

Configuratie van TACACS+ op Cisco ONS 15454/NCS2000 met ACS-server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft stap-voor-stap instructies hoe u terminaal toegangscontrollersysteem (TACACS+) kunt configureren op ONS 15454/NCS2000-apparaten en Cisco Access Control System (ACS). Alle onderwerpen omvatten voorbeelden. De lijst van eigenschappen in dit document is niet volledig of gezaghebbend en kan te allen tijde zonder bijwerking van dit document worden gewijzigd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Transport Controller (CTC) GU
- ACS-server

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

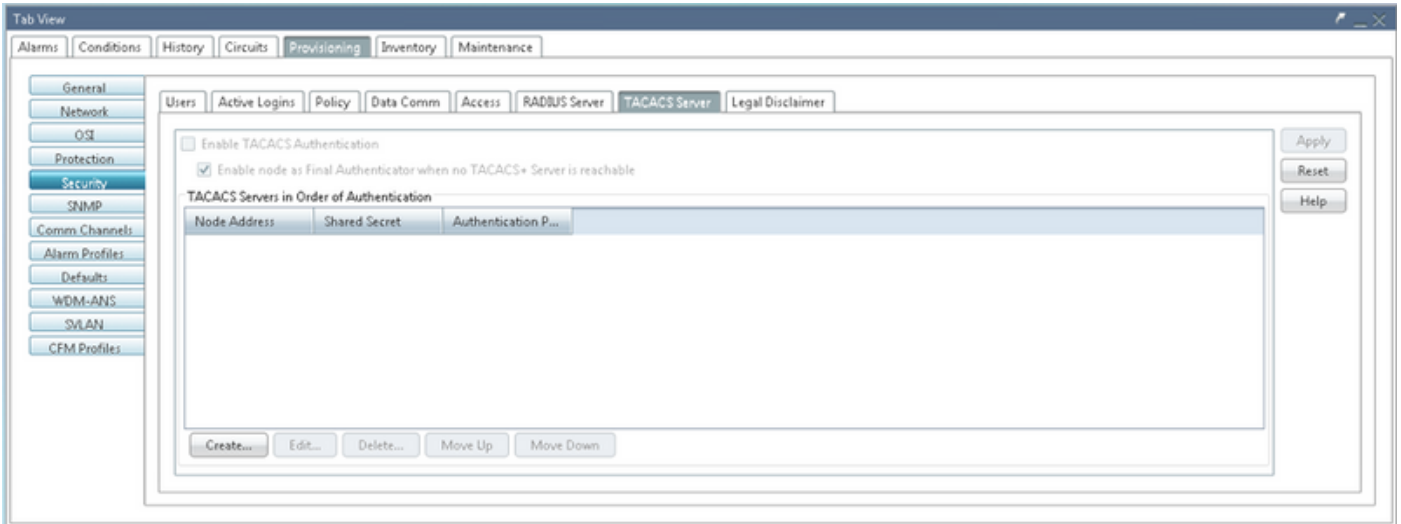
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie.

Opmerking: Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

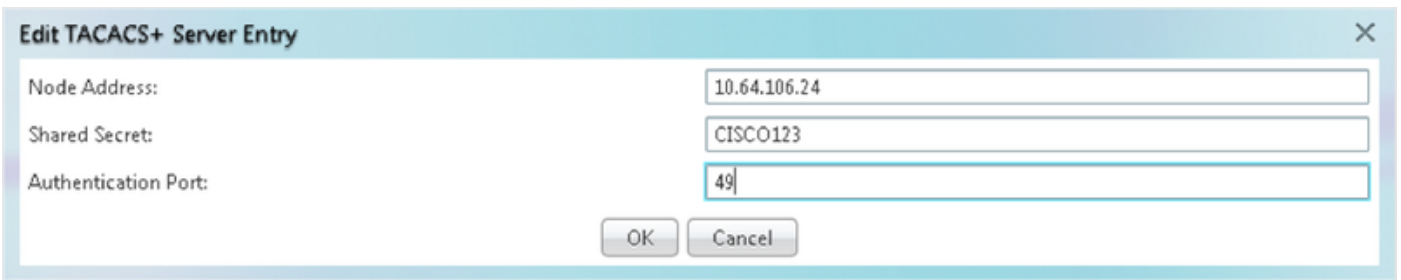
Configureren

Configuraties vereist op ONS 15454/NCS2000:

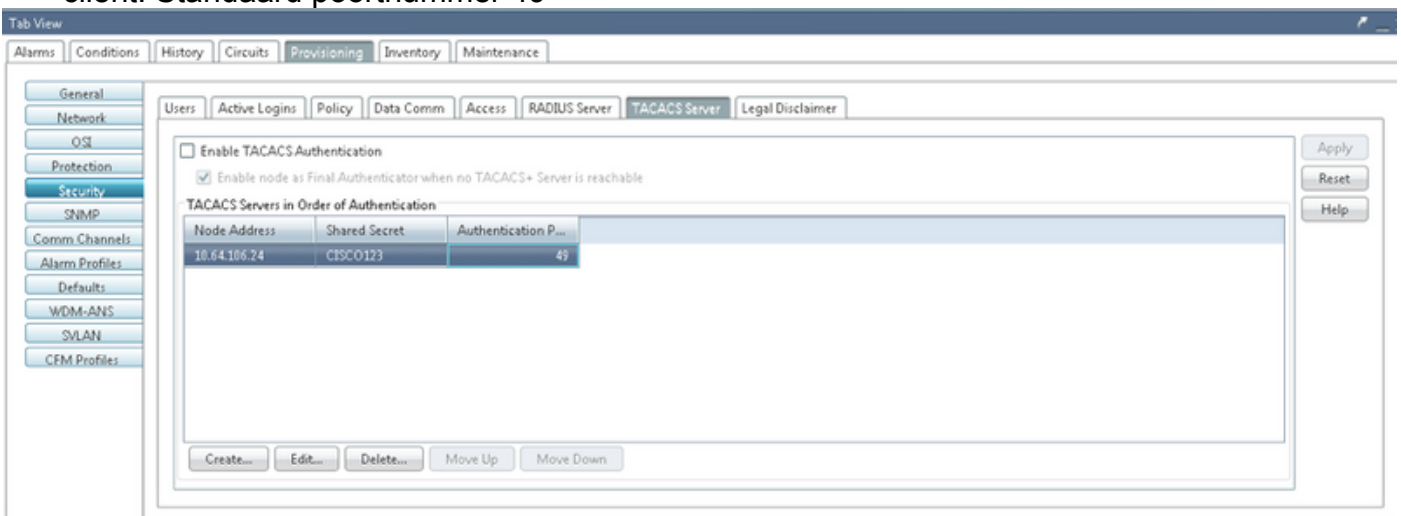
1. U kunt de TACACS-serverconfiguratie vanuit dit tabblad configureren. Navigeren in naar **Provisioning > Security > TACACS-server** zoals in de afbeelding wordt getoond.



2. Als u de TACACS+ servergegevens wilt toevoegen, klikt u op de knop **Maken**. Het wordt het configuratievenster TACACS+ geopend zoals in deze afbeelding.



- Voer het IP-adres van de server in
- Voeg het gedeelde geheim tussen Knooppunt en de TACACS+ server toe
- Voeg het authenticatiepoortnummer toe. In deze poort luistert de TACACS+ server naar de client. Standaard poortnummer 49



3. Om de TACACS+ serverconfiguratie op KNOOPPUNT te activeren, controleert u het selectieteken **TACACS-verificatie inschakelen** en klikt u op de knop **Toepassen** zoals in de afbeelding wordt weergegeven.

Enable TACACS Authentication

4. Als u het knooppunt als de laatste authenticator wilt inschakelen en er geen server beschikbaar is, klikt u op in het selectieteken zoals in de afbeelding.

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

5. Als u de serverconfiguratie wilt wijzigen, selecteert u de betreffende serverconfiguratie, klikt u op de knop **Bewerken** om de configuratie te wijzigen.

6. Als u de serverconfiguratie wilt verwijderen, selecteert u de betreffende serverconfiguratie rij, klikt u op de knop **Verwijderen** om de configuratie te verwijderen.

Configuraties vereist op ACS-server:

1. Maak een netwerkapparaat en een AAA-client en klik op de knop **maken** in het deelvenster **Netwerkbronnen** zoals in de afbeelding wordt weergegeven.



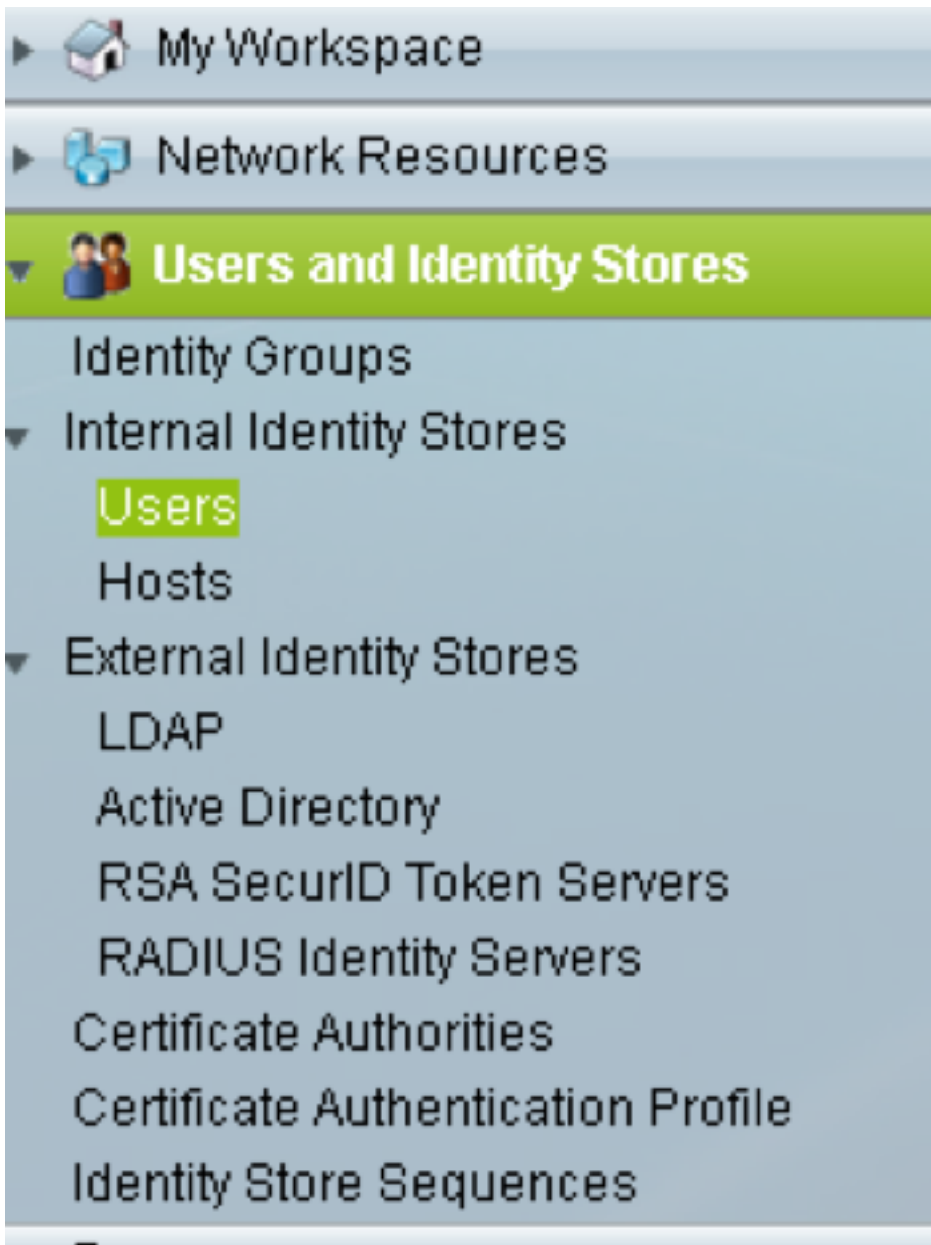
2. Geef hetzelfde **gedeelde geheim** als gegeven in de ONS-knoopconfiguratie. Anders zal de authenticatie mislukken.

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. Maak een gebruikersnaam en wachtwoord voor de gewenste gebruiker zodat deze geauthentiseerd kan worden in het deelvenster **Gebruikers en identiteitsopslag** zoals in de afbeelding.



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. shell profielen maken in het venster **Policy Elementen**:

a. Selecteer het voorkeursniveau (0 tot 3):





0 voor Retrieve gebruiker.

1 voor onderhoudsgebruiker.

2 voor Provisioning-gebruiker.

3 voor Superuser.

b. Maak een aangepaste eigenschap in het paneel **Klantkenmerken** voor de eigenschap **Werkeltijd**.

- ▶  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

Idletime "0" geeft aan dat verbinding nooit uitkomt en het zal nooit eeuwig zijn. Als gebruiker een andere tijd specificeert, zal verbinding beschikbaar zijn voor die vele seconden.

General Common Tasks **Custom Attributes**

Common Tasks Attributes

Attribute	Requirement	Value
Assigned Privilege Level	Mandatory	2


Manually Entered

Attribute	Requirement	Value
idletime	Mandatory	0

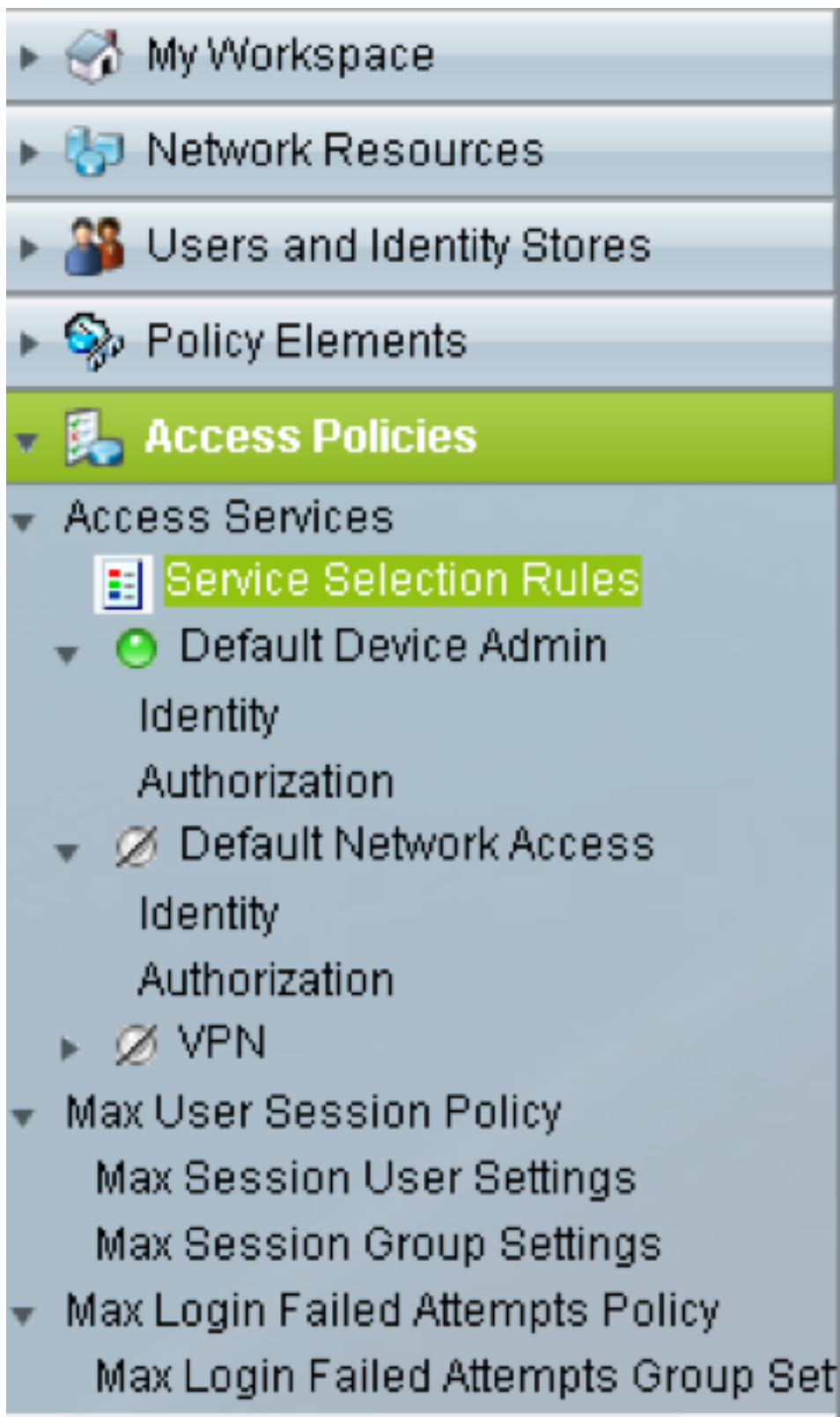
Attribute:

Requirement: Mandatory ▾

Attribute Value: Static ▾

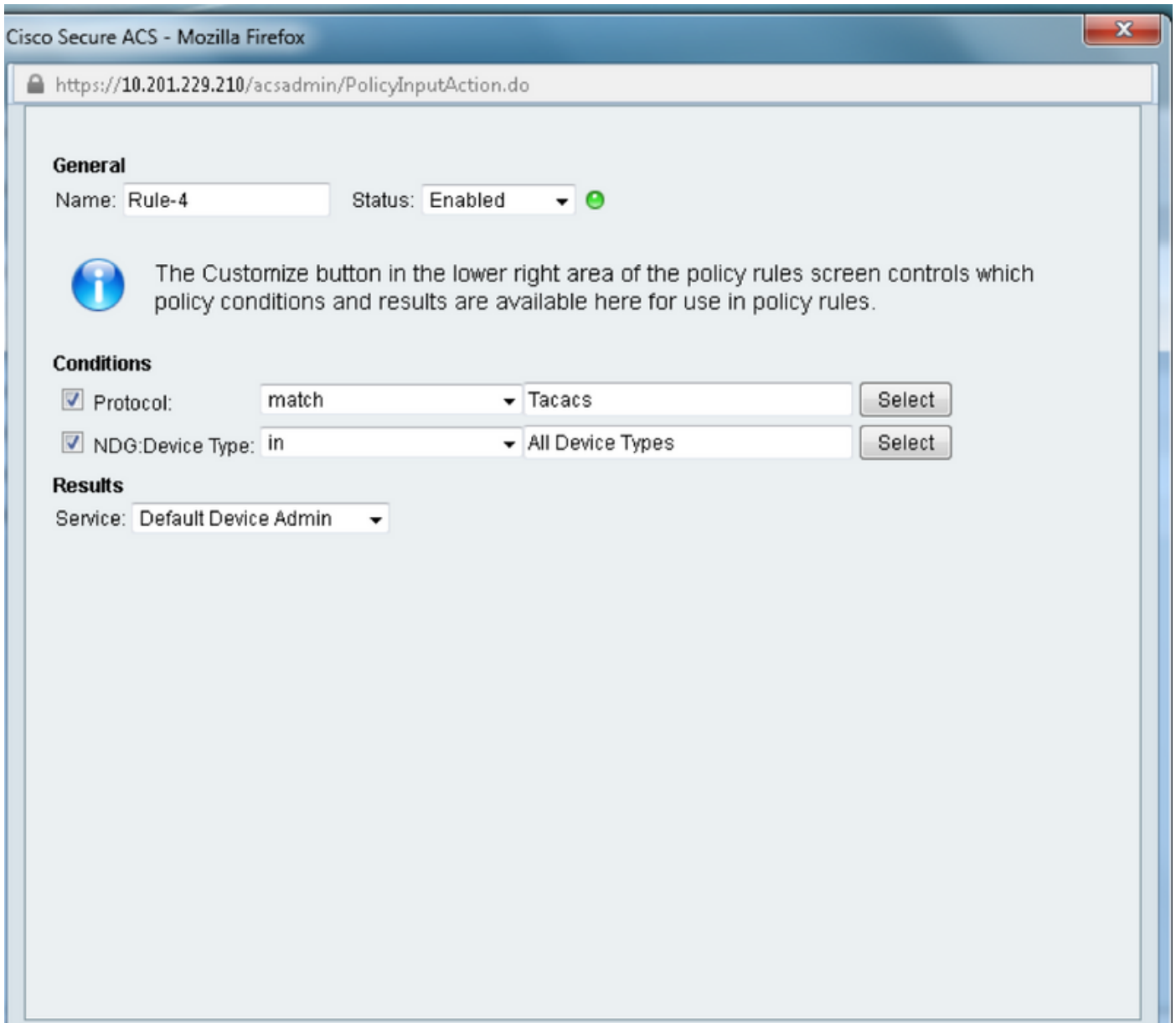


5. Toegangsbeleid maken in het paneel **Toegangsbeleid**:












a. Klik op **Service Selection Regels** en maak een regel:

- Selecteer TACACS als protocol
- Het apparaat als Alle apparaat of specifiek vergelijkbaar met dat dat dat eerder gemaakt is
- Servicetype als **standaard apparaatbeheer**.

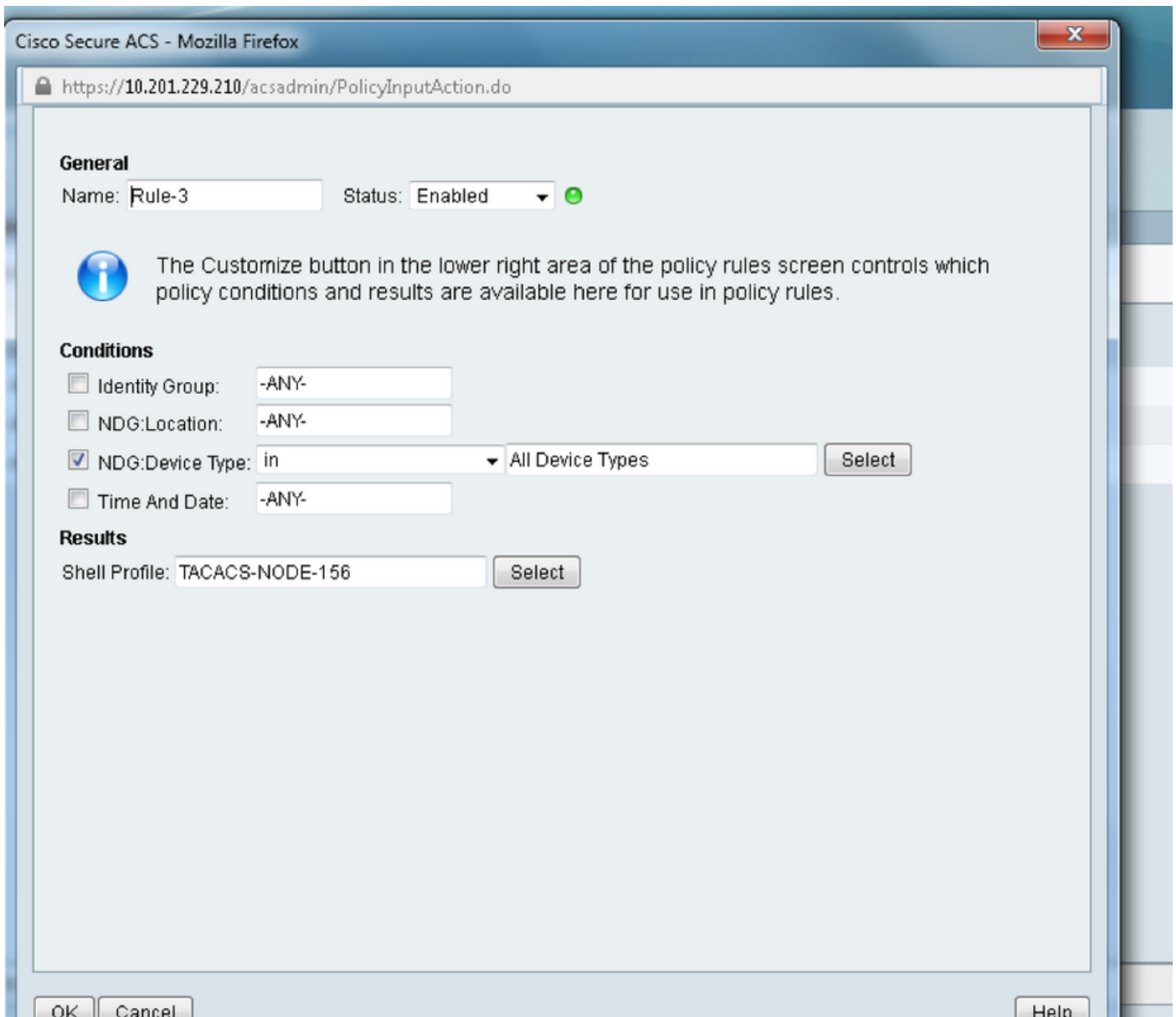


b. Selecteer **autorisatie** en maak een regel voor autorisatie in het keuzerondje **Default Devices Admin**:

- **Reeds gemaakt** shell-profiel selecteren
- Selecteer een specifiek apparaat of alle apparaten in een apparaattype

- ▶  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] ▶



Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.