

Configuración de TACACS+ en Cisco ONS15454/NCS2000 con servidor ACS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe las instrucciones paso a paso sobre cómo configurar el Sistema de control de acceso del controlador de acceso de terminal (TACACS+) en dispositivos ONS15454/NCS2000 y Cisco Access Control System (ACS). Todos los temas incluyen ejemplos. La lista de atributos proporcionada en este documento no es exhaustiva ni fidedigna y podría cambiar en cualquier momento sin actualizar este documento.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- GU del controlador de transporte de Cisco (CTC)
- Servidor ACS

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

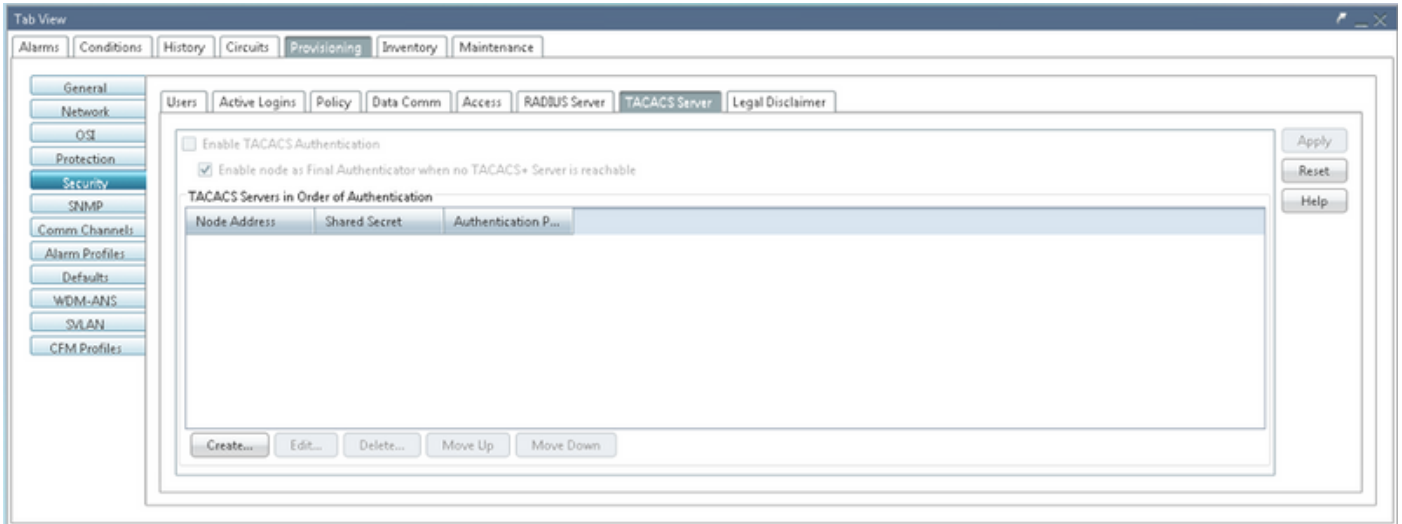
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration.

Nota: Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuraciones necesarias en ONS15454/NCS2000:

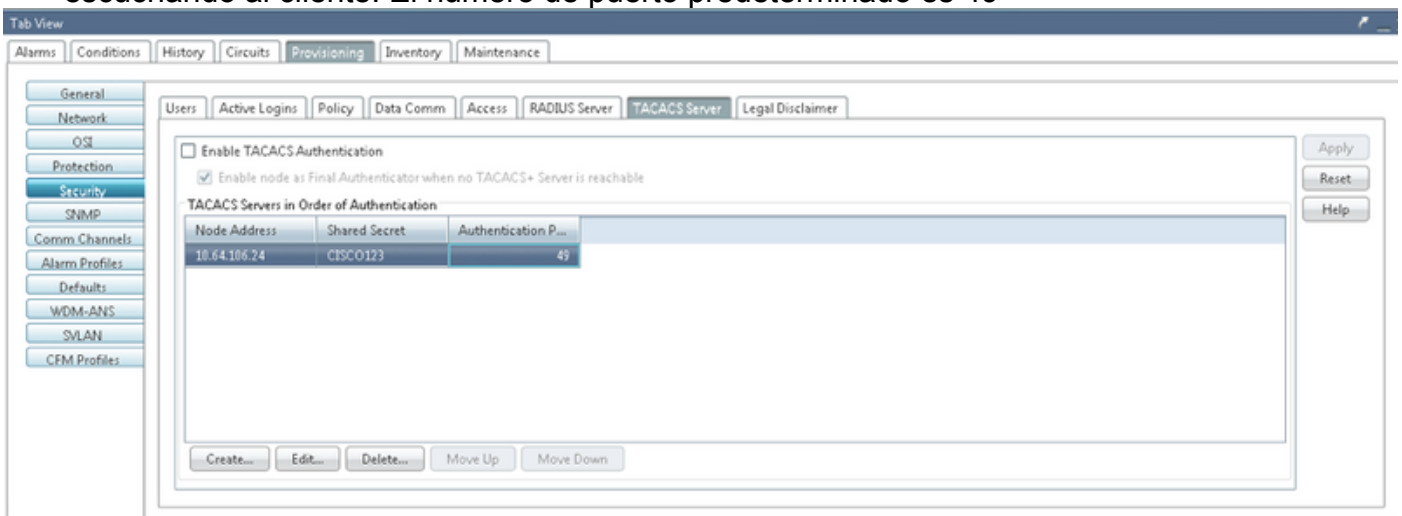
1. Puede configurar la configuración del servidor TACACS desde esta pestaña. Vaya a **Provisioning > Security > TACACS Server** como se muestra en la imagen.



2. Para agregar los detalles del servidor TACACS+, haga clic en el botón **Create**. Se abrirá la ventana de configuración TACACS+ como se muestra en esta imagen.



- Introduzca la dirección IP del servidor
- Agregar el secreto compartido entre el nodo y el servidor TACACS+
- Agregue el número de puerto de autenticación. En este puerto, el servidor TACACS+ está escuchando al cliente. El número de puerto predeterminado es 49



3. Para activar la configuración del servidor TACACS+ en NODE, marque la casilla **Enable TACACS Authentication** y haga clic en el botón **Apply** como se muestra en la imagen.

Enable TACACS Authentication

4. Para habilitar el Nodo como autenticador final, cuando no se puede alcanzar ningún servidor,

haga clic en la casilla de verificación como se muestra en la imagen.

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

5. Para modificar la configuración del servidor en particular, seleccione la fila de configuración del servidor correspondiente, haga clic en el botón **Edit** para modificar la configuración.

6. Para eliminar la configuración del servidor en particular, seleccione la fila de configuración del servidor correspondiente, haga clic en el botón **Delete** para eliminar la configuración.

Configuraciones requeridas en el servidor ACS:

1. Cree el dispositivo de red y el cliente AAA y haga clic en el botón **crear** en el panel **Recursos de red** como se muestra en la imagen.



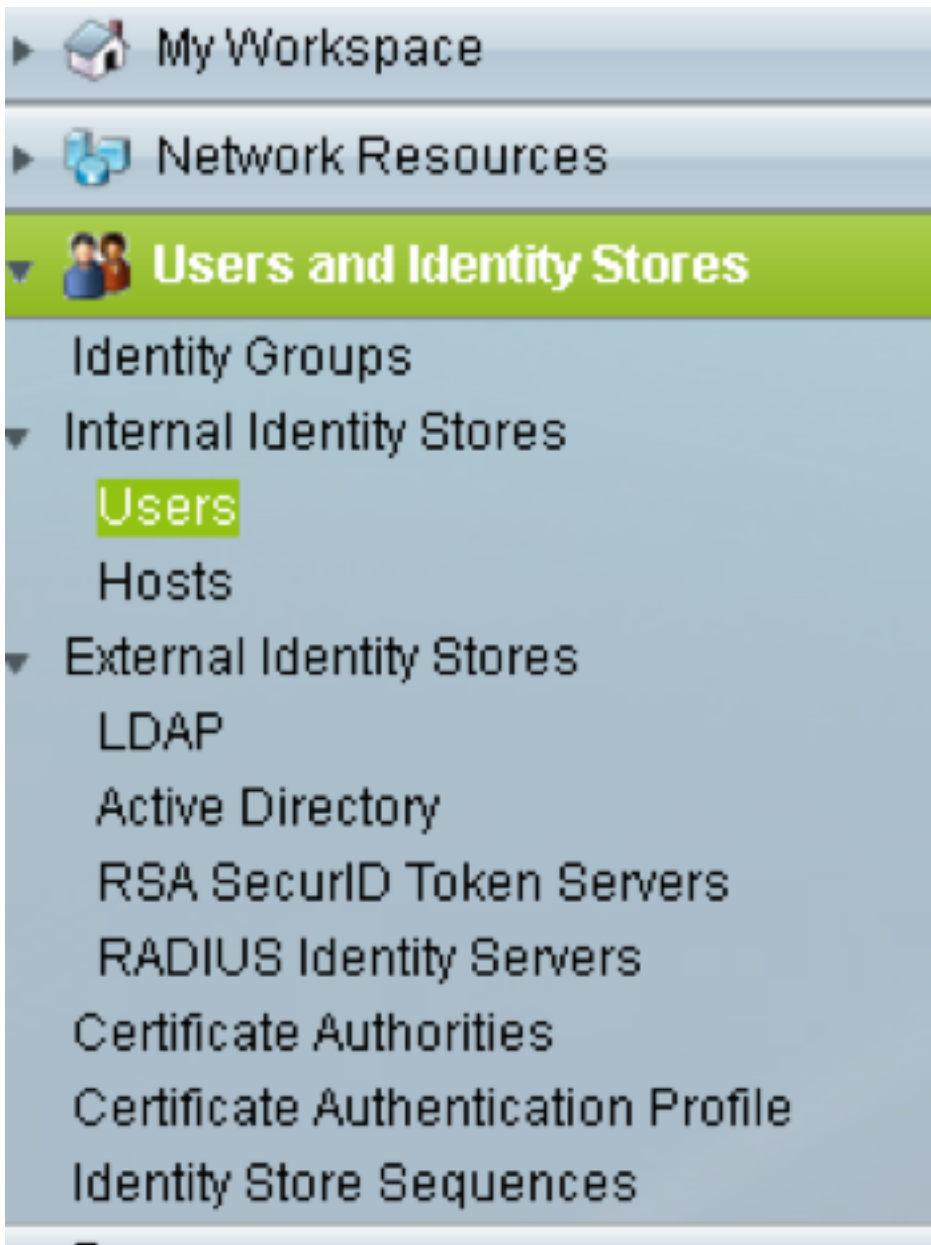
2. Dé el mismo **Secreto Compartido** que en la configuración del nodo ONS. De lo contrario, se producirá un error en la autenticación.

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. Cree un nombre de usuario y una contraseña para que el usuario requerido se autentique en el Panorama **Usuarios e Identidades** como se muestra en la imagen.



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. Crear perfiles de shell en el panel **Elementos de política**:

a. Seleccione el nivel de privilegio (0 a 3):





0 para recuperar el usuario.

1 para el usuario de mantenimiento.

2 para el usuario de aprovisionamiento.

3 para superusuario.

b. Cree un atributo personalizado en el panel **Atributos del cliente** para el atributo **Tiempo de inactividad**.

- ▶  My Workspace
- ▶  Network Resources
- ▶  Users and Identity Stores
- ▼  **Policy Elements**
- ▼ Session Conditions
 - Date and Time
 - Custom
 - ▼ Network Conditions
 - End Station Filters
 - Device Filters
 - Device Port Filters
- ▼ Authorization and Permissions
 - ▼ Network Access
 - Authorization Profiles
 - ▼ Device Administration
 - Shell Profiles**
 - Command Sets
 - ▼ Named Permission Objects
 - Downloadable ACLs

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

Idle time "0" indica que la conexión nunca se agota y será para siempre. El usuario si especifica otra hora, la conexión estará disponible durante tantos segundos.

General Common Tasks **Custom Attributes**

Common Tasks Attributes

Attribute	Requirement	Value
Assigned Privilege Level	Mandatory	2

Manually Entered

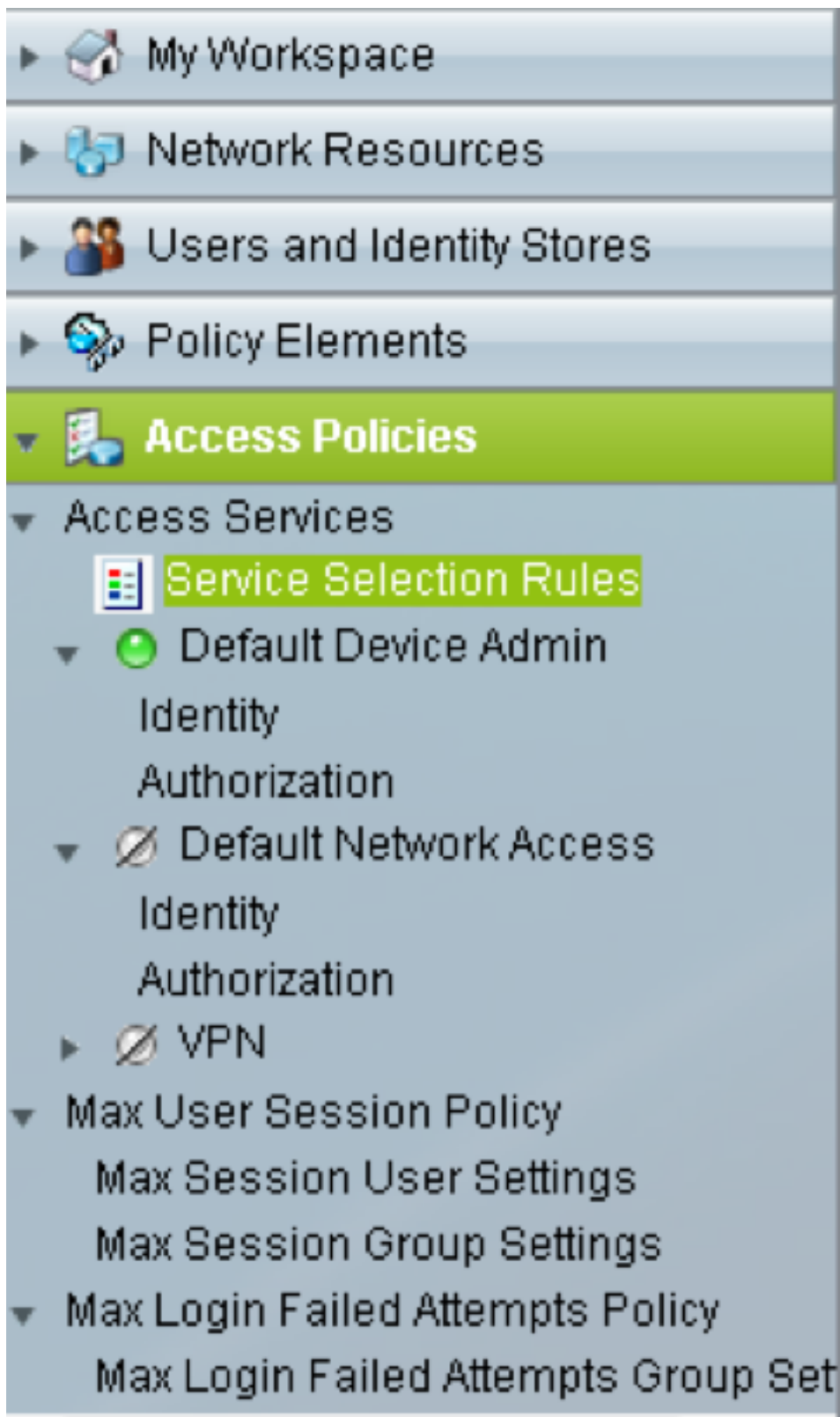
Attribute	Requirement	Value
idletime	Mandatory	0

Attribute:

Requirement: Mandatory ▾

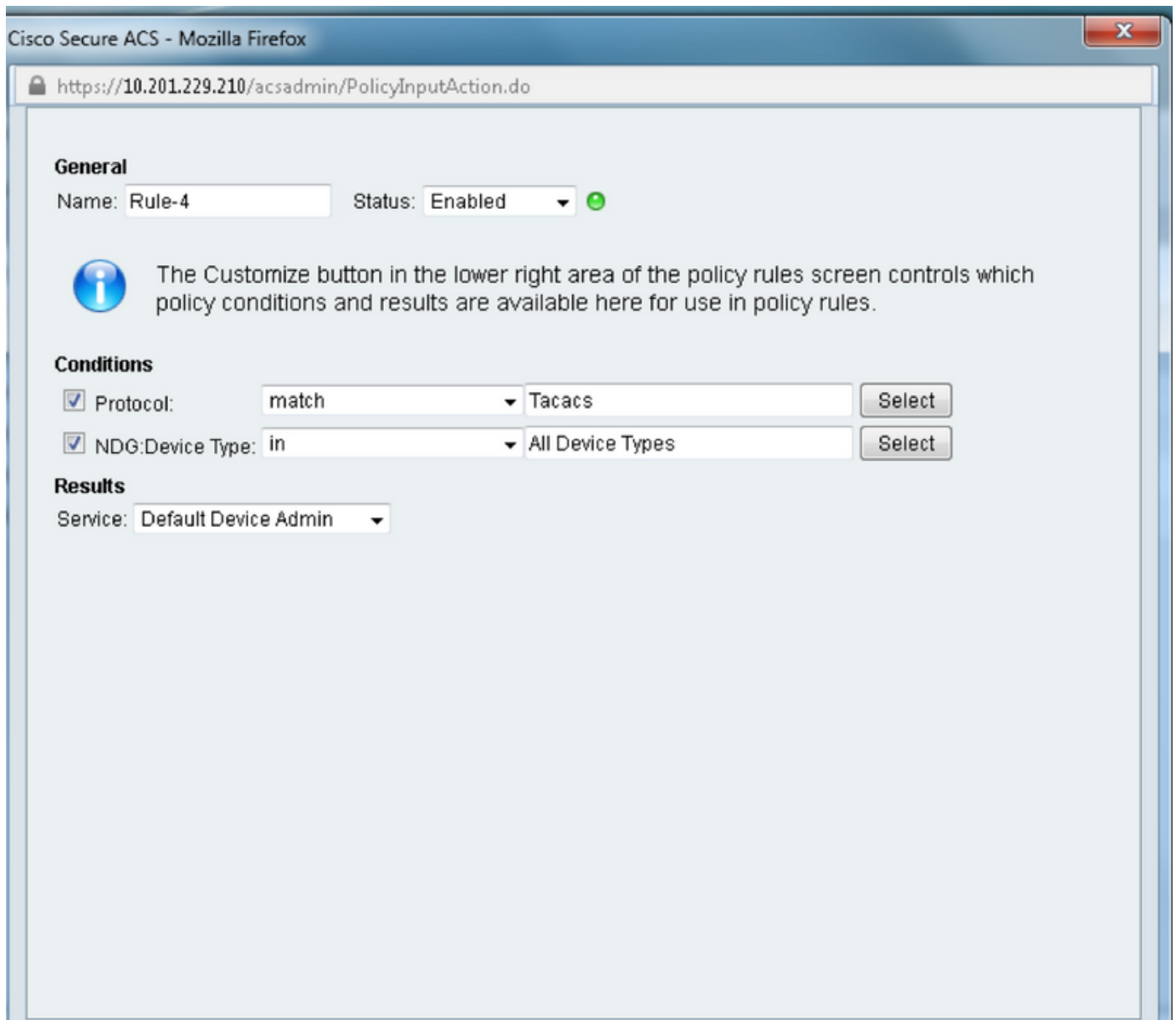
Attribute Value: Static ▾

5. Cree políticas de acceso en el panel **Políticas de acceso**:












a. Haga clic en **Service Selection Rules** y cree una regla:

- Seleccionar TACACS como protocolo
- El dispositivo es All device o específico similar al que se creó anteriormente
- Tipo de servicio como **Administrador de dispositivos predeterminado**.

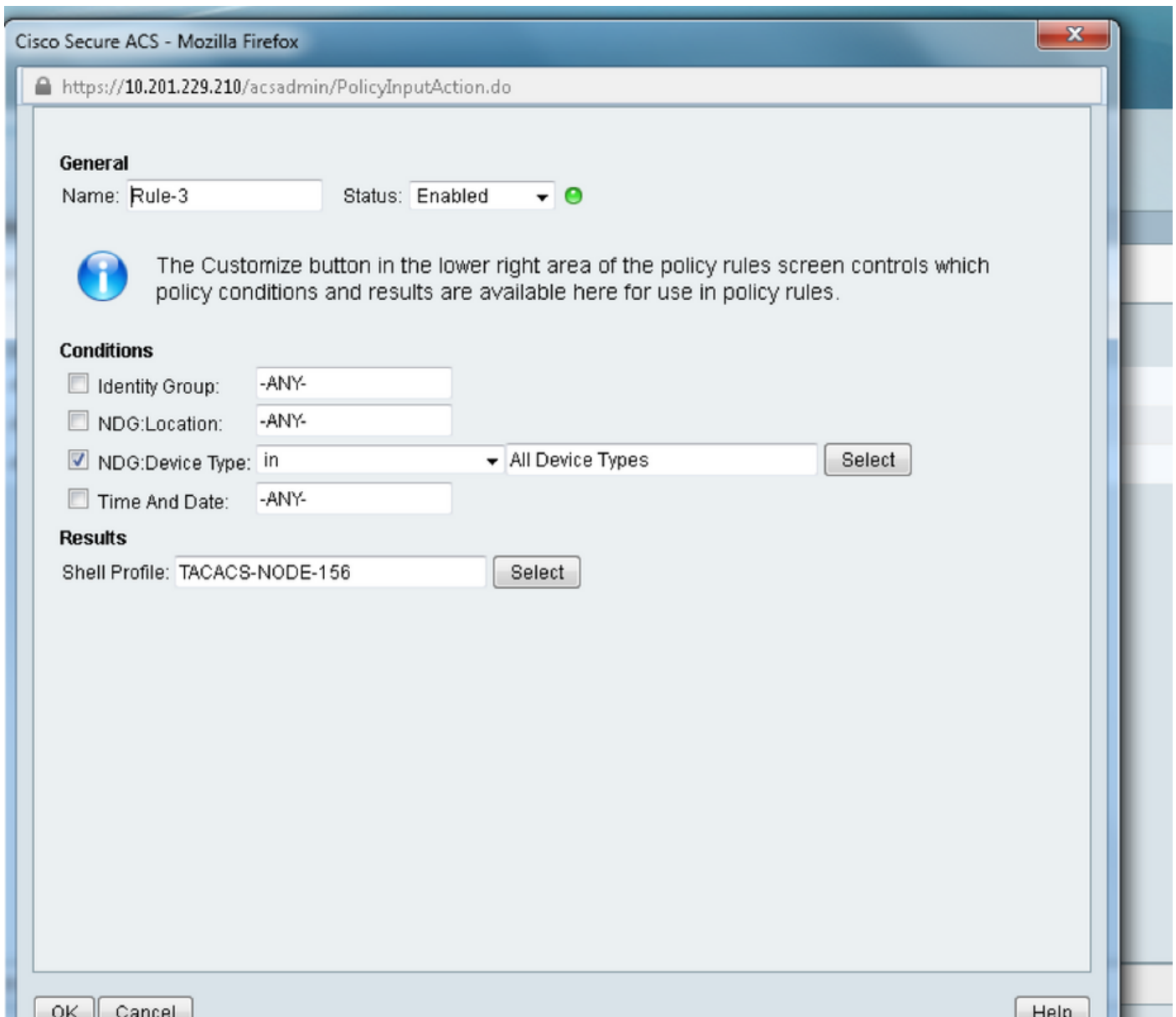


b. Seleccione **Authorization** y cree una regla para la autorización en el botón de opción **Default Device Admin**:

- Seleccione el perfil del shell **ya creado**
- Seleccione un dispositivo específico o todos los dispositivos del 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] ▶



Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.