Konfigurationsbeispiel für ACS Version 5.2 und WLC für die WLAN-Authentifizierung

Inhalt

Einführung

Dieses Dokument enthält ein Konfigurationsbeispiel, um den benutzerbasierten Zugriff auf ein Wireless LAN (WLAN) basierend auf der Service Set Identifier (SSID) zu beschränken.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Konfigurieren von Wireless LAN Controller (WLC) und Lightweight Access Point (LAP) für den Basisbetrieb
- Konfigurieren des Cisco Secure Access Control Server (ACS)
- LWAPP (Lightweight Access Point Protocol) und Wireless-Sicherheitsmethoden

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco WLC der Serie 5500 mit Firmware-Version 7.4.110
- Cisco LAP der Serie 1142
- Cisco Secure ACS Server Version 5.2.0.26.11

Konfigurieren

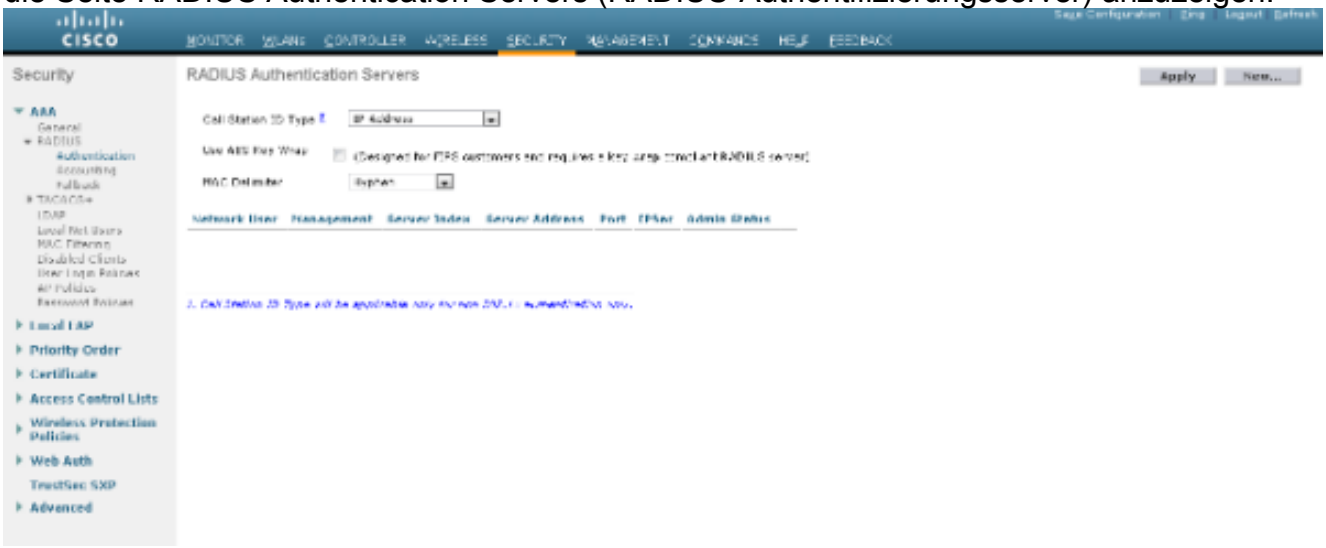
Um die Geräte für diese Konfiguration zu konfigurieren, müssen Sie:

1. Konfigurieren Sie den WLC für die beiden WLANs und den RADIUS-Server.
2. Konfigurieren Sie den Cisco Secure ACS.
3. Konfigurieren Sie die Wireless-Clients, und überprüfen Sie die Konfiguration.

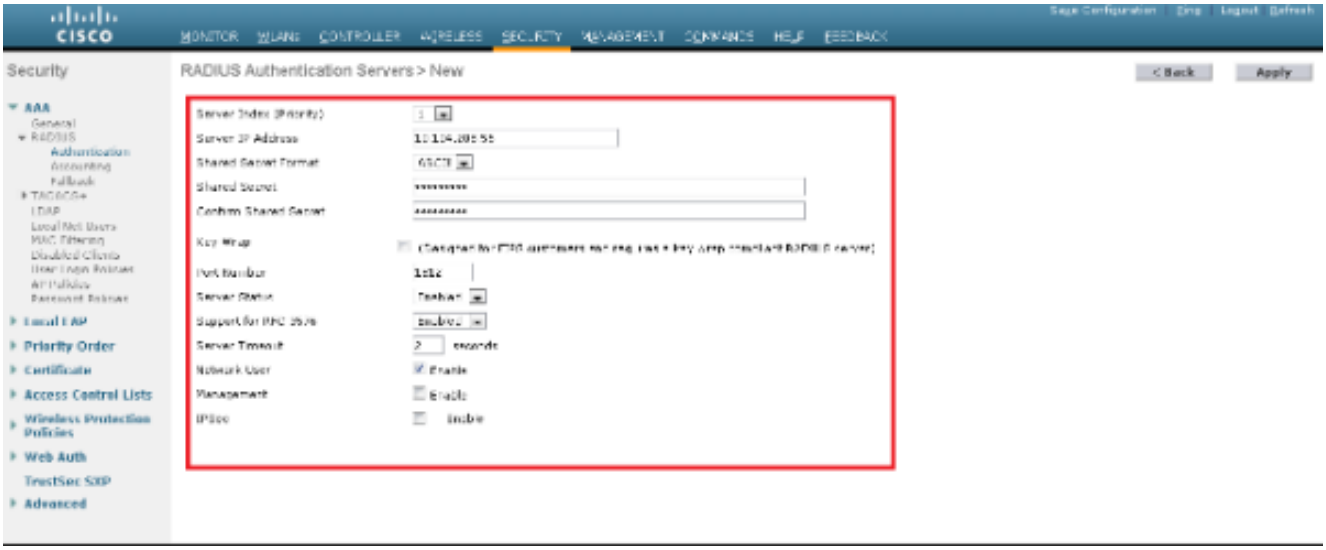
Konfigurieren des WLC

Führen Sie die folgenden Schritte aus, um den WLC für diese Einrichtung zu konfigurieren:

1. Konfigurieren Sie den WLC, um die Benutzeranmeldeinformationen an einen externen RADIUS-Server weiterzuleiten. Der externe RADIUS-Server (in diesem Fall Cisco Secure ACS) validiert dann die Benutzeranmeldeinformationen und ermöglicht den Zugriff auf die Wireless-Clients. Gehen Sie wie folgt vor: Wählen Sie **Security > RADIUS Authentication (Sicherheit > RADIUS-Authentifizierung)** in der Benutzeroberfläche des Controllers aus, um die Seite RADIUS Authentication Servers (RADIUS-Authentifizierungsserver) anzuzeigen.



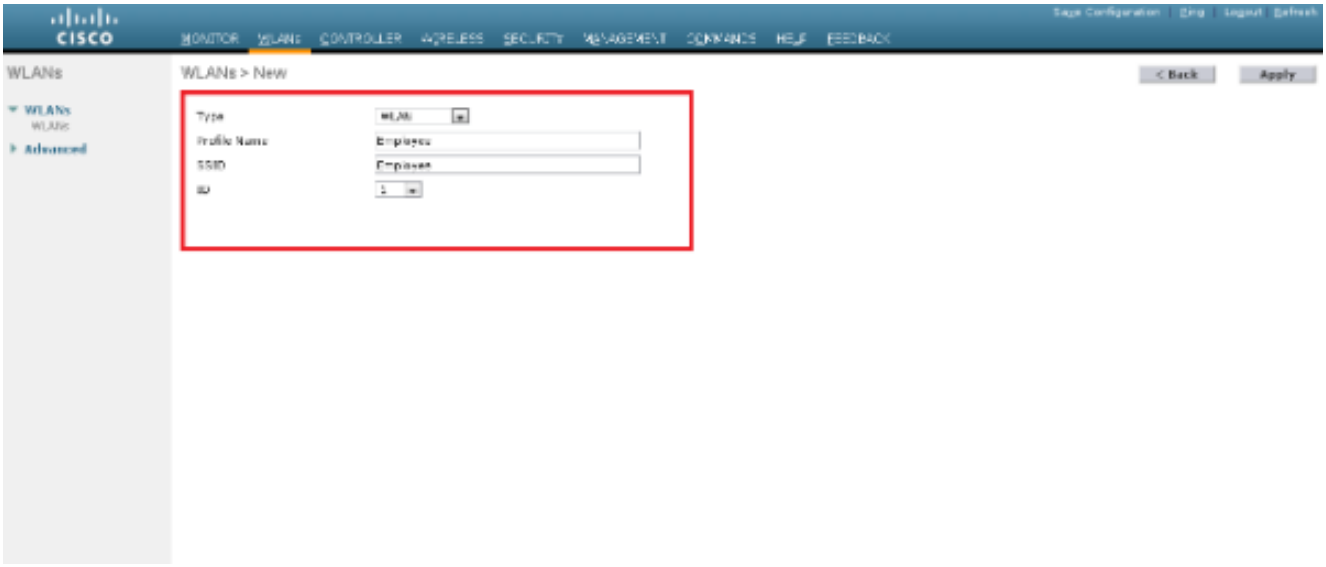
Klicken Sie auf **Neu**, um die RADIUS-Serverparameter zu definieren. Zu diesen Parametern gehören die IP-Adresse des RADIUS-Servers, der Shared Secret, die Portnummer und der Serverstatus. Die Kontrollkästchen für Netzwerkbenutzer und -verwaltung legen fest, ob die RADIUS-basierte Authentifizierung für Verwaltungs- und Netzwerkbenutzer gilt. In diesem Beispiel wird Cisco Secure ACS als RADIUS-Server mit der IP-Adresse 10.104.208.56 verwendet.



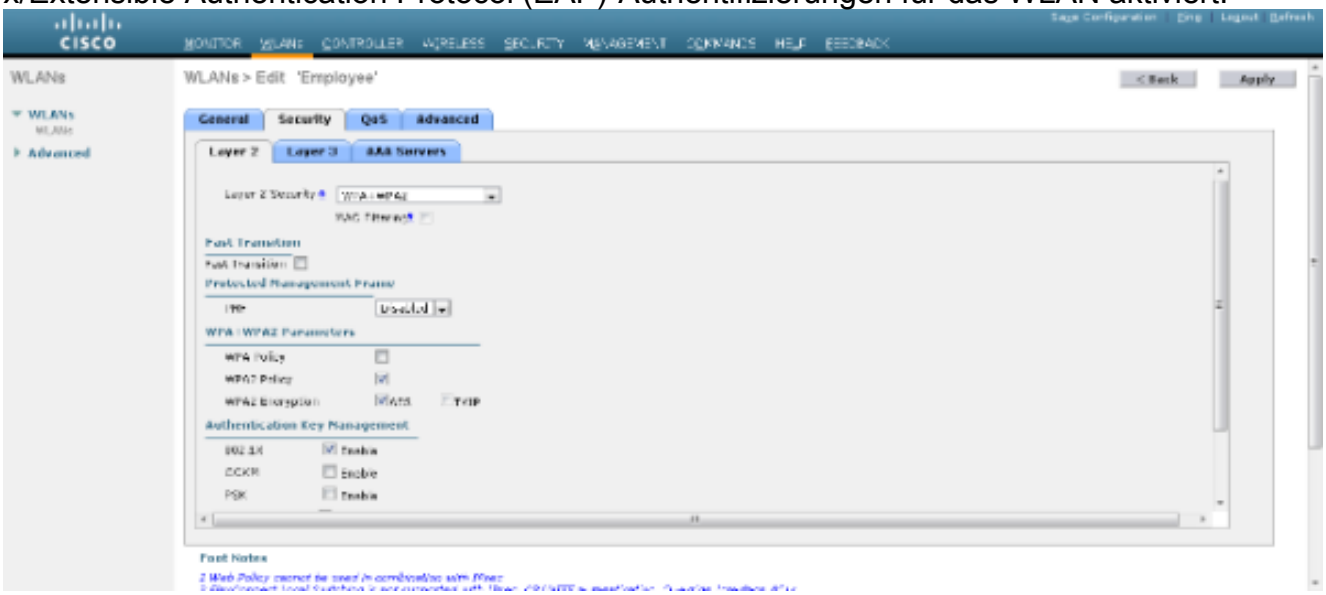
Klicken Sie auf **Übernehmen**.

2. Führen Sie diese Schritte aus, um ein WLAN für den Mitarbeiter mit SSID-**Mitarbeiter** und

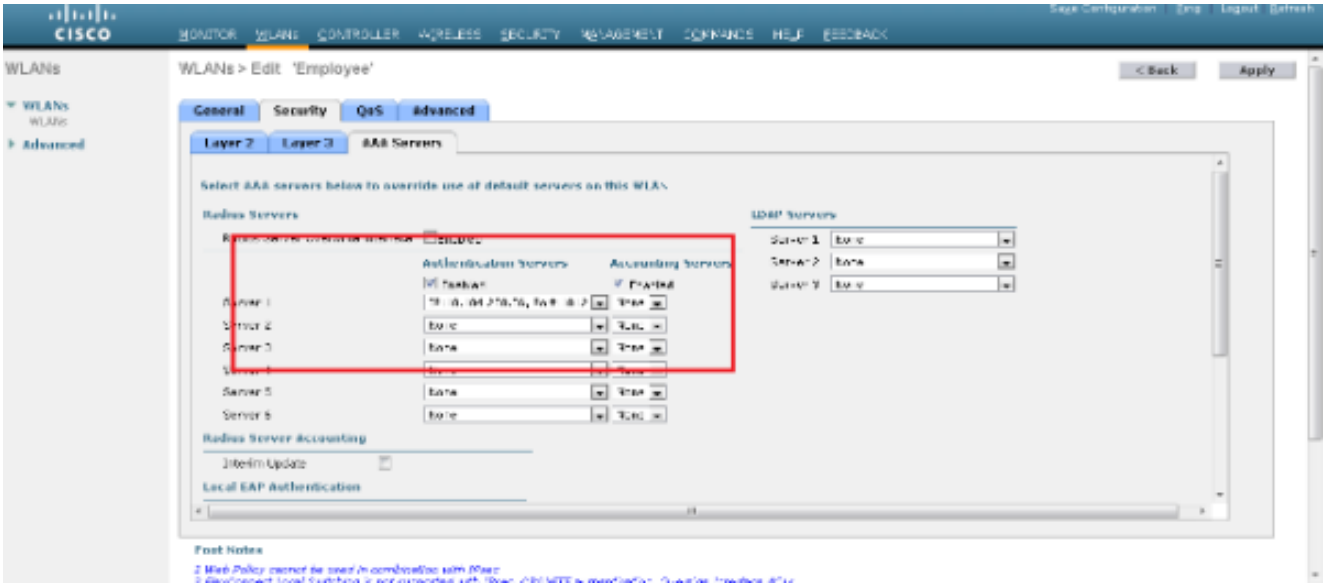
das andere WLAN für Auftragnehmer mit SSID-**Auftragnehmer** zu konfigurieren. Klicken Sie in der Controller-GUI auf **WLANs**, um ein WLAN zu erstellen. Das Fenster WLANs wird angezeigt. In diesem Fenster werden die auf dem Controller konfigurierten WLANs aufgeführt.Klicken Sie auf **Neu**, um ein neues WLAN zu konfigurieren.In diesem Beispiel wird ein WLAN mit dem Namen Employee erstellt, und die WLAN-ID ist 1. Klicken Sie auf **Übernehmen**.



Wählen Sie das Fenster **WLAN > Bearbeiten** aus, und definieren Sie die für das WLAN spezifischen Parameter: Wählen Sie auf der Registerkarte Layer-2-Sicherheit die Option **802.1x aus**. Standardmäßig ist die Layer-2-Sicherheitsoption 802.1x. Dadurch werden 802.1 x/Extensible Authentication Protocol (EAP)-Authentifizierungen für das WLAN aktiviert.



Wählen Sie auf der Registerkarte "AAA-Server" den entsprechenden RADIUS-Server aus der Dropdown-Liste unter "RADIUS-Server" aus. Die anderen Parameter können je nach Anforderung des WLAN-Netzwerks geändert werden. Klicken Sie auf **Übernehmen**.



Um ein WLAN für Auftragnehmer zu erstellen, wiederholen Sie die Schritte b bis d.

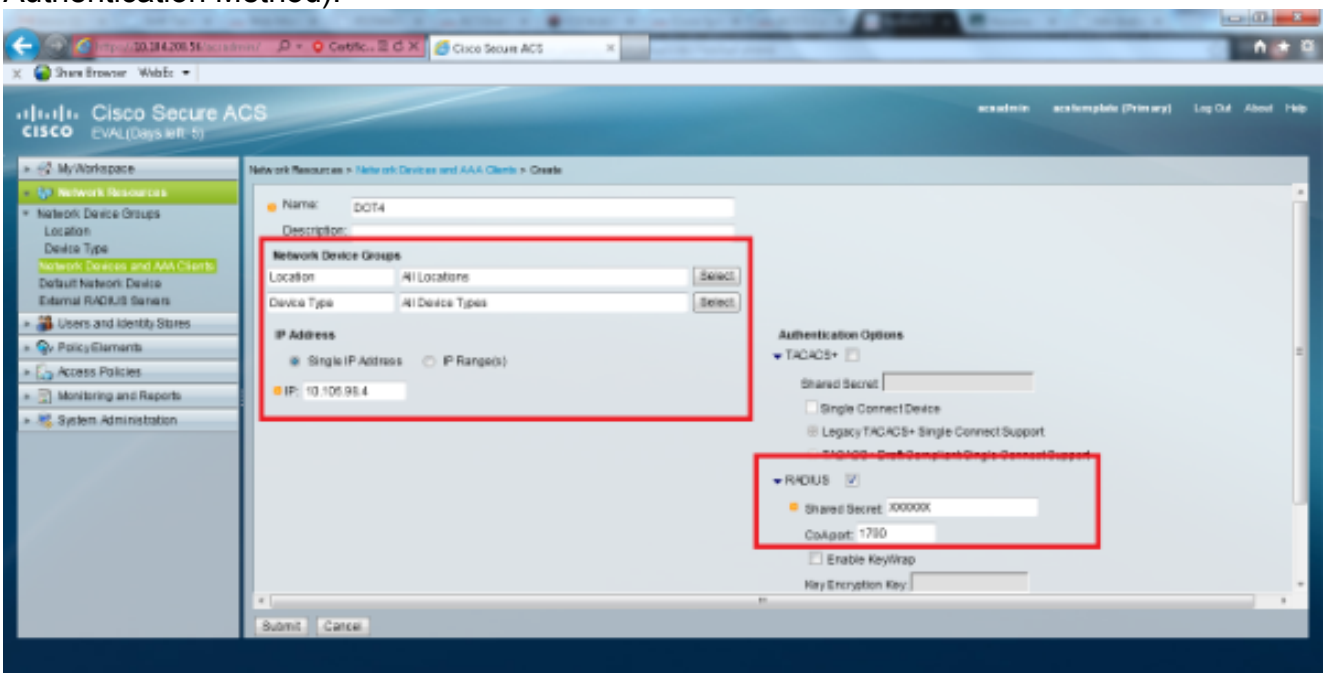
Konfigurieren von Cisco Secure ACS

Auf dem Cisco Secure ACS-Server müssen Sie:

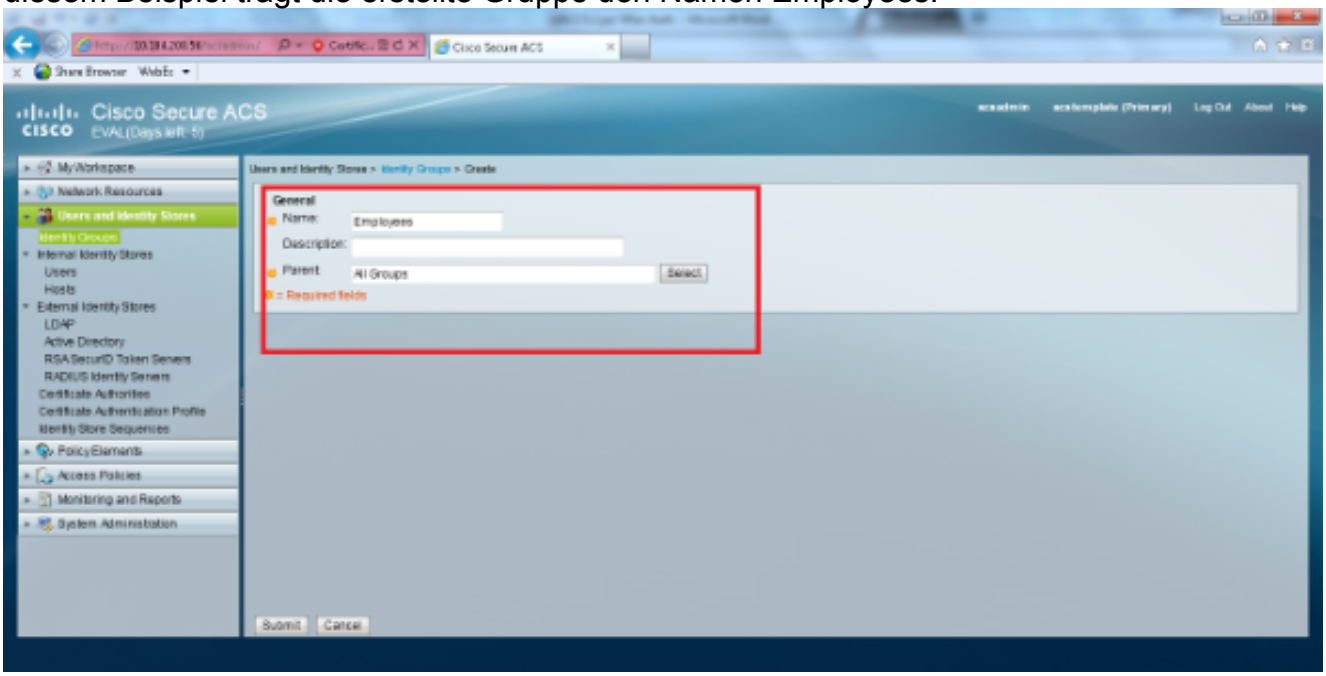
1. Konfigurieren Sie den WLC als AAA-Client.
2. Erstellen Sie die Benutzerdatenbank (Anmeldeinformationen) für die SSID-basierte Authentifizierung.
3. Aktivieren Sie die EAP-Authentifizierung.

Gehen Sie wie folgt vor:

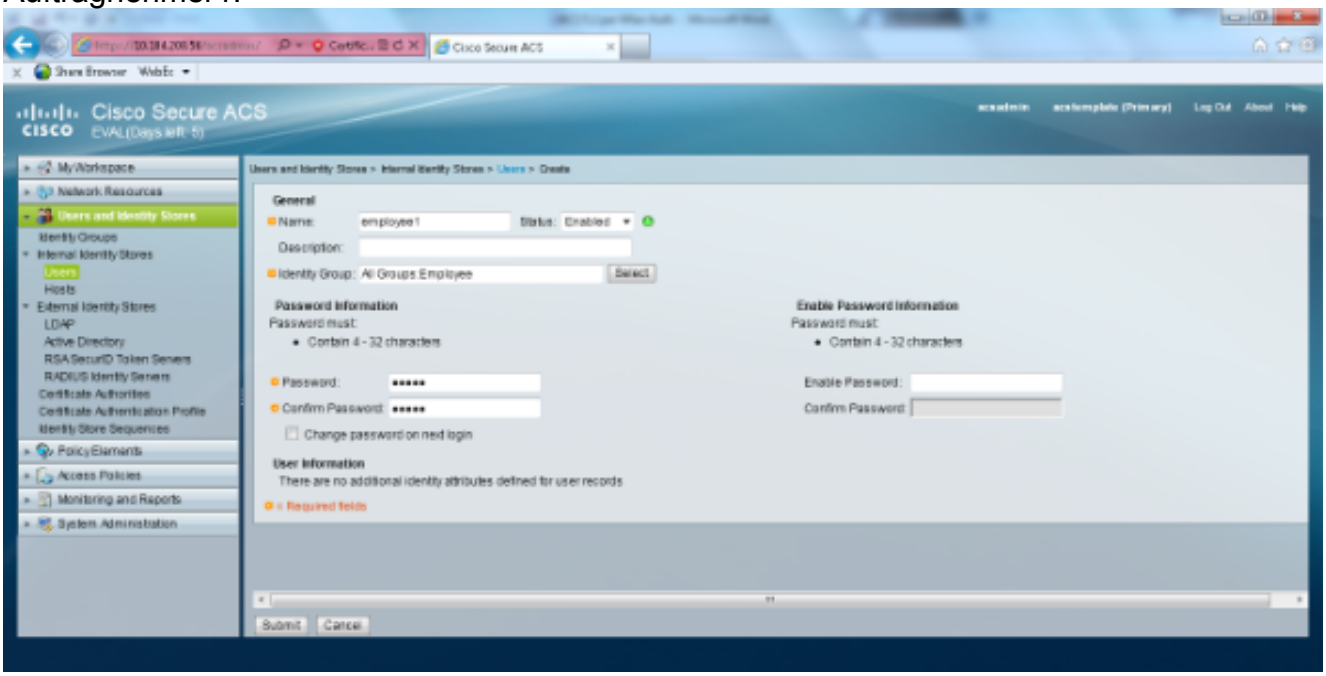
1. Um den Controller als AAA-Client auf dem ACS-Server zu definieren, wählen Sie **Network Resources > Network Devices and AAA Clients** aus der ACS GUI aus. Klicken Sie unter Netzwerkgeräte und AAA-Clients auf **Erstellen.**
2. Wenn die Seite "Network Configuration" (Netzwerkkonfiguration) angezeigt wird, definieren Sie den Namen des WLC, die IP-Adresse sowie die RADIUS-Methode (Shared geheim und Authentication Method).



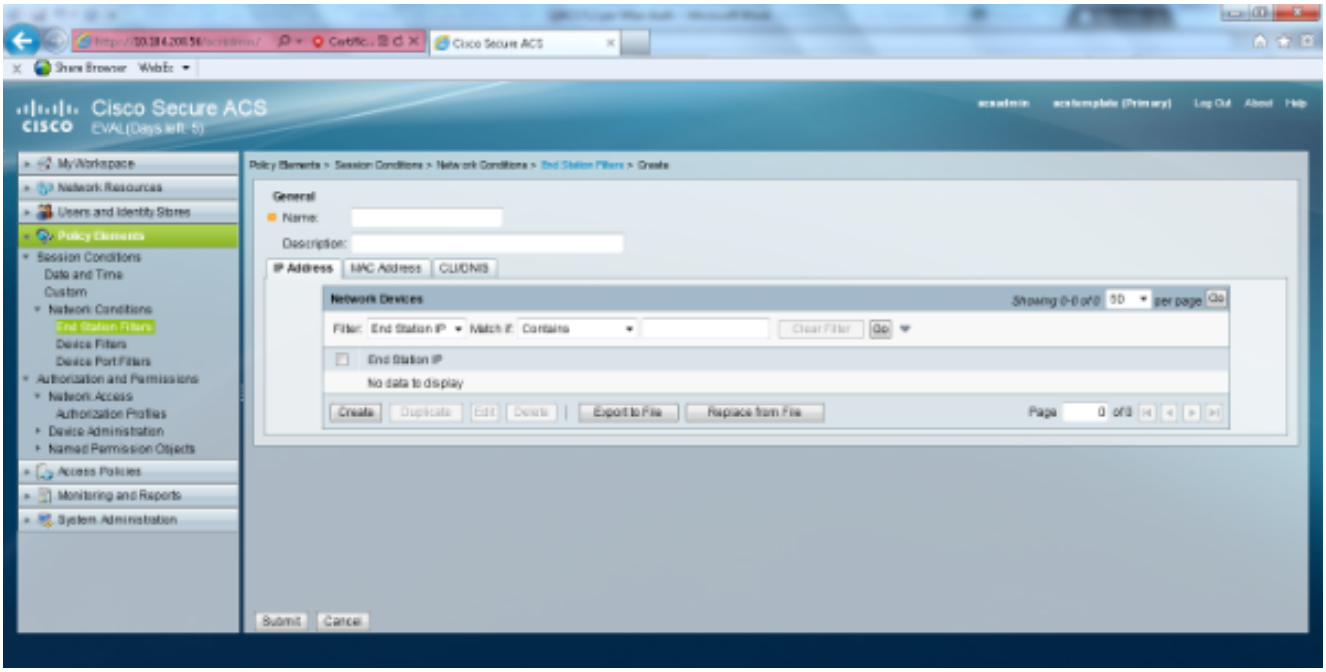
3. Wählen Sie **Benutzer und Identitätsdaten > Identitätsgruppen** in der ACS-GUI aus. Erstellen Sie die entsprechenden Gruppen für Mitarbeiter und AN, und klicken Sie auf **Erstellen**. In diesem Beispiel trägt die erstellte Gruppe den Namen Employees.



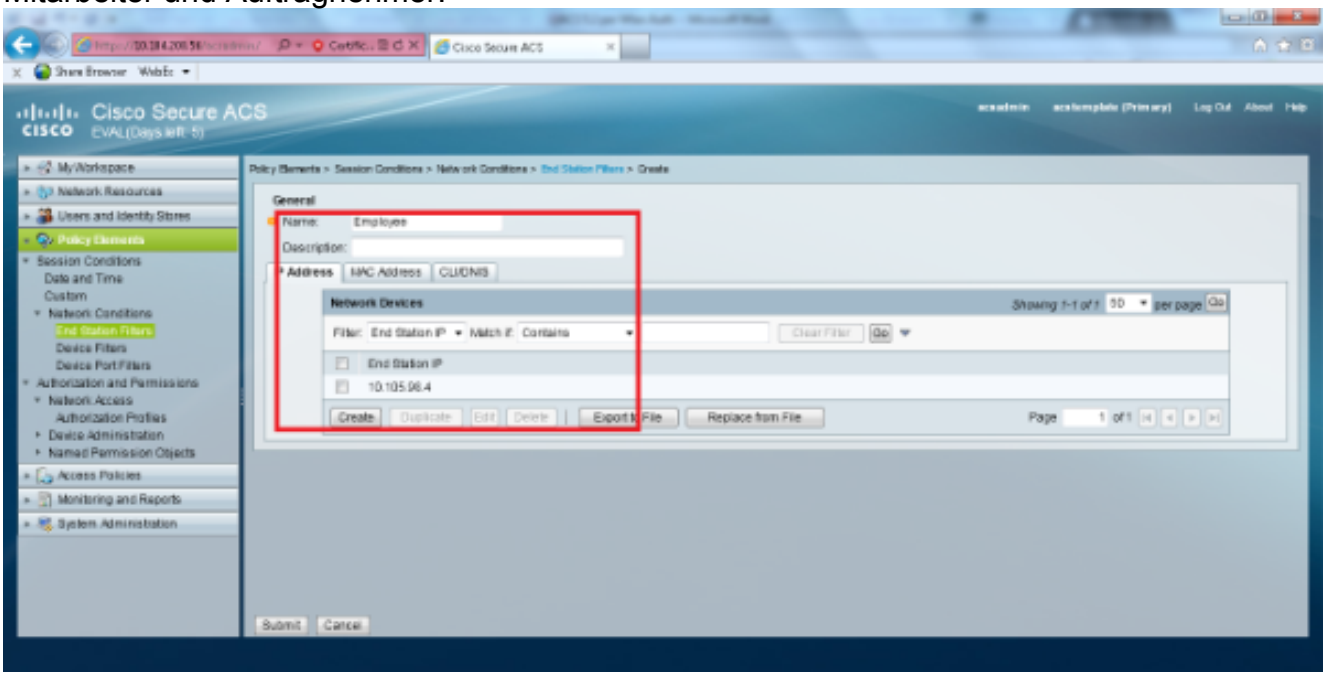
4. Wählen Sie **Benutzer und Identitätsdaten > Interne Identitätsdatenbanken aus**. Klicken Sie auf **Erstellen**, und geben Sie den Benutzernamen ein. Platzieren Sie sie in der richtigen Gruppe, definieren Sie ihr Kennwort, und klicken Sie auf **Senden**.In diesem Beispiel wird ein Benutzer mit dem Namen employee1 in der Gruppe Employee erstellt. Erstellen Sie unter den Auftragnehmern der Gruppe einen Benutzer mit dem Namen Auftragnehmer1.



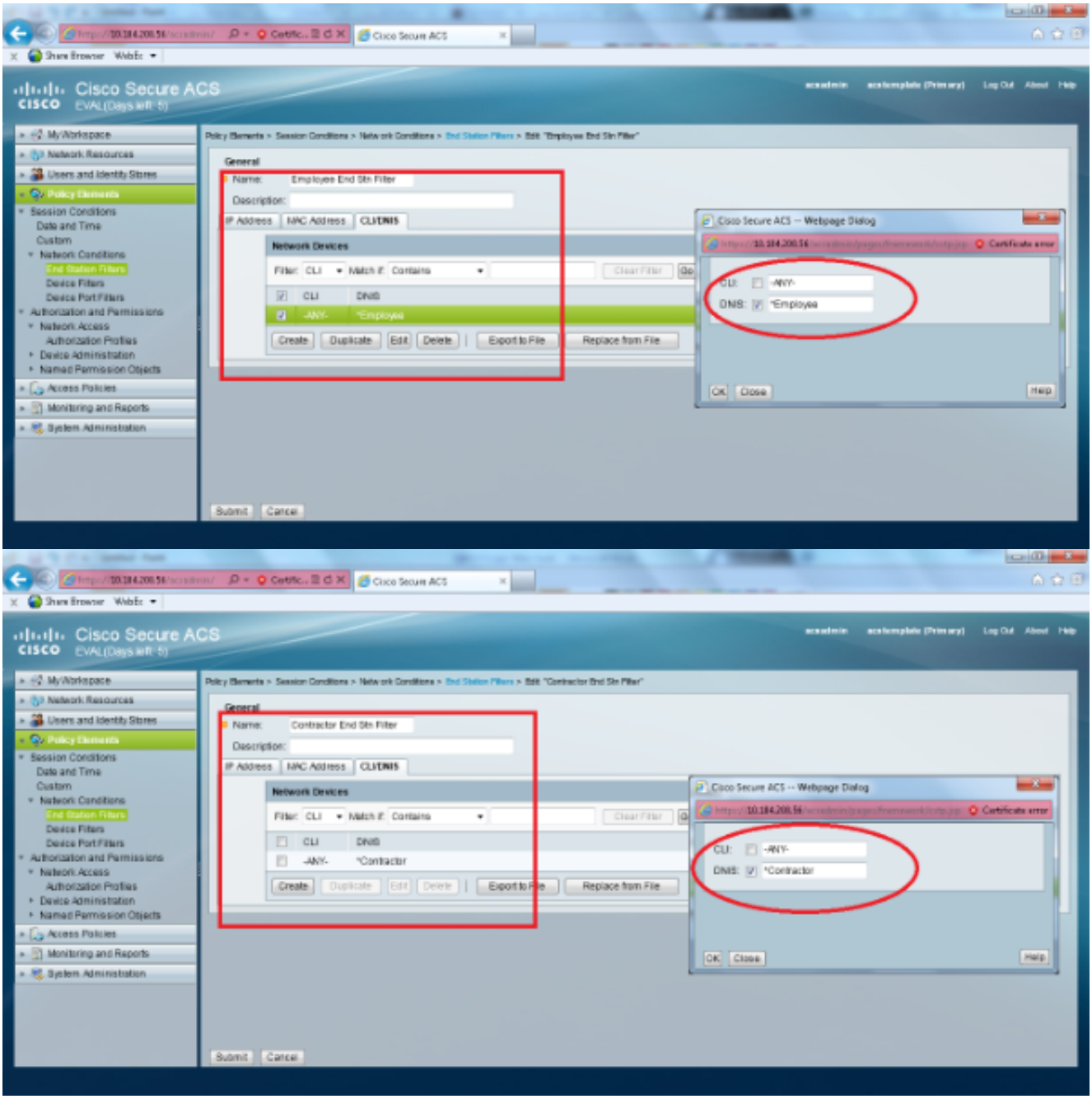
5. Wählen Sie **Richtlinienelemente > Netzwerkbedingungen > Filter für Endstationen aus**. Klicken Sie auf **Erstellen**.



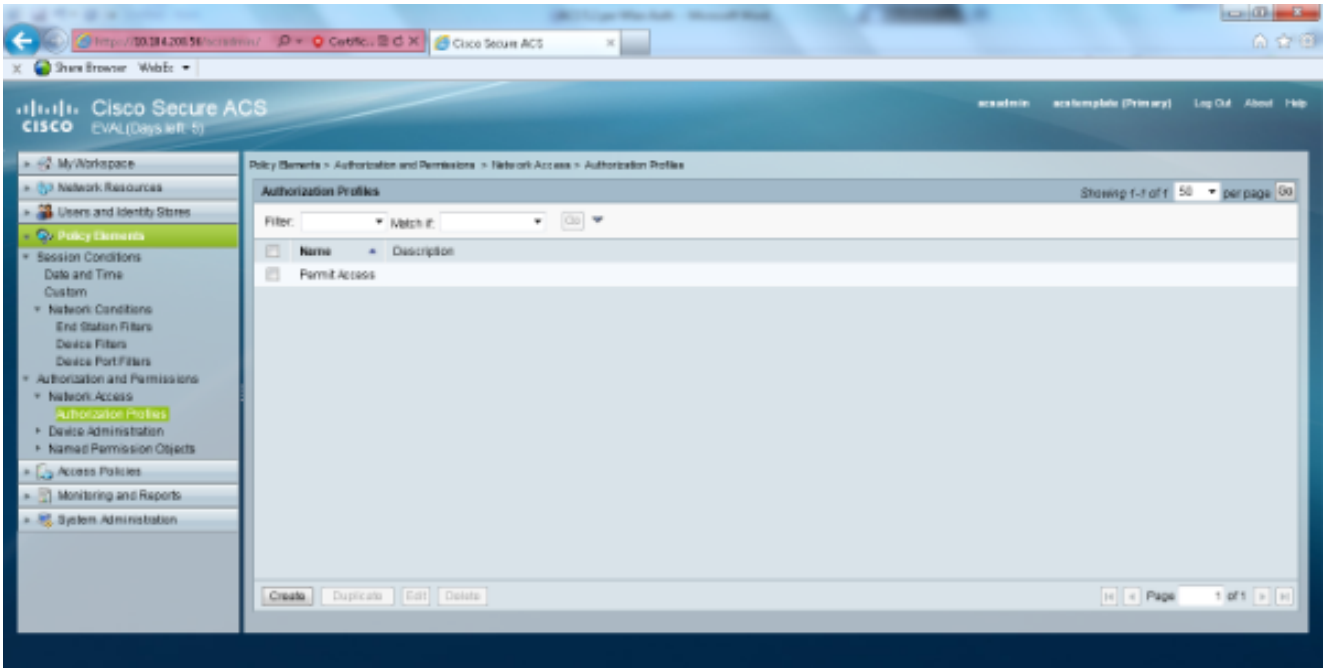
Geben Sie einen aussagekräftigen Namen ein, und geben Sie unter der Registerkarte **IP address (IP-Adresse)** die IP-Adresse des WLC ein. In diesem Beispiel sind die Namen Mitarbeiter und Auftragnehmer.



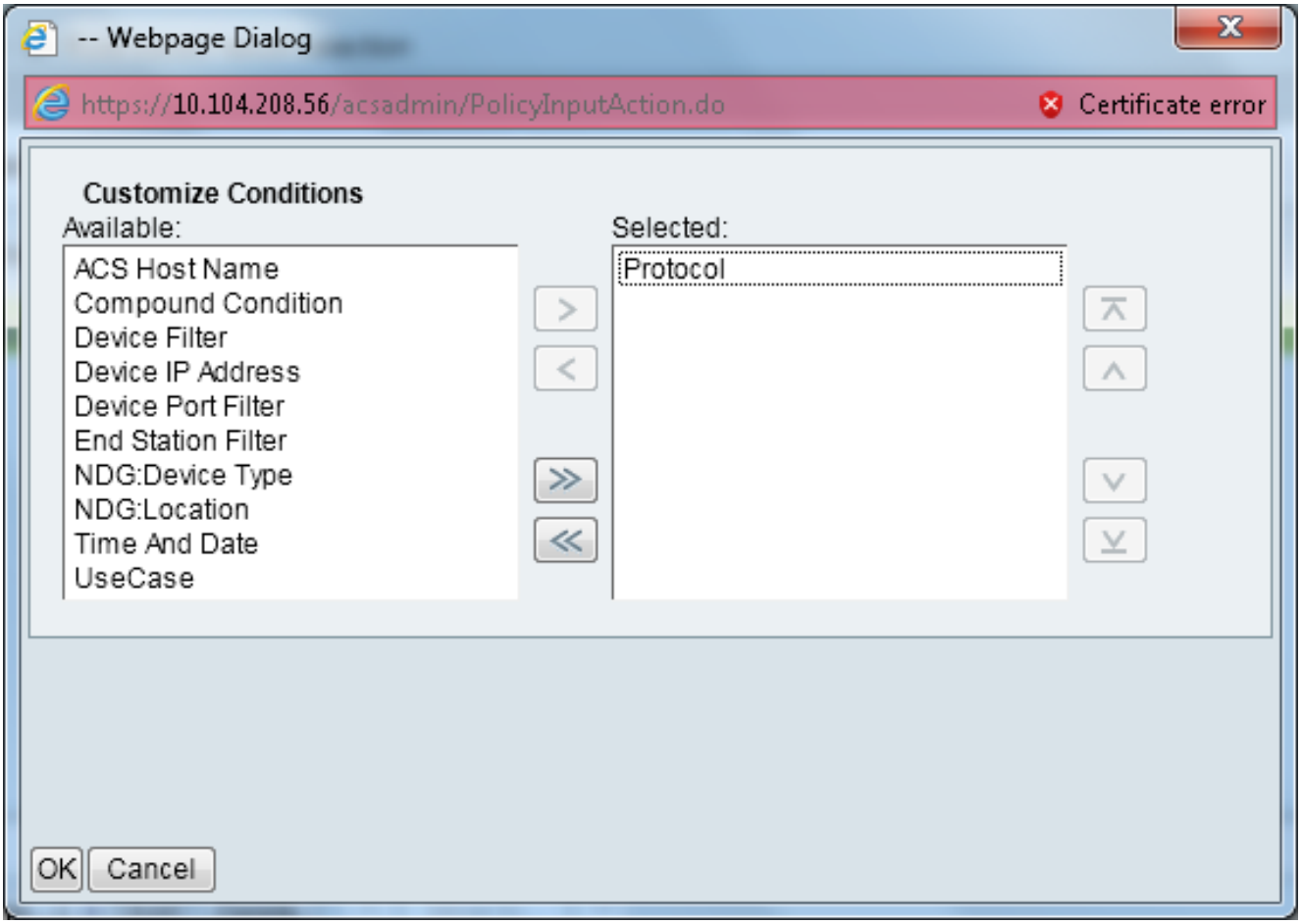
Belassen Sie auf der Registerkarte CLI/DNIS die CLI als -ANY-, und geben Sie DNIS als *<SSID> ein. In diesem Beispiel wird das DNIS-Feld als *Employee eingegeben, da dieser Endstation-Filter verwendet wird, um den Zugriff auf das Employee WLAN zu beschränken. Das DNIS-Attribut definiert die SSID, auf die der Benutzer zugreifen darf. Der WLC sendet die SSID im DNIS-Attribut an den RADIUS-Server.Wiederholen Sie die gleichen Schritte für den Auftragnehmer-Endstationsfilter.

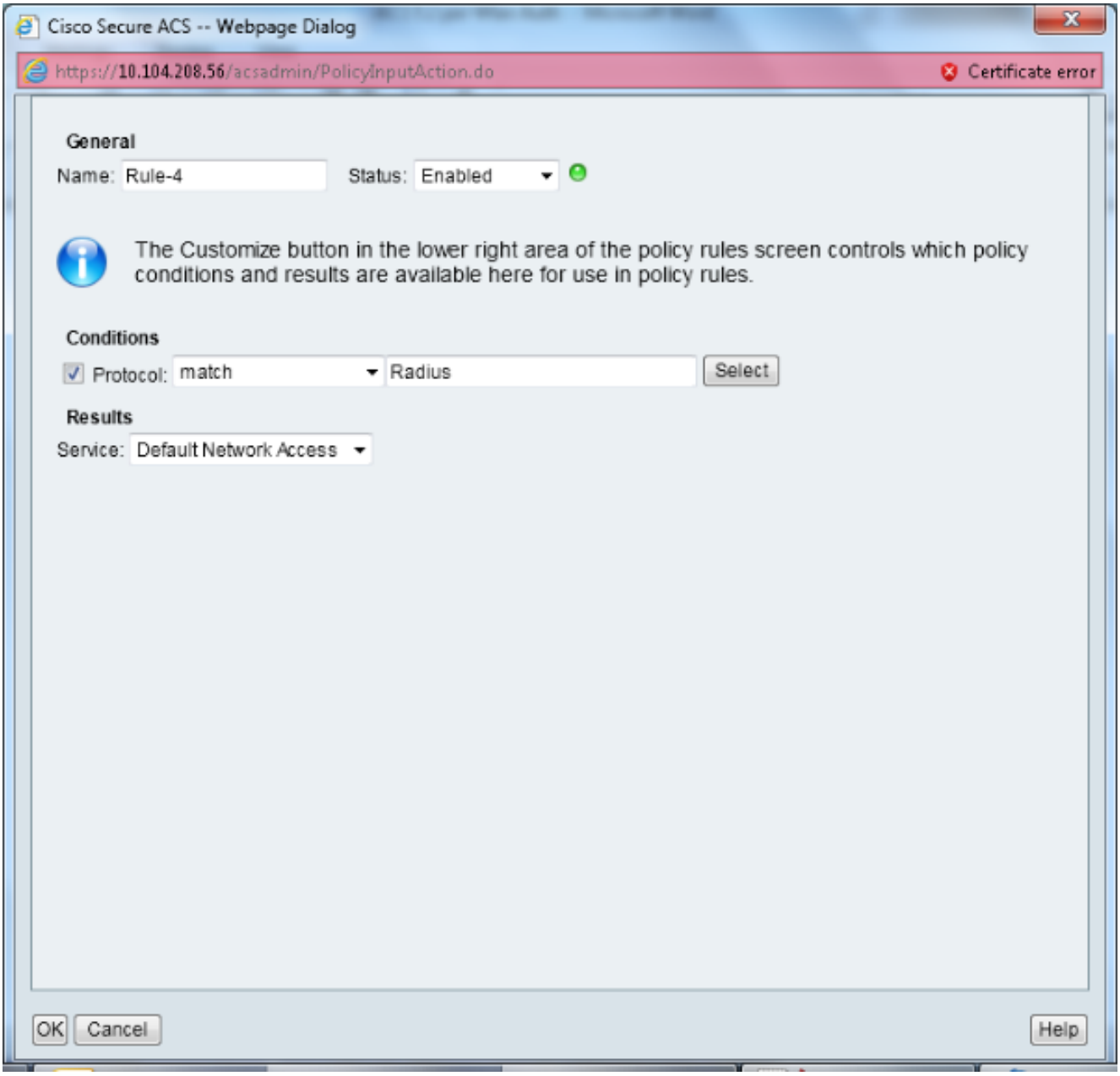


6. Wählen Sie **Richtlinienelemente > Autorisierung und Berechtigungen > Netzwerkzugriff > Autorisierungsprofile aus**. Es sollte ein Standardprofil für "Zugriff zulassen" vorhanden sein.

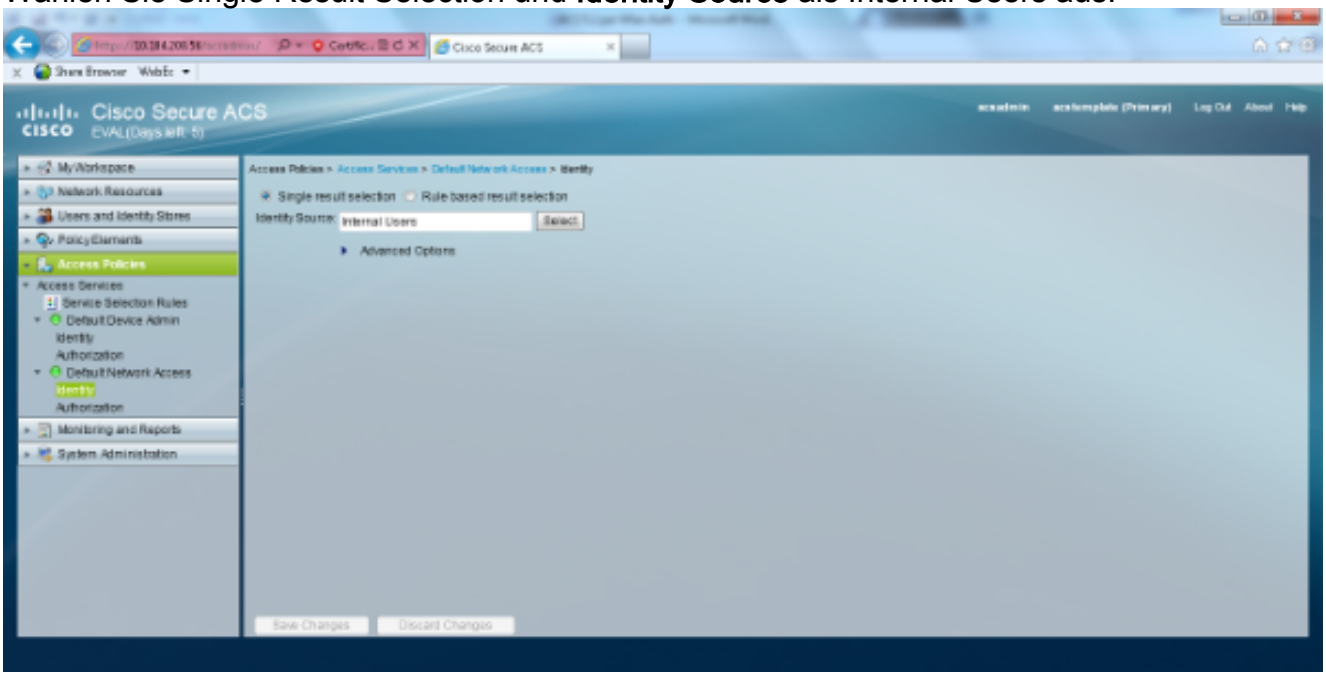


7. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Serviceauswahlregeln aus**. Klicken Sie auf **Anpassen**. Fügen Sie eine geeignete Bedingung hinzu. In diesem Beispiel wird Protocol als Radius als übereinstimmende Bedingung verwendet.Klicken Sie auf **Erstellen**. Nennen Sie die Regel. Wählen Sie **Protokoll** und dann **Radius** aus.Wählen Sie unter **Ergebnisse** den entsprechenden Zugriffsdienst aus. In diesem Beispiel wird es als **Standard-Netzwerkzugriff** beibehalten.

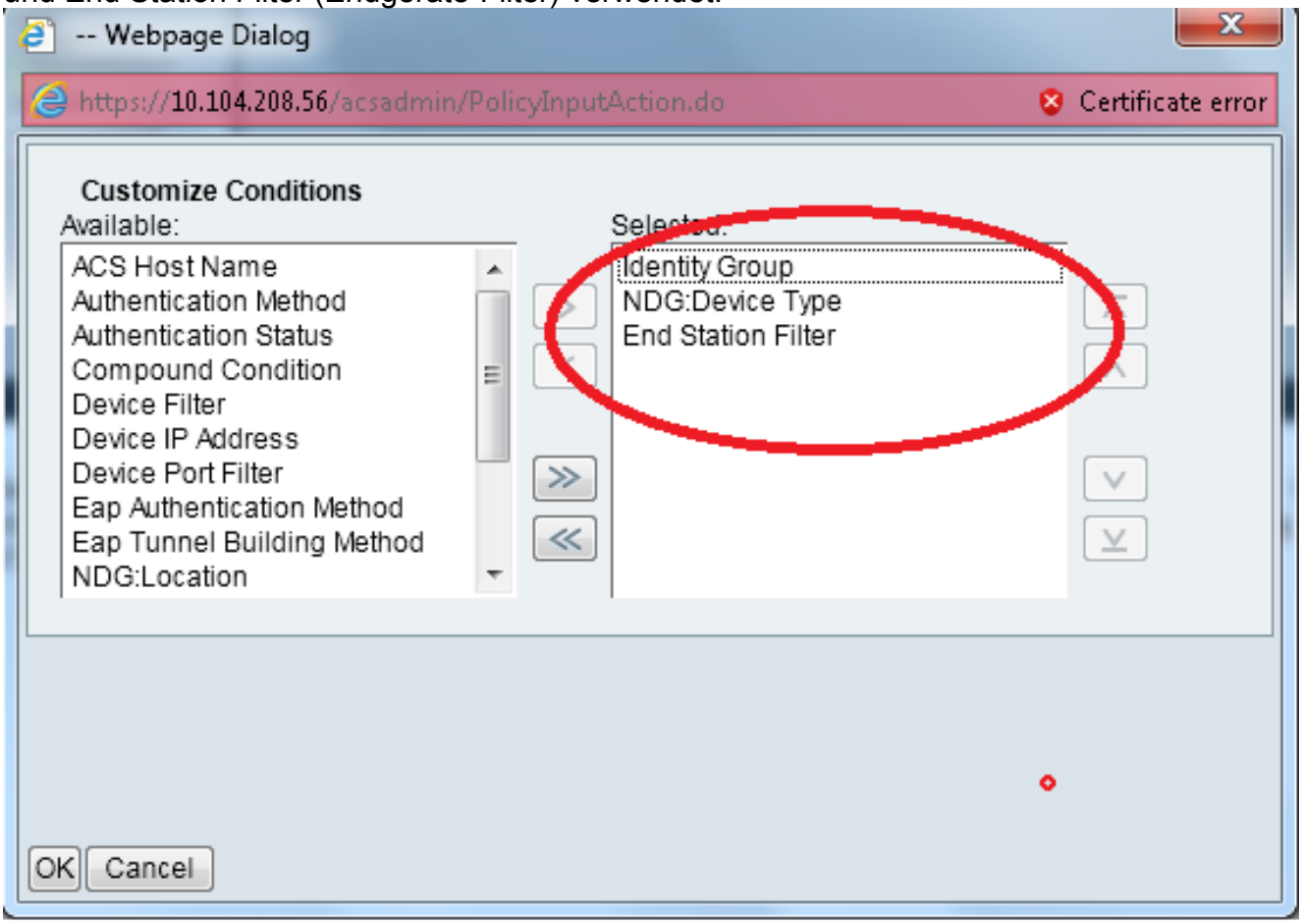




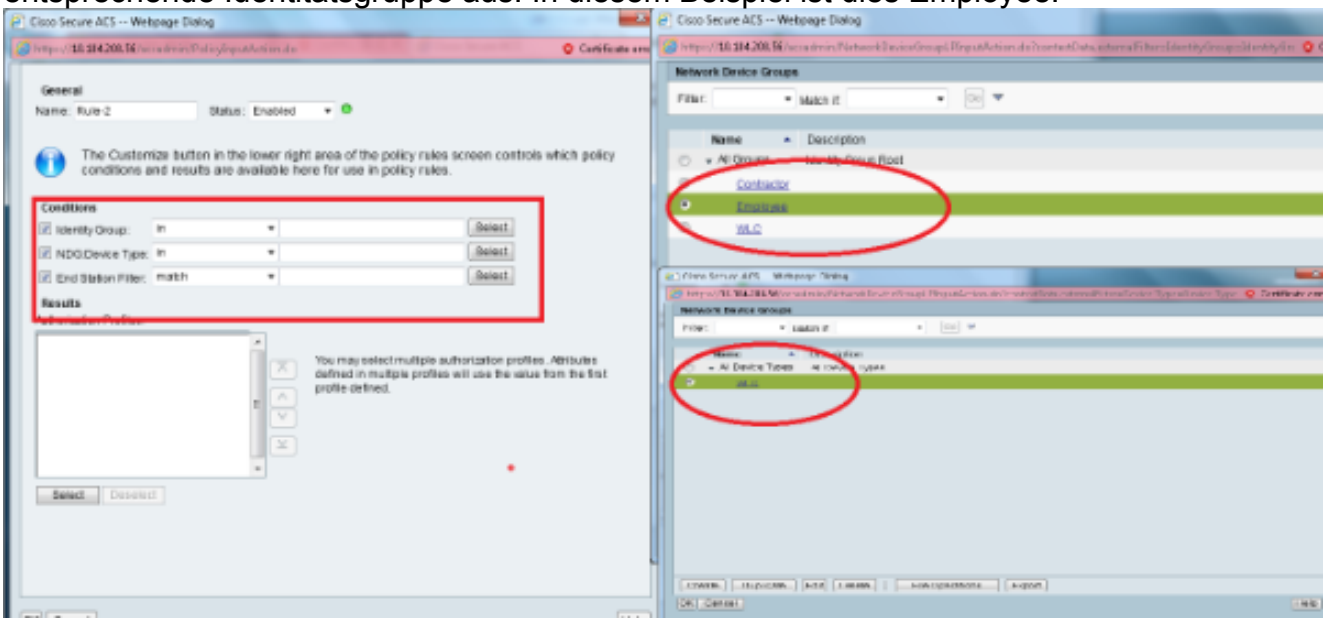
8. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standardnetzwerkzugriff > Identität aus**. Wählen Sie Single Result Selection und **Identity Source** als Internal Users aus.



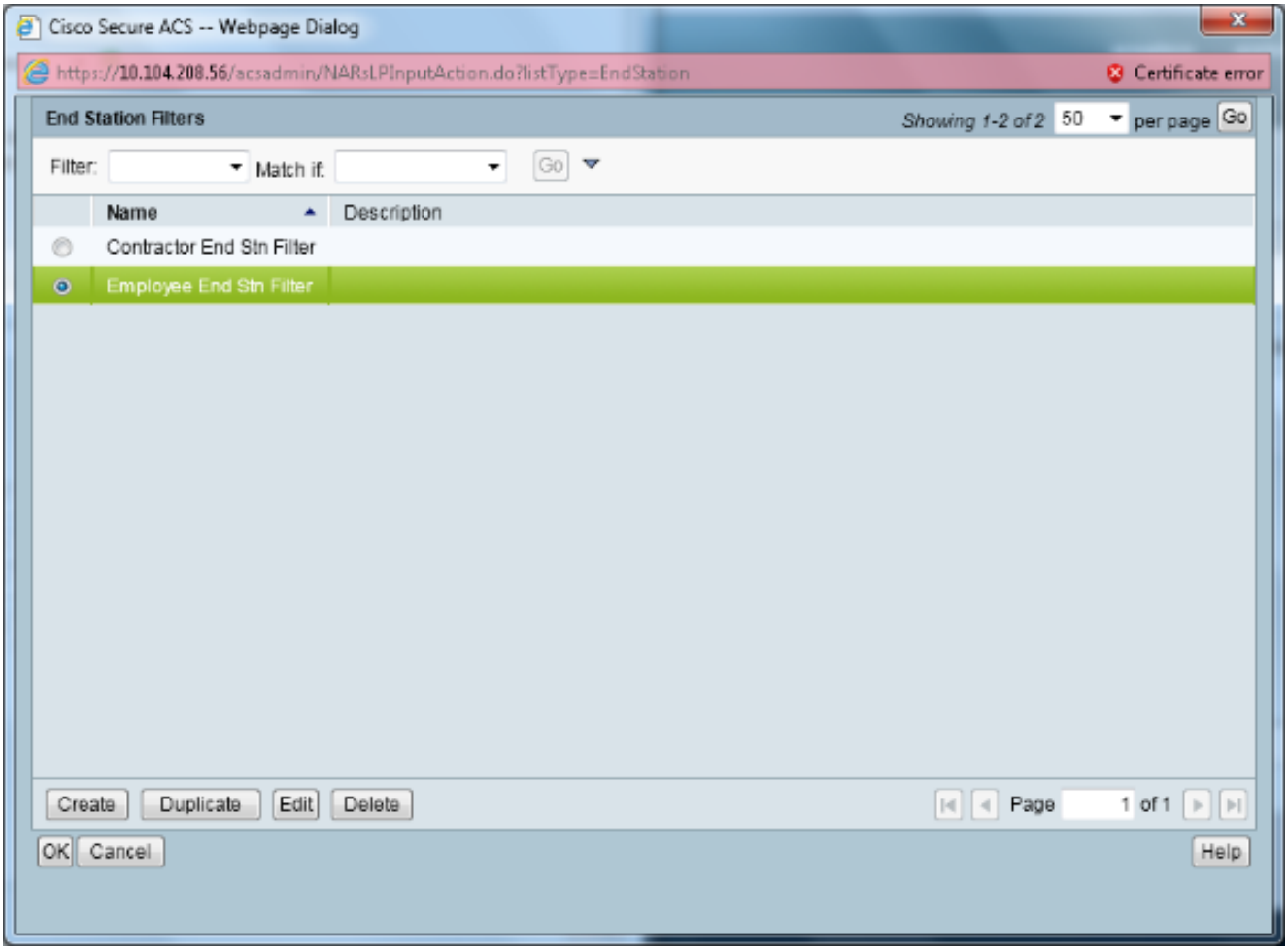
Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standardnetzwerkzugriff > Autorisierung aus.** Klicken Sie auf **Anpassen** und fügen Sie die angepassten Bedingungen hinzu. In diesem Beispiel werden in dieser Reihenfolge Identity Group, NDG:Device Type (Gerätetyp) und End Station Filter (Endgeräte-Filter) verwendet.



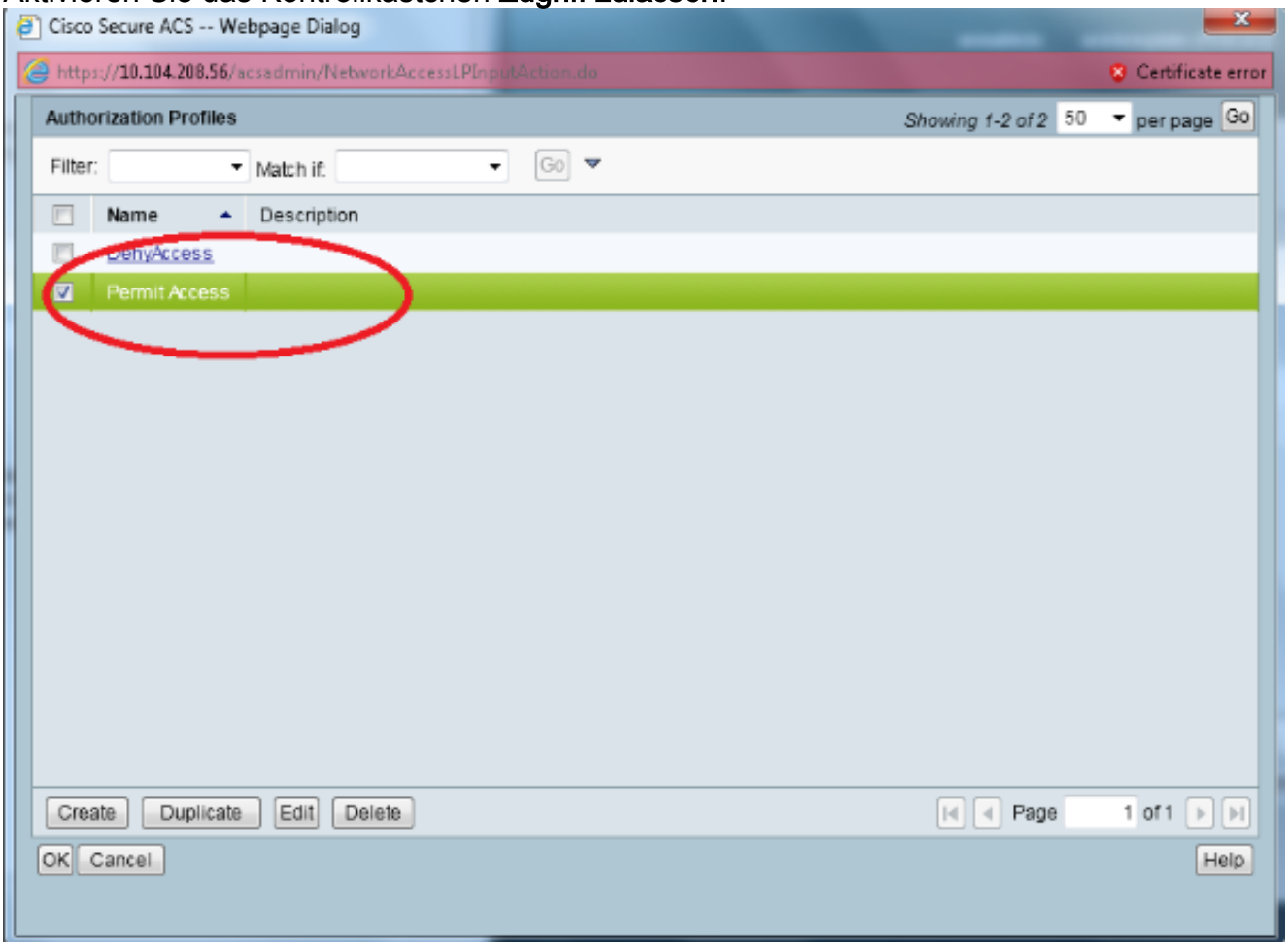
Klicken Sie auf **Erstellen**. Nennen Sie die Regel, und wählen Sie unter Alle Gruppen die entsprechende Identitätsgruppe aus. In diesem Beispiel ist dies Employee.



Klicken Sie auf das Optionsfeld **Employee End Stn Filter**, oder geben Sie den Namen ein, den Sie in Schritt 1b im Abschnitt "Konfigurieren des WLC" eingeben.

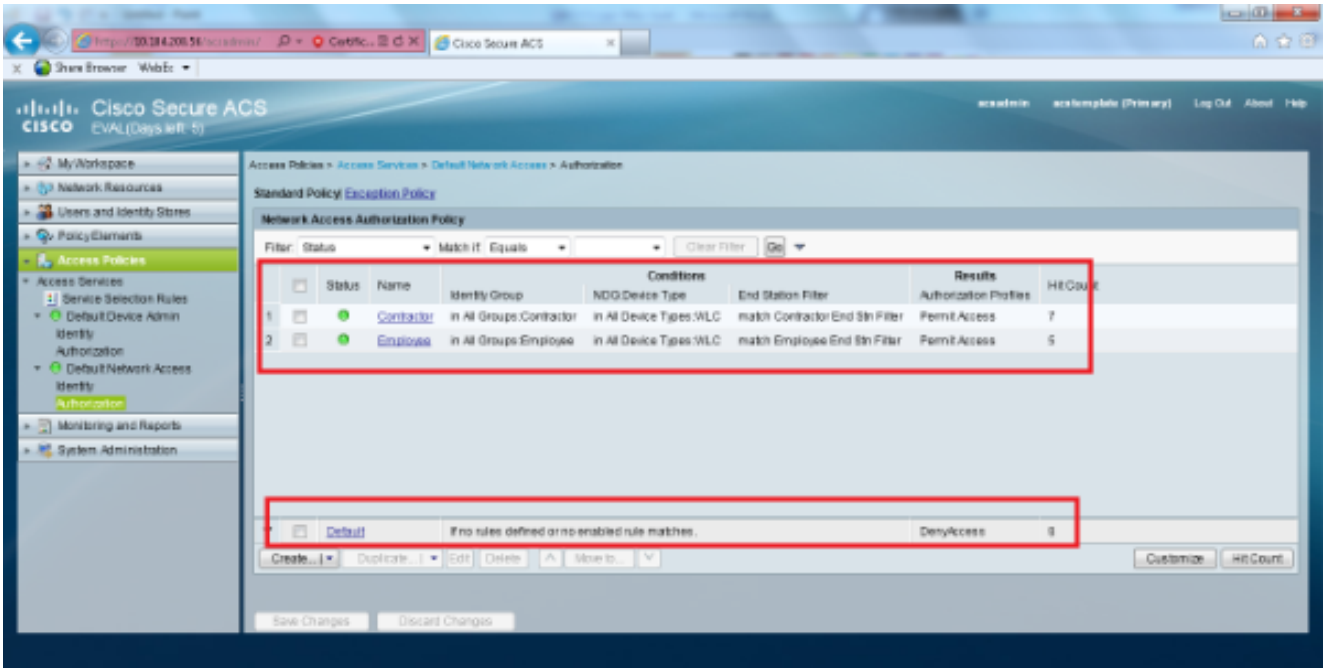


Aktivieren Sie das Kontrollkästchen **Zugriff zulassen**.



Wiederholen Sie die oben genannten Schritte auch für die Regeln des AN. Stellen Sie sicher,

dass die Standardaktion "**Zugriff verweigern**" lautet. Wenn Sie Schritt e abgeschlossen haben, sollten Ihre Regeln wie folgt
aussehen:



Damit ist die Konfiguration abgeschlossen. Nach diesem Abschnitt muss der Client für die Verbindung entsprechend mit der SSID und den Sicherheitsparametern konfiguriert werden.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.