Exemple de configuration d'authentification ACS version 5.2 et WLC pour chaque WLAN

Contenu

Introduction

Ce document fournit un exemple de configuration pour restreindre l'accès par utilisateur à un réseau local sans fil (WLAN) en fonction de l'identificateur SSID (Service Set Identifier).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment configurer le contrôleur de réseau local sans fil (WLC) et le point d'accès léger (LAP) pour un fonctionnement de base
- Configuration du serveur de contrôle d'accès sécurisé Cisco (ACS)
- Méthodes de sécurité LWAPP (Lightweight Access Point Protocol) et sans fil

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC de la gamme Cisco 5500 qui exécute le microprogramme version 7.4.110
- LAP de la gamme Cisco 1142
- Serveur Cisco Secure ACS Version 5.2.0.26.11

Configuration

Pour configurer les périphériques de cette configuration, vous devez :

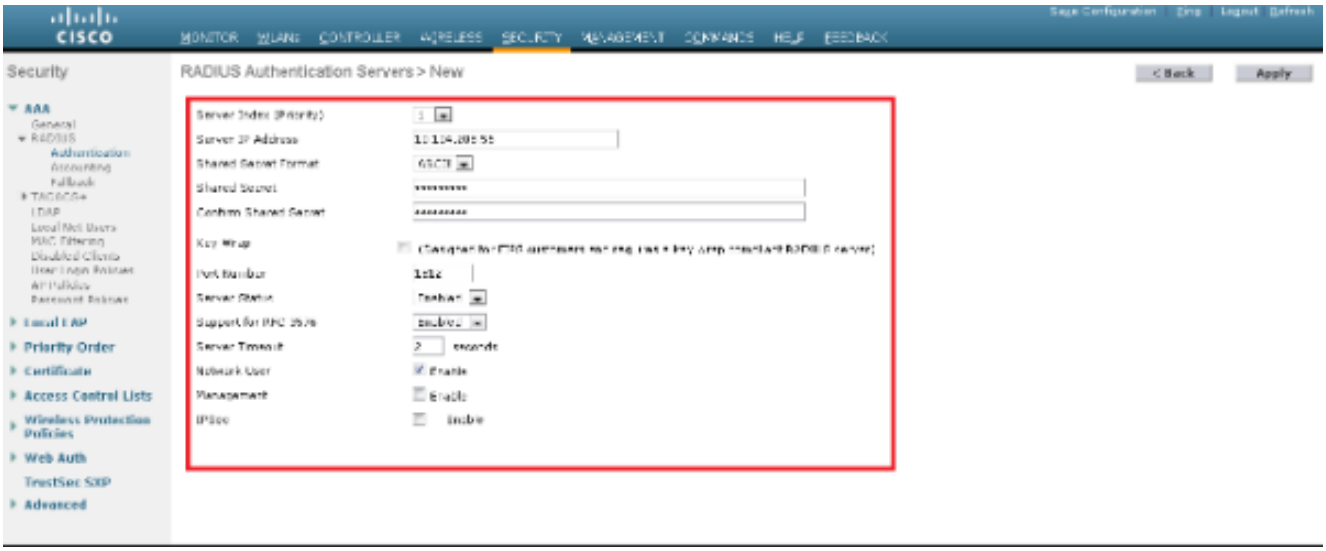
1. Configurez le WLC pour les deux WLAN et le serveur RADIUS.
2. Configurez Cisco Secure ACS.
3. Configurez les clients sans fil et vérifiez la configuration.

Configurer le WLC

Complétez ces étapes afin de définir le WLC pour cette configuration :

1. Configurez le WLC afin de transmettre les informations d'identification de l'utilisateur à un serveur RADIUS externe. Le serveur RADIUS externe (Cisco Secure ACS dans ce cas) valide ensuite les informations d'identification de l'utilisateur et fournit l'accès aux clients sans fil. Procédez comme suit : Sélectionnez **Security > RADIUS Authentication** dans l'interface graphique du contrôleur afin d'afficher la page RADIUS Authentication Servers.

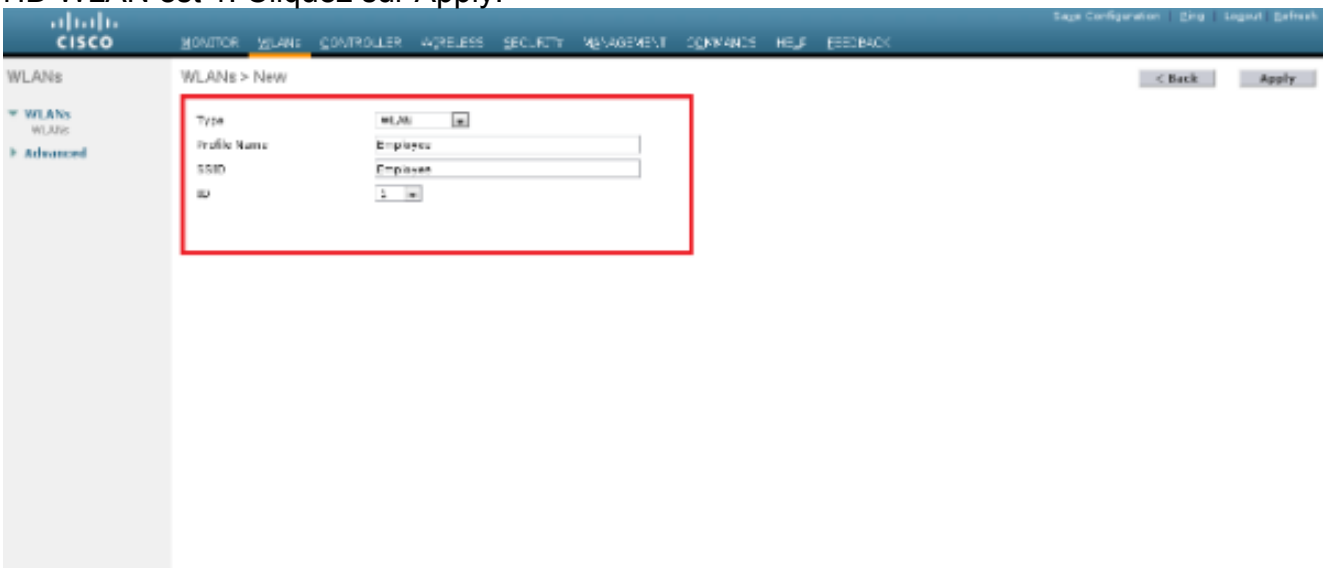
Cliquez sur **Nouveau** afin de définir les paramètres du serveur RADIUS. Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du serveur. Les cases à cocher Network User and Management déterminent si l'authentification RADIUS s'applique à la gestion et aux utilisateurs réseau. Cet exemple utilise Cisco Secure ACS comme serveur RADIUS avec l'adresse IP 10.104.208.56.



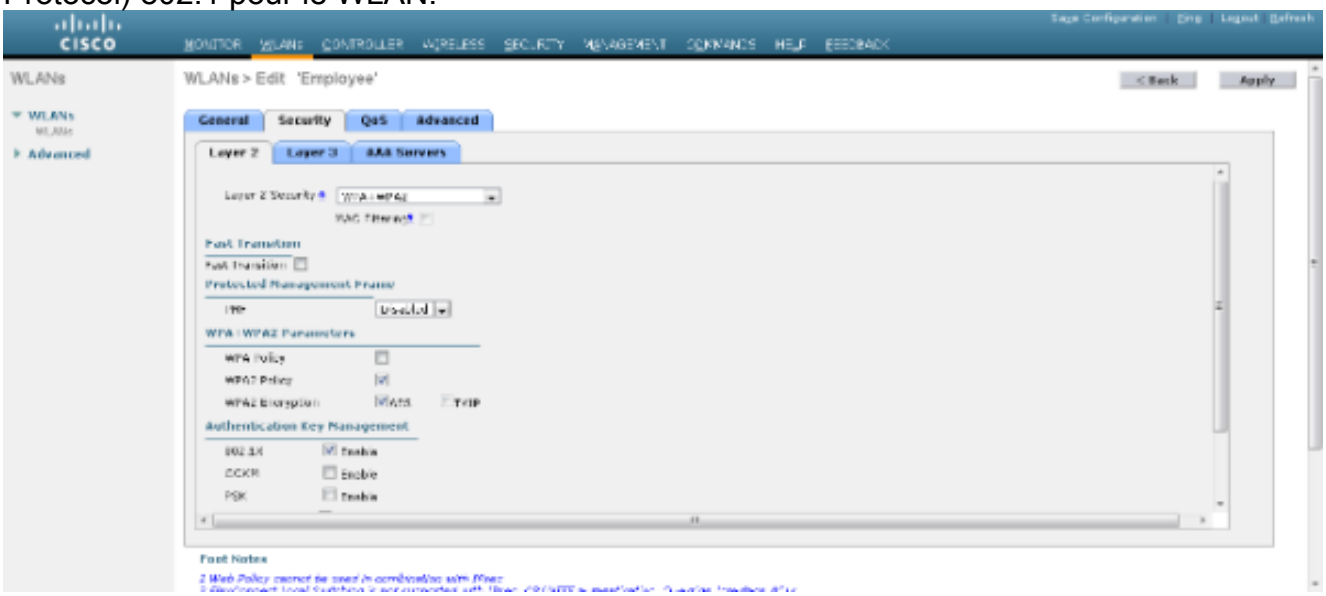
Cliquez sur Apply.

2. Complétez ces étapes afin de configurer un WLAN pour l'Employé avec SSID **Employee** et l'autre WLAN pour les Entrepreneurs avec SSID **Entrepreneur**. Cliquez sur **WLANs depuis**

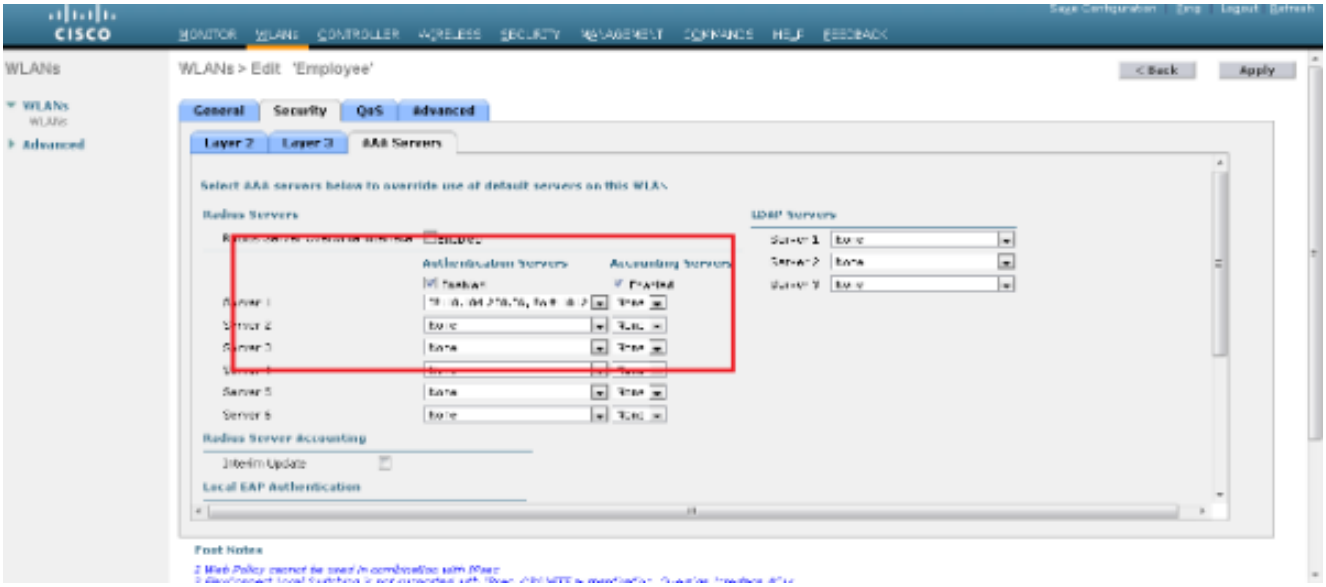
l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN. La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.Cliquez sur **New pour configurer un nouveau WLAN.**Cet exemple crée un WLAN nommé Employee et l'ID WLAN est 1. Cliquez sur Apply.



Sélectionnez la fenêtre **WLAN > Edit** et définissez les paramètres spécifiques au WLAN : Dans l'onglet Sécurité de couche 2, sélectionnez **802.1x**. Par défaut, l'option de sécurité de couche 2 est 802.1x. Cela active les authentifications EAP (Extensible Authentication Protocol) 802.1 pour le WLAN.



Dans l'onglet AAA servers, sélectionnez le serveur RADIUS approprié dans la liste déroulante sous RADIUS Servers. Les autres paramètres peuvent être modifiés sur les conditions requises du réseau WLAN. Cliquez sur Apply.



De même, afin de créer un WLAN pour les entrepreneurs, répétez les étapes b à d.

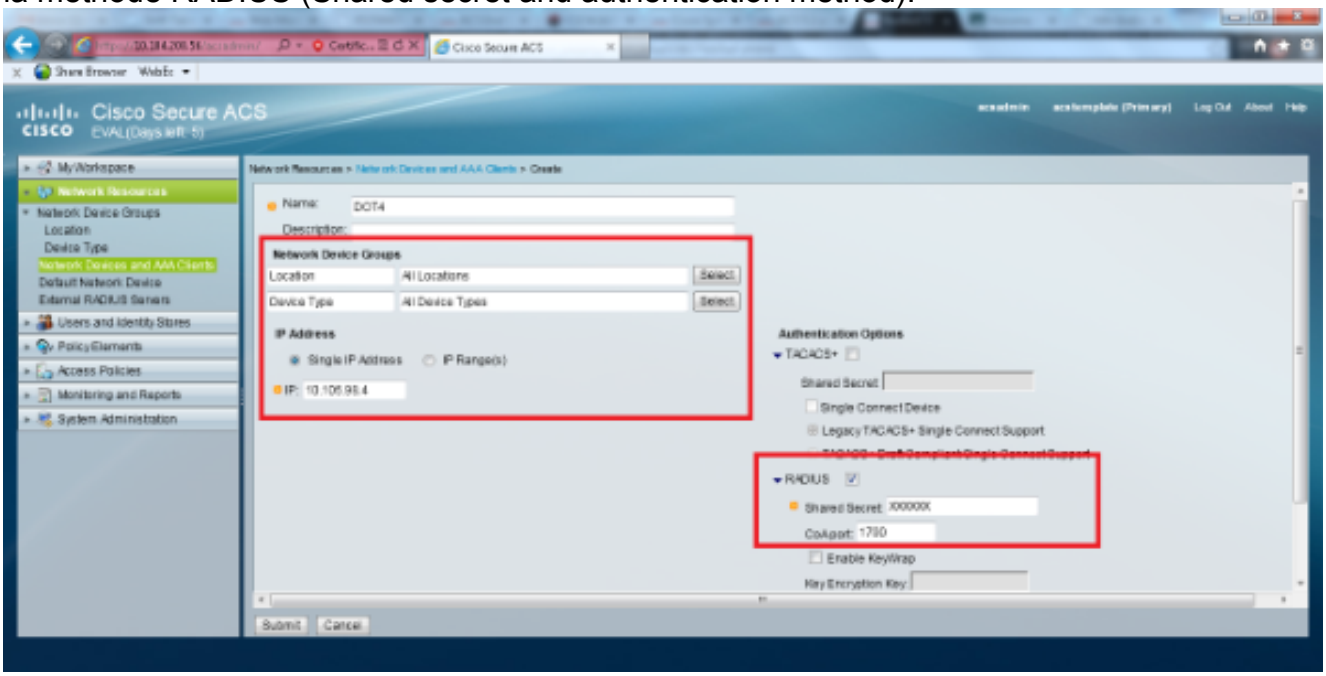
Configurer Cisco Secure ACS

Sur le serveur Cisco Secure ACS, vous devez :

1. Configurez le WLC en tant que client AAA.
2. Créez la base de données utilisateur (informations d'identification) pour l'authentification basée sur le SSID.
3. Activez l'authentification EAP.

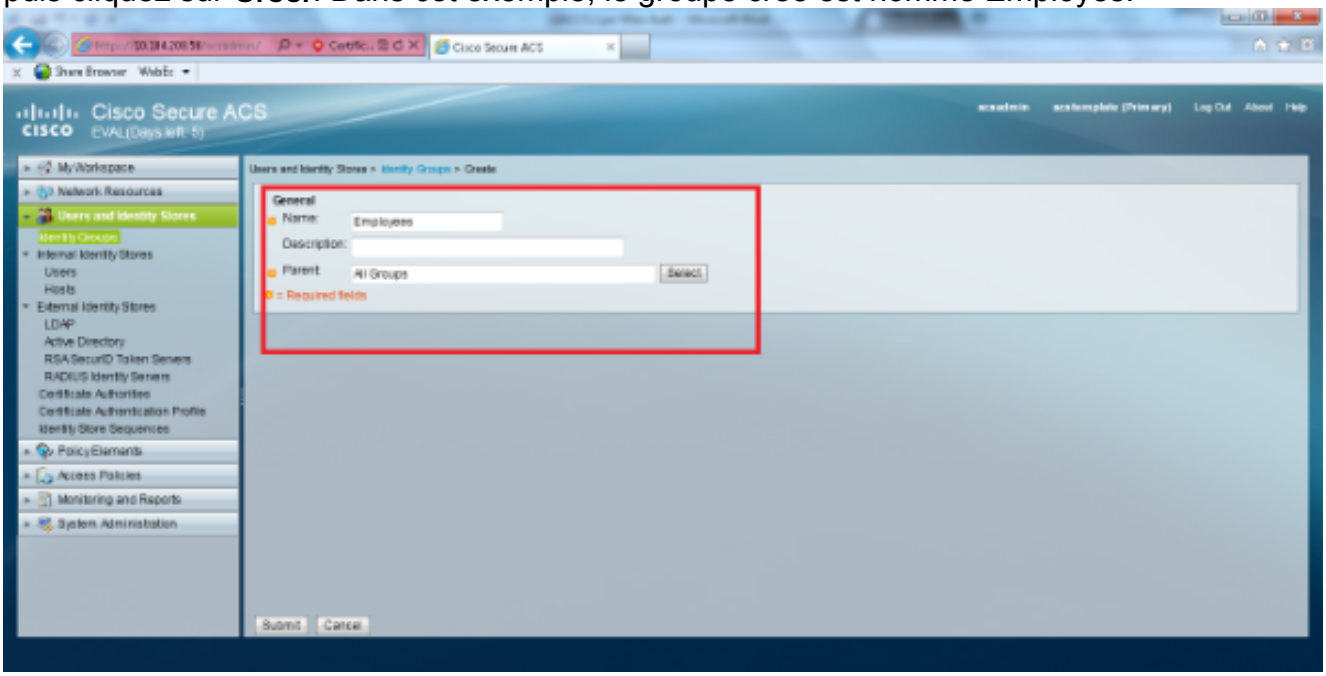
Suivez ces étapes sur Cisco Secure ACS :

1. Afin de définir le contrôleur en tant que client AAA sur le serveur ACS, sélectionnez **Ressources réseau > Périphériques réseau et clients AAA** dans l'interface utilisateur graphique ACS. Sous Network Devices and AAA Clients**,** cliquez sur **Create.**
2. Lorsque la page Network Configuration apparaît, définissez le nom du WLC, l'adresse IP et la méthode RADIUS (Shared secret and authentication method).

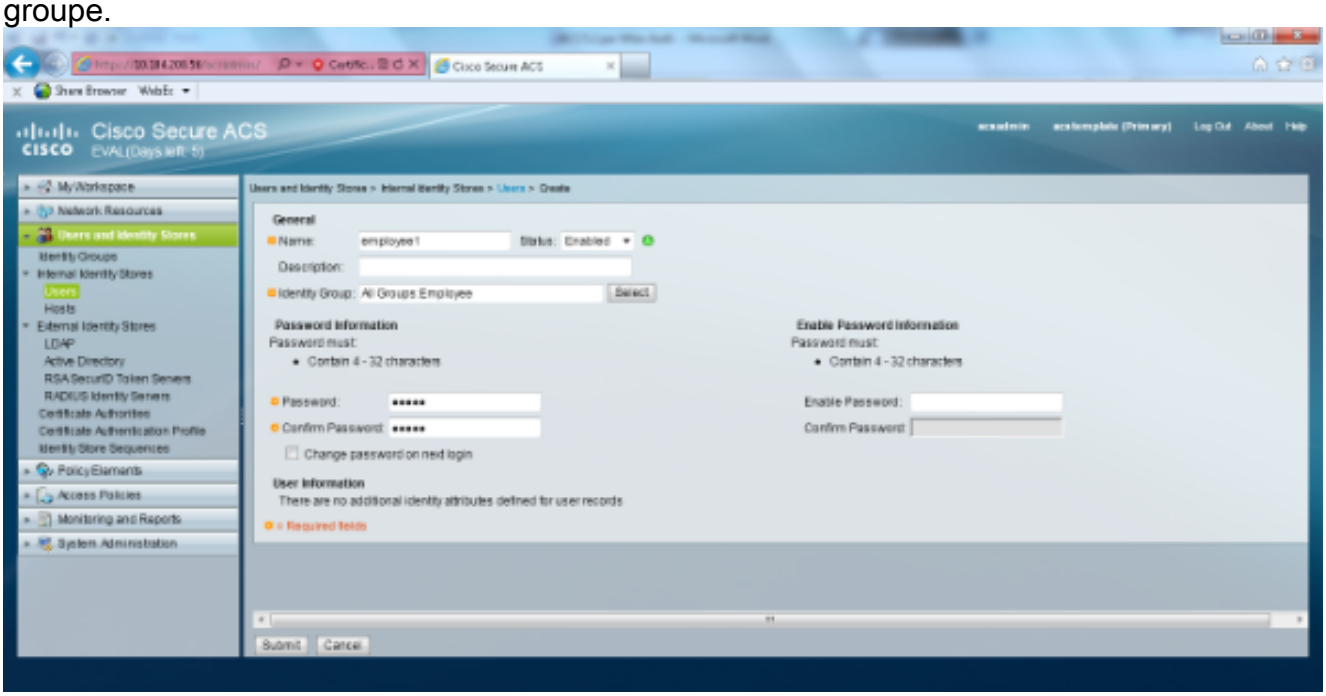


3. Sélectionnez **Utilisateurs et magasins d'identités > Groupes d'identités** dans l'interface

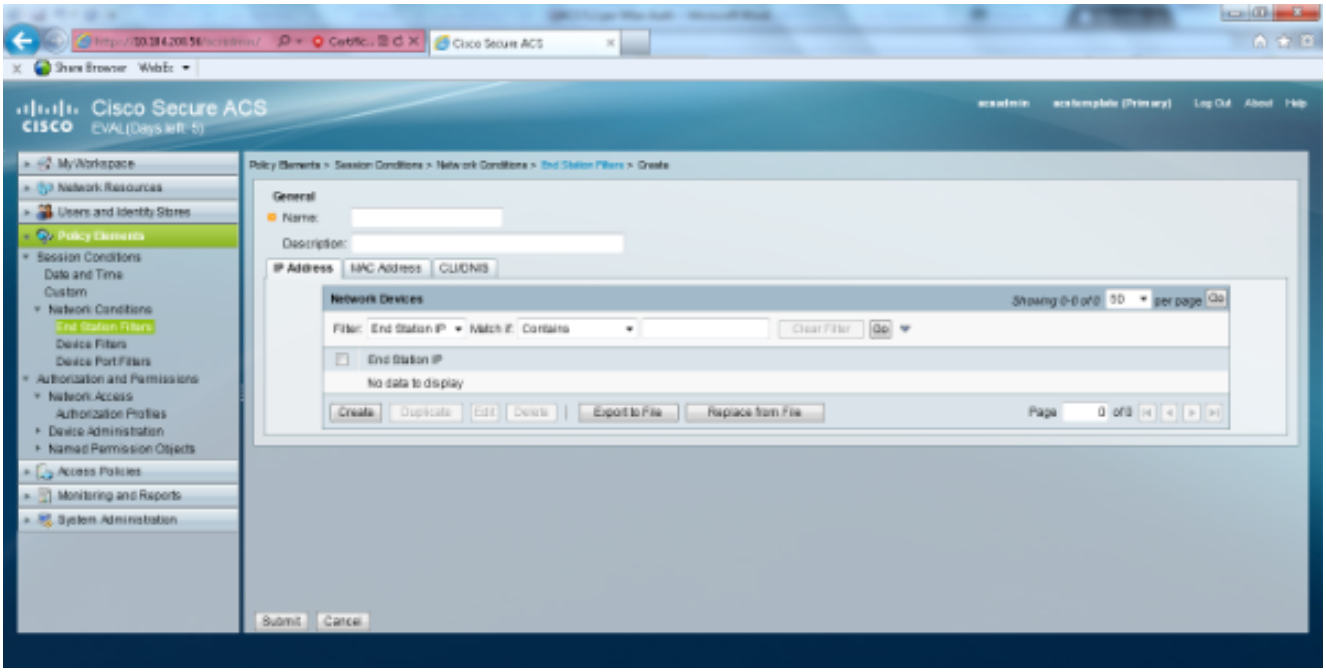
utilisateur graphique ACS. Créez les groupes respectifs des employés et des sous-traitants, puis cliquez sur **Créer**. Dans cet exemple, le groupe créé est nommé Employés.



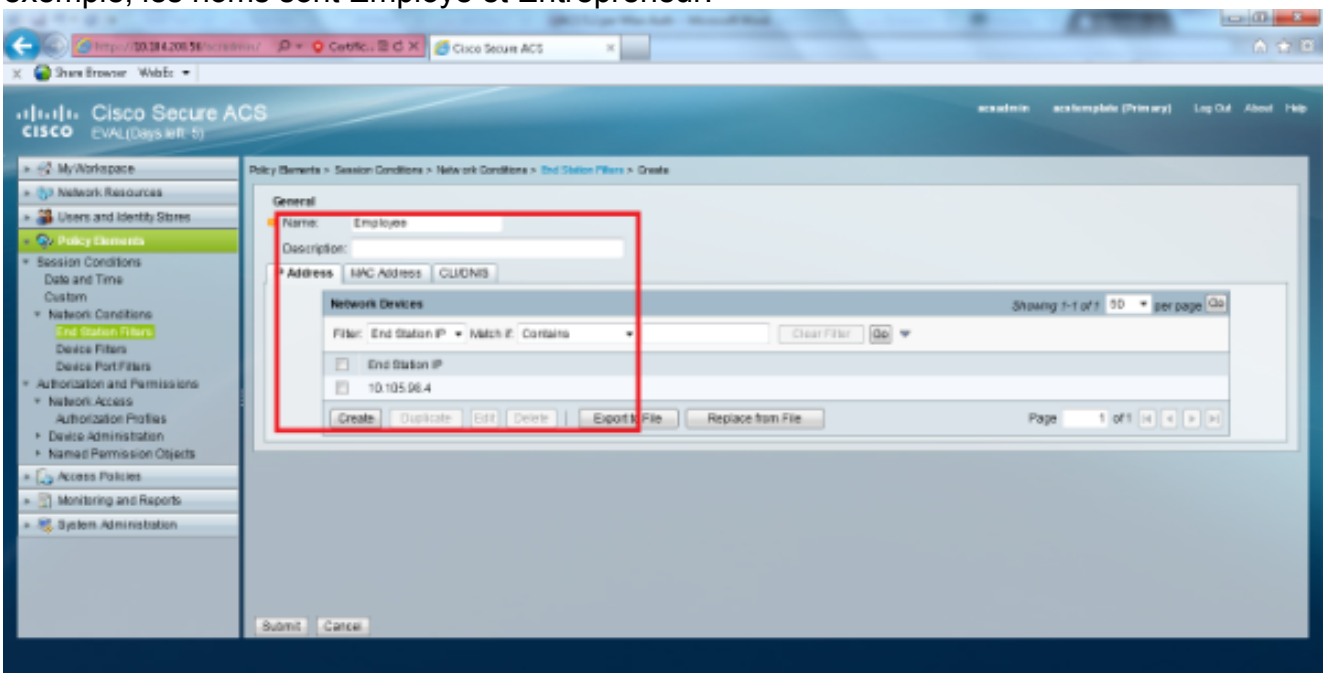
4. Sélectionnez **Utilisateurs et magasins d'identité > Magasins d'identité internes**. Cliquez sur **Créer** et saisissez le nom d'utilisateur. Placez-les dans le groupe approprié, définissez leur mot de passe et cliquez sur **Soumettre**.Dans cet exemple, un utilisateur nommé Employee1 est créé dans le groupe Employee. De même, créez un utilisateur nommé entrepreneur1 sous les sous-traitants de
groupe.



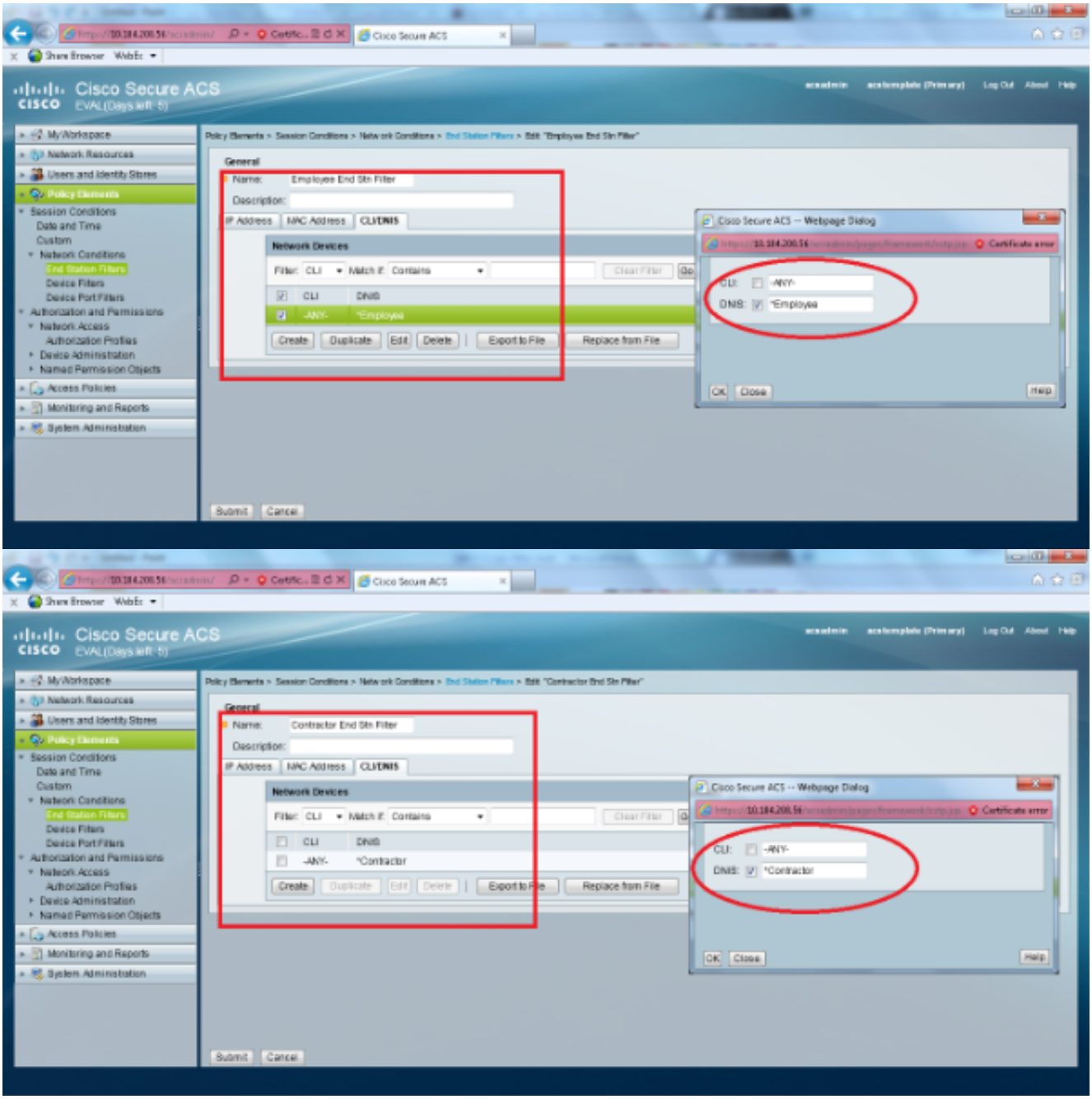
5. Sélectionnez **Eléments de stratégie > Conditions réseau > Filtres de station d'extrémité**. Click **Create**.



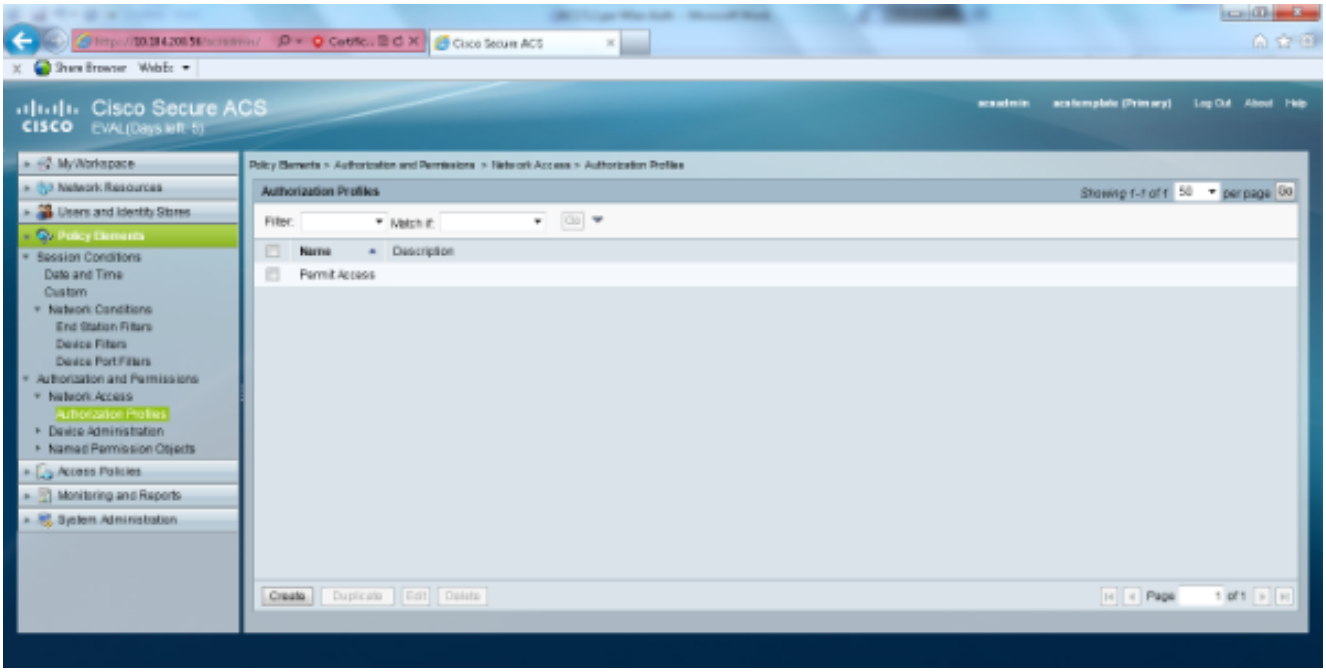
Entrez un nom significatif et sous l'onglet **Adresse IP**, entrez l'adresse IP du WLC. Dans cet exemple, les noms sont Employé et Entrepreneur.



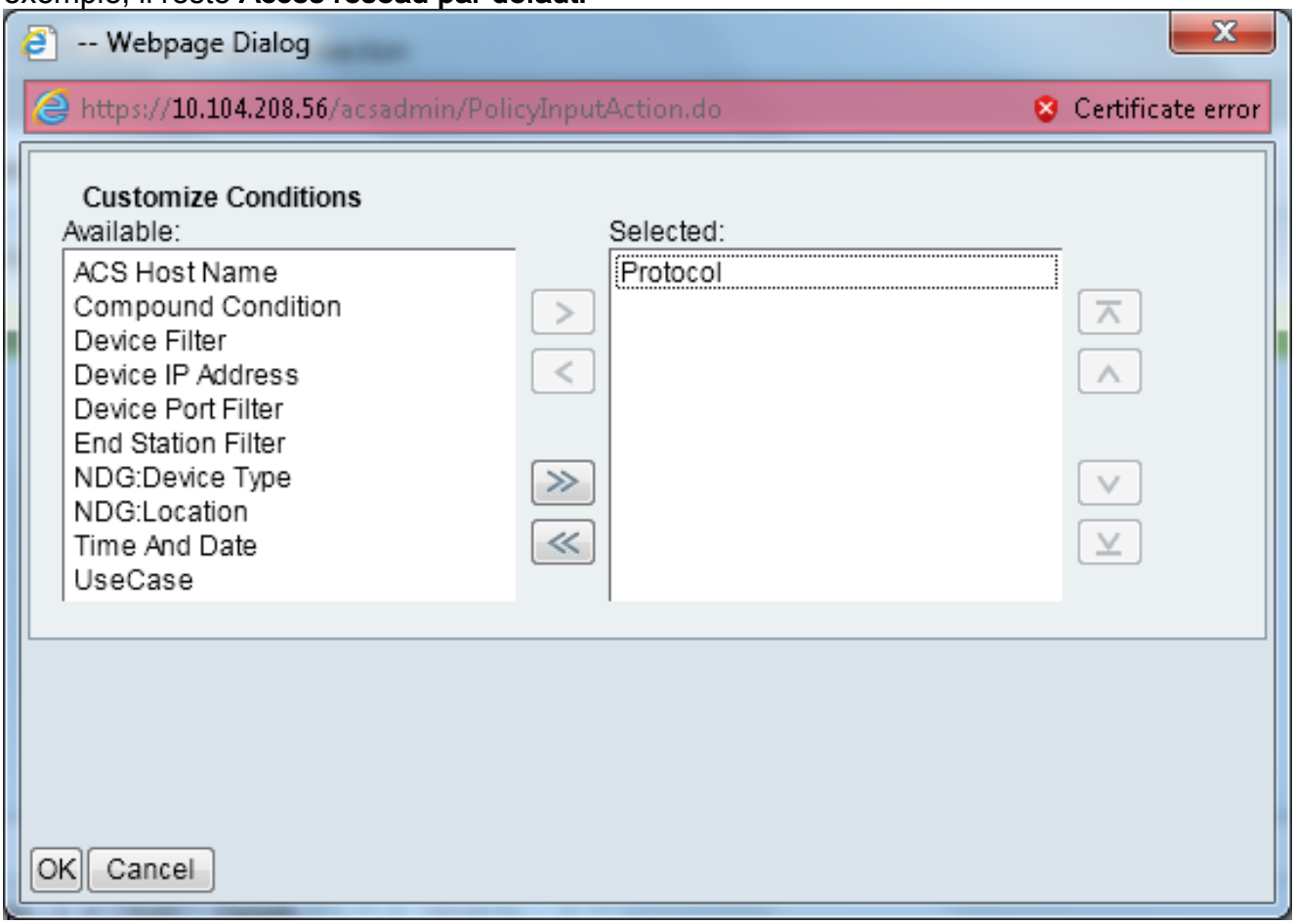
Sous l'onglet CLI/DNIS, laissez CLI comme -ANY- et saisissez DNIS comme *<SSID>. Dans cet exemple, le champ DNIS est entré en tant que *Employé car ce filtre de station d'extrémité est utilisé pour restreindre l'accès uniquement au WLAN Employé. L'attribut DNIS définit le SSID auquel l'utilisateur est autorisé à accéder. Le WLC envoie le SSID dans l'attribut DNIS au serveur RADIUS.Répétez les mêmes étapes pour le filtre de station d'extrémité du fournisseur.

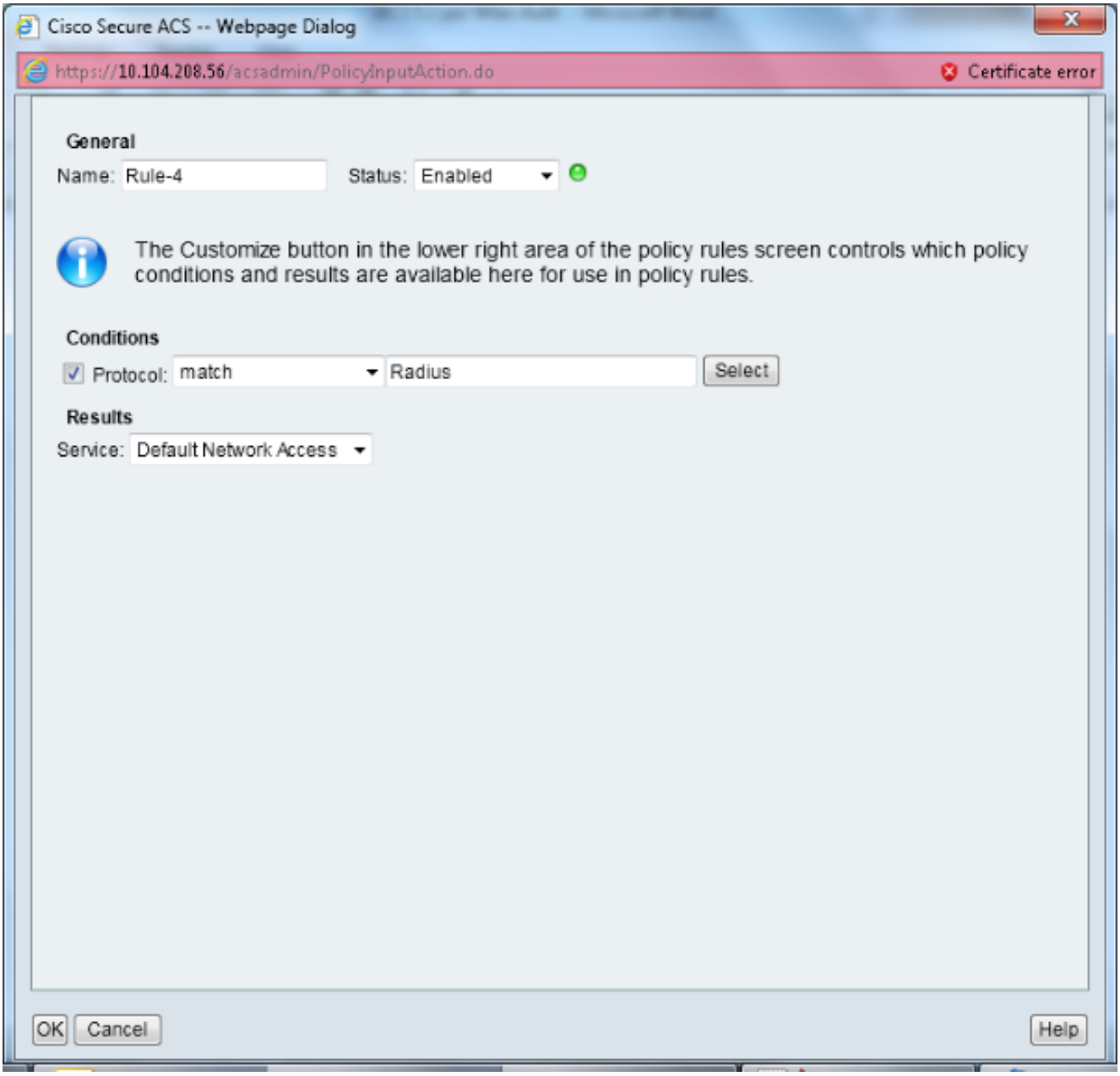


6. Sélectionnez **Eléments de stratégie > Autorisation et autorisations > Accès réseau > Profils d'autorisation**. Il doit exister un profil par défaut pour Autoriser l'accès.

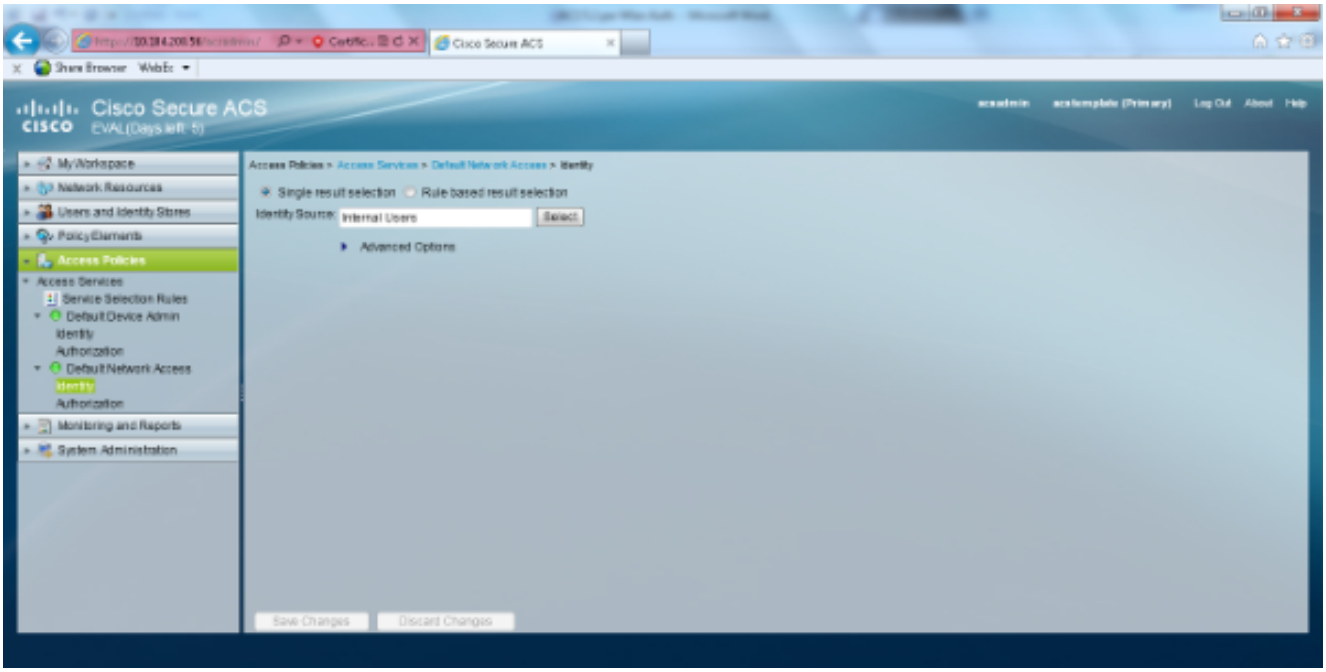


7. Sélectionnez **Politiques d'accès > Services d'accès > Règles de sélection de service**. Cliquez sur **Personnaliser**. Ajoutez toute condition appropriée. Cet exemple utilise Protocol comme Radius comme condition correspondante.Click **Create**. Nommez la règle. Sélectionnez **Protocole** et **Rayon.**Sous **Résultats**, sélectionnez le service d'accès approprié. Dans cet exemple, il reste **Accès réseau par défaut.**

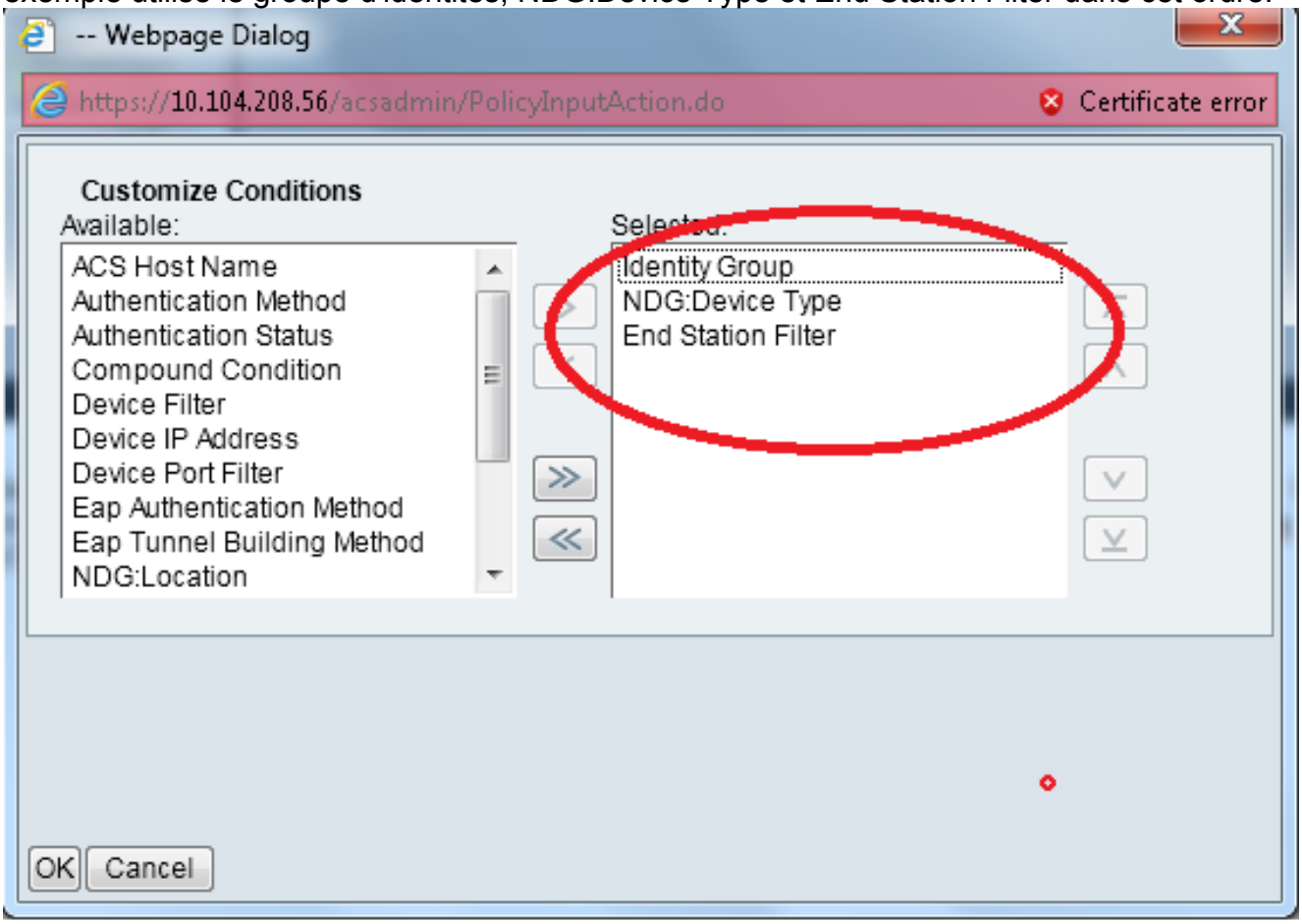




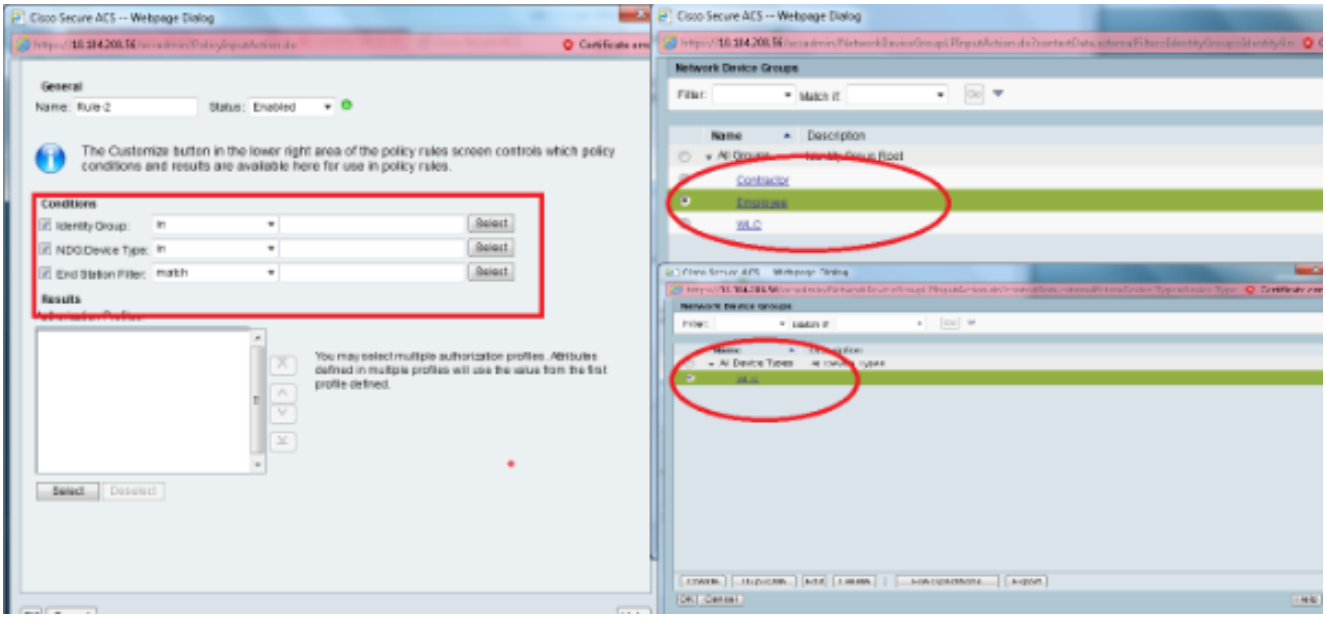
8. Sélectionnez **Access Policies > Access Services > Default Network Access > Identity**. Sélectionnez Sélection de résultats uniques et **Source d'identité** en tant qu'utilisateurs internes.



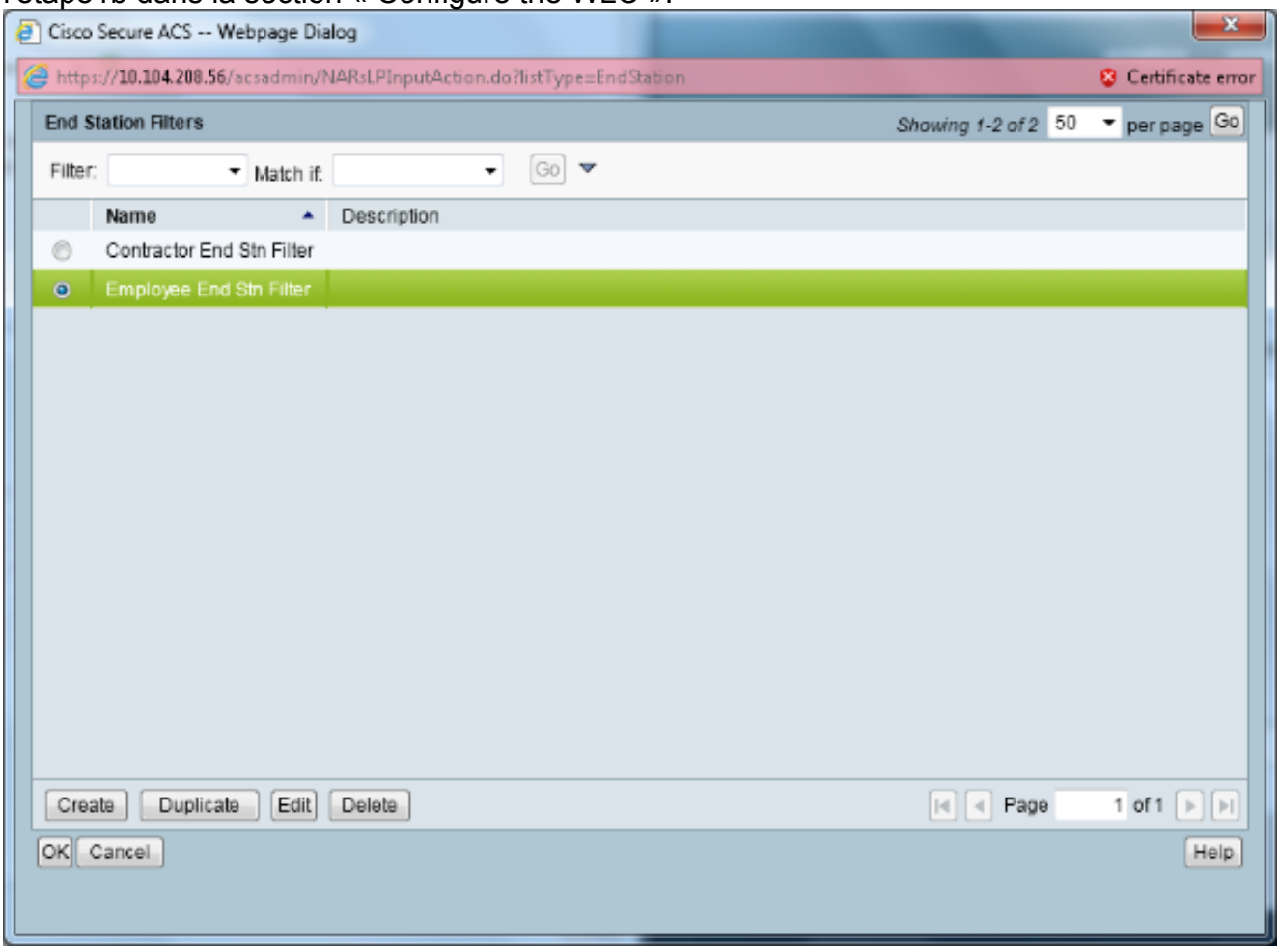
Sélectionnez **Politiques d'accès > Services d'accès > Accès réseau par défaut > Autorisation.** Cliquez sur **Personnaliser** et ajoutez les conditions personnalisées. Cet exemple utilise le groupe d'identités, NDG:Device Type et End Station Filter dans cet ordre.



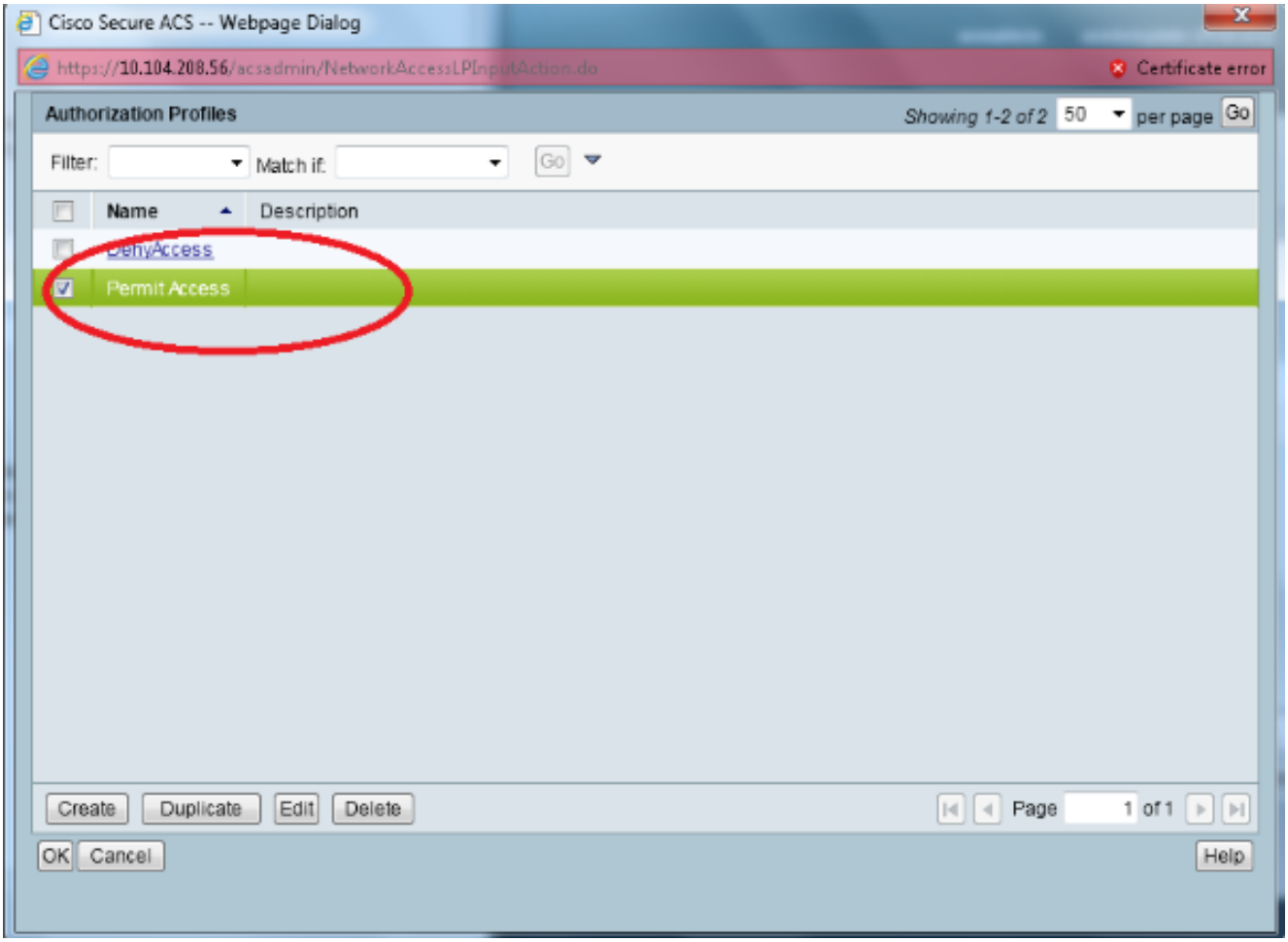
Click **Create**. Nommez la règle et choisissez le groupe d'identités approprié sous Tous les groupes. Dans cet exemple, il s'agit d'Employé.



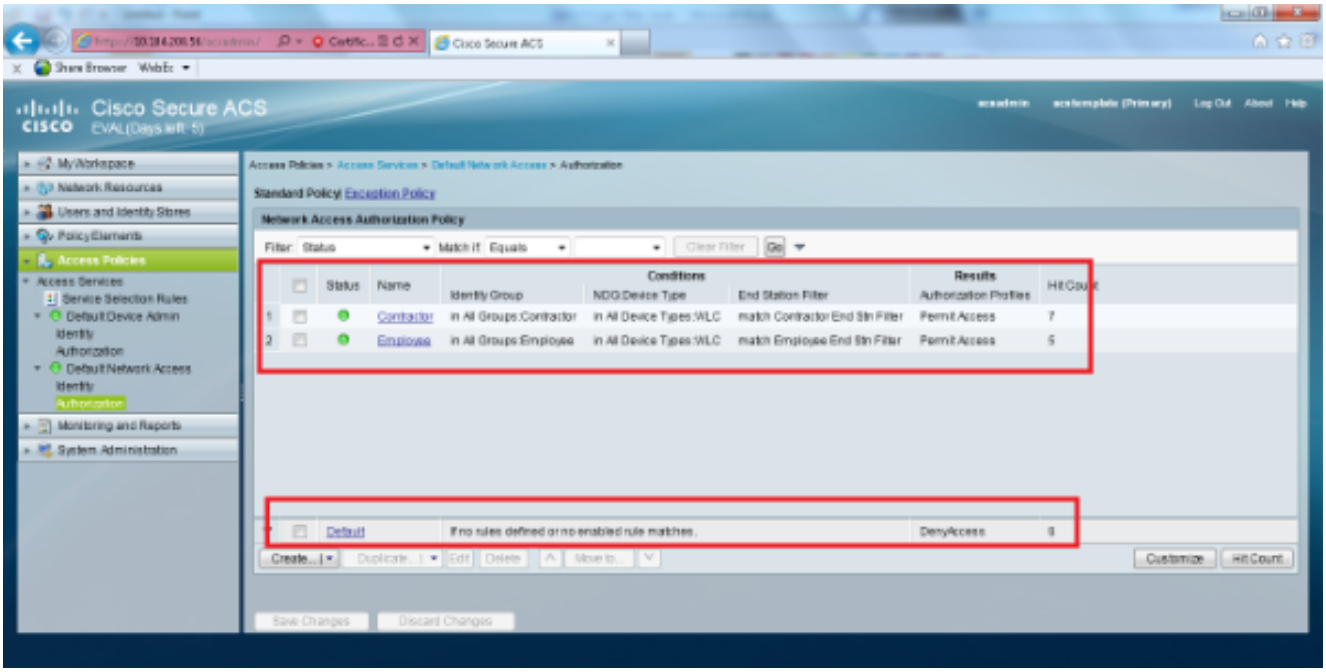
Cliquez sur la case d'option **Employee End Stn Filter** ou entrez le nom que vous avez entré à l'étape1b dans la section « Configure the WLC ».



Cochez la case **Autoriser l'accès**.



Répétez également les mêmes étapes ci-dessus pour les règles de l'entrepreneur. Assurez-vous que l'action par défaut est de **refuser l'accès**. Une fois l'étape e terminée, vos règles doivent ressembler à cet exemple
:



La configuration est terminée. Après cette section, le client doit être configuré en conséquence avec le SSID et les paramètres de sécurité afin de se connecter.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.