

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

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

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。

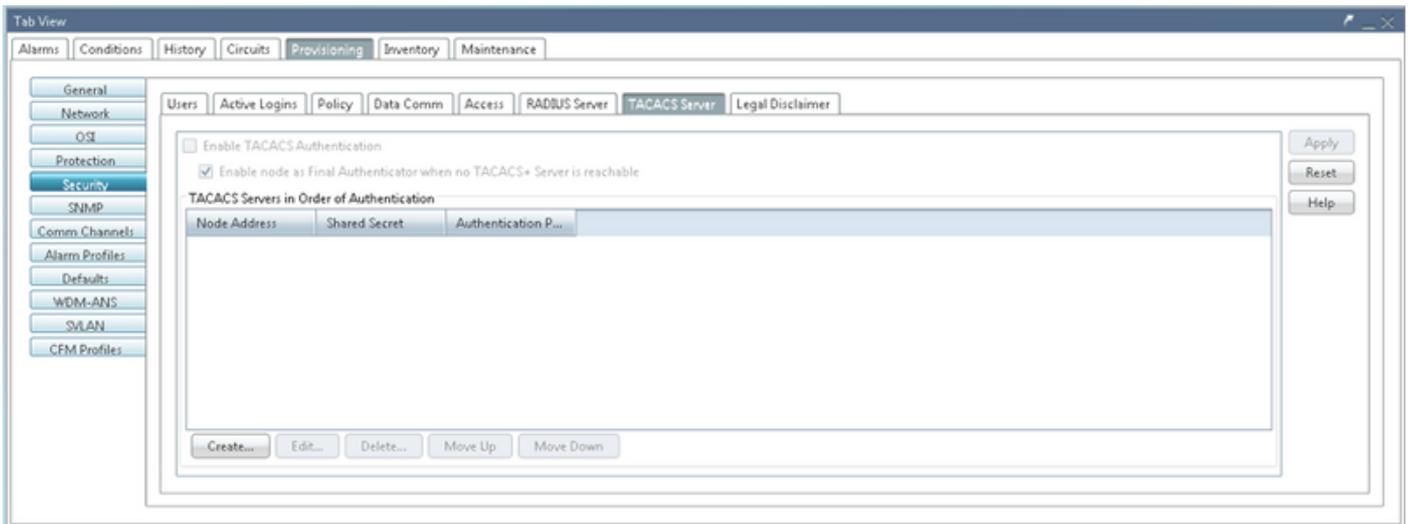
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。

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。

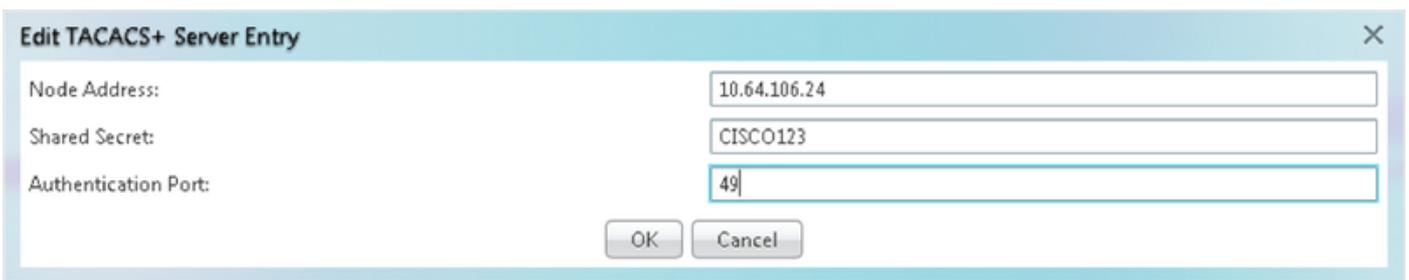
設定

ONS15454/NCS2000で必要な設定：

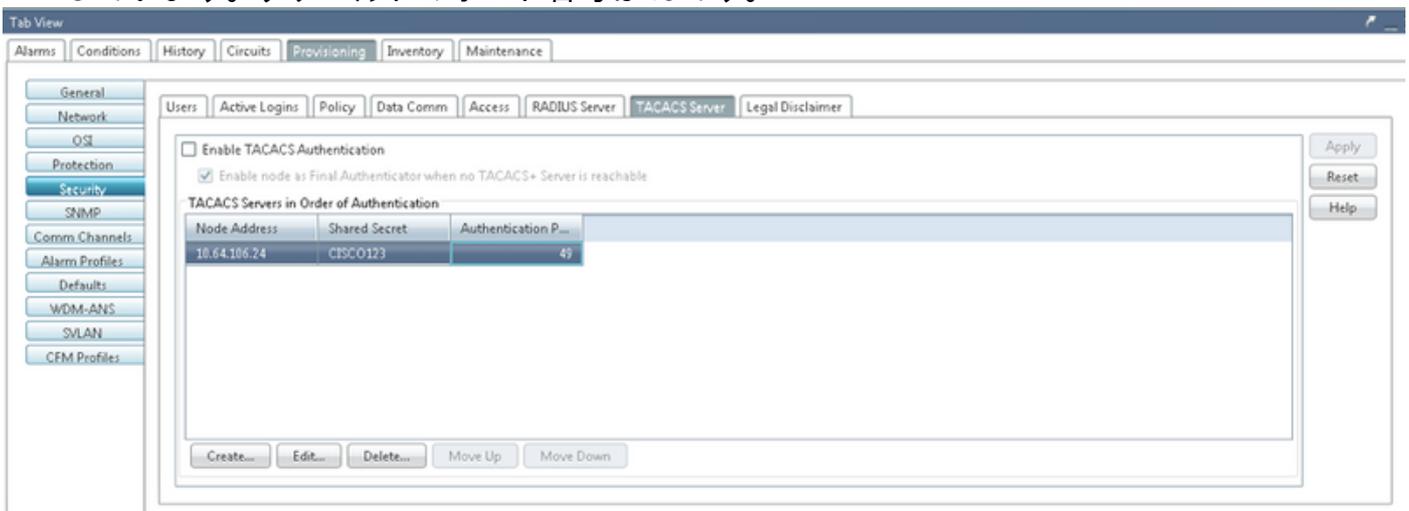
1.このタブからTACACSサーバ設定を設定できます。図に示すように、[Provisioning] > [Security] > [TACACS Server]に移動します。



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。

Enable TACACS Authentication

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。

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

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サーバに必要な設定：

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。



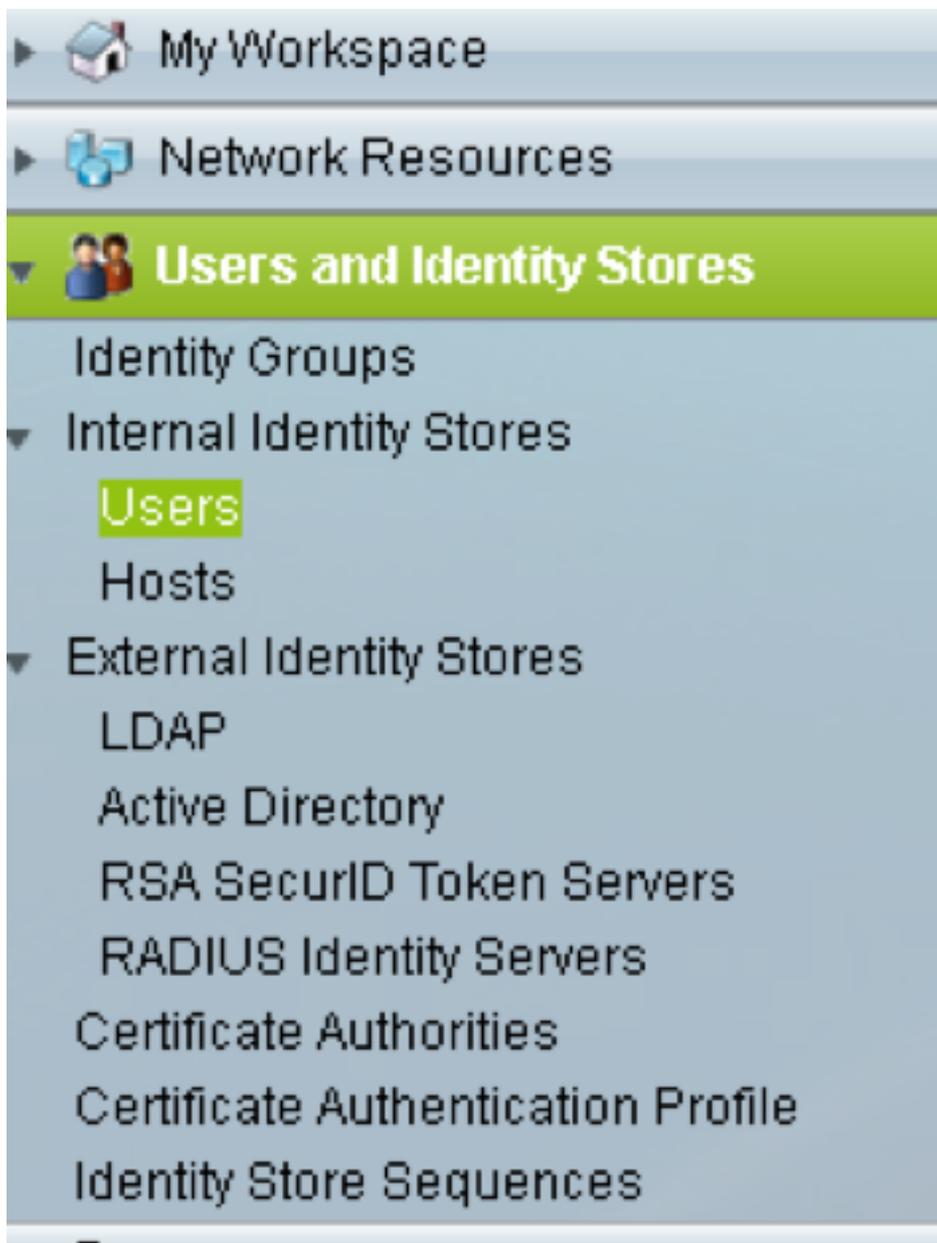
2. ONSノード構成で指定したものと同一共有秘密を指定します。そうしないと、認証に失敗します。

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.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。



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. [ポリシー要素]ペインでシエ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。

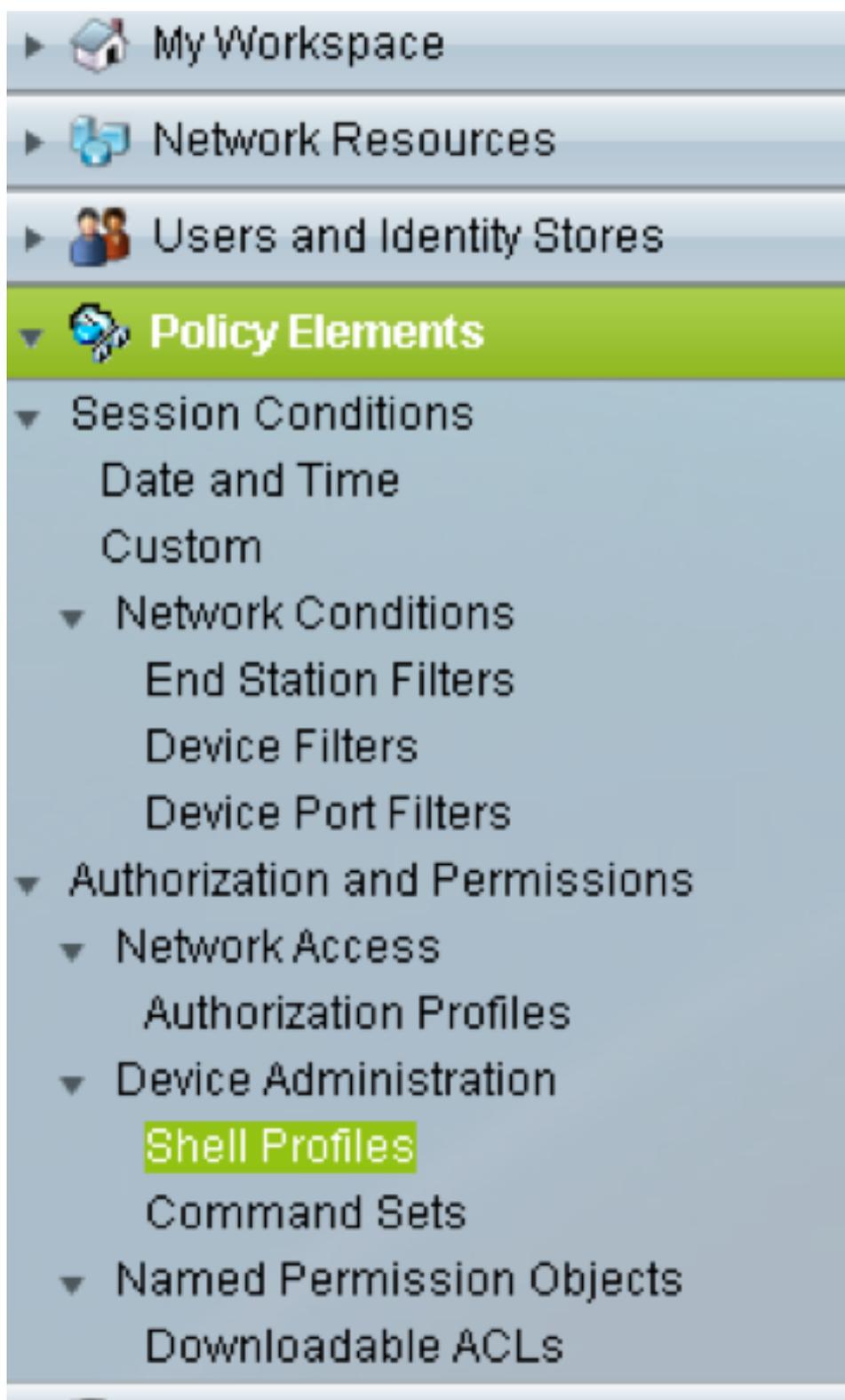
0を指定します。

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。



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" is not a timeout, it indicates that the connection is persistent. If a user specifies a time, the connection can be used for a few seconds.

General Common Tasks **Custom Attributes**

Common Tasks Attributes

Attribute	Requirement	Value
Assigned Privilege Level	Mandatory	2

Manually Entered

Attribute	Requirement	Value
idletime	Mandatory	0

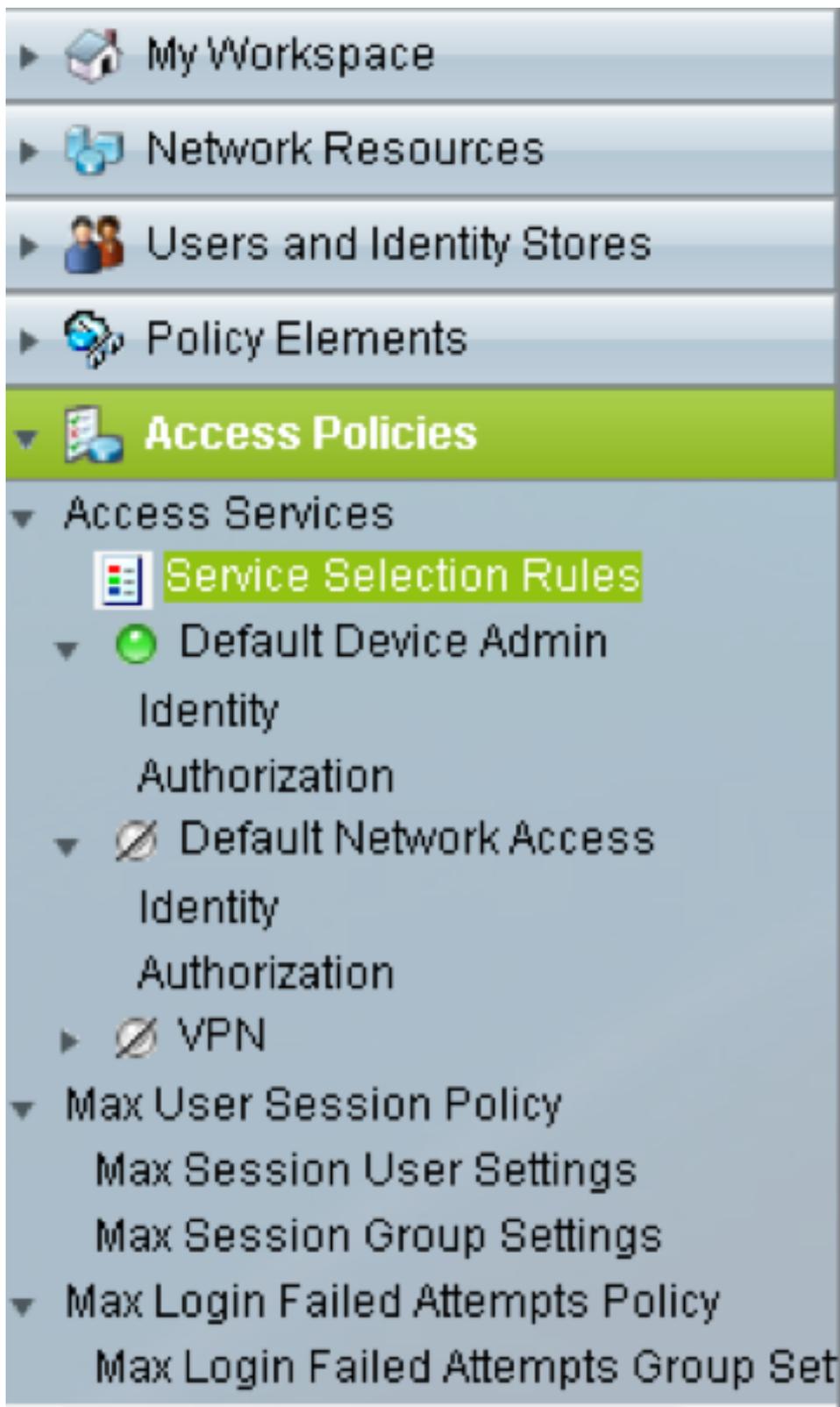
Attribute:

Requirement: Mandatory ▾

Attribute Value: Static ▾



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。

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

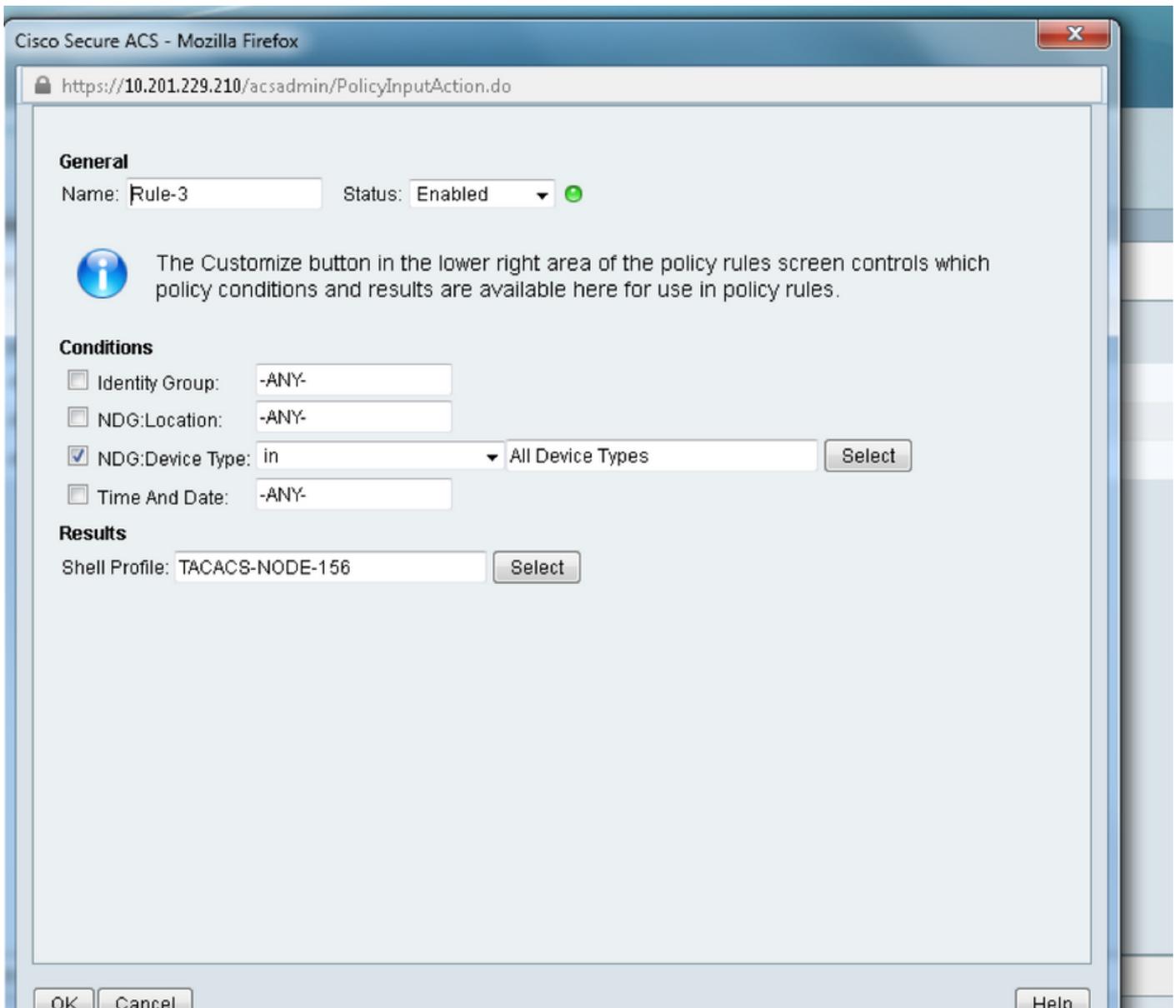
Service: Default Device Admin

b.[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フファイル]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

◀ [Progress Bar] ▶



確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

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はありません。