

# Exemplo de Configuração do ACS Versão 5.2 e WLC para Autenticação por WLAN

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurar o WLC](#)

[Configurar o Cisco Secure ACS](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

Este documento fornece um exemplo de configuração para restringir o acesso por usuário a uma LAN sem fio (WLAN) com base no identificador do conjunto de serviços (SSID).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar o Wireless LAN Controller (WLC) e o Lightweight Access Point (LAP) para operação básica
- Como configurar o Cisco Secure Access Control Server (ACS)
- Lightweight Access Point Protocol (LWAPP) e métodos de segurança sem fio

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5500 Series WLC que executa a versão de firmware 7.4.110
- LAP Cisco 1142 Series
- Cisco Secure ACS Server versão 5.2.0.26.11

## Configurar

Para configurar os dispositivos para esta configuração, você precisa:

1. Configure a WLC para as duas WLANs e o servidor RADIUS.

2. Configure o Cisco Secure ACS.
3. Configure os clientes sem fio e verifique a configuração.

## Configurar o WLC

Conclua estes passos para configurar a WLC para esta configuração:

1. Configure a WLC para encaminhar as credenciais do usuário a um servidor RADIUS externo. O servidor RADIUS externo (Cisco Secure ACS, neste caso) valida as credenciais do usuário e fornece acesso aos clientes sem fio. Conclua estes passos: Selecione **Security > RADIUS Authentication** na GUI do controlador para exibir a página RADIUS Authentication Servers.



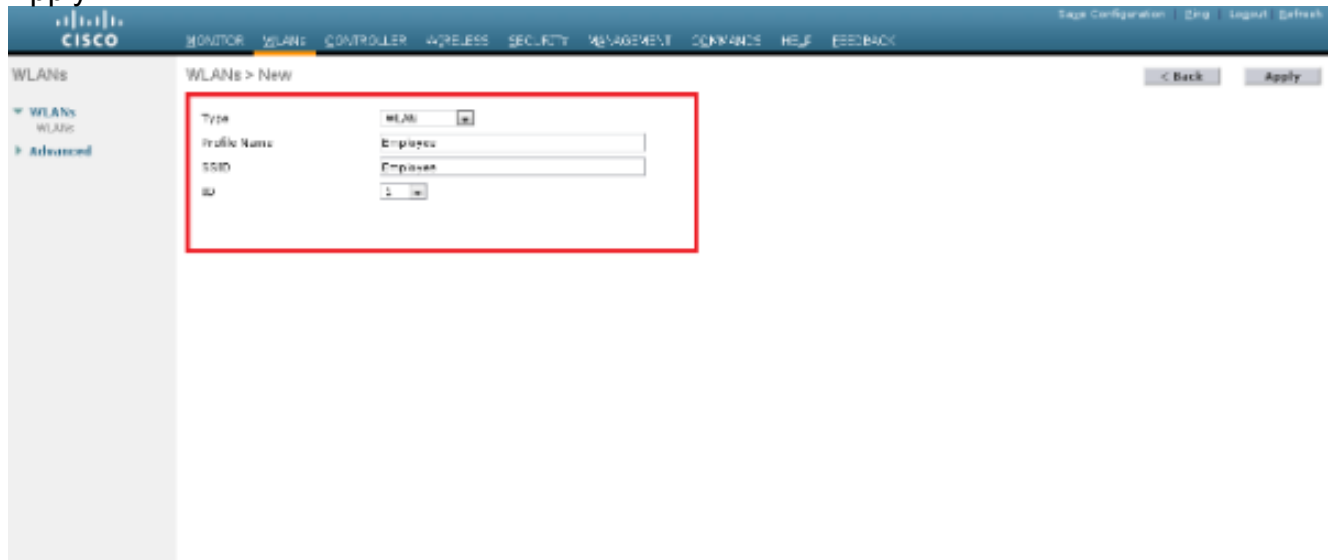
Clique em **New** para definir os parâmetros do servidor RADIUS. Esses parâmetros incluem o endereço IP do servidor RADIUS, o segredo compartilhado, o número da porta e o status do servidor. As caixas de seleção Network User and Management determinam se a autenticação baseada em RADIUS se aplica a usuários de gerenciamento e rede. Este exemplo usa o Cisco Secure ACS como o servidor RADIUS com endereço IP 10.104.208.56.



Clique em **Apply**.

2. Conclua estes passos para configurar uma WLAN para o Funcionário com o **Funcionário** SSID e a outra WLAN para Contratante com o **Contratante** de SSID. Clique em **WLANs** na GUI do controlador para criar uma WLAN. A janela WLANs será exibida. Essa janela lista as

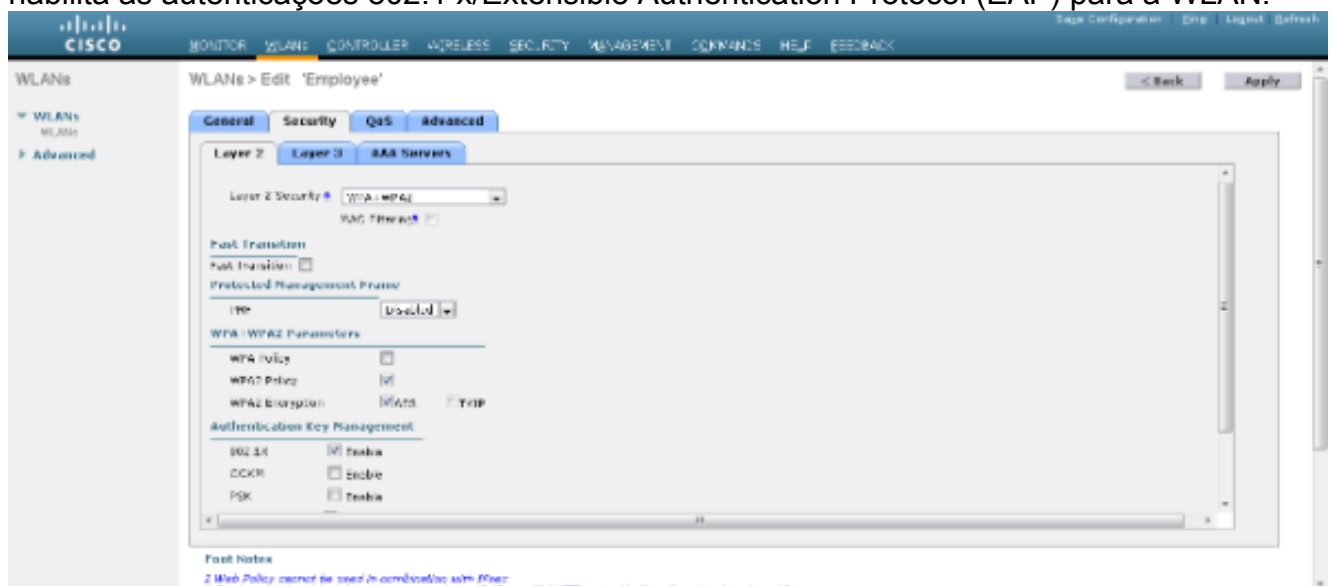
WLANs configuradas no controlador. Clique em **Novo para configurar uma nova WLAN**. Este exemplo cria uma WLAN chamada Employee (Funcionário) e a ID da WLAN é 1. Clique em **Apply**.



The screenshot shows the Cisco configuration interface for creating a new WLAN. The page title is 'WLANs > New'. The form contains the following fields:

Type	WLAN
Profile Name	Employee
SSID	Employee
ID	1

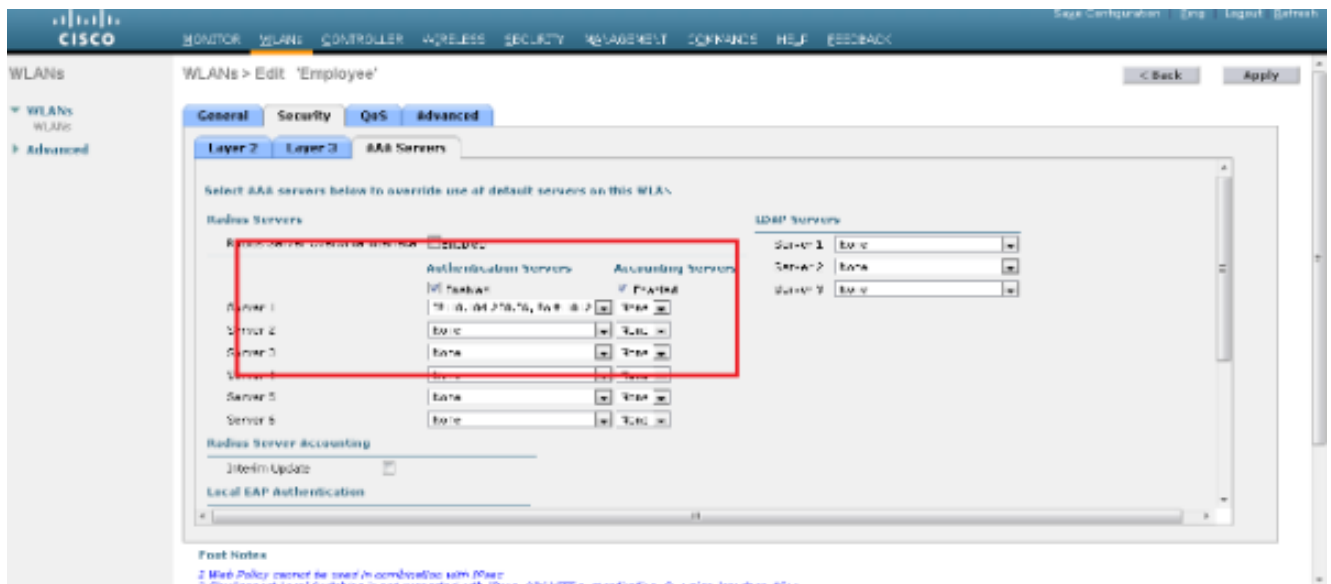
Selecione a janela **WLAN > Edit** e defina os parâmetros específicos da WLAN: Na guia Layer 2 Security, selecione **802.1x**. Por padrão, a opção Layer 2 Security é 802.1x. Isso habilita as autenticações 802.1 x/Extensible Authentication Protocol (EAP) para a WLAN.



The screenshot shows the Cisco configuration interface for editing the 'Employee' WLAN. The page title is 'WLANs > Edit: Employee'. The 'Layer 2 Security' is set to 'WPA + WPA2'. The 'AAA Servers' tab is selected, showing a list of servers with 'RADIUS' selected.

Layer 2 Security	AAA Servers
WPA + WPA2	RADIUS

Na guia servidores AAA, selecione o servidor RADIUS apropriado na lista suspensa em Servidores RADIUS. Os outros parâmetros podem ser modificados com base no requisito da rede WLAN. Clique em **Apply**.



Da mesma forma, para criar uma WLAN para os Contratante, repita as etapas de b a d.

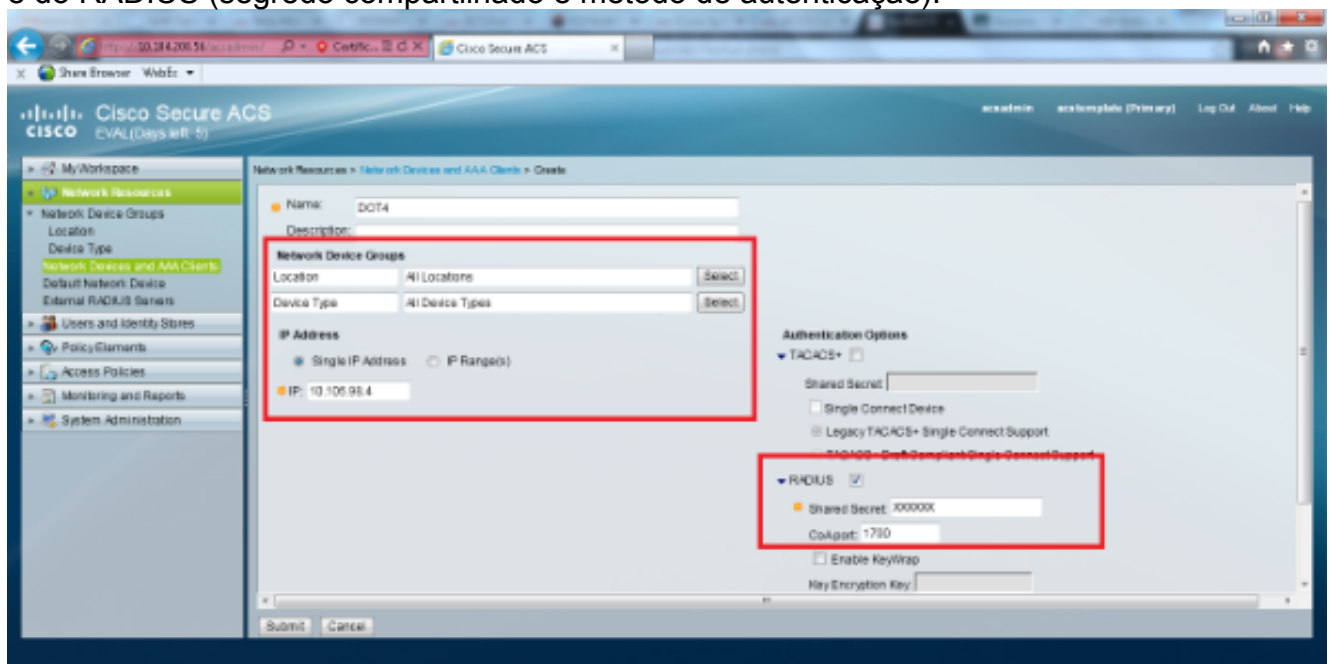
## Configurar o Cisco Secure ACS

No servidor Cisco Secure ACS você precisa:

1. Configure a WLC como um cliente AAA.
2. Crie o banco de dados de usuários (Credenciais) para autenticação baseada em SSID.
3. Ative a autenticação EAP.

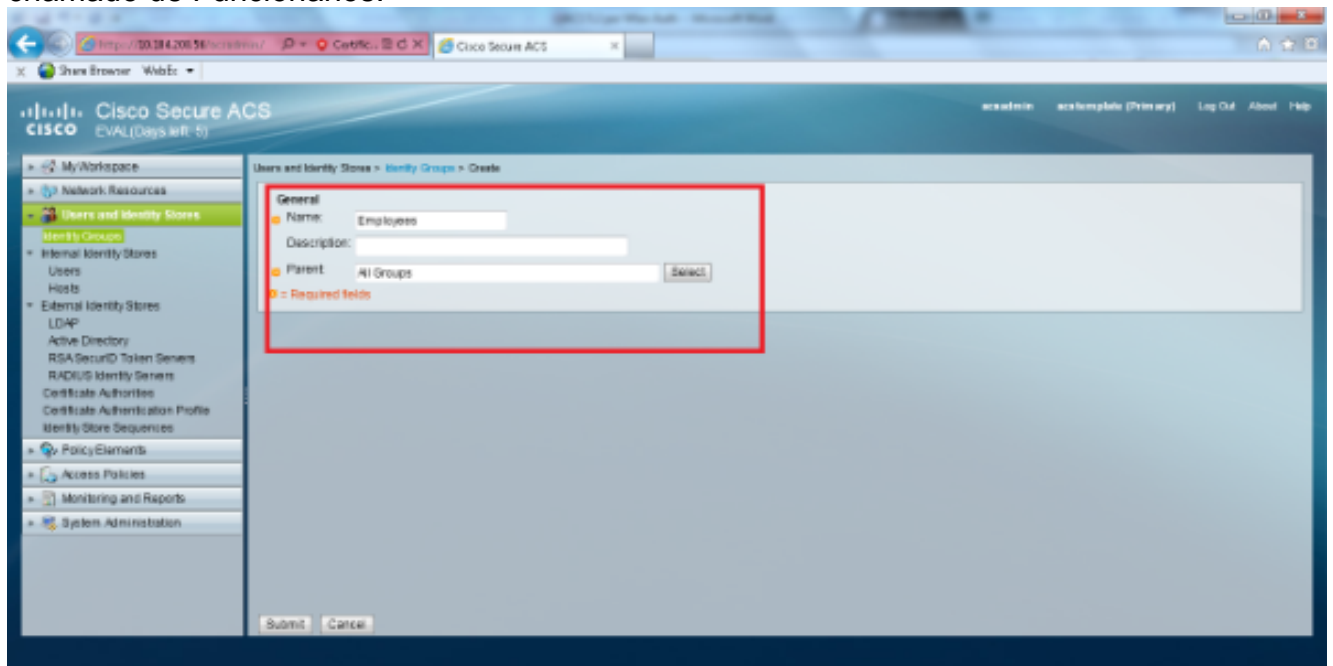
Conclua estes passos no Cisco Secure ACS:

1. Para definir o controlador como um cliente AAA no servidor ACS, selecione **Network Resources > Network Devices and AAA Clients** na GUI do ACS. Em Dispositivos de rede e Clientes AAA, clique em **Criar**.
2. Quando a página Network Configuration for exibida, defina o nome da WLC, do endereço IP e do RADIUS (segredo compartilhado e método de autenticação).

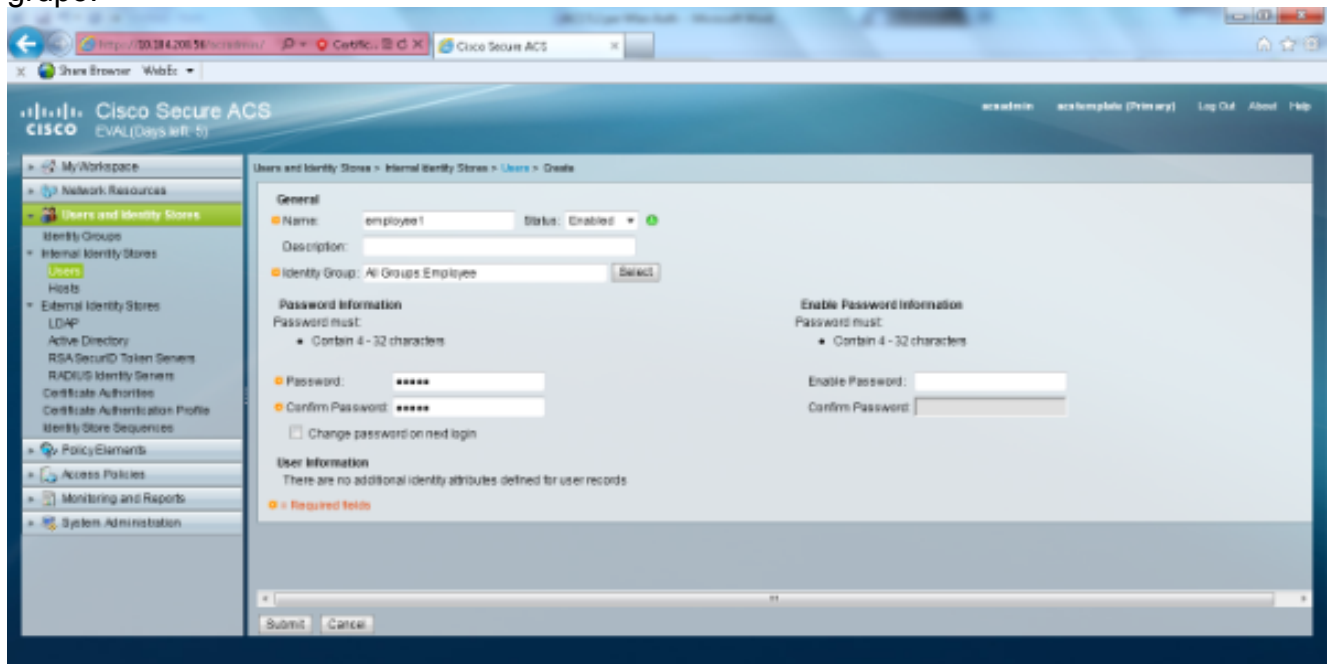


3. Selecione **Users and Identity Stores > Identity Groups** na GUI do ACS. Crie os respectivos Grupos para Funcionário e Contratante e clique em **Criar**. Neste exemplo, o grupo criado é

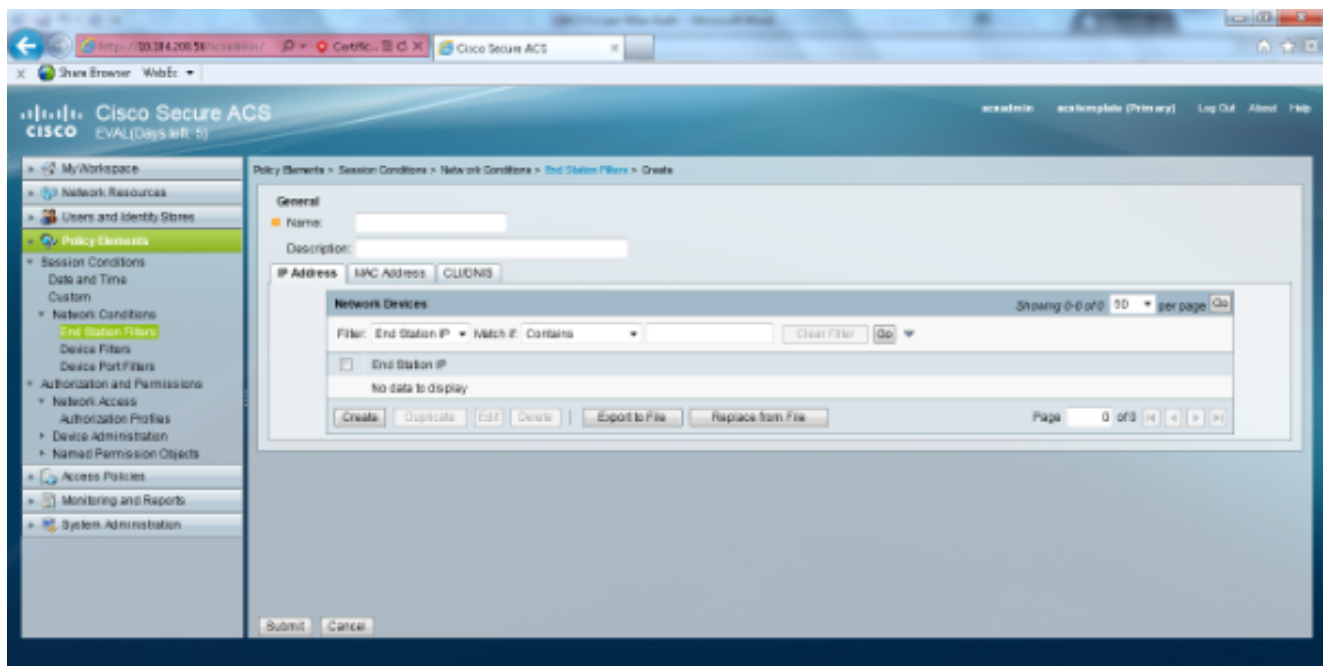
chamado de Funcionários.



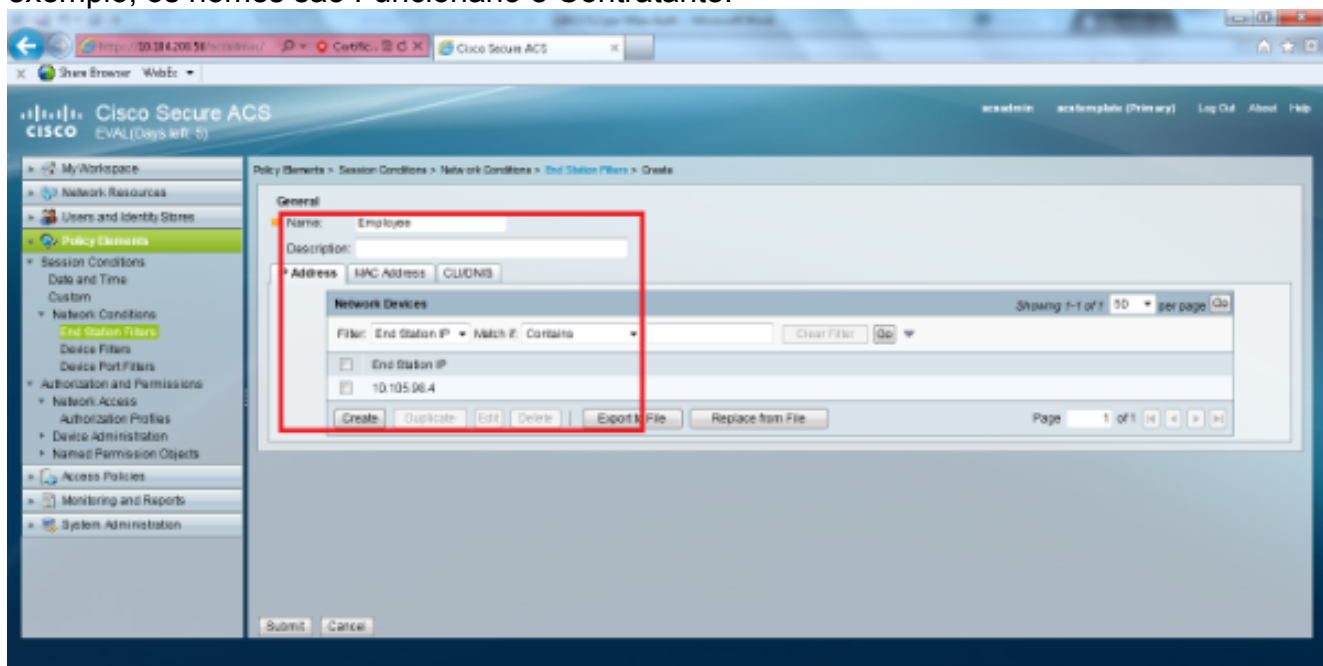
4. Selecione **Usuários e Repositórios de identidades > Repositórios internos de identidades**. Clique em **Criar** e digite o nome de usuário. Coloque-os no grupo correto, defina sua senha e clique em **Enviar**. Neste exemplo, um usuário chamado **funcionário1** no grupo **Funcionário** é criado. Da mesma forma, crie um usuário chamado **contratante1** sob os **contratados** do grupo.



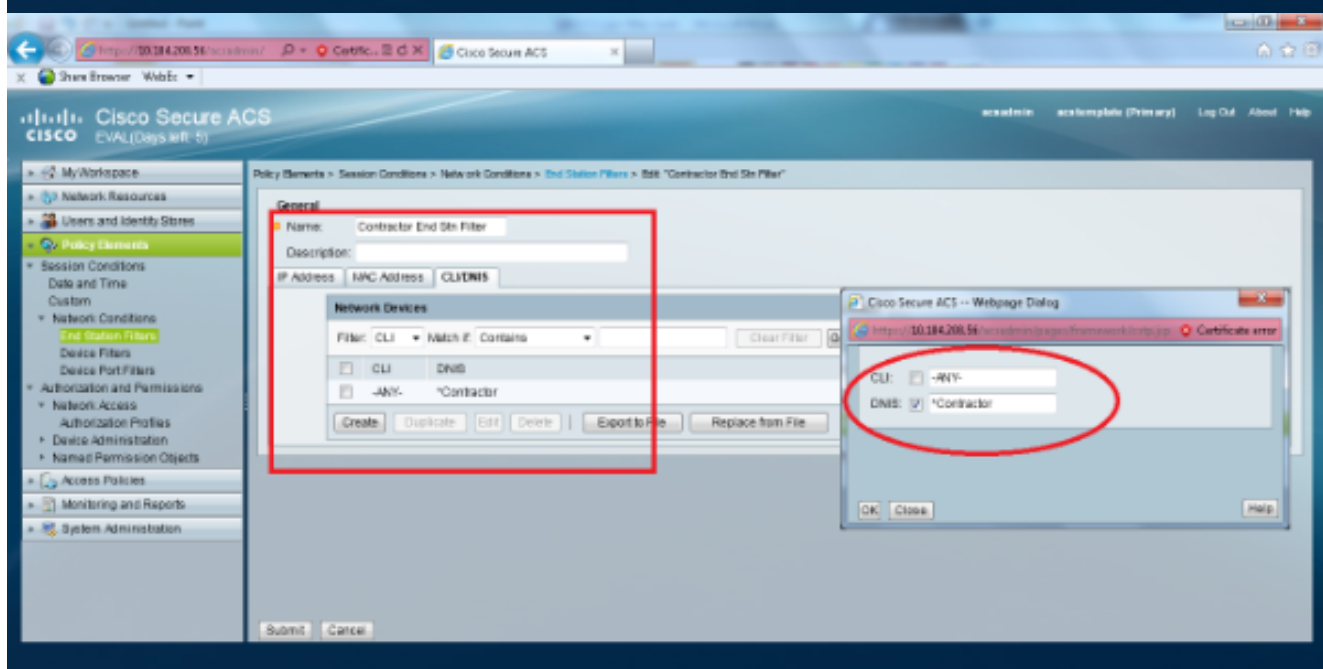
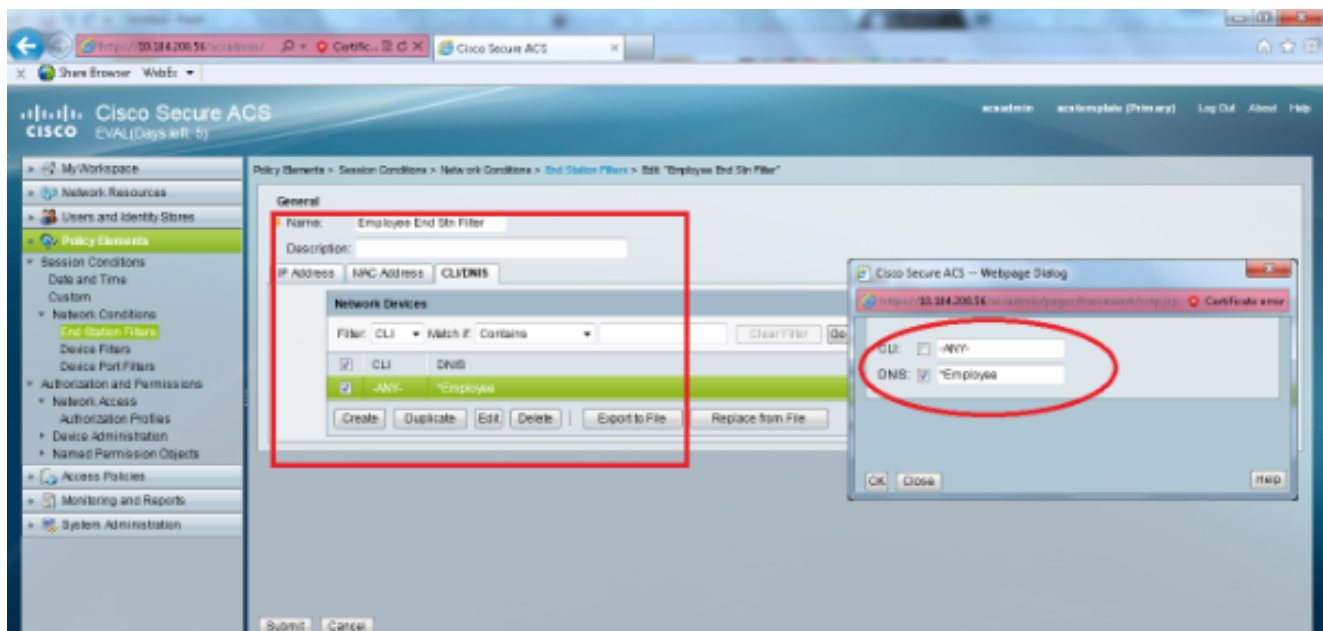
5. Selecione **Elementos de política > Condições de rede > Filtros de estação final**. Clique em **Criar**.



Insira um nome significativo e, na guia **IP address**, insira o endereço IP da WLC. Neste exemplo, os nomes são Funcionário e Contratante.

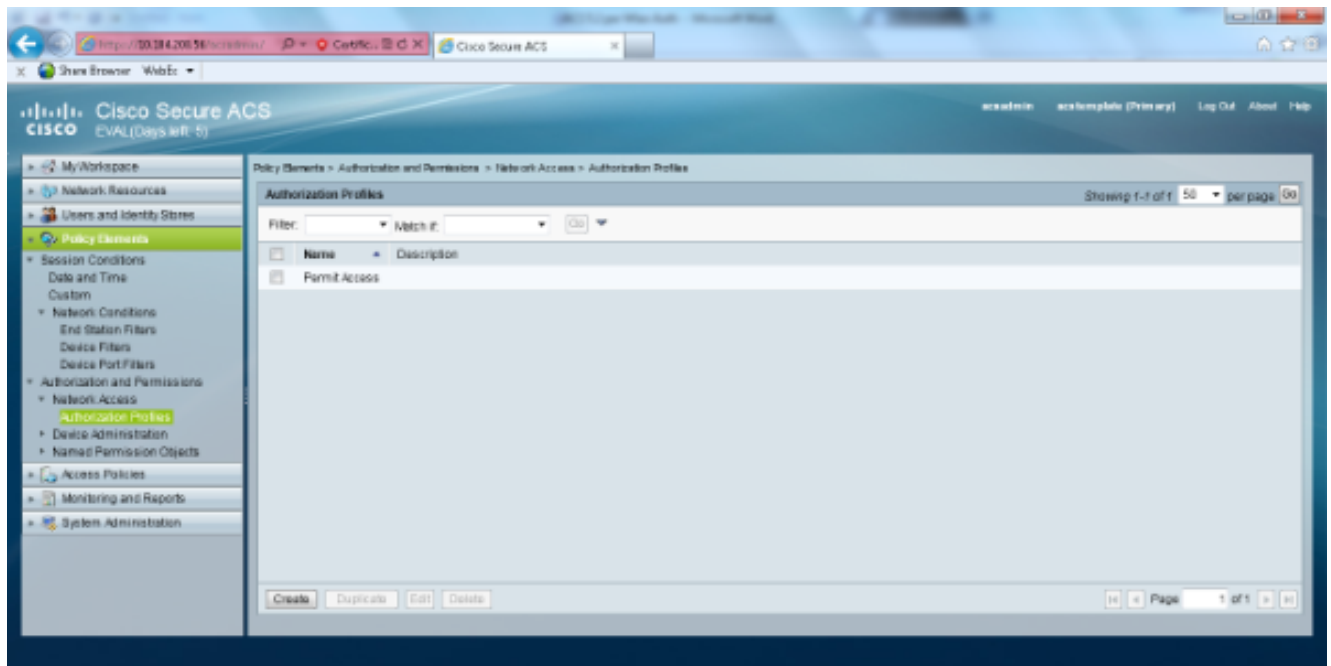


Na guia CLI/DNIS, deixe CLI como **-ANY-** e insira DNIS como **\*<SSID>**. Neste exemplo, o campo DNIS é inserido como **\*Funcionário**, pois esse filtro de estação final é usado para restringir o acesso somente à WLAN do Funcionário. O atributo DNIS define o SSID que o usuário pode acessar. A WLC envia o SSID no atributo DNIS para o servidor RADIUS. Repita as mesmas etapas para o filtro da estação final do Contratante.

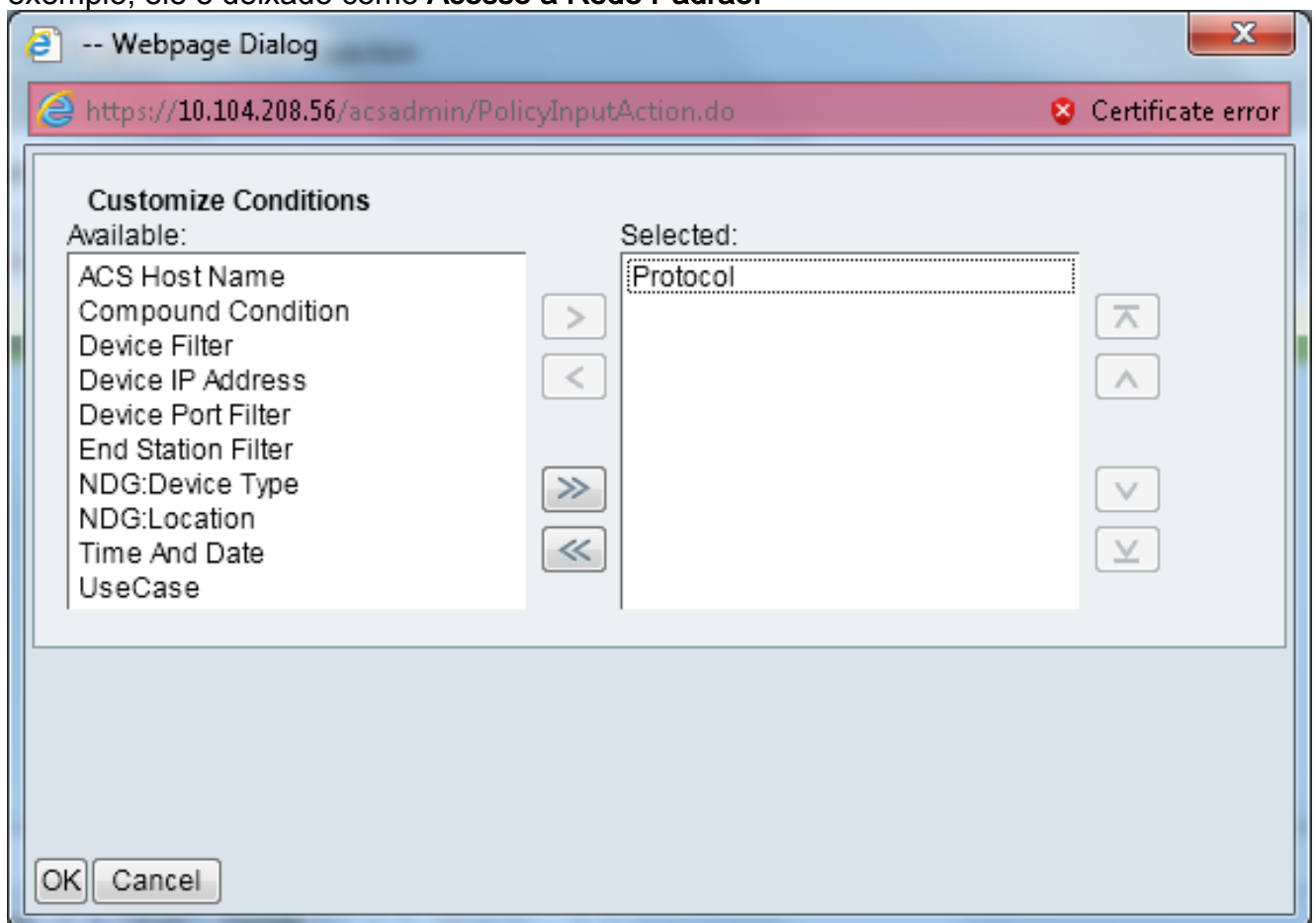


6. Selecione **Elementos de política > Autorização e permissões > Acesso à rede > Perfis de autorização**. Deve haver um perfil padrão para permitir acesso.

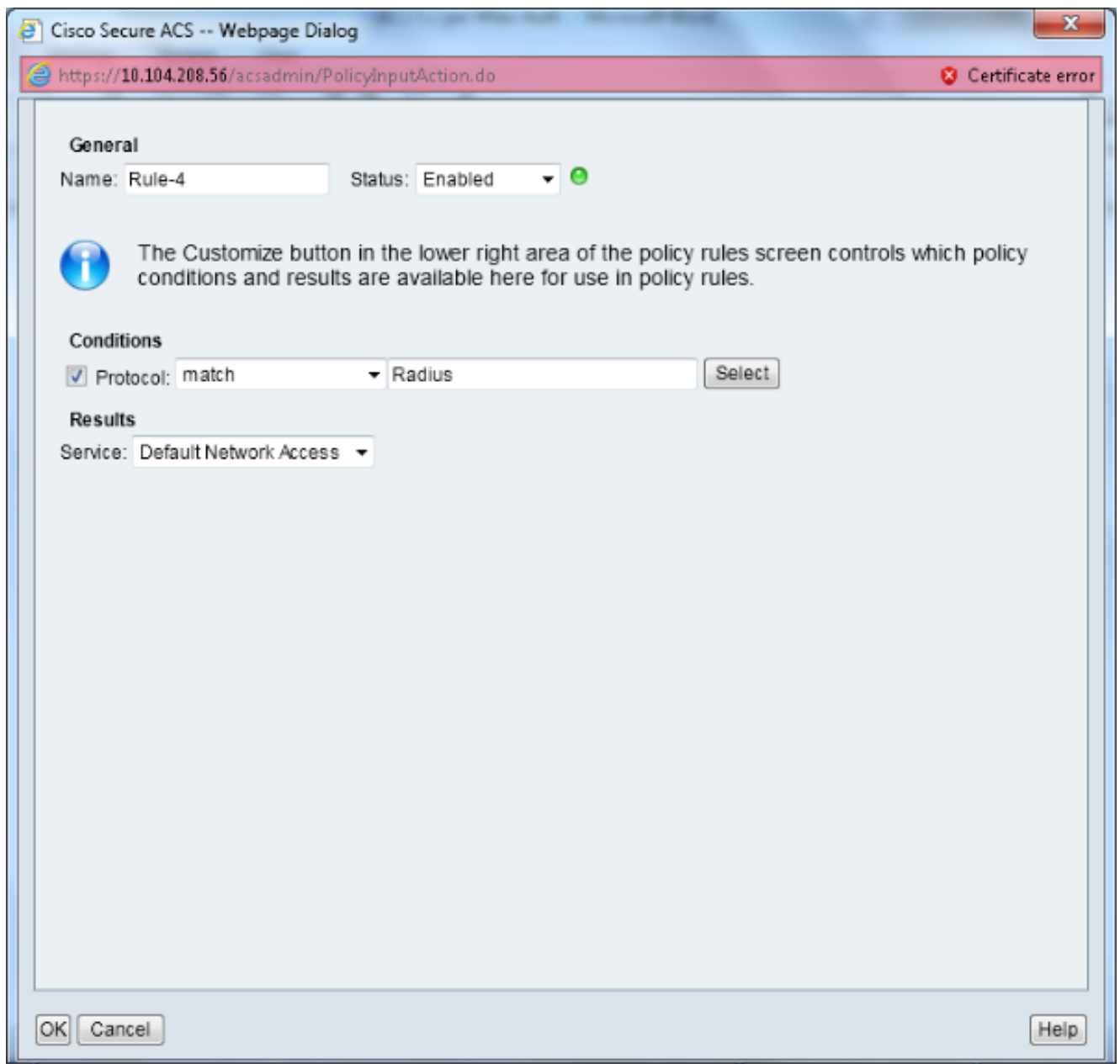




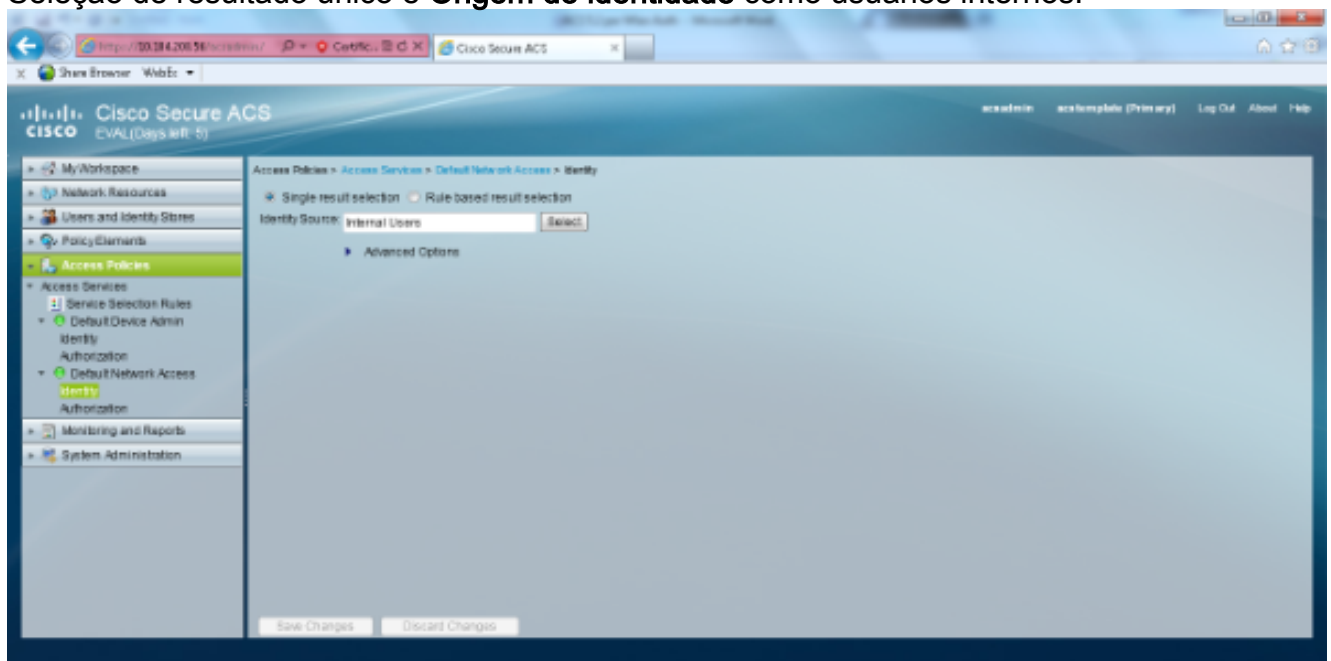
7. Selecione **Access Policies > Access Services > Service Selection Rules**. Clique em **Personalizar**. Adicione qualquer condição adequada. Este exemplo usa o protocolo como **RADIUS** como a condição correspondente. Clique em **Criar**. Nomeie a regra. Selecione **Protocolo** e selecione **Raio**. Em **Results**, escolha o Access Service apropriado. Neste exemplo, ele é deixado como **Acesso à Rede Padrão**.



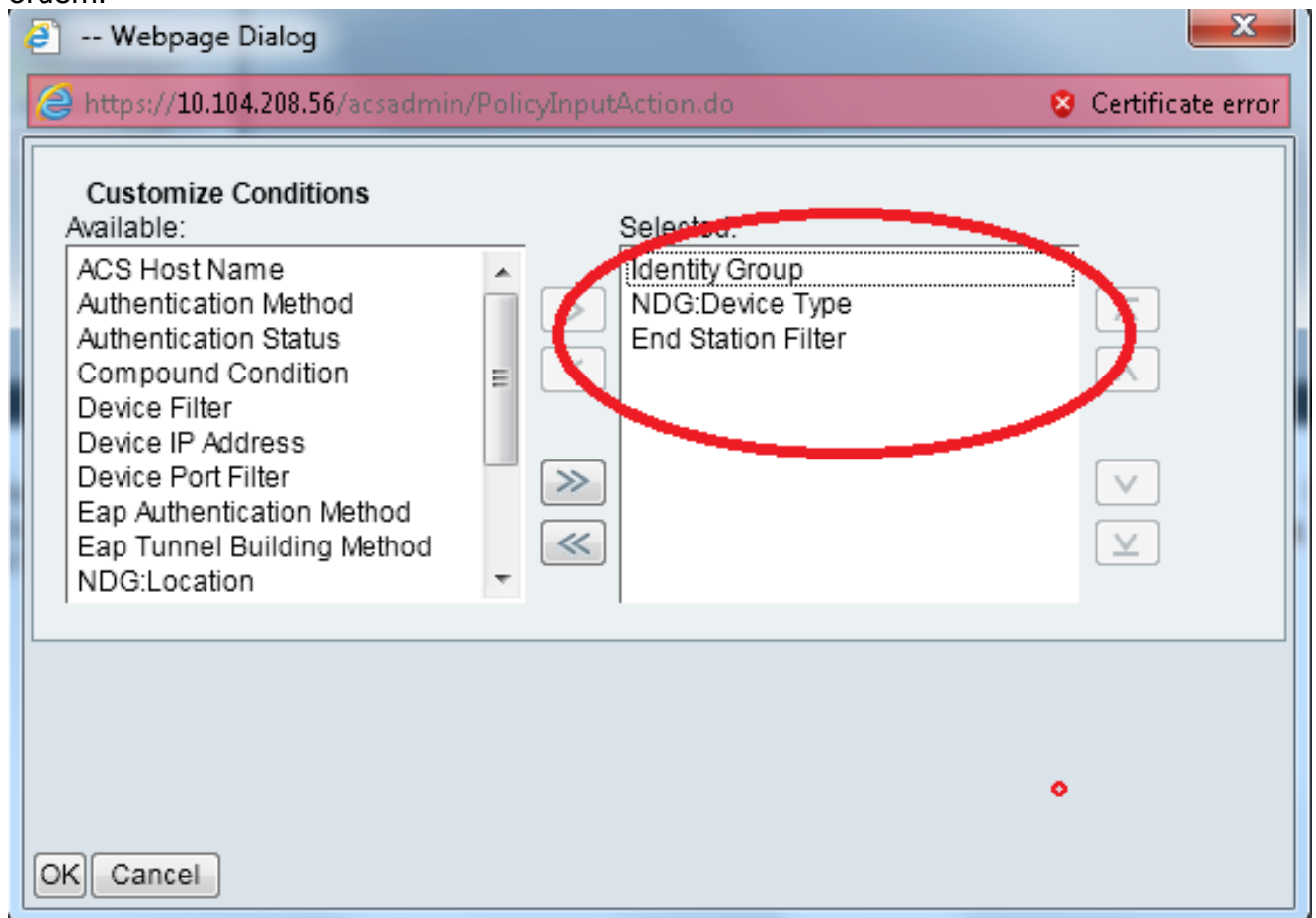




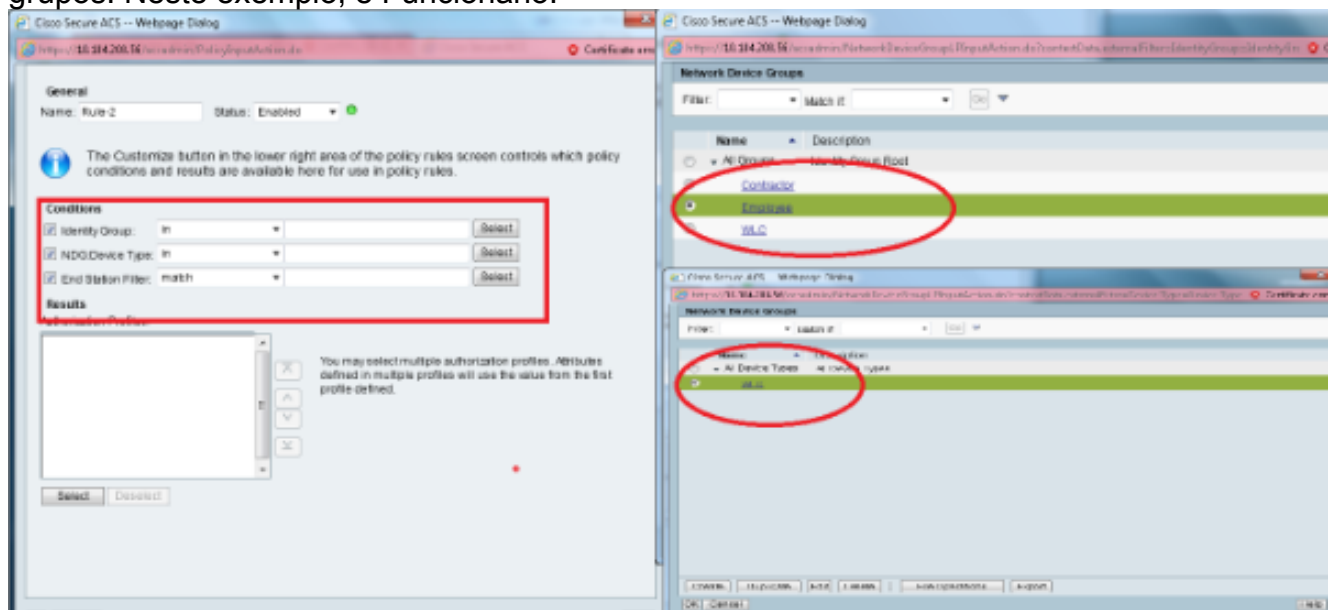
8. Selecione **Access Policies > Access Services > Default Network Access > Identity**. Escolha Seleção de resultado único e **Origem de identidade** como usuários internos.



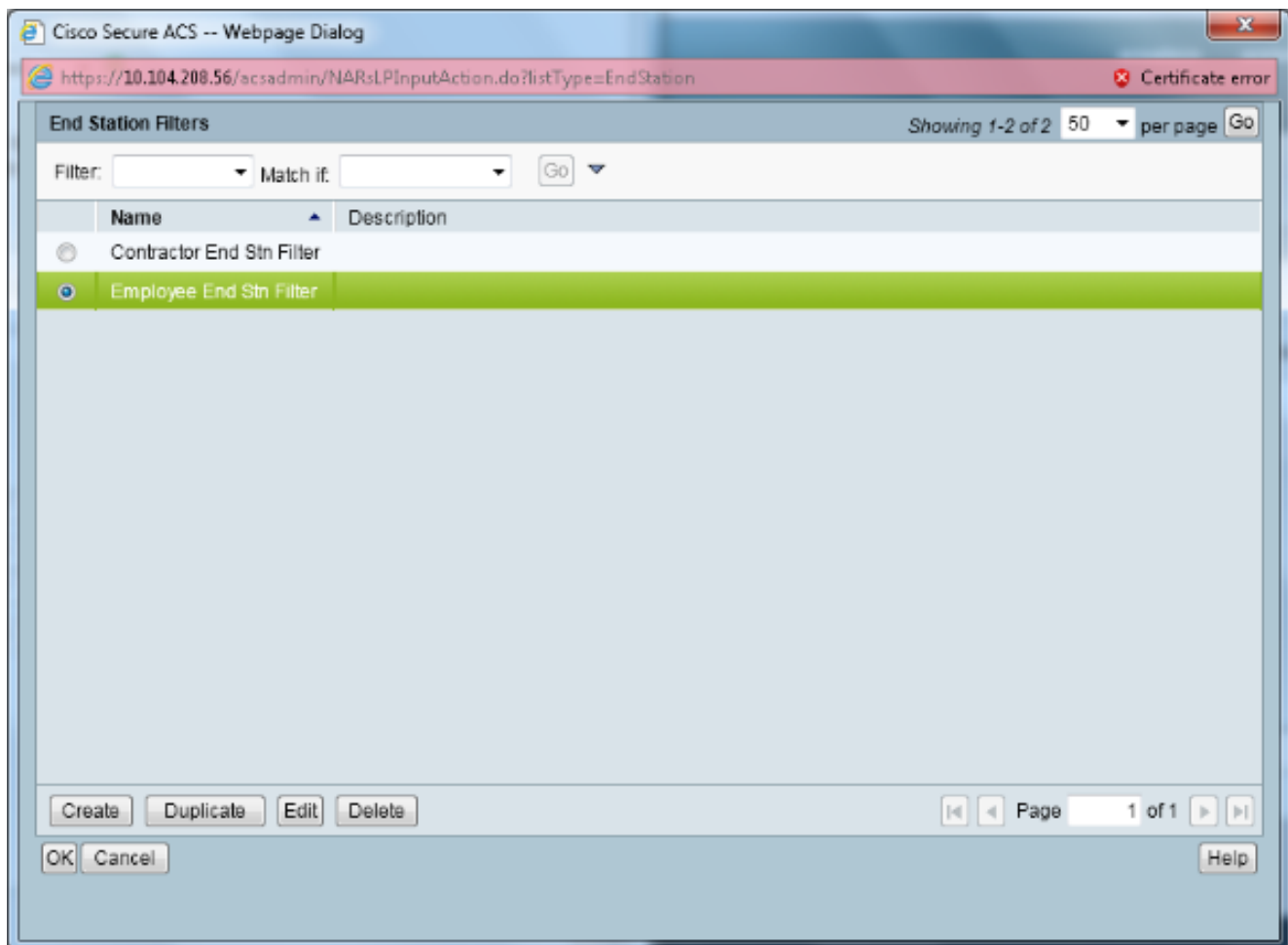
Selecione **Access Policies > Access Services > Default Network Access > Authorization**. Clique em **Personalizar** e adicione as condições Personalizadas. Este exemplo usa Grupo de identidade, NDG:Tipo de dispositivo e Filtro de estação final nessa ordem.



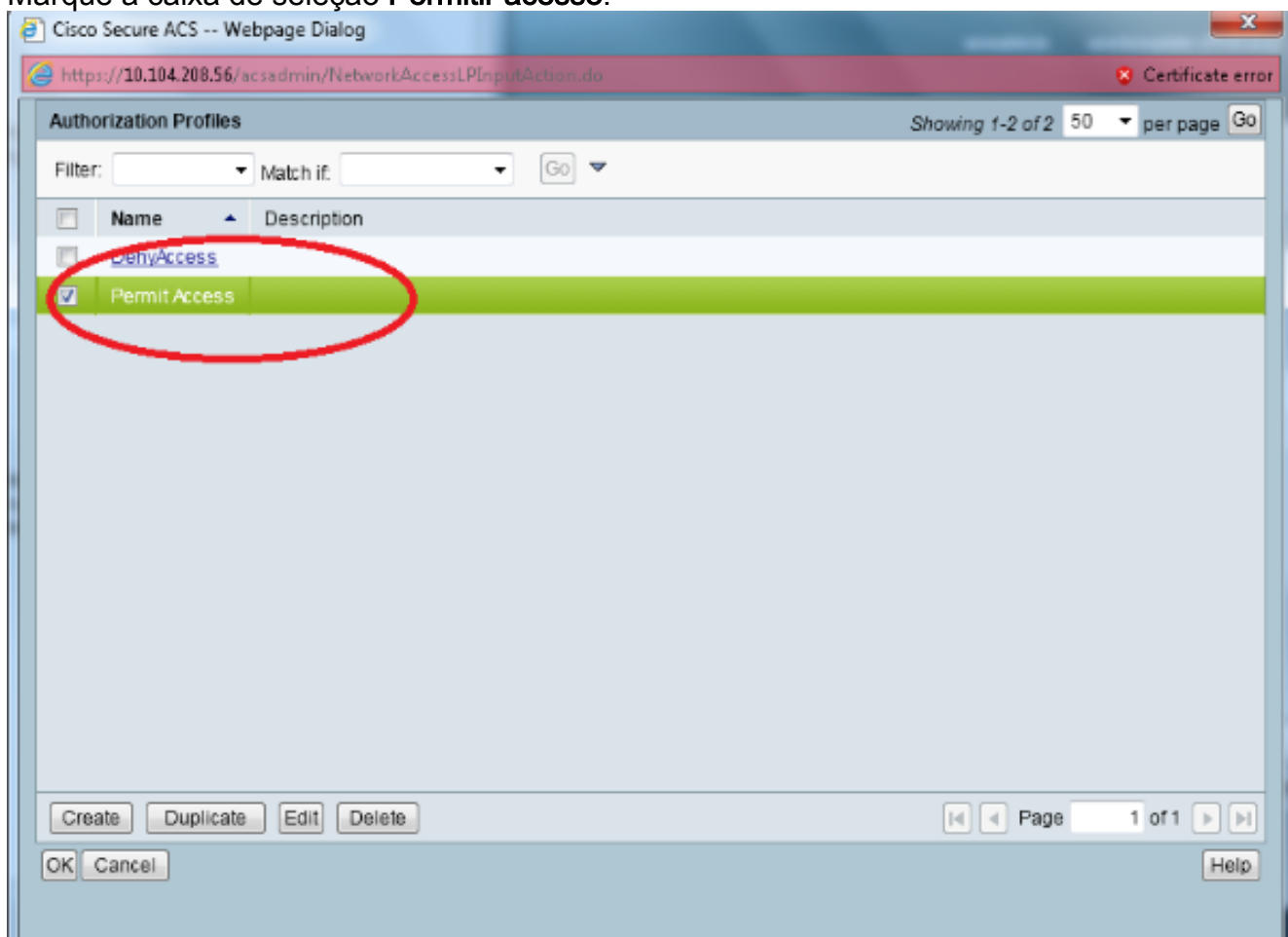
Clique em **Criar**. Nomeie a regra e escolha o Grupo de identidade apropriado em Todos os grupos. Neste exemplo, é Funcionário.



Clique no botão de opção **Employee End Stn Filter** ou insira o nome digitado na Etapa 1b na seção "Configure the WLC".

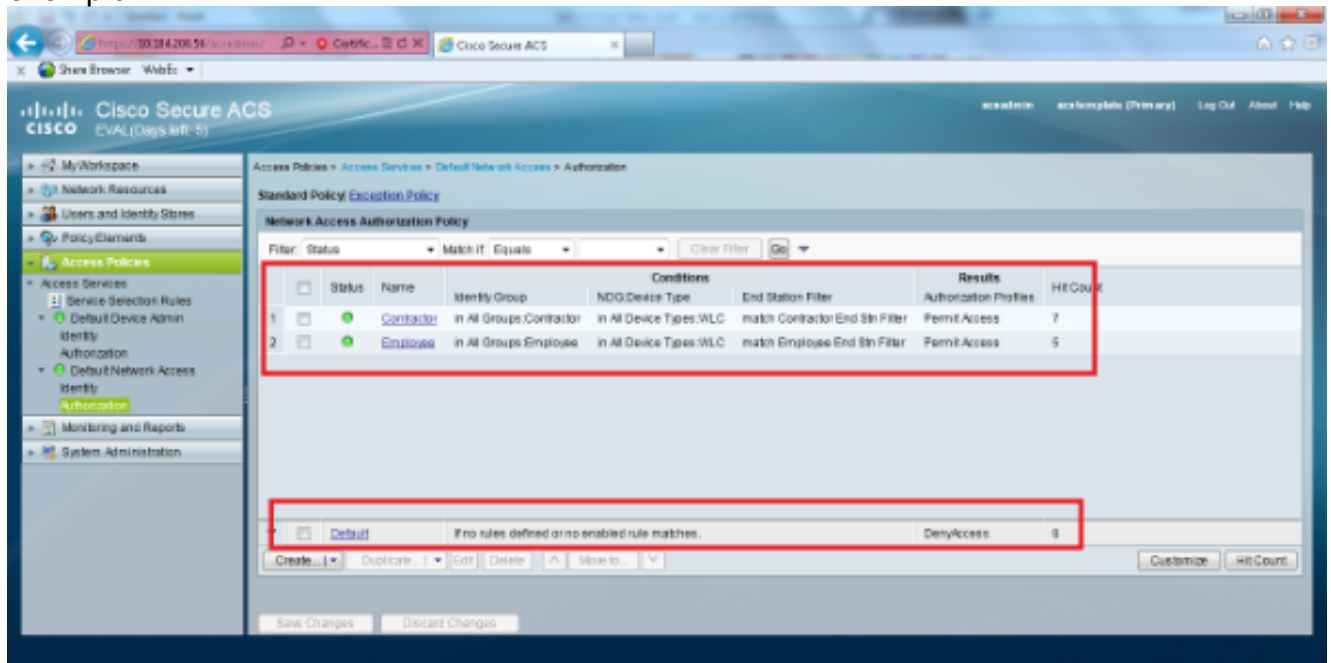


Marque a caixa de seleção **Permitir acesso**.



Repita as mesmas etapas acima para Regras do Contratante também. Verifique se a ação

padrão é **negar acesso**. Depois de concluir a etapa e, suas regras devem se parecer com este exemplo:



Isso conclui a configuração. Depois desta seção, o cliente precisa ser configurado de acordo com o SSID e os parâmetros de segurança para se conectar.

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.