

# Configure TACACS+ over TLS 1.3 on a Nexus Device with ISE

## Contents

---

### [Introduction](#)

[Overview](#)

[Using this Guide](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Licensing](#)

### [Configure ISE for Device Admin](#)

[Generate Certificate Signing Request for TACACS+ Server Authentication](#)

[Upload Root CA Certificate for TACACS+ Server Authentication](#)

[Bind the Signed Certificate Signing Request \(CSR\) to ISE](#)

[Enable TLS 1.3](#)

[Enable Device Administration on ISE](#)

[Enable TACACS Over TLS](#)

[Network Device and Network Device Groups](#)

[Configure Identity Stores](#)

[Configure TACACS+ Shell Profiles](#)

[NX-OS Admin](#)

[NX-OS HelpDesk](#)

[Configure Device Admin Policy Sets](#)

### [Configure Cisco NX-OS for TACACS+ over TLS](#)

[TACACS+ Server Configuration](#)

[Trustpoint Configuration](#)

[TACACS+ TLS Configuration](#)

[AAA Configuration](#)

### [Test and Troubleshoot User Access for NX-OS](#)

[Verification](#)

[Troubleshooting](#)

---

## Introduction

This document describes an example for TACACS+ over TLS with Cisco Identity Services Engine (ISE) as server and a Cisco NX-OS device as client.

## Overview

The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol [RFC8907] enables centralized device administration for routers, network access servers, and other networked devices through

one or more TACACS+ servers. It provides authentication, authorization, and accounting (AAA) services, specifically tailored for device administration use cases.

TACACS+ over TLS 1.3 [RFC8446] enhances the protocol by introducing a secure transport layer, safeguarding highly sensitive data. This integration ensures confidentiality, integrity, and authentication for the connection and network traffic between TACACS+ clients and servers.

## Using this Guide

This guide divides the activities into two parts to enable ISE to manage administrative access for Cisco NX-OS based network devices.

- Part 1 – Configure ISE for Device Admin
- Part 2 – Configure Cisco NX-OS for TACACS+ over TLS

## Prerequisites

### Requirements

Prerequisites to configure TACACS+ over TLS:

- A Certificate Authority (CA) to sign the certificate used by TACACS+ over TLS to sign the certificates of ISE and network devices.
- The root certificate from the Certificate Authority (CA).
- Network devices and ISE have DNS reachability and can resolve hostnames.

### Components Used

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

- ISE VMware virtual appliance, Release 3.4 patch 2.
- Nexus 9000 switch model C9364D-GX2A, Cisco NX-OS version 10.5(3t).

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.

### Licensing

A Device Administration license allows you to use TACACS+ services on a Policy Service node. In a high availability (HA) standalone deployment, a Device Administration license permits you to use TACACS+ services on a single Policy Service node in the HA pair.

## Configure ISE for Device Admin

### Generate Certificate Signing Request for TACACS+ Server Authentication

Step 1. Log in to the ISE **admin web portal** using one of the supported browsers.

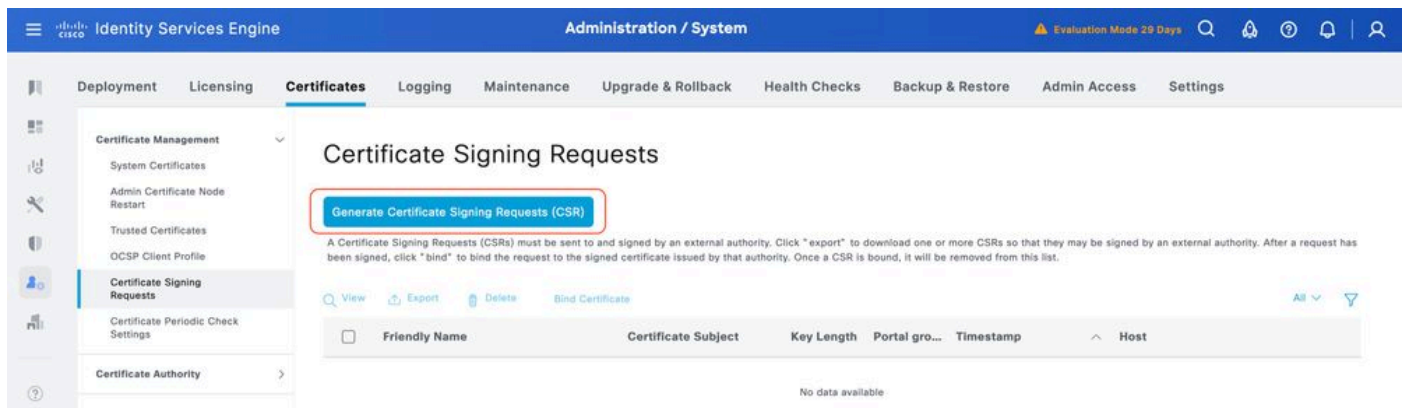
By default, ISE uses a self-signed certificate for all services. The first step is to generate a Certificate Signing Request (CSR) to have it signed by our Certificate Authority (CA).

Step 2. Navigate to **Administration > System > Certificates**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes the Cisco logo and the text 'Identity Services Engine'. A notification banner at the top right states: 'Your Evaluation license expires in 83 days. You will be notified when the license expires.' Below the notification, there are four tabs: 'Summary', 'Endpoints', 'Guests', and 'Vulnerability'. The 'Summary' tab is selected. The main content area displays a table with the following columns: 'Name', 'Status', and 'Actions'. The table is currently empty.

| Name | Status | Actions |
|------|--------|---------|
|------|--------|---------|

Step 3. Under **Certificate Signing Requests**, click **Generate Certificate Signing Request**.



Step 4. Select **TACACS** in **Usage**.

## Usage

Certificate(s) will be used for **TACACS** 

---

Allow Wildcard Certificates ☐ 

Step 5. Select the **PSNs** that has TACACS+ enabled.

## Node(s)

Generate CSR's for these Nodes:

| Node                                     | CSR Friendly Name |
|------------------------------------------|-------------------|
| <input checked="" type="checkbox"/> ISE1 | ISE1#TACACS       |

Step 6. Fill the **Subject** fields with the appropriate information.

## Subject

Common Name (CN)  
\$FQDN\$



Organizational Unit (OU)  
CX



Organization (O)  
Cisco



City (L)  
Raleigh

State (ST)  
North Carolina

Country (C)  
US

Step 7. Add the **DNS Name** and **IP Address** under **Subject Alternative Name (SAN)**.

### Subject Alternative Name (SAN)

|   |            |   |                |   |   |   |
|---|------------|---|----------------|---|---|---|
| ⋮ | DNS Name   | ▼ | ISE1.lab       | — | + |   |
| ⋮ | IP Address | ▼ | 10.225.253.209 | — | + | ① |

Step 8. Click **Generate** and then **Export**.



Now, you can have the certificate (CRT) signed by your Certificate Authority (CA).

## Upload Root CA Certificate for TACACS+ Server Authentication

Step 1. Navigate to **Administration > System > Certificates**. Under **Trusted Certificates**, click **Import**.

| <input type="checkbox"/> | Friendly Name               | Trusted For                      | Serial Number    | Issued To            | Issued By            | Valid From       | Expiration Date   | Status |
|--------------------------|-----------------------------|----------------------------------|------------------|----------------------|----------------------|------------------|-------------------|--------|
| <input type="checkbox"/> | Amazon root CA              | Infrastructure<br>Cisco Services | 06 6C 9F CF ...  | Amazon Root CA 1     | Amazon Root CA 1     | Tue, 26 May 2015 | Sun, 17 Jan 2...  | Enr    |
| <input type="checkbox"/> | Cisco ECC Root CA 2099      | Cisco Services                   | 03               | Cisco ECC Root CA    | Cisco ECC Root CA    | Thu, 4 Apr 2013  | Mon, 7 Sep 2...   | Enr    |
| <input type="checkbox"/> | Cisco Licensing Root CA     | Cisco Services                   | 01               | Cisco Licensing R... | Cisco Licensing R... | Thu, 30 May 2013 | Sun, 30 May 2...  | Enr    |
| <input type="checkbox"/> | Cisco Manufacturing CA SHA2 | Endpoints<br>Infrastructure      | 02               | Cisco Manufactur...  | Cisco Root CA M2     | Mon, 12 Nov 2012 | Thu, 12 Nov 2...  | Enr    |
| <input type="checkbox"/> | Cisco Root CA 2048          | Endpoints<br>Infrastructure      | 5F F8 7B 28 2... | Cisco Root CA 20...  | Cisco Root CA 20...  | Fri, 14 May 2004 | Mon, 14 May ...   | Dis    |
| <input type="checkbox"/> | Cisco Root CA 2099          | Cisco Services                   | 01 9A 33 58 7... | Cisco Root CA 20...  | Cisco Root CA 20...  | Tue, 9 Aug 2016  | Sun, 9 Aug 20...  | Enr    |
| <input type="checkbox"/> | Cisco Root CA M1            | Cisco Services                   | 2E D2 0E 73 4... | Cisco Root CA M1     | Cisco Root CA M1     | Tue, 18 Nov 2008 | Fri, 18 Nov 20... | Enr    |
| <input type="checkbox"/> | Cisco Root CA M2            | Infrastructure<br>Endpoints      | 01               | Cisco Root CA M2     | Cisco Root CA M2     | Mon, 12 Nov 2012 | Thu, 12 Nov 2...  | Enr    |
| <input type="checkbox"/> | Cisco RXC-R2                | Cisco Services                   | 01               | Cisco RXC-R2         | Cisco RXC-R2         | Wed, 9 Jul 2014  | Sun, 9 Jul 2034   | Enr    |

Step 2. Select the **certificate** issued by the Certificate Authority (CA) that signed your TACACS Certificate Signing Request (CSR). Make sure that the **Trust for authentication within ISE** option is enabled.

## Import a new Certificate into the Certificate Store

\* Certificate File  ISE SVSLab CA.crt

Friendly Name

Trusted For: ☐

- ☒ Trust for authentication within ISE
- ☐ Trust for client authentication and Syslog
  - ☐ Trust for certificate based admin authentication
- ☐ Trust for authentication of Cisco Services
- ☐ Trust for Native IPSec certificate based authentication
- ☐ Validate Certificate Extensions

Description

Submit

Cancel

Click **Submit**. The certificate must now appear under **Trusted Certificates**.

| <input type="checkbox"/> | Friendly Name                           | Trusted For                                                | Serial Number    | Issued To            | Issued By            | Valid From       | Expiration Date   | Status |
|--------------------------|-----------------------------------------|------------------------------------------------------------|------------------|----------------------|----------------------|------------------|-------------------|--------|
| <input type="checkbox"/> | CN=SVS LabCA, OU=SVS, O=Cisco, L=...    | Infrastructure<br>Cisco Services<br>Endpoints<br>AdminAuth | 20 CD 74 02 ...  | SVS LabCA            | SVS LabCA            | Mon, 28 Apr 2025 | Sat, 28 Apr 2...  | Ens    |
| <input type="checkbox"/> | Default self-signed server certificate  | Endpoints<br>Infrastructure                                | 02 36 30 F4 6... | ISE2.tmo.svs.com     | ISE2.tmo.svs.com     | Fri, 11 Jul 2025 | Sun, 11 Jul 2...  | Ens    |
| <input type="checkbox"/> | DigiCert Global Root CA                 | Cisco Services                                             | 08 3B E0 56 9... | DigiCert Global R... | DigiCert Global R... | Fri, 10 Nov 2006 | Mon, 10 Nov ...   | Ens    |
| <input type="checkbox"/> | DigiCert Global Root G2 CA              | Cisco Services                                             | 03 3A F1 E6 ...  | DigiCert Global R... | DigiCert Global R... | Thu, 1 Aug 2013  | Fri, 15 Jan 20... | Ens    |
| <input type="checkbox"/> | DigiCert root CA                        | Endpoints<br>Infrastructure                                | 02 AC 5C 26 ...  | DigiCert High Ass... | DigiCert High Ass... | Fri, 10 Nov 2006 | Mon, 10 Nov ...   | Ens    |
| <input type="checkbox"/> | DigiCert SHA2 High Assurance Server ... | Endpoints<br>Infrastructure                                | 04 E1 E7 A4 ...  | DigiCert SHA2 Hi...  | DigiCert High Ass... | Tue, 22 Oct 2013 | Sun, 22 Oct 2...  | Ens    |

## Bind the Signed Certificate Signing Request (CSR) to ISE

Once the Certificate Signing Request (CSR) is signed, you can install the signed certificate on ISE.

Step 1. Navigate to **Administration > System > Certificates**. Under **Certificate Signing Requests**, select the **TACACS CSR** generated in the previous step and click **Bind Certificate**.

| <input type="checkbox"/> | Friendly Name | Certificate Subject | Key Length | Portal gro... | Timestamp | Host |
|--------------------------|---------------|---------------------|------------|---------------|-----------|------|
|--------------------------|---------------|---------------------|------------|---------------|-----------|------|

Step 2. Select the **signed certificate** and ensure the **TACACS** checkbox under Usage remains selected.

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

**Certificate Management**

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

### Bind CA Signed Certificate

\* Certificate File

Friendly Name

Validate Certificate Extensions ☐

Usage

☒ TACACS: Use certificate for TACACS Server

**Submit** **Cancel**

Step 3. Click **Submit**. If you receive a warning about replacing the existing certificate, click **Yes** to proceed.



## Warning

The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

Do you wish to replace the existing certificate?

**No** **Yes**

The certificate must now be correctly installed. You can verify this under **System Certificates**.

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

**Certificate Management**

- System Certificates**
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- Certificate Authority

### System Certificates

For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

[Edit](#) [Generate Self Signed Certificate](#) [Import](#) [Export](#) [Delete](#) [View](#)

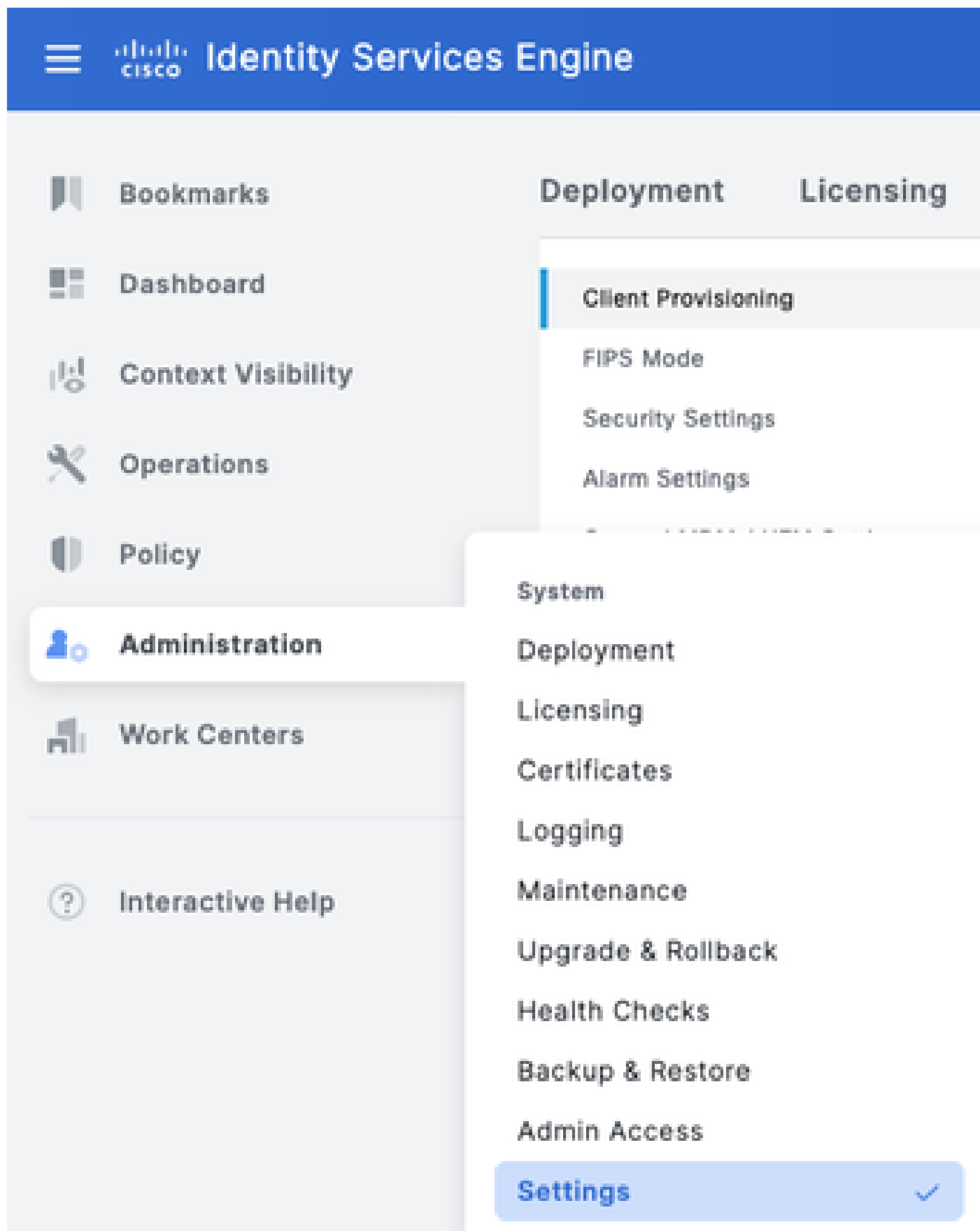
| Friendly Name                                                        | Used By | Portal group tag | Issued To | Issued By | Valid From       | Expiration Date  | Status |
|----------------------------------------------------------------------|---------|------------------|-----------|-----------|------------------|------------------|--------|
| ISE1                                                                 |         |                  |           |           |                  |                  |        |
| C=US, ST=NC, L=Raleigh, O=Cisco, OU=SVS, CN=I SE1.lab#ISE1.lab#00010 | TACACS  |                  | ISE1.lab  | ISE1.lab  | Wed, 10 Sep 2025 | Fri, 10 Sep 2027 | Active |

## Enable TLS 1.3

TLS 1.3 is not enabled by default in ISE 3.4.x. It must be manually enabled.



Step 1. Navigate to **Administration** > **System** > **Settings**.



Step 2. Click **Security Settings**, select the **check box** next to **TLS1.3** under TLS Version Settings, then, click **Save**.

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

General MDM / UEM Settings

Posture

Profiling

Protocols

## Security Settings

Choose the security settings you want to enable to ensure safe communications across your network.

### TLS Versions Settings

TLS 1.2 is enabled by default and can't be deselected. Choose one or a range of consecutive TLS versions.

☐ TLS 1.0

☐ TLS 1.1

☒ TLS 1.2

☒ TLS 1.3



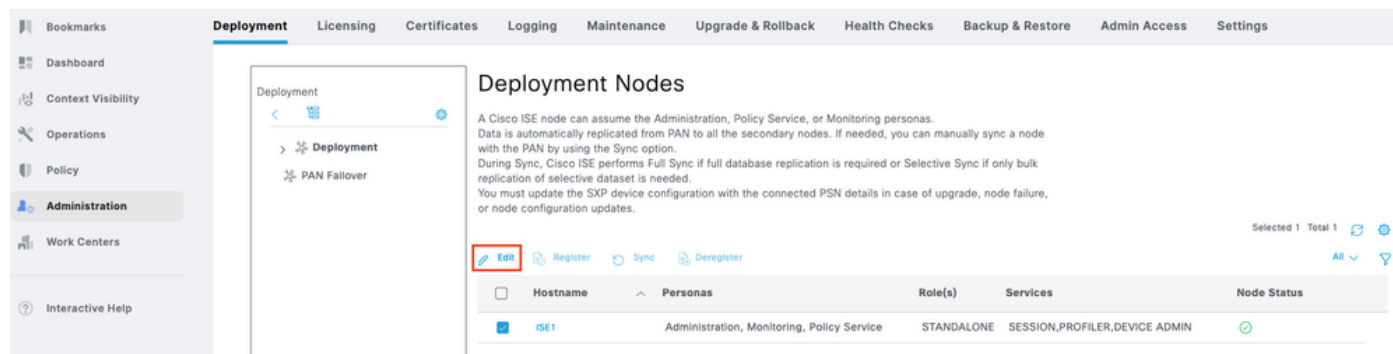
**Warning:** When you change the TLS version, the Cisco ISE application server restarts on all the Cisco ISE deployment machines.

## Enable Device Administration on ISE

The Device Administration service (TACACS+) is not enabled by default on an ISE node. Enable

TACACS+ on a PSN node.

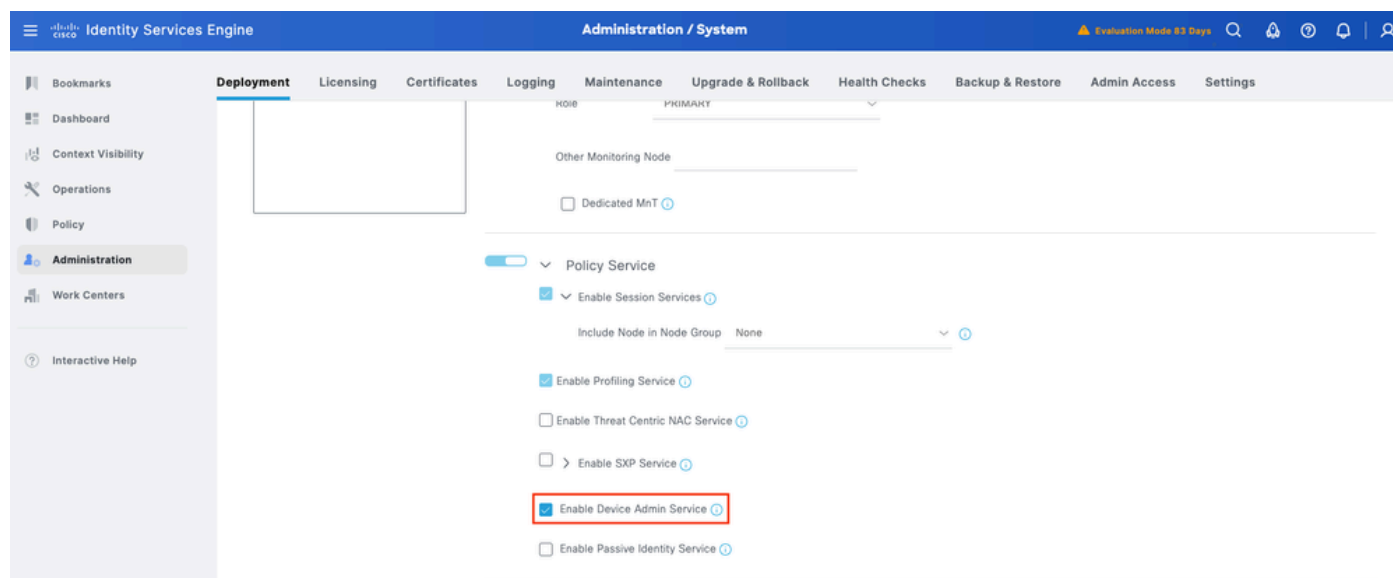
Step 1. Navigate to **Administration > System > Deployment**. Select the **check box** next to the **ISE node** and click **Edit**.



The screenshot shows the 'Deployment Nodes' page in the Cisco ISE GUI. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The top navigation bar includes: Deployment (selected), Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings. The main content area is titled 'Deployment Nodes' and includes a description of ISE node roles and a table of nodes. The 'Edit' button for the 'ISE1' node is highlighted with a red box.

| Hostname | Personas                                   | Role(s)    | Services                        | Node Status |
|----------|--------------------------------------------|------------|---------------------------------|-------------|
| ISE1     | Administration, Monitoring, Policy Service | STANDALONE | SESSION, PROFILER, DEVICE ADMIN | ✓           |

Step 2. Under **General Settings**, scroll down and select the **check box** next to **Enable Device Admin Service**.

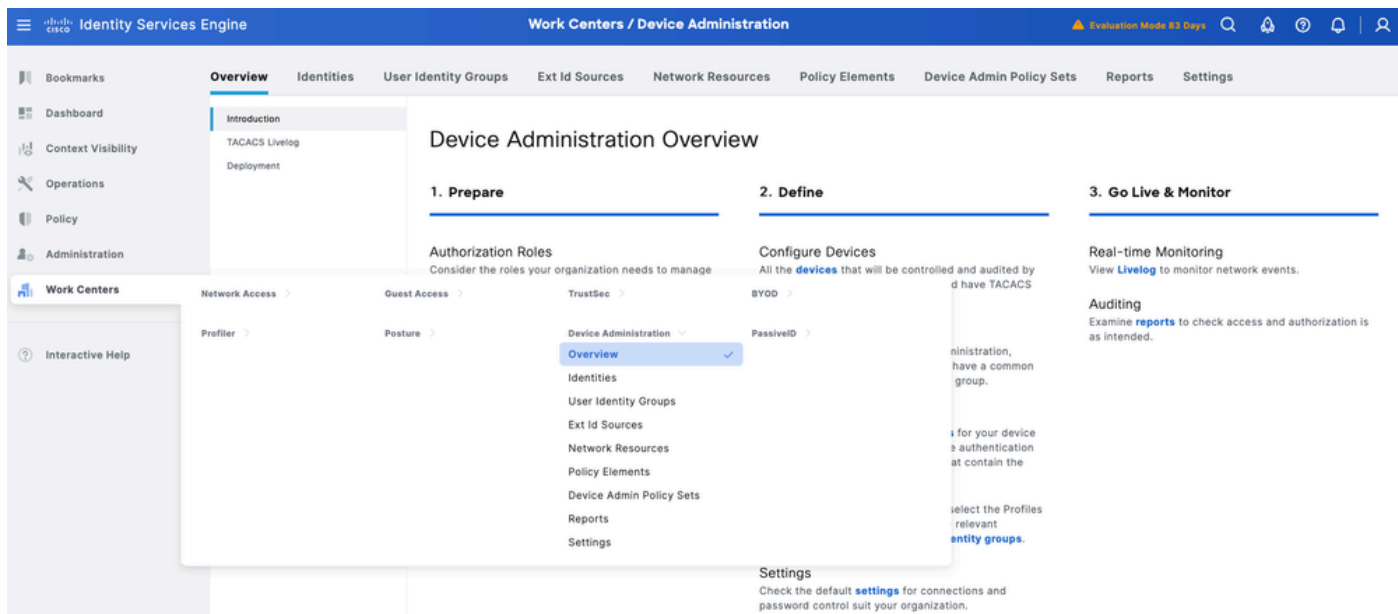


The screenshot shows the 'Administration / System' page in the Cisco ISE GUI. The left sidebar is the same as in the previous screenshot. The top navigation bar includes: Administration / System (selected), Evaluation Mode 87 Days, and search, help, and user icons. The main content area is titled 'Administration / System' and includes a 'Deployment' tab. The 'Enable Device Admin Service' checkbox is highlighted with a red box.

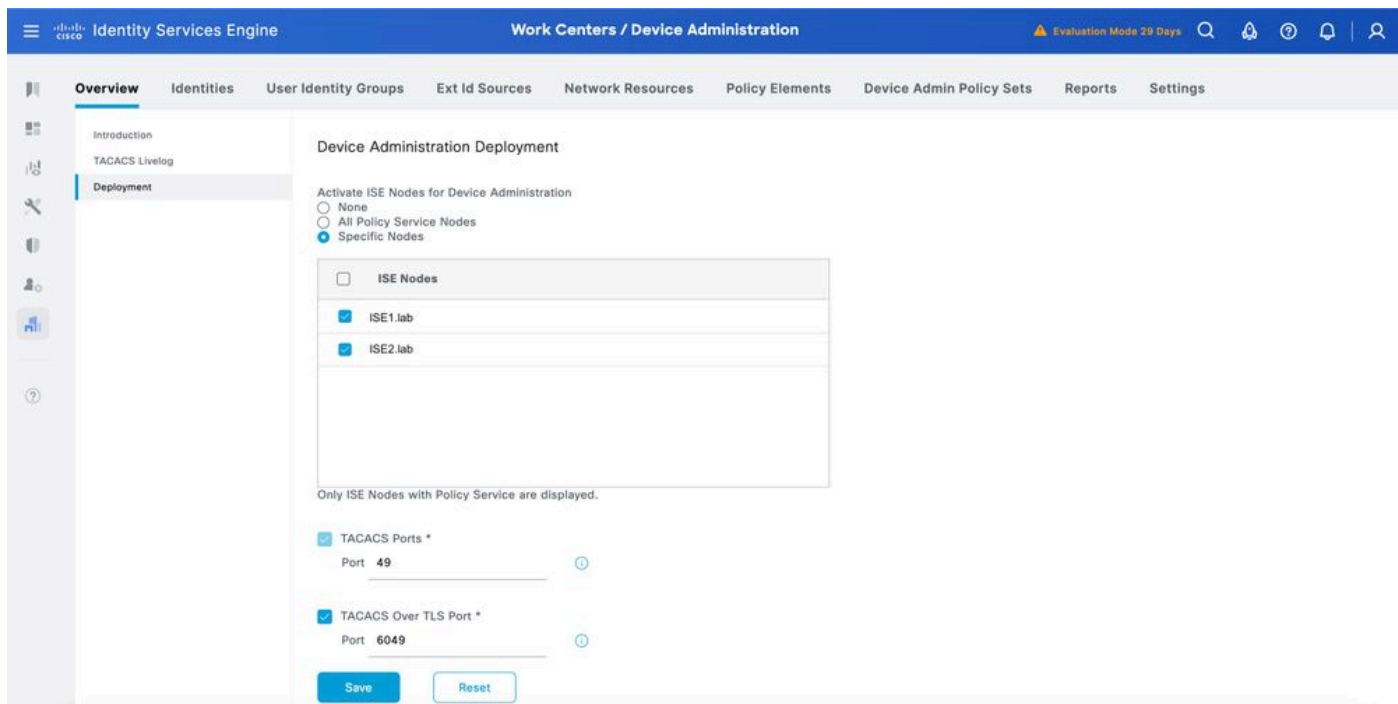
Step 3. **Save** the configuration. Device Admin Service is now enabled on ISE.

## Enable TACACS Over TLS

Step 1. Navigate to **Work Centers > Device Administration > Overview**.



Step 2. Click **Deployment**. Select the **PSN nodes** where you want to enable TACACS over TLS.



Step 3. Keep the default port **6049** or specify a different TCP port for TACACS over TLS, then click **Save**.

## Network Device and Network Device Groups

ISE provides powerful device grouping with multiple device group hierarchies. Each hierarchy represents a distinct and independent classification of network devices.

Step 1. Navigate to **Work Centers > Device Administration > Network Resource**. Click **Network Device Groups**.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources **Network Resources** Policy Elements Device Admin Policy Sets Reports Settings

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

All Groups Choose group

Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

| Name               | Description                        | No. of Network Devices |
|--------------------|------------------------------------|------------------------|
| > All Device Types | All Device Types                   | --                     |
| > All Locations    | All Locations                      | --                     |
| Atlanta            |                                    | 0                      |
| Los Angeles        |                                    | 0                      |
| New York           |                                    | 0                      |
| > Is IPSEC Device  | Is this a RADIUS over IPSEC Device | --                     |

All Device Types and All Locations are default hierarchies provided by ISE. You add your own hierarchies and define the various components in identifying a Network Device which can be used later in the Policy Condition.

Step 2. Now, add a NS-OX device as a Network Device. Navigate to **Work Centers > Device Administration > Network Resources**. Click **Add** to add a new Network Device POD2IPN2.

Identity Services Engine Administration / Network Resources

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM More

Network Devices List > POD2IPN2

Network Devices

Name POD2IPN2

Description

IP Address \* IP: 10.225.253.177 / 32

Device Profile Cisco

Model Name C9364D-GX2A

Software Version 10.5(3t)

Network Device Group

Location Atlanta Set To Default

IPSEC No Set To Default

Device Type NXOS Set To Default

Step 3. Enter the **IP address** of the Device and make sure to map the **Location** and **Device Type** for the Device. Finally, enable the **TACACS+ over TLS Authentication Settings**.

Identity Services Engine

Administration / Network Resources

Evaluation Mode 83 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

External MDM

More

Network Devices

Default Device

Device Security Settings

☐ RADIUS Authentication Settings

☐ TACACS Authentication Settings

☒ TACACS over TLS Authentication Settings

This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.

Subject Alternative Name (SAN)

Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.

☐ IP Address

The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details [Show](#)

Additional SAN Attributes

☒ Enable Single Connect Mode

Allow a network device to use one TCP connection for all TACACS+ requests, reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

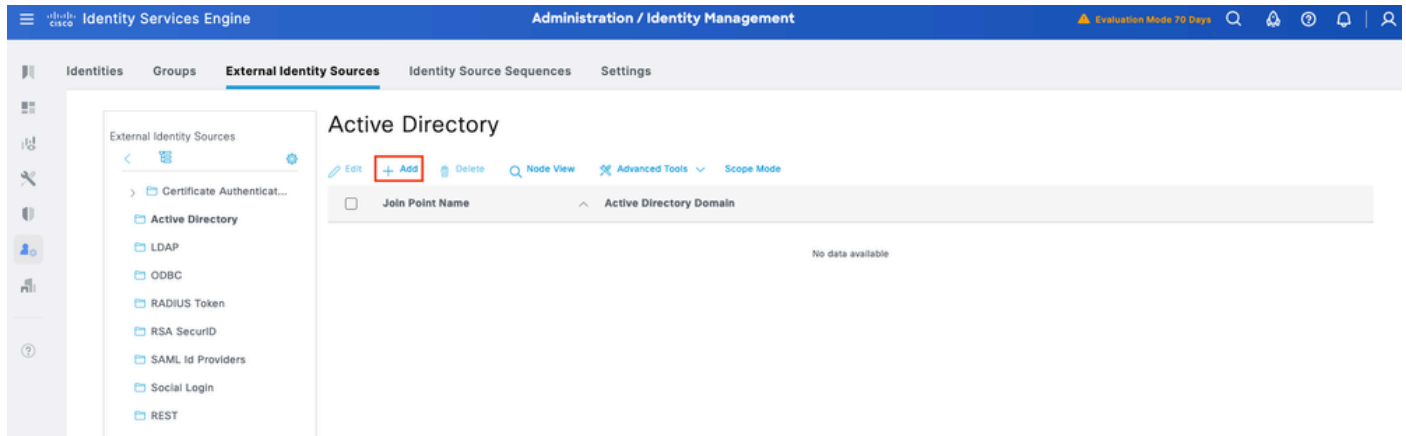
A large, pixelated black silhouette of a person in a dynamic, dancing pose, set against a white background. The figure is composed of many small black squares, giving it a blocky, digital appearance. The person's arms are raised and bent, and their legs are in a wide, expressive stance, suggesting movement like a breakdance move or a stylized dance pose. The overall shape is roughly circular at the top and tapers towards the bottom.

**Tip:** It is recommended to enable Single Connect Mode to avoid restarting the TCP session each time a command is sent to the device.

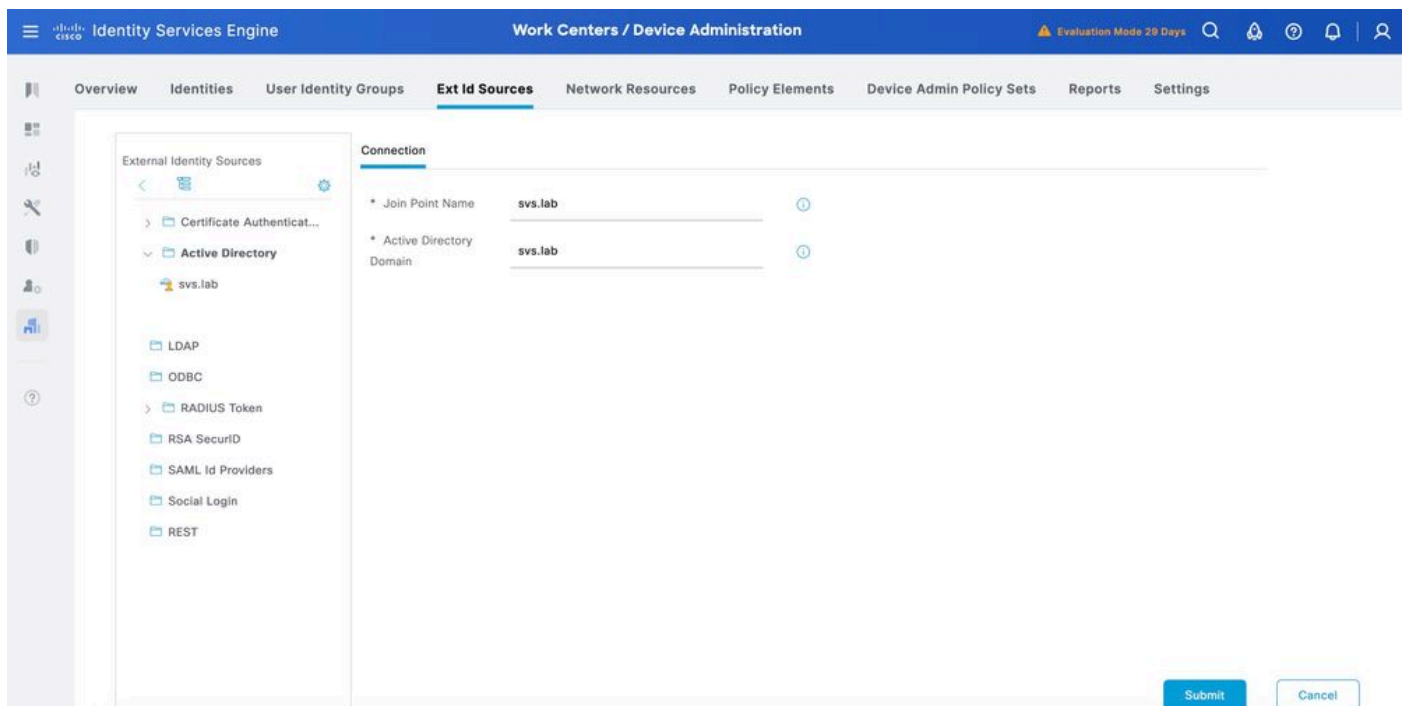
## Configure Identity Stores

This section defines an Identity Store for the Device Administrators, which can be the ISE Internal Users and any supported External Identity Sources. Here uses Active Directory (AD), an External Identity Source.

Step1. Navigate to **Administration > Identity Management > External Identity Stores > Active Directory**. Click **Add** to define a new AD Joint Point.



Step 2. Specify the **Join Point name** and the **AD domain name** and click **Submit**.



Step 3. Click **Yes** when prompted “Would you like to Join all ISE Nodes to this Active Directory Domain?”



## Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Yes

Step 4. Input the **credentials** with AD join privileges, and **Join** ISE to AD. Check the Status to verify it operational.



## Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

\* AD User Name ⓘ administrator

\* Password .....

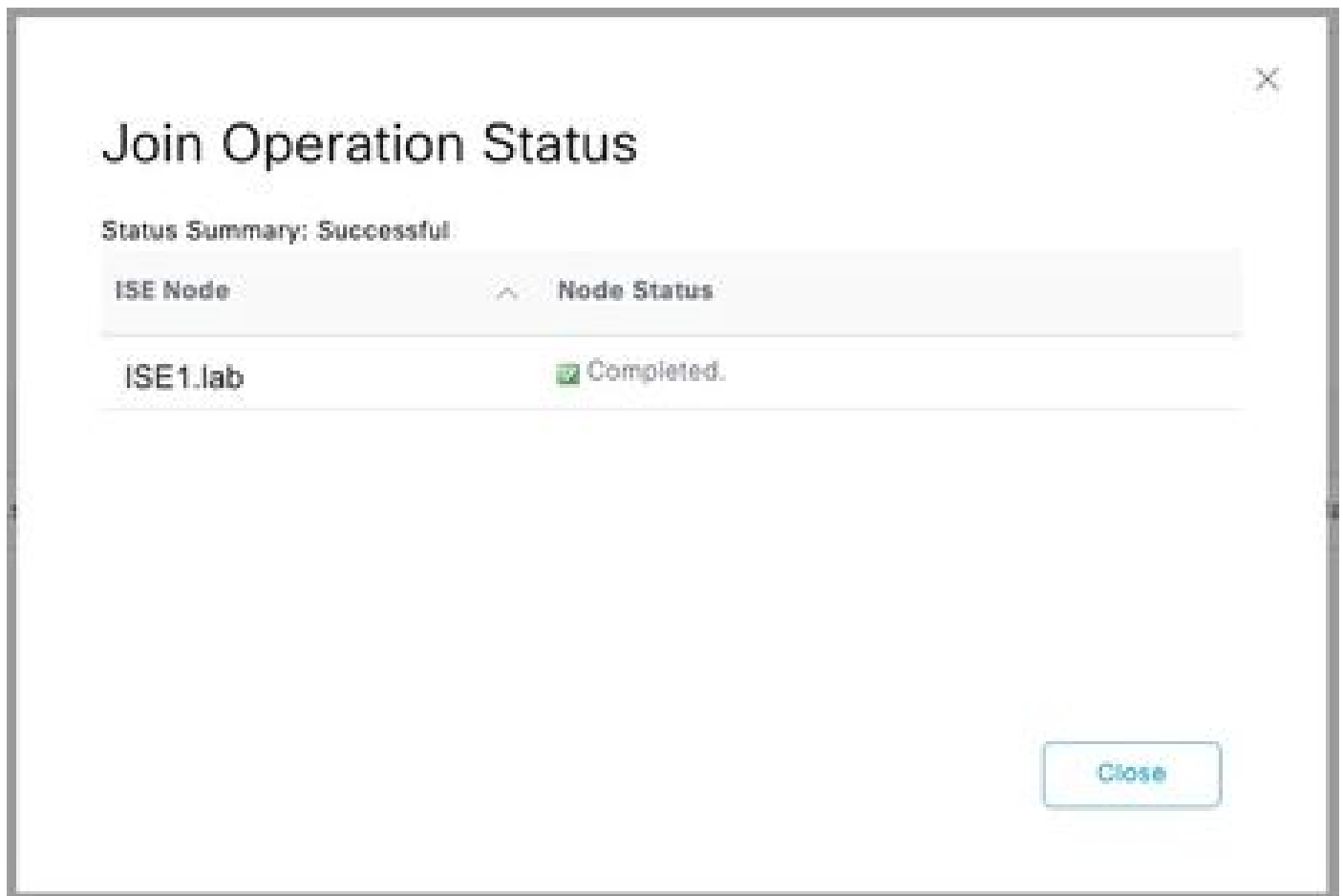
☐ Specify Organizational Unit ⓘ

☒ Store Credentials ⓘ

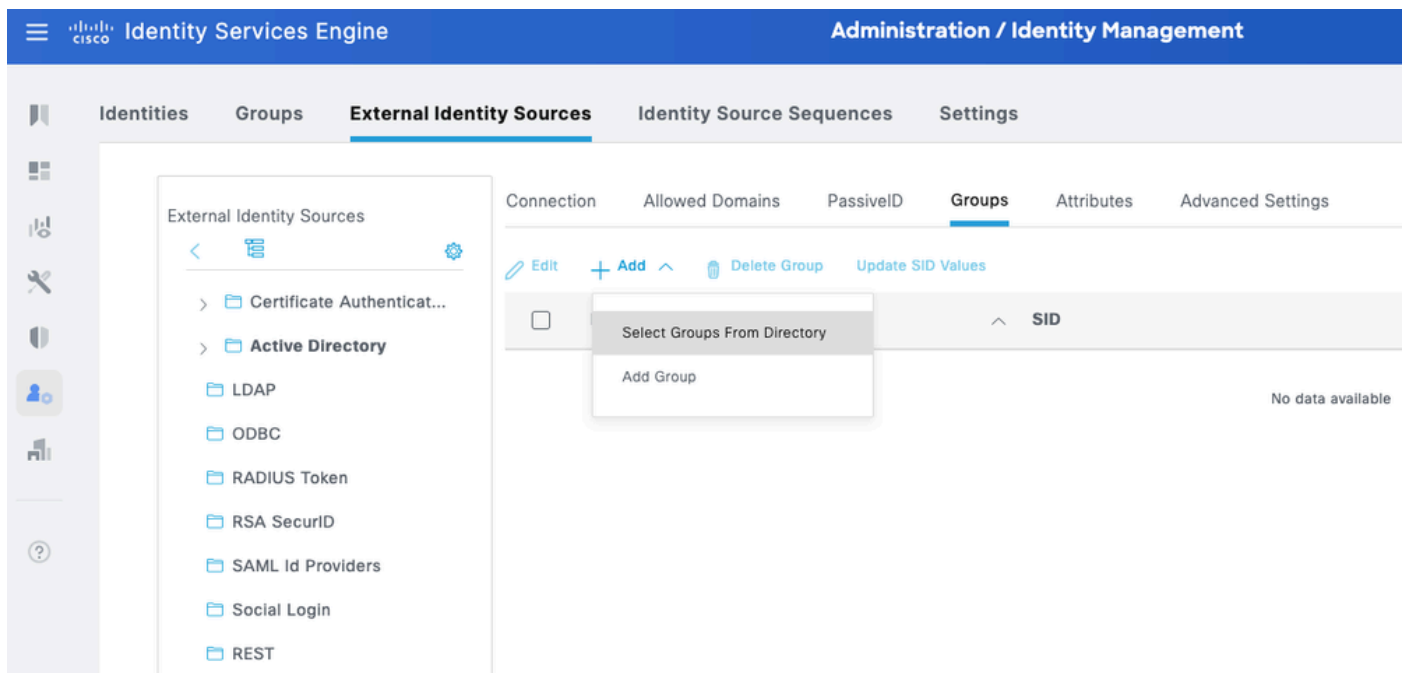
Cancel

OK





Step 5. Navigate to the **Groups** tab, and click **Add** to get all the groups needed based on which the users are authorized for the device access. This example shows the groups used in the Authorization Policy in this guide.



# Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

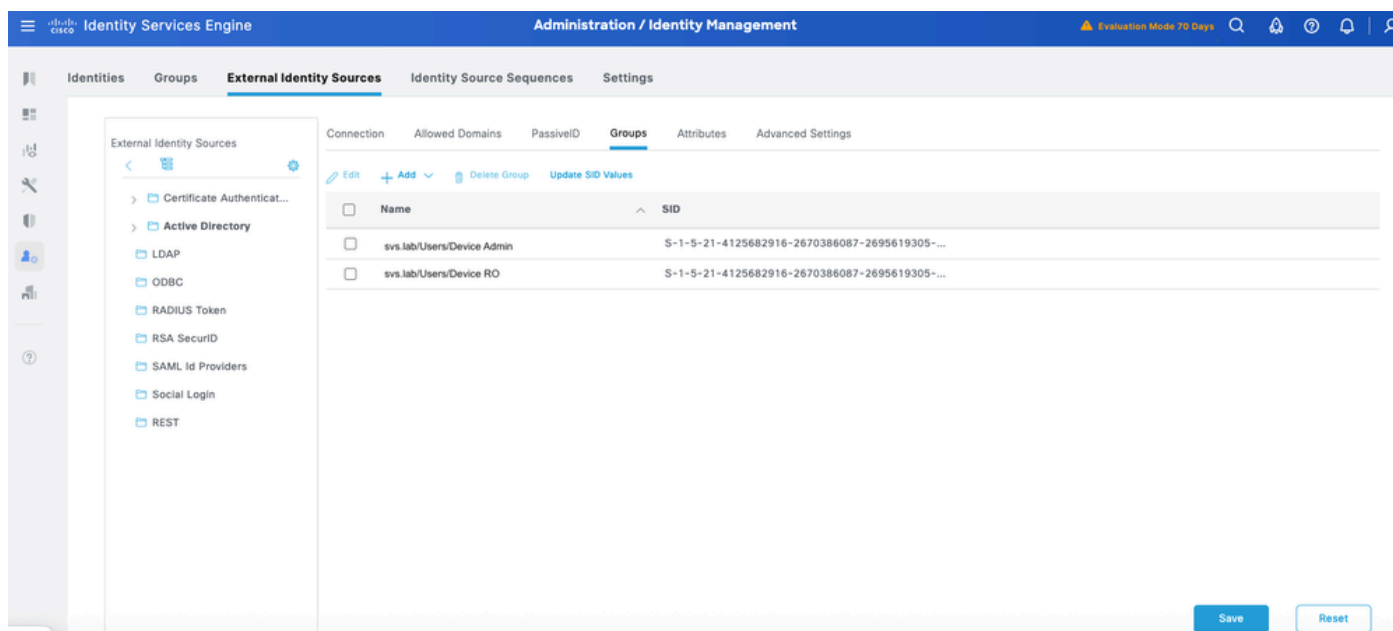
Name  SID

Filter  Filter

Type

2 Groups Retrieved.

| <input type="checkbox"/> | Name                       | Group SID                                  | Group Type |
|--------------------------|----------------------------|--------------------------------------------|------------|
| <input type="checkbox"/> | svs.lab/Users/Device Admin | S-1-5-21-4125682916-2670386087-26956193... | GLOBAL     |
| <input type="checkbox"/> | svs.lab/Users/Device RO    | S-1-5-21-4125682916-2670386087-26956193... | GLOBAL     |



## Configure TACACS+ Shell Profiles

Unlike Cisco IOS devices, which use privilege levels for authorization, Cisco NX-OS devices implement role-based access control (RBAC). In ISE, you can map TACACS+ profiles to user roles on Cisco NX-OS devices using Nexus-type Common Tasks.

The predefined roles on NX-OS devices differ among NX-OS platforms. Two common ones are:

- network-admin – predefined network admin role has complete read-and-write access to all commands on the switch; available in the default virtual device context (VDC) only if the devices (for example, Nexus 7000) have multiple VDCs. Use NX-OS CLI command **show cli syntax roles network-admin** to see the full command list available for this role.
- network-operator – predefined network admin role has complete read access to all commands on the switch; available in the default VDC only if the devices (for example, Nexus 7000) have multiple VDCs. Use NX-OS CLI command **show cli syntax roles network-operator** to see the full command list available for this role.

Next, it is defined two TACACS Profiles – NXOS Admin and NXOS HelpDesk.

## NX-OS Admin

Step 1. Add another **profile** and name it **NX-OS Admin**.

Step 2. Select **Mandatory** from the **Set attributes as** drop down. Select **Administrator** from **Network-role** option under **Common Tasks**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Overview', 'Identities', 'User Identity Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements' (selected), 'Device Admin Policy Sets', 'Reports', and 'Settings'. The left sidebar shows a tree view with 'Conditions', 'Network Conditions', 'Results', 'Allowed Protocols', 'TACACS Command Sets', and 'TACACS Profiles' (selected). The main content area is titled 'TACACS Profile' and shows the configuration for 'NXOS Admin'. The 'Name' field is 'NXOS Admin' and the 'Description' field is empty. Below the 'Task Attribute View' tab, the 'Common Tasks' section shows 'Common Task Type' set to 'Nexus'. The 'Set attributes as' dropdown is set to 'Mandatory'. The 'Network role' section has three radio buttons: 'None', 'Operator (Read Only)', and 'Administrator (Read Write)' (selected). The 'VDC role' section has three radio buttons: 'None' (selected), 'Operator (Read Only)', and 'Administrator (Read Write)'.

Step 3. Click **Submit** to save the profile.

## NX-OS HelpDesk

Step 1. From ISE UI, navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**. Add a new **TACACS Profile** and name it **NXOS HelpDesk**. Go to the Common Task Type drop down and choose **Nexus**.

You can see the template changes specific to user role. You can select these options corresponding to the user role you want to configure.

Step 2. Select **Mandatory** from the **Set attributes as** drop down. Select **Operator** from **Network-role** option under **Common Tasks**.

The screenshot shows the 'Policy Elements' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The left sidebar contains navigation links: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. The main content area is titled 'TACACS Profile' and includes a breadcrumb 'TACACS Profiles > NXOS HelpDesk'. The 'Name' field is set to 'NXOS HelpDesk'. Below it is a 'Description' text area. There are tabs for 'Task Attribute View' and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'Nexus'. Below this, there are two sections: 'Set attributes as' (set to 'Optional') and 'Network role' (with radio buttons for 'None', 'Operator (Read Only)' (selected), and 'Administrator (Read Write)'). A 'VDC role' section also has radio buttons for 'None' (selected), 'Operator (Read Only)', and 'Administrator (Read Write)'.

Step 3. Click **Save** to save the profile.

## Configure Device Admin Policy Sets

Policy Sets are enabled by default for Device Administration. Policy Sets can divide polices based on the Device Types so to ease application of TACACS profiles. For example, Cisco IOS devices use Privilege Levels and/or Command Sets whereas Cisco NX-OS devices use Custom Attributes.

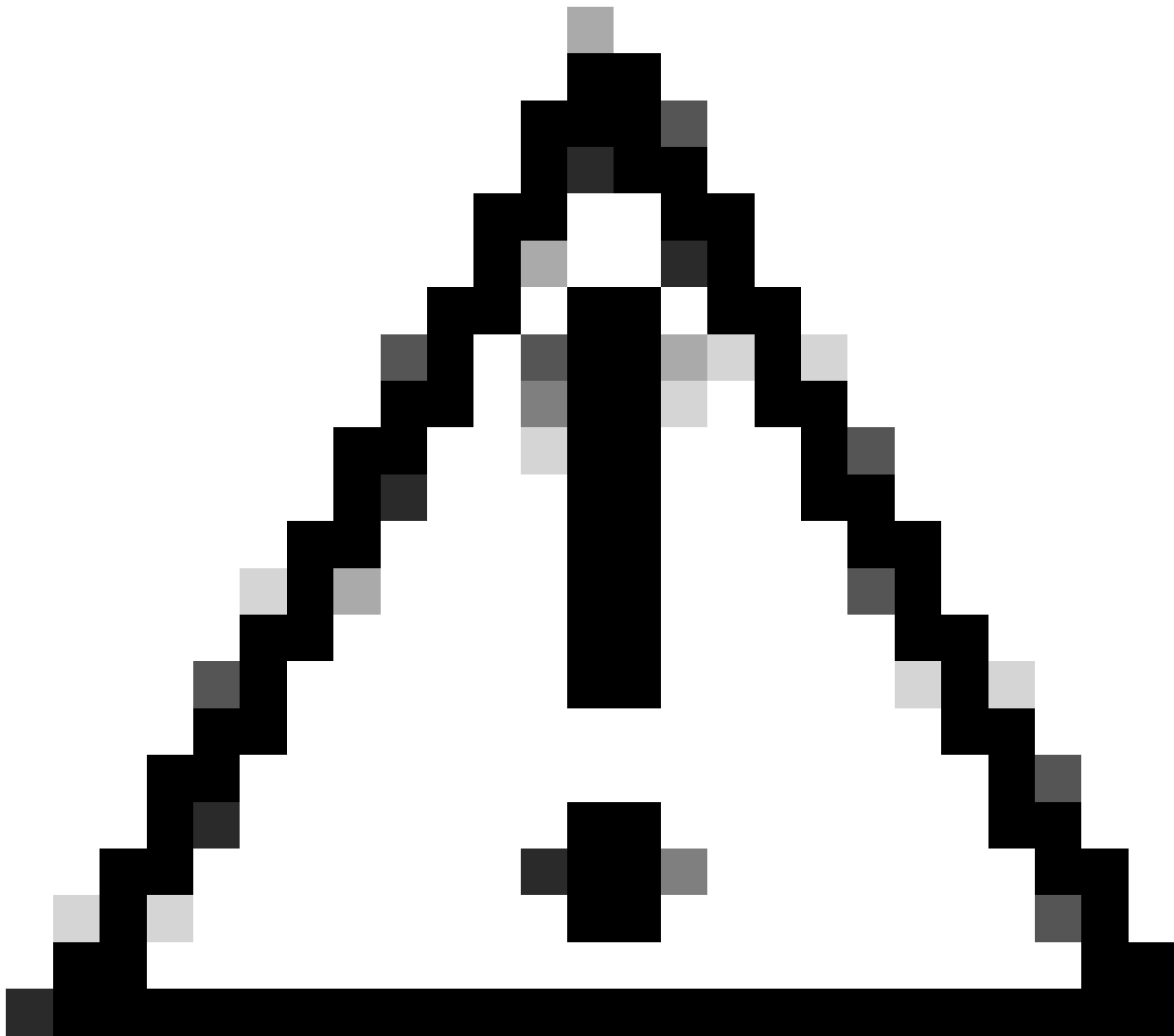
Step 1. Navigate to **Work Centers > Device Administration > Device Admin Policy Sets**. Add a new Policy Set **NX-OS Devices**. Under **condition**, specify **DEVICE:Device Type EQUALS All Device Types#NXOS**. Under **Allowed Protocols**, select **Default Device Admin**.

The screenshot shows the 'Device Admin Policy Sets' configuration page in the Cisco ISE 'Work Centers / Device Administration' section. The left sidebar is the same as the previous screenshot. The main content area is titled 'Policy Sets' and includes buttons for 'Reset', 'Reset Policy Set Hit Counts', and 'Save'. Below these is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The table contains one entry: 'NX-OS Devices' with a status of 'On' (green dot) and a condition of 'DEVICE:Device Type EQUALS All Device Types#NXOS'. The 'Allowed Protocols / Server Sequence' column shows 'Default Device Admin' with a dropdown arrow and a plus sign. At the bottom right, there is a gear icon and a right-pointing arrow.

Step 2. Click **Save** and click the **right** arrow to configure this Policy Set.

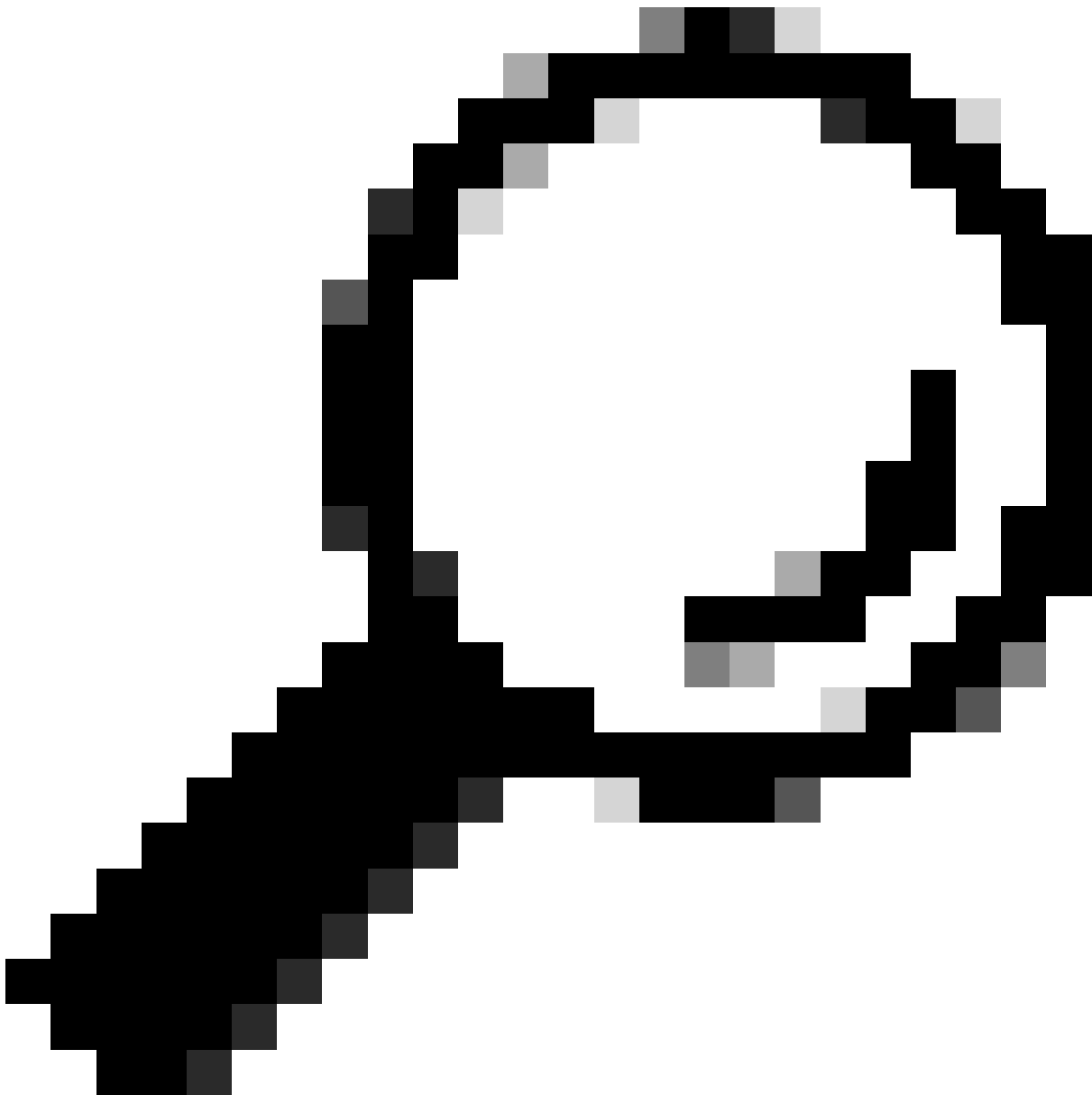
Step 3. Create the **Authentication Policy**. For Authentication, you use the **AD** as the **ID Store**. Leave the default options under **If Auth fail**, **If User not found** and **If Process fail**.





**Caution:** Ensure that the console connection is reachable and functioning properly.

---



**Tip:** It is recommended to configure a temporary user and change the AAA authentication and authorization methods to use local credentials instead of TACACS while making configuration changes, to avoid being locked out of the device.

---

## TACACS+ Server Configuration

Step 1. Initial configuration.

```
POD2IPN2# sho run tacacs
```

```
feature tacacs+
```

```
tacacs-server host 10.225.253.209 key 7 "F1whg.123"  
aaa group server tacacs+ tacacs2  
server 10.225.253.209
```

use-vrf management

## Trustpoint Configuration

Step 1. Create a **key label**, in your case, use ecc key pair.

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto key generate ecc label ec521-label exportable modulus 521
```

Step 2. Associate this with a trustpoint.

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto ca trustpoint ec521-tp
```

```
POD2IPN2(config-trustpoint)#
```

```
ecckeypair ec521-label
```

Step 3. Install the **CA public key**.

```
<#root>
```

```
POD2IPN2(config)#
```

```
crypto ca authenticate ec521-tp
```

input (cut & paste) CA certificate (chain) in PEM format;  
end the input with a line containing only END OF INPUT :

```
-----BEGIN CERTIFICATE-----
```

```
MIIFlDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE  
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo  
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TVlMgTGFi  
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV  
UzEXMBUAGA1UECBM0Tm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxDjAM  
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMWYwJDQTC  
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq  
2YjwZlZSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW  
Vwv4MBBjHfM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF30  
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m  
mutNo7IhbJSrgAFxmjlBbjMmgspObULO/wxMHdTbtPBf11HRHTkNIo3qy04UADL2  
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm  
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gXl0jKyLP/gC7j8AeP03ir+KZui8  
b8X4iYn/67SbzZFhwn3chkw4JYhQ4AImw1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN  
gJ+kQXe7QtT/u6m1MrtjE3gAEVpl334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA  
z1XCoONX+6a1ekmXuAOI+tt3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4  
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
```



```
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQOMFgpTVlMgTGF iENBMAOGCSqGSib3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLFiNHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TFITVmAzcX8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfPiYtprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1POdsS/i6Lo7ypYX0eB9HgVDckzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOX E/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
-----END CERTIFICATE-----
```

**END OF INPUT**

Fingerprint(s): SHA1

Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

Do you accept this certificate? [yes/no]:yes

POD2IPN2(config)#

POD2IPN2(config)#

**show crypto ca certificates ec521-tp**

Trustpoint: ec521-tp

CA certificate 0:

subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA

issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA

serial=20CD7402C4DA37F5

notBefore=Apr 28 17:05:00 2025 GMT

notAfter=Apr 28 17:05:00 2035 GMT

SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

purposes: sslserver sslclient

POD2IPN2(config)#

Step 4. Generate **switch identity certificate request**.

<#root>

POD2IPN2(config)#

**crypto ca enroll ec521-tp**

Create the certificate request ..

Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate.

For security reasons your password will not be saved in the configuration.

Please make a note of it.

Password:C1sco.123

The subject name in the certificate will be the name of the switch.

Include the switch serial number in the subject name? [yes/no]:

**yes**

The serial number in the certificate will be: FD026490P4T

Include an IP address in the subject name [yes/no]:

yes

ip address:10.225.253.177

Include the Alternate Subject Name ? [yes/no]:

no

The certificate request will be displayed...

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBtjCCARcCAQAwKTERMA8GA1UEAwIUE9EMk1QTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw70vqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6Lzpk0hPAGE4jBveNHxYeIA7PfNWvJ7xTBWjDNX
/IYBm6E7Hd7q420mCe8Mef+bqJBdJ9wzpyEjhI21IIoXt4814nBxObkIWWyR5cZN
IiXtLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MC0GCSqGSIb3DQEJDDjEgMB4wHAYDVR0RAQH/BBIwEIIIIUE9EMk1QTjKHBArh/bEw
CgYIKoZIzj0EAwIDgYwAMIGIAkIAtzQ/knrW2ovCvOHAuq1v2cr0n3NenS/441u1
+3H1y52vn4Rm4CGU3wkzXU3qG03YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt30hpaDD0TWzzvZY7qFf1C015p6pvUpHi gqoZNg5
9xhNdM1CQSyk0g==
```

-----END CERTIFICATE REQUEST-----

Step 5. Import the **switch identity certificate** signed by CA.

<#root>

POD2IPN2(config)#

**crypto ca import ec521-tp certificate**

input (cut & paste) certificate in PEM format:

-----BEGIN CERTIFICATE-----

```
MIIDzTCCABwGAWIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmFzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdu1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcnMjUwNTA3MTkxMDAwWhcnMjUwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
TOQySVBOMjEUMBIGA1UEBRMLRkRPMjY0OTBQNFQwgZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhpSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMFAmM1f8hgGboTsd3urjY6YJ7wx5/5uokF0n3D0n
ISOEjaUgihe3jzXicHE5uQhZbJH1xk0iJdMuTw/ggxm8+ryNGcQtHF3xEaNAMD4w
HgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAzBgNVHREBAf8EEjAQgghQ
TOQySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msod0QK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZ01PUXNTyZidXpGd/yTrdQA15JzpW4pEudrbCJMZEYtqoP
wD+40E8vKoYEgyW1DrpRZ0ZG1usZczuUhlZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
1iToeYy2Q0cTesSZCKvRBv6Ewj5JuSLeMURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61Ln1VxhXombiS6
INoa0GvQONr1+1fT8ADidZ/Ukd5Ubhc9bh/sYzf4MwtK1wV016Hv7vGpSMYonD6
a271im+tJPYKneezQ60yKz1GqSL/Ta6J0dip/fEYp8UmRq9InDh23gDjqrojlW7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJT1nuk5KCqFx//4P7mAoyZYiTiDp1pkYS
VK65fJKD+pYxIhSP9wN8rnwtzSCWb0Z78sg006Y6wIXyTP0UB3FWhD+GxttkmEce
ZnAQbgxpgrg51hpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
1fKuuebdZkbwz72r70yyX/U=
```

-----END CERTIFICATE-----

POD2IPN2(config)#

Verify the switch identity certificate is enrolled.

<#root>

POD2IPN2(config)#

**show crypto ca certificates ec521-tp**

Trustpoint: ec521-tp

certificate:

subject=CN = POD2IPN2, serialNumber = FD026490P4T

issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA

serial=0BACD2EFA5D80E6F

notBefore=May 7 19:10:00 2025 GMT

notAfter=May 7 19:10:00 2026 GMT

SHA1 Fingerprint=CA:B2:BF:3F:ED:2F:06:0B:C1:E4:DC:21:9F:9D:54:61:98:32:C5:13

purposes: sslserver sslclient

CA certificate 0:

subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA

issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA

serial=20CD7402C4DA37F5

notBefore=Apr 28 17:05:00 2025 GMT

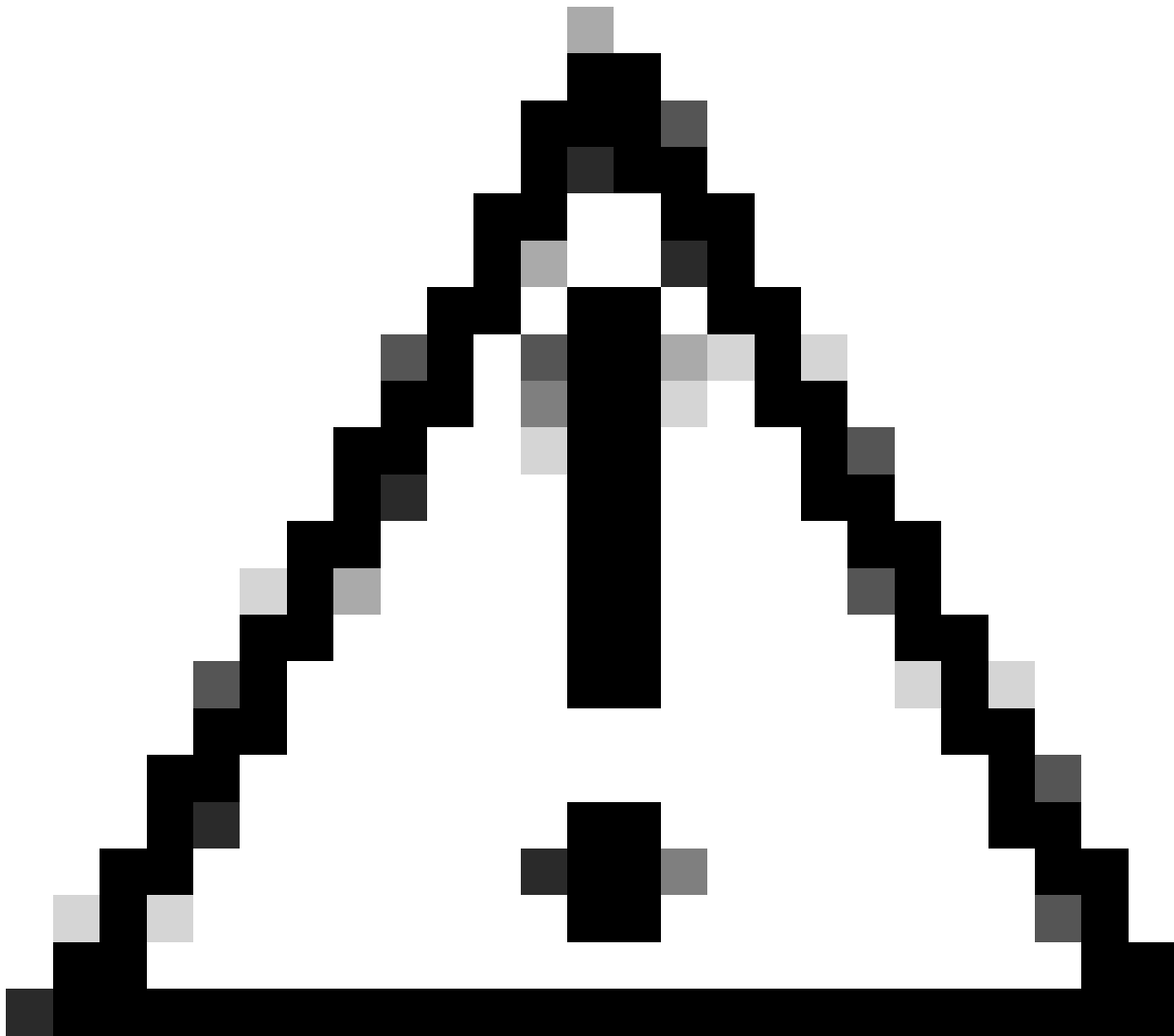
notAfter=Apr 28 17:05:00 2035 GMT

SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

purposes: sslserver sslclient

POD2IPN2(config)#

## TACACS+ TLS Configuration



**Caution:** Perform these configuration changes through console with local credentials.

---

Step 1. Configure **global tacacs tls**.

```
<#root>  
POD2IPN2(config)#  
tacacs-server secure tls
```

Step 2. Change the ISE port to TLS port that ISE server is configured with.

```
<#root>  
POD2IPN2(config)#  
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

Step 3. Associate the ISE server configure on the switch to the trust point for TLS connection.

```
<#root>
POD2IPN2(config)#
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

Step 4. Create **tacacs server group**.

```
<#root>
POD2IPN2(config)#
aaa group server tacacs+ tacacs2

POD2IPN2(config-tacacs+)#
server 10.225.253.209

POD2IPN2(config-tacacs+)#
use-vrf management
```

Step 5. Verify the configuration.

```
<#root>
POD2IPN2#
sho run tacacs

feature tacacs+

tacacs-server secure tls
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
aaa group server tacacs+ tacacs2
    server 10.225.253.209
    use-vrf management
```

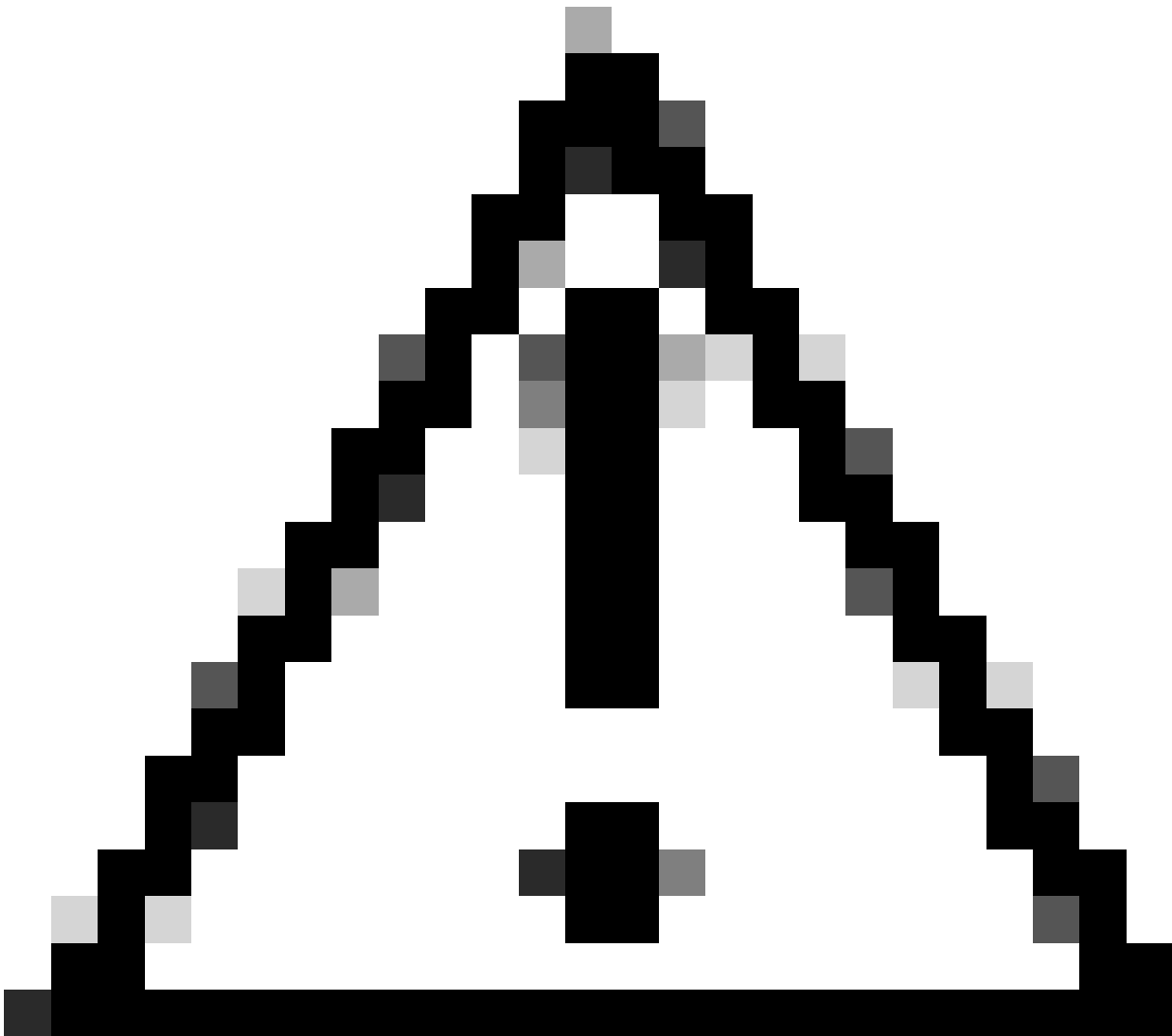
Step 6. Test the remote user before configuring AAA authentication.

```
<#root>
POD2IPN2#
test aaa group tacacs2 <username> <password>

user has been authenticated
```

## AAA Configuration

---



**Caution:** Ensure remote user authentication is successful before proceeding with AAA configurations.

---

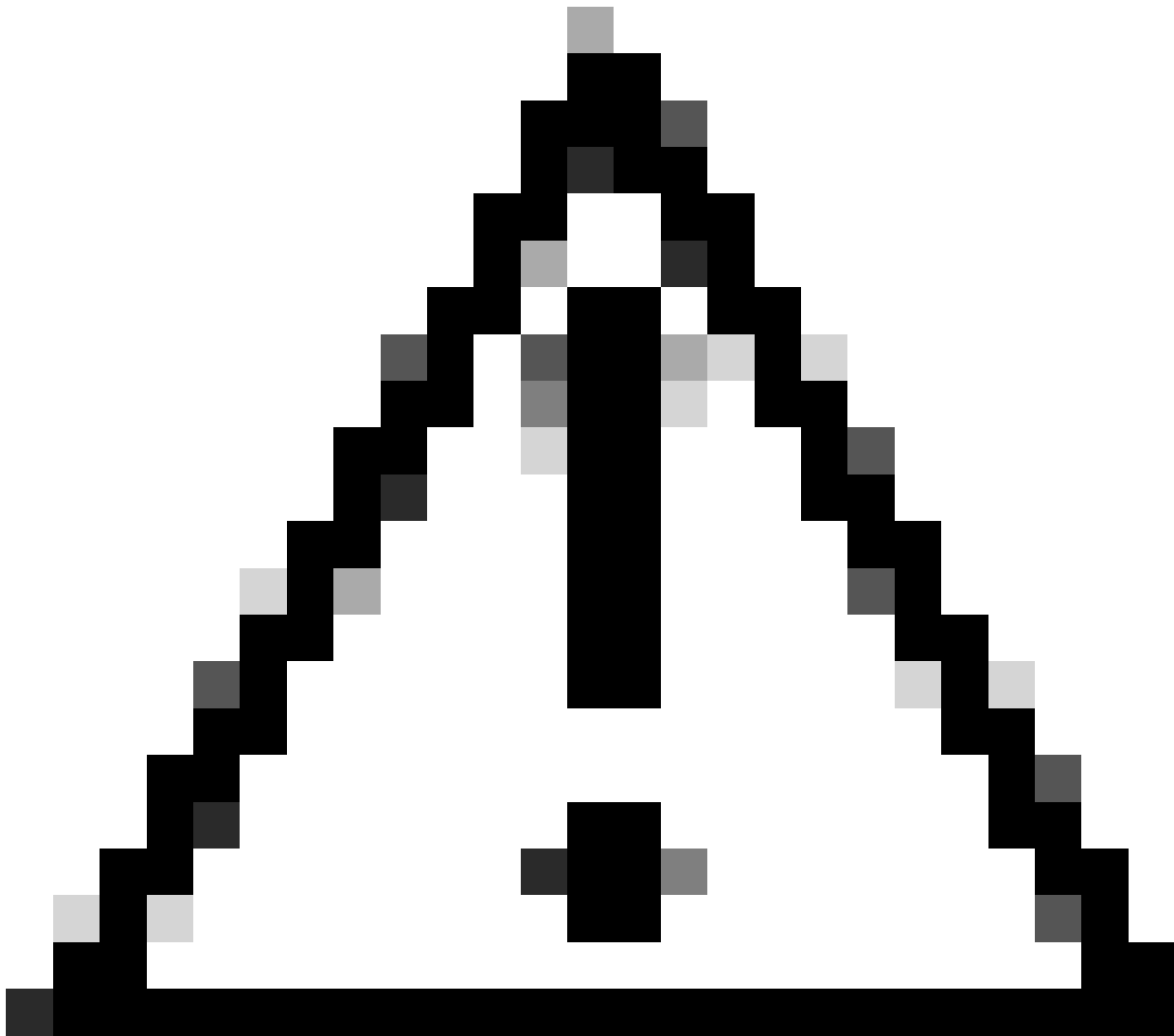
Step 1. Configure **AAA remote authentication**.

```
<#root>
```

```
POD2IPN2(config)#
```

```
aaa authentication login default group tacacs2
```

Step 2. Configure **AAA remote authorization** after testing the command.



**Caution:** Ensure that you see authorization-status" as "AAA\_AUTHOR\_STATUS\_PASS\_ADD.

---

```
<#root>
```

```
POD2IPN2#
```

```
test aaa authorization command-type config-commands default user <username> command "feature bgp"
```

```
sending authorization request for: user: pamemart, author-type:3, cmd "feature bgp"
```

```
user pamemart, author type 3, command: feature bgp, authorization-status:0x1(AAA_AUTHOR_STATUS_PASS_ADD)
```

Step 3. Configure **AAA command** and **config-command** authorization.

```
<#root>
```

```
POD2IPN2(config)#
```

```
aaa authorization config-commands default group tacacs2 local
```

```
POD2IPN2(config)#
```

```
aaa authorization commands default group tacacs2 local
```

## Test and Troubleshoot User Access for NX-OS

### Verification

Configuration for Device Administration for Cisco NX-OS is completed. You need to validate the configuration.

Step 1. SSH and log into the **NX-OS devices** as various roles.

Step 2. Once on the device command-line interface (CLI), verify that the user has access to the right commands. For example, a Helpdesk user must be able to ping a regular IP address (for example, 10.225.253.129) but denied to show the running configuration.

```
POD2IPN1# ping 10.225.253.129 vrf management
PING 10.225.253.129 (10.225.253.129): 56 data bytes
64 bytes from 10.225.253.129: icmp_seq=0 ttl=254 time=0.817 ms
64 bytes from 10.225.253.129: icmp_seq=1 ttl=254 time=0.638 ms
64 bytes from 10.225.253.129: icmp_seq=2 ttl=254 time=0.642 ms
64 bytes from 10.225.253.129: icmp_seq=3 ttl=254 time=0.651 ms
64 bytes from 10.225.253.129: icmp_seq=4 ttl=254 time=0.712 ms

--- 10.225.253.129 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.638/0.692/0.817 ms
POD2IPN1#
POD2IPN1# show running-config
% Permission denied for the role
```

### Troubleshooting

NX-OS Configuration Validation.

```
POD2IPN2# show crypto ca certificates
POD2IPN2# show crypto ca trustpoints
POD2IPN2# show tacacs-server statistics <server ip>
```

To show the user connections and role(s), use these commands.

```
show users
show user-account [<user-name>]
A sample output is shown below:
POD2IPN1# show users
```



NAME LINE TIME IDLE PID COMMENT

Admin-ro pts/5 May 15 23:49 . 16526 (10.189.1.151) session=ssh \*

POD2IPN1# show user-account Admin-ro

user:Admin-ro

roles:network-operator

account created through REMOTE authentication

Credentials such as ssh server key will be cached temporarily only for this user account

Local login not possible...

These are useful debugs in troubleshooting TACACS+:

debug TACACS+ aaa-request

```
2016 Jan 11 03:03:08.652514 TACACS[6288]: process_aaa_tplus_request:Checking for state of mgmt0 port w
2016 Jan 11 03:03:08.652543 TACACS[6288]: process_aaa_tplus_request: Group demoTG found. corresponding
2016 Jan 11 03:03:08.652552 TACACS[6288]: process_aaa_tplus_request: checking for mgmt0 vrf:management
2016 Jan 11 03:03:08.652559 TACACS[6288]: process_aaa_tplus_request:port_check will be done
2016 Jan 11 03:03:08.652568 TACACS[6288]: state machine count 0
2016 Jan 11 03:03:08.652677 TACACS[6288]: is_intf_up_with_valid_ip(1258):Proper IOD is found.
2016 Jan 11 03:03:08.652699 TACACS[6288]: is_intf_up_with_valid_ip(1261):Port is up.
2016 Jan 11 03:03:08.653919 TACACS[6288]: debug_av_list(797):Printing list
2016 Jan 11 03:03:08.653930 TACACS[6288]: 35 : 4 : ping
2016 Jan 11 03:03:08.653938 TACACS[6288]: 36 : 12 : 10.1.100.255
2016 Jan 11 03:03:08.653945 TACACS[6288]: 36 : 4 : <cr>
2016 Jan 11 03:03:08.653952 TACACS[6288]: debug_av_list(807):Done printing list, exiting function
2016 Jan 11 03:03:08.654004 TACACS[6288]: tplus_encrypt(659):key is configured for this aaa sessin.
2016 Jan 11 03:03:08.655054 TACACS[6288]: num_inet_addrs: 1 first s_addr: -1268514550 10.100.1.10 s6_a
2016 Jan 11 03:03:08.655065 TACACS[6288]: non_blocking_connect(259):interface ip_type: IPV4
2016 Jan 11 03:03:08.656023 TACACS[6288]: non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 TACACS[6288]: non_blocking_connect(388): setsockopt success error:22
2016 Jan 11 03:03:08.656694 TACACS[6288]: non_blocking_connect(489): connect() is in-progress for serv
2016 Jan 11 03:03:08.679815 TACACS[6288]: tplus_decode_authen_response: copying hostname into context
```

Enable SSL debug.

```
touch '/bootflash/.enable_ssl_debugs'
```

Show debug file contents.

```
cat /tmp/ssl_wrapper.log.*
```

From the ISE GUI, navigate to **Operations > TACACS Livelog**. All the TACACS authentication and authorization requests are captured here, and the details button provides detailed information about why a particular transaction passed/failed.

