

# Configure TACACS+ on Cisco ONS15454/NCS2000 with ACS Server

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

## Introduction

This document describes step-by-step instructions on how to configure Terminal Access Controller Access Control System (TACACS+) on ONS15454/NCS2000 devices and Cisco Access Control System (ACS). All topics include examples. The list of attributes provided in this document is not exhaustive or authoritative and might change at any time without an update to this document.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Transport Controller (CTC) GU
- ACS Server

### Components Used

This document is not restricted to specific software and hardware versions.

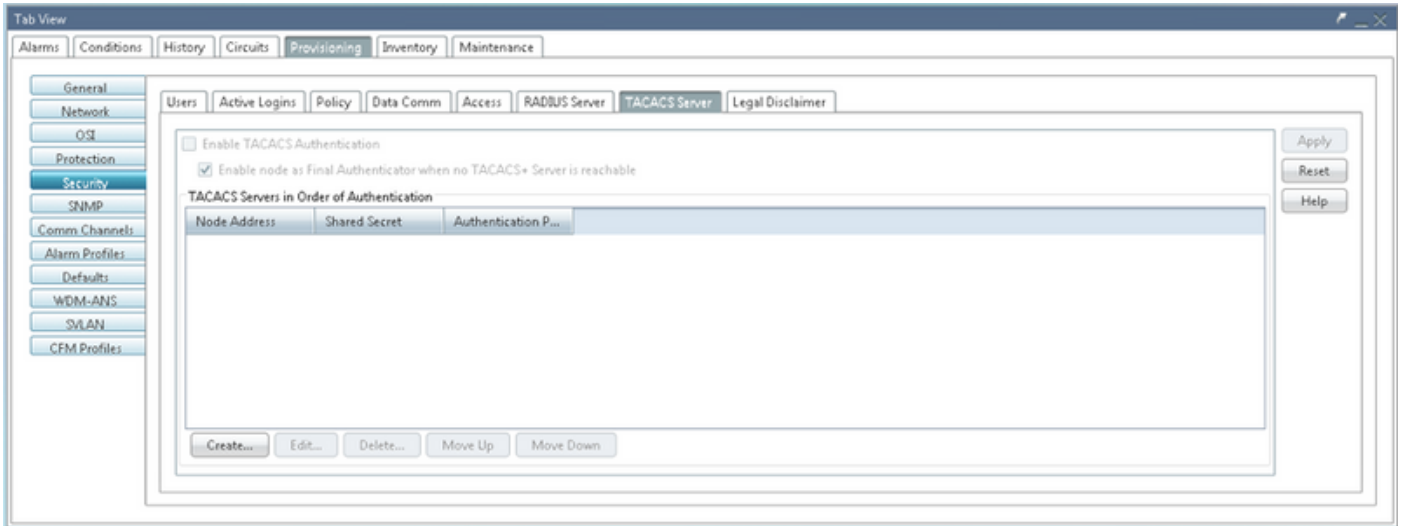
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration.

**Note:** If your network is live, ensure that you understand the potential impact of any command.

## Configure

Configurations required on ONS15454/NCS2000:

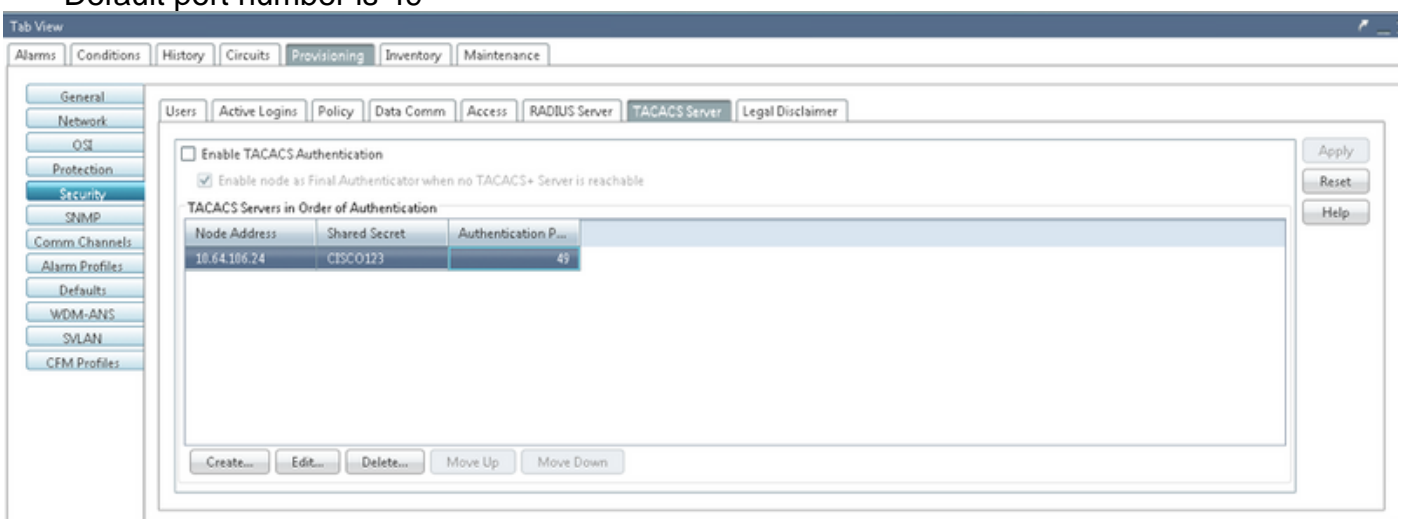
1. You can configure TACACS server configuration from this Tab. Navigate to **Provisioning > Security > TACACS Server** as shown in the image.



2. In order to add the TACACS+ server details, click on the **Create** button. It will open the TACACS+ configuration window as shown in this image.



- Enter the Server IP address
- Add the Shared secret between Node and the TACACS+ server
- Add the authentication port number. At this port, TACACS+ server is listening for the client. Default port number is 49



3. In order to activate the TACACS+ server configuration on NODE, check the checkbox **Enable TACACS Authentication** and click on the **Apply** button as shown in the image.

Enable TACACS Authentication

4. In order to enable the Node as the final authenticator, when no server is reachable, click on the

checkbox as shown in the image.

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

5. In order to modify the particular server configuration, select the corresponding server configuration row, click on the **Edit** button in order to modify the configuration.

6. In order to delete the particular server configuration, select the corresponding server configuration row, click on **Delete** button to delete the configuration.

Configurations required on ACS Server:

1. Create Network device and AAA client and click on the **create** button in **Network Resources** pan as shown in the image.



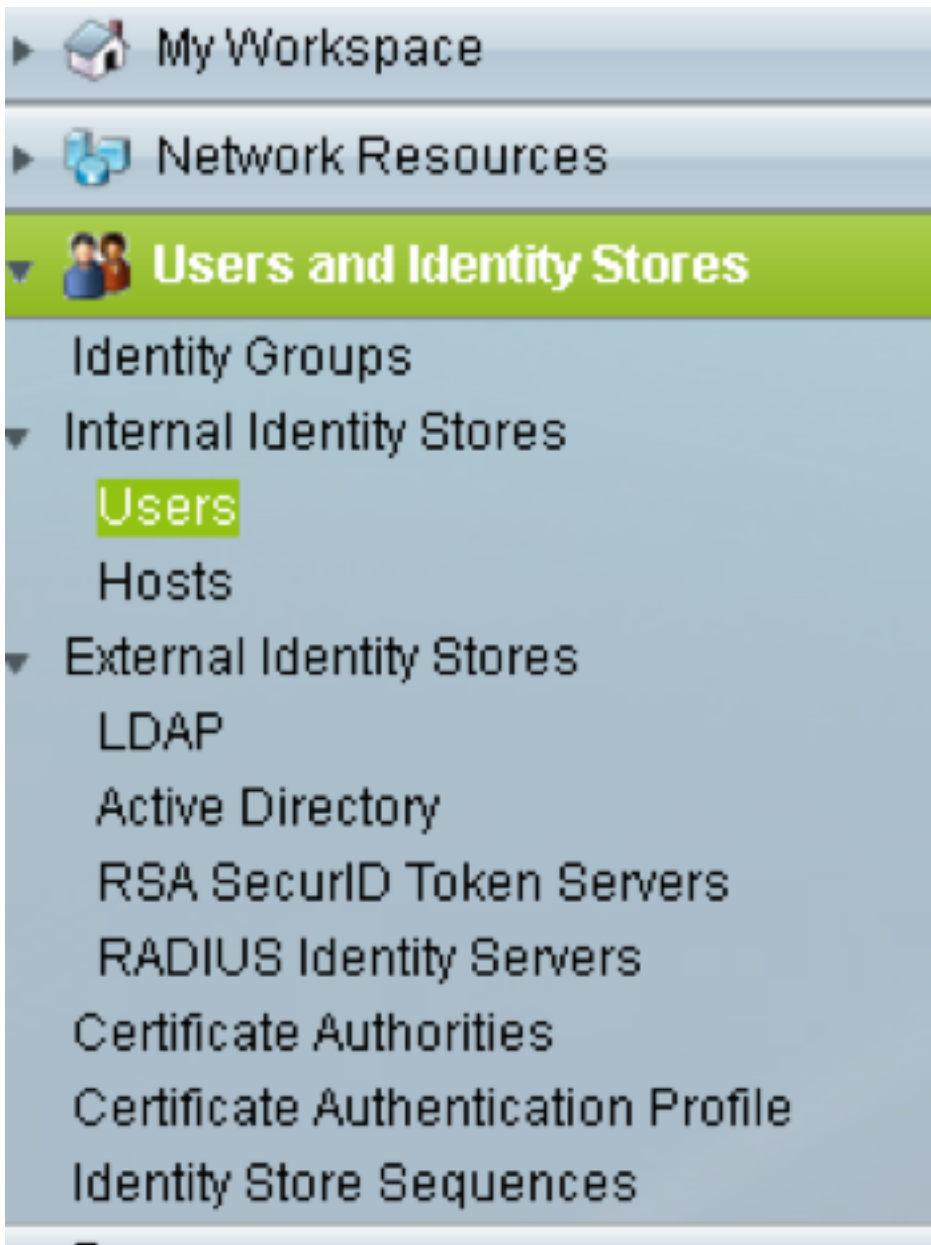
2. Give same **Shared Secret** as given in ONS node configuration. Otherwise, authentication will be failed.

**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. Create a username and password for the required user to get authenticated in the **Users and Identity Stores** Pan as shown in the 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. Create shell profiles in the **Policy Elements** pane:

a. Select the privilege level (0 to 3):

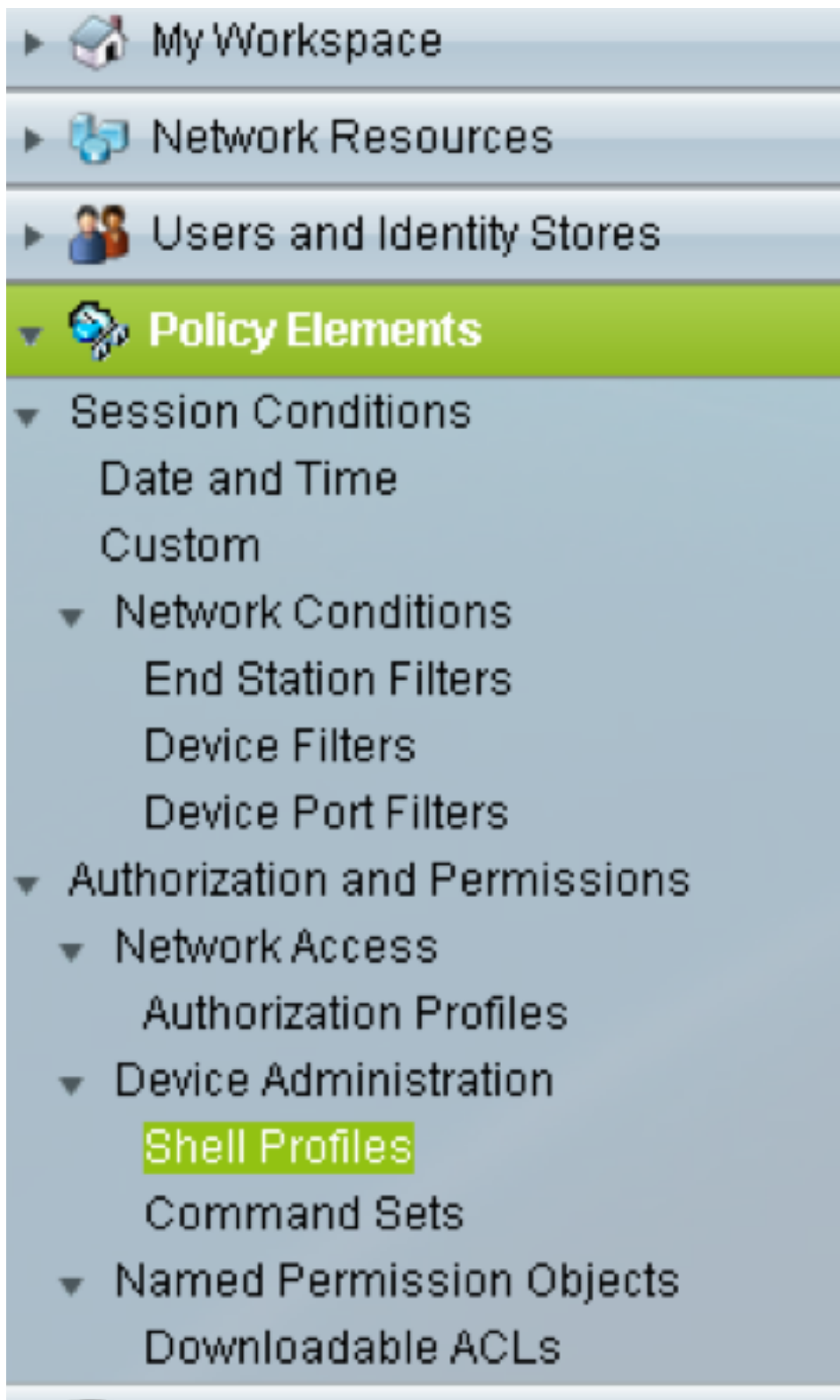
0 for Retrieve user.

1 for Maintenance user.

2 for Provisioning user.

3 for Superuser.

b. Create a custom attribute in **Customer Attributes** panel for **Idle Time** attribute.



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” indicates that connection never times out and it will be forever. If user specifies any other time, connection will be available for that many **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:

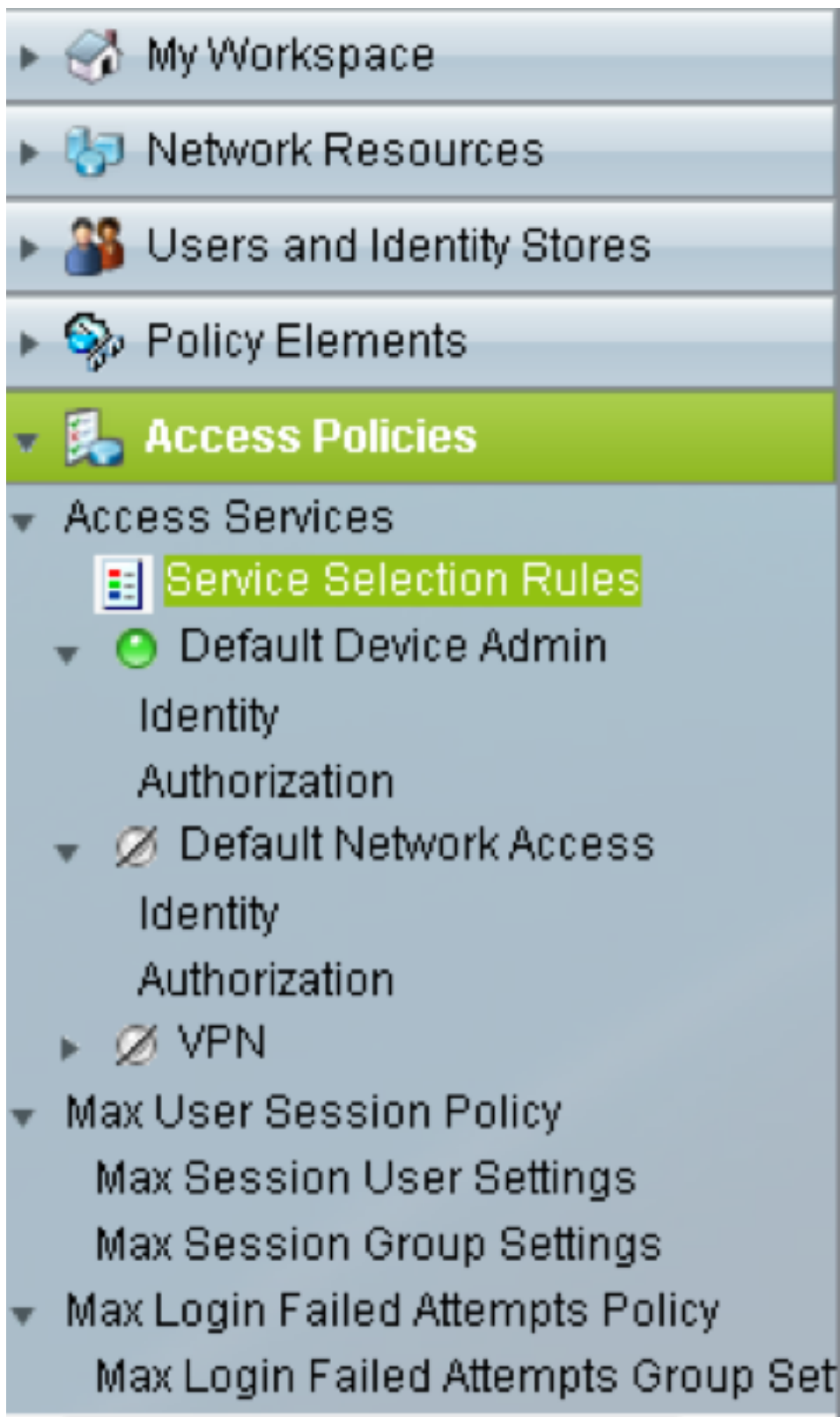
Requirement: Mandatory ▾

Attribute Value: Static ▾



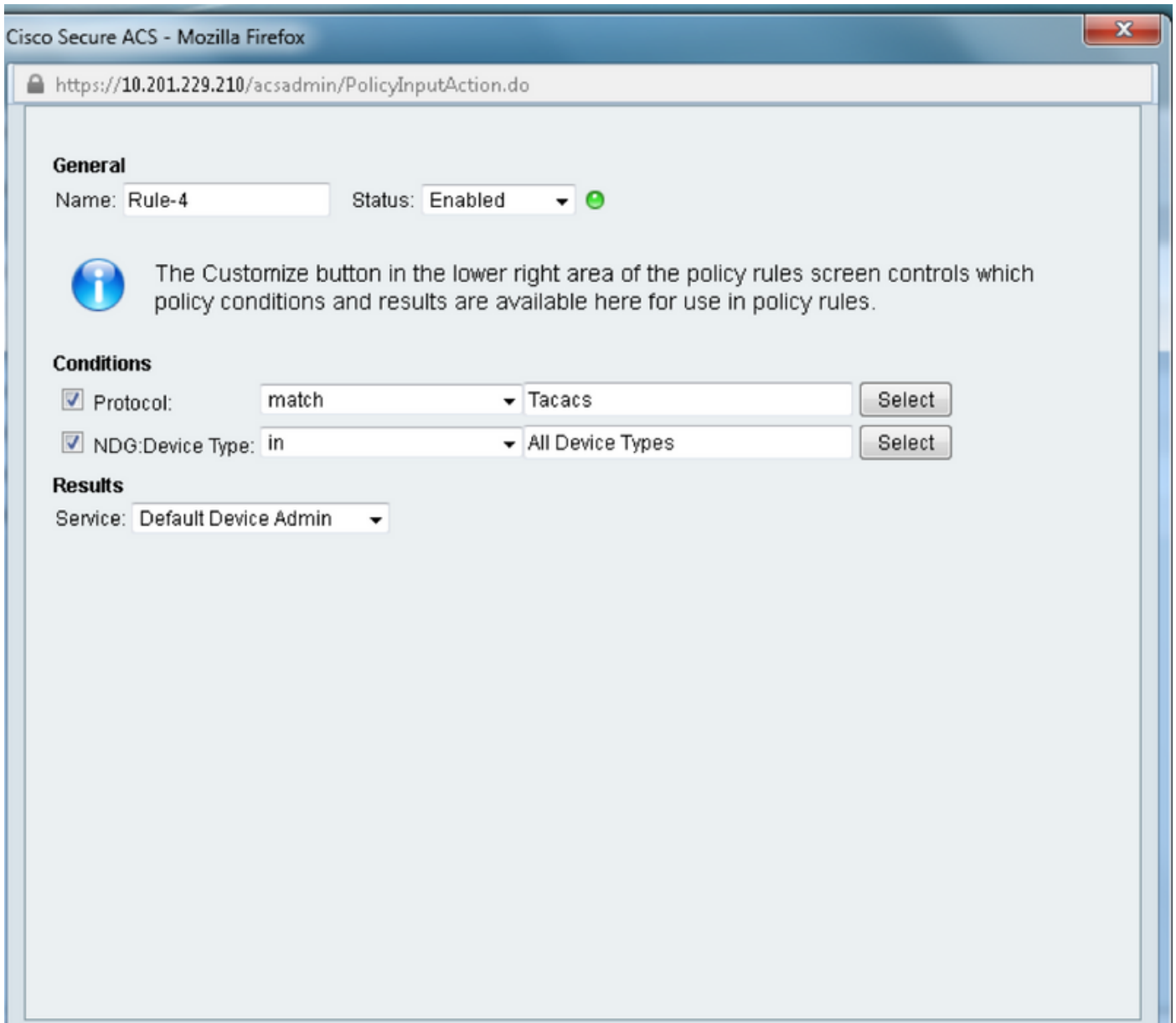
5. Create Access policies in the **Access Policies** panel:














a. Click on **Service Selection Rules** and create a rule:

- Select TACACS as protocol
- The device as All device or specific similar to which created earlier
- Service type as **Default Device Admin**.

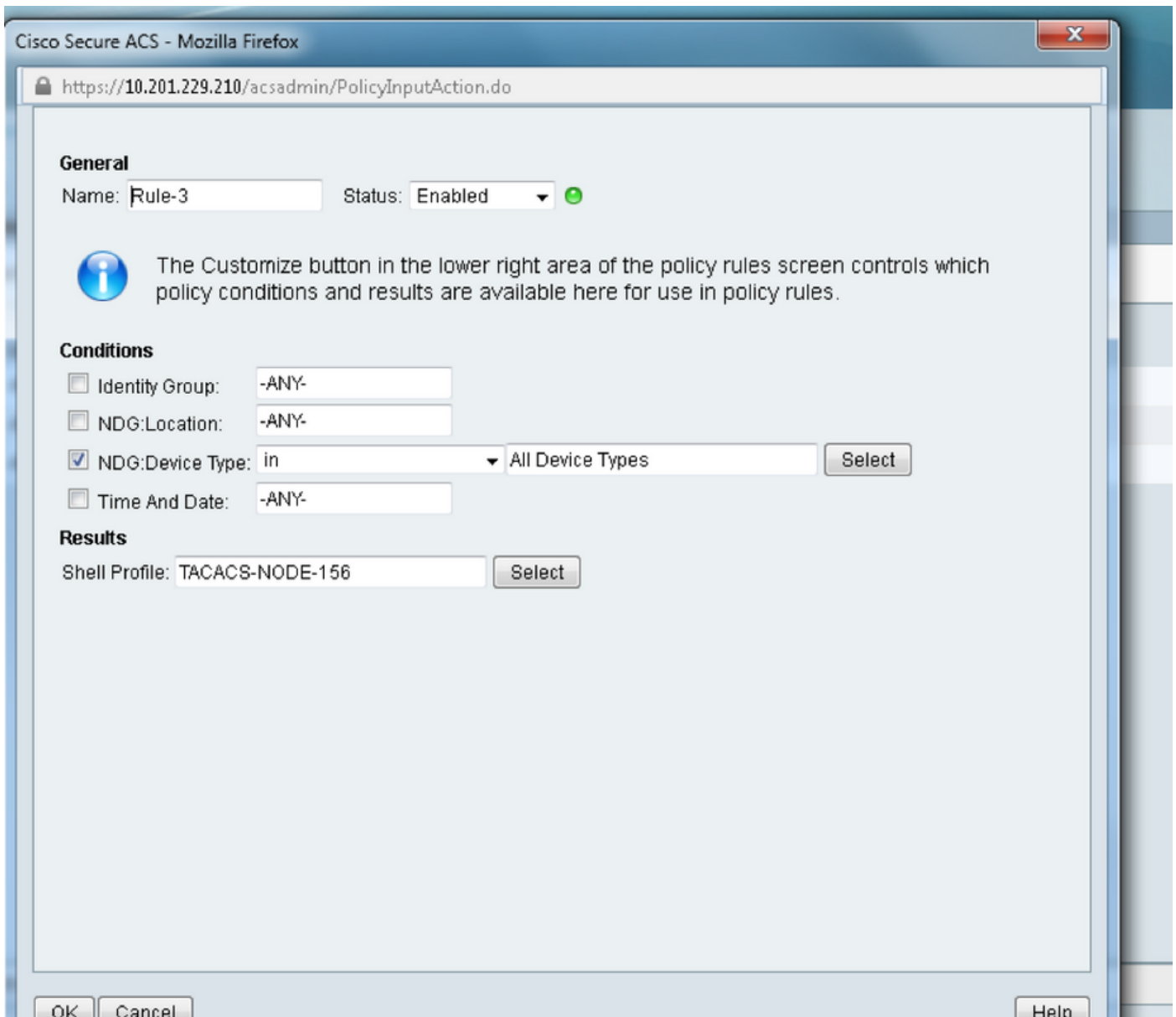


b. Select **Authorization** and create a rule for authorization in under **Default Device Admin** radio button:

- Select **Already Created** shell profile
- Select a specific device or all devices in device type

- ▶  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] ▶



## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.