

Konfigurieren von TACACS+ auf Cisco ONS15454/NCS2000 mit ACS-Server

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt Schritt-für-Schritt-Anweisungen zur Konfiguration des Terminal Access Controller Access Control System (TACACS+) auf ONS15454/NCS2000-Geräten und dem Cisco Access Control System (ACS). Alle Themen enthalten Beispiele. Die Liste der in diesem Dokument enthaltenen Attribute ist weder vollständig noch autoritär und kann jederzeit ohne Aktualisierung dieses Dokuments geändert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

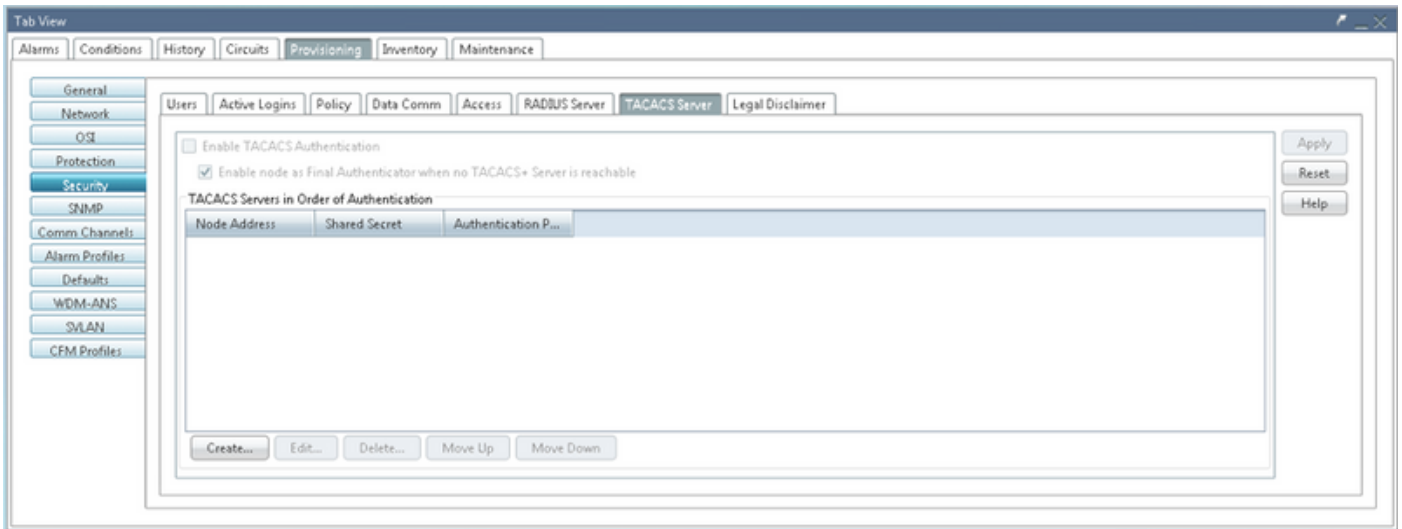
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen.

Hinweis: Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

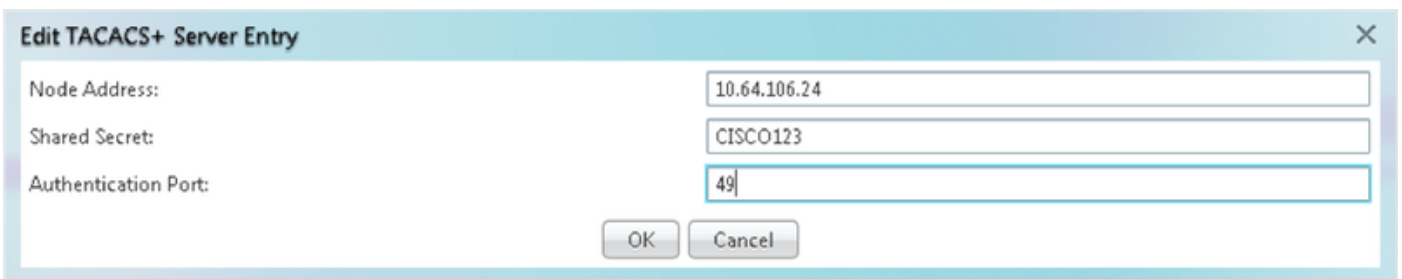
Konfigurieren

Auf ONS15454/NCS200 erforderliche Konfigurationen:

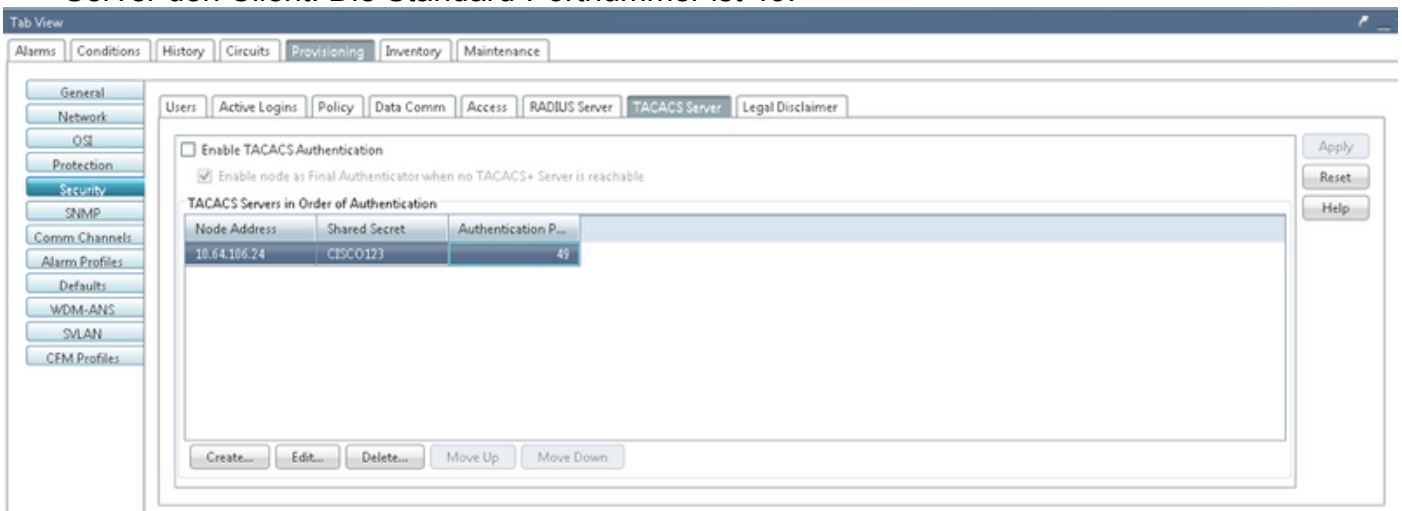
1. Sie können die TACACS-Serverkonfiguration über diese Registerkarte konfigurieren. Navigieren Sie zu **Provisioning > Security > TACACS Server (Bereitstellung > Sicherheit > TACACS-Server)** wie im Bild gezeigt.



2. Um die TACACS+-Serverdetails hinzuzufügen, klicken Sie auf die Schaltfläche **Erstellen**. Es öffnet das Konfigurationsfenster TACACS+, wie in diesem Bild gezeigt.



- Geben Sie die Server-IP-Adresse ein
- Fügen Sie den Shared geheimen Knoten und den TACACS+-Server hinzu.
- Fügen Sie die Authentifizierungsportnummer hinzu. An diesem Port überwacht der TACACS+-Server den Client. Die Standard-Portnummer ist 49.



3. Um die TACACS+-Serverkonfiguration im NODE zu aktivieren, aktivieren Sie das Kontrollkästchen **Enable TACACS Authentication (TACACS-Authentifizierung aktivieren)**, und klicken Sie auf die Schaltfläche **Apply** (Anwenden), wie im Bild gezeigt.

Enable TACACS Authentication

4. Um den Knoten als letzten Authentifizierer zu aktivieren, wenn kein Server erreichbar ist, aktivieren Sie das Kontrollkästchen, wie im Bild gezeigt.

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

5. Um die jeweilige Serverkonfiguration zu ändern, wählen Sie die entsprechende Serverkonfigurationszeile aus, und klicken Sie auf die Schaltfläche **Bearbeiten**, um die Konfiguration zu ändern.

6. Um die bestimmte Serverkonfiguration zu löschen, wählen Sie die entsprechende Serverkonfigurationszeile aus, und klicken Sie auf die **Schaltfläche Löschen**, um die Konfiguration zu löschen.

Auf dem ACS-Server erforderliche Konfigurationen:

1. Erstellen Sie ein Netzwerkgerät und einen AAA-Client, und klicken Sie auf die Schaltfläche **Erstellen** im Bereich **Netzwerkressourcen**, wie im Bild gezeigt.



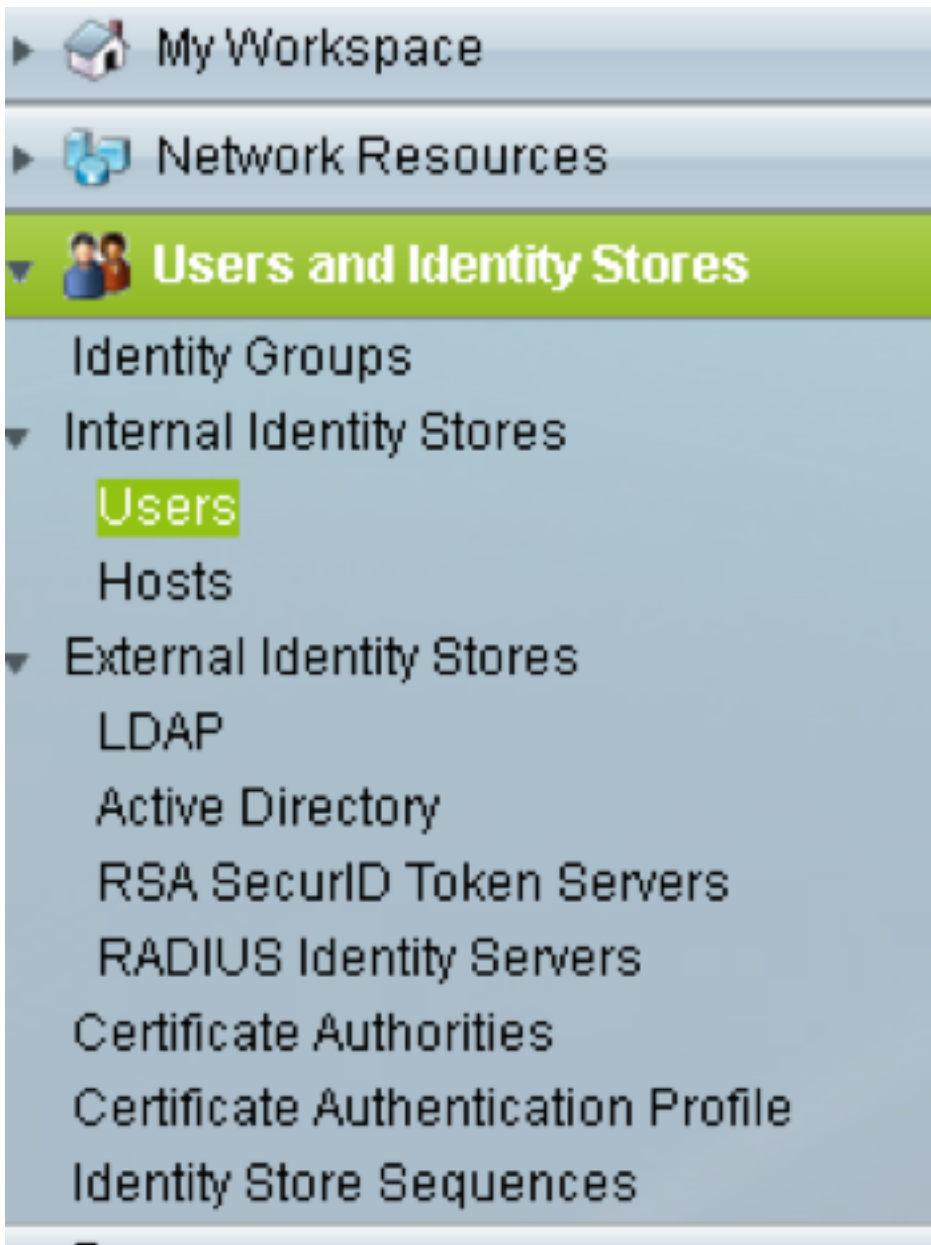
2. Geben Sie den gleichen **Shared Secret** wie in der ONS-Knotenkonfiguration. Andernfalls wird die Authentifizierung fehlgeschlagen.

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. Erstellen Sie einen Benutzernamen und ein Kennwort, damit der erforderliche Benutzer sich im Plan für **Benutzer und Identitätsdaten** authentifizieren lässt, wie im Bild gezeigt.



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. Erstellen von Shell-Profilen im Bereich Richtlinienelemente:

a) Wählen Sie die Berechtigungsstufe (0 bis 3) aus:





0 für Benutzer abrufen.

1 für Wartungsbenutzer.

2 für Provisioning User.

3 für Superuser.

b) Erstellen Sie ein benutzerdefiniertes Attribut im Bereich **Kundenattribute** für das **Idle Time**-Attribut.

- ▶  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" gibt an, dass die Verbindung nie ausfällt und für immer verfügbar ist. Der Benutzer eine andere Zeit angibt, ist die Verbindung für diese **Sekunden** verfügbar.

General Common Tasks **Custom Attributes**

Common Tasks Attributes

Attribute	Requirement	Value
Assigned Privilege Level	Mandatory	2


Manually Entered

Attribute	Requirement	Value
idletime	Mandatory	0

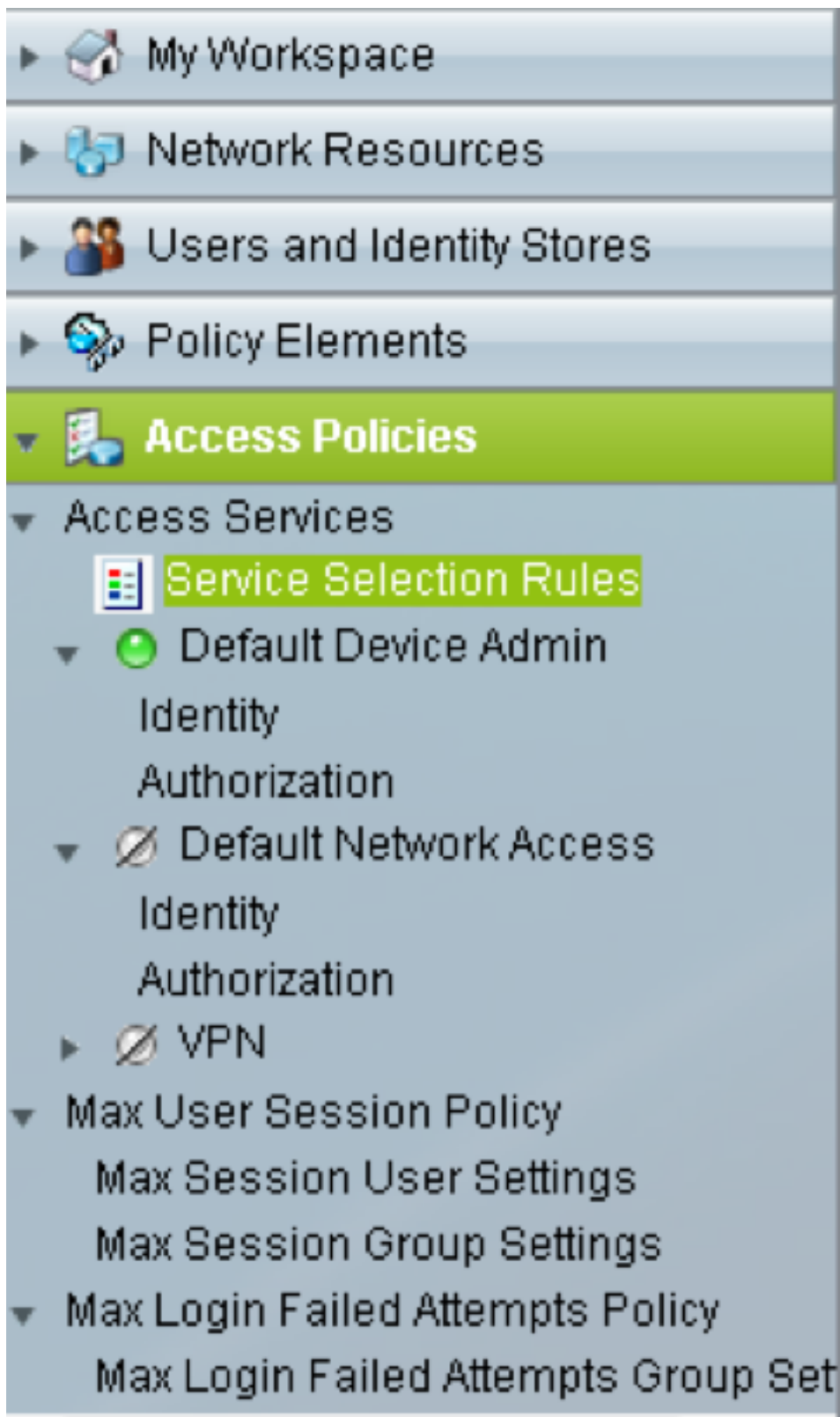
Attribute:

Requirement:

Attribute Value:



5. Erstellen Sie im Bereich **Zugriffsrichtlinien** Zugriffsrichtlinien:





a) Klicken Sie auf **Service Selection Rules** und erstellen Sie eine Regel:

- Wählen Sie TACACS als Protokoll aus
- Das Gerät ist "Alle" oder "Speziell", ähnlich dem, das zuvor erstellt wurde.
- Servicetyp als **Standard-Geräteadministrator**.

Cisco Secure ACS - Mozilla Firefox

https://10.201.229.210/acsadmin/PolicyInputAction.do

General
Name: Rule-4 Status: Enabled 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions










Protocol: match Tacacs

NDG:Device Type: in All Device Types

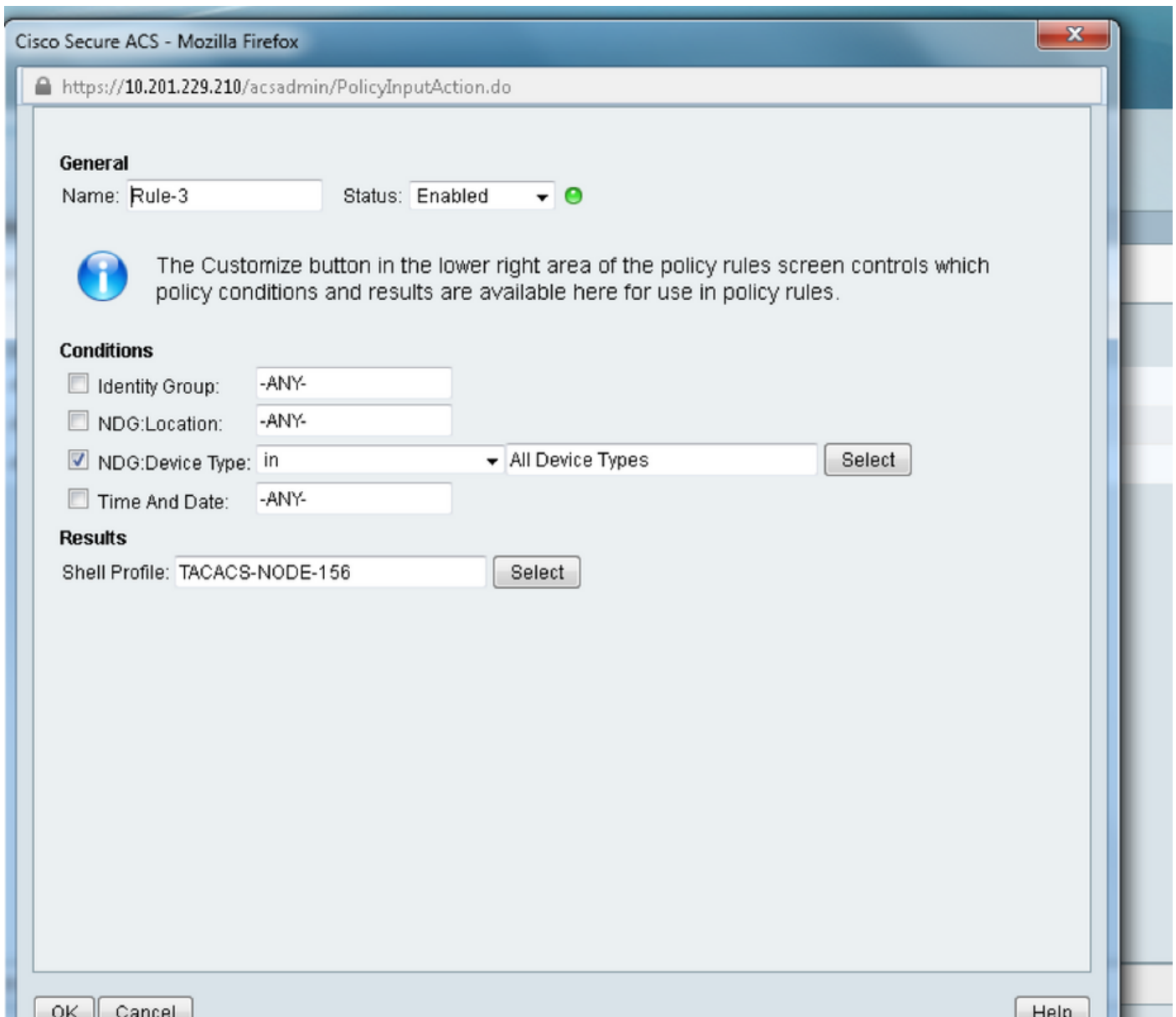
Results
Service: Default Device Admin

b) Wählen Sie **Authorization (Autorisierung) aus**, und erstellen Sie eine Regel für die Autorisierung in unter dem Optionsfeld **Default Device Admin (Standardgeräteadministrator)**:

- Wählen Sie **Already Created Shell-Profil** aus
- Wählen Sie ein bestimmtes Gerät oder alle Geräte im Gerätetyp aus.

- ▶  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] ▶



Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.