

# Configure Custom TACACS Role for Nexus 9K Using ISE 3.2

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Configure](#)

[Network Diagram](#)

[Step 1: Configure Nexus 9000](#)

[Step 2. Configure Identity Service Engine 3.2](#)

### [Verify](#)

### [Troubleshoot](#)

---

## Introduction

This document describes how to configure a customized Nexus role for TACACS via CLI on NK9.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- TACACS+
- ISE 3.2

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco Nexus9000, NXOS image file is: bootflash:///nxos.9.3.5.bin
- Identity Service Engine version 3.2

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

## Background Information

Licensing Requirements:

Cisco NX-OS - TACACS+ requires no license.

Cisco Identity Service Engine - For fresh ISE installations you have 90 days evaluation period license that has access to all ISE features, if you do not have an evaluation license, in order to use ISE TACACS feature you need a Device Admin license for the Policy Server Node that does the authentication.

After the Admin/Help desk users authenticate on the Nexus device ISE returns the desired Nexus shell role.

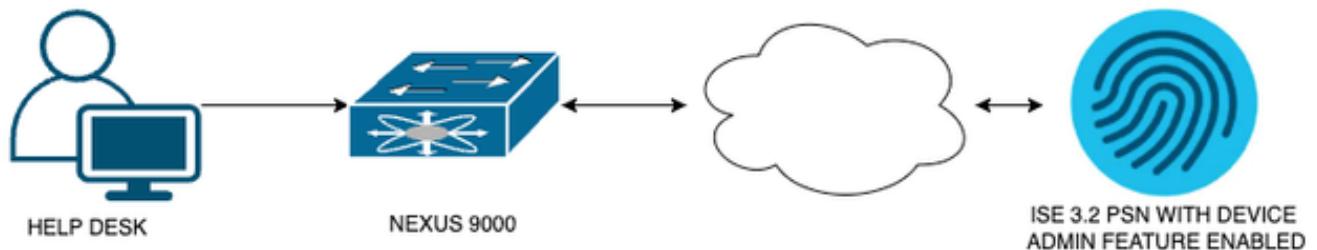
The user assigned with this role can perform basic troubleshooting and bounce certain ports.

The TACACS session that gets the Nexus role must be able to only use and run the next commands and actions:

- Access to configure terminal to ONLY execute shut down and no shut-on interfaces from 1/1-1/21 and 1/25-1/30
- ssh
- ssh6
- telnet
- Telnet6
- Traceroute
- Traceroute6
- Ping
- Ping6
- Enable

## Configure

### Network Diagram



*Flow Components Diagram*

### Step 1: Configure Nexus 9000

1. AAA configuration.



**Warning:** After you enable TACACS authentication, the Nexus device stops using local authentication and starts using AAA server based authentication.

```
Nexus9000(config)# feature tacacs+
Nexus9000(config)# tacacs-server host <Your ISE IP> key 0 Nexus3xample
Nexus9000(config)# tacacs-server key 0 "Nexus3xample"
Nexus9000(config)# aaa group server tacacs+ IsePsnServers
Nexus9000(config-tacacs+)# server <Your ISE IP>
Nexus9000(config)# aaa authentication login default group IsePsnServers local
```

2. Configure the customized role with the requirements specified.

```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)#   description Can perform basic Troubleshooting and bounce certain ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
```

```

Nexus9000(config-role)# rule 4 permit command ssh6 *
Nexus9000(config-role)# rule 5 permit command ping *
Nexus9000(config-role)# rule 6 permit command ping6 *
Nexus9000(config-role)# rule 7 permit command telnet *
Nexus9000(config-role)# rule 8 permit command traceroute *
Nexus9000(config-role)# rule 9 permit command traceroute6 *
Nexus9000(config-role)# rule 10 permit command telnet6 *
Nexus9000(config-role)# rule 11 permit command config t ; interface * ; shutdown
Nexus9000(config-role)# rule 12 permit command config t ; interface * ; no shutdown

vlan policy deny
interface policy deny

Nexus9000(config-role-interface)#          permit interface Ethernet1/1
Nexus9000(config-role-interface)#          permit interface Ethernet1/2
Nexus9000(config-role-interface)#          permit interface Ethernet1/3
Nexus9000(config-role-interface)#          permit interface Ethernet1/4
Nexus9000(config-role-interface)#          permit interface Ethernet1/5
Nexus9000(config-role-interface)#          permit interface Ethernet1/6
Nexus9000(config-role-interface)#          permit interface Ethernet1/7
Nexus9000(config-role-interface)#          permit interface Ethernet1/8
Nexus9000(config-role-interface)#          permit interface Ethernet1/8
Nexus9000(config-role-interface)#          permit interface Ethernet1/9
Nexus9000(config-role-interface)#          permit interface Ethernet1/10
Nexus9000(config-role-interface)#          permit interface Ethernet1/11
Nexus9000(config-role-interface)#          permit interface Ethernet1/12
Nexus9000(config-role-interface)#          permit interface Ethernet1/13
Nexus9000(config-role-interface)#          permit interface Ethernet1/14
Nexus9000(config-role-interface)#          permit interface Ethernet1/15
Nexus9000(config-role-interface)#          permit interface Ethernet1/16
Nexus9000(config-role-interface)#          permit interface Ethernet1/17
Nexus9000(config-role-interface)#          permit interface Ethernet1/18
Nexus9000(config-role-interface)#          permit interface Ethernet1/19
Nexus9000(config-role-interface)#          permit interface Ethernet1/20
Nexus9000(config-role-interface)#          permit interface Ethernet1/21
Nexus9000(config-role-interface)#          permit interface Ethernet1/22
Nexus9000(config-role-interface)#          permit interface Ethernet1/25
Nexus9000(config-role-interface)#          permit interface Ethernet1/26
Nexus9000(config-role-interface)#          permit interface Ethernet1/27
Nexus9000(config-role-interface)#          permit interface Ethernet1/28
Nexus9000(config-role-interface)#          permit interface Ethernet1/29
Nexus9000(config-role-interface)#          permit interface Ethernet1/30

Nexus9000# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...

Copy complete.

```

## Step 2. Configure Identity Service Engine 3.2

1. Configure the identity that is used during Nexus TACACS session.

ISE local authentication is used.

Navigate to the **Administration > Identity Management > Groups** tab and create the group that the user needs to be part of, the identity group created for this demonstration is **iseUsers**.

Cisco ISE Administration · Identity Management Evaluation Mode 29 Days

Identities Groups External Identity Sources Identity Source Sequences Settings

User Identity Groups > New User Identity Group

Identity Groups

Identity Group

\* Name iseUsers

Description

Submit Cancel

This screenshot shows the 'User Identity Groups' section in Cisco ISE. A new group named 'iseUsers' is being created. The 'Name' field is filled with 'iseUsers'. The 'Submit' button is highlighted in blue at the bottom right.

Creating a user group

Click the **Submit** button.

Next navigate to **Administration > Identity Management > Identity** tab.

Press on the **Add Button**.

Cisco ISE Administration · Identity Management Evaluation Mode 29 Days

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 0

Edit **+ Add** Change Status Import Export Delete All

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Adr
No data available							

This screenshot shows the 'Network Access Users' page in Cisco ISE. The 'Add' button is highlighted with a red box. The table below shows no data available.

User creation

As part of the mandatory fields, start with the name of the user, the username **iseiscool** is used in this example.

## ✓ Network Access User

\* Username iseiscool

Status  Enabled

Account Name Alias



Email

*Naming the User and Creating it*

The next step is to assign a password to the username created, VainillaISE97 is the password used in this demonstration.

## ✓ Passwords

Password Type: Internal Users

Password Lifetime:

 With Expiration 

Password will expire in 60 days

 Never Expires 

Password

Re-Enter Password

\* Login Password .....

Enable Password

*Password assignment*

Finally, assign the user to the group previously created, which is in this case **iseUsers**.

## ✓ User Groups

iseUsers

*Group assignation*

## 2. Configure and Add the Network Device.

Add the NEXUS 9000 device to ISE **Administration > Network Resources > Network Devices**

Click the **Add** button in order to start.

The screenshot shows the 'Network Devices' page in Cisco ISE. At the top, there is a toolbar with icons for Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete. Below the toolbar is a header row with columns: Name, IP/Mask, Profile Name, Location, and Type. The 'Name' column has a checkbox icon. The 'Profile Name' column is currently empty. The 'Location' and 'Type' columns also have empty fields. The 'IP/Mask' column contains a dropdown menu with options like 'IP Address', 'MAC Address', and 'Range'. The 'Add' button in the toolbar is highlighted with a red box.

*Network Access Device Page*

Enter the values to the form, assign a name to the NAD you are creating, and an IP from which the NAD contacts ISE for the TACACS conversation.

The screenshot shows the 'New Network Device' configuration page in Cisco ISE. The left sidebar lists 'Network Devices', 'Network Device Groups', 'Default Devices', 'TACACS External Servers', and 'TACACS Server Sequence'. The main area is titled 'Network Devices' and contains fields for 'Name' (set to 'NEXUS9K'), 'Description' (set to 'Nexus Device For TACACS'), 'IP Address' (set to 'A.B.C.D'), 'Device Profile' (set to 'Cisco'), 'Model Name', 'Software Version', and 'Network Device Group'. The 'IP Address' field is highlighted with a red box.

*Configure Network Device*

The drop-down options can be left in blank and can be omitted, these options are intended to categorize your NADs by Location, Device type, Version, and then change the authentication flow based on these filters.

On the **Administration > Network Resources > Network Devices > Your NAD > TACACS Authentication Settings**.

Add the Shared Secret that you used under your NAD configuration for this demonstration, Nexus3xample is used in this demonstration.

## TACACS Authentication Settings

Shared Secret **Nexus3xample**

[Hide](#)

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

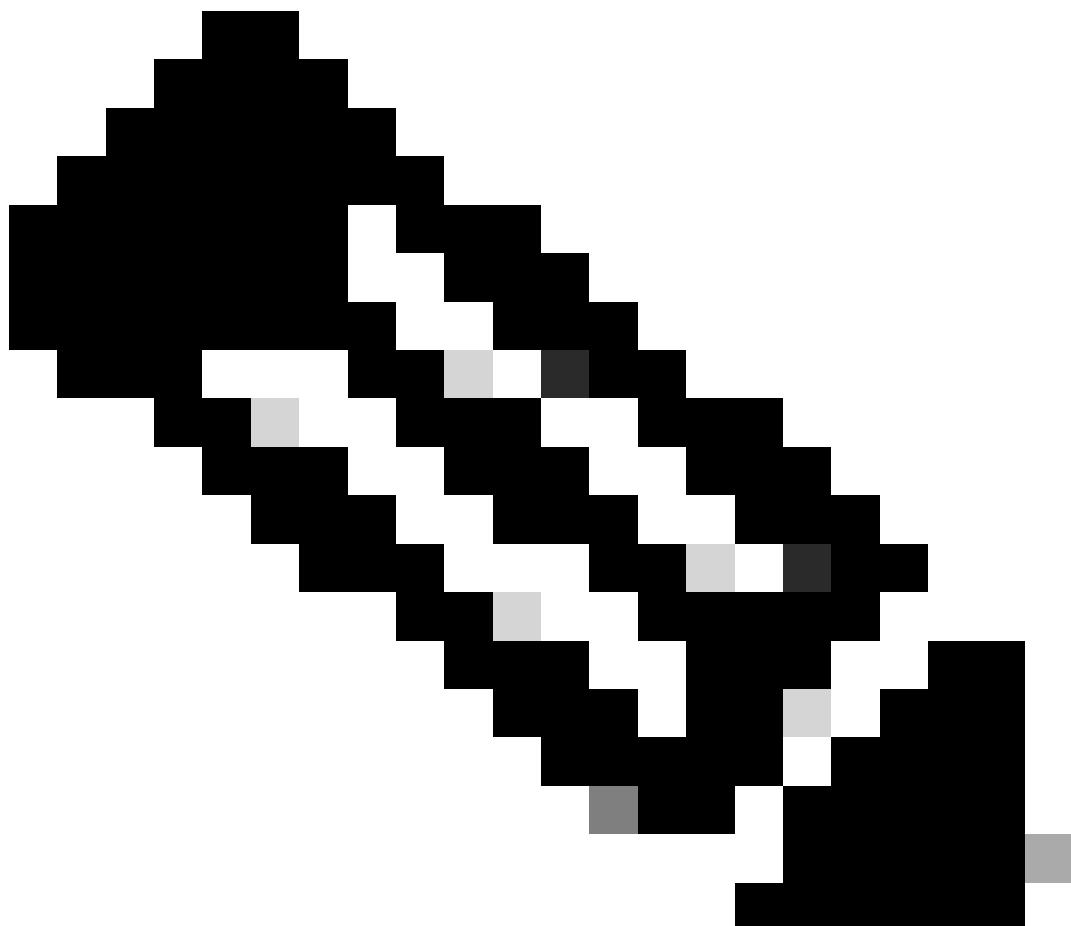
*TACACS configuration section*

Save the changes by clicking the **Submit** button.

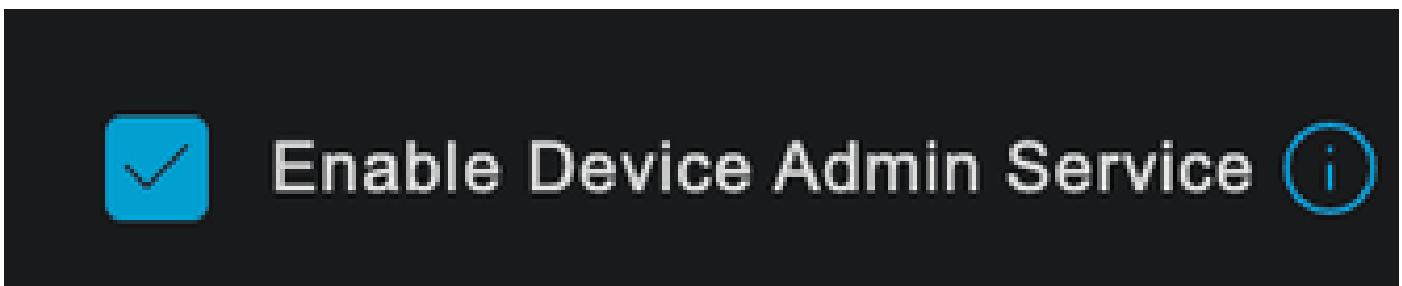
### 3. TACACS configuration on ISE.

Double-check that the PSN you configured in the Nexus 9k has the option **Device Admin** enabled.

---



**Note:** Enable Device Admin Service does NOT cause a restart on ISE.



*PSN Device Admin feature check*

This can be checked under ISE menu **Administration > System > Deployment > Your PSN > Policy Server section > Enable Device Admin Services**.

- Create a TACACS profile, that returns the role helpdesk to the Nexus device if the authentication is successful.

From the ISE Menu, navigate to **Workcenters > Device Administration > Policy Elements > Results > TACACS Profiles** and click the **Add** button.

Screenshot of the Cisco ISE web interface showing the TACACS Profiles page. The left sidebar has sections like Conditions, Network Conditions, and Results. The main area shows a table of existing profiles: Default Shell Profile (Shell, Description: Default Shell Profile) and Deny All Shell Profile (Shell, Description: Deny All Shell Profile). A red box highlights the 'Add' button at the top of the table.

*TACACS Profile*

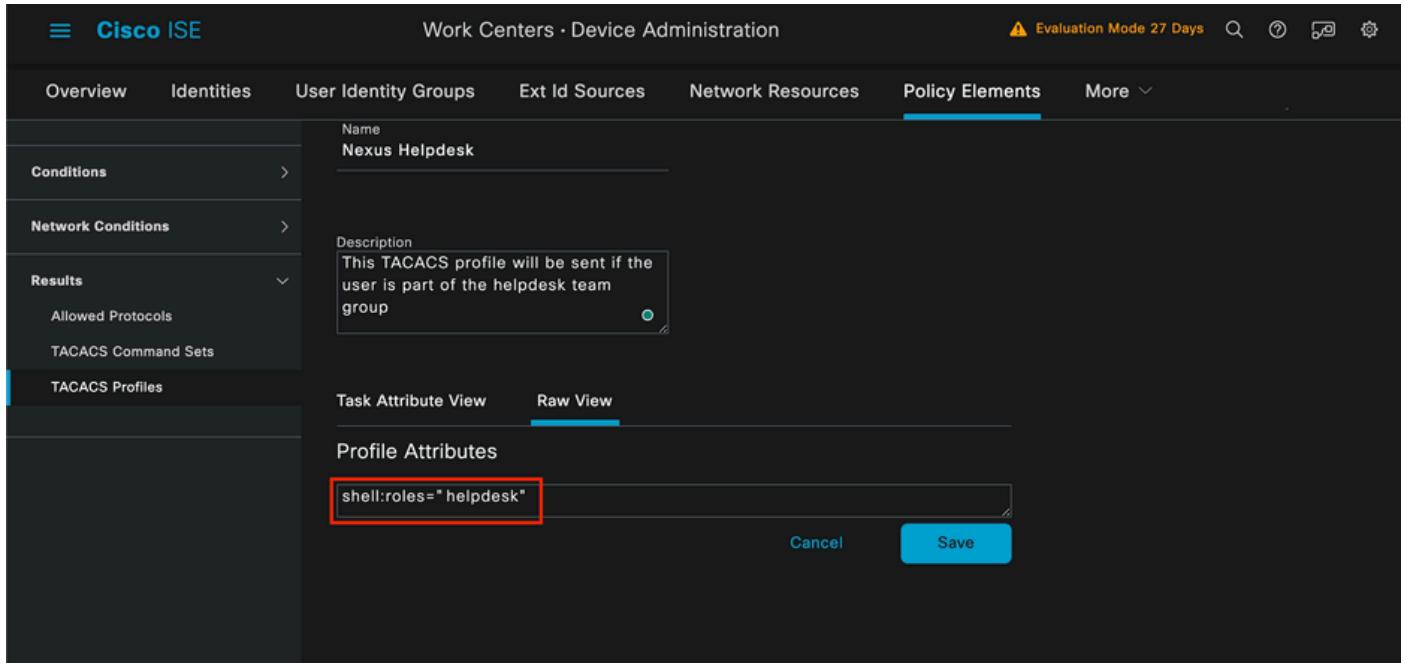
Assign a Name, and optionally a description.

Screenshot of the Cisco ISE web interface showing the 'New TACACS Profile' configuration page. The left sidebar has sections like Conditions, Network Conditions, and Results. The main area shows fields for Name (Nexus Helpdesk) and Description (This TACACS profile will be sent if the user is part of the helpdesk team group).

## Naming Tacacs profile

Ignore the **Task Attribute View** section and navigate to the **Raw View** section.

And enter the value **shell:roles="helpdesk"**.



The screenshot shows the Cisco ISE interface under 'Work Centers - Device Administration'. A 'Policy Elements' card is open, specifically for a TACACS profile named 'Nexus Helpdesk'. The 'Raw View' tab is selected. In the 'Profile Attributes' section, the attribute 'shell:roles="helpdesk"' is listed and highlighted with a red box. The 'Save' button is visible at the bottom right.

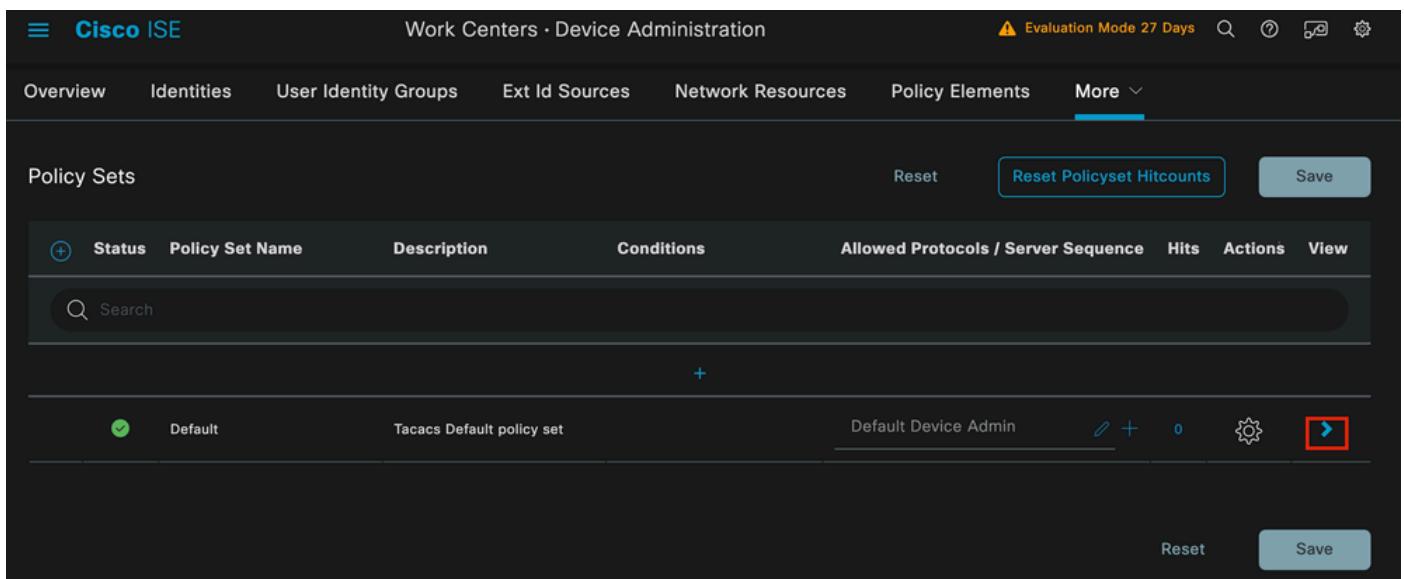
## Adding Profile Attribute

Configure the Policy Set that includes the Authentication Policy and the Authorization Policy.

On the ISE menu access **Work Centers > Device Administration > Device Admin Policy Sets**.

For demonstration purposes, the Default Policy set is used. However, another Policy set can be created, with conditions in order to match specific scenarios.

Click the arrow at the end of the row.



The screenshot shows the 'Device Admin Policy Sets' page in Cisco ISE. A table lists a single policy set named 'Default'. The 'Actions' column for this row contains several icons, with the edit icon highlighted by a red box. Other columns include 'Status', 'Policy Set Name', 'Description', 'Conditions', 'Allowed Protocols / Server Sequence', 'Hits', and 'View'.

## Device Admin Policy Sets page

Once inside the policy set configuration scroll down and expand the **Authentication Policy** section.

Click the **Add** icon.

For this configuration example, the Name value is **Internal Authentication** and the condition chosen is the Network Device (Nexus) IP (substitute the **A.B.C.D.**). This Authentication policy uses the Internal Users Identity Store.

The screenshot shows the Cisco ISE Work Centers - Device Administration interface. In the center, there's a table with columns: Status, Rule Name, Conditions, Use, Hits, and Actions. A search bar is at the top left. On the right, there's a sidebar with sections like Options, If Auth fail, If User not found, If Process fail, and All\_User\_ID\_Stores. A gear icon is at the bottom right of the sidebar.

Key elements highlighted with red boxes:

- Internal Authentication** (under Status)
- Network Access-Device IP Address EQUALS A.B.C.D** (under Conditions)
- Internal Users** (under Use)

#### Authentication Policy

Here is how the condition was configured.

Select the **Network Access > Device IP address Dictionary Attribute**.

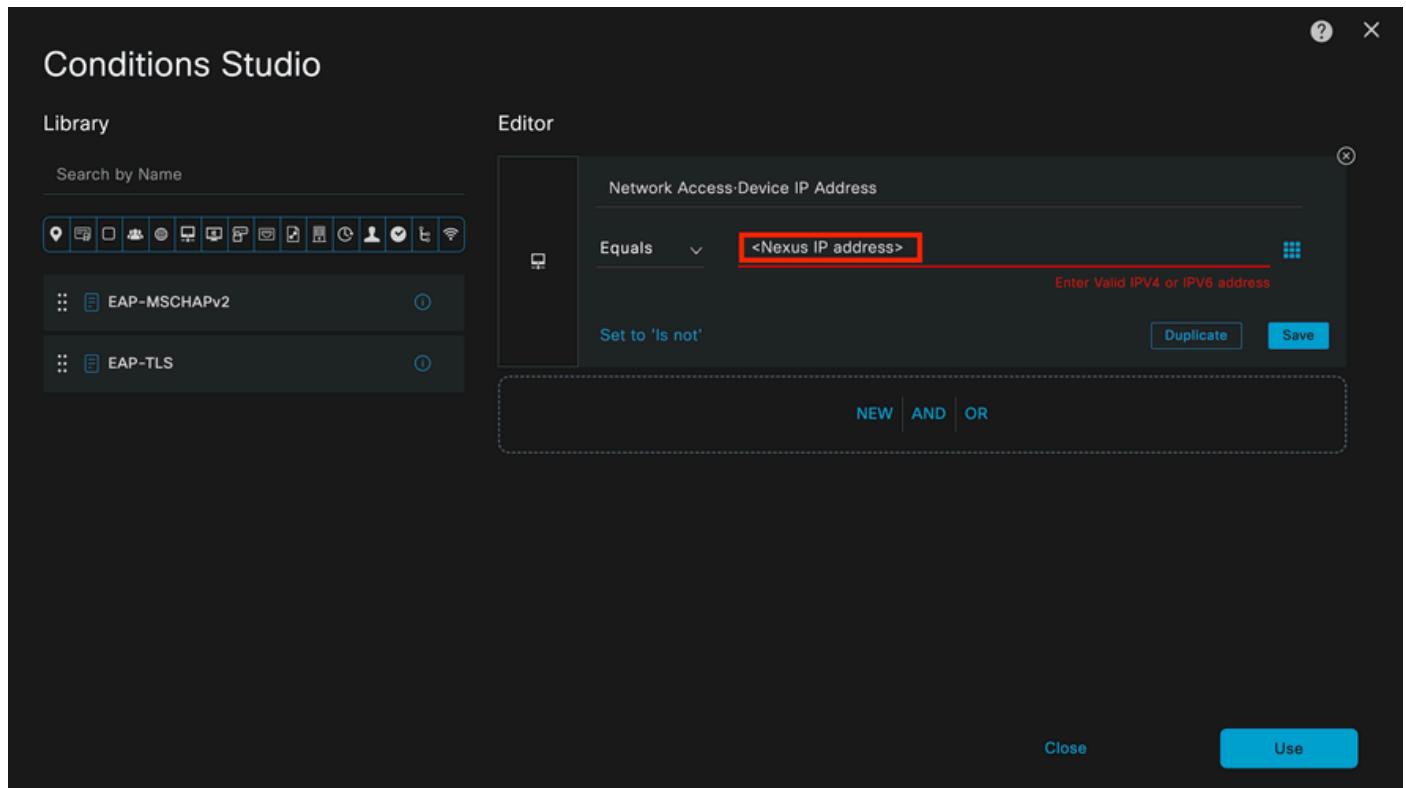
The screenshot shows the Conditions Studio dialog box. The left pane is a library with icons for various authentication methods like EAP-MSCHAPv2 and EAP-TLS. The right pane is the Editor, which has a search bar and a table titled "Select attribute for condition".

Key elements highlighted with blue boxes:

- Network Access-Device IP Address** (in the search bar)
- Dictionary** (column header in the table)
- Attribute** (column header in the table)
- Device IP Address** (highlighted row in the table)

Condition studio for authentication policy

Replace the <Nexus IP address> comment with the correct IP.



Adding the IP filter

Click on the **Use** button.

This condition is hit only by the Nexus Device you configured, however, if the purpose is to enable this condition for a large amount of devices, a different condition must be considered.

Then navigate to the **Authorization Policy** section and expand it.

Click on the + (plus) icon.

The screenshot shows the Cisco ISE Device Admin Policy Sets page. In the navigation bar, 'Device Admin Policy Sets' is highlighted. The main table has columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A search bar is at the top. Below the table, there are sections for Authentication Policy (2), Authorization Policy - Local Exceptions, Authorization Policy - Global Exceptions, and Authorization Policy (1). The 'Authorization Policy (1)' section is expanded and highlighted with a red box. It contains a table with columns for Status, Rule Name, Conditions, Command Sets, Shell Profiles, Hits, and Actions. A search bar is at the top of this section. A red box highlights the 'DenyAllCommands' command set. At the bottom right of the section, there are buttons for 'Deny All Shell Profile' and other actions.

Authorization policy section

In this example **NEXUS HELP DESK** as the name of the Authorization Policy was used.

The screenshot shows the 'Condition studio for Authorization Policy' screen. It displays a table with columns for Status, Rule Name, Conditions, Command Sets, Shell Profiles, Hits, and Actions. A search bar is at the top. A condition row is selected and highlighted with a red box, showing 'Network Access-Device IP Address EQUALS A.B.C.D'. In the Shell Profiles column, a profile named 'Nexus Helpdesk' is selected and highlighted with a red box. At the bottom right, there are 'Reset' and 'Save' buttons, with the 'Save' button highlighted with a red box.

Condition studio for Authorization Policy

The same condition that was configured in the Authentication Policy is used for the Authorization policy.

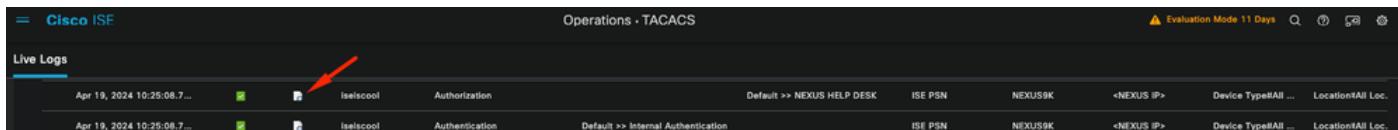
In the Shell Profiles column, the Profile configured before **Nexus Helpdesk** was selected.

Finally, click the **Save** button.

## Verify

Use this section in order to confirm that your configuration works properly.

From ISE GUI, navigate to **Operations > TACACS > Live Logs**, identify the record that matches the username used, and click the Live Log Detail of the Authorization event.



The screenshot shows the Cisco ISE Operations - TACACS interface. At the top, there's a navigation bar with 'Cisco ISE' on the left and 'Operations - TACACS' in the center. On the right, there are icons for evaluation mode (11 days), search, and other system status. Below the navigation bar is a 'Live Logs' section. A red arrow points to a small icon next to the log entry for 'Apr 19, 2024 10:25:08.7...'. The log entries show two rows of data. The first row has columns: 'Apr 19, 2024 10:25:08.7...', 'iseiscool', 'Authorization', 'Default >> NEXUS HELP DESK', 'ISE PSN', 'NEXUS9K', '<NEXUS IP>', 'Device Type>All ...', and 'Location>All Loc.'. The second row has similar columns: 'Apr 19, 2024 10:25:08.7...', 'iseiscool', 'Authentication', 'Default >> Internal Authentication', 'ISE PSN', 'NEXUS9K', '<NEXUS IP>', 'Device Type>All ...', and 'Location>All Loc.'

#### TACACS Live Log

As part of the details that this report includes, it can be found a **Response** section, where you can see how ISE returned the value shell:roles="helpdesk"

#### Response

```
{Author-Reply-Status=PassRepl;  
AVPair=shell:roles=" helpdesk" ; }
```

#### Live Log Detail Response

On the Nexus device:

```
Nexus9000 login: iseiscool  
Password: VainillaISE97
```

```
Nexus9000# conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Nexus9000(config)# interface ethernet 1/23  
% Interface permission denied
```

```
Nexus9000(config)# ?  
  interface  Configure interfaces  
  show       Show running system information  
  end        Go to exec mode  
  exit       Exit from command interpreter
```

```
Nexus9000(config)# role name test  
% Permission denied for the role
```

```
Nexus9000(config)#
```

```
Nexus9000(config)# interface loopback 0  
% Interface permission denied
```

```
Nexus9000(config)#  
Nexus9000# conf t
```

```
Nexus9000(config)# interface ethernet 1/5  
Notice that only the commands allowed are listed.  
Nexus9000(config-if)# ?
```

```
  no          Negate a command or set its defaults  
  show        Show running system information  
  shutdown   Enable/disable an interface  
  end        Go to exec mode  
  exit       Exit from command interpreter
```

```
Nexus9000(config-if)# cdp  
Nexus9000(config-if)# cdp enable  
% Permission denied for the role  
Nexus9000(config-if)#
```

# Troubleshoot

- Verify that ISE is reachable from the Nexus device.  
Nexus9000# ping <Your ISE IP>  
PING <Your ISE IP> (<Your ISE IP> 56 data bytes  
64 bytes from <Your ISE IP> : icmp\_seq=0 ttl=59 time=1.22 ms  
64 bytes from <Your ISE IP> : icmp\_seq=1 ttl=59 time=0.739 ms  
64 bytes from <Your ISE IP> : icmp\_seq=2 ttl=59 time=0.686 ms  
64 bytes from <Your ISE IP> : icmp\_seq=3 ttl=59 time=0.71 ms  
64 bytes from <Your ISE IP> : icmp\_seq=4 ttl=59 time=0.72 ms
- Verify, that port 49 is opened, between ISE and the Nexus device.  
Nexus9000# telnet <Your ISE IP> 49  
Trying <Your ISE IP> ...  
Connected to <Your ISE IP> .  
Escape character is '^]'.  
• Use these debugs:

```
debug tacacs+ all
Nexus9000#
Nexus9000# 2024 Apr 19 22:50:44.199329 tacacs: event_loop(): calling process_rd_fd_set
2024 Apr 19 22:50:44.199355 tacacs: process_rd_fd_set: calling callback for fd 6
2024 Apr 19 22:50:44.199392 tacacs: fsrv didnt consume 8421 opcode
2024 Apr 19 22:50:44.199406 tacacs: process_implicit_cfs_session_start: entering...
2024 Apr 19 22:50:44.199414 tacacs: process_implicit_cfs_session_start: exiting; we are in distribution
disabled state
2024 Apr 19 22:50:44.199424 tacacs: process_aaa_tplus_request: entering for aaa session id 0
2024 Apr 19 22:50:44.199438 tacacs: process_aaa_tplus_request:Checking for state of mgmt0 port with
servergroup IsePsnServers
2024 Apr 19 22:50:44.199451 tacacs: tacacs_global_config(4220): entering ...
2024 Apr 19 22:50:44.199466 tacacs: tacacs_global_config(4577): GET_REQ...
2024 Apr 19 22:50:44.208027 tacacs: tacacs_global_config(4701): got back the return value of global
Protocol configuration operation:SUCCESS
2024 Apr 19 22:50:44.208045 tacacs: tacacs_global_config(4716): REQ:num server 0
2024 Apr 19 22:50:44.208054 tacacs: tacacs_global_config: REQ:num group 1
2024 Apr 19 22:50:44.208062 tacacs: tacacs_global_config: REQ:num timeout 5
2024 Apr 19 22:50:44.208070 tacacs: tacacs_global_config: REQ:num deadtime 0
2024 Apr 19 22:50:44.208078 tacacs: tacacs_global_config: REQ:num encryption_type 7
2024 Apr 19 22:50:44.208086 tacacs: tacacs_global_config: returning retval 0
2024 Apr 19 22:50:44.208098 tacacs: process_aaa_tplus_request:group_info is populated in aaa_req, so
Using servergroup IsePsnServers
2024 Apr 19 22:50:44.208108 tacacs: tacacs_servergroup_config: entering for server group, index 0
2024 Apr 19 22:50:44.208117 tacacs: tacacs_servergroup_config: GETNEXT_REQ for Protocol server
group index:0 name:
2024 Apr 19 22:50:44.208148 tacacs: tacacs_pss2_move2key: rcode = 40480003 syserr2str = no such pss
key
2024 Apr 19 22:50:44.208160 tacacs: tacacs_pss2_move2key: calling pss2_getkey
2024 Apr 19 22:50:44.208171 tacacs: tacacs_servergroup_config: GETNEXT_REQ got Protocol server
group index:2 name:IsePsnServers
2024 Apr 19 22:50:44.208184 tacacs: tacacs_servergroup_config: got back the return value of Protocol
group operation:SUCCESS
2024 Apr 19 22:50:44.208194 tacacs: tacacs_servergroup_config: returning retval 0 for Protocol server
group:IsePsnServers
2024 Apr 19 22:50:44.208210 tacacs: process_aaa_tplus_request: Group IsePsnServers found.
```

corresponding vrf is default, source-intf is 0  
2024 Apr 19 22:50:44.208224 tacacs: process\_aaa\_tplus\_request: checking for mgmt0 vrf:management against vrf:default of requested group  
2024 Apr 19 22:50:44.208256 tacacs: process\_aaa\_tplus\_request:mgmt\_if 83886080  
2024 Apr 19 22:50:44.208272 tacacs: process\_aaa\_tplus\_request:global\_src\_intf : 0, local src\_intf is 0 and vrf\_name is default  
2024 Apr 19 22:50:44.208286 tacacs: create\_tplus\_req\_state\_machine(902): entering for aaa session id 0  
2024 Apr 19 22:50:44.208295 tacacs: state machine count 0  
2024 Apr 19 22:50:44.208307 tacacs: init\_tplus\_req\_state\_machine: entering for aaa session id 0  
2024 Apr 19 22:50:44.208317 tacacs: init\_tplus\_req\_state\_machine(1298):tplus\_ctx is NULL it should be if author and test  
2024 Apr 19 22:50:44.208327 tacacs: tacacs\_servergroup\_config: entering for server group IsePsnServers, index 0  
2024 Apr 19 22:50:44.208339 tacacs: tacacs\_servergroup\_config: GET\_REQ for Protocol server group index:0 name:IsePsnServers  
2024 Apr 19 22:50:44.208357 tacacs: find\_tacacs\_servergroup: entering for server group IsePsnServers  
2024 Apr 19 22:50:44.208372 tacacs: tacacs\_pss2\_move2key: rcode = 0 syserr2str = SUCCESS  
2024 Apr 19 22:50:44.208382 tacacs: find\_tacacs\_servergroup: exiting for server group IsePsnServers index is 2  
2024 Apr 19 22:50:44.208401 tacacs: tacacs\_servergroup\_config: GET\_REQ: find\_tacacs\_servergroup error 0 for Protocol server group IsePsnServers  
2024 Apr 19 22:50:44.208420 tacacs: tacacs\_pss2\_move2key: rcode = 0 syserr2str = SUCCESS  
2024 Apr 19 22:50:44.208433 tacacs: tacacs\_servergroup\_config: GET\_REQ got Protocol server group index:2 name:IsePsnServers  
2024 A2024 Apr 19 22:52024 Apr 19 22:52024 Apr 19 22:5  
Nexus9000#

- Perform a packet capture (In order to see the packet details you must change Wireshark TACACS+ Preferences, and update the shared key used by the Nexus and ISE)

No.	Time	Protocol	Length	Info
66	22:25:08.757401	TACACS+	107	R: Authorization

```

> Transmission Control Protocol, Src Port: 49, Dst Port: 58863, Seq: 1, Ack: 90, Len: 41
  TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 2
    Flags: 0x00 (Encrypted payload, Multiple Connections)
    Session ID: 1136115821
    Packet length: 29
    Encrypted Reply
    Decrypted Reply
      Auth Status: PASS_REPL (0x02)
      Server Msg length: 0
      Data length: 0
      Arg count: 1
      Arg[0] length: 22
      Arg[0] value: shell:roles="helpdesk"

```

- Verify that the shared key is the same on ISE and Nexus side. This can also be checked in Wireshark.

54 22:25:08.701757

... ... TACACS+

121 Q: Authentication

TACACS+

Major version: TACACS+  
Minor version: 1  
Type: Authentication (1)  
Sequence number: 1  
Flags: 0x00 (Encrypted payload, Multiple Connections)  
Session ID: 232251350  
Packet length: 43  
Encrypted Request  
Decrypted Request  
Action: Inbound Login (1)  
Privilege Level: 1  
Authentication type: PAP (2)  
Service: Login (1)  
User len: 9  
User: iseiscool  
Port len: 1  
Port: 0  
Remaddr len: 12  
Remote Address: [REDACTED]  
Password Length: 13  
Password: VainillaISE97

*Authentication Packet*