

Configure o TACACS+ no Cisco ONS15454/NCS2000 com servidor ACS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve instruções passo a passo sobre como configurar o TACACS+ (Terminal Access Controller Access Control System, sistema de controle de acesso do controlador de acesso de terminal) em dispositivos ONS15454/NCS2000 e o ACS (Cisco Access Control System, sistema de controle de acesso Cisco). Todos os tópicos incluem exemplos. A lista de atributos fornecida neste documento não é exaustiva ou autoritativa e pode ser alterada a qualquer momento sem uma atualização deste documento.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Transport Controller (CTC) GU
- Servidor ACS

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

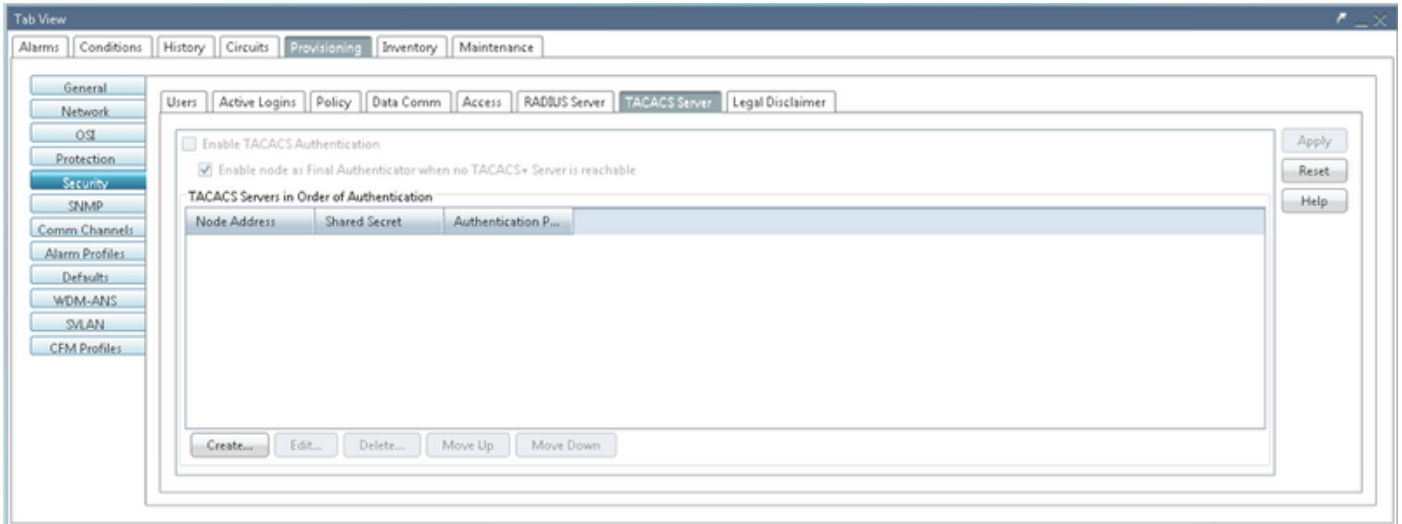
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration.

Note: Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Configurações necessárias no ONS15454/NCS2000:

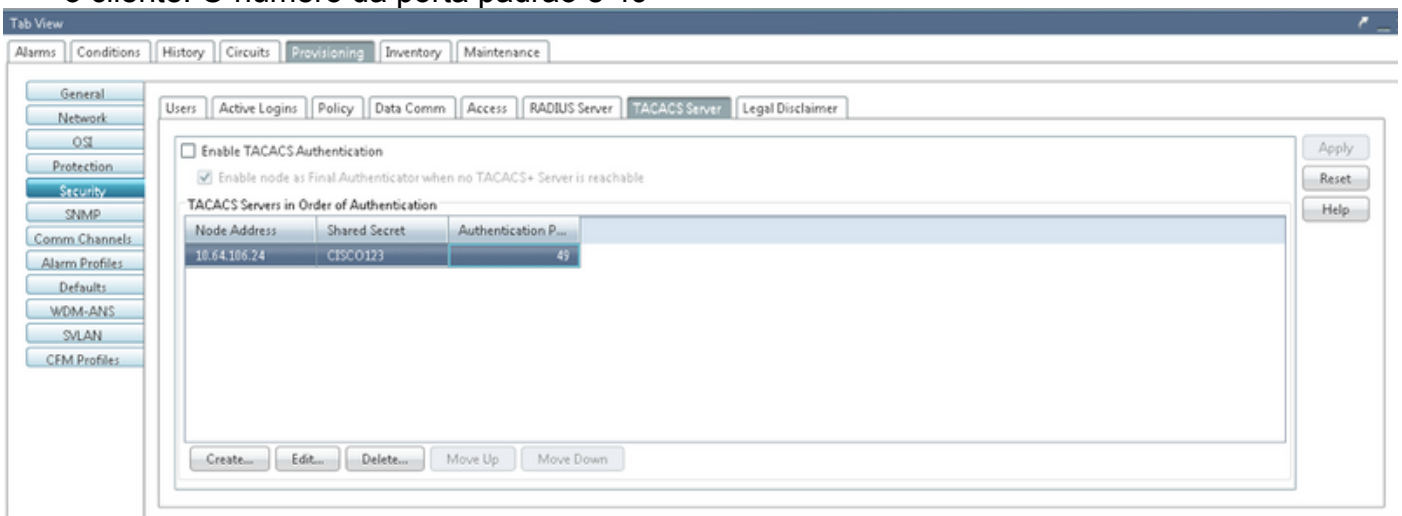
1. Você pode configurar a configuração do servidor TACACS nesta guia. Navegue até **Provisioning > Security > TACACS Server** conforme mostrado na imagem.



2. Para adicionar os detalhes do servidor TACACS+, clique no botão **Criar**. Ele abrirá a janela de configuração TACACS+ como mostrado nesta imagem.



- Insira o endereço IP do servidor
- Adicione o segredo compartilhado entre o nó e o servidor TACACS+
- Adicione o número da porta de autenticação. Nesta porta, o servidor TACACS+ está ouvindo o cliente. O número da porta padrão é 49



3. Para ativar a configuração do servidor TACACS+ no NODE, marque a caixa de seleção **Enable TACACS Authentication** e clique no botão **Apply** como mostrado na imagem.

Enable TACACS Authentication

4. Para ativar o Nó como o autenticador final, quando nenhum servidor estiver acessível, clique

na caixa de seleção como mostrado na imagem.

Enable node as Final Authenticator when no TACACS+ Server is reachable

5. Para modificar a configuração específica do servidor, selecione a linha de configuração do servidor correspondente, clique no botão **Editar** para modificar a configuração.

6. Para excluir a configuração específica do servidor, selecione a linha de configuração do servidor correspondente, clique no botão **Excluir** para excluir a configuração.

Configurações necessárias no servidor ACS:

1. Crie o dispositivo de rede e o cliente AAA e clique no botão **criar** no **painel Recursos de rede**, como mostrado na imagem.



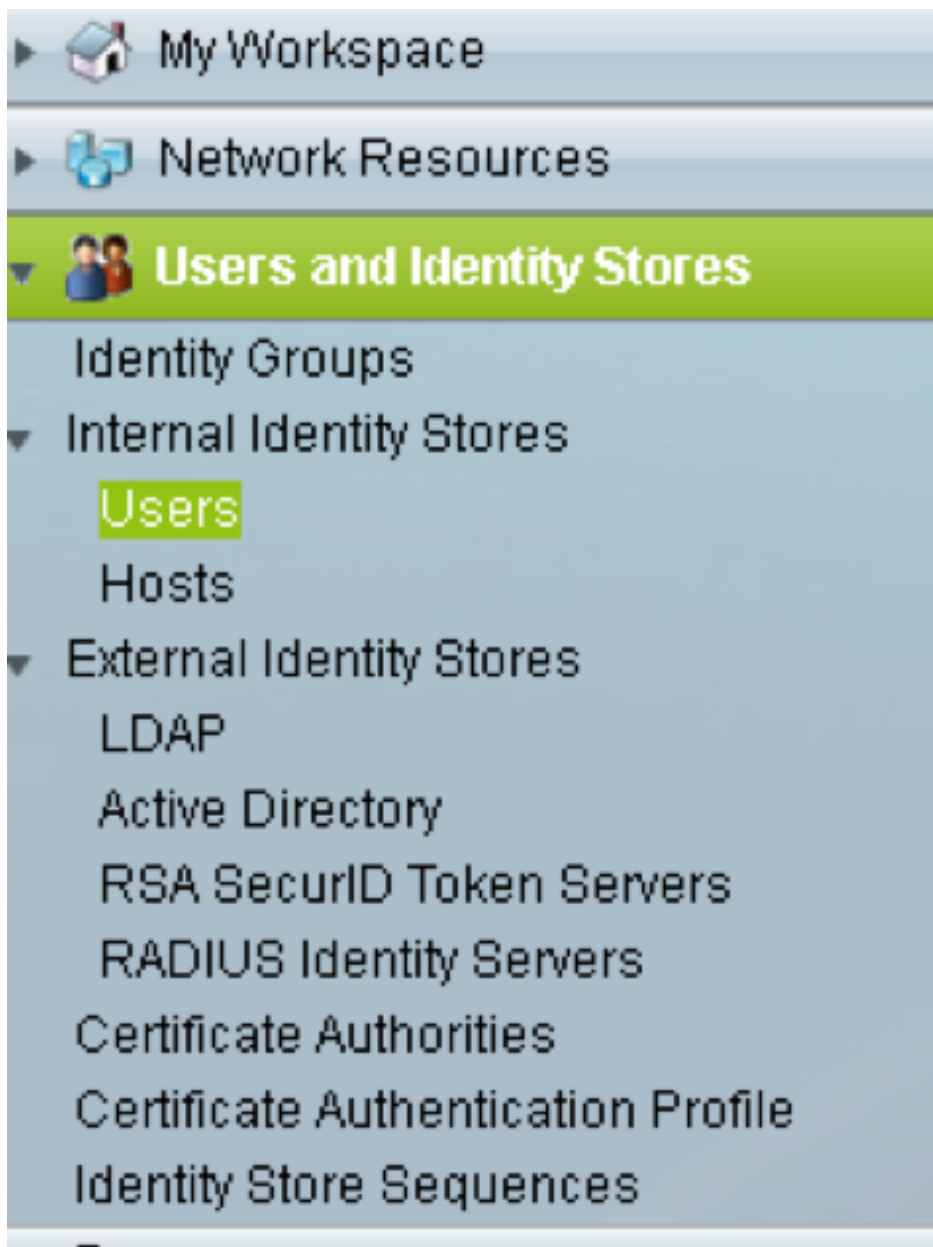
2. Forneça o mesmo **segredo compartilhado** fornecido na configuração do nó ONS. Caso contrário, a autenticação falhará.

Network Device Groups
Location:
Device Type:

IP Address
 Single IP Address IP Subnets IP Range(s)

Authentication Options
▼ TACACS+
Shared Secret:
 Single Connect Device
 Legacy TACACS+ Single Connect Support
 TACACS+ Draft Compliant Single Connect Support
▼ RADIUS
Shared Secret:
CoA port:
 Enable KeyWrap
Key Encryption Key:
Message Authenticator Code Key:
Key Input Format: ASCII HEXADECIMAL

3. Crie um nome de usuário e uma senha para que o usuário necessário seja autenticado no painel **Usuários e armazenamento de identidade**, como mostrado na imagem.



Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: raamu Status: Enabled

Description:

Identity Group: All Groups

Email Address:

Account Disable

Disable Account if Date Exceeds: 2015-Nov-21 (yyyy-Mmm-dd)

Disable account after 3 successive failed attempts

Password Hash

Enable Password Hash

Applicable only for Internal Users to store password as hash. Authentication types CHAP/MSCHAP will not work if this option is enabled. While disabling the hash, ensure that password is reconfigured using change password option.

Password Lifetime

Password Never Expired/Disabled: Overwrites user account blocking in case password expired/disabled

Password Information

Password must:

- Contain 4 - 32 characters

Password Type: Internal Users

Password:

Confirm Password:

Change password on next login

Enable Password Information

Password must:

- Contain 4 - 128 characters

Enable Password:

Confirm Password:

User Information

These are additional identity attributes defined for your users.

4. Criar perfis de shell no painel **Elementos de Política**:

a. Selecione o nível de privilégio (0 a 3):

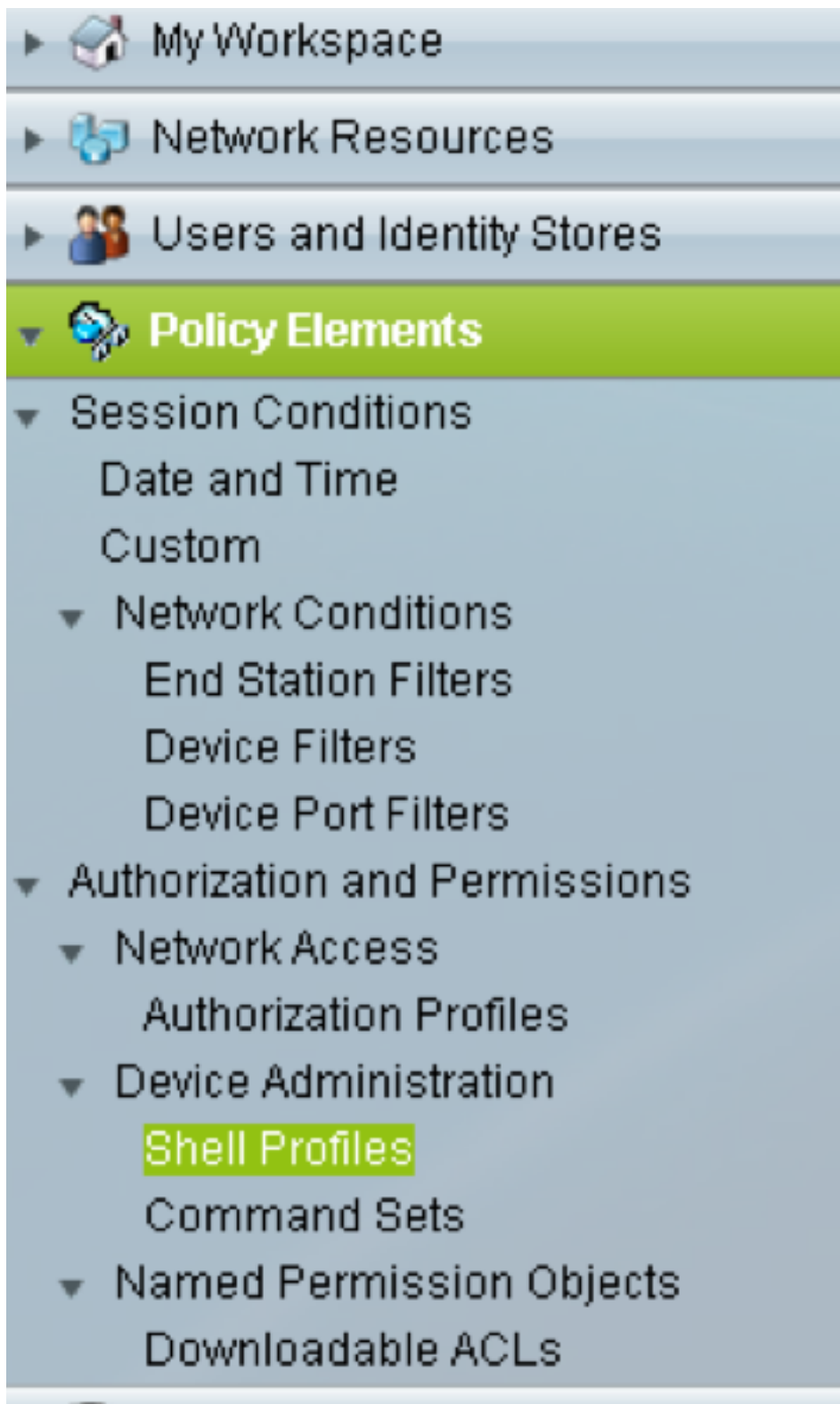
0 para Recuperar usuário.

1 para usuário de manutenção.

2 para usuário do Provisionamento.

3 para Superusuário.

b. Crie um atributo personalizado no painel **Atributos do cliente** para o atributo **Tempo ocioso**.



General **Common Tasks** Custom Attributes

Privilege Level

Default Privilege: Static Value 2

Maximum Privilege: Not in Use

Shell Attributes

Access Control List: Not in Use

Auto Command: Not in Use

No Callback Verify: Not in Use

No Escape: Not in Use


No Hang Up: Not in Use

Timeout: Not in Use

Idle Time: Not in Use

Callback Line: Not in Use

Callback Rotary: Not in Use

 = Required fields

Tempo ocioso "0" indica que a conexão nunca expira e será eterna.se o usuário especificar qualquer outro tempo, a conexão estará disponível por esses segundos.

General Common Tasks **Custom Attributes**

Common Tasks Attributes

Attribute	Requirement	Value
Assigned Privilege Level	Mandatory	2

Manually Entered

Attribute	Requirement	Value
idletime	Mandatory	0

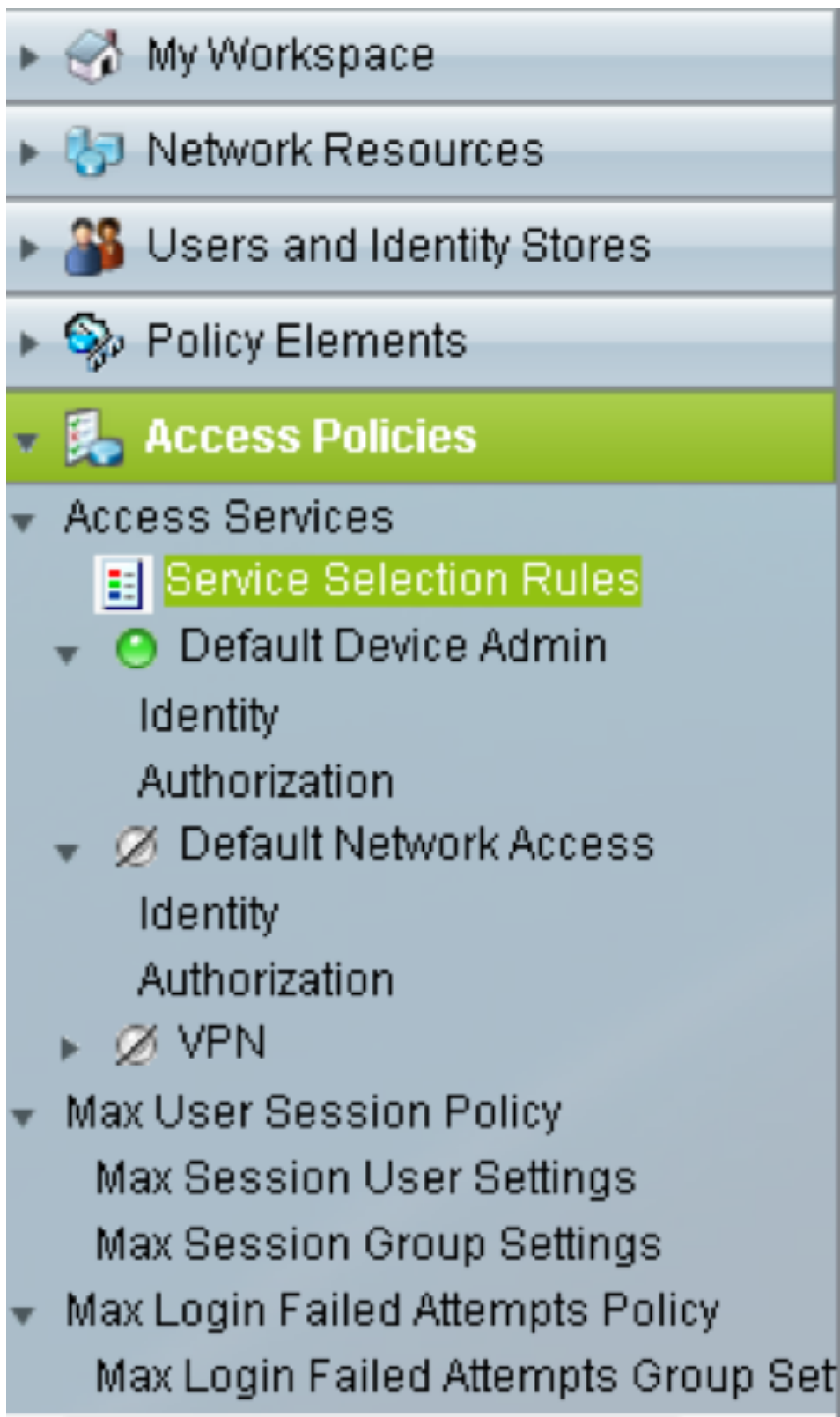
Attribute:

Requirement: Mandatory ▾

Attribute Value: Static ▾

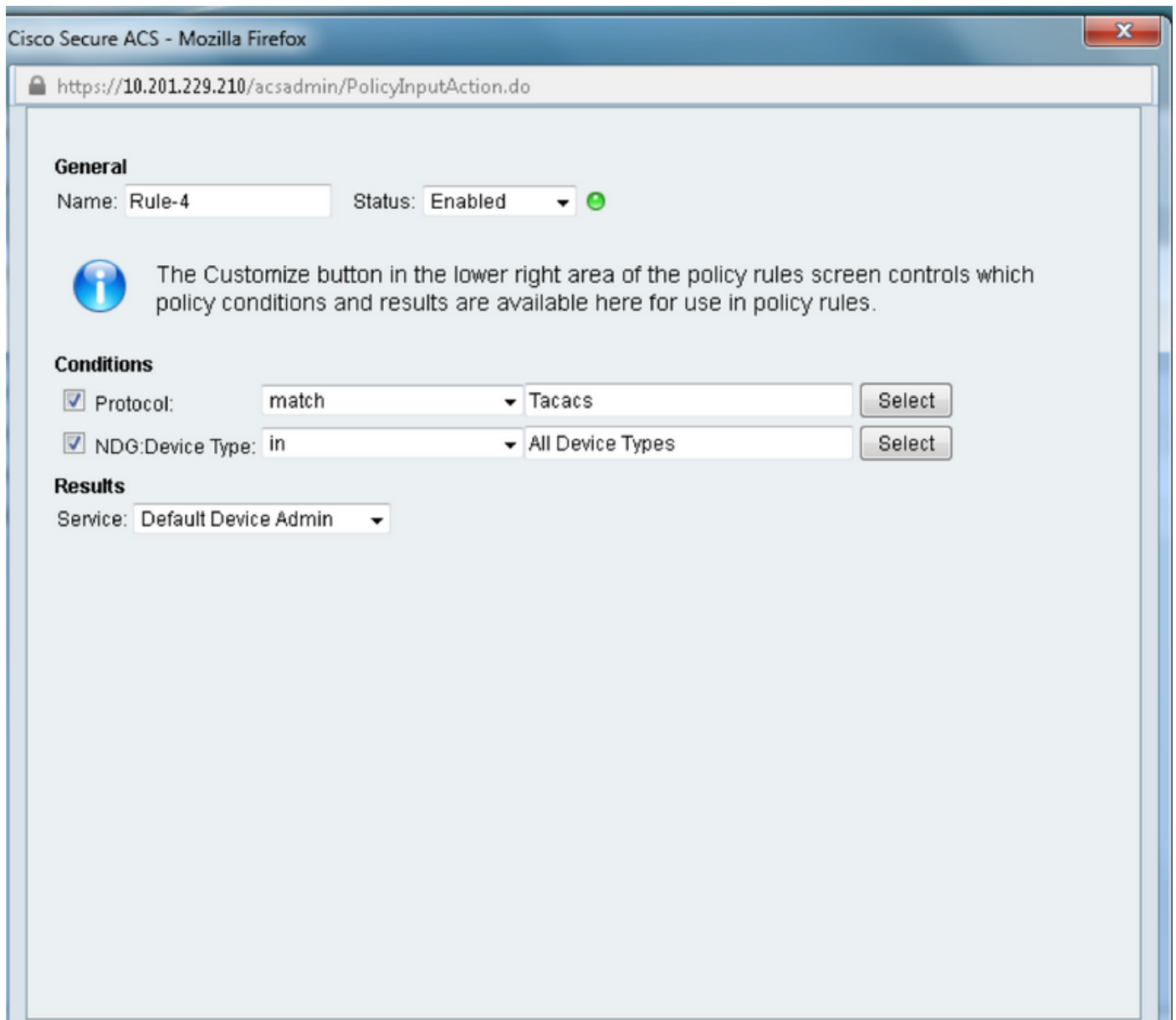
Submit Cancel

5. Crie políticas de acesso no painel **Políticas de acesso**:












a. Clique em **Regras de seleção de serviço** e crie uma regra:

- Selecionar TACACS como protocolo
- O dispositivo como Todos os dispositivos ou um dispositivo específico similar ao criado anteriormente
- Tipo de serviço como **Default Device Admin**.

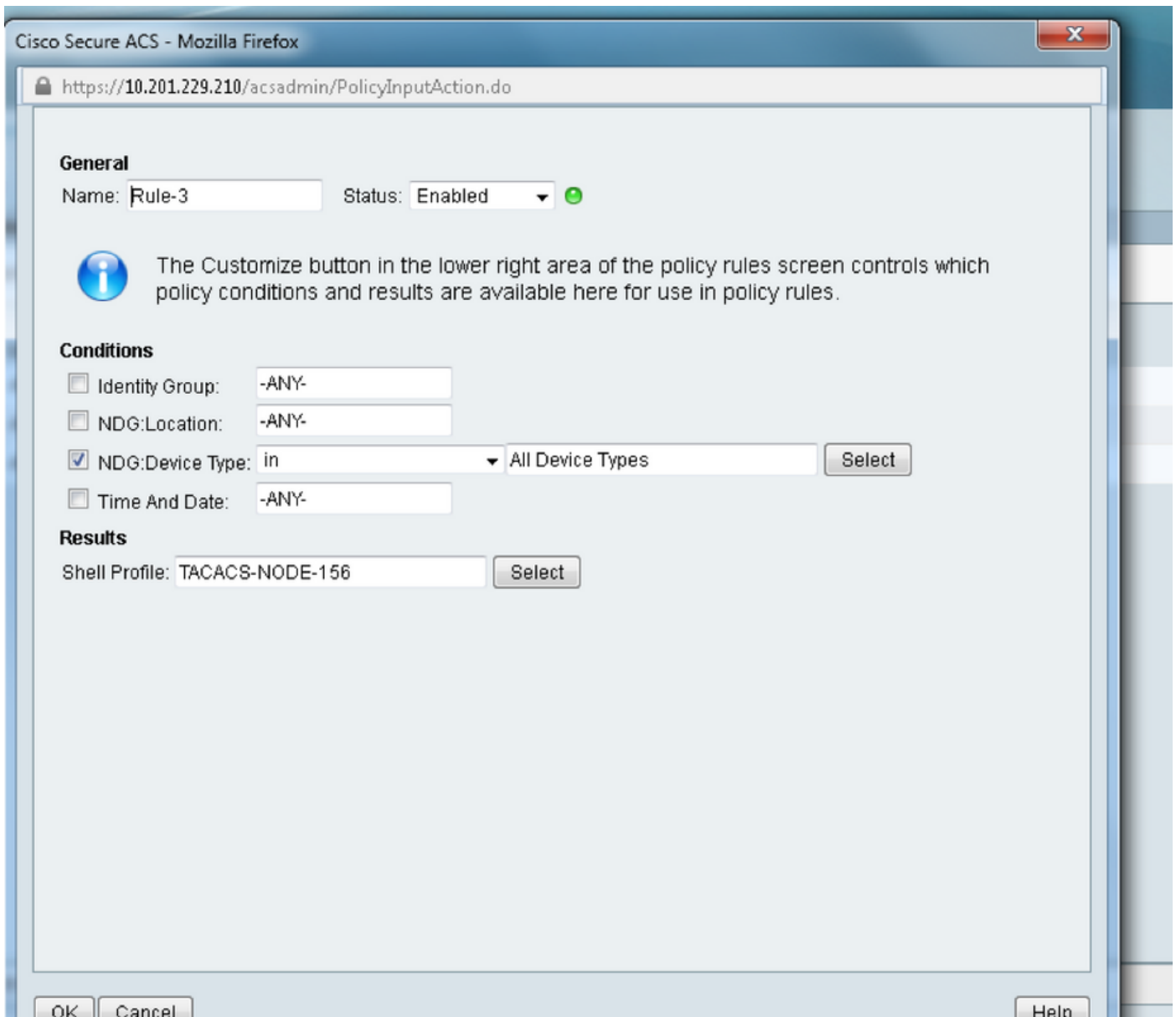


b. Selecione **Authorization** e crie uma regra para autorização em no botão de opção **Default Device Admin**:

- Selecionar perfil de shell **já criado**
- Selecione um dispositivo específico ou todos os dispositivos no tipo de dispositivo

- ▶  My Workspace
- ▶  Network Resources
- ▶  Users and Identity Stores
- ▶  Policy Elements
- ▼  **Access Policies**
- ▼ Access Services
 -  Service Selection Rules
 - ▼  Default Device Admin Identity
 - Authorization**
 - ▼  Default Network Access Identity
 - Authorization
 - ▶  VPN
- ▼ Max User Session Policy
 - Max Session User Settings
 - Max Session Group Settings
- ▼ Max Login Failed Attempts Policy
 - Max Login Failed Attempts Group Set

◀ [Progress Bar] ▶



Verificar

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

Troubleshoot

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