

Configure TACACS+ over TLS 1.3 on an IOS XE Device with ISE

Contents

[Introduction](#)

[Overview](#)

[Using this Guide](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Licensing](#)

[Part 1 -ConfigureISE for Device Administration](#)

[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](#)

[Create Network Device and Network Device Groups](#)

[ConfigureIdentity Stores](#)

[ConfigureTACACS+ Profiles](#)

[IOS XE_RW - Administrator Profile](#)

[IOS XE_RO - Operator Profile](#)

[ConfigureTACACS+ Command Sets](#)

[CISCO IOS XE_RW - Administrator Command Set](#)

[CISCO IOS XE_RO - Operator Command Set](#)

[ConfigureDevice Admin Policy Sets](#)

[Part 2 - Configure CiscoIOS XE forTACACS+ over TLS 1.3](#)

[Configuration Method 1 - Device Generated Key-pair](#)

[TACACS+ Server Configuration](#)

[Trustpoint Configuration](#)

[TACACS & AAA with TLS Configuration](#)

[Configuration Method 2 - CA Generated Key-Pair](#)

[TACACS & AAA with TLS Configuration](#)

[Verification](#)

Introduction

This document describes an example for TACACS+ over TLS with Cisco Identity Services Engine (ISE) as server and a Cisco IOS® XE 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 IOS XE based network devices.

- Part 1 – Configure ISE for Device Admin
- Part 2 – Configure Cisco IOS XE for TACACS+ over TLS

Prerequisites

Requirements

Requirements 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 these software and hardware versions:

- ISE VMware virtual appliance, release 3.4 patch 2
- Cisco IOS XE Software, version 17.15+

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.

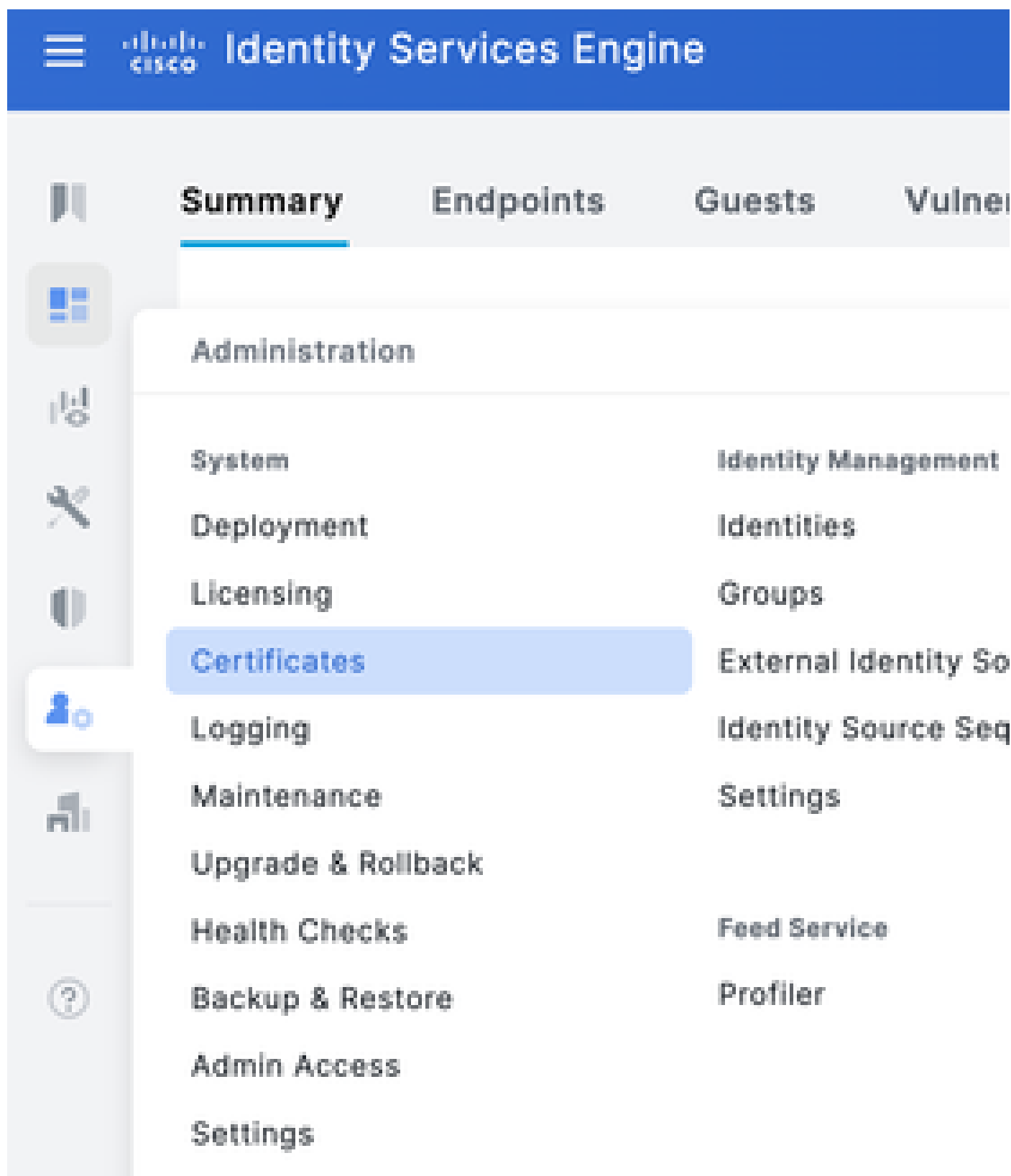
Part 1 - Configure ISE for Device Administration

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**.



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 **PSN**s that will have TACACS+ enabled.

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ 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

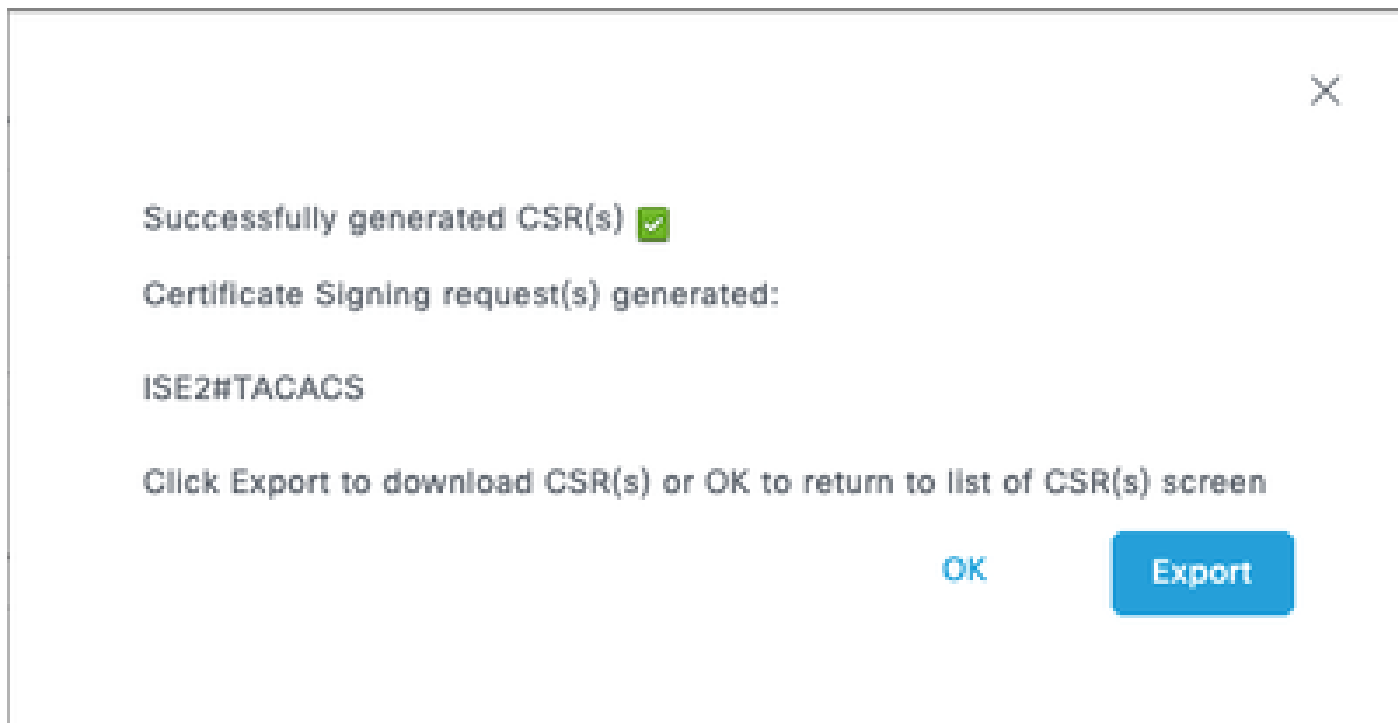
Country (C)
US

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**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is **Administration / System**. The left sidebar shows the **Certificates** menu with **Trusted Certificates** selected. The main content area displays the **Trusted Certificates** table. The **Import** button is highlighted with a red circle.

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐	Amazon root CA	Infrastructure Cisco Services	06 6C 9F CF ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2015	Sun, 17 Jan 2...	End
☐	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2...	End
☐	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	End
☐	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	End
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 20...	Cisco Root CA 20...	Fri, 14 May 2004	Mon, 14 May ...	Dis
☐	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...	End
☐	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...	End
☐	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	End
☐	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034	End

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 **Examinar...** 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

Step 3. Click **Submit**. The certificate must now appear under **Trusted Certificates**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is titled 'Trusted Certificates' and includes a table with columns: Friendly Name, Trusted For, Serial Number, Issued To, Issued By, Valid From, Expiration Date, and Status. A single certificate is listed with the Friendly Name 'CN=SVS LabCA, OU=SVS, O=Cisco, L=...' and a status of 'Valid'.

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**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is titled 'Certificate Signing Requests' and includes a button 'Generate Certificate Signing Requests (CSR)'. Below the button is a text box explaining that CSRs must be sent to and signed by an external authority. A table with columns: Friendly Name, Certificate Subject, Key Length, Portal gro..., Timestamp, and Host is visible. A 'Bind Certificate' button is highlighted in the interface.

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

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?

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.

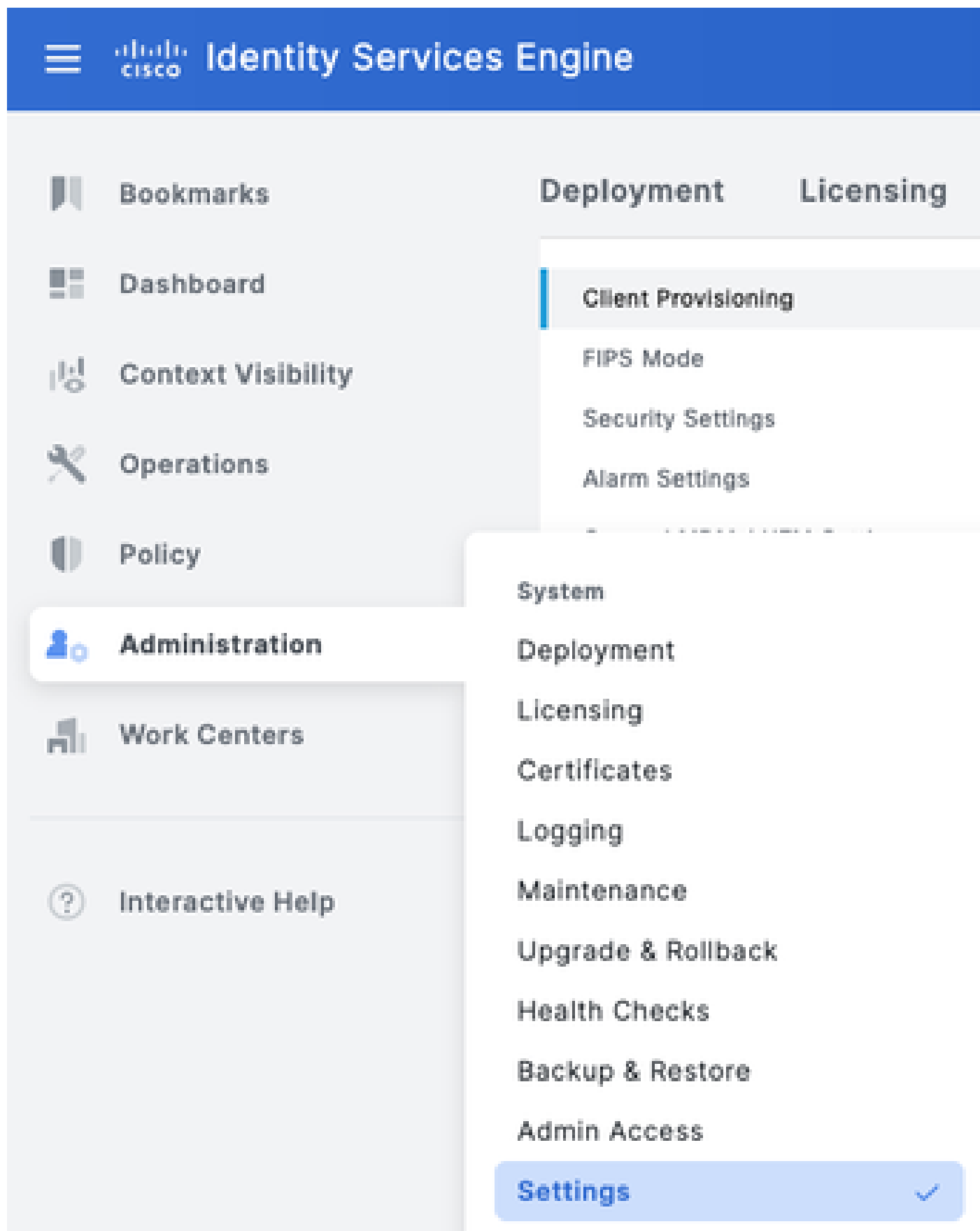
[Edit](#) [Generate Self Signed Certificate](#) [Import](#) [Export](#) [Delete](#) [View](#)

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#000010	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 Cisco ISE Administration console. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, **Administration**, Work Centers, and Interactive Help. The main content area is titled 'Deployment Nodes' and includes a sub-menu on the left with 'Deployment' and 'PAN Failover'. The 'Deployment' sub-menu is expanded, showing a list of nodes. The 'Edit' button for the 'ISE1' node is highlighted with a red box. The table below shows the details of the selected node.

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

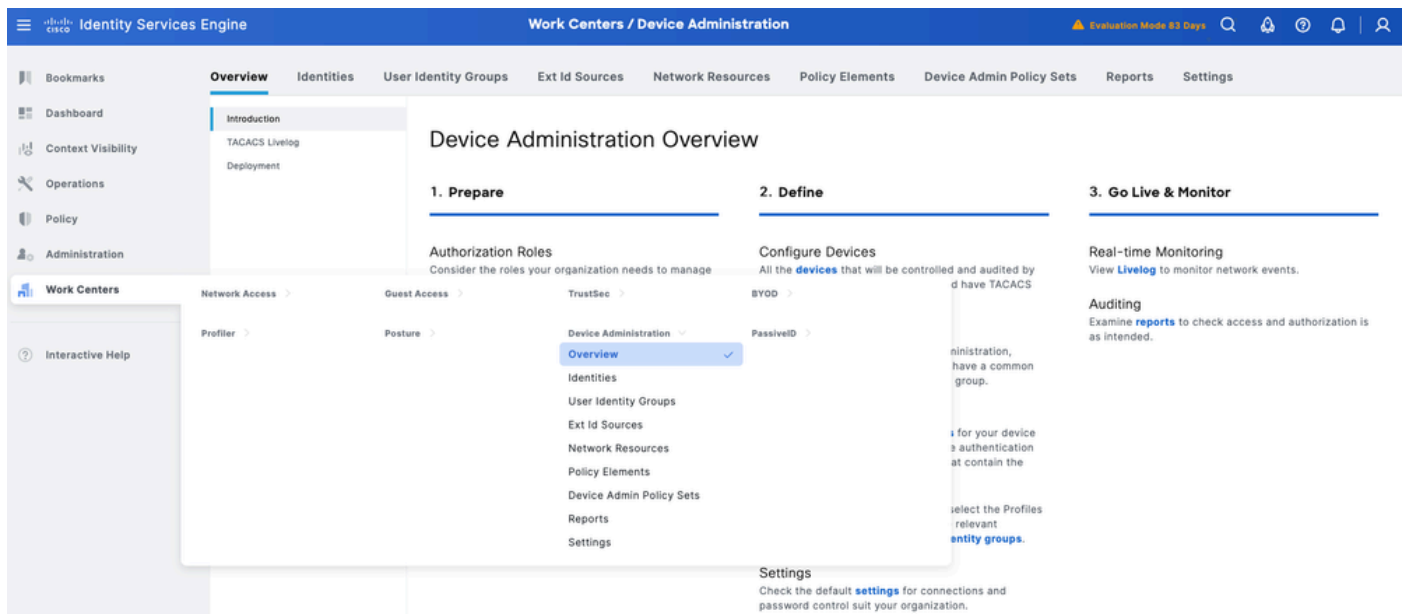
Step 2. Under **General Settings**, scroll down and select the **check box** next to **Enable Device Admin Service**.

The screenshot shows the Cisco ISE Administration console. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, **Administration**, Work Centers, and Interactive Help. The main content area is titled 'Administration / System' and includes a sub-menu on the left with 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade & Rollback', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Deployment' sub-menu is expanded, showing a list of nodes. The 'General Settings' section is visible, and the 'Enable Device Admin Service' checkbox is highlighted with a red box.

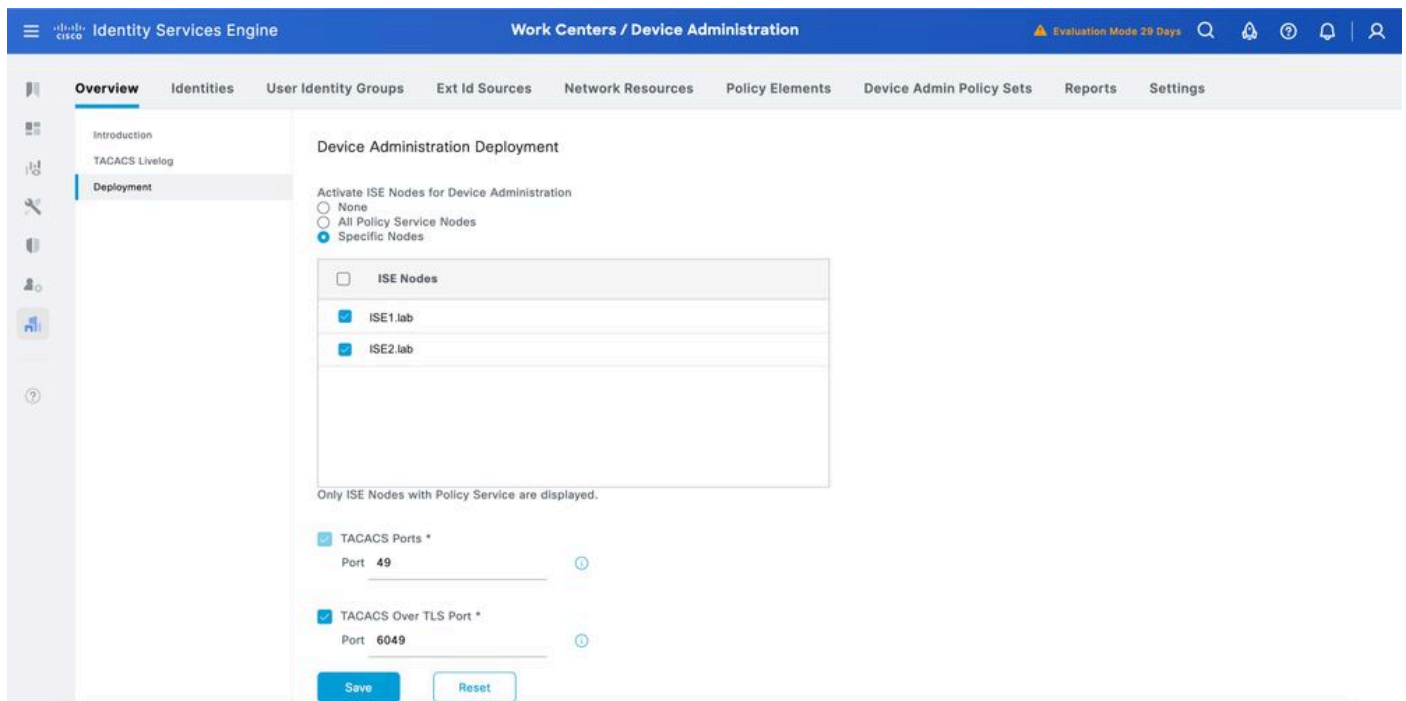
Step 3. **Save** the configuration. Device Admin Service is now enabled on ISE.

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**.

Create 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 Resources**. Click **Network Device Groups** and create a group with the name **IOS XE**.

Add Group

Name*

IOSXE



Description

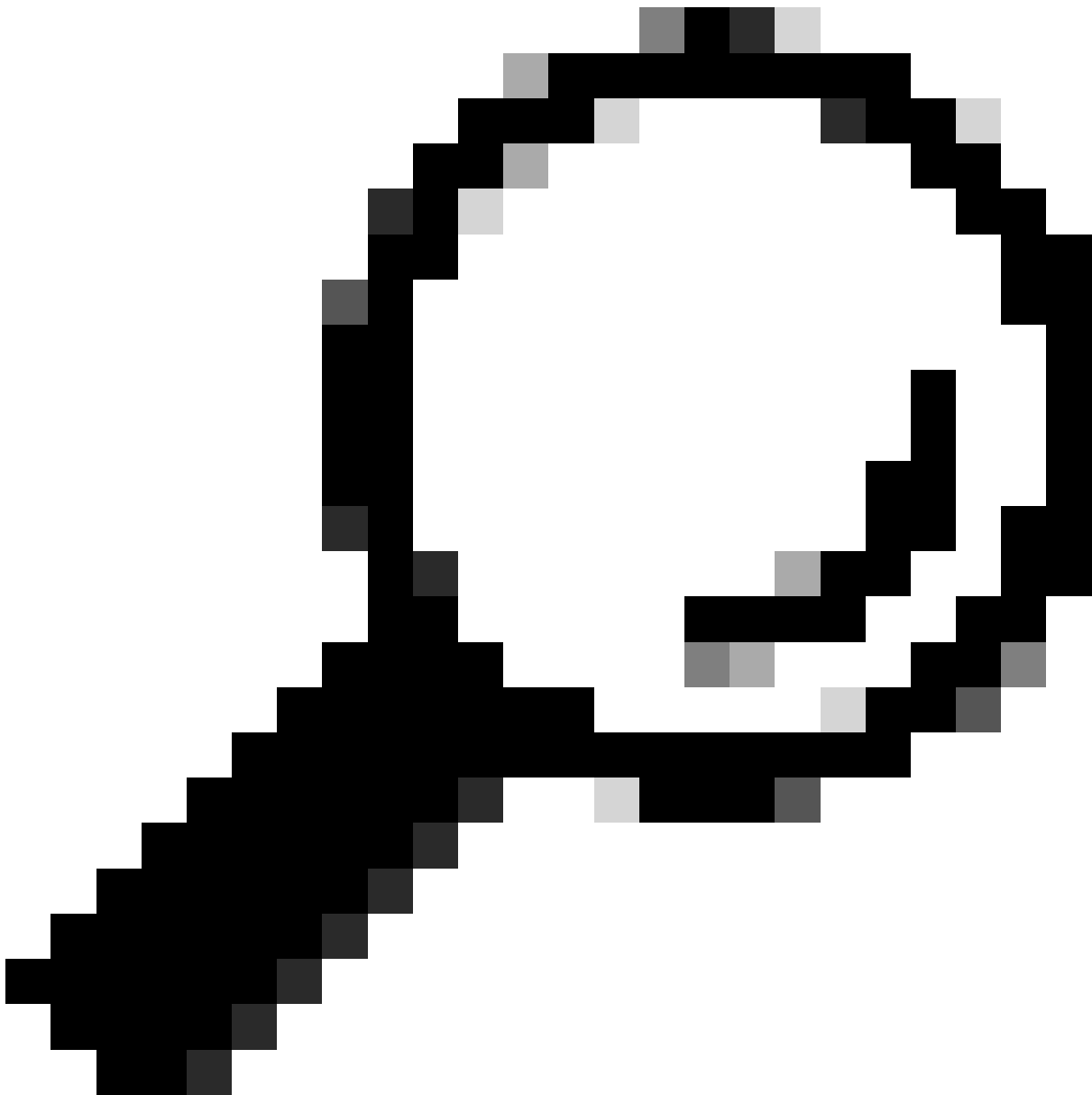
Parent Group*

Select Group or Add as root group



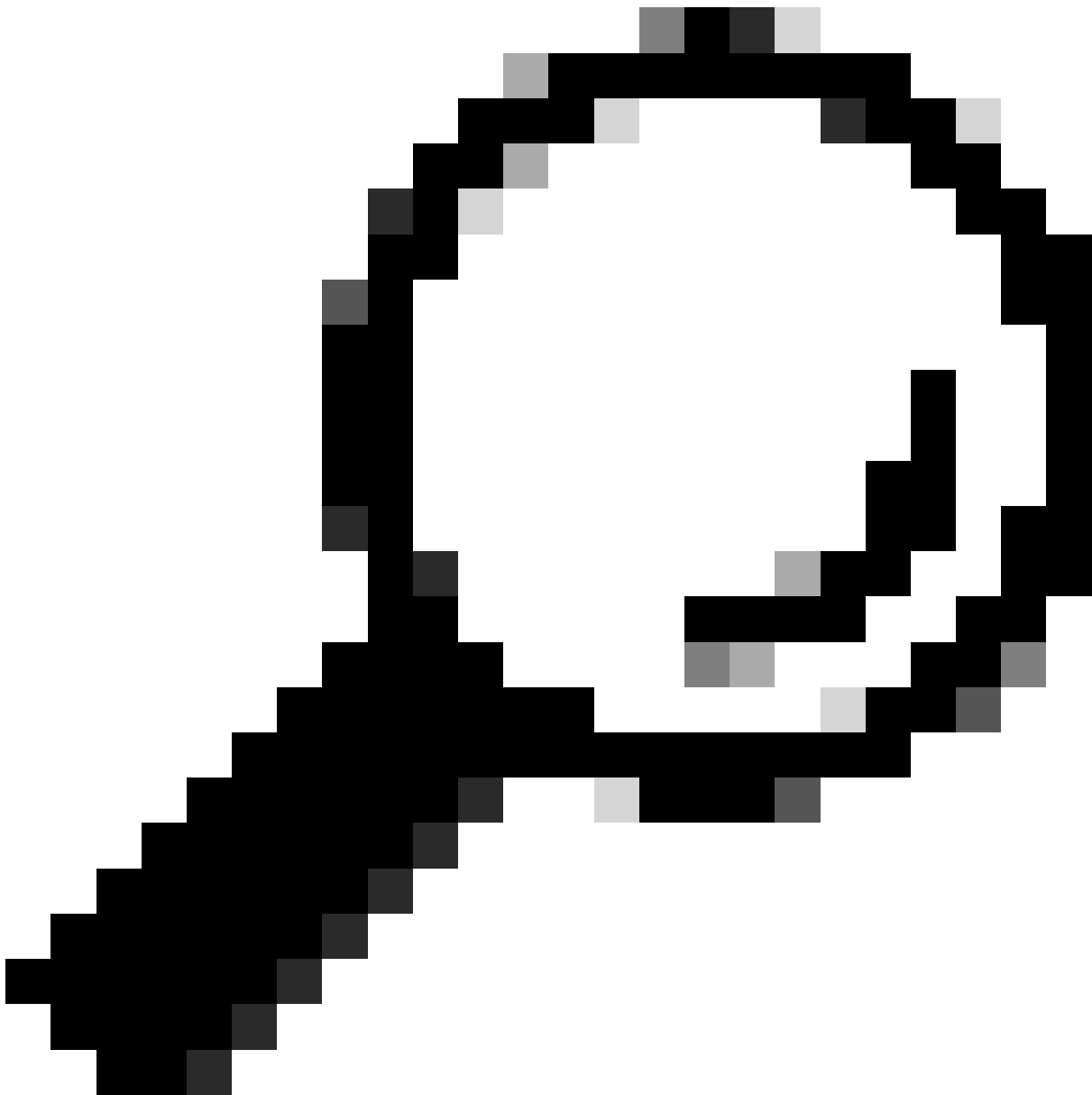
Cancel

Save



Tip: All Device Types and All Locations are default hierarchies provided by ISE. You can 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 Cisco IOS XE device as a Network Device. Navigate to **Work Centers > Device Administration > Network Resources > Network Devices**. Click **Add** to add a new Network Device. For this test, it would be **SVS_BRPASR1K**.

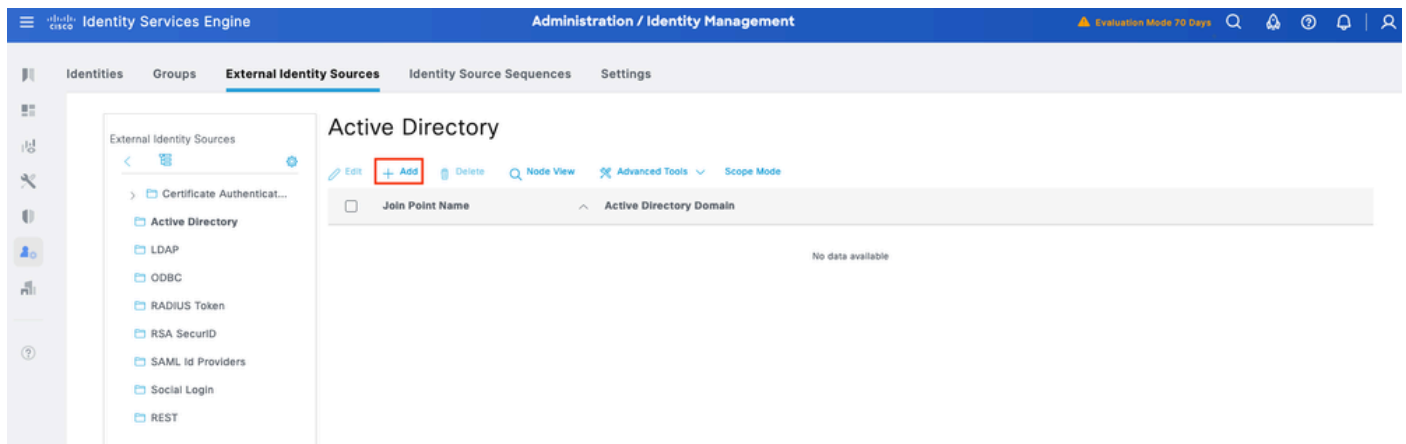


Tip: It is recommended to Enable Single Connect Mode to avoid restarting the TCP session each time a command is sent to the device.

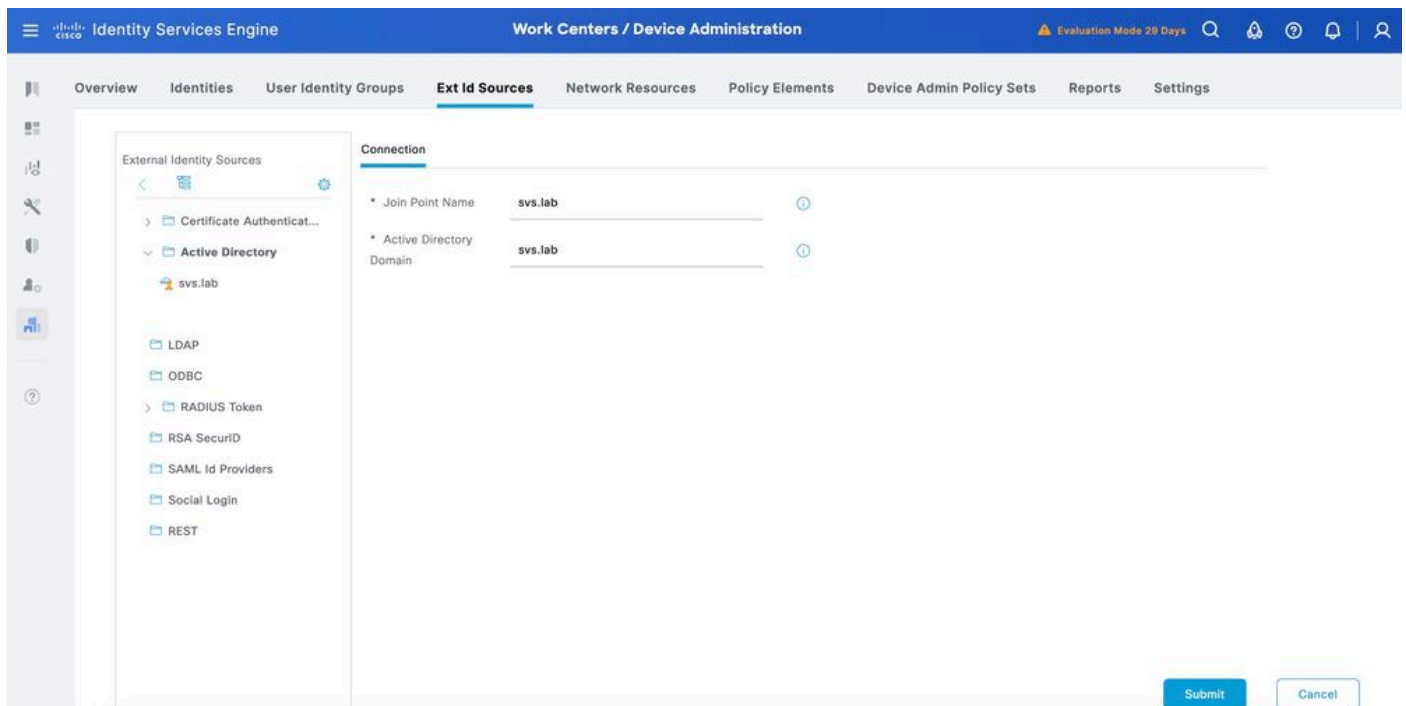
Configure Identity Stores

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.

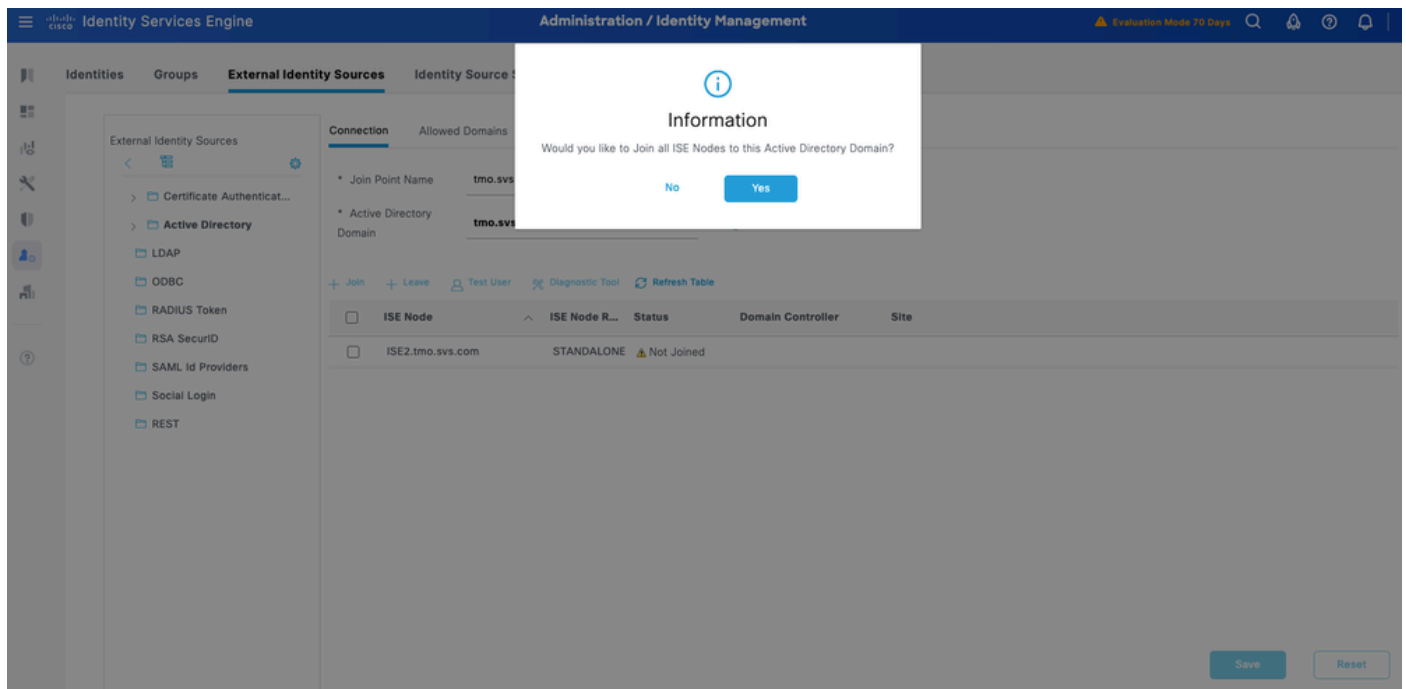
Step1. Navigate to **Administration > Identity Management > External Identity Stores > Active Directory**. Click **Add** to define a new AD Joint Point.



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?**



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

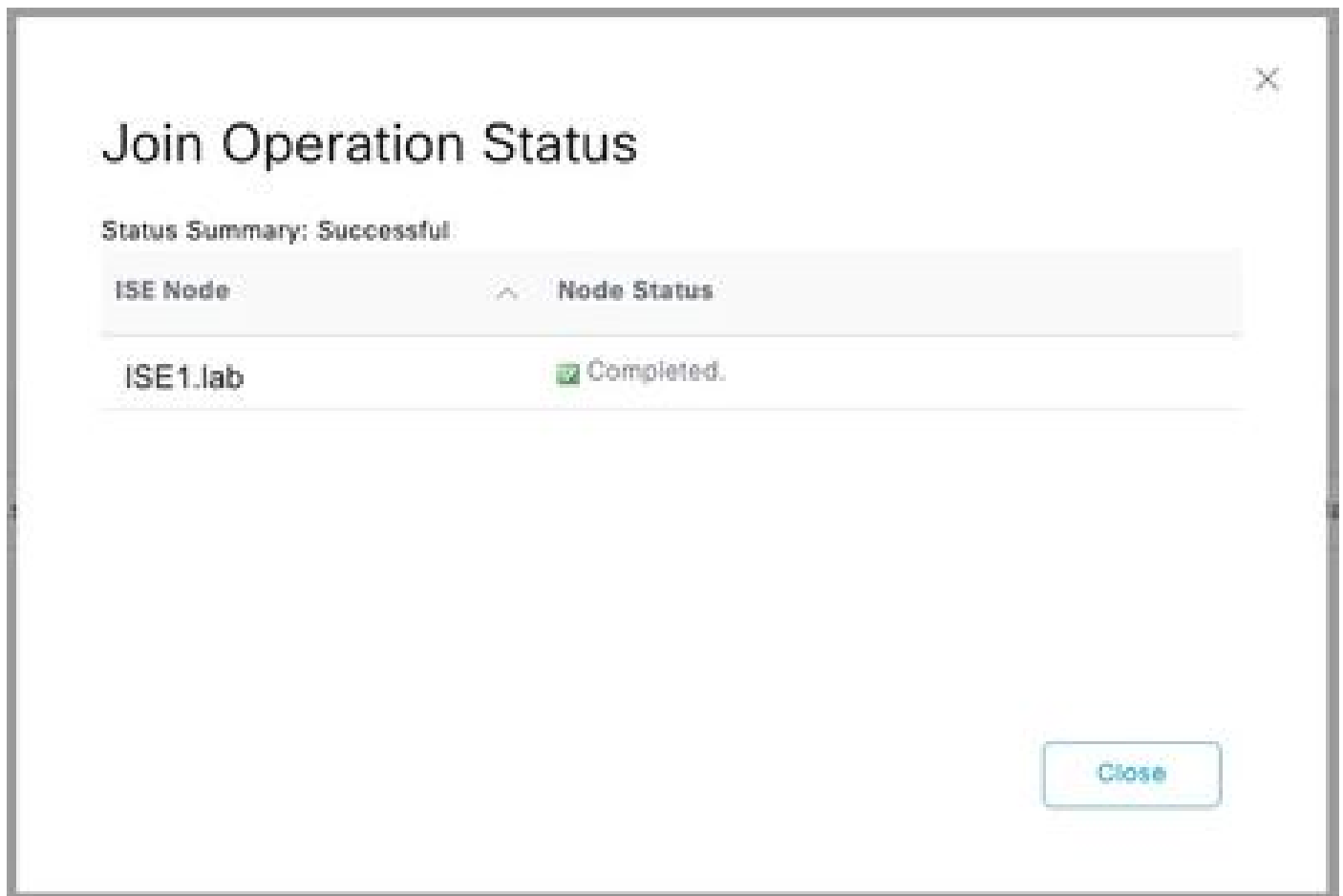
* Password ⓘ

☐ Specify Organizational Unit ⓘ

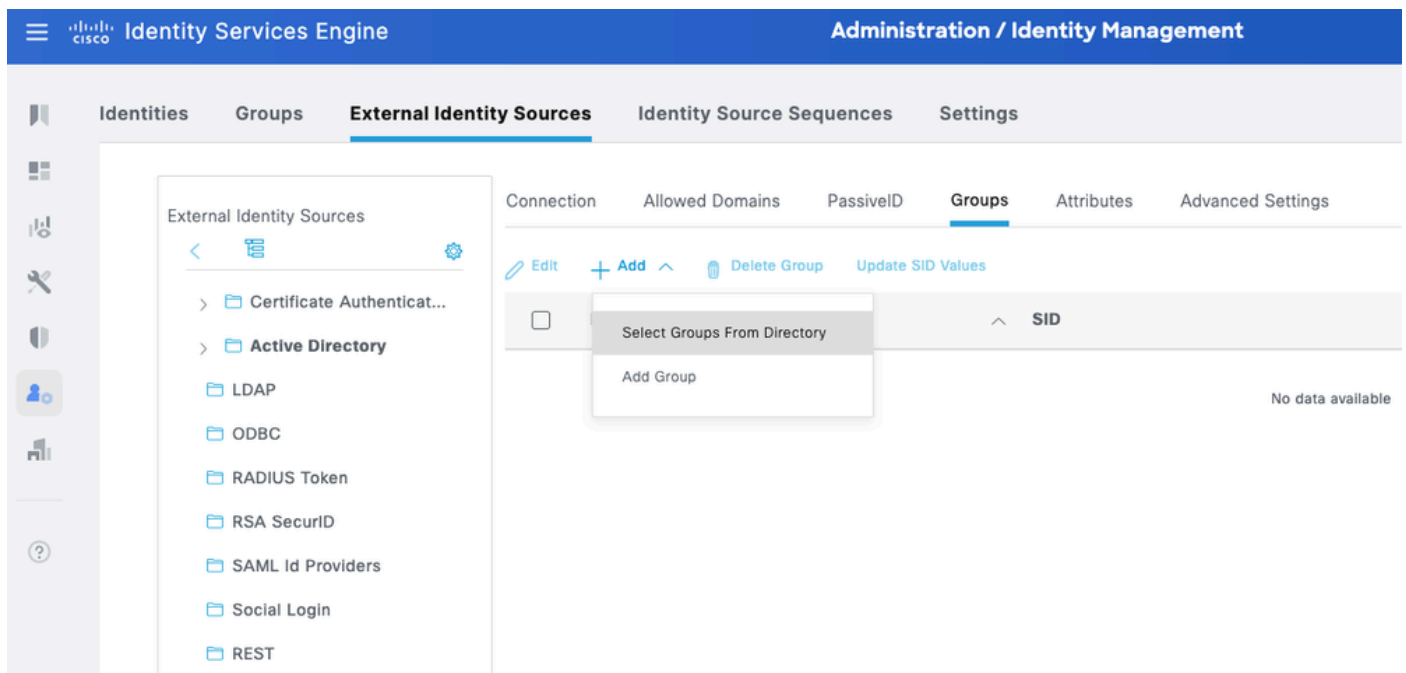
☒ Store Credentials ⓘ

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

svs.lab

Name

Device *

SID *

Type

Filter

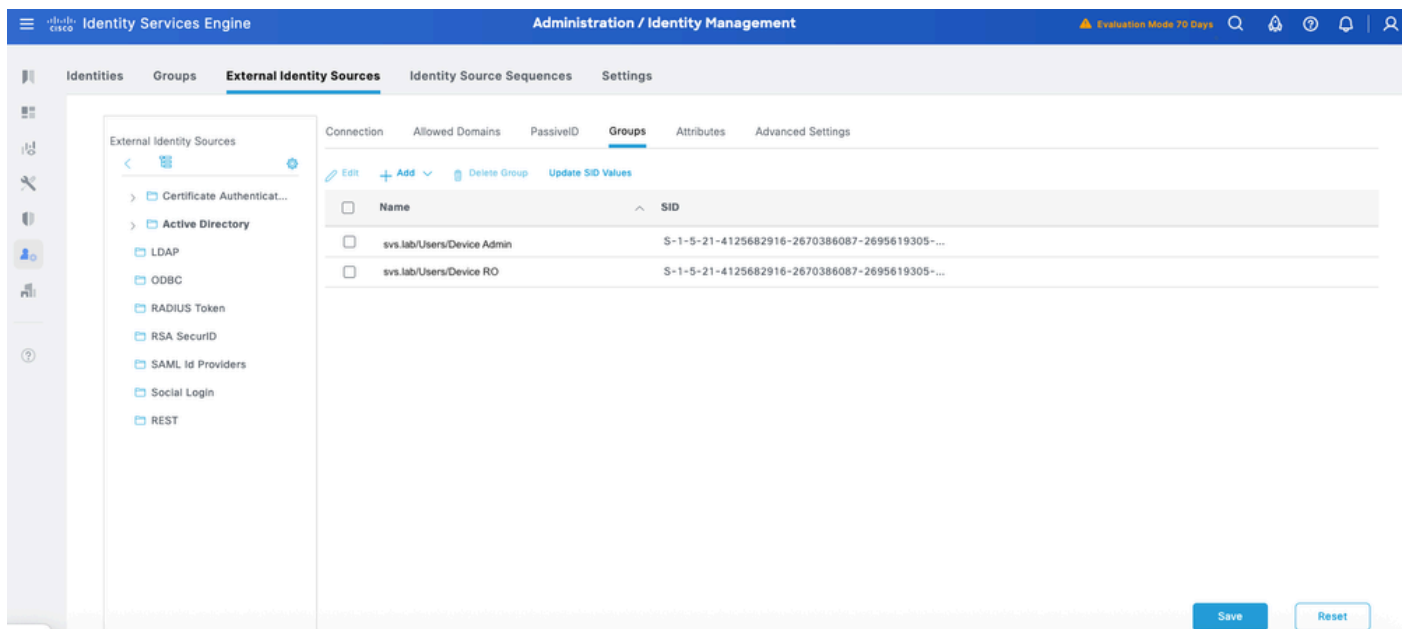
Filter

ALL

Retrieve Groups...

2 Groups Retrieved.

☐	Name	Group SID	Group Type
☐	svs.lab/Users/Device Admin	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL
☐	svs.lab/Users/Device RO	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL



ConfigureTACACS+ Profiles

You are going to map the TACACS+ Profiles to the two main user roles on the Cisco IOS XE devices:

- Root System Administrator – This is the highest-privileged role in the device. The user with the root system administrator role has full administrative access to all system commands and configuration capabilities.
- Operator –This role is intended for users who need read-only access to the system for monitoring and troubleshooting purposes.

These are defined as two TACACS+ Profiles: IOS_XE_RW and IOSXR_RO.

IOS_XE_RW - Administrator Profile

Step 1 Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**. Add a new TACACS Profile and name it **IOS_XE_RW**.

Step 2. Check and set the **Default Privilege** and **Maximum Privilege** as **15**.

Step 3. Confirm the config and **Save**.

Identity Services Engine

Work Centers / Device Administration

OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork ResourcesPolicy ElementsDevice Admin Policy SetsMore

Conditions>

Network Conditions>

Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles > IOSXE_RW

TACACS Profile

Name

IOSXE_RW

Description

Task Attribute ViewRaw View

Common Tasks

Common Task TypeShell

☒ Default Privilege

15

(Select 0 to 15)

☒ Maximum Privilege

15

(Select 0 to 15)

IOS XE_RO - Operator Profile

Step 1 Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**. Add a new **TACACS Profile** and name it **IOS XE_RO**.

Step 2. Check and set the **Default Privilege** and **Maximum Privilege** as **1**.

Step 3. Confirm the config and **Save**.

Identity Services Engine

Work Centers / Device Administration

OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork ResourcesPolicy ElementsDevice Admin Policy SetsMore

Conditions>

Network Conditions>

Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles > IOSXE_RO

TACACS Profile

Name

IOSXE_RO

Description

Task Attribute ViewRaw View

Common Tasks

Common Task TypeShell

☒ Default Privilege

1

(Select 0 to 15)

☒ Maximum Privilege

1

(Select 0 to 15)

☐ Access Control List

☐ Auto Command

ConfigureTACACS+ Command Sets

these are defined as two TACACS+ Commands Sets: **CISCO_IOS XE_RW** and **CISCO_IOS XE_RO**.

CISCO_IOS XE_RW - Administrator Command Set

Step 1. Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets**. Add a new **TACACS Command Set** and name it **CISCO_IOS XE_RW**.

Step 2. Check the **Permit any command that is not listed below** checkbox (this allows any command for the administrator role) and click **Save**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Work Centers / Device Administration'. The left sidebar contains a menu with 'Overview', 'Identities', 'User Identity Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements', 'Device Admin Policy Sets', and 'More'. The 'Policy Elements' section is active, showing a breadcrumb trail: 'TACACS Command Sets > CISCO_IOSXE_RW Command Set'. The main content area has a 'Name' field with the value 'CISCO_IOSXE_RW' and a 'Description' text area. Below these is the 'Commands' section, which includes a checkbox labeled 'Permit any command that is not listed below' that is checked. At the bottom, there is a table with columns 'Grant', 'Command', and 'Arguments'. The 'Grant' column has a checkbox, and the 'Command' column has a dropdown menu.

CISCO_IOS XE_RO - Operator Command Set

Step 1 From ISE UI, navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets**. Add a new **TACACS Command Set** and name it **CISCO_IOS XE_RO**.

Step 2. In **Commands section**, add a new **command**.

Step 3. Select **Permit** from the dropdown list for **Grant** column and enter **show** on the **Command** column; and click the **check arrow**.

Step 4. Confirm the data and click **Save**.

Policy Elements

TACACS Command Sets > CISCO_IOSXE_RO

Command Set

Name: CISCO_IOSXE_RO

Description:

Commands

Permit any command that is not listed below ☐

Add Trash Edit Move Up Move Down

Grant	Command	Arguments
☐	PERMIT	show

Configure Device Admin Policy Sets

Policy Sets are enabled by default for Device Administration. Policy Sets can divide policies based on the Device Types so to ease application of TACACS profiles.

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

Device Admin Policy Sets

Reset Reset Policy Set Hit Counts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
☒	IOS-XE devices		DEVICE:Device Type EQUALS All Device Types#IOS-XE	Default Device Admin	0		

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**.

The screenshot shows the Cisco ISE Work Centers / Device Administration interface. The 'Device Admin Policy Sets' tab is selected, displaying a table of policy sets for 'IOS-XE devices'. The table has columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A search bar is located above the table. Below the table, an 'Authentication Policy(1)' section is visible, showing a 'Default' policy. On the right, a sidebar for 'svs.lab' displays configuration options: 'If Auth fail' set to REJECT, 'If User not found' set to REJECT, and 'If Process fail' set to DROP. Buttons for 'Reset', 'Reset Policy Set Hit Counts', and 'Save' are at the top right.

Step 4. Define the Authorization Policy.

Create the **authorization policy** based on user groups in Active Directory (AD).

For Example:

- Users in the AD group **Device RO** are assigned the **CISCO_IOSXR_RO** Command Set and the **IOSXR_RO** Shell Profile.
- Users in the AD group **Device Admin** are assigned the **CISCO_IOSXR_RW** Command Set and the **IOSXR_RW** Shell Profile.

Identity Services Engine

Work Centers / Device Administration

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

More

Policy Sets→ IOS-XE devices

Reset

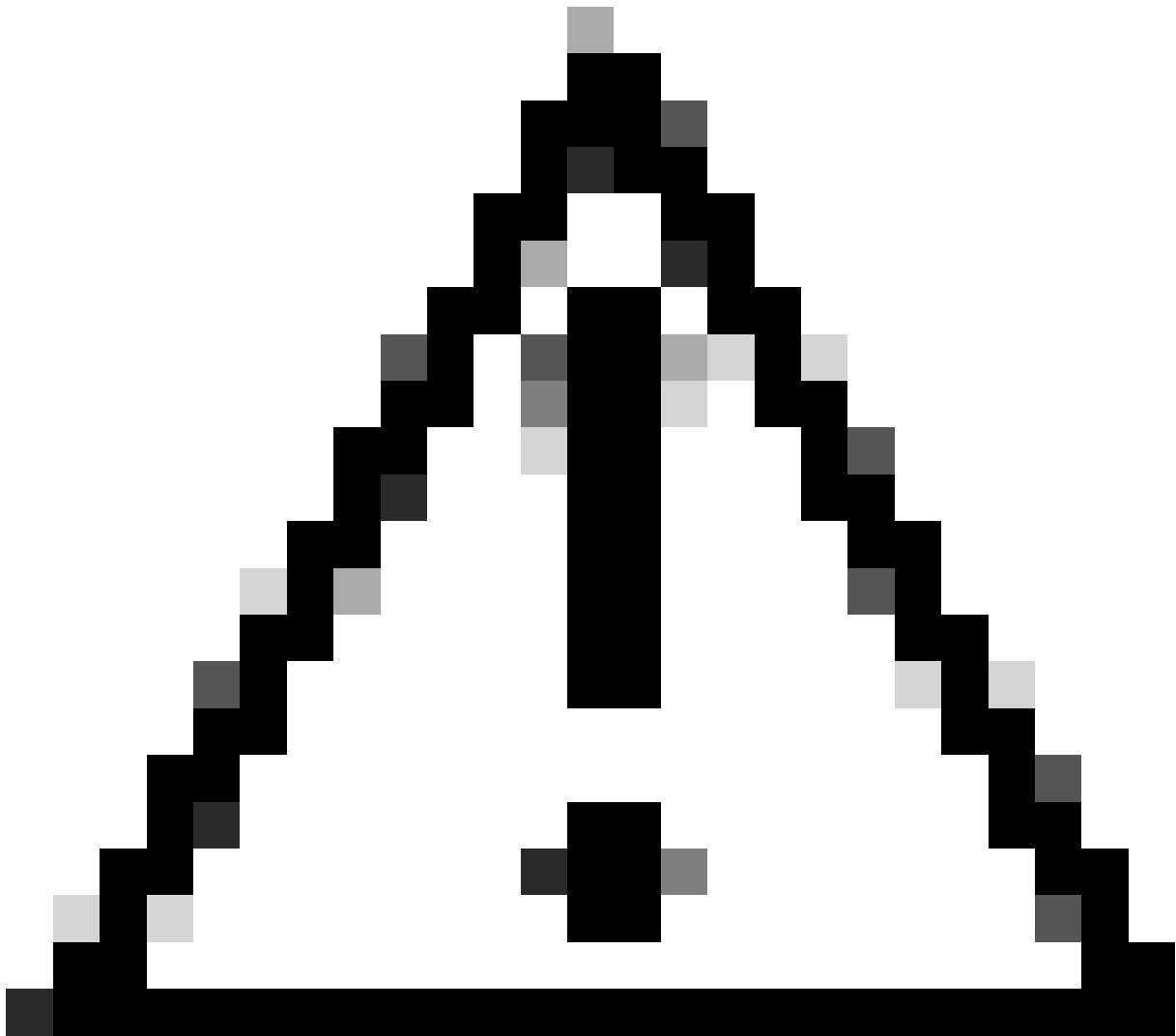
Reset Policy Set Hit Counts

Save

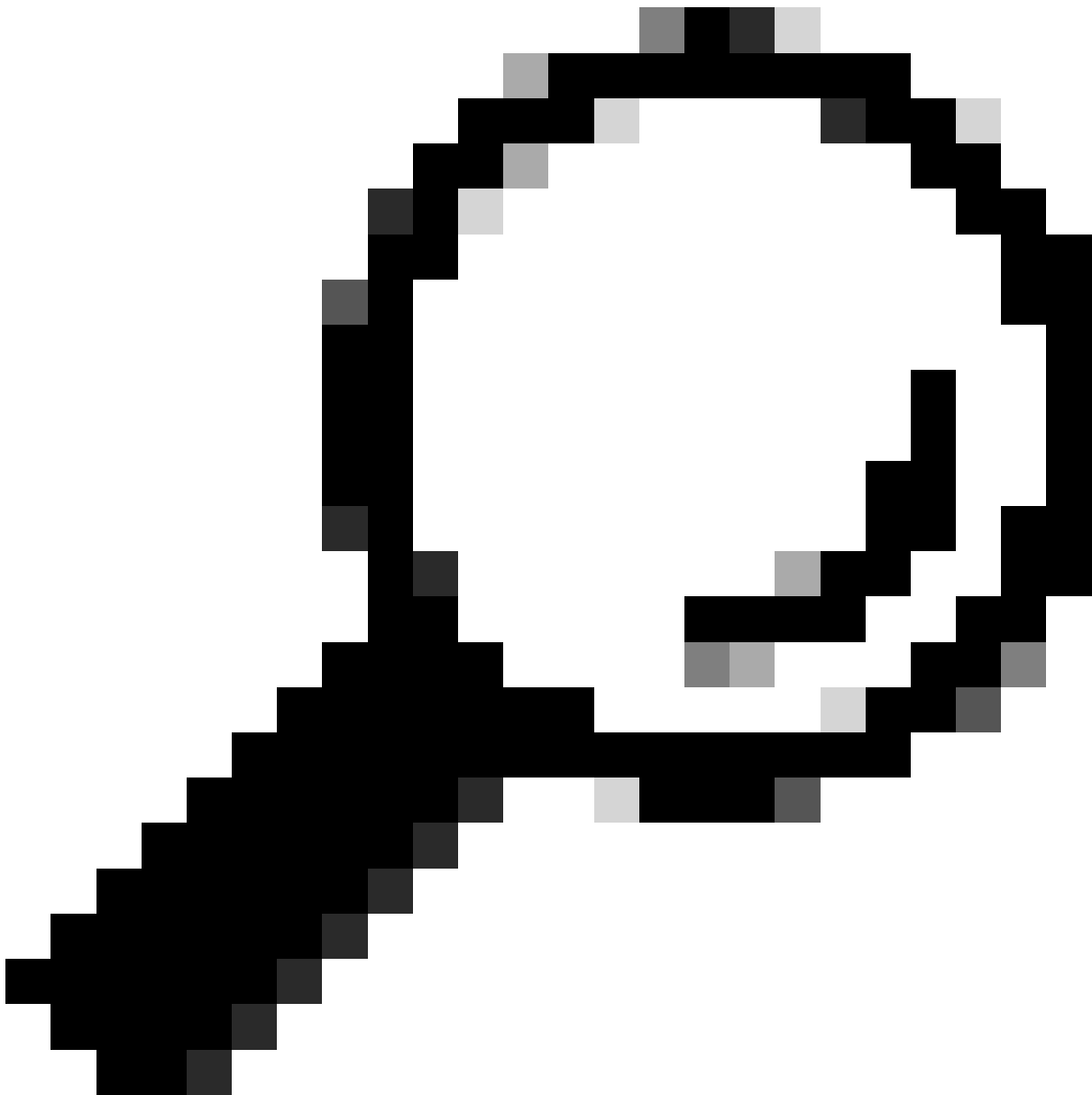
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Q Search	✓ IOS-XE devices		DEVICE-Device Type EQUALS All Device Types#IOS-XE	Default Device Admin +	0
> Authentication Policy(1)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
< Authorization Policy(3)					

				Results			
+ Status	Rule Name	Conditions		Command Sets	Shell Profiles	Hits	Actions
Q Search							
✓	Authorization Rule RO	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device RO		CISCO_IOSXE_RO +	IOSXE_RO +	0	
✓	Authorization Rule RW	svs.lab-ExternalGroups EQUALS svs.lab/Users/Device Admin		CISCO_IOSXE_RW +	IOSXE_RW +	0	
✓	Default			DenyAllCommands +	Deny All Shell Profile +	0	

Part 2 - Configure Cisco IOS XE for TACACS+ over TLS 1.3



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.

Configuration Method 1 - Device Generated Key-pair

TACACS+ Server Configuration

Step 1 Configure **domain name** and generate a **key-pair** used for router trustpoint.

```
ip domain name svcs.lab
```

```
crypto key generate ec keysize 256 label svcs-256ec-key
```

Trustpoint Configuration

Step 1 Create **router trustpoint** and associate the key-pair.

```
crypto pki trustpoint svcs_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair svcs-256ec-key
```

Step 2. Authenticate Trustpoint by installing **CA certificate**.

<#root>

cat9k(config)#

crypto pki authenticate svcs_cat9k

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

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

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmFzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMTM9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZGJAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTyy+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBBjHfM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF30
jMBSqwa4/wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFxmjlBjMmgspObULo/wxMHDtbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzzFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIKB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QbnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBQADAgAHMBkGCWCGSAGG+EIBDQQMFGpTV1MgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
```

```
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfPiYTpokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOmN7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXe/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTwL1It/9T1/F0b0xZRugWcpJrVoTgDGuA==
```

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

Certificate has the following attributes:

Fingerprint MD5: D9C404B2 EC08A260 EC3539E7 F54ED17D

Fingerprint SHA1: 0EB181E9 5A3ED780 3BC5A805 9A854A95 C83AC737

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

yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

cat9k(config)#

Step 3. Generate **Certificate Signing Request (CSR)**.

<#root>

cat9k(config)#

crypto pki enroll svcs_cat9k

% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab

% The subject name in the certificate will include: cat9k.svs.lab

Display Certificate Request to terminal? [yes/no]:

yes

Certificate Request follows:

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

```
MIIBfDCCASMAQAwgYQxGjAYBgNVBAMTEWhtdD1rLnRtby5zdnMuY29tMQwwCgYD
VQQLewNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAxGjAIBgNVBAGT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2F0OWsudG1vLnN2cy5j
b20wWTATBgqhkJOPQIBggqhkJOPQMBBwNCAATpYE7atscrt14ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMSOwKzAcBgNVHREEFATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTWm3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
```

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

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:

no

cat9k(config)#

Step 4. Import **CA signed certificate**.

<#root>

cat9k(config)#

crypto pki import svcs_cat9k certificate

Enter the base 64 encoded certificate.

End with a blank line or the word "quit" on a line by itself

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

```
MIID8zCCAduGAWIBAgIIKfdYWg5WpskWdQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmFzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcnMjUwNTEOMTUxMjAwWhcNMjYwNTEOMTUxMjAwWjCBhDEaMBGGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ21zY28x
DDAKBgNVBACATA1JUDELMAkGA1UECBMCTkMxCzAJBgNVBAYTA1VTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IAB01gtTq2xyu2Xh1168KHdSDGNiLg3igEZaukkFy0rLiYjXmLpFc03uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQRRFg94Y2EgY2Vy
dG1maWNhdGUwHAYDVRORBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMAOGCSqGSIb3DQEBGwUAA4ICAQB0bgKVykeyVC9Usvuu0AUsgaZHGwy2H9Yd
m5vIauI6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAHzY
RtmIM5KIojiDHLtiFpayxv9juDu0ZRx+wYR2PIQ5eLv1bafg7K8E82sq0Cf0tcPr
Oc0NU8UCxq0bd0gu4XsdBN1+wcWFqeQSDLmP7nxvh00m/LXwCWUhwgVio0AuU2Fe
k5NthtvdXNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyZCsTBb6RvL+HsXqBgXGc5
1xCSolTY0dUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvIj4rSPUHQSY+4m
Qq2Sn3iqf4mGh/A08T4iXfWDwfNezh7ZxMsCSCK/ZR1ELZ2hj60fzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxNHFSLBVX5yHXCLEL+CQ7n8Z/pxcB
VVRpItwN3Zb09poZyWiRLTnBsb42xNaWiL9bjQznA0iTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+41OTMawDgGiEv7iaiJ6xWc95EC+Adm0x3FvBXMtIM9qr7WwHW6
3C2hVYHJH254e1V5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAH0FcyXrvG6
3i/1b9erGQ==
```

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

% Router Certificate successfully imported

cat9k(config)#

TACACS & AAA with TLS Configuration

Step 1. Create **TACACSS server** and **AAA groups**, associate the client (router) trustpoint.

```
tacacs server svcs_tacacs
address ipv4 10.225.253.209
single-connection
tls port 6049
```

```
tls idle-timeout 60
tls connection-timeout 60
tls trustpoint client svcs_cat9k
tls ip tacacs source-interface GigabitEthernet0/0
tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svcs_tls
server name svcs_tacacs
ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Step 2. Configure AAA methods.

```
aaa authentication login default group svcs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svcs_tls enable
aaa authorization config-commands
aaa authorization exec default group svcs_tls local if-authenticated
aaa authorization commands 1 default group svcs_tls local if-authenticated
aaa authorization commands 15 default group svcs_tls
aaa accounting exec default start-stop group svcs_tls
aaa accounting commands 1 default start-stop group svcs_tls
aaa accounting commands 15 default start-stop group svcs_tls
aaa session-id common
```

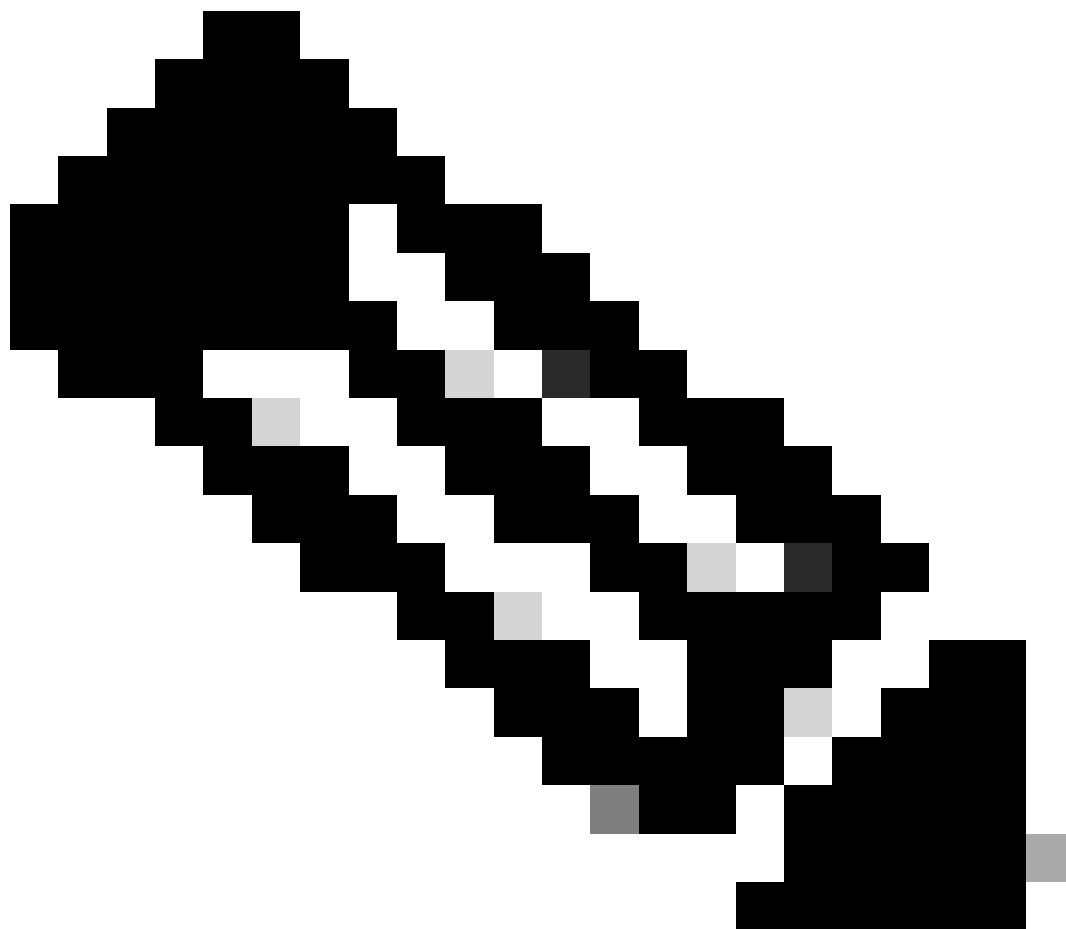
Configuration Method 2 - CA Generated Key-Pair

If you are importing the keys as well as device and CA certificates directly in a PKCS#12 format instead of CSR method, you can use the this method.

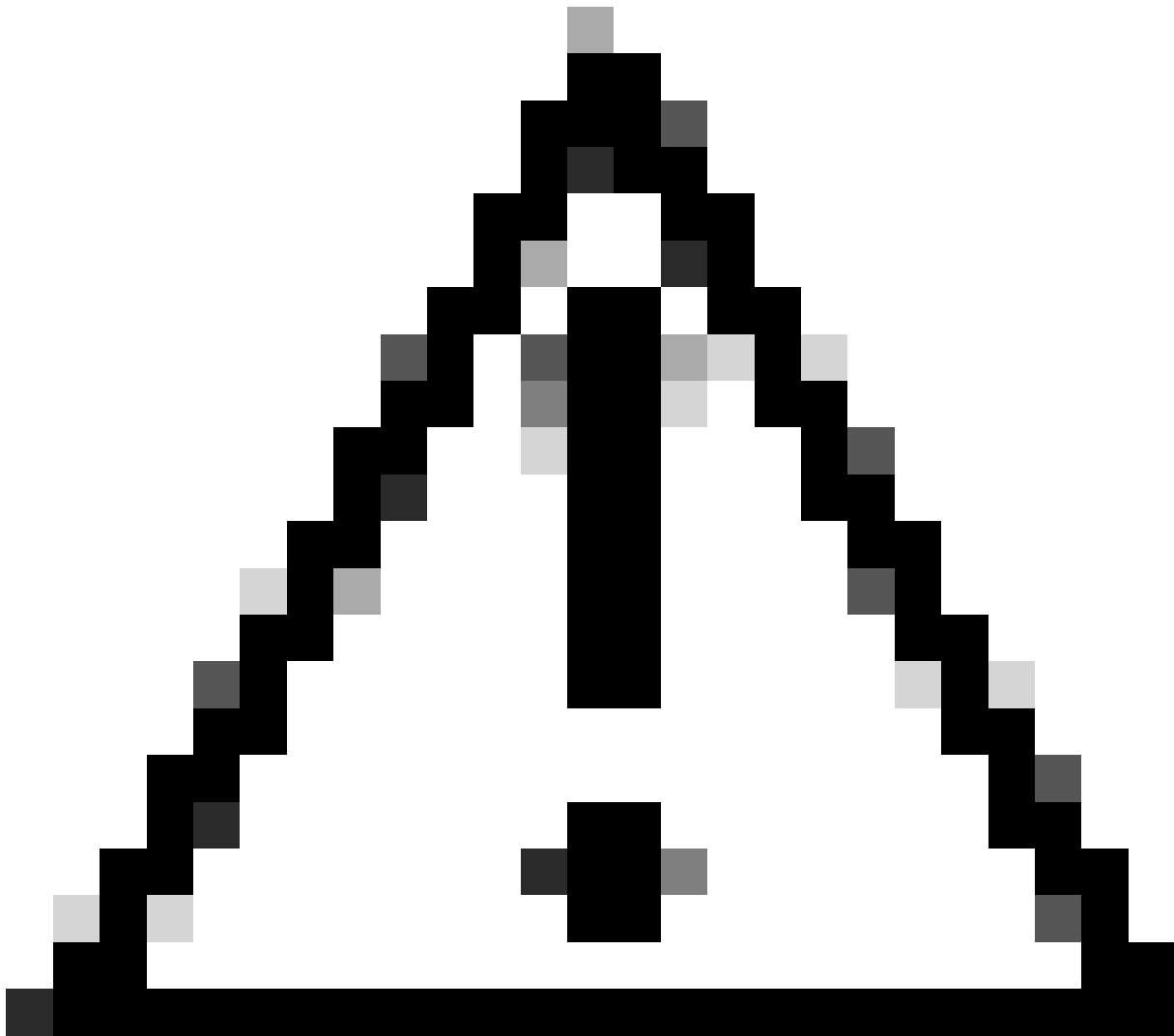
Step 1. Create **client trustpoint**.

```
cat9k(config)#crypto pki trustpoint svcs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

Step 2. Copy the **PKCS#12 file** into bootflash.



Note: Ensure that PKCS#12 file contains the complete certificate chain and the private key as encrypted file.



Caution: Keys in the imported PKCS#12 must be of RSA (E.g.: RSA 2048) type, not ECC.

```
<#root>
```

```
cat9k#
```

```
copy sftp bootflash: vrf Mgmt-vrf
```

```
Address or name of remote host [10.225.253.247]?
```

```
Source username [svs-user]?
```

```
Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx
```

```
Destination filename [cat9k-25jun17.pfx]?
```

```
Password:
```

```
!
```

```
2960 bytes copied in 3.022 secs (979 bytes/sec)
```

Step 3. Import the **PKCS#12 file** using the import command.

```
<#root>
```

cat9k#

crypto pki import svcs_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx

password C1sco.123

% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx

CRYPTO_PKI: Imported PKCS12 file successfully.

cat9k#

cat9k#

show crypto pki certificates svcs_cat9k_25jun17

Certificate

Status: Available

Certificate Serial Number (hex): 5860BF33A2033365

Certificate Usage: General Purpose

Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Subject:

Name: cat9k.svs.lab

e=pkalkur@cisco.com

cn=cat9k.svs.lab

ou=svs

o=cisco

l=rtp

st=nc

c=us

Validity Date:

start date: 17:56:00 UTC Jun 17 2025

end date: 17:56:00 UTC Jun 17 2026

Associated Trustpoints: svcs_cat9k_25jun17

CA Certificate

Status: Available

Certificate Serial Number (hex): 20CD7402C4DA37F5

Certificate Usage: General Purpose

Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Subject:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

Validity Date:

start date: 17:05:00 UTC Apr 28 2025

end date: 17:05:00 UTC Apr 28 2035

Associated Trustpoints: svcs_cat9k_25jun17 svcs_cat9k

Storage: nvram:SVSLabCA#37F5CA.cer

TACACS & AAA with TLS Configuration

Step 1. Create **TACACS server** and **AAA groups**, associate the client (router) trustpoint.

```
tacacs server sv_s_tacacs
address ipv4 10.225.253.209
single-connection
tls port 6049
tls idle-timeout 60
tls connection-timeout 60
tls trustpoint client sv_s_cat9k
tls ip tacacs source-interface GigabitEthernet0/0
tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ sv_s_tls
server name sv_s_tacacs
ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

Step 2. Configure AAA methods.

```
aaa authentication login default group sv_s_tls local enable
aaa authentication login console local enable
aaa authentication enable default group sv_s_tls enable
aaa authorization config-commands
aaa authorization exec default group sv_s_tls local if-authenticated
aaa authorization commands 1 default group sv_s_tls local if-authenticated
aaa authorization commands 15 default group sv_s_tls
aaa accounting exec default start-stop group sv_s_tls
aaa accounting commands 1 default start-stop group sv_s_tls
aaa accounting commands 15 default start-stop group sv_s_tls
aaa session-id common
```

Verification

Verify the configuration.

```
show tacacs
show crypto pki certificates <>
show crypto pki trustpoints <>
```

Debug for AAA & TACACS+.

```
debug aaa authentication
debug aaa authorization
```

```
debug aaa accounting
debug aaa subsys
debug aaa protocol local
debug tacacs authentication
debug tacacs authorization
debug tacacs accounting
debug tacacs events
debug tacacs packet
debug tacacs
debug tacacs secure
```

! Below debugs will be needed only if there is any issue with SSL Handshake

```
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```