在帶ACS伺服器的Cisco ONS15454/NCS2000上配置TACACS+

目錄

簡介

本文說明如何在ONS15454/NCS2000裝置和思科存取控制系統(ACS)上設定終端存取控制器存取控制系統(TACACS+)的逐步指示。 所有主題均包含示例。本檔案提供的屬性清單並不詳盡，也不具權威性，可能會隨時變更，無需更新本檔案即可。

必要條件

需求

思科建議您瞭解以下主題：

- 思科傳輸控制器(CTC)GU
- ACS伺服器

採用元件

本文件所述內容不限於特定軟體和硬體版本。

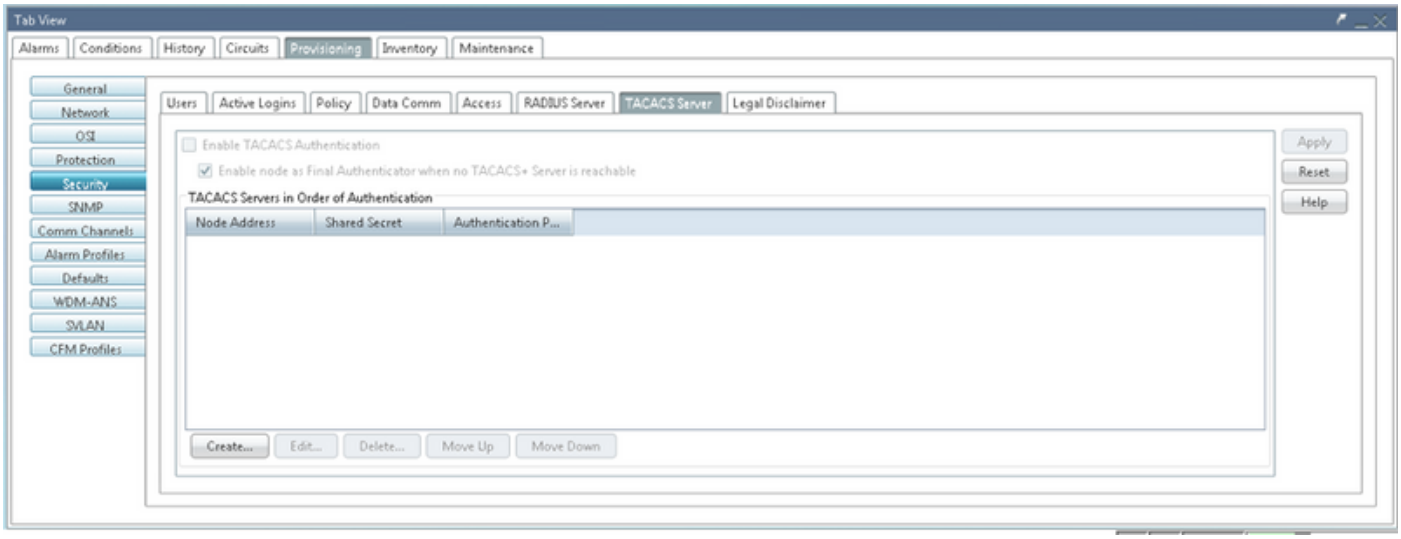
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。

> **附註**：如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

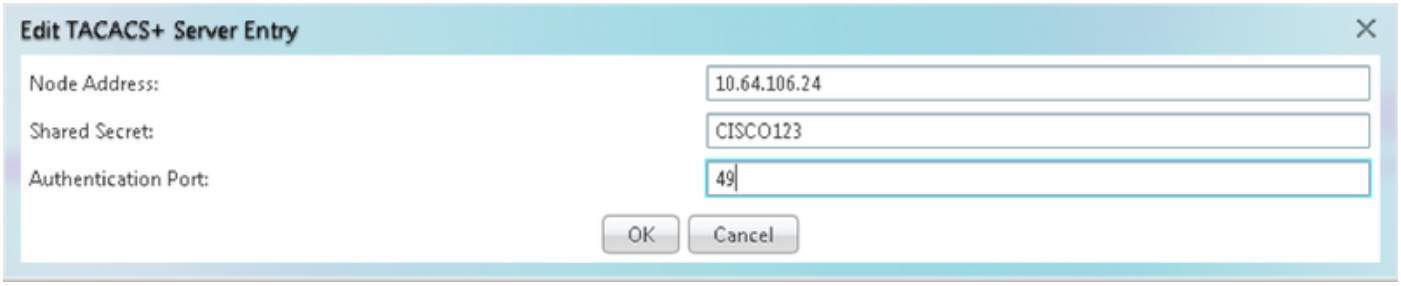
設定

ONS15454/NCS2000所需的配置：

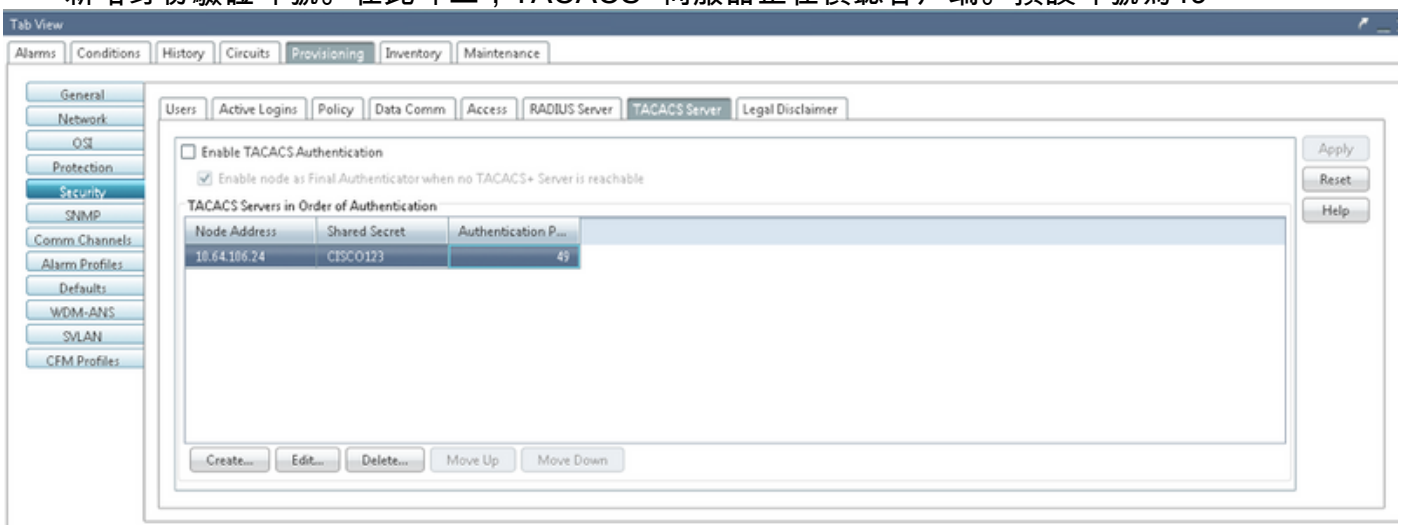
1.您可以從此選項卡配置TACACS伺服器配置。導航到**Provisioning > Security > TACACS Server**，如下圖所示。



2.若要新增TACACS+伺服器詳細資訊，請按一下**Create**按鈕。它會開啟TACACS+配置視窗，如下圖所示。

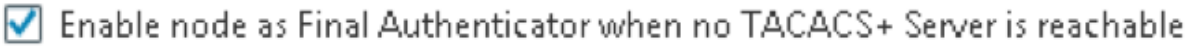


- 輸入伺服器IP地址
- 在節點和TACACS+伺服器之間新增共用金鑰
- 新增身份驗證埠號。在此埠上，TACACS+伺服器正在偵聽客戶端。預設埠號為49



3.若要在NODE上啟用TACACS+伺服器配置，請勾選**Enable TACACS Authentication**覈取方塊，然後按一下**Apply**按鈕，如下圖所示。

4.要使節點成為最終驗證者，當無法訪問伺服器時，請按一下覈取方塊，如下圖所示。



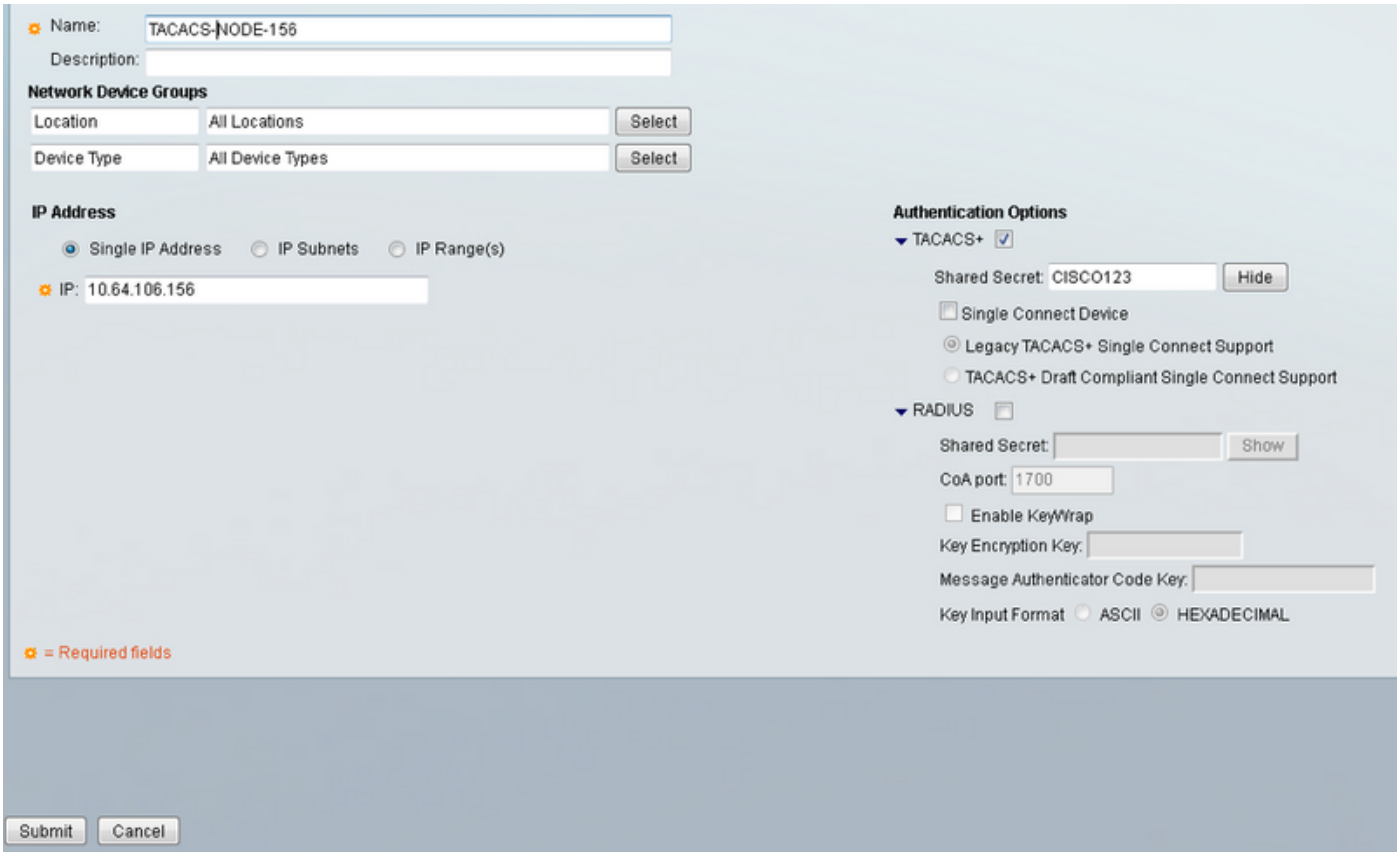
5.要修改特定的伺服器配置，請選擇相應的伺服器配置行，按一下**Edit**按鈕以修改配置。

6.要刪除特定的伺服器配置，請選擇相應的伺服器配置行，按一下**Delete**按鈕刪除該配置。

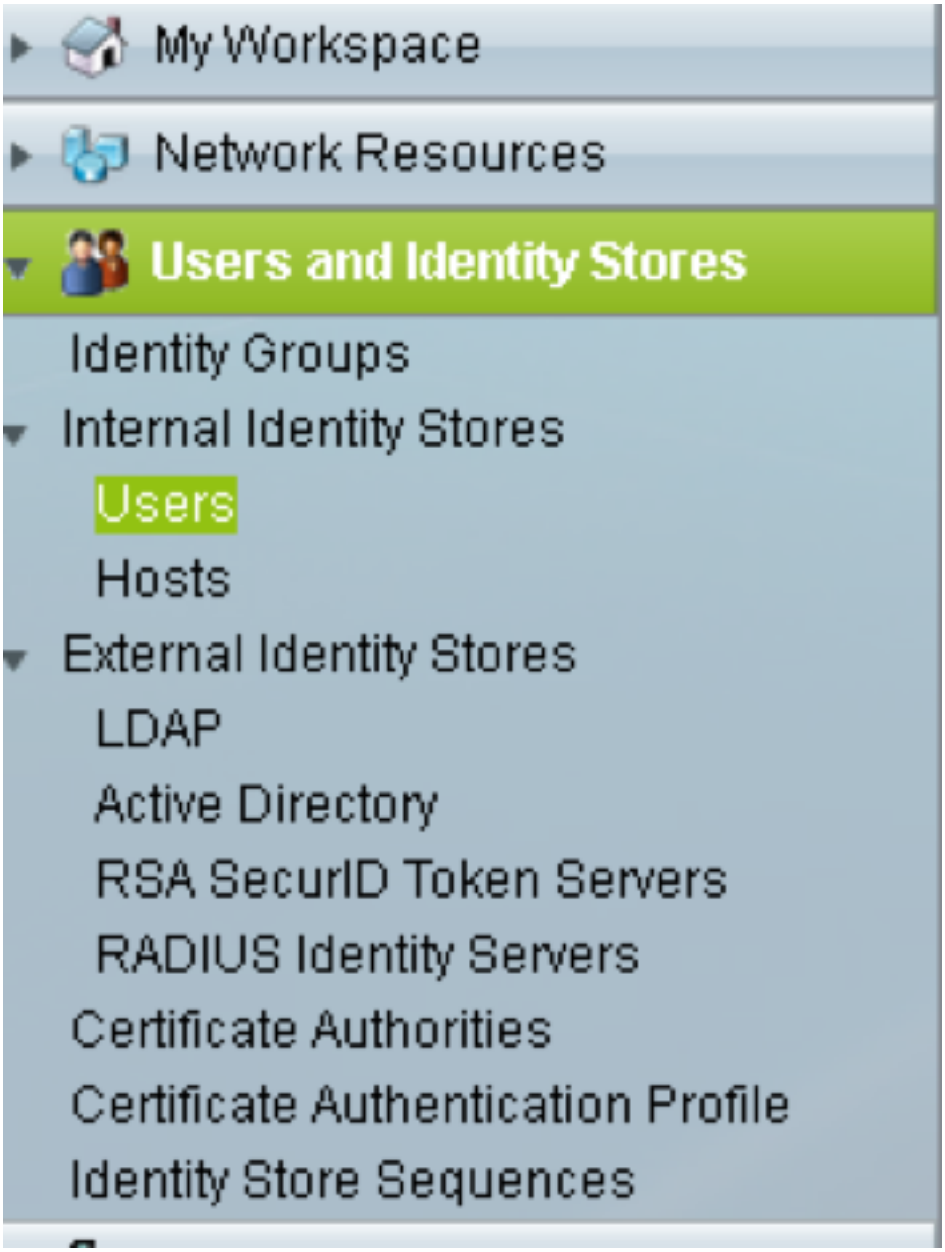
ACS伺服器上所需的配置：

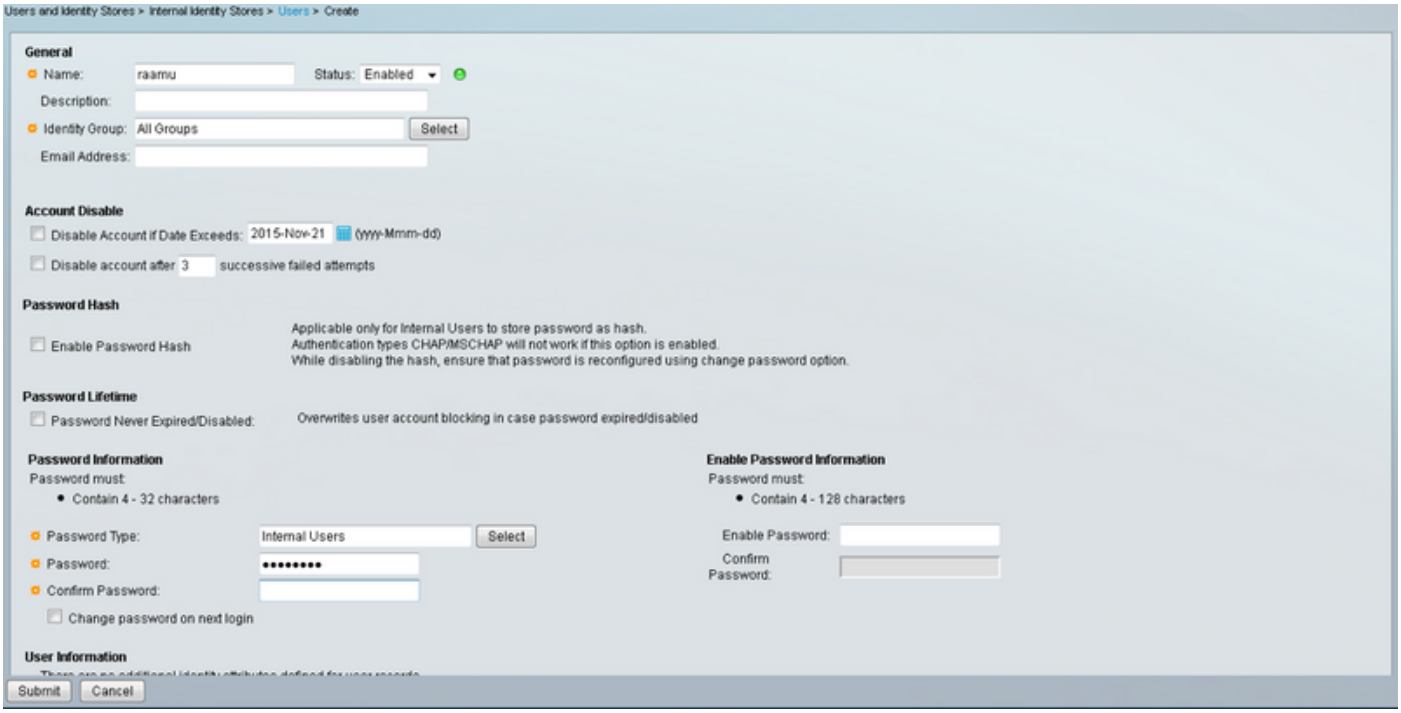
1. 建立網路裝置和AAA客戶端，然後在**網路資源**窗格中按一下**create**按鈕，如下圖所示。

2. 提供與ONS節點配置中給定的**共用金鑰**。否則，身份驗證將失敗。



3.為需要在**Users and Identity Stores** Pan中進行身份驗證的使用者名稱和密碼，如下圖所示。





4. 在**Policy** Elements窗格中建立**殼配置**檔案：

a.選擇許可權級別（0到3）：

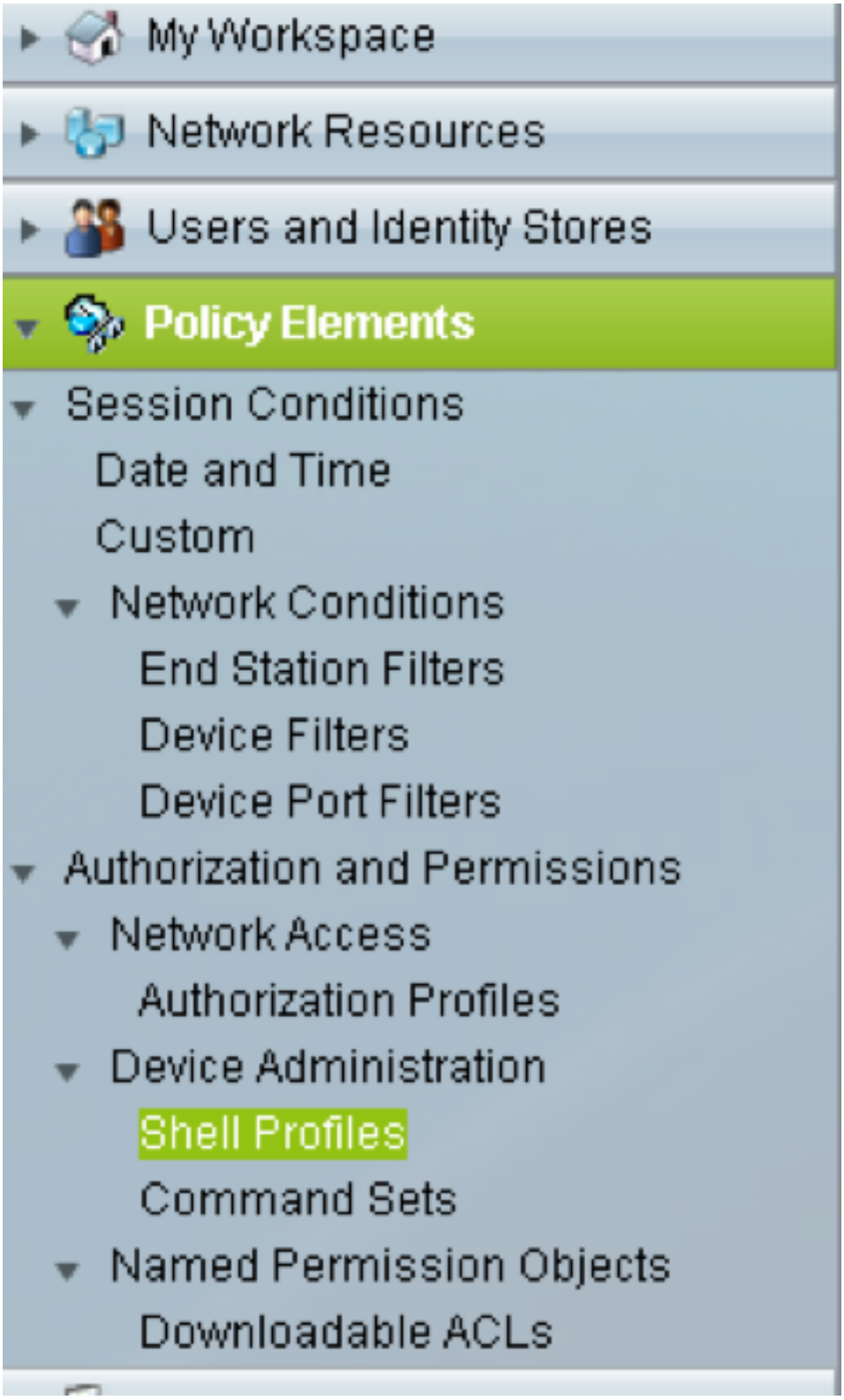
0，表示檢索使用者。

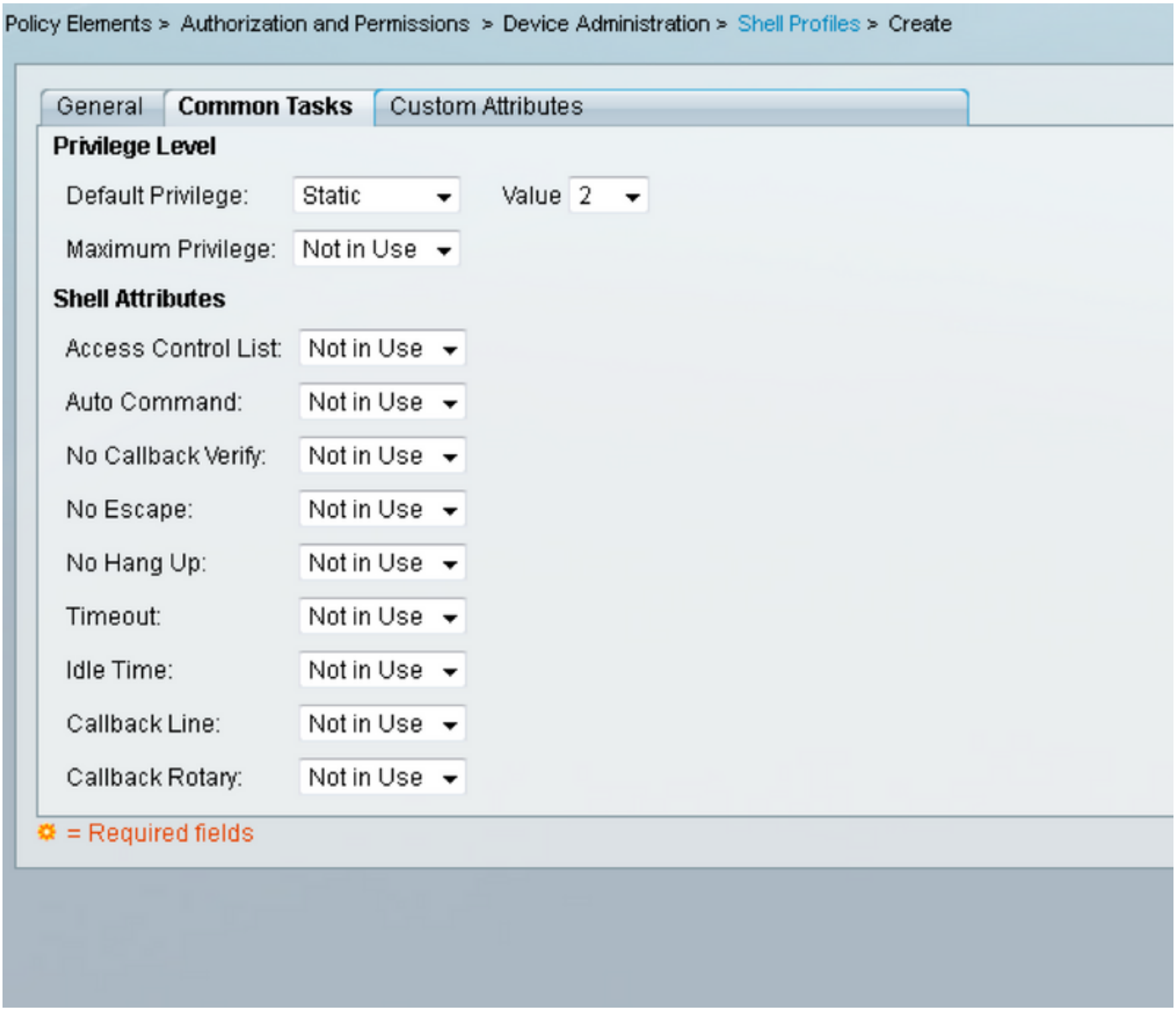
1表示維護使用者。

2表示調配使用者。

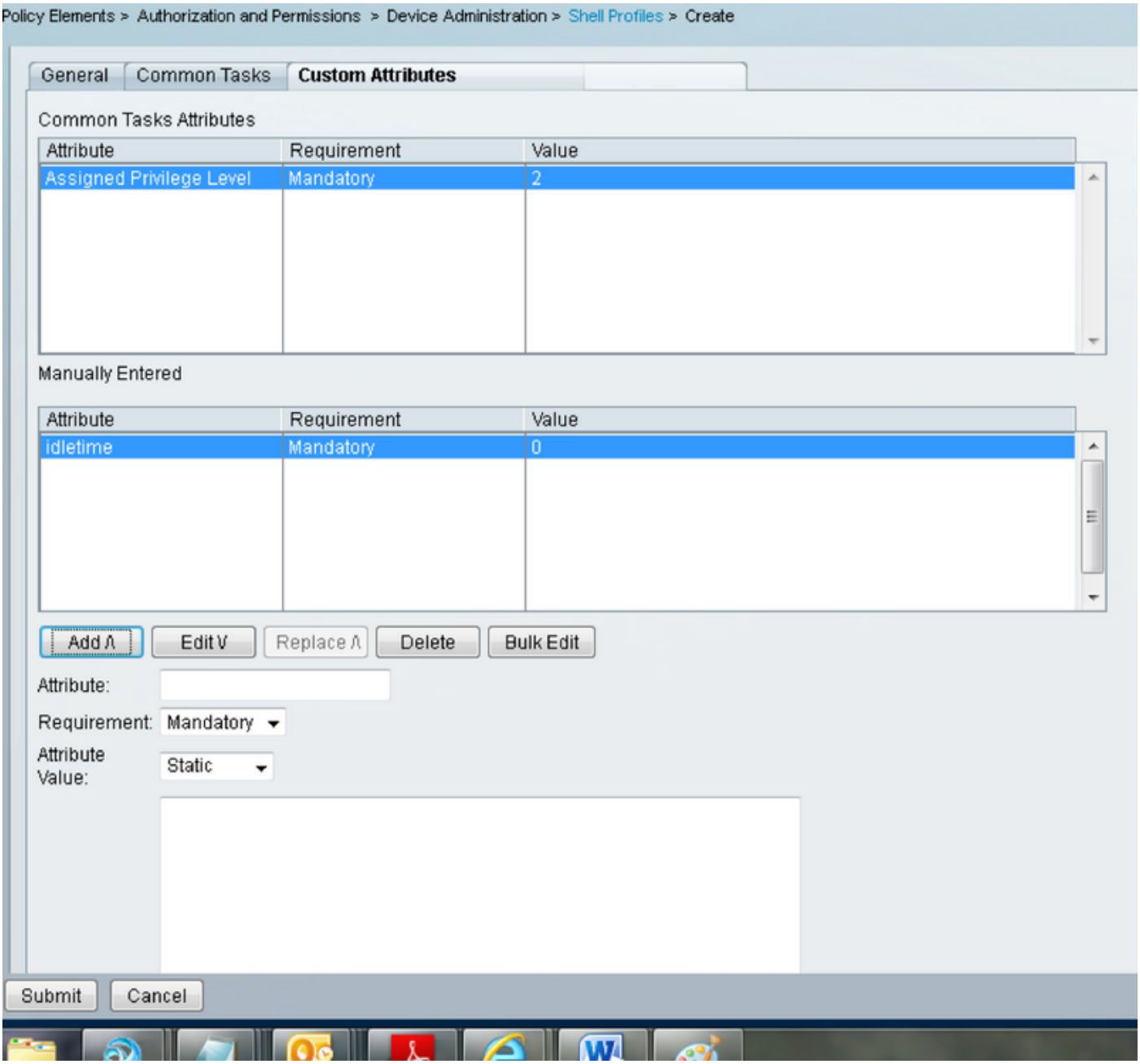
3代表超級使用者。

b.在**Customer Attributes**（客戶屬性）面板中為**Idle Time**（空閒時間）屬性建立自定義屬性。

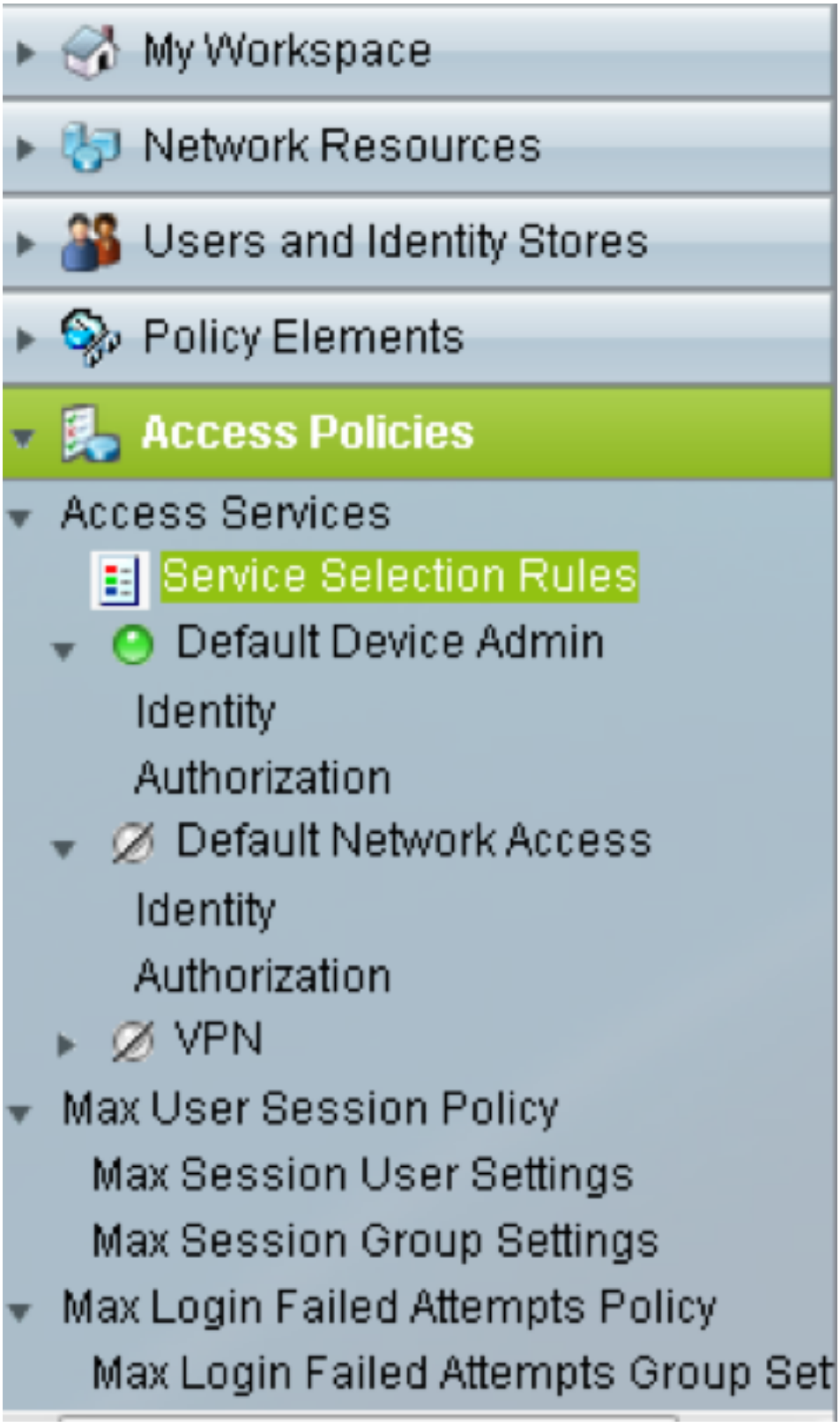

My Workspace
Network Resources
Users and Identity Stores
Policy Elements
Session Conditions
Date and Time
Custom
Network Conditions
End Station Filters
Device Filters
Device Port Filters
Authorization and Permissions
Network Access
Authorization Profiles
Device Administration
Shell Profiles
Command Sets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



Idletime**"0"**表示連線永不過時，且將永久。如果使用者指定任何其他時間，則連線將可用那麼多**秒**。

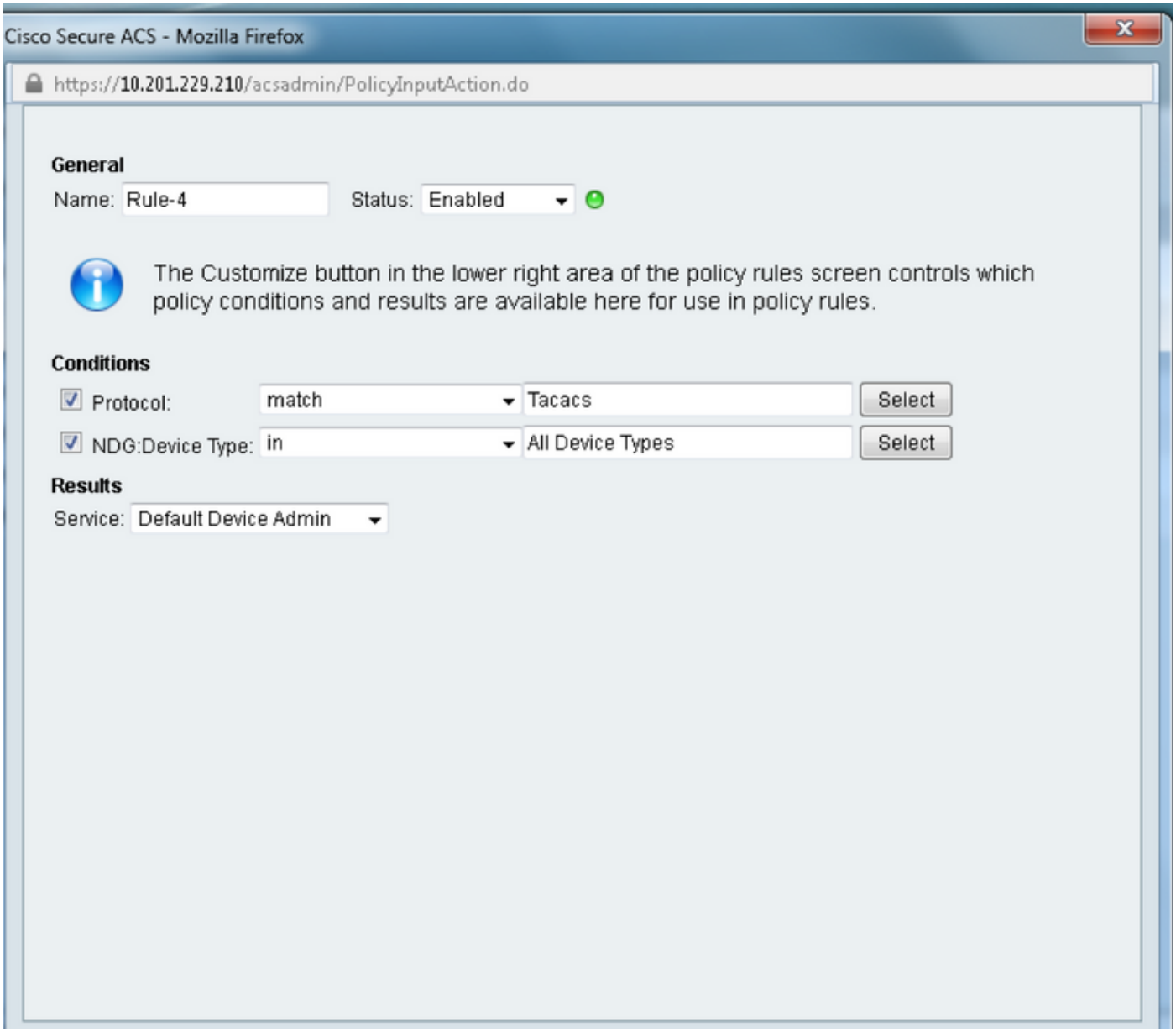


5. 在「訪問策略」面板中**建立訪問**策略：



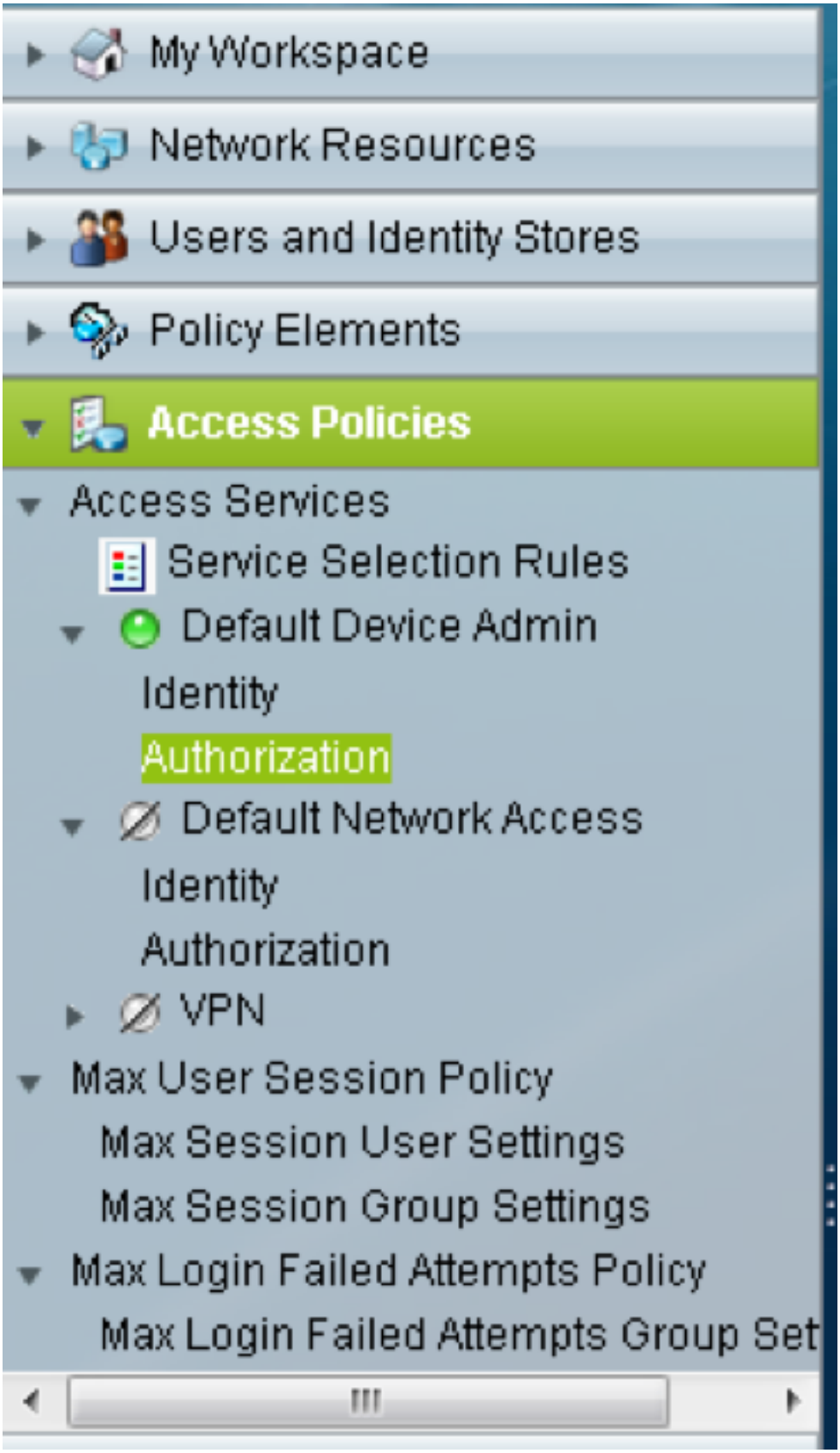
a.按一下**Service Selection Rules**並建立規則：

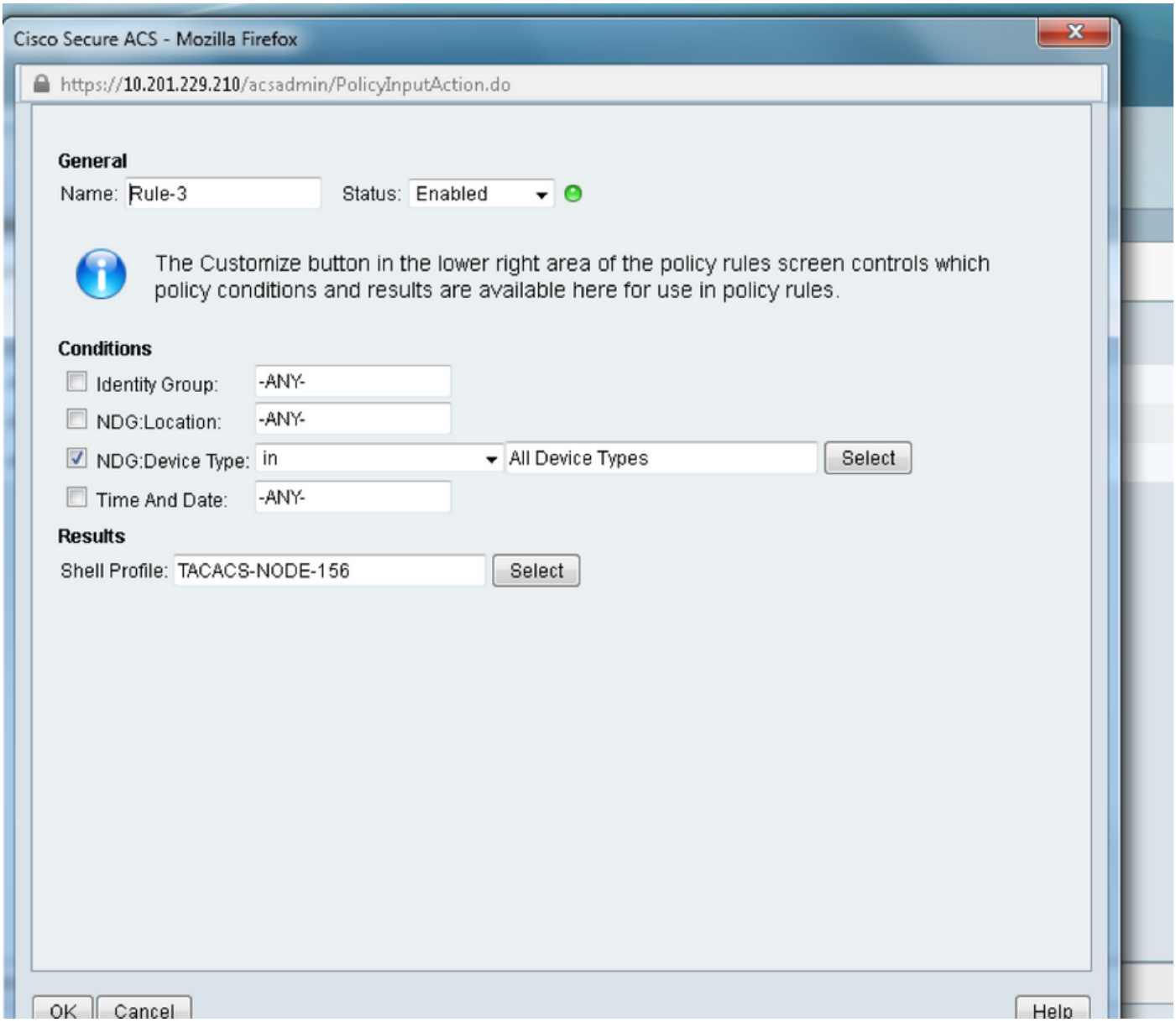
- 選擇TACACS作為協定
- 作為所有裝置或與之前建立的裝置相似的裝置
- 服務型別**Default Device Admin**。



b.在**Default Device Admin**單選按鈕下選擇**Authorization**並建立用於進行授權的規則：

- 選擇**已建立shell**配置檔案
- 選擇特定裝置或裝置型別中的所有裝置


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



驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。