ACSサーバを使用したCisco ONS15454/NCS2000でのTACACS+の設定

内容

概要

このドキュメントでは、ONS15454/NCS2000デバイスおよびCisco Access Control System(ACS)でTerminal Access Controller Access Control System(TACACS+)を設定する手順について説明します。 これらにはすべて例が示されます。このドキュメントで提供されている属性のリストは、すべてを網羅しているわけでも、信頼できるものでもなく、このドキュメントを更新しなければ随時変更される可能性があります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Transport Controller(CTC)GU
- ACSサーバ

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

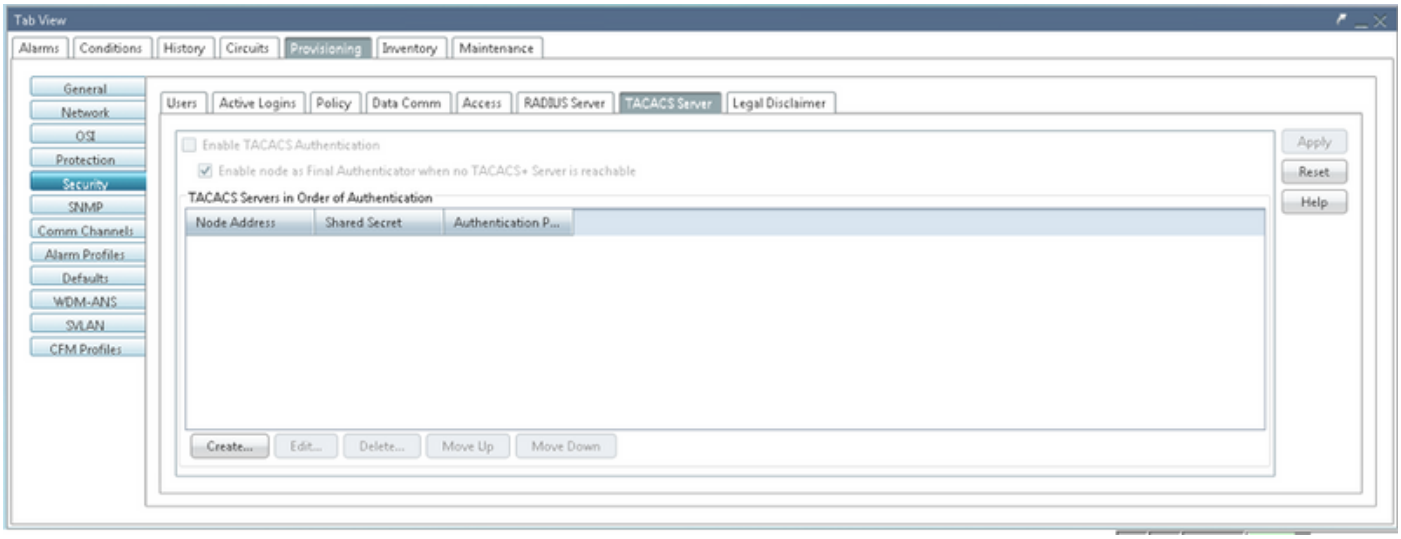
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。

> **注**：本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

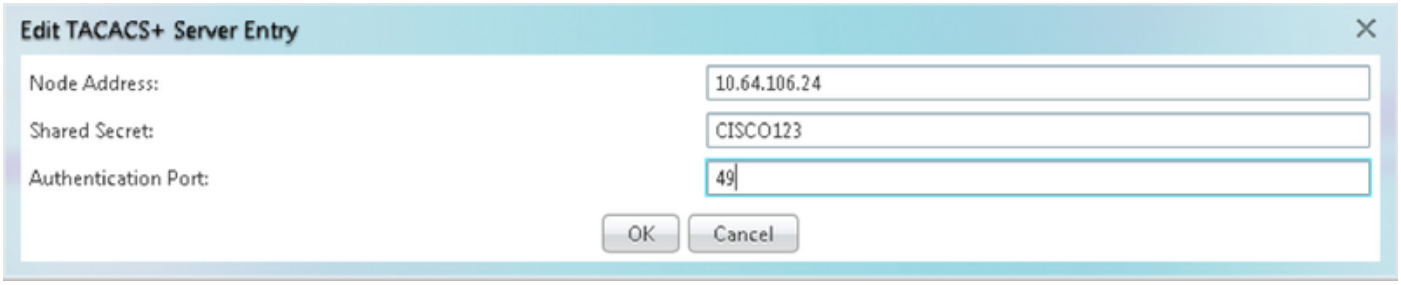
設定

ONS15454/NCS2000で必要な設定：

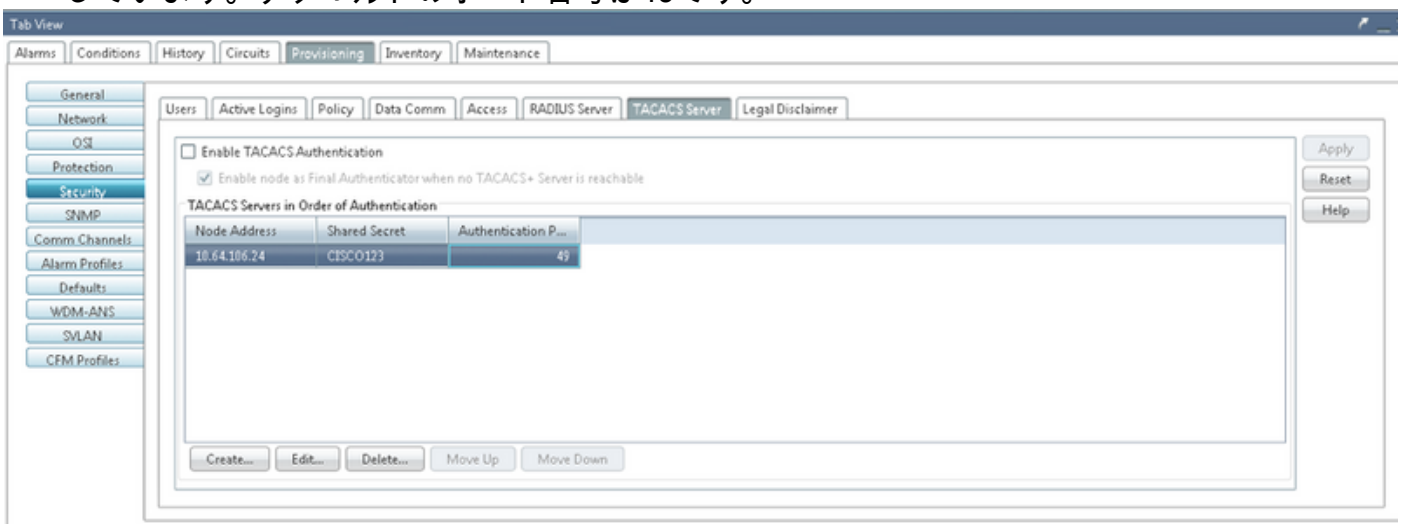
1.このタブからTACACSサーバ設定を設定できます。図に示すように、**[Provisioning] > [Security] > [TACACS Server]に移動します。**



2. TACACS+サーバの詳細を追加するには、[Create]ボタンをクリックします。次の図に示すように、TACACS+設定ウィンドウが開きます。

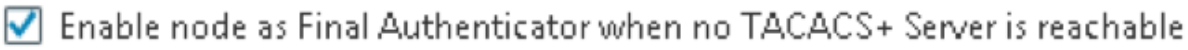


- サーバのIPアドレスを入力します
- ノードとTACACS+サーバ間の共有秘密の追加
- 認証ポート番号を追加します。このポートでは、TACACS+サーバがクライアントをリッスンしています。デフォルトのポート番号は49です。



3. NODEでTACACS+サーバ設定をアクティブにするには、**Enable TACACS Authenticationチェックボックスをオンにして**、図に示すように**Applyボタンをクリック**します。

4.最後のオーセンティケータとしてノードを有効にするには、サーバに到達可能なサーバがない場合、図に示すようにチェックボックスをクリックします。



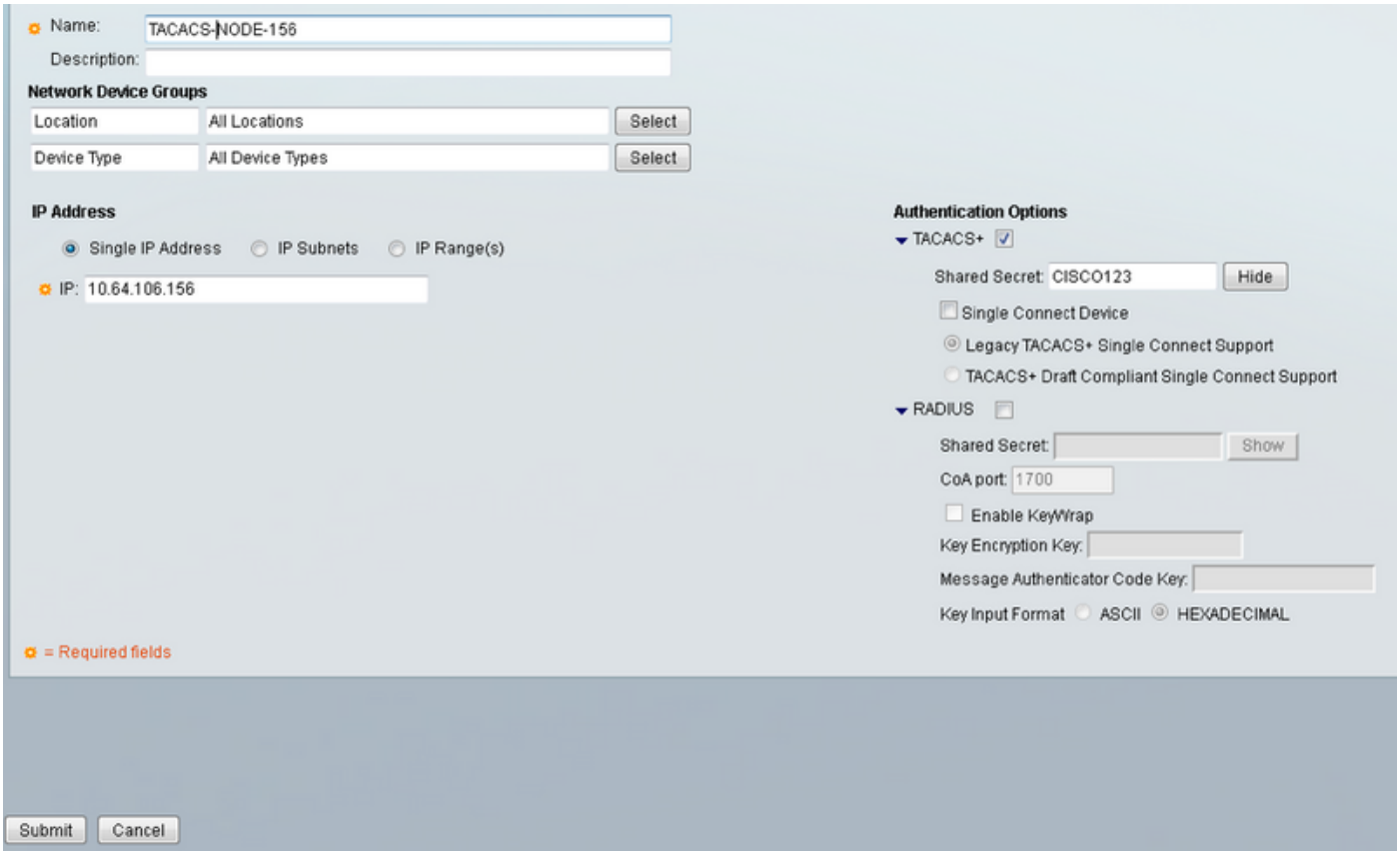
5.特定のサーバ設定を変更するには、対応するサーバ設定行を選択し、[Edit]ボタンをクリックして設定を変更します。

6.特定のサーバ設定を削除するには、対応するサーバ設定行を選択し、[Delete]ボタンをクリックして設定を削除します。

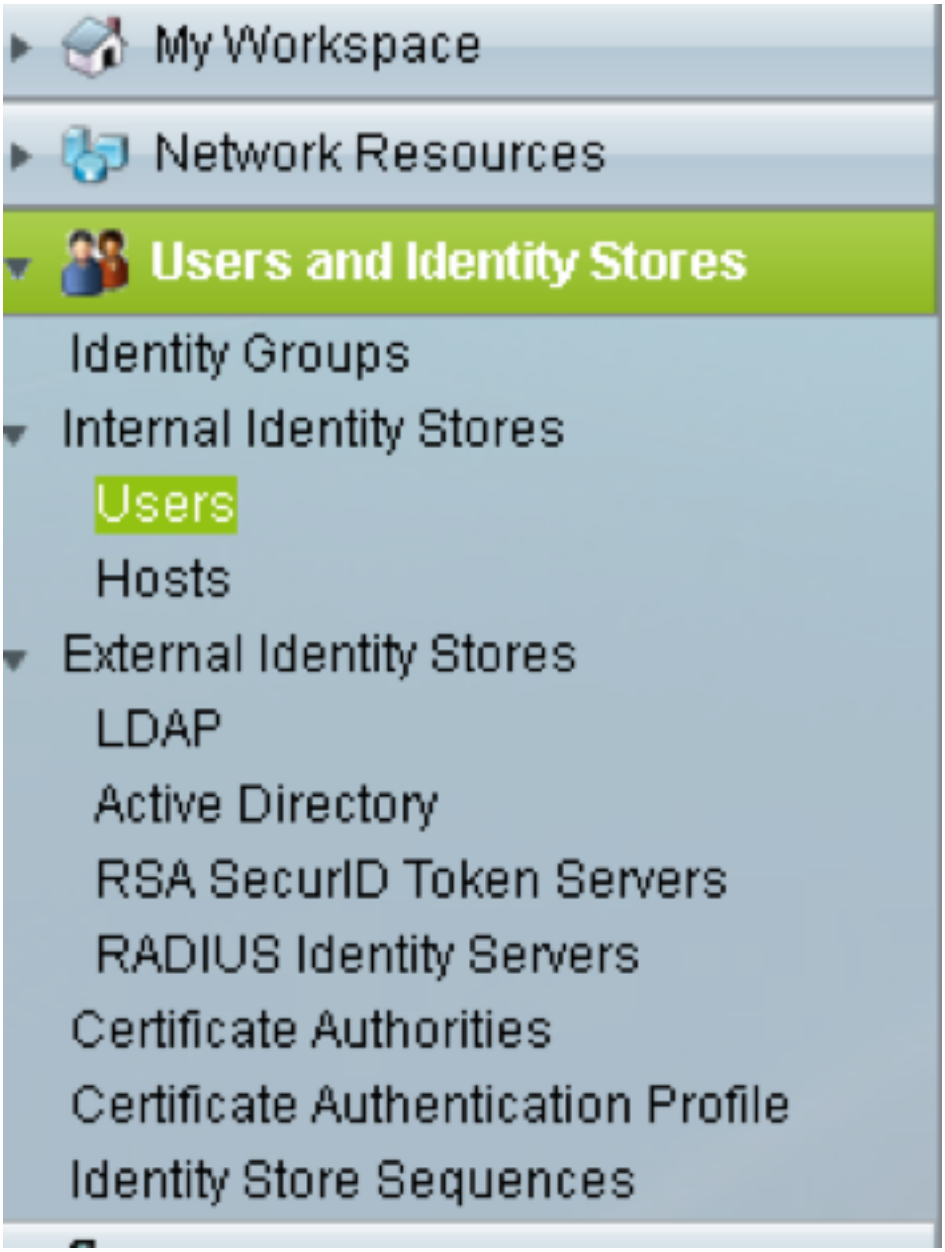
ACSサーバで必要な設定：

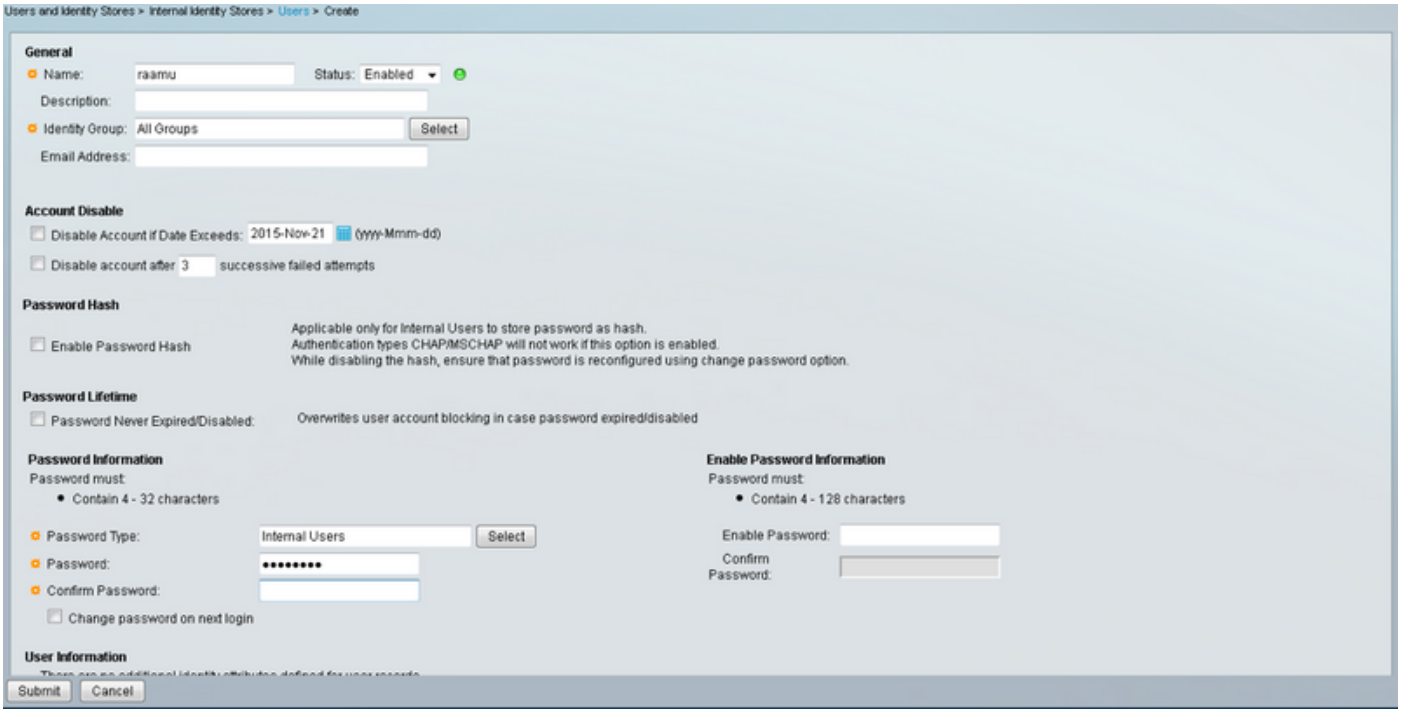
1. ネットワークデバイスとAAAクライアントを作成し、図に示すように[Network Resources]パンの[create]ボタンをクリックします。

2. ONSノード構成で指定したものと同じ共有秘密を指定します。そうしないと、認証に失敗します。



3.図に示すように、[Users and **Identity Stores** Pan]で認証を受けるために必要なユーザのユーザ名とパスワードを作成します。





4. [ポリシー要素]ペインでシェル**プロファイルを**作成します。

a.特権レベル(0 ~ 3)を選択します。

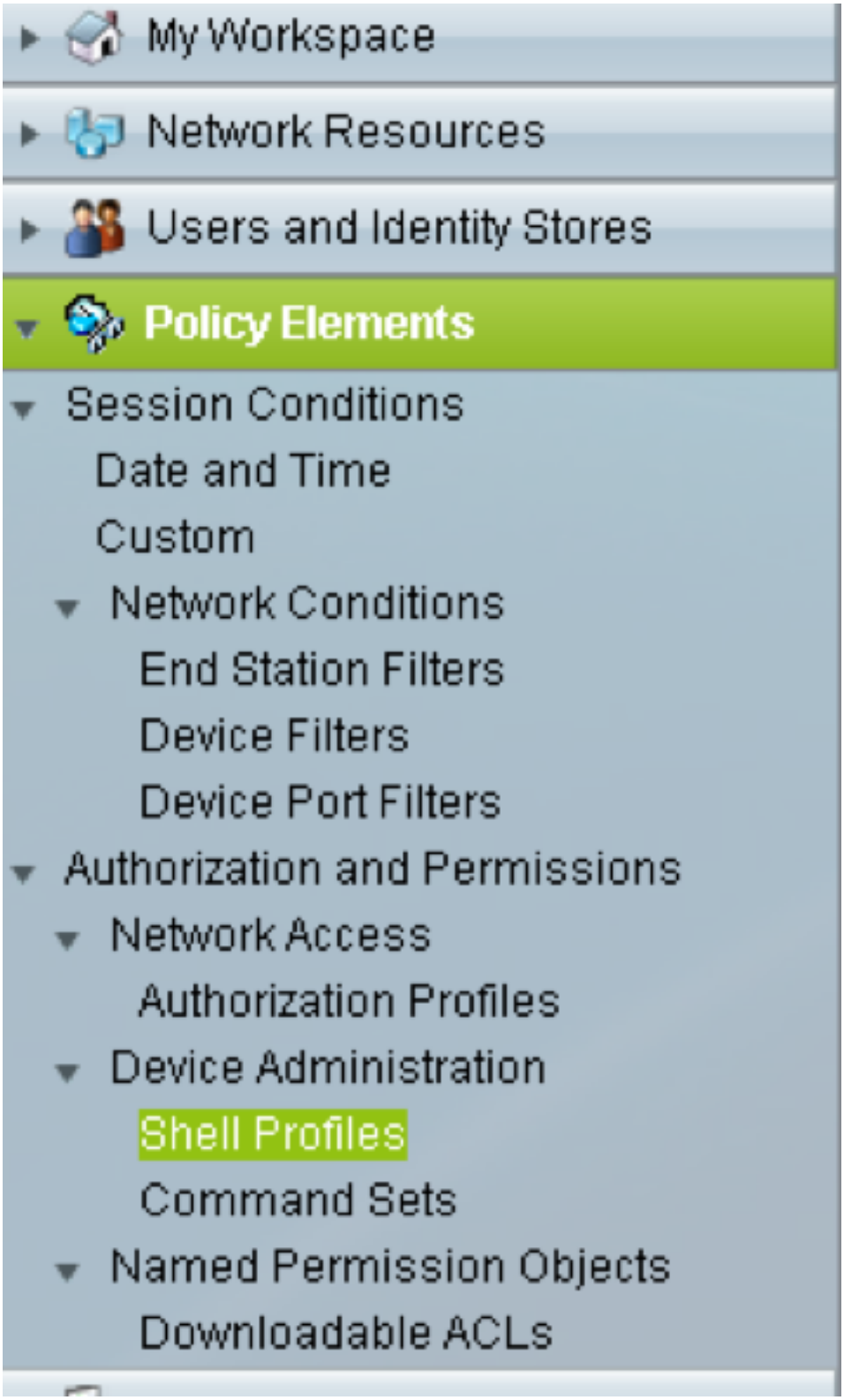
0を指定します。

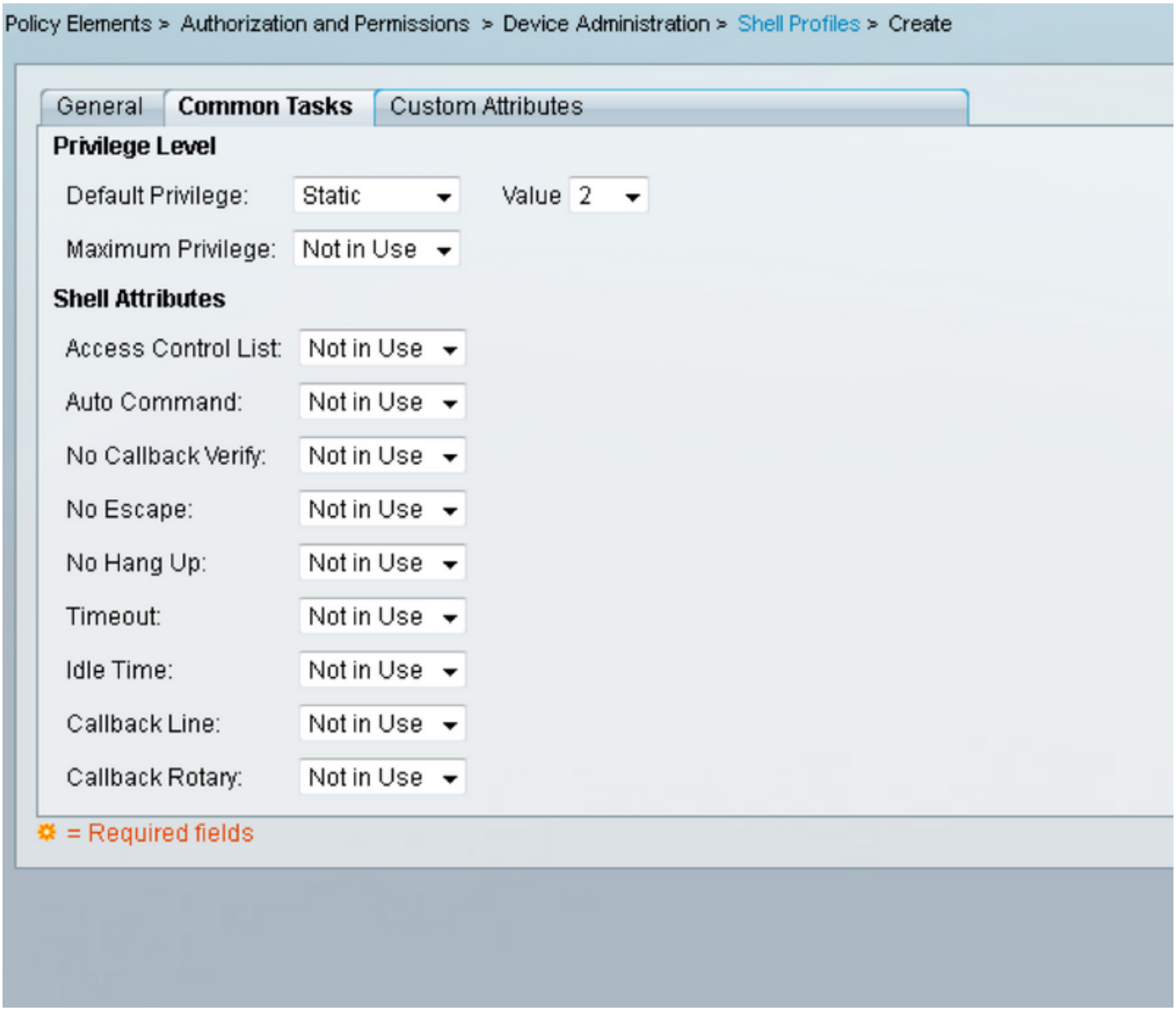
1（メンテナンスユーザ）

2（Provisioningユーザ）。

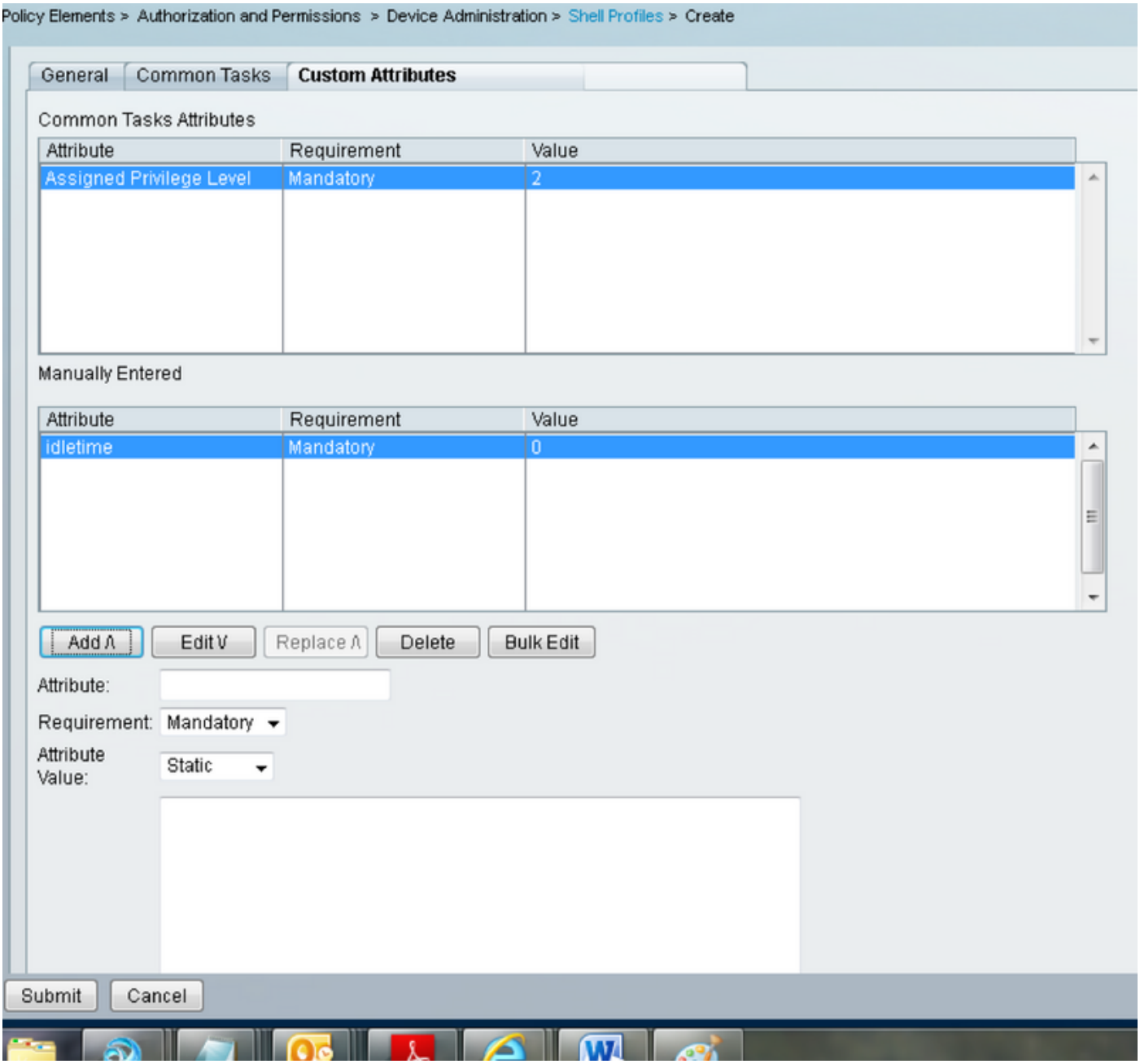
3（スーパーユーザ）

b.[Customer Attributes]パネルの[Idle Time]属性に対するカスタム属性を作成します。

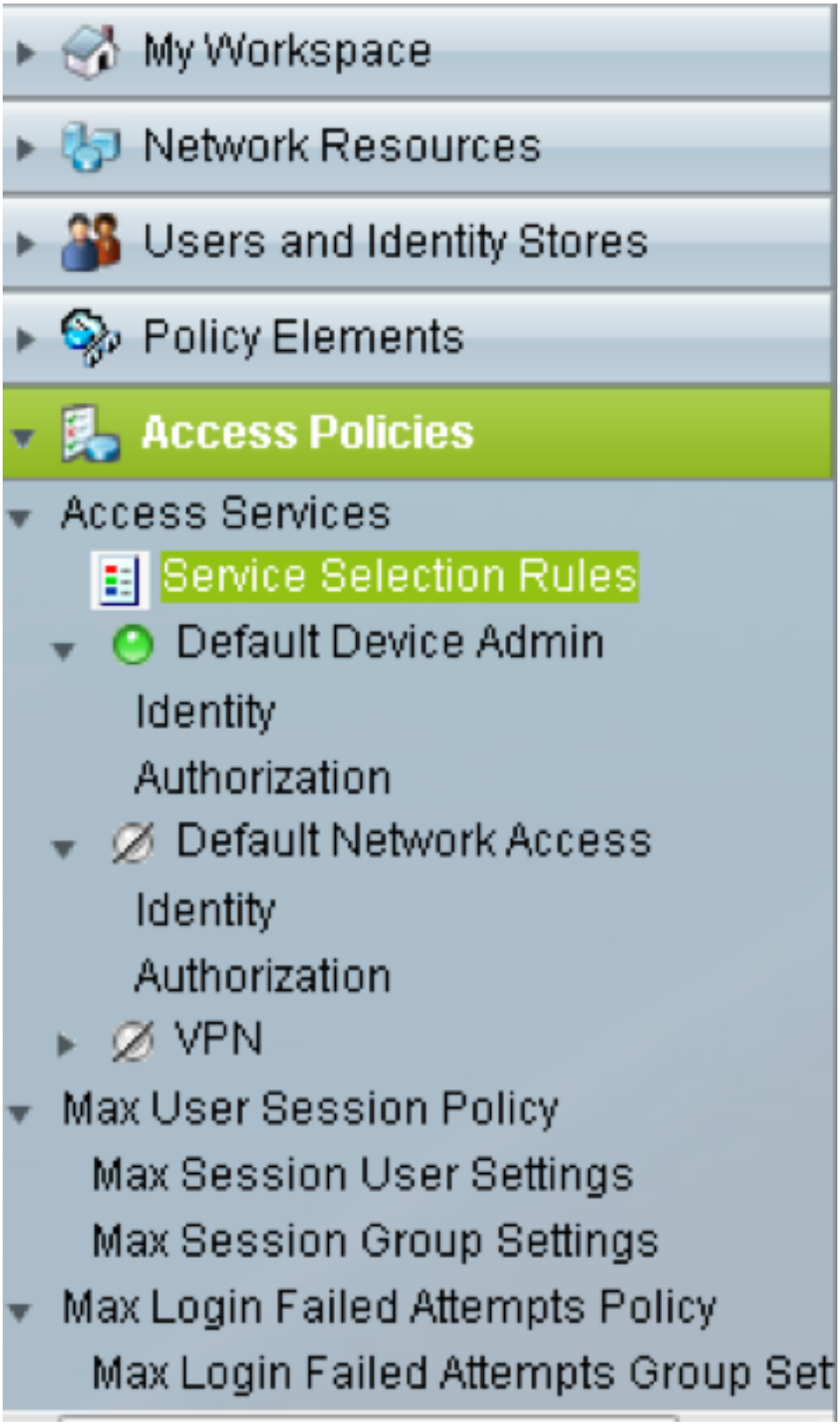




Idletime**"0"は、接続がタイムアウトすることはな**く、永続的であることを示します。ユーザが他の時間を指定した場合、接続はその数秒間利用**できます**。

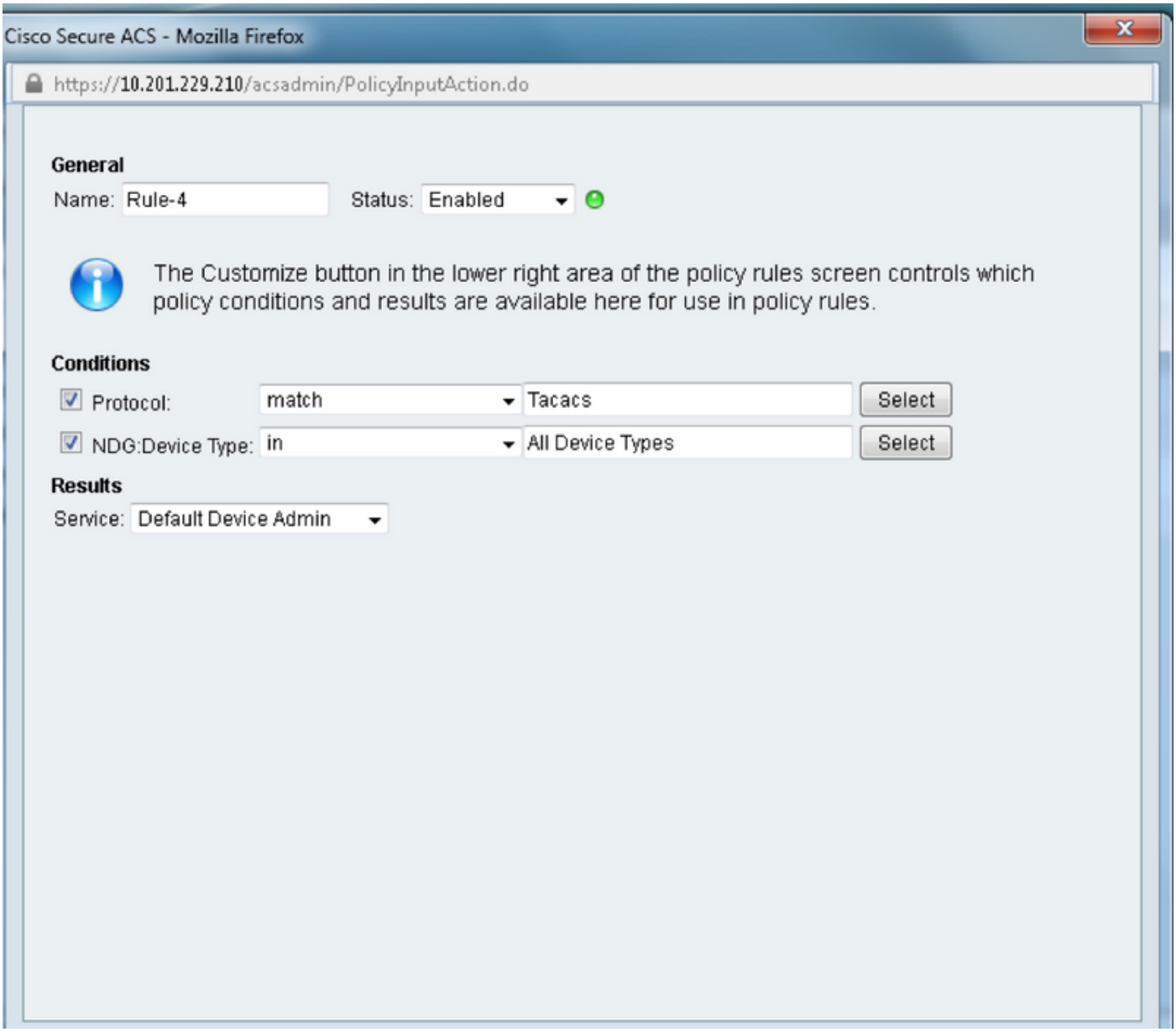


5. [アクセスポリシー]パネルでアクセ**スポリシーを**作成します。



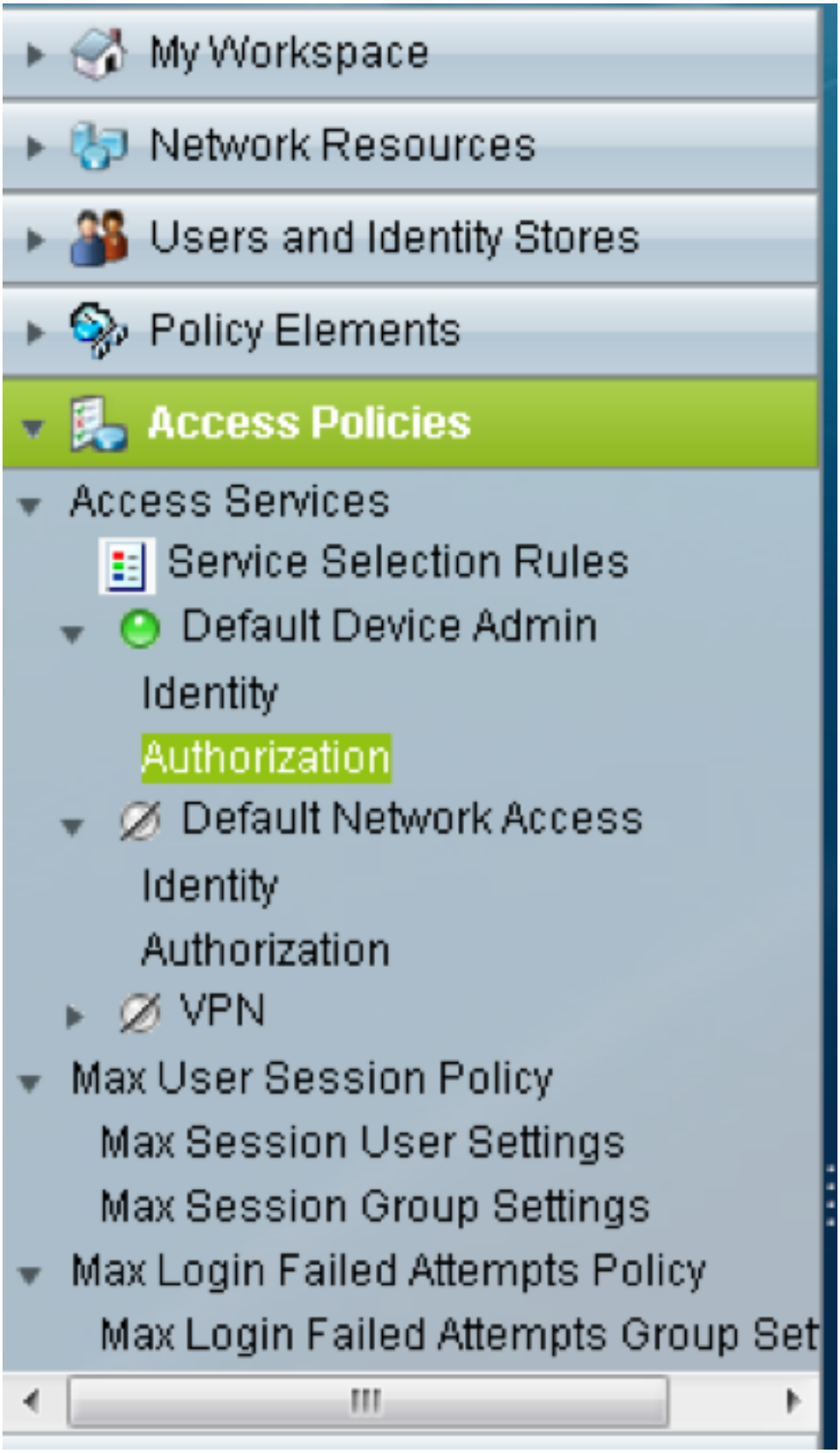
a.[**Service Selection Rules**]**をクリック**し、ルールを作成します。

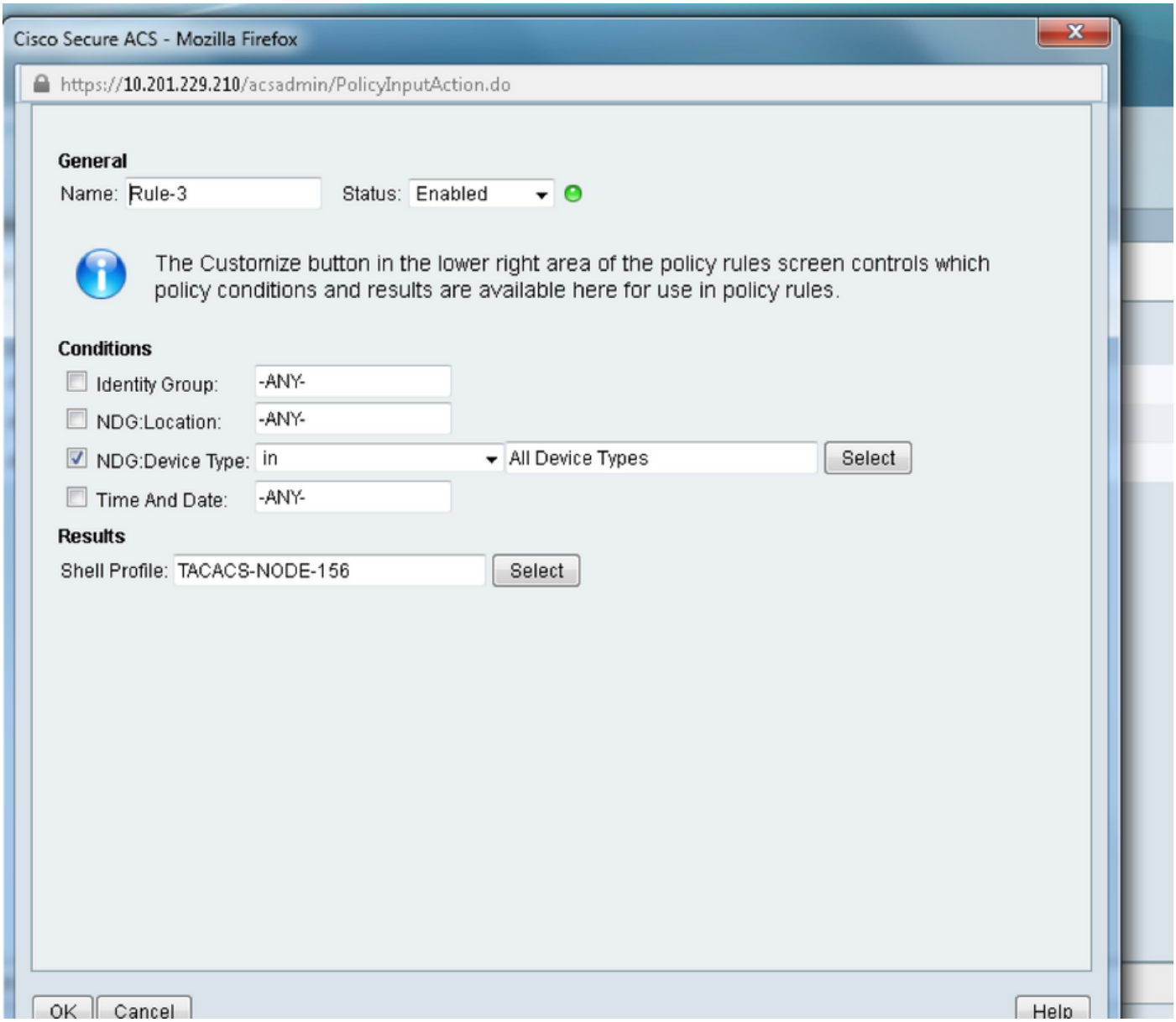
- プロトコルとしてTACACSを選択
- [すべてのデバイス(All device)]または以前に作成したデバイスに類似した特定のデバイス
- デフォルトのデバイス管理と**してのサービスタイプ**。



b.[Authorization]**を選択**し、[**Default Device Admin**]ラジオボタンで許可のルー**ルを作成**します。

- [既に作成さ**れたシェルプロフ**ァイル]を選択
- デバイスタイプ内の特定のデバイスまたはすべてのデバイスを選択します


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



確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。