

Configurazione di TACACS+ su Cisco ONS15454/NCS2000 con server ACS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento vengono fornite istruzioni dettagliate su come configurare Terminal Access Controller Access Control System (TACACS+) sui dispositivi ONS15454/NCS2000 e Cisco Access Control System (ACS). Tutti gli argomenti includono esempi. L'elenco degli attributi fornito in questo documento non è esaustivo né autorevole e può essere modificato in qualsiasi momento senza un aggiornamento del documento.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- GU Cisco Transport Controller (CTC)
- Server ACS

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

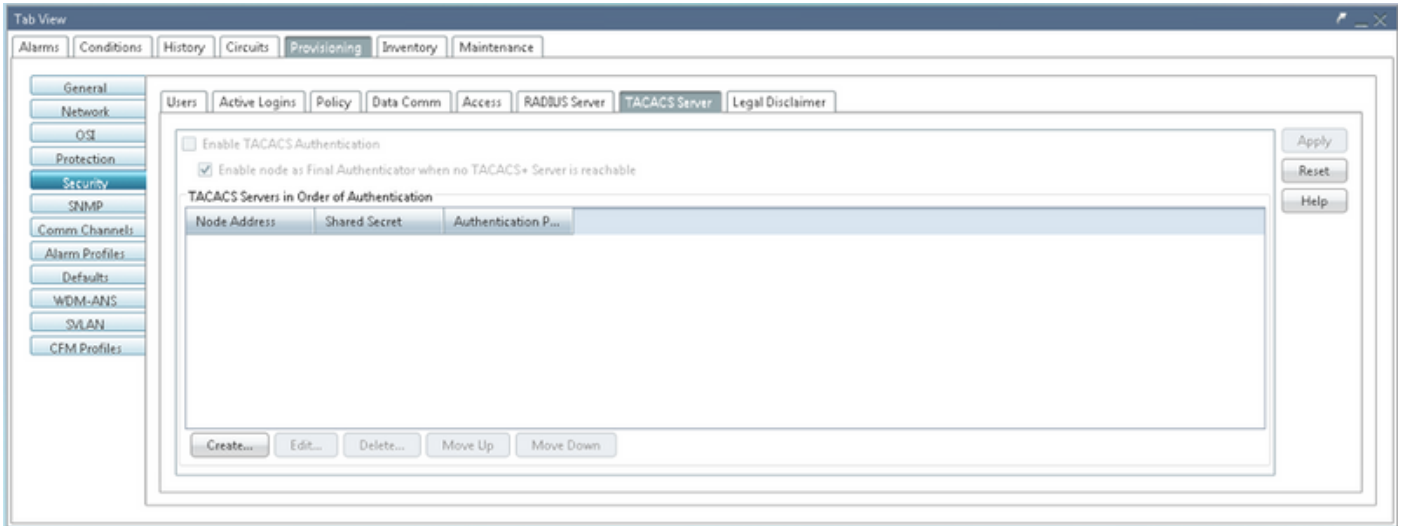
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti.

Nota: Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazioni richieste su ONS15454/NCS2000:

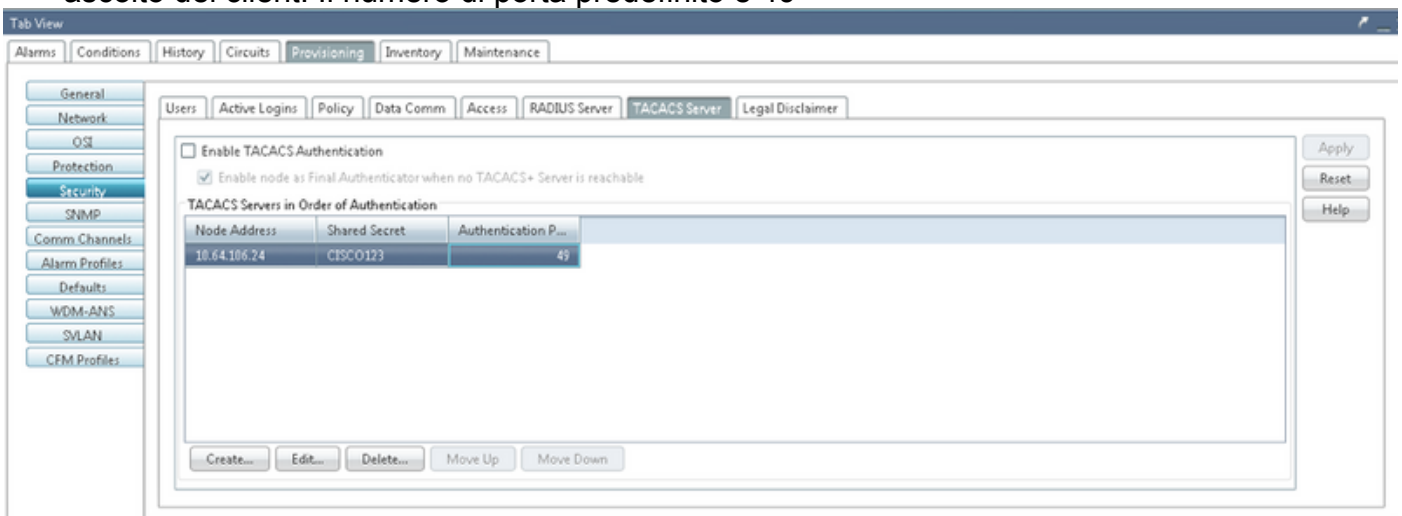
1. È possibile configurare la configurazione del server TACACS da questa scheda. Passare a **Provisioning > Sicurezza > Server TACACS** come mostrato nell'immagine.



2. Per aggiungere i dettagli del server TACACS+, fare clic sul pulsante **Create** (Crea). Viene visualizzata la finestra di configurazione TACACS+, come mostrato nell'immagine.



- Immettere l'indirizzo IP del server
- Aggiungere il segreto condiviso tra il nodo e il server TACACS+
- Aggiungere il numero della porta di autenticazione. A questa porta, il server TACACS+ è in ascolto del client. Il numero di porta predefinito è 49



3. Per attivare la configurazione del server TACACS+ su NODE, selezionare la casella di controllo **Enable TACACS Authentication** (Abilita autenticazione TACACS) e fare clic sul pulsante **Apply** (Applica), come mostrato nell'immagine.

Enable TACACS Authentication

4. Per abilitare il Nodo come autenticatore finale, quando nessun server è raggiungibile, fare clic sulla casella di spunta come mostrato nell'immagine.

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

5. Per modificare la configurazione del server, selezionare la riga di configurazione del server corrispondente e fare clic sul pulsante **Modifica** per modificare la configurazione.

6. Per eliminare una determinata configurazione del server, selezionare la riga di configurazione del server corrispondente e fare clic sul pulsante **Elimina** per eliminare la configurazione.

Configurazioni richieste sul server ACS:

1. Creare un dispositivo di rete e un client AAA e fare clic sul pulsante **crea** nel riquadro **Risorse di rete**, come mostrato nell'immagine.



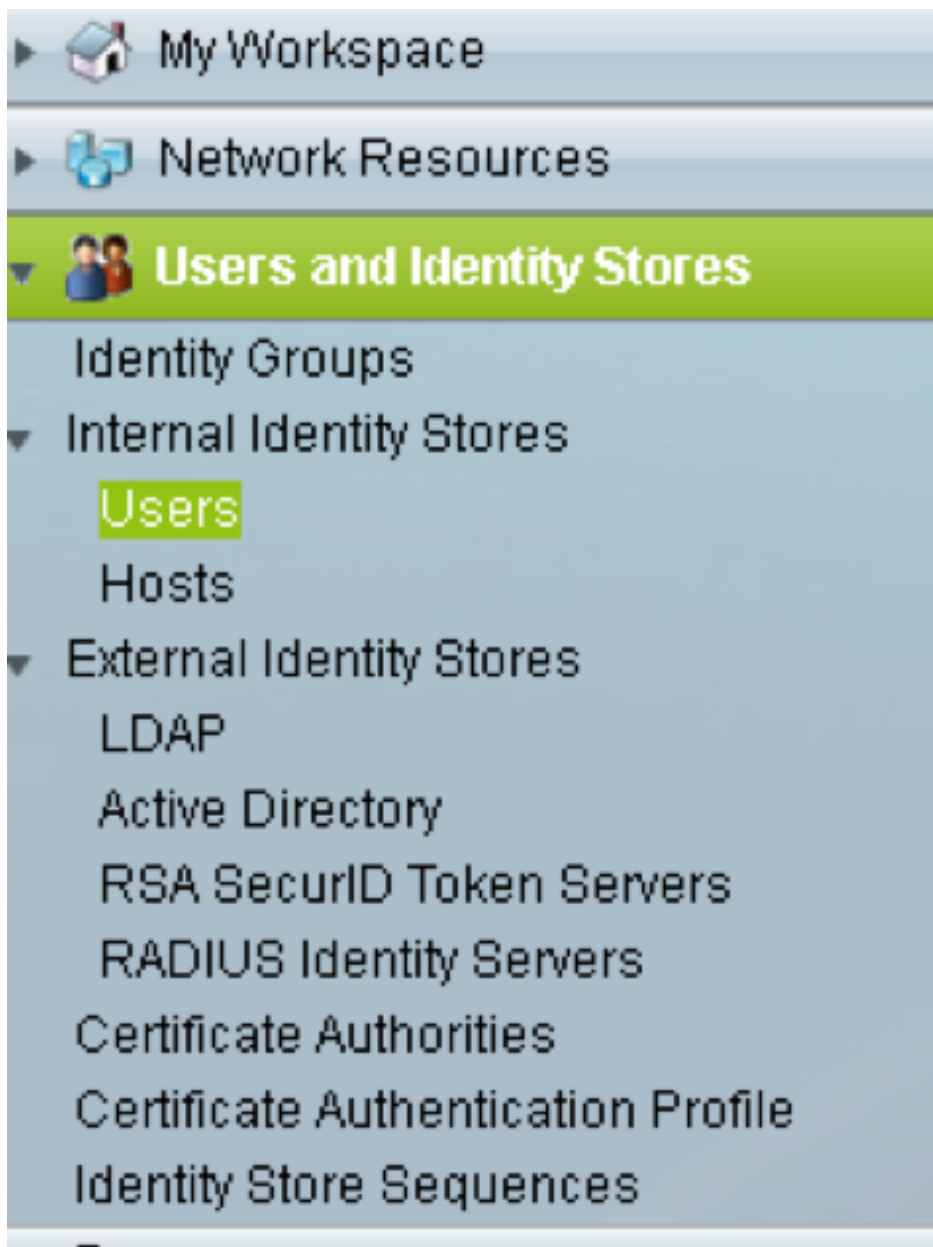
2. Assegnare lo stesso **segreto condiviso** specificato nella configurazione del nodo ONS. In caso contrario, l'autenticazione non riuscirà.

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. Creare un nome utente e una password per l'utente richiesto per l'autenticazione nel riquadro **Utenti e archivi identità**, come mostrato nell'immagine.



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. Creare profili di shell nel riquadro **Elementi criteri**:

r. Selezionare il livello di privilegio (da 0 a 3):

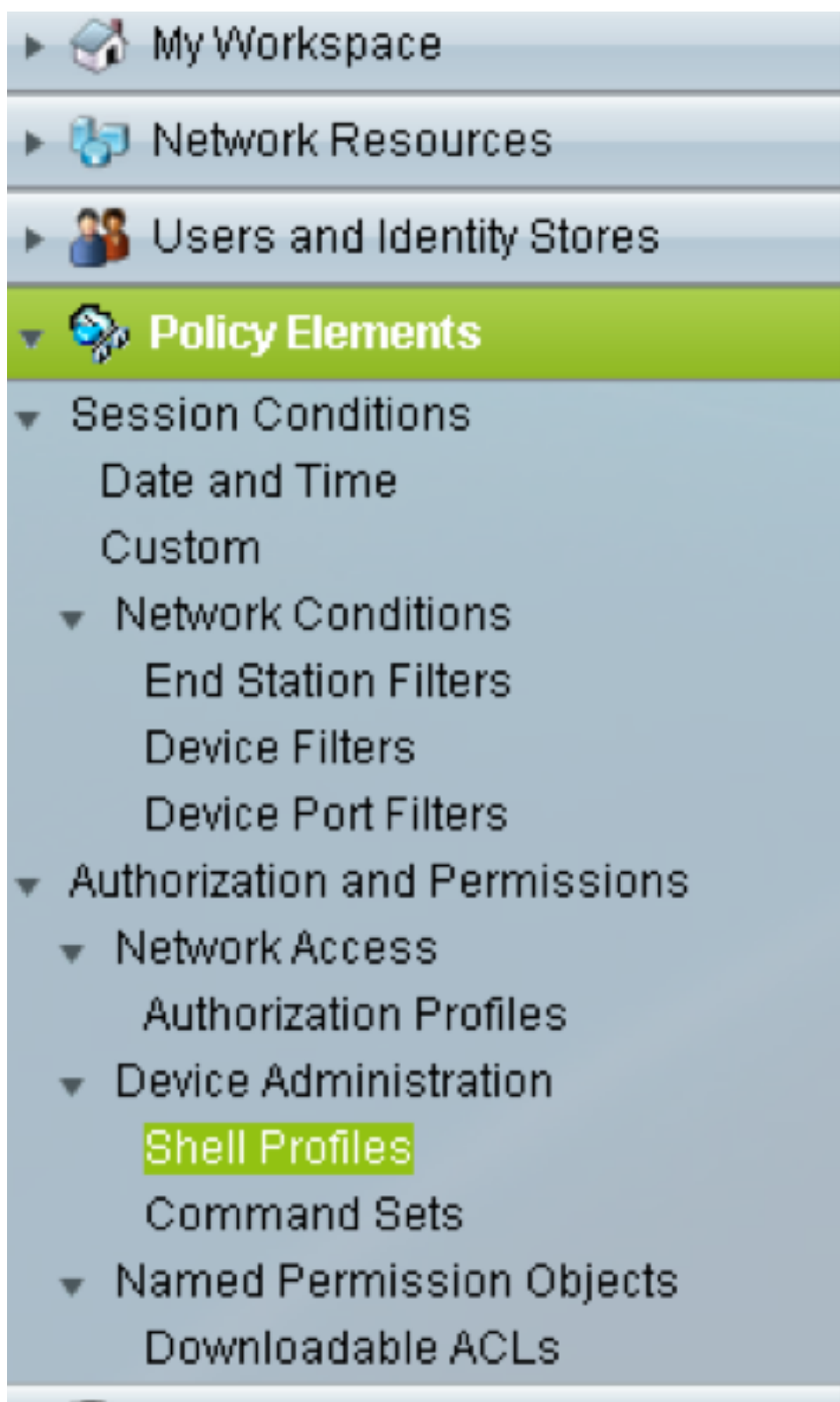
0 per l'utente Retrieve.

1 per l'utente Maintenance.

2 per l'utente del provisioning.

3 per Superuser.

b. Creare un attributo personalizzato nel pannello **Attributi cliente** per l'attributo **Tempo inattività**.



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 che la connessione non si interrompe mai e sarà per sempre. Se l'utente specifica un'altra ora, la connessione sarà disponibile per il numero di **secondi specificato**.

General Common Tasks **Custom Attributes**

Common Tasks Attributes

Attribute	Requirement	Value
Assigned Privilege Level	Mandatory	2


Manually Entered

Attribute	Requirement	Value
idletime	Mandatory	0

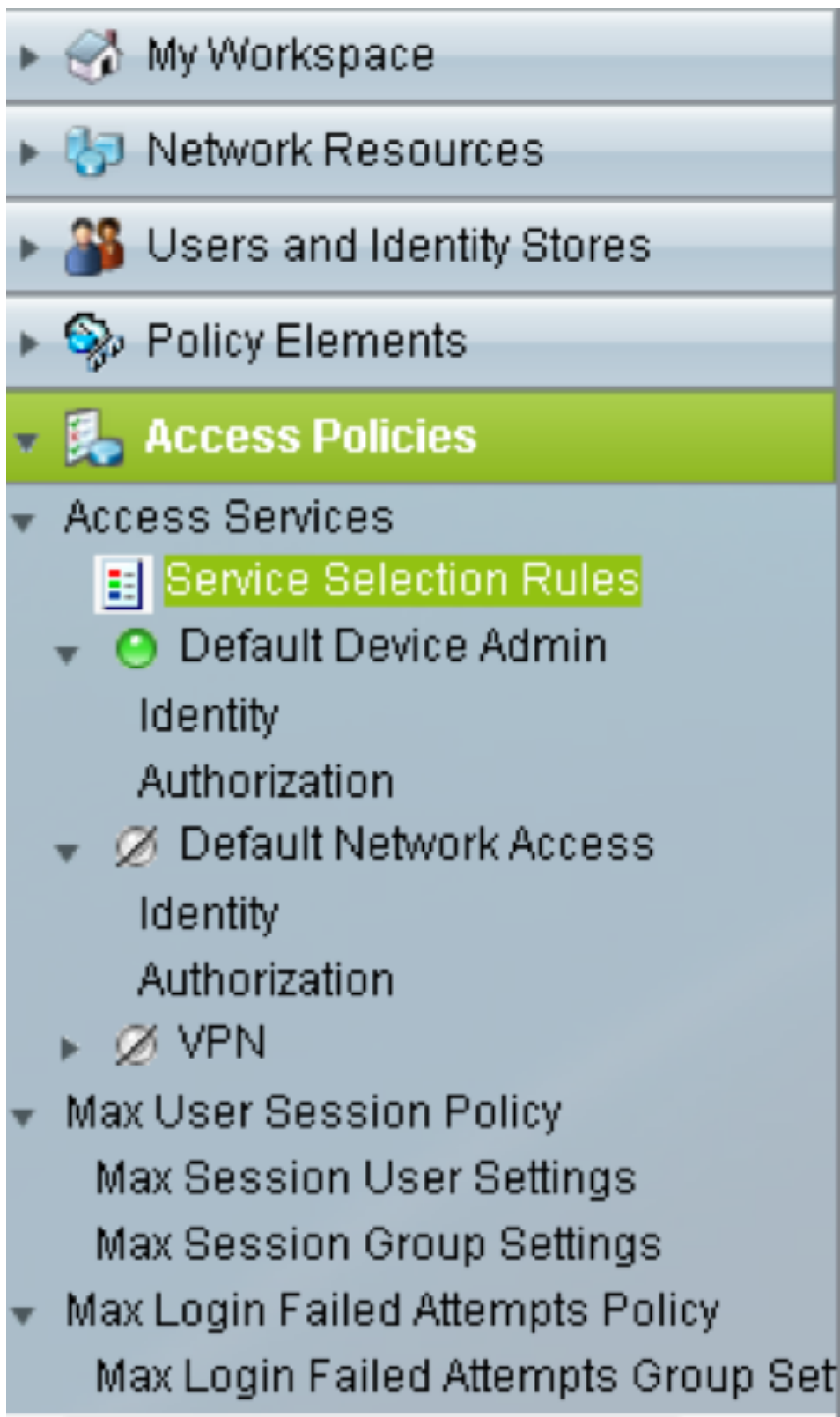
Attribute:

Requirement:

Attribute Value:



5. Creare criteri di accesso nel pannello **Criteri di accesso**:





r. Fare clic su **Regole selezione servizio** e creare una regola:

- Selezionare TACACS come protocollo
- Il dispositivo come Tutti i dispositivi o un dispositivo specifico simile a quello creato in precedenza
- Tipo di servizio come **amministratore predefinito del dispositivo**.

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

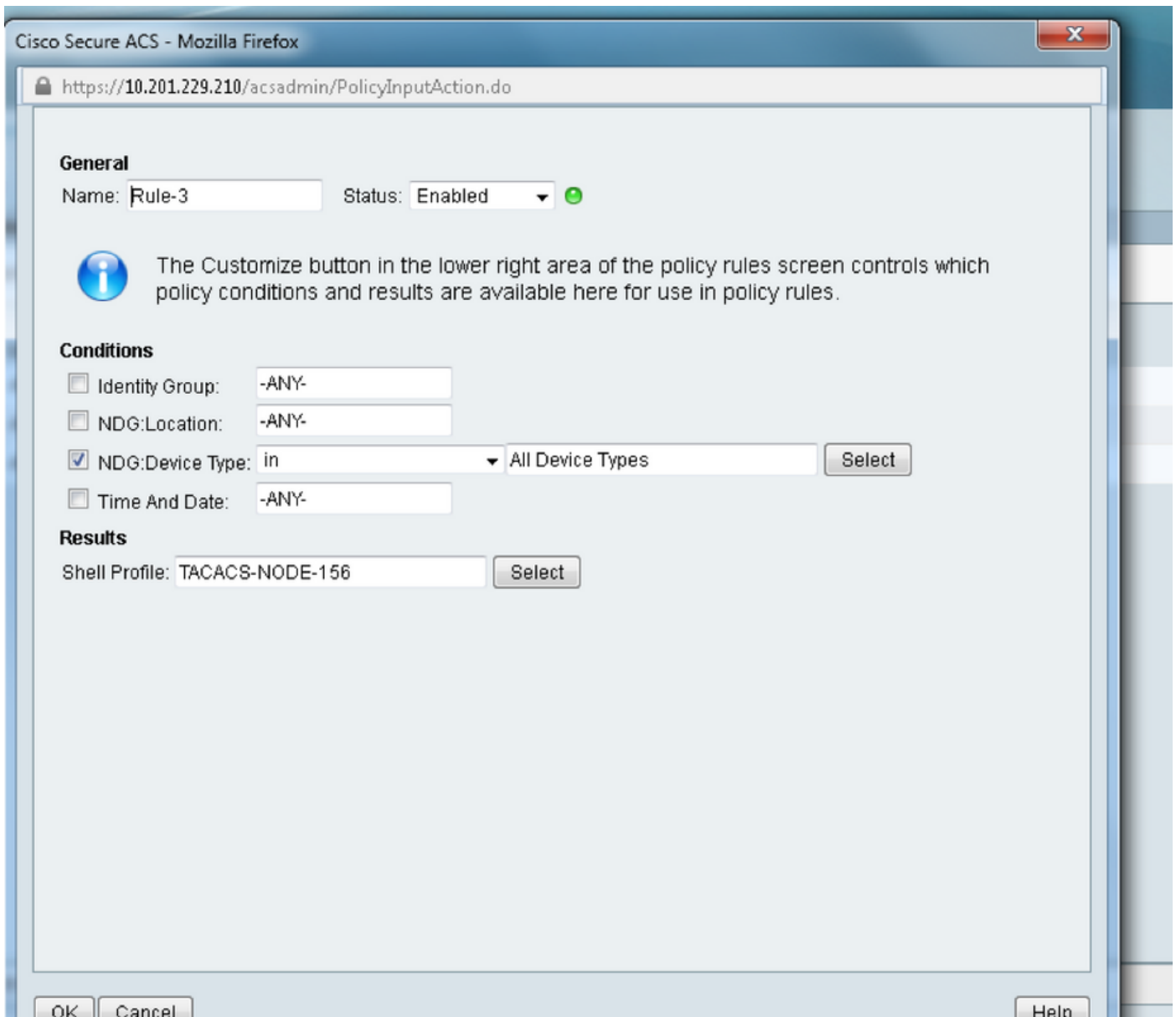
Service: Default Device Admin

b. Selezionare **Authorization** (Autorizzazione) e creare una regola per l'autorizzazione in (Pulsante di scelta **Default Device Admin**):

- Seleziona profilo shell **già creato**
- Selezionare un dispositivo specifico o tutti i dispositivi nel tipo

- ▶  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] ▶



Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.