

使用ACS服务器在Cisco ONS15454/NCS2000上配置TACACS+

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何在ONS15454/NCS2000设备和思科访问控制系统(ACS)上配置终端访问控制器访问控制系统(TACACS+)的分步说明。所有主题都包括示例。本文档中提供的属性列表并非详尽或权威，在不更新本文档的情况下随时可能更改。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科传输控制器(CTC)GU
- ACS服务器

使用的组件

本文档不限于特定的软件和硬件版本。

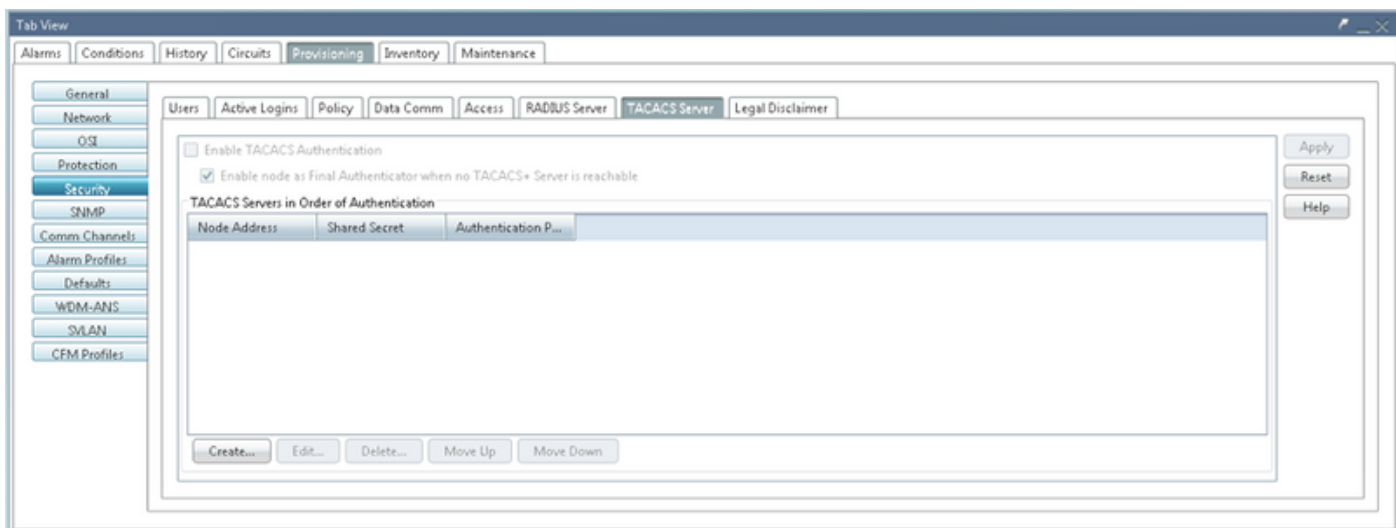
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。

注意：如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

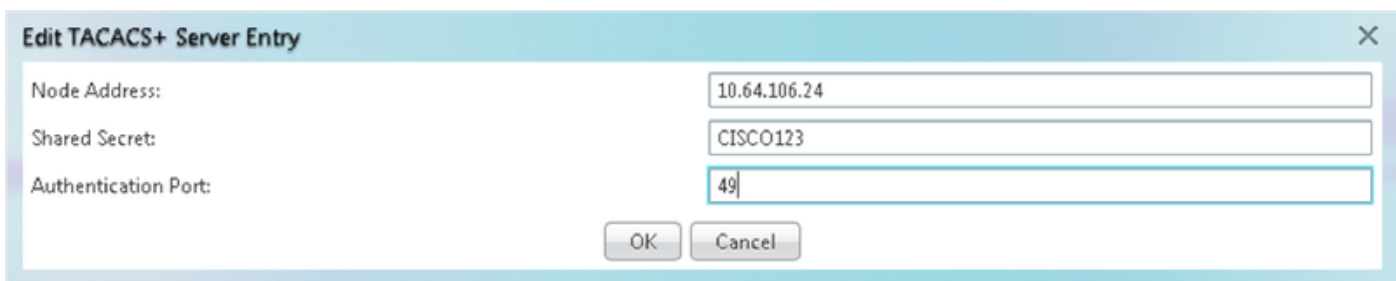
配置

ONS15454/NCS2000所需的配置：

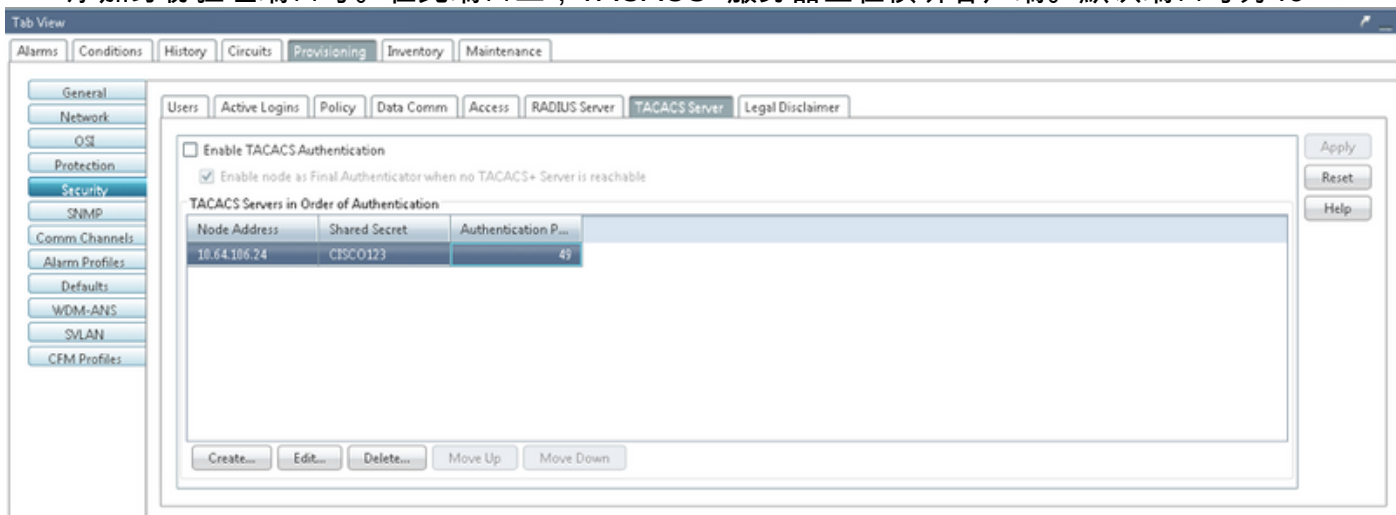
1.您可以从此选项卡配置TACACS服务器配置。导航至Provisioning > Security > TACACS Server，如图所示。



2.要添加TACACS+服务器详细信息，请单击“创建”按钮。它将打开TACACS+配置窗口，如下图所示。



- 输入服务器IP地址
- 在节点和TACACS+服务器之间添加共享密钥
- 添加身份验证端口号。在此端口上，TACACS+服务器正在侦听客户端。默认端口号为49



3.要激活NODE上的TACACS+服务器配置，请选中启用TACACS身份验证复选框，然后单击应用按钮，如图所示。

Enable TACACS Authentication

4.要启用节点作为最终身份验证器，当无法访问任何服务器时，请点击图像所示的复选框。

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

5.要修改特定服务器配置，请选择相应的服务器配置行，单击“编辑”按钮以修改配置。

6.要删除特定服务器配置，请选择相应的服务器配置行，单击“删除”按钮以删除配置。

ACS服务器上所需的配置：

1. 创建网络设备和AAA客户端，然后单击**Network Resources**（网络资源）窗格中的**Create**按钮，如图所示。



2. 提供与ONS节点配置中给定的相同的共享密钥。否则，身份验证将失败。

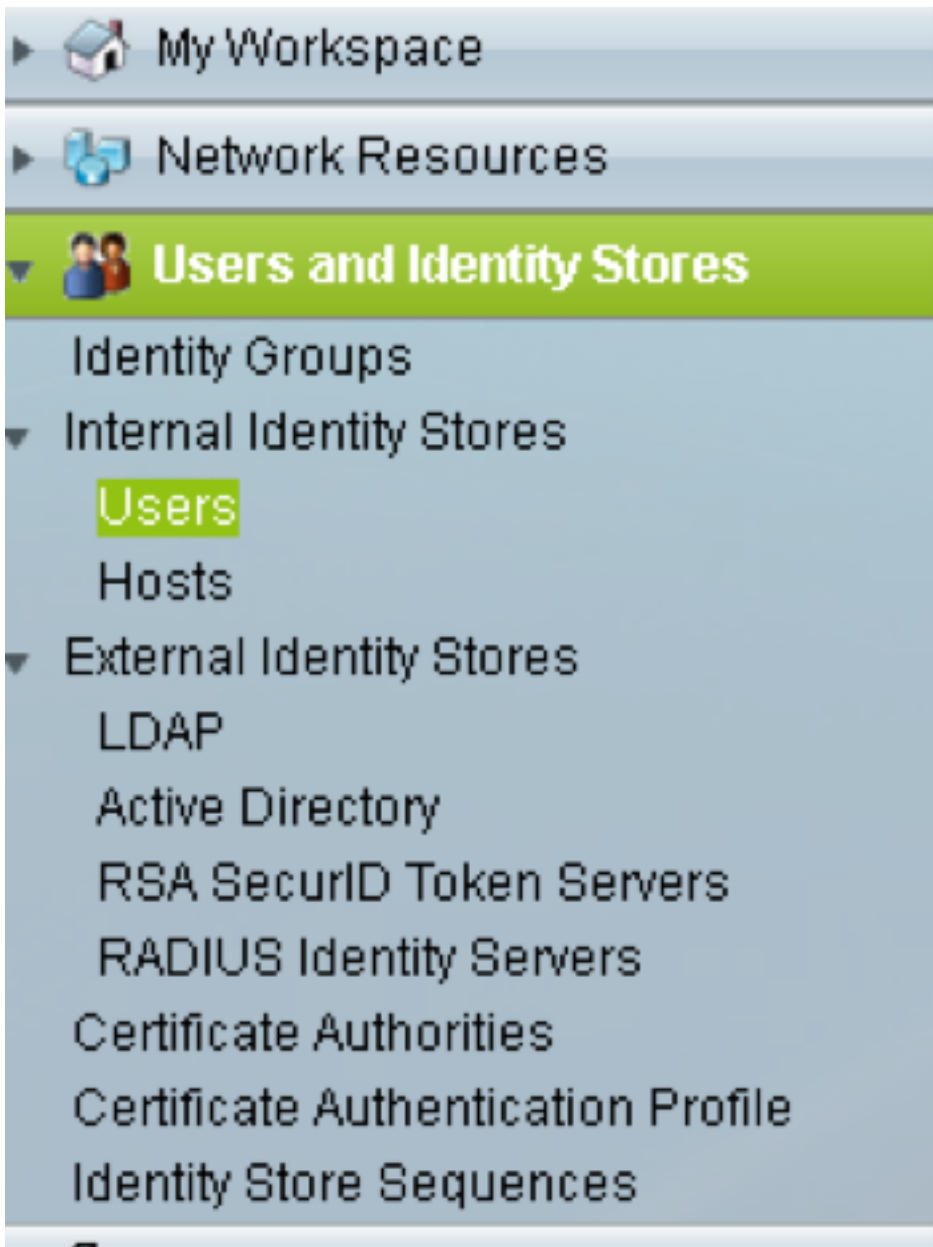
Network Device Groups
Location:
Device Type:

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

= Required fields

3.如图所示，在“用户和身份库”Pan中为需要通过身份验证的用户创建用户名和密码。



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. 在“策略元素”(Policy Elements)窗格中创建外壳配置文件：

a.选择权限级别（0到3）：

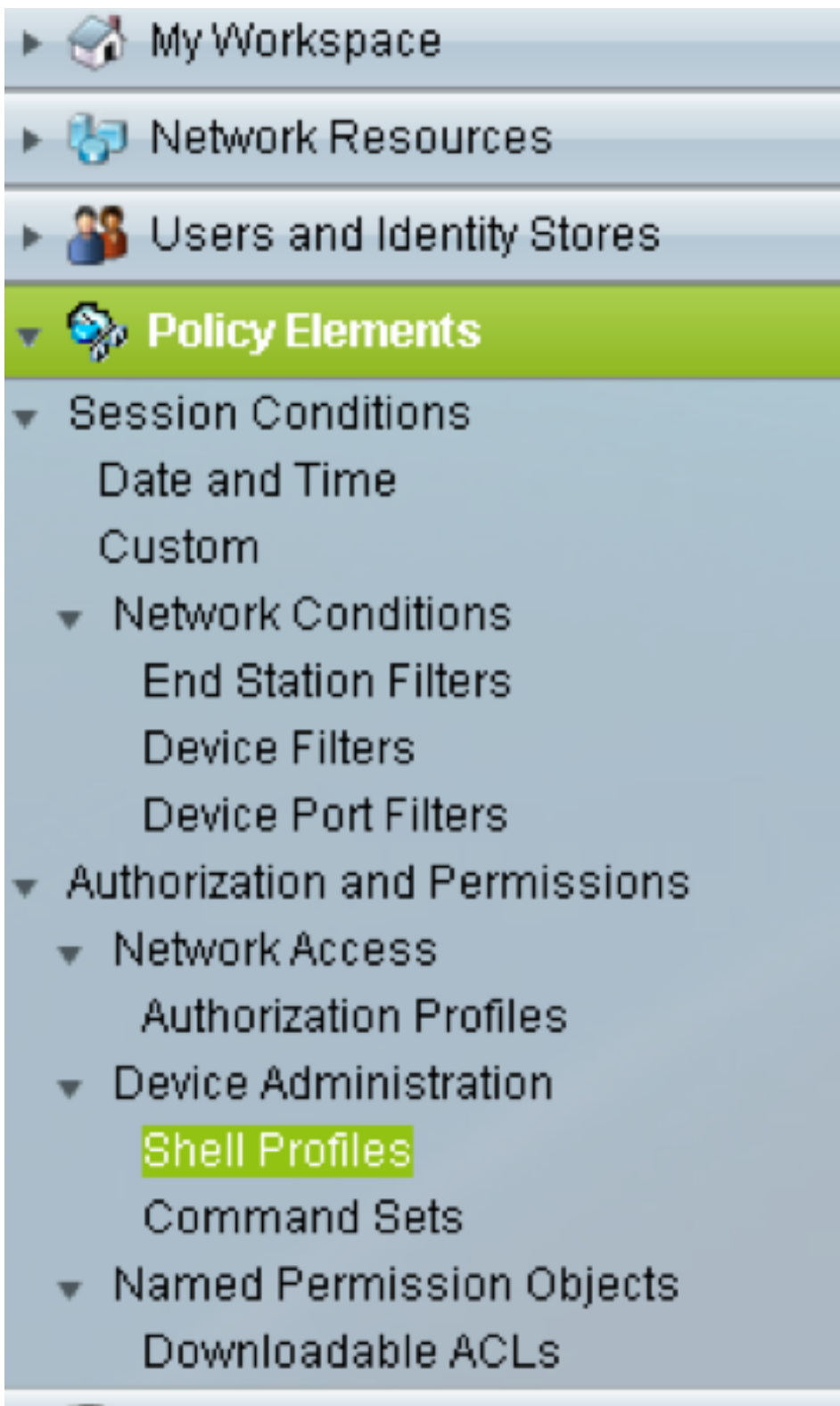
0，用于检索用户。

1用于维护用户。

2用于调配用户。

3（超级用户）。

b.在“客户属性”面板中为“空闲时间”属性创建自定义属性。



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

空闲时间“0”表示连接永不超时，并且将永远超时。如果用户指定任何其他时间，则连接将可用这么多秒。

General Common Tasks **Custom Attributes**

Common Tasks Attributes

Attribute	Requirement	Value
Assigned Privilege Level	Mandatory	2


Manually Entered

Attribute	Requirement	Value
idletime	Mandatory	0

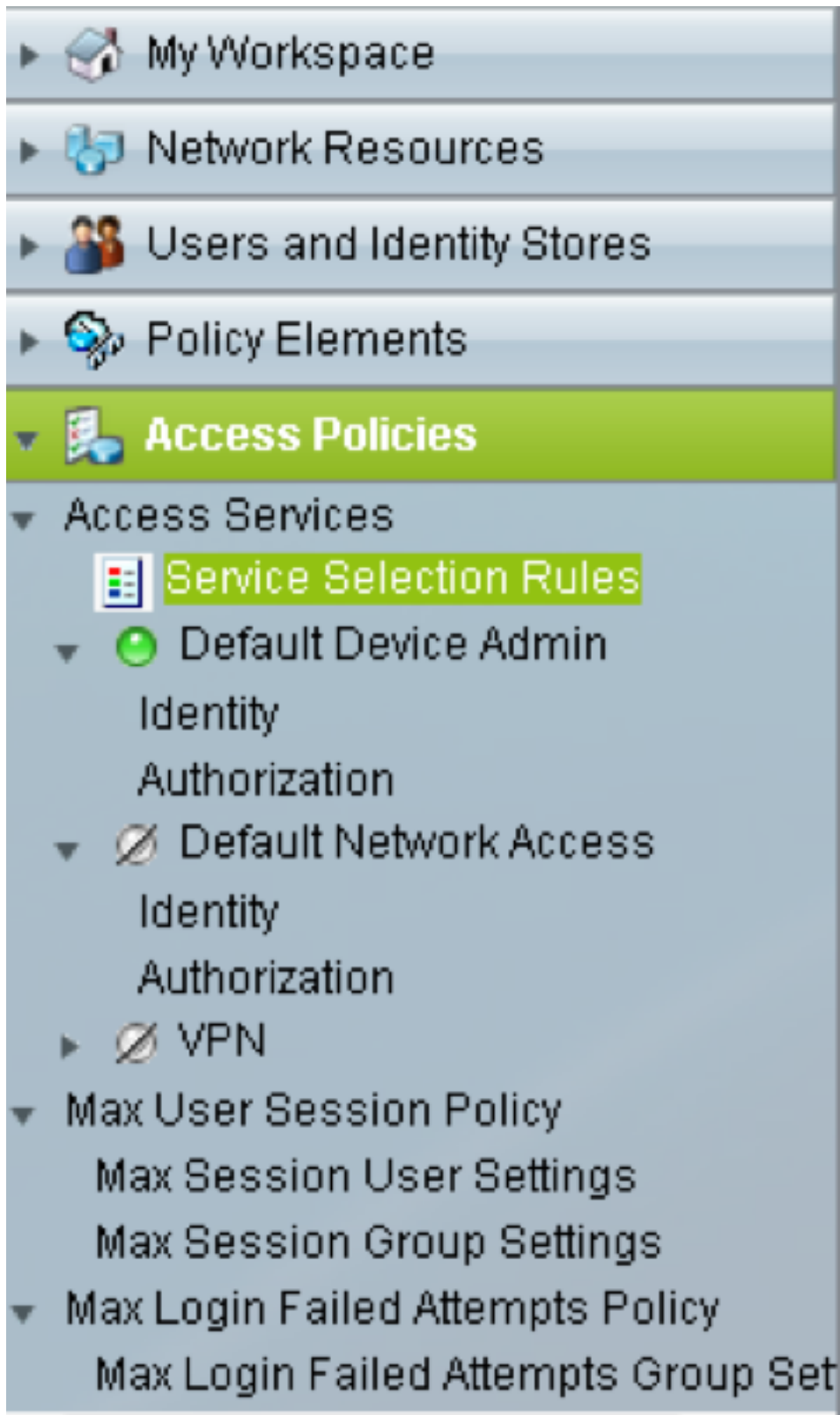
Attribute:

Requirement: Mandatory ▾

Attribute Value: Static ▾

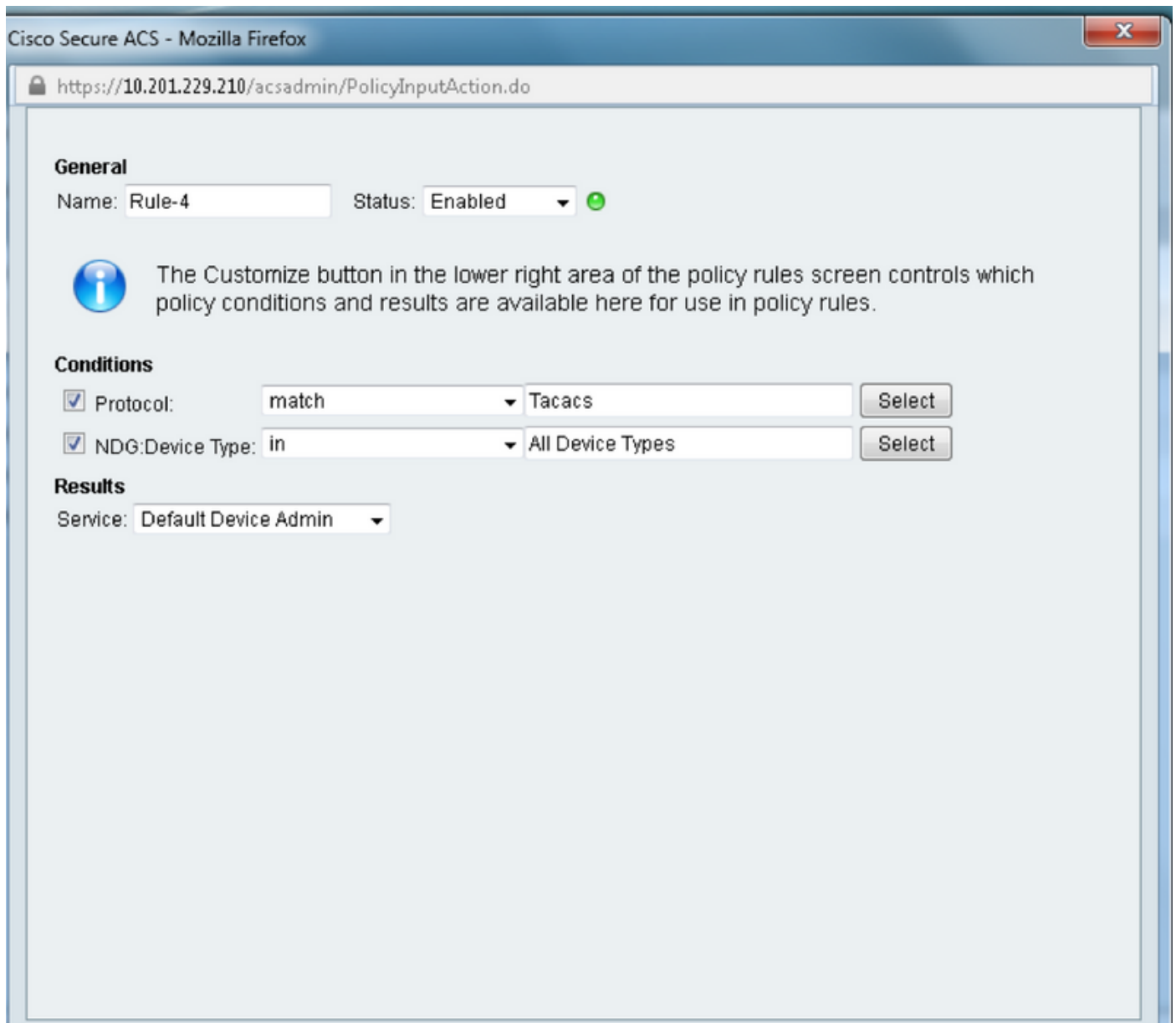


5. 在“访问策略”面板中**创建访问策略**：












a. 单击“服务选择规则”并创建规则：

- 选择TACACS作为协议
- 设备为All设备或与之前创建的设备类似的特定设备
- 服务类型为**Default Device Admin**。

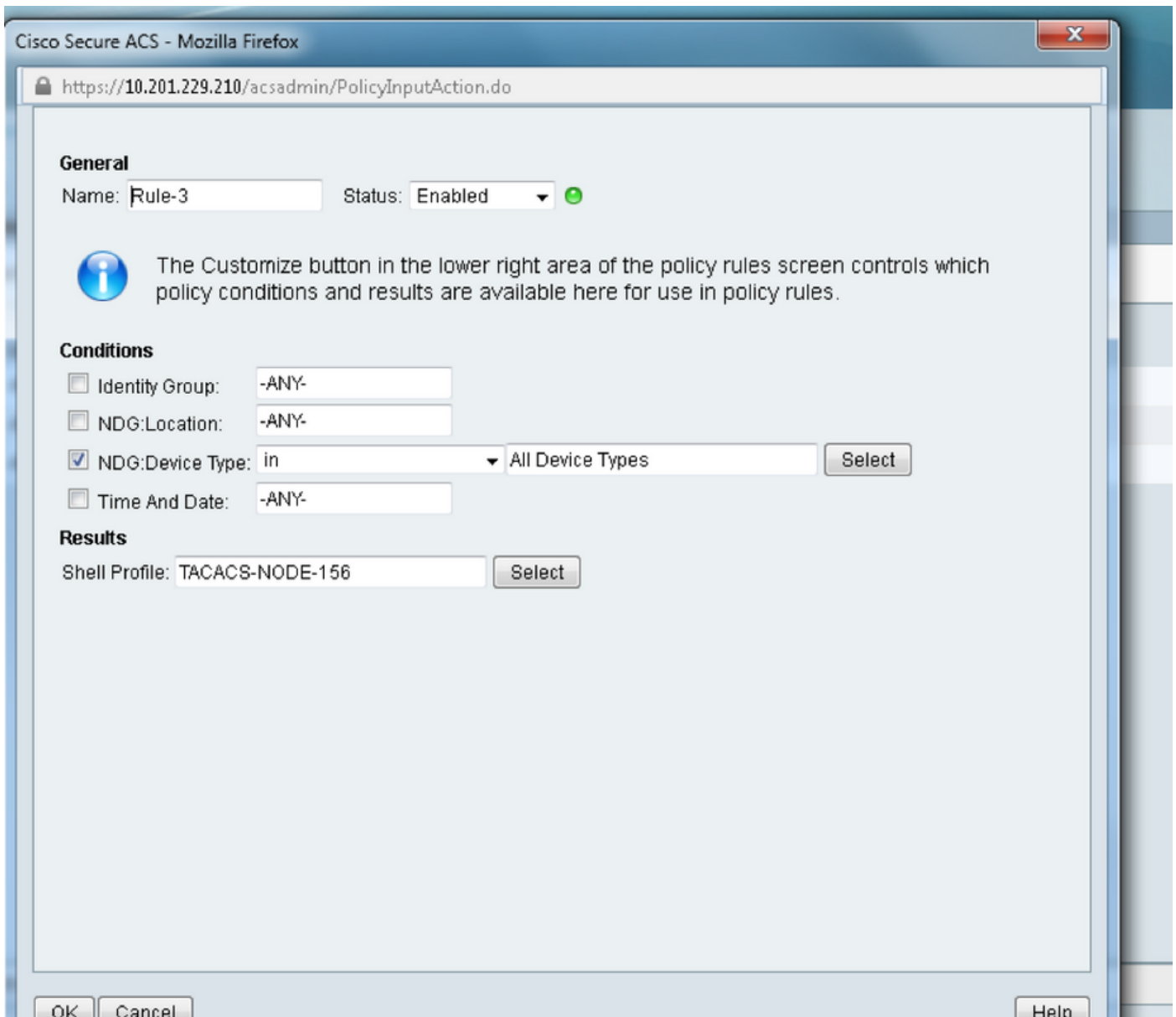


b.选择Authorization并在Default Device Admin单选按钮下创建用于授权的规则：

- 选择“已创建的亮配置文件”
- 选择特定设备或设备类型中的所有设备

- ▶  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] ▶



验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。