

Configurer TACACS+ sur Cisco ONS15454/NCS2000 avec serveur ACS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit les instructions pas à pas sur la façon de configurer le système TACACS+ (Terminal Access Controller Access Control System) sur les périphériques ONS15454/NCS2000 et Cisco Access Control System (ACS). Tous les sujets incluent des exemples. La liste d'attributs fournie dans ce document n'est ni exhaustive ni faisant autorité et peut changer à tout moment sans mise à jour de ce document.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- GU Cisco Transport Controller (CTC)
- Serveur ACS

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

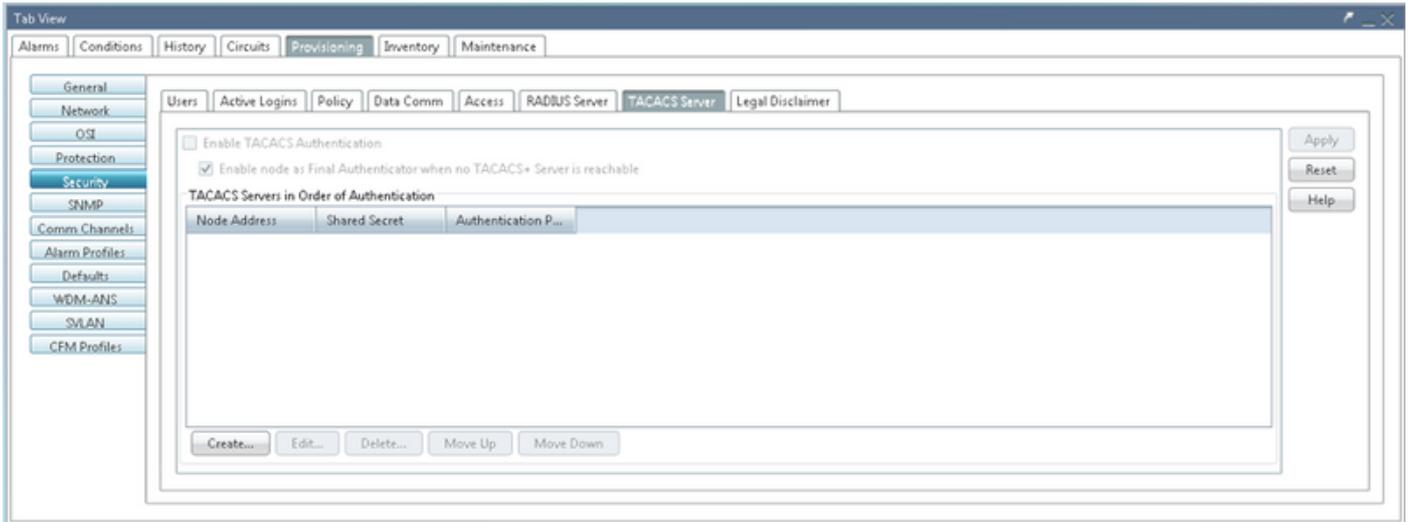
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration.

Note: Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

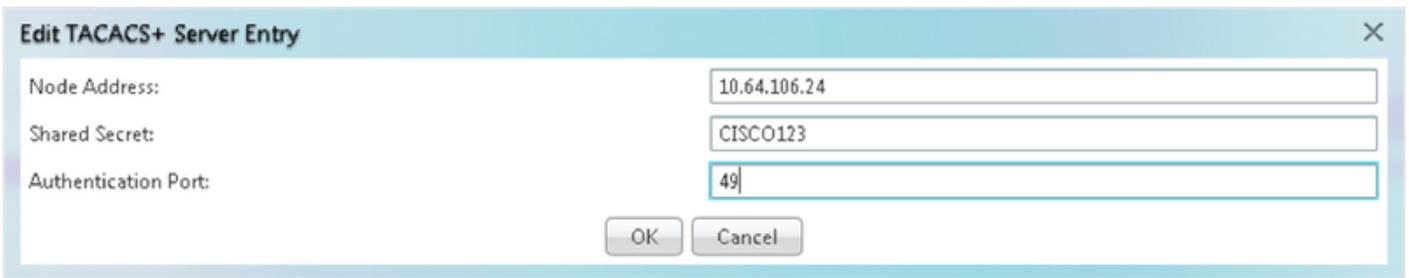
Configuration

Configurations requises sur ONS15454/NCS2000 :

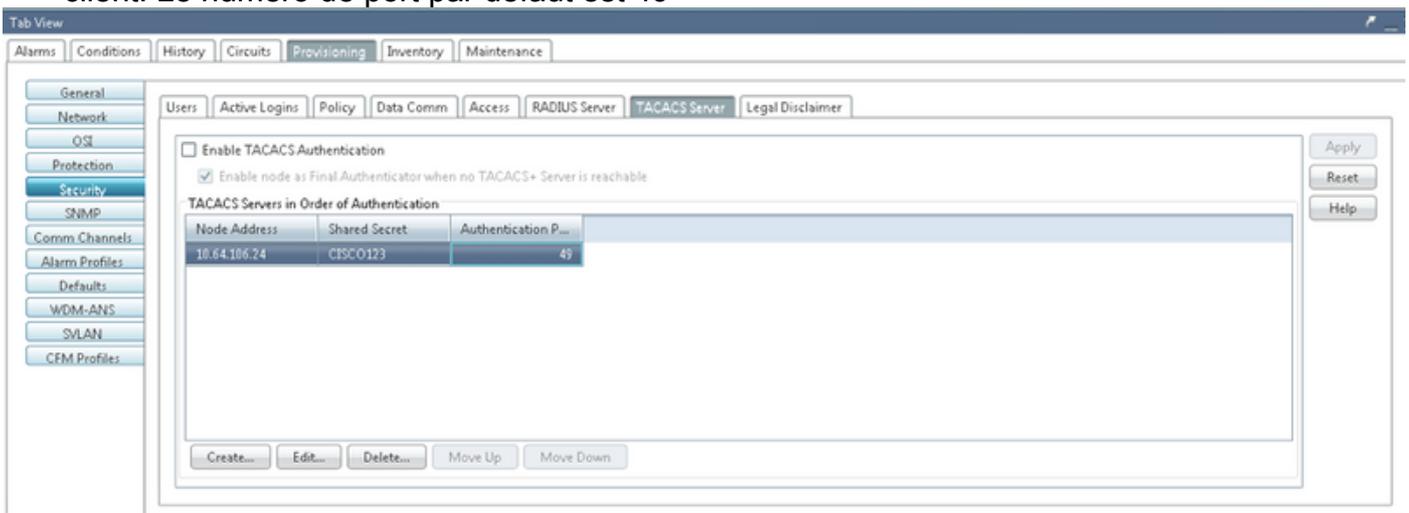
1. Vous pouvez configurer la configuration du serveur TACACS à partir de cet onglet. Accédez à **Provisioning > Security > TACACS Server** comme indiqué dans l'image.



2. Pour ajouter les détails du serveur TACACS+, cliquez sur le bouton **Créer**. La fenêtre de configuration TACACS+ s'ouvre, comme illustré dans cette image.



- Entrez l'adresse IP du serveur
- Ajouter le secret partagé entre le noeud et le serveur TACACS+
- Ajoutez le numéro de port d'authentification. Sur ce port, le serveur TACACS+ écoute le client. Le numéro de port par défaut est 49



3. Afin d'activer la configuration du serveur TACACS+ sur NODE, cochez la case **Enable TACACS Authentication** et cliquez sur le bouton **Apply** comme indiqué dans l'image.

Enable TACACS Authentication

4. Afin d'activer le noeud comme authentificateur final, lorsqu'aucun serveur n'est accessible,

cochez la case comme indiqué dans l'image.

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

5. Afin de modifier la configuration du serveur spécifique, sélectionnez la ligne de configuration du serveur correspondante, cliquez sur le bouton **Modifier** afin de modifier la configuration.

6. Afin de supprimer la configuration de serveur particulière, sélectionnez la ligne de configuration de serveur correspondante, cliquez sur le bouton **Supprimer** pour supprimer la configuration.

Configurations requises sur ACS Server :

1. Créez un périphérique réseau et un client AAA, puis cliquez sur le bouton **Créer** dans le plan **Ressources réseau** comme indiqué dans l'image.



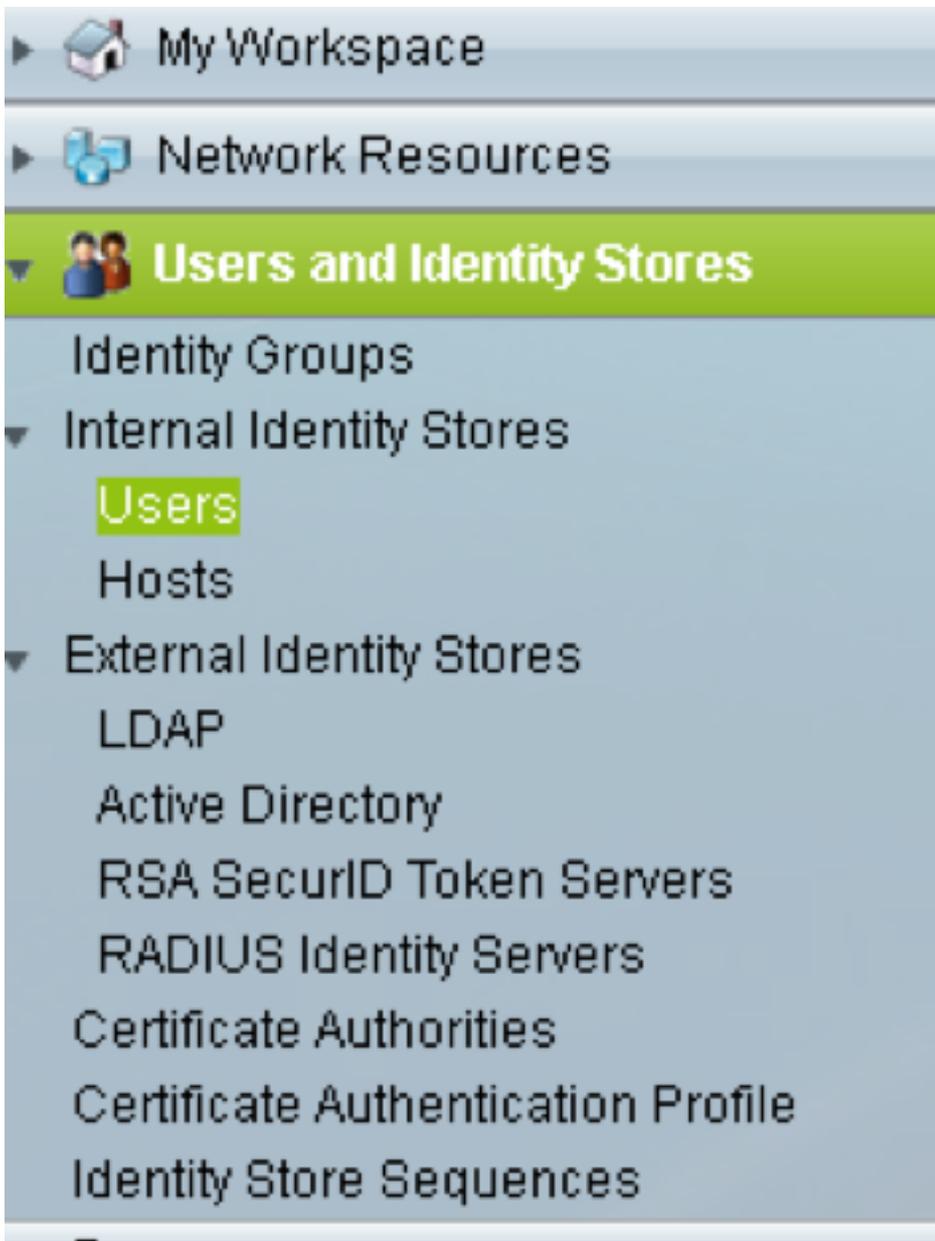
2. Donnez le même **secret partagé** que celui indiqué dans la configuration du noeud ONS. Sinon, l'authentification échouera.

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. Créez un nom d'utilisateur et un mot de passe pour que l'utilisateur requis puisse s'authentifier dans le plan **Utilisateurs et magasins d'identité** comme indiqué dans l'image.



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. Créer des profils de shell dans le volet **Eléments de stratégie** :

a. Sélectionnez le niveau de privilège (0 à 3) :

0 pour l'utilisateur Récupérer.

1 pour l'utilisateur Maintenance.

2 pour l'utilisateur Provisioning.

3 pour Superuser.

b. Créez un attribut personnalisé dans le panneau **Attributs client** pour l'attribut **Durée d'inactivité**.

- ▶  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 ” indique que la connexion ne expire jamais et qu'elle sera éternelle. Si l'utilisateur spécifie une autre heure, la connexion sera disponible pendant ces nombreuses **secondes**.

General Common Tasks **Custom Attributes**

Common Tasks Attributes

Attribute	Requirement	Value
Assigned Privilege Level	Mandatory	2

Manually Entered

Attribute	Requirement	Value
idletime	Mandatory	0

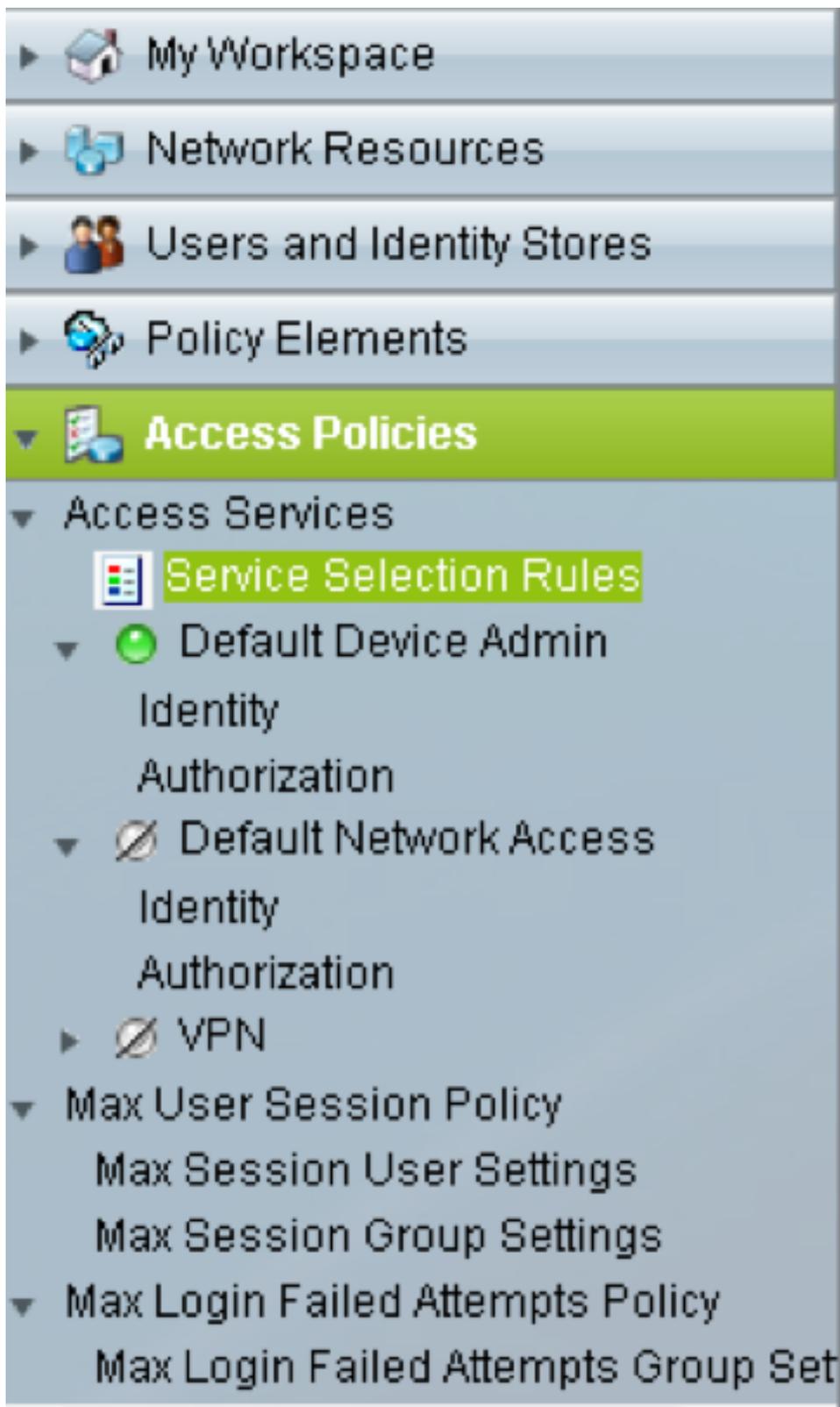
Attribute:

Requirement:

Attribute Value:

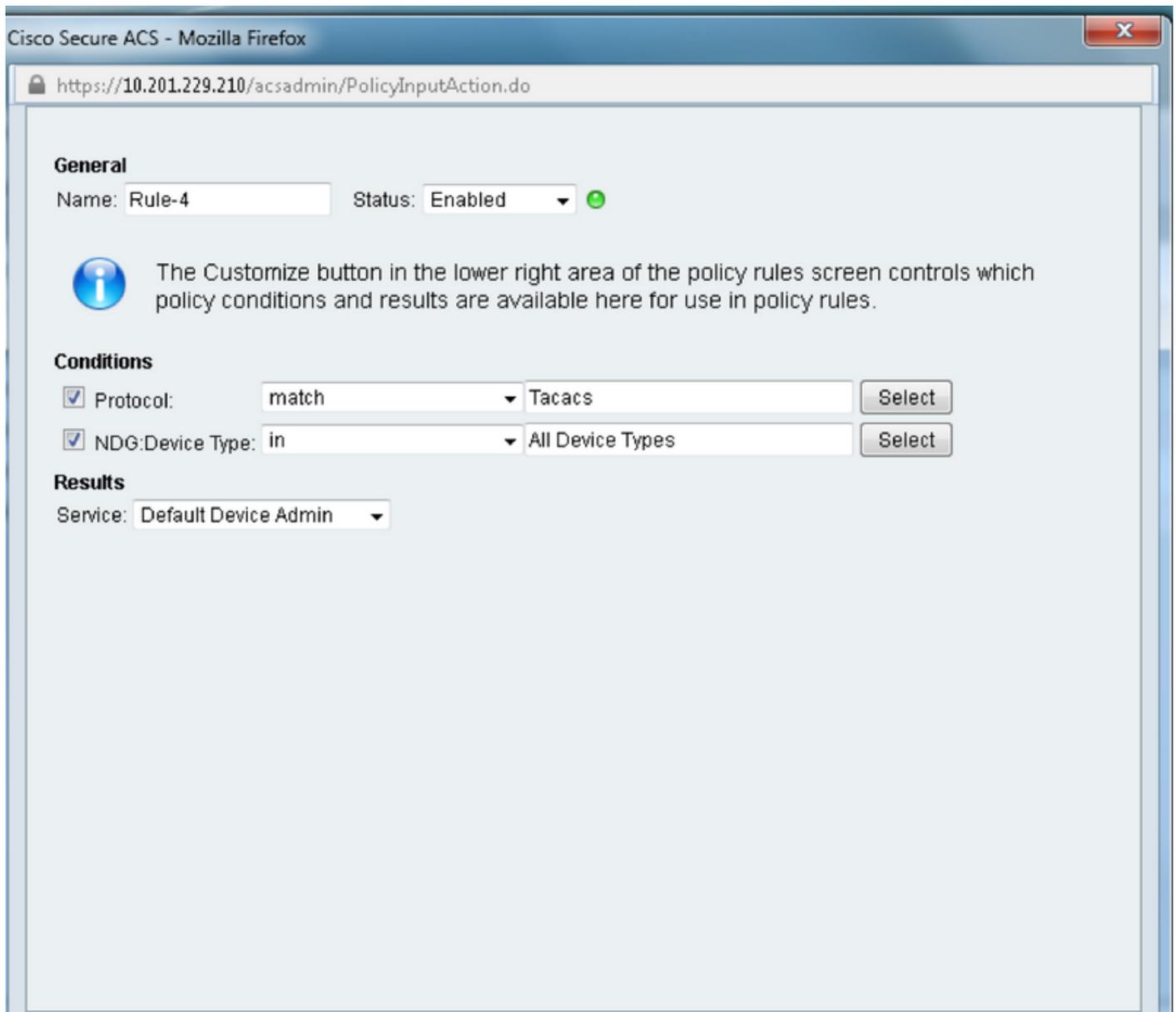


5. Créer des stratégies d'accès dans le panneau **Politiques d'accès** :



a. Cliquez sur **Règles de sélection de service** et créez une règle :

- Sélectionner TACACS comme protocole
- Le périphérique en tant que périphérique All ou spécifique similaire à celui créé précédemment
- Type de service en tant qu'**administrateur de périphérique par défaut**.

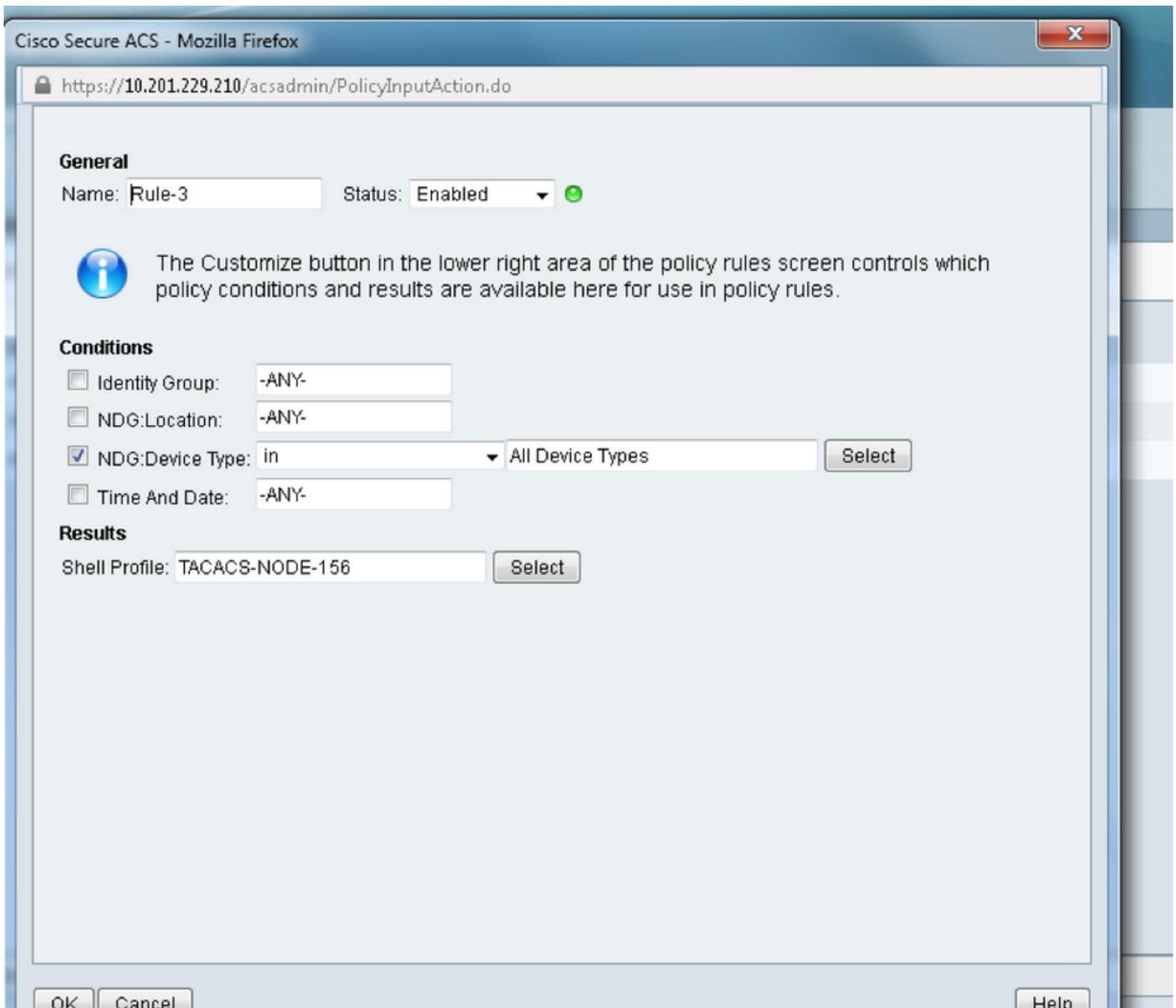


b. Sélectionnez **Autorisation** et créez une règle d'autorisation dans sous la case d'option **Admin du périphérique par défaut** :

- Sélectionner le profil de shell **déjà créé**
- Sélectionner un périphérique spécifique ou tous les périphériques du type de périphérique

- ▶  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] ▶



Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.