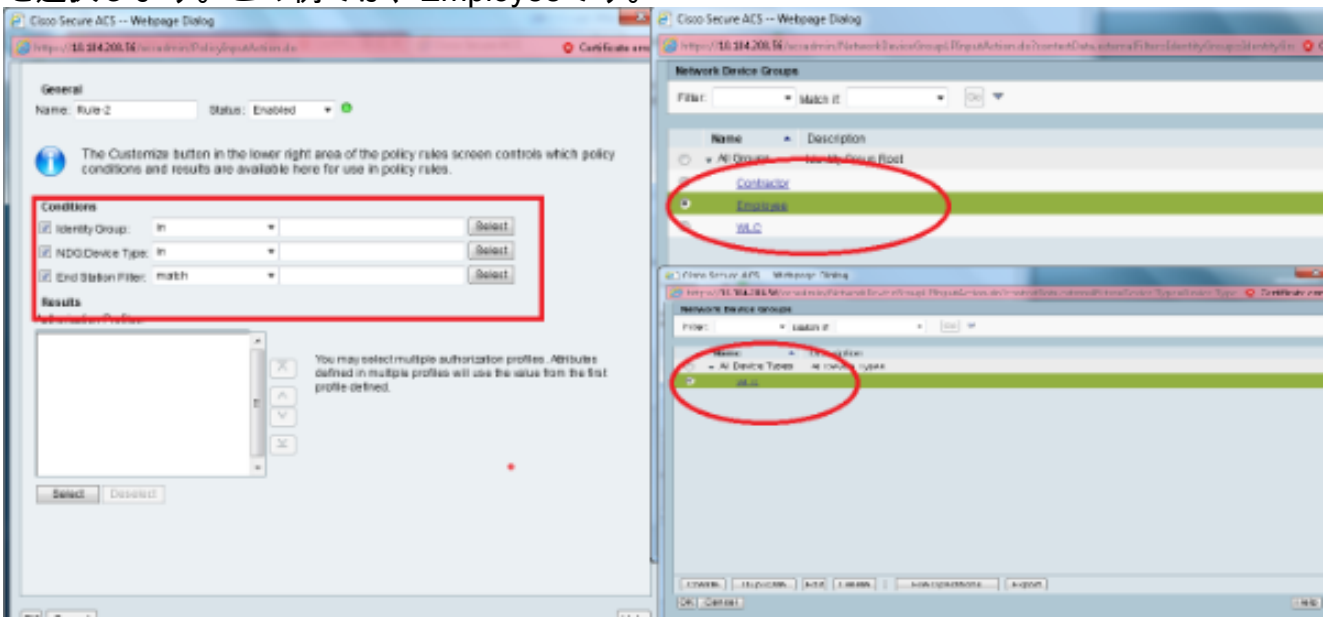
8. [Access Policies] > [Access Services] > [Default Network Access] > [Identity]を選択します。[Single Result Selection]と[Identity Source]を[Internal users]に選択します。



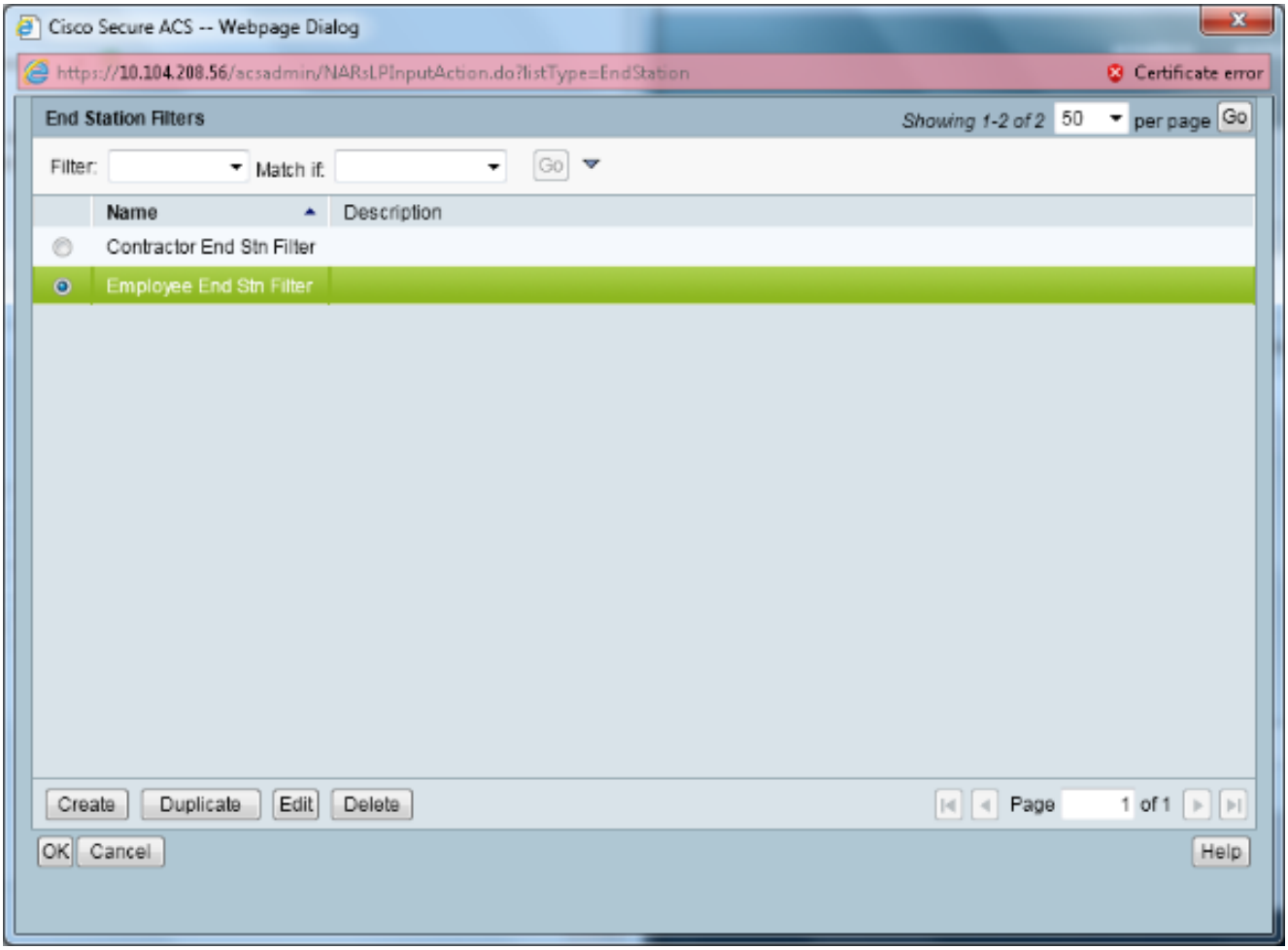
[Access Policies] > **[Access Services] > [Default Network Access] > [Authorization]を選択します。[Customize]をクリック**し、[Customized]**条件**を追加します。この例では、[Identity Group]、[NDG:Device Type]、および[End Station Filter]の順に使用しています。



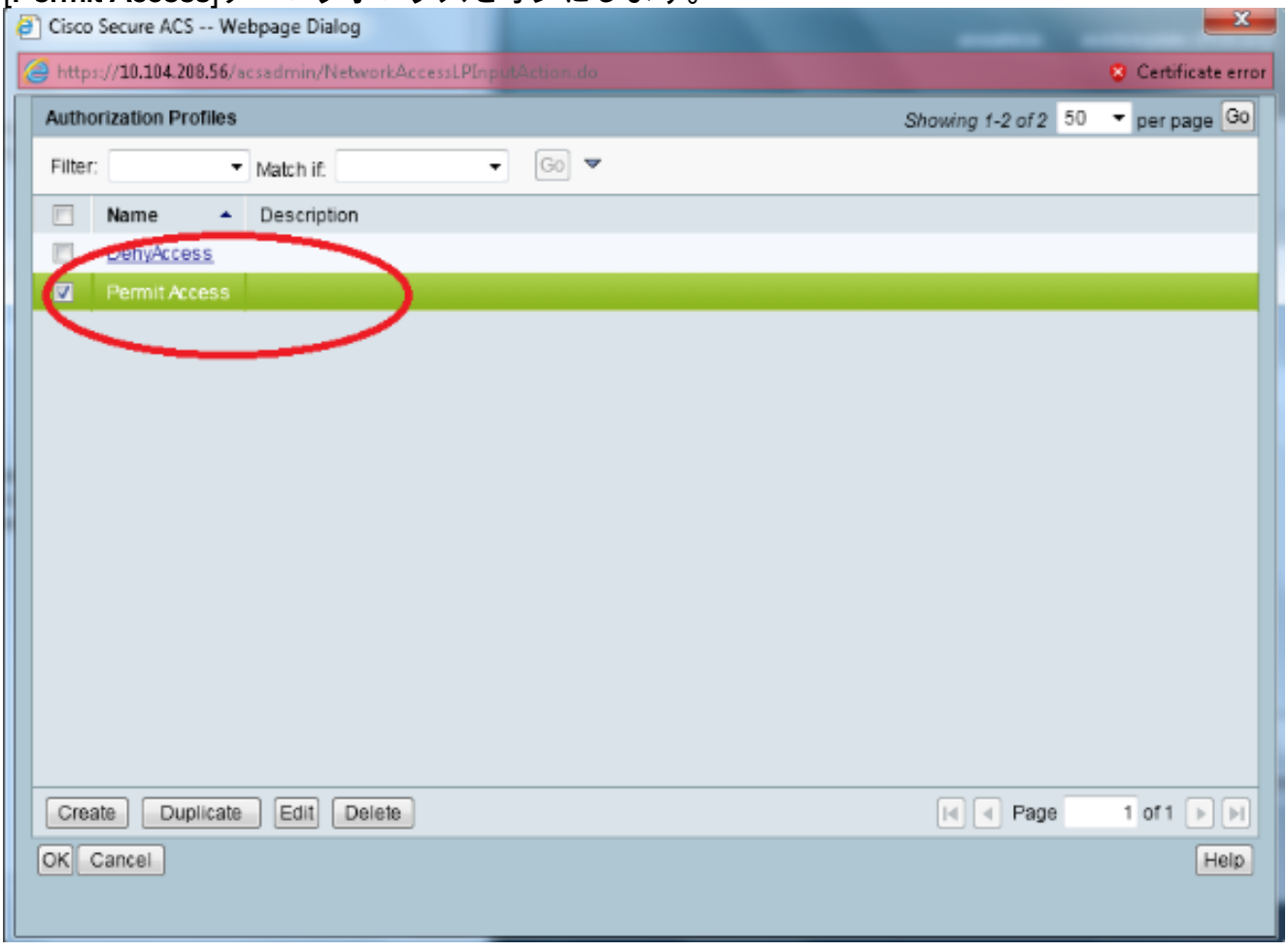
[作成（Create）] をクリックします。ルールに名前を付け、[All Groups]で適切なIDグループを選択します。この例では、Employeeです。



[Employee End Stn Filter]**オプションボタンをクリック**するか、[Configure the WLC]セクションのステップ1bで入力した名前を入力します。

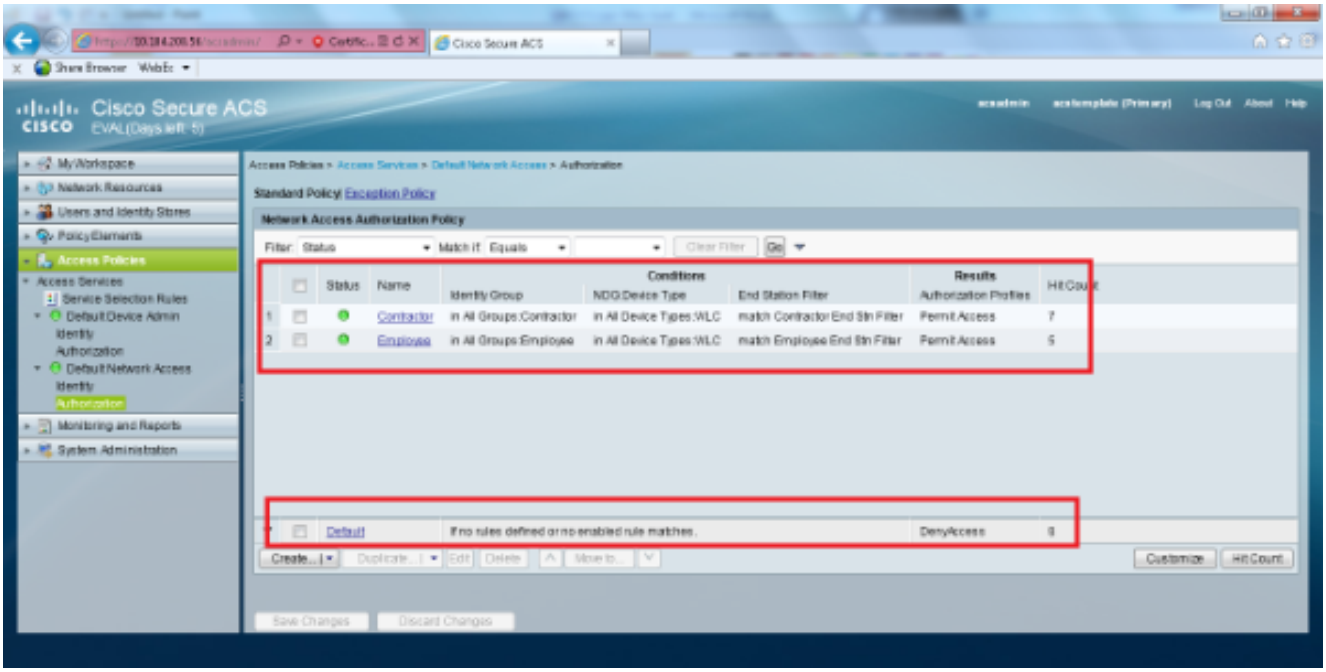


[Permit Access]チェックボックスをオンにします。



契約作業員ルールについても、上記と同じ手順を繰り返します。[Default Action]が[Deny

Access]になっていることを確認します。 手順eを完了すると、ルールは次の例のようになります。



これで設定は終了です。このセクションの後、接続するには、SSIDとセキュリティパラメータに従ってクライアントを設定する必要があります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。