Configure TACACS with ISE Gigabit Ethernet 1 Interface

Contents

Introduction

Background Information

Prerequisites

- Requirements
- Components Used

Configure

Network Diagram

Configuration of Identity Services Engine for TACACS+

- Configure IP Address for Gigabit Ethernet 1 Interface in ISE
- Enable Device Administration in ISE
- Add a Network Device in ISE
- Configure TACACS+ Command Sets
- Configure the TACACS+ Profile
- Configure TACACS+ Authentication and Authorization Profile
- Configure Network Access Users for NAD's TACACS Authentication in ISE

Configure Router for TACACS+

- Configure Cisco IOS Router for TACACS+ Authentication and Authorization

Configure Switch for TACACS+

- Configure Switch for TACACS+ Authentication and Authorization

Verification

- Verification from Router
- Verification of the Switch

Troubleshoot

- Verification from the Network Device (Switch)
- Verification from the Network Device (Switch)

Reference

Introduction

This document describes ISE TACACS+ configuration with Gigabit Ethernet 1 Interface where router and switches work as network devices.

Background Information

Cisco ISE supports up to 6 Ethernet interfaces. It can only have three bonds; bond 0, 1, and 2. You cannot change the interfaces that are part of a bond or change the role of the interface in a bond.

Prerequisites

Requirements

Cisco recommends that you have knowledge on these topics:

- Basic networking knowledge
- Cisco Identity Service Engine

Components Used

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

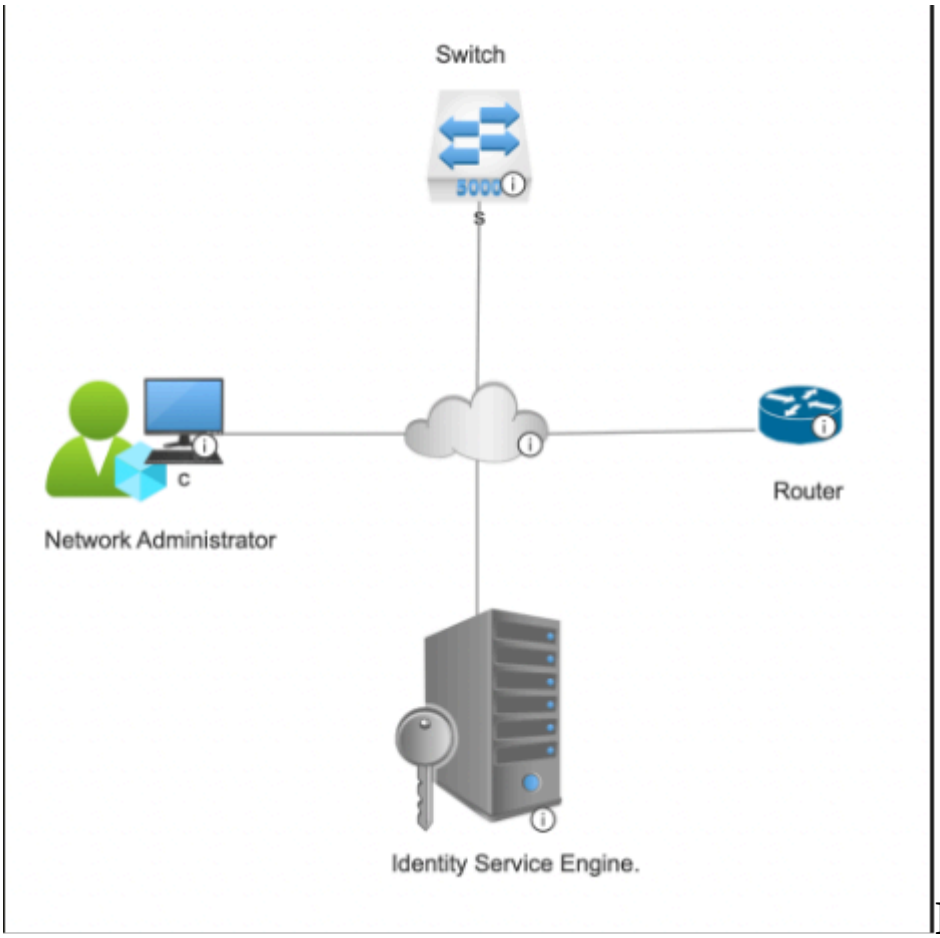
- Cisco C9200 Switch
- Cisco IOS® Software Release 17.x
- Cisco Identity Service Engine v3.3 and above

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.

Configure

The purpose of Configure Gigabit Ethernet 1 of ISE for TACACS+ configuration is to authenticate the router and switch with TACACS+ with ISE as the authentication server.

Network Diagram



Network Topology

Configuration of Identity Services Engine for TACACS+

Configure IP Address for Gigabit Ethernet 1 Interface in ISE

1. Log in to the CLI of the ISE PSN node where the device admin is enabled and verify the available interfaces by running the **show interface** command:

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 629139  bytes 226044590 (215.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 674817  bytes 100272799 (95.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 438392  bytes 363642766 (346.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 481076  bytes 369977760 (352.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1271564  bytes 203676256 (194.2 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 76672  bytes 116577841 (111.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 262  bytes 36180 (35.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7  bytes 606 (606.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 2
        flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:50:56:8b:f8:5f  txqueuelen 1000  (Ethernet)
        RX packets 268  bytes 36228 (35.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 516 (516.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Verification of Interfaces in ISE

Note: In this configuration, only three interfaces are configured in ISE, with a focus on the Gigabit Ethernet 1 interface. The same procedure can be applied to configure the IP address for all interfaces. By default, ISE supports up to six Gigabit Ethernet interfaces.

---

2. From CLI in the same PSN node, assign an IP address to the Gigabit Ethernet 1 Interface by running these commands:

- hostnameofise#**configure t**
- hostnameofise/admin(config)#**interface Gigabit Ethernet 1**
- hostnameofise/admin(config-GigabitEthernet-1)# **<ip address> <subnet netmask> % Changing the IP address might cause ise services to restart**
- **Continue with IP address change?**
- **Proceed? [yes,no] yes**

---

3. Performing Step 2 drives the ISE node services to restart. To verify the status of the ISE services, run the **show application status ise** command and ensure the status of the services is running, similar to the next screenshot:

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          1739169
Database Server                        running          102 PROCESSES
Application Server                     running          1755746
Profiler Database                      running          1746379
ISE Indexing Engine                    running          1757121
AD Connector                           running          1759148
M&T Session Database                   running          1752122
M&T Log Processor                      running          1755926
Certificate Authority Service          running          1759026
EST Service                            running          1786647
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          1743222
ISE API Gateway Database Service       running          1745409
ISE API Gateway Service                running          1750887
ISE pxGrid Direct Service              running          1874179
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          1760519
ISE Prometheus Service                 running          1762540
ISE Grafana Service                    running          1765779
ISE MNT LogAnalytics Elasticsearch     running          1768218
ISE Logstash Service                   running          1773207
ISE Kibana Service                     running          1774914
ISE Native IPSec Service               running          1779658
MFC Profiler                           running          1932013
```

ISE service status verification

---

4. Verify the IP address of the Gig1 interface by running the **show interface** command:

```
honey/admin#show interface
cni-podman1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::8ca9:c4ff:fe1b:6827  prefixlen 64  scopeid 0x20<link>
        ether 8e:a9:c4:1b:68:27  txqueuelen 1000  (Ethernet)
        RX packets 633876  bytes 228753800 (218.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 680052  bytes 102100762 (97.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

cni-podman2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd00::1:8:1  prefixlen 112  scopeid 0x0<global>
        inet6 fe80::304a:47ff:fe59:264a  prefixlen 64  scopeid 0x20<link>
        ether 32:4a:47:59:26:4a  txqueuelen 1000  (Ethernet)
        RX packets 503576  bytes 516105026 (492.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 595701  bytes 383404526 (365.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:1b81  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:1b:81  txqueuelen 1000  (Ethernet)
        RX packets 1387052  bytes 213478717 (203.5 MiB)
        RX errors 0  dropped 266  overruns 0  frame 0
        TX packets 136494  bytes 261900250 (249.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 1
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fe80::250:56ff:fe8b:e1af  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8b:e1:af  txqueuelen 1000  (Ethernet)
        RX packets 5165  bytes 1072036 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2260 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Verification of ISE Gig2 interface IP address from CLI

---

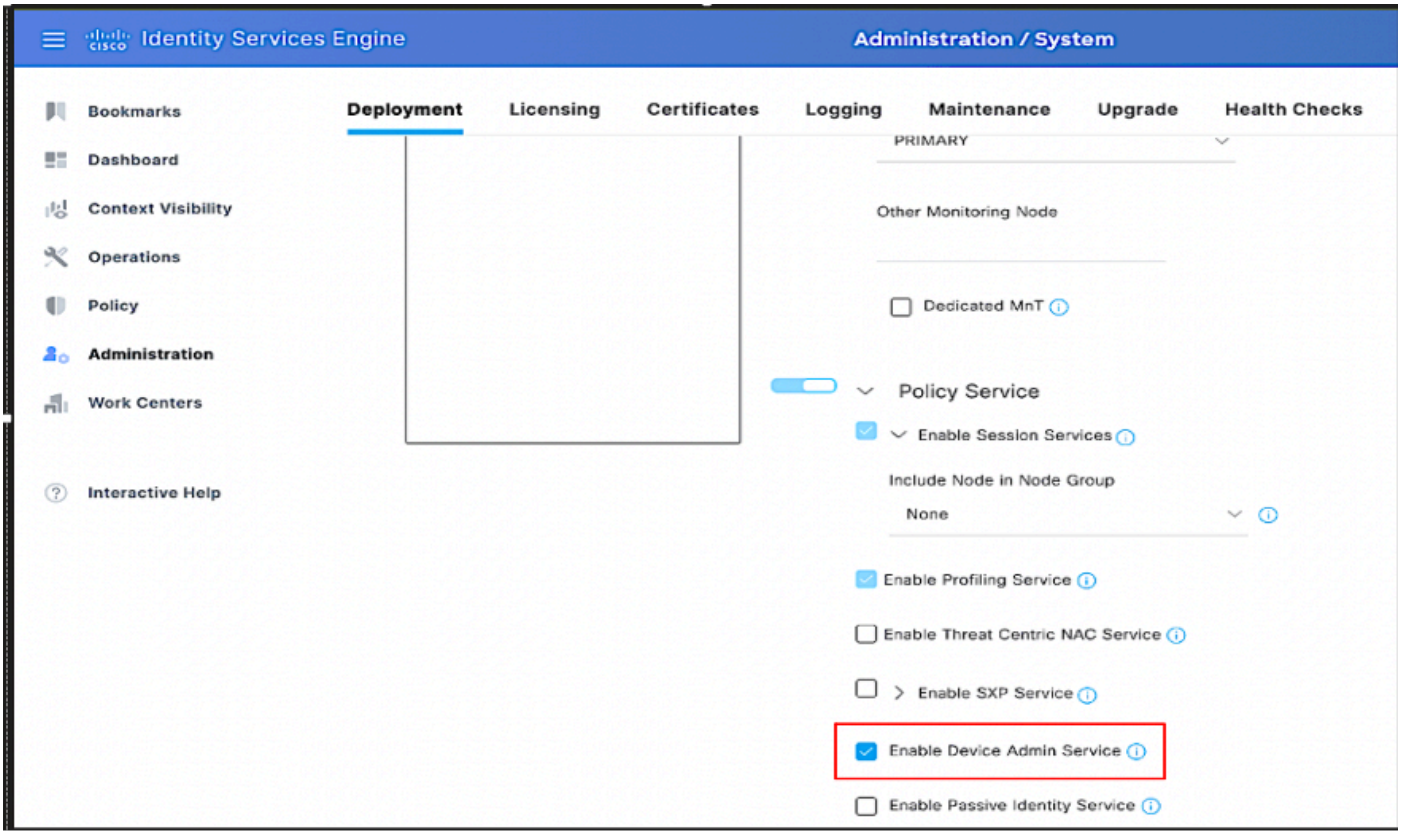
5. Verify the allowance of port 49 in the ISE node by running the **show ports | inc 49** command:

```
honey/admin#show ports | include 49
        tcp: 127.0.0.1:8888, 169.254.4.1:49, 169.254.2.1:49, [redacted]:49, [redacted]:49,
```

verification of port 49 allowance in ISE

Enable Device Administration in ISE

1. Navigate to **GUI of ISE > Administration > Deployment > Select the PSN node**, then check the **Enable Device Admin Service**:

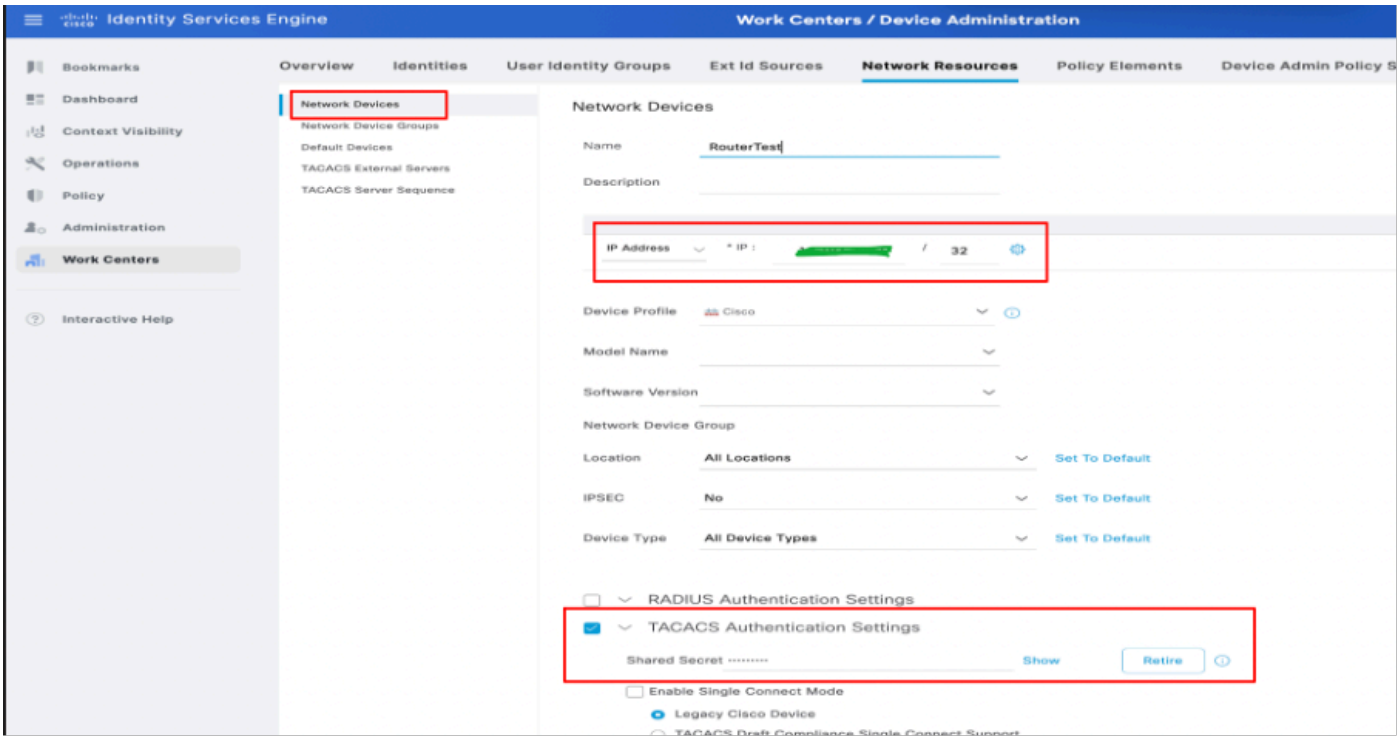


Enabling Device administration service in ISE

Note: To enable the Device Admin service, a Device Administration License is required.

Add a Network Device in ISE

1. Navigate to **Work Centers > Device Administration > Network Resources > Network Devices**. Click **Add** and Provide Name and the IP Address. Select the **TACACS+ Authentication Settings** checkbox and provide the Shared Secret key.



Configuration of Network Device in ISE

---

2. Review the steps for this procedure by adding all required network devices for TACACS authentication.

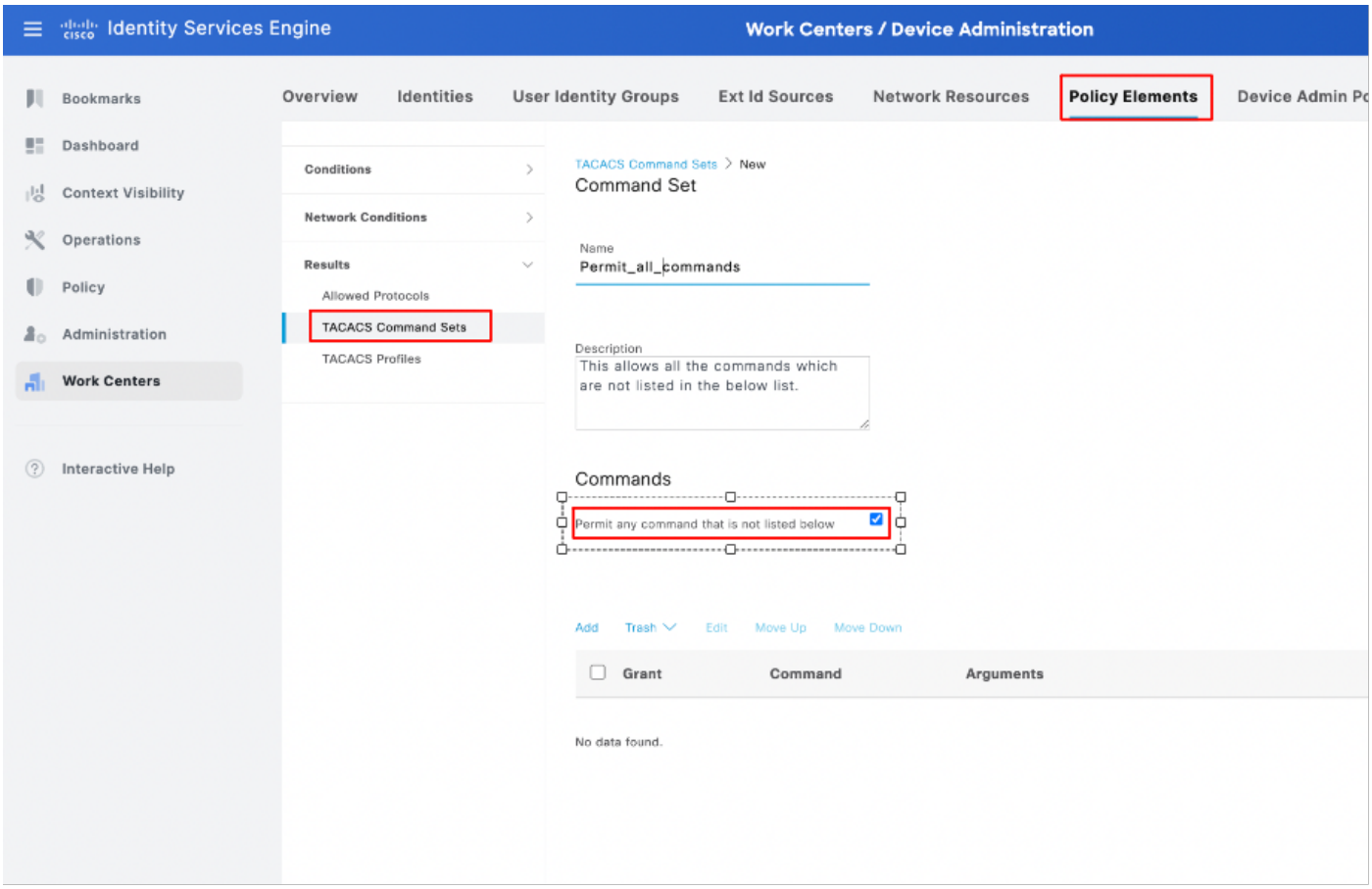
Configure TACACS+ Command Sets

Two command sets are configured for the next demonstration:

- ***Permit_all_commands***, is assigned to the user admin and allows all commands on the device.
- ***permit_show_commands***, is assigned to a user and permits only *show* commands

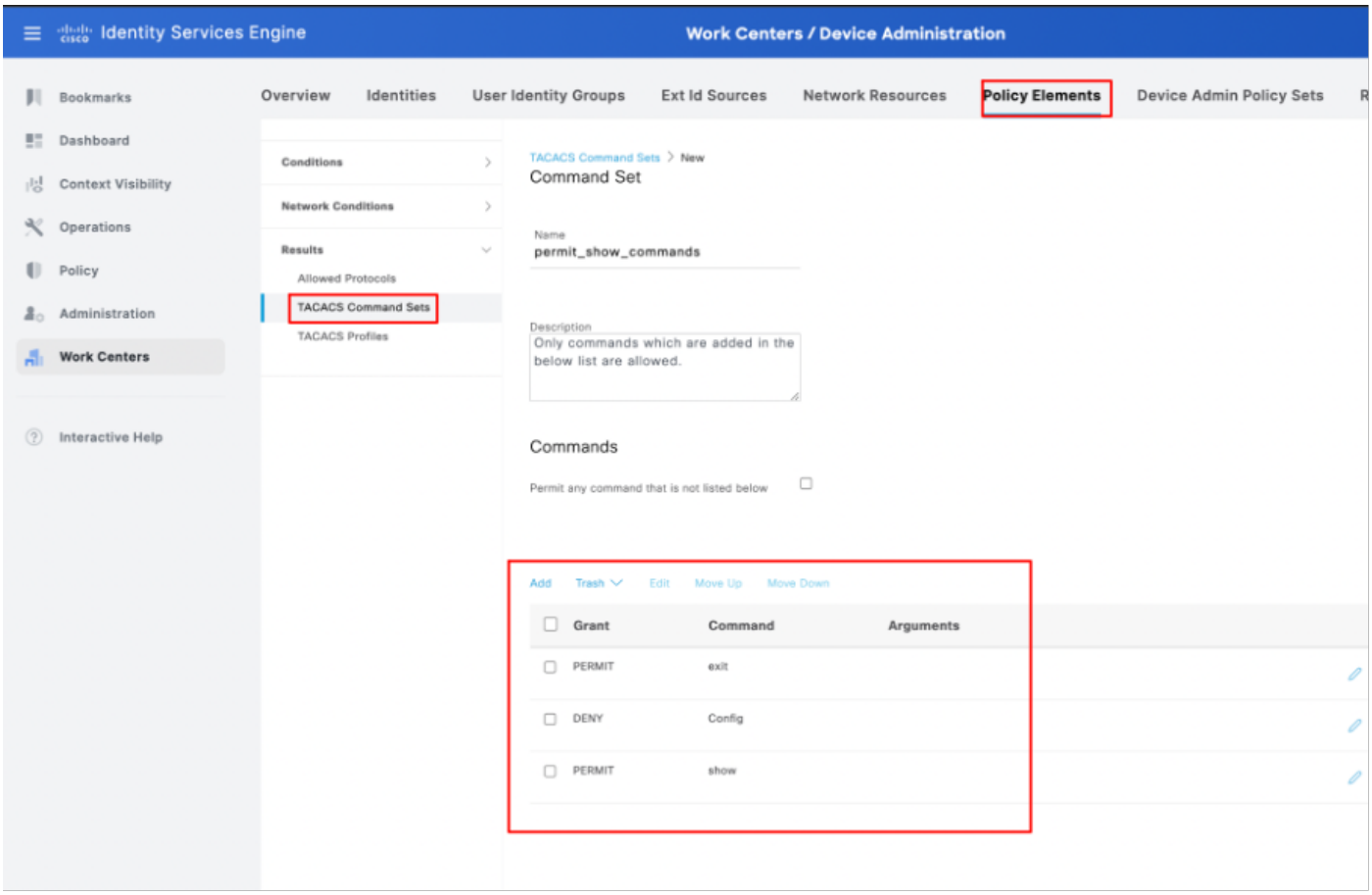
---

1. Navigate to **Work Centers > Device Administration > Policy Results > TACACS Command Sets**. Click **Add** and Provide the Name **PermitAllCommands**, then choose the **Permit any command** checkbox that is not listed and click **Submit.**



Configuration of Command Sets in ISE

2. Navigate to **Work Centers > Device Administration > Policy Results > TACACS Command Sets**.Click **Add** and Provide the Name **PermitShowCommands**, click **Add**, then finally, permit **show** and **exit** commands. By default, if arguments are left blank, all arguments are included. Click **Submit.**



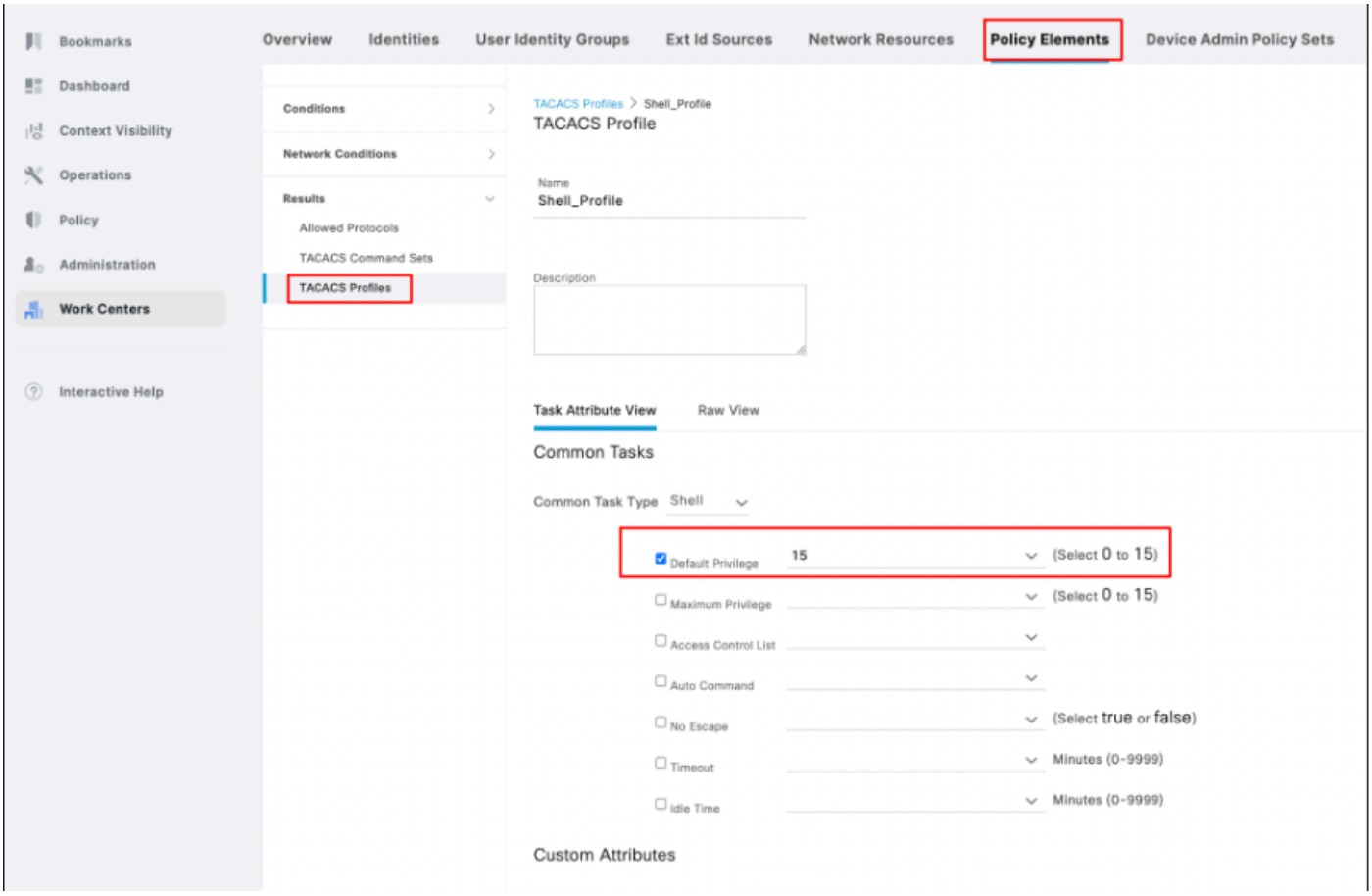
Configuration of permit_show_commands in ISE

Configure the TACACS+ Profile

A single TACACS+ profile is configured, and the command authorization is carried out via command sets.

---

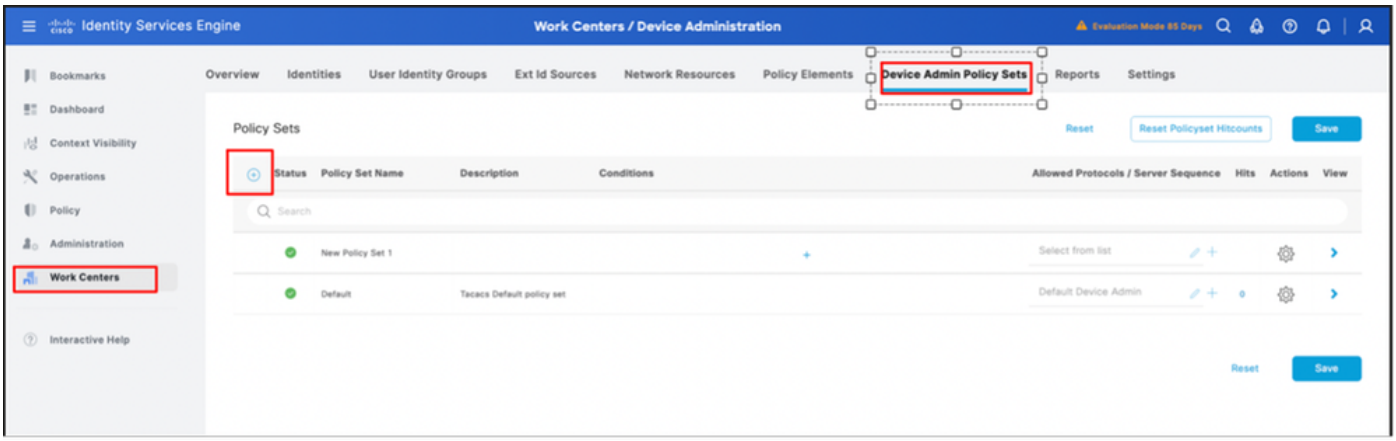
1. To configure a TACACS+ profile, navigate to **Work Centers > Device Administration > Policy Results > TACACS Profiles**. Click **Add** and provide a name for the Shell Profile. Then, select the **Default Privilege** checkbox, and enter the value **15**, and click **Submit**.



Configuration of TACACS profile in ISE

Configure TACACS+ Authentication and Authorization Profile

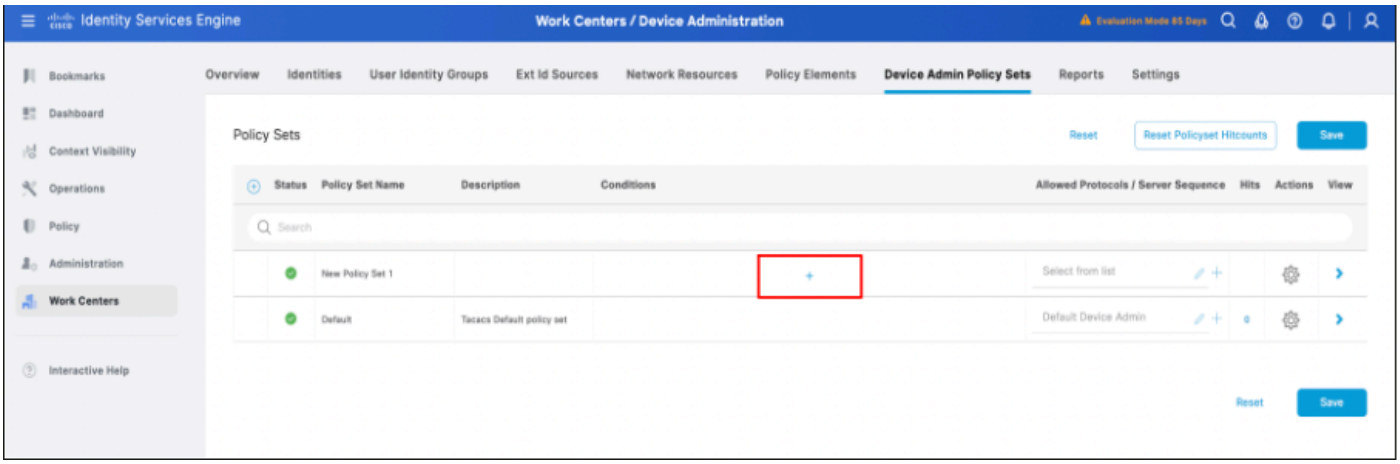
1. Log in to the **ISE PAN GUI > Administration > Work Centers > Device Administration > Device Admin Policy Sets**. Click the + icon to create a new policy. In this example, the policy set is named **New Policy Set 1**.



Configuration of policy set in ISE

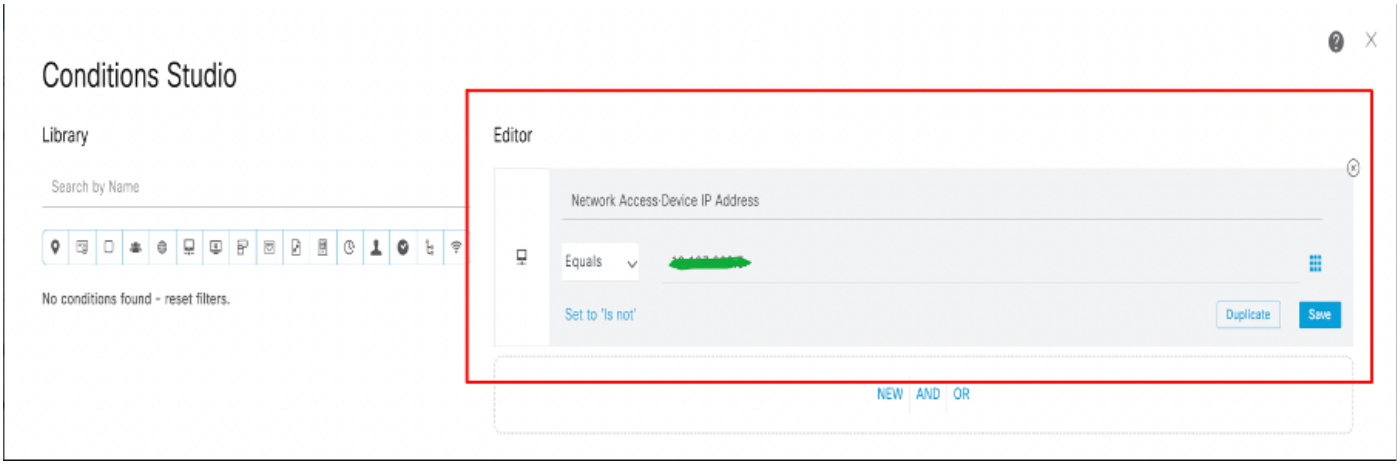
---

2. Before saving the policy set, it is required to configure the conditions. Click the + icon to configure conditions for the policy set.



Configuration of policy set conditions in ISE

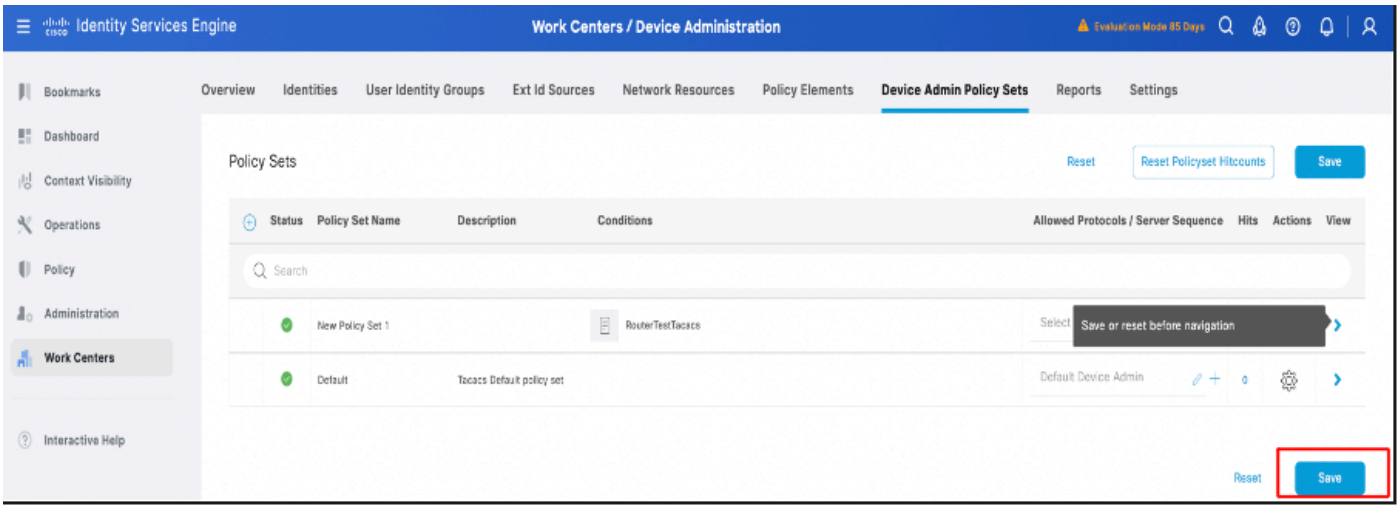
3. After clicking the + icon in Step 2, the conditions studio dialog box opens. Configure the conditions required and **Save** the condition with the new or existing conditions, scroll. Click **Use**.



Configuration of policy set conditions in ISE

Note: For this documentation, the conditions are matched with network device IP. However, the conditions can be varied as per the deployment requirements.

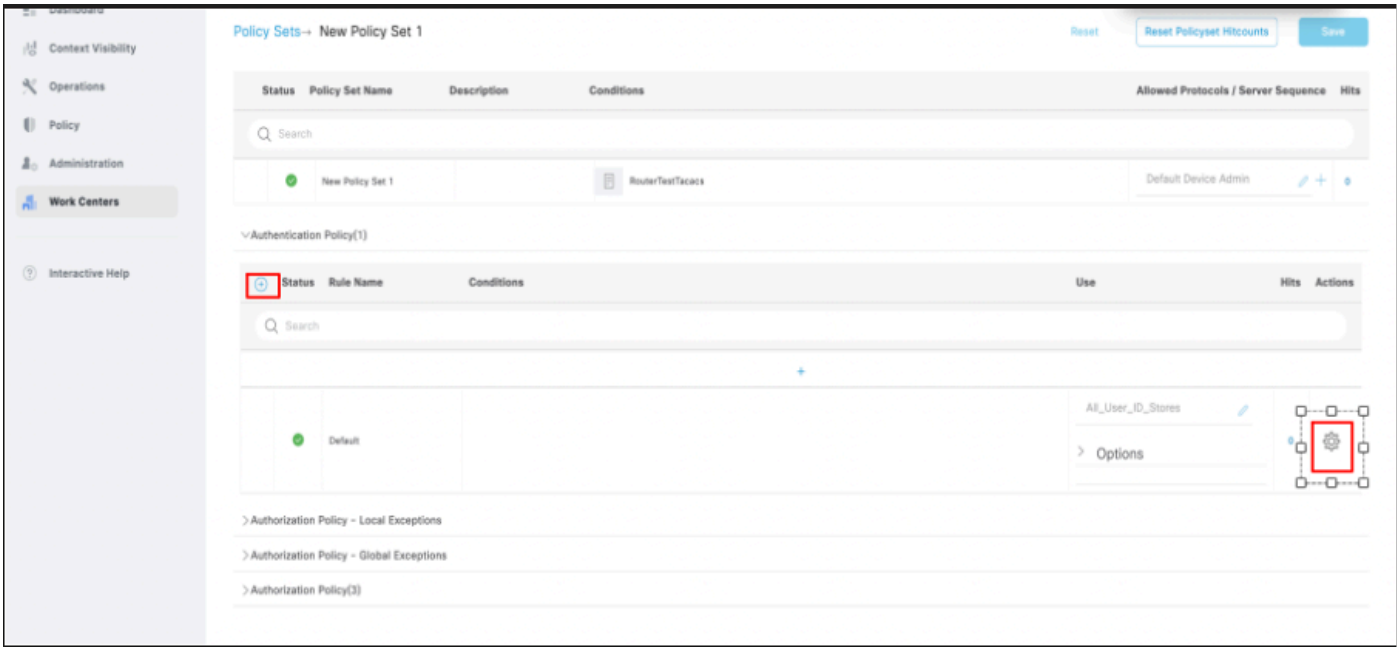
4. After the conditions are configured and saved, configure the allowed protocols as **Default Device Admin.** Save the policy set created by clicking on the **Save** option.



Policy set configuration confirmation.

---

5. Expand the **New Policy Set > Authentication Policy (1) >** Create a new authentication policy by clicking the + Icon or by clicking the **gear icon**. Then, insert a new row.

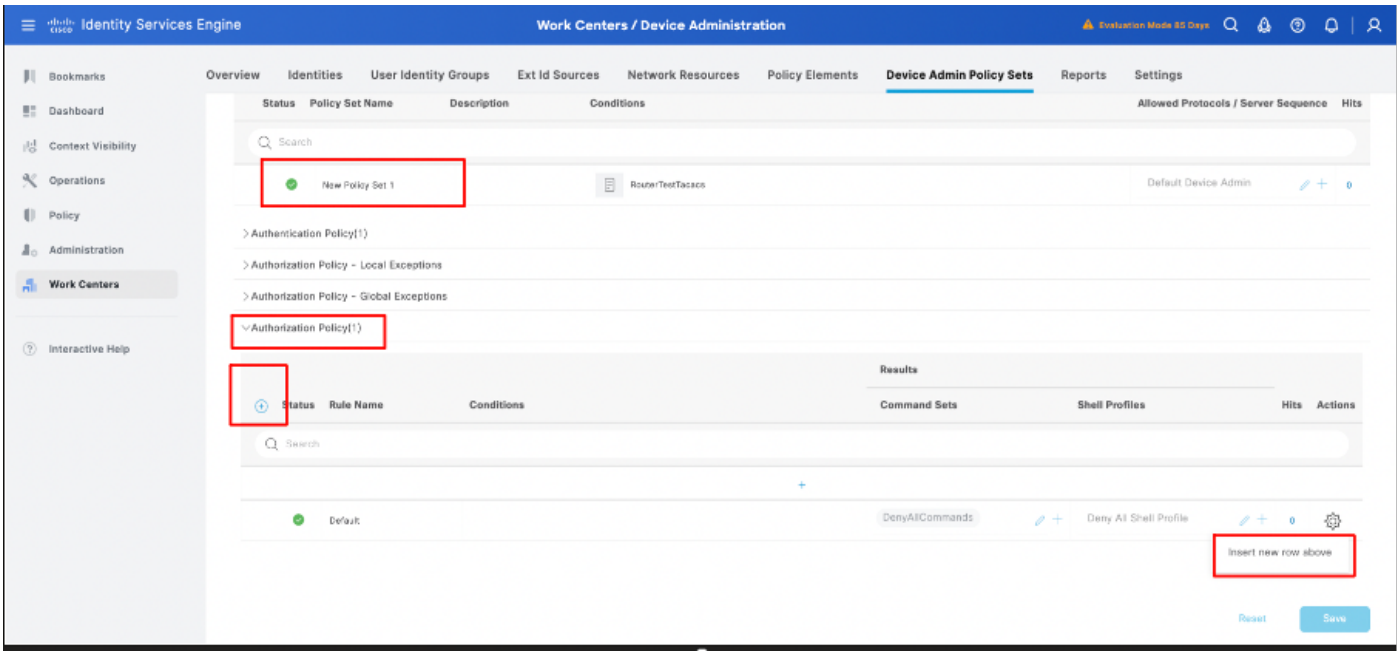


Configuration of Authentication Policy in the policy set.

Note: For this example, the default Authentication Policy Set with All_User_ID_Stores is used. However, the use of the Identity stores is customizable per the deployment requirements.

---

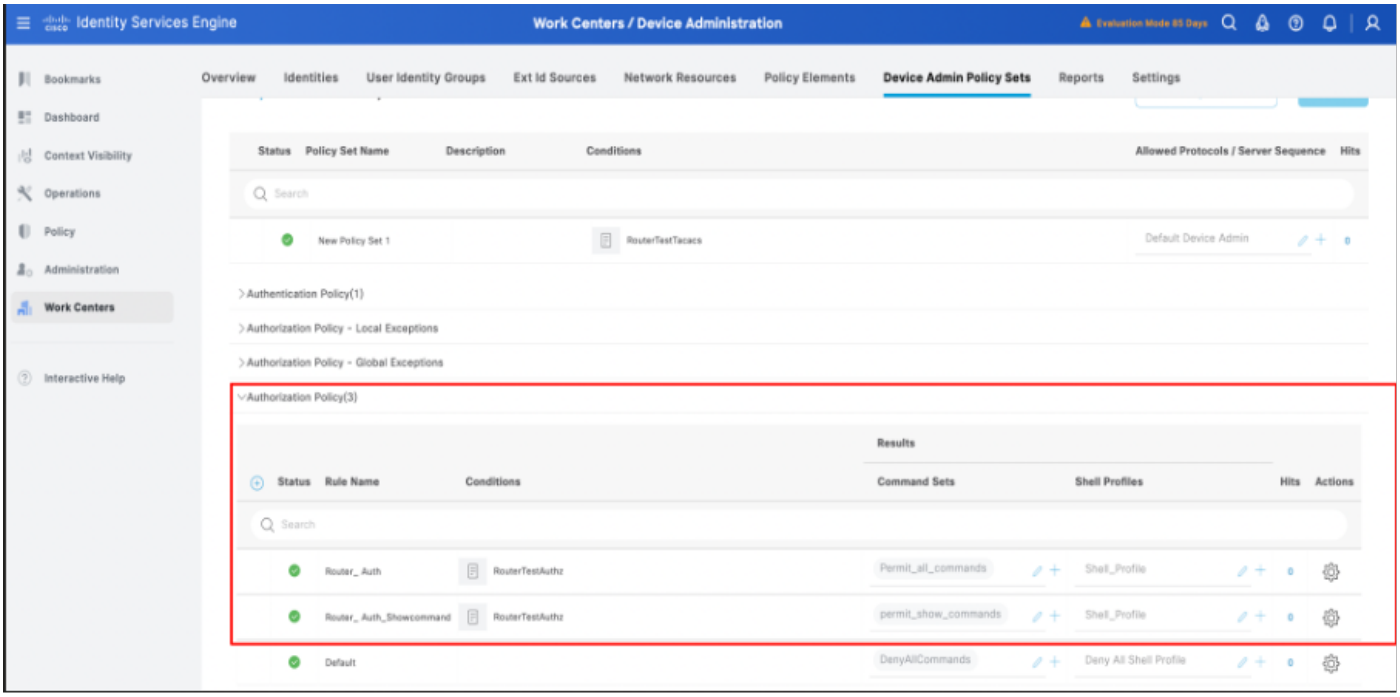
6. Expand the **New Policy Set > Authorization Policy (1)**. Either click the + icon or click the **gear icon**. Then, insert a new row for creating an authorization policy.



Configuration of Authorization Policy

---

7. Configure the Authorization Policy with conditions, command sets, and a Shell profile mapped to the authorization policies.



Complete configuration of Authorization policy in ISE

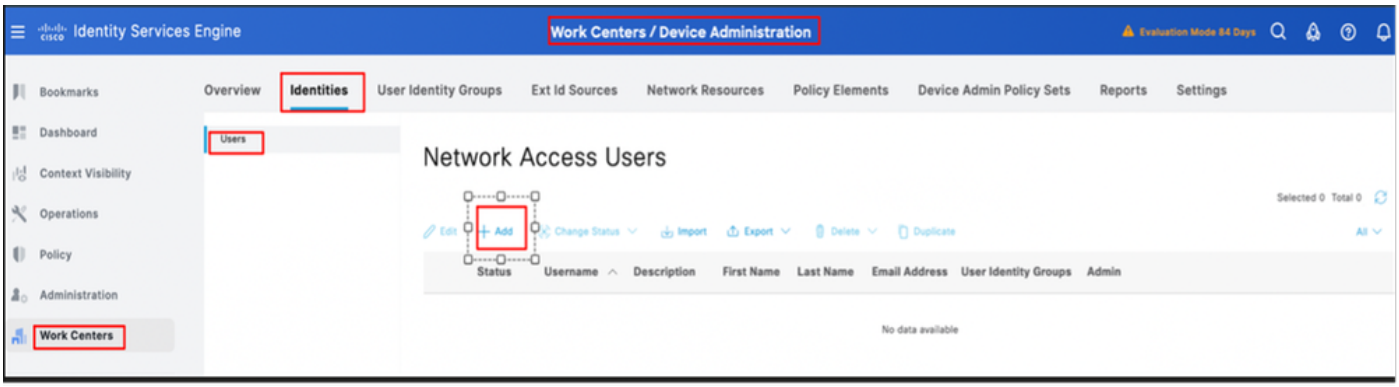
Note: The conditions configured are as per the lab environment and can be configured as per the deployment requirements.

---

8. Review the first 6 steps for configuring Policy Sets for switch and any other network devices used for TACACS+.

Configure Network Access Users for NAD's TACACS Authentication in ISE

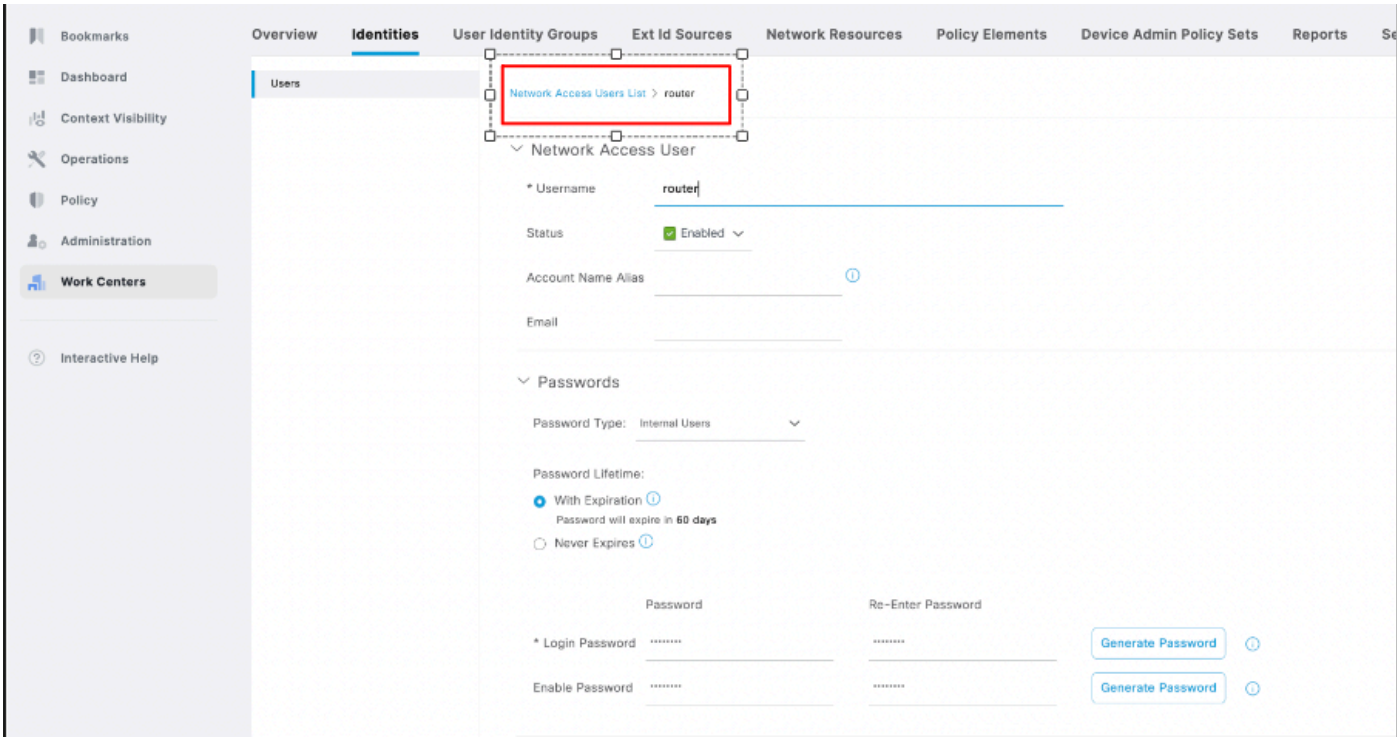
1. Navigate to **Work Centers > Device Administration > Identities > Users**. Click the **+** icon to create a new user.



Configure network access users in ISE

---

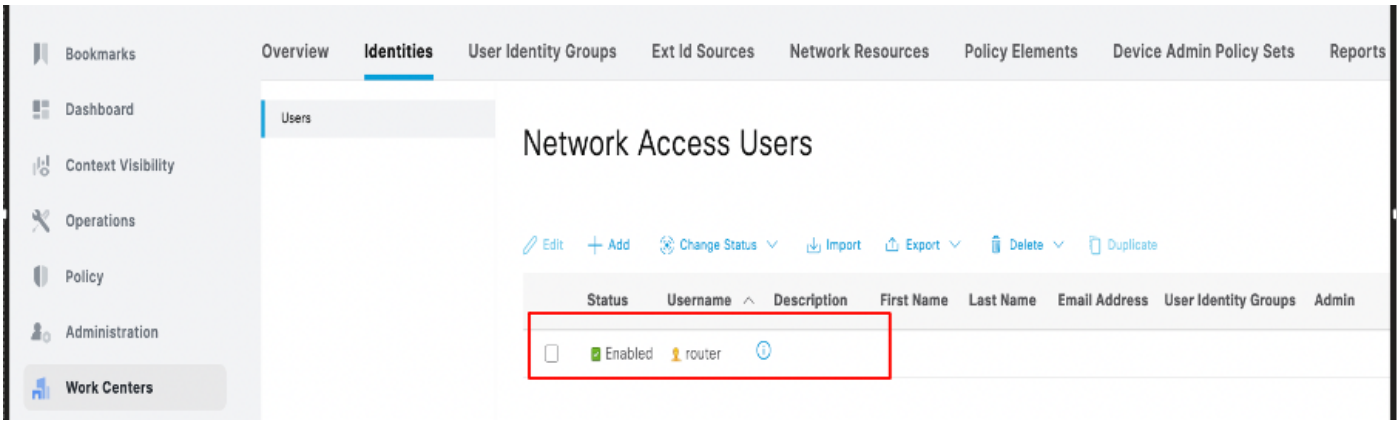
2. Provide the **Username** and **Password** details, map the user to an User Identity Group (optional), then click **Submit**.



Configure network access users - Continue

---

3. After submitting the username configuration in **Work Centers > Identities > Users > Network Access Users**, the user is visibly configured and enabled.



Confirmation of Network access user configuration.

Configure Router for TACACS+

Configure Cisco IOS Router for TACACS+ Authentication and Authorization

1. Log in to the CLI of the router and run these commands for configuring TACACS in the router:

- ASR1001-X(config)#aaa new-model --- **command required to enable aaa in NAD**
- ASR1001-X(config)#aaa session-id common. ----**command required to enable aaa in NAD.**
- ASR1001-X(config)#aaa authentication login default group tacacs+ local
- ASR1001-X(config)#aaa authorization exec default group tacacs+
- ASR1001-X(config)#aaa authorization network list1 group tacacs+
- ASR1001-X(config)#tacacs server ise1
- ASR1001-X(config-server-tacacs)#address ipv4 <IP address of TACACS server > . --- **ISE interface G1 IP address.**
- ASR1001-X(config-server-tacacs)# key XXXXX
- ASR1001-X(config)# aaa group server tacacs+ isegroup
- ASR1001-X(config-sg-tacacs+)#server name ise1
- ASR1001-X(config-sg-tacacs+)#ip vrf forwarding Mgmt-intf
- ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet0
- ASR1001-X(config-sg-tacacs+)#ip tacacs source-interface GigabitEthernet1
- ASR1001-X(config)#exit

---

2. After saving the router TACACS+ configurations, verify the TACACS+ configuration by running the **show run aaa** command:

ASR1001-X#show run aaa

```
!
aaa authentication login default group isegroup local
aaa authorization exec default group isegroup
aaa authorization network list1 group isegroup
username admin password 0 XXXXXXX
!
tacacs server ise1
 address ipv4 <IP address of TACACS server>
 key XXXXX
!
!
aaa group server tacacs+ isegroup
 server name ise1
 ip vrf forwarding Mgmt-intf
 ip tacacs source-interface GigabitEthernet1
!
!
!
aaa new-model
aaa session-id common
```

!

!

Configure Switch for TACACS+

Configure Switch for TACACS+ Authentication and Authorization

1. Log in to the CLI of the switch and run these commands for configuring TACACS in the switch:

- C9200L-48P-4X#configure t
- Enter configuration commands, one per line. End with CNTL/Z.
- C9200L-48P-4X(config)#aaa new-model. --- **command required to enable aaa in NAD**
- C9200L-48P-4X(config)#aaa session-id common. --- **command required to enable aaa in NAD.**
- C9200L-48P-4X(config)#aaa authentication login default group isegroup local
- C9200L-48P-4X(config)#aaa authorization exec default group isegroup
- C9200L-48P-4X(config)#aaa authorization network list1 group isegroup
- C9200L-48P-4X(config)#tacacs server ise1
- C9200L-48P-4X(config-server-tacacs)#address ipv4 <IP address of TACACS server> -- I**SE Interface G1 IP address.**
- C9200L-48P-4X(config-server-tacacs)#key XXXXX
- C9200L-48P(config)#aaa group server tacacs+ isegroup
- C9200L-48P(config-sg-tacacs+)#server name ise1
- C9200L-48P-4X(config)#exit
- C9200L-48P-4X#wr mem



Note: In the NAD TACACS+ configuration, **tacacs+** is the group that can be customized per the deployment requirements.

---

2. After saving the switch TACACS+ configurations, verify the TACACS+ configuration by running the **show run aaa** command.

C9200L-48P#show run aaa

!

aaa authentication login default group isegroup local

```
aaa authorization exec default group isegroup

aaa authorization network list1 group isegroup

username admin password 0 XXXXX

!

!

tacacs server ise1

 address ipv4 <IP address of TACACS server>

 key XXXXX

!

!

aaa group server tacacs+ isegroup

 server name ise1

!

!

!

aaa new-model

aaa session-id common

!

!
```

Verification

Verification from Router

From the CLI of the router, verity the authentication of TACACS+ against ISE with Gigabit Ethernet 1 interface by running the **test aaa group tacacsgroupname username password new** command.

This is a sample output from the router and ISE:

Verification of port 49 from Router:

ASR1001-X#telnet ISE Gig 1 interface IP 49

Trying to ISE GIg 1 interface IP, 49... Open

ASR1001-X#test aaa group isegroup router XXXX new

Sending password

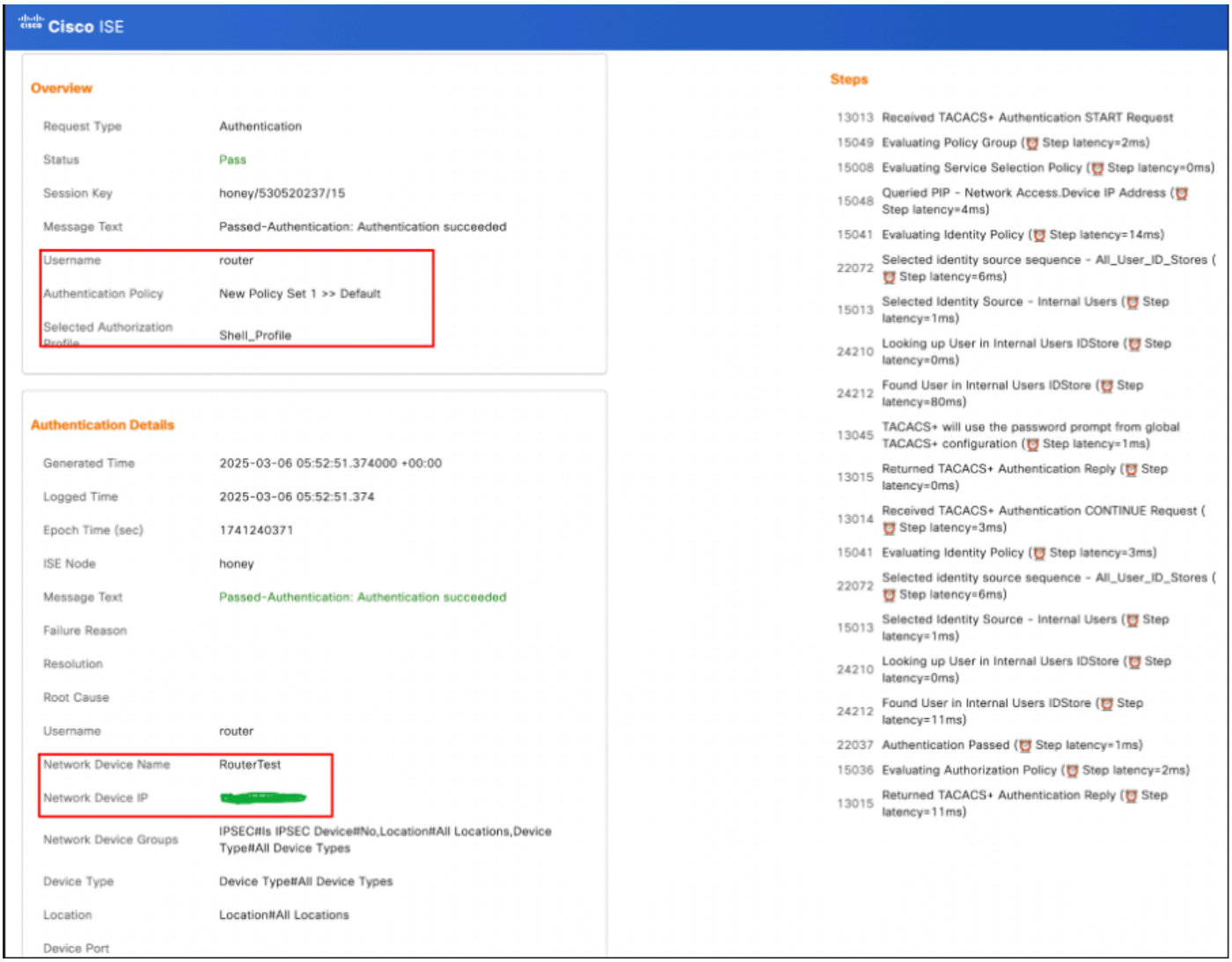
User successfully authenticated

USER ATTRIBUTES

username 0 "router"

reply-message 0 "Password:"

For verification from ISE, log in to the **GUI > Operations > TACACS live logs**, then filter with the router IP in the **Network Device Details** field:



TACACS live logs from ISE - Router Verification.

Verification of the Switch

From the CLI of the switch, verify the authentication of TACACS+ against ISE with Gigabit Ethernet 1 interface by running the **test aaa group tacacsgroupname username password newn** command:

This is a sample output from the switch and ISE:

Verification of port 49 from switch:

C9200L-48P# telnet ISE Gig1 interface IP 49

Trying to ISE Gig1 interface IP, 49... Open

C9200L-48P#test aaa group isegroup switch XXXX new

Sending password

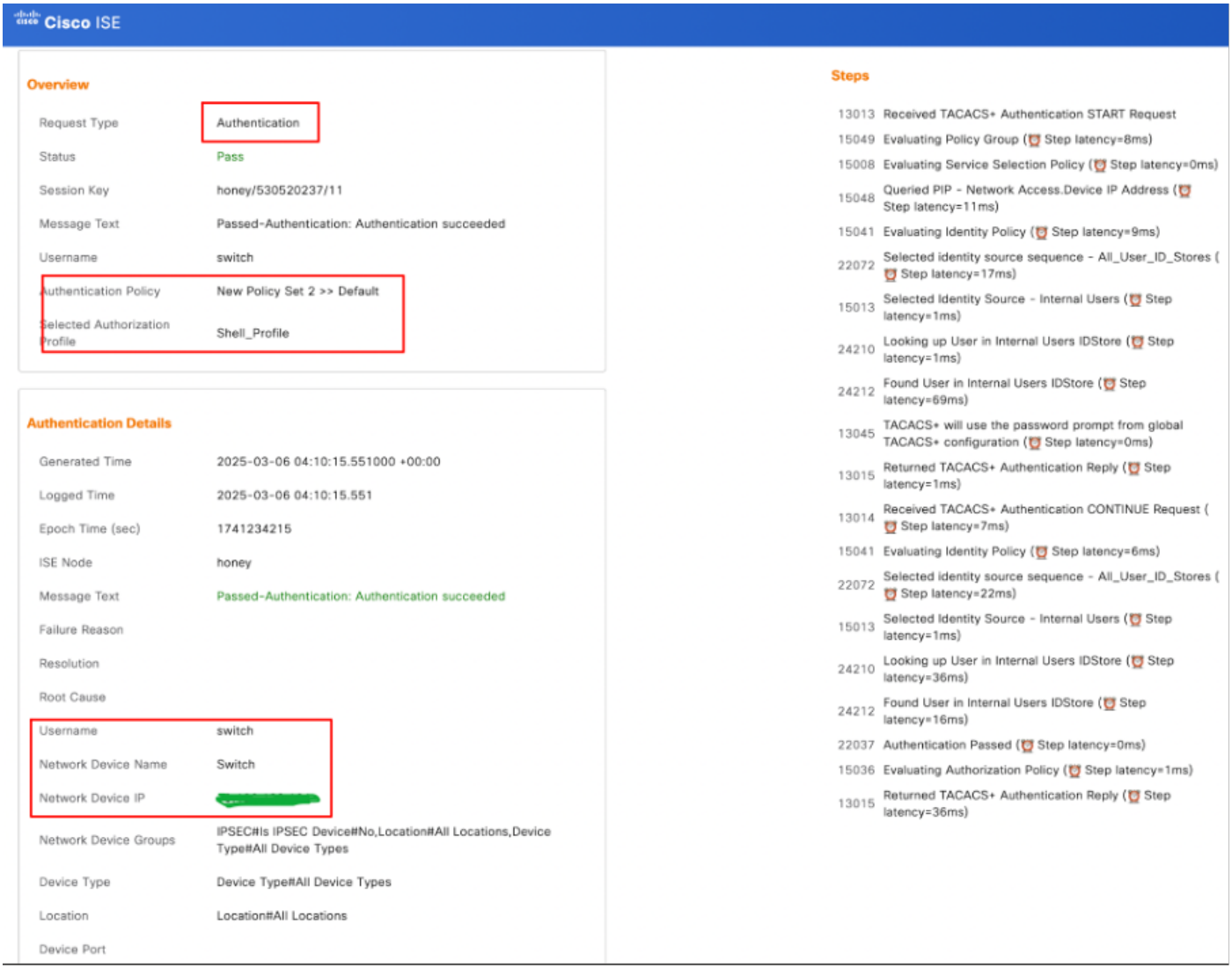
User successfully authenticated

USER ATTRIBUTES

username 0 "switch"

reply-message 0 "Password:"

For verification from ISE, log in to the **GUI > Operations > TACACS live logs**, then filter with the switch IP in the **Network Device Details** field.



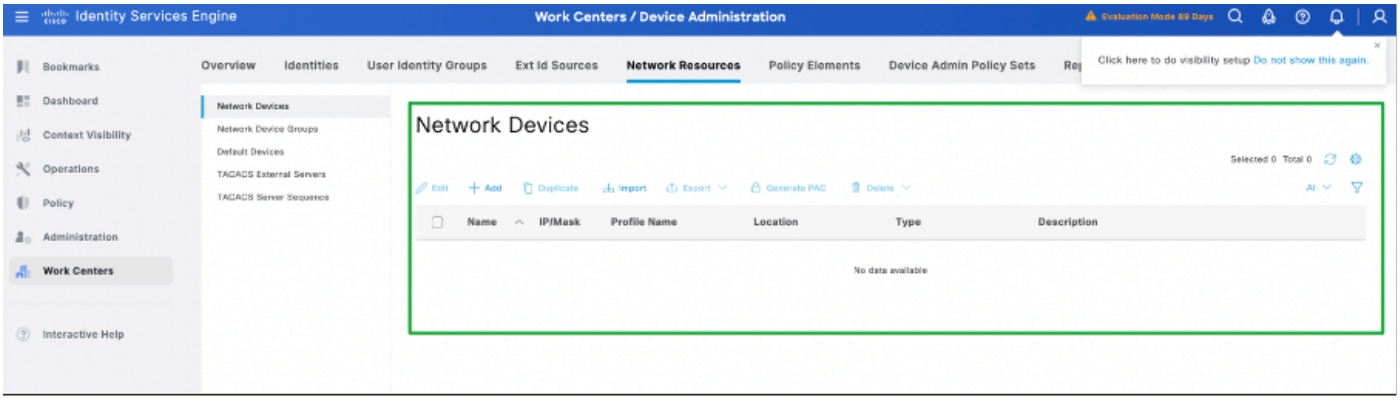
TACACS live logs from ISE - Switch verification.

Troubleshoot

This section discusses some common issues related to TACACS+ authentications.

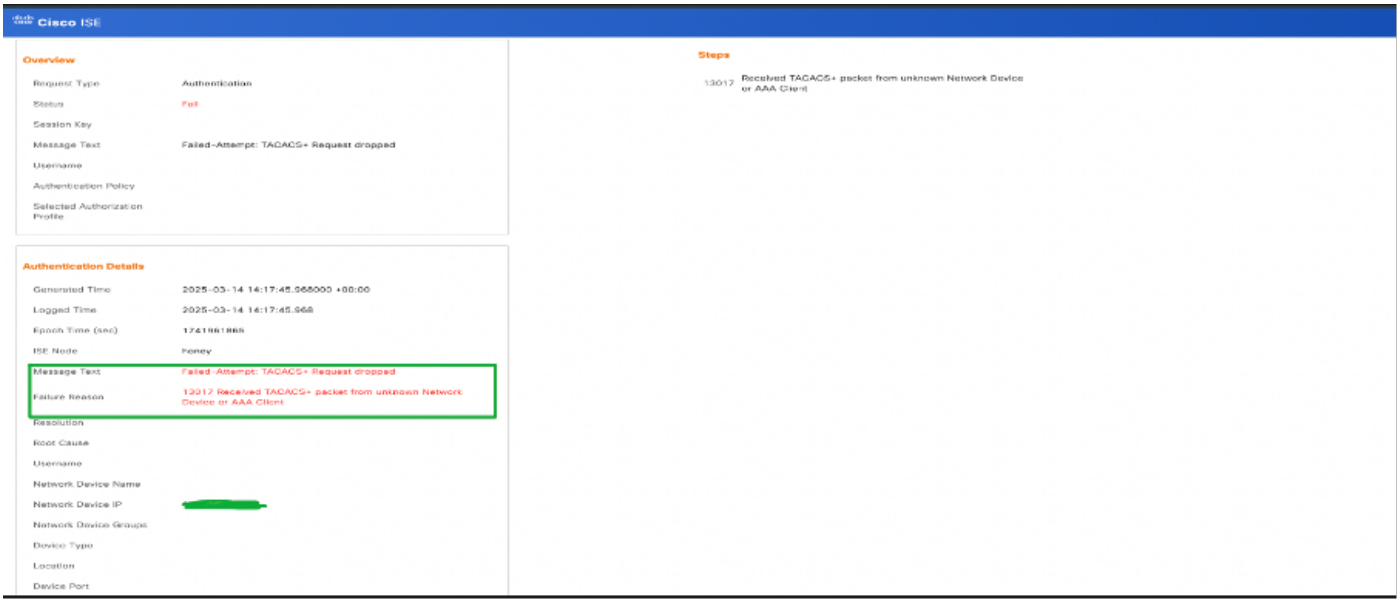
Scenario 1: TACACS+ authentication fails with "**Error: 13017 Receved TACACS+ packet from unknown Network Device or AAA Client**".

This scenario occurs when the network device is not added as Network Resources in ISE. In the next screenshot, the switch is not added in the network resources of ISE.



Troubleshooting scenario - Network devices are not added in ISE.

When testing the authentication from the switch/network device, the packet reaches ISE as expected. However, the authentication fails with the error "**Error: 13017 Received TACACS+ packet from unknown Network Device or AAA Client**."



TACACS live logs - Failure when network device is not added to ISE.

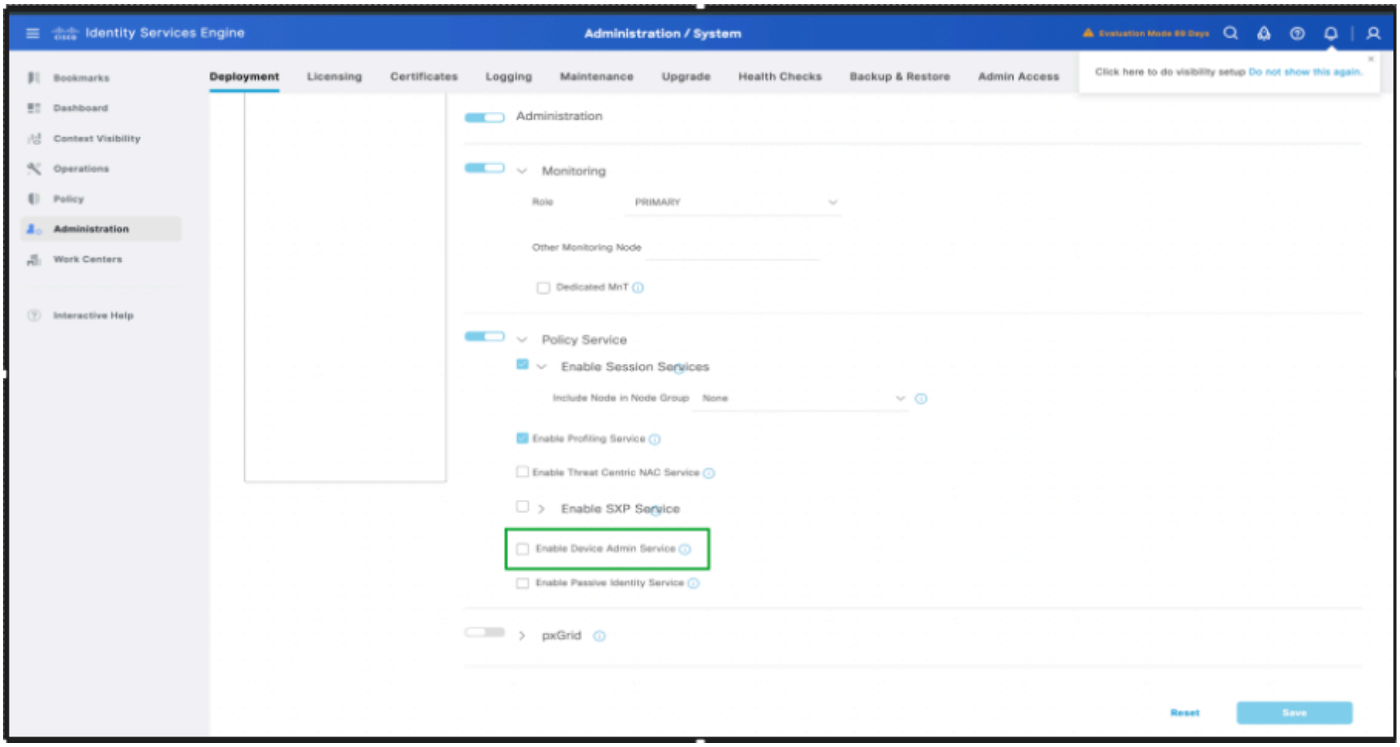
Verification from the Network Device (Switch)

```
Switch#test aaa group isegroup switch XXXXXX new
User rejected
```

Solution: Verify if the switch/router/network device is added as the **Network device in ISE**. If the device is not added, add the network device to the network device list in ISE.

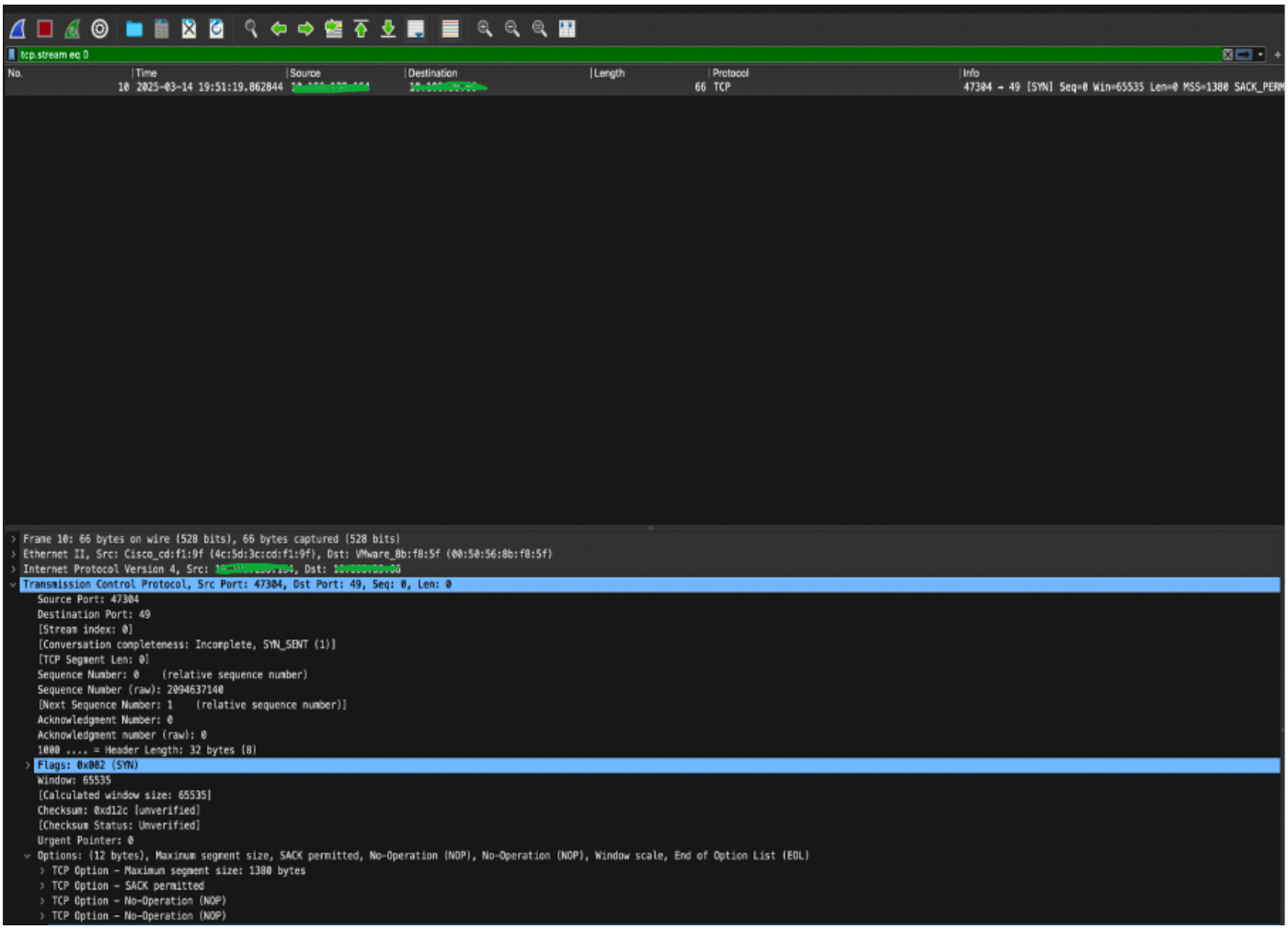
Scenario 2: ISE drops the TACACS+ packet silently without any information

This scenario occurs when the Device Administration Service is disabled in ISE. In this scenario, ISE drops the packet and no live logs are seen even though authentication is initiated from the network device which is added to the Network Resources of ISE. In this screenshot, Device Administration is disabled in ISE.



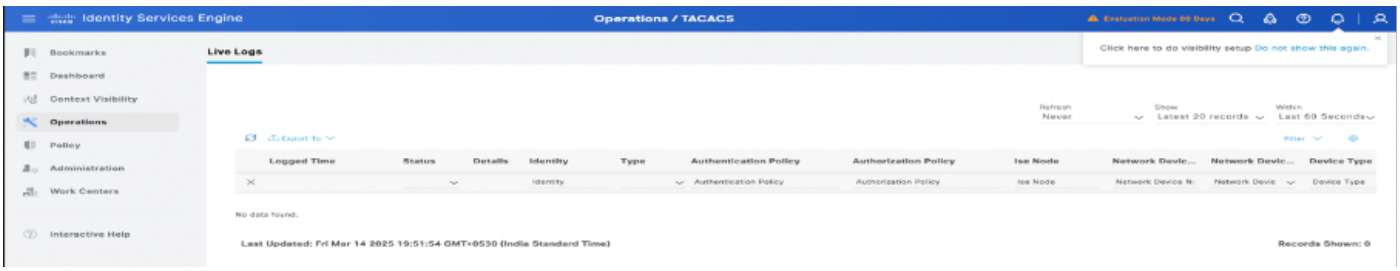
Scenario, device administration is not enabled in ISE.

When a user initiates authentication from the network device, ISE silently drops the packets without any information in the live logs and ISE does not respond to the Syn packet sent by the network device to complete the TACACS authentication process.



ISE dropping packets silently during TACACS

ISE shows **no live logs** during authentication.



No TACACS live logs - Verification from ISE

Verification from the Network Device (Switch)

Switch#
Switch#test aaa group isegroup switch XXXX new
User rejected
Switch#
*Mar 14 13:54:28.144: T+: Version 192 (0xC0), type 1, seq 1, encryption 1, SC 0
*Mar 14 13:54:28.144: T+: session_id 10158877 (0x9B031D), dlen 14 (0xE)
*Mar 14 13:54:28.144: T+: type:AUTHEN/START, priv_lvl:15 action:LOGIN ascii
*Mar 14 13:54:28.144: T+: svc:LOGIN user_len:6 port_len:0 (0x0) raddr_len:0 (0x0) data_len:0

```
*Mar 14 13:54:28.144: T+: user:  switch
*Mar 14 13:54:28.144: T+: port:
*Mar 14 13:54:28.144: T+: rem_addr:
*Mar 14 13:54:28.144: T+: data:
*Mar 14 13:54:28.144: T+: End Packet
```

Solution: Enable **Device Administration** in ISE.

Reference

- Troubleshoot TACACS Authentication Issues
- Cisco Identity Services Engine Administrator Guide, Release 3.3
- VRF for TACACS Servers