

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

Contents

[Introduction](#)

[Overview](#)

[Using this Guide](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Licensing](#)

[Part 1 - ISE Configuration 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](#)

[Configure Identity Stores](#)

[Configure TACACS+ Profiles](#)

[IOS XR RW - Administrator Profile](#)

[IOS XR RO - Operator Profile](#)

[Configure TACACS+ Command Sets](#)

[CISCO IOS XR RW - Administrator Command Set](#)

[CISCO IOS XR RO - Operator Command Set](#)

[Configure Device Admin Policy Sets](#)

[Part 2 - Configure Cisco IOS XR for TACACS+ over TLS 1.3](#)

[Initial Configurations](#)

[Configure Trustpoint](#)

[Configure TACACS & AAA with TLS](#)

[Certificate Renewal](#)

[Verification](#)

[Troubleshooting](#)

Introduction

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

- Part 1 – Configure ISE for Device Admin
- Part 2 - Configure Cisco IOS XR 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 8201 Router, release 25.3.1

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 - ISE Configuration for Device Administration

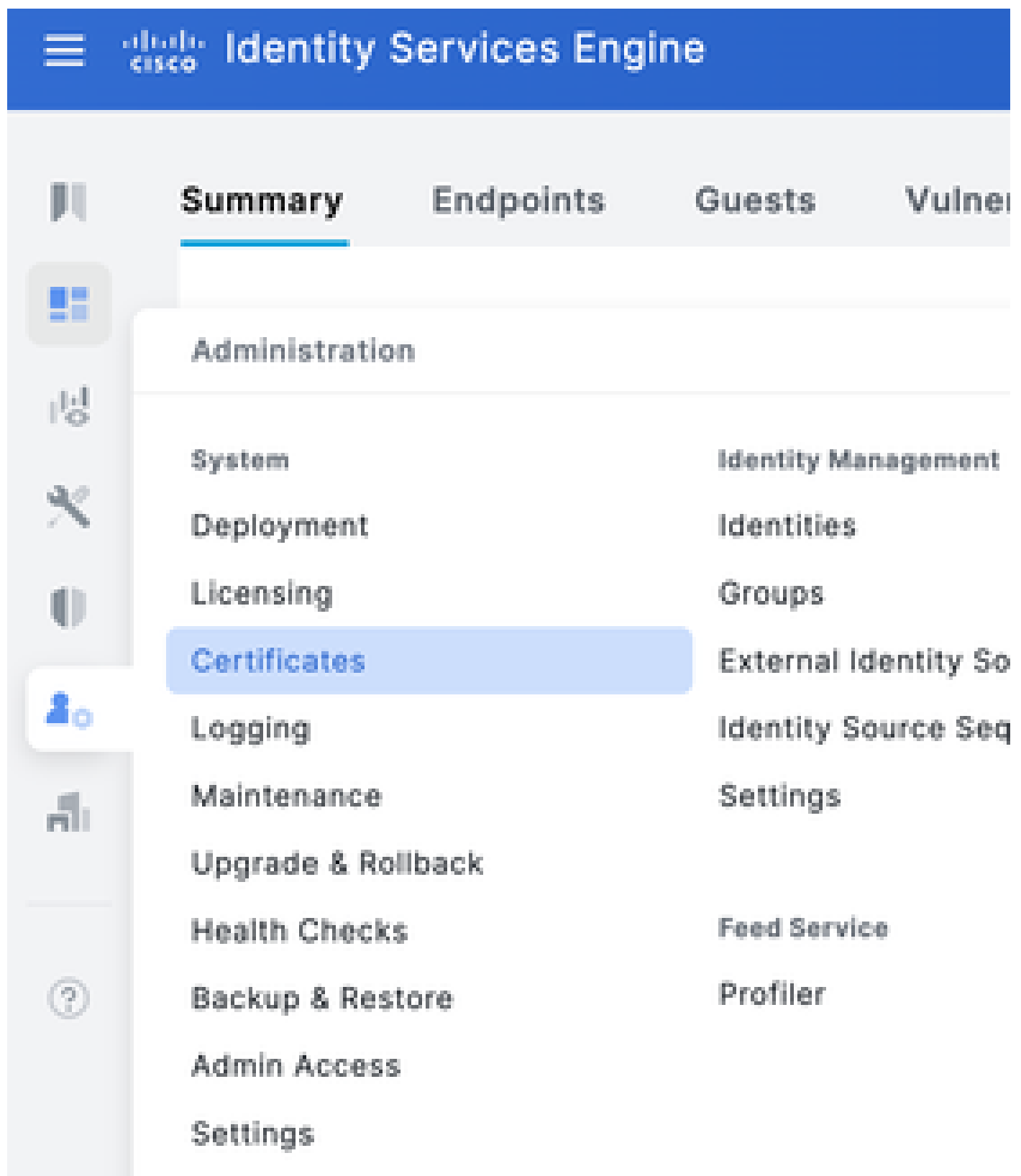
Generate Certificate Signing Request for TACACS+ Server Authentication

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 **PSNs** that 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)

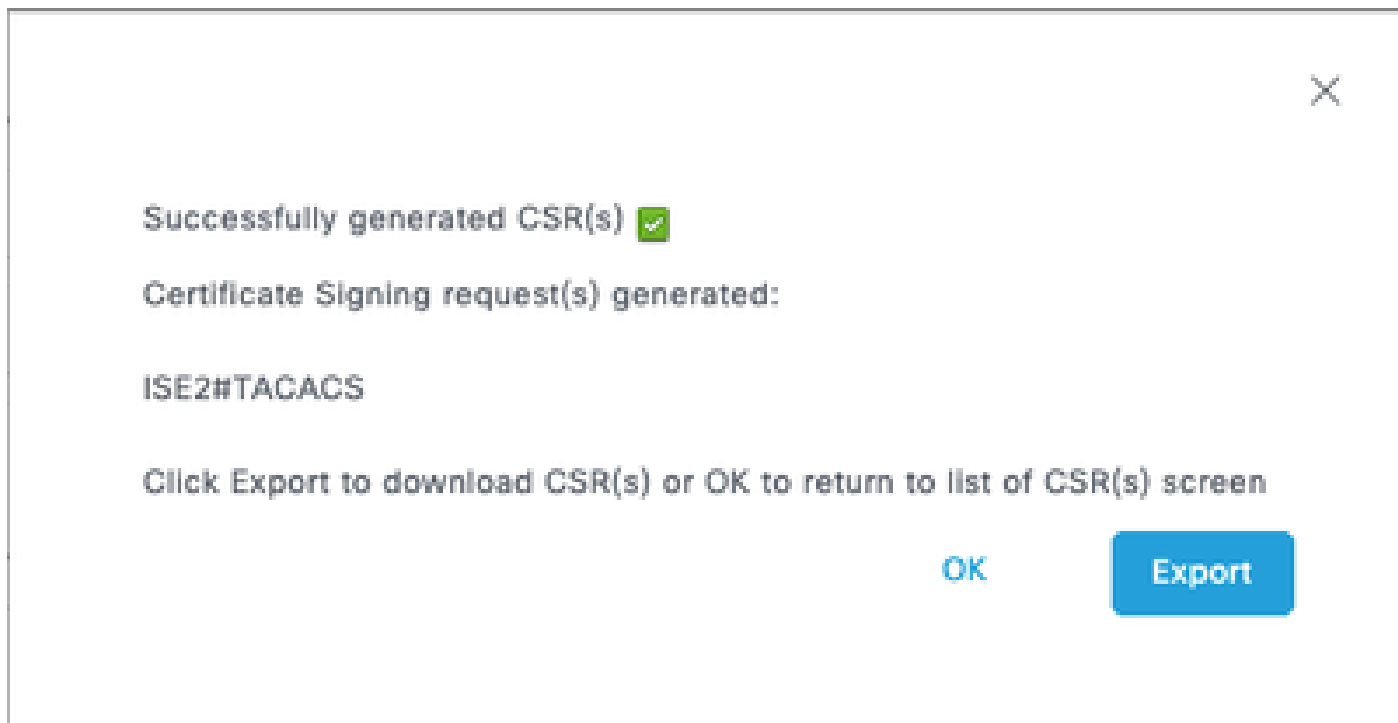
US

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 on **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**.

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

Trusted Certificates For disaster recovery it is recommended to export and backup all your trusted certificates.

Edit Import Export Delete View show internal CA certificates All

☐	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...	Ent
☐	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2...	Ent
☐	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	Ent
☐	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	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...	Ent
☐	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...	Ent
☐	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Ent
☐	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034	Ent

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

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 warning: 'For disaster recovery it is recommended to export and backup all your trusted certificates.' Below this is a table of trusted certificates.

	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Sta
☐	CN=SVS LabCA, OU=SVS, O=Cisco, L=...	Infrastructure Cisco Services Endpoints AdminAuth	20 CD 74 02 ...	SVS LabCA	SVS LabCA	Mon, 28 Apr 2025	Sat, 28 Apr 2...	

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, specifically the 'Certificate Signing Requests' section. The left sidebar is the same as the previous screenshot. The main content area is titled 'Certificate Signing Requests' and includes a button 'Generate Certificate Signing Requests (CSR)'. Below this is a text block explaining the process of signing and binding CSRs. At the bottom, there is a table of certificate signing requests.

	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

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.

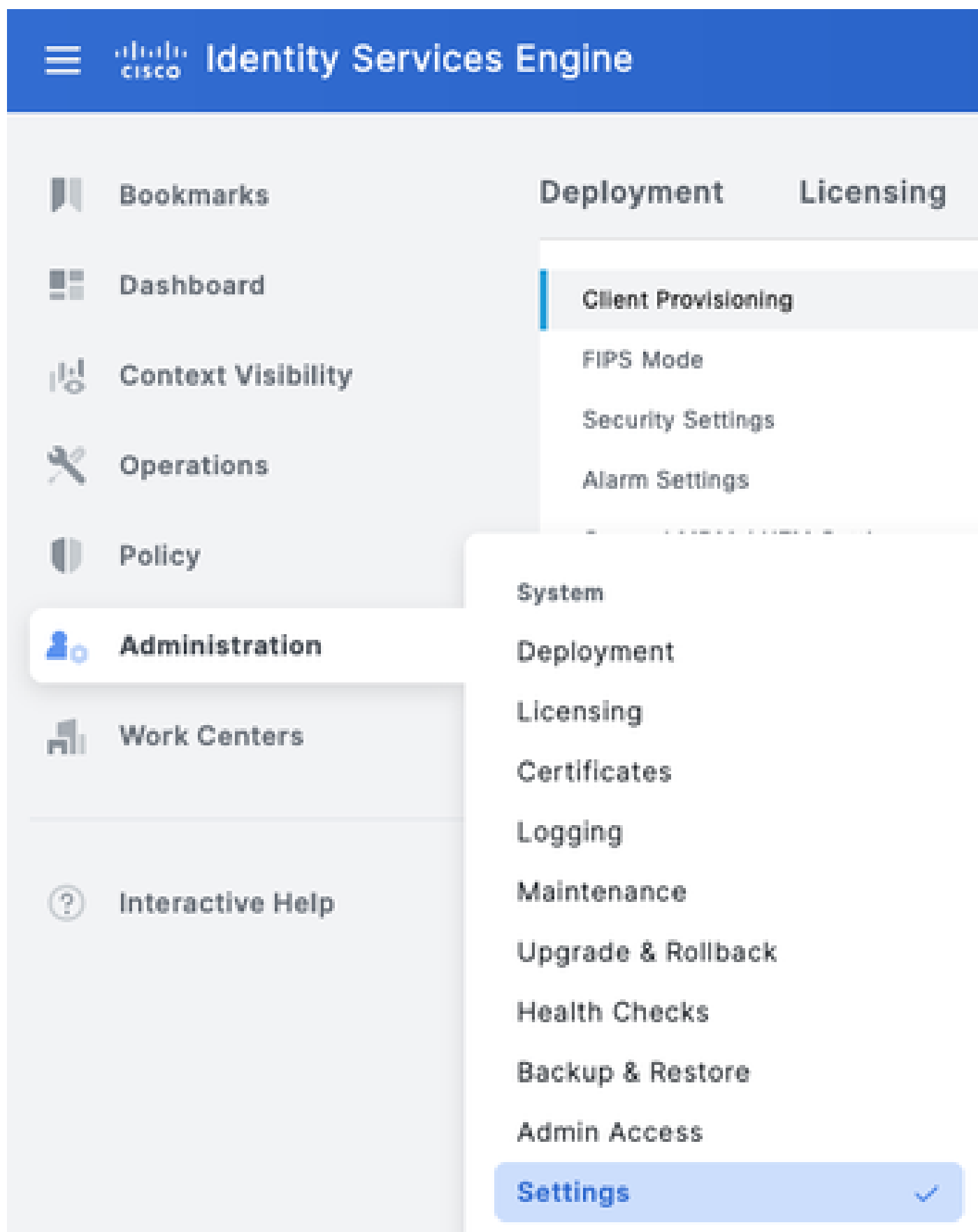
[Edit](#) [Generate Self Signed Certificate](#) [Import](#) [Export](#) [Delete](#) [View](#)

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#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. To 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 (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'. It contains a description of a Cisco ISE node and its roles. Below the description, there is a table of deployment 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	✓

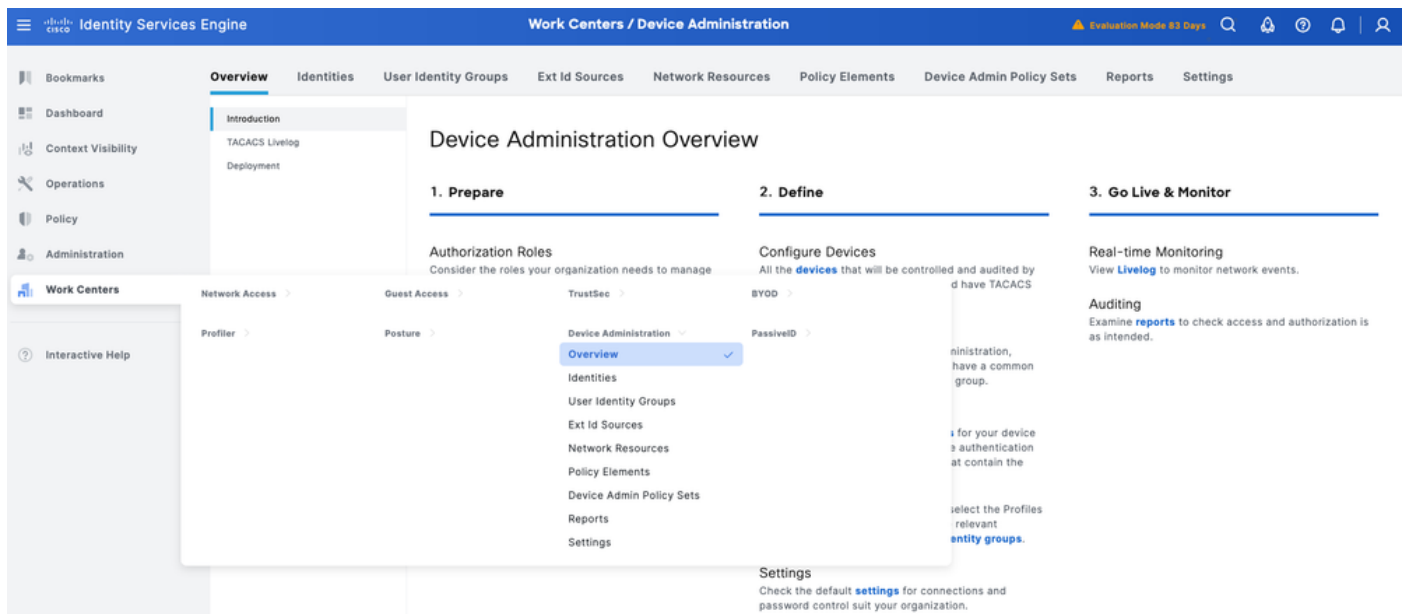
Step 2. Under **General Settings**, scroll down and select the check box next to **Enable Device Admin Service**.

The screenshot shows the Cisco ISE Administration console. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The top navigation bar includes: Administration / System (selected), Evaluation Mode 87 Days, Search, and other icons. The main content area is titled 'General Settings'. It contains various configuration options. The 'Enable Device Admin Service' checkbox is highlighted with a red box.

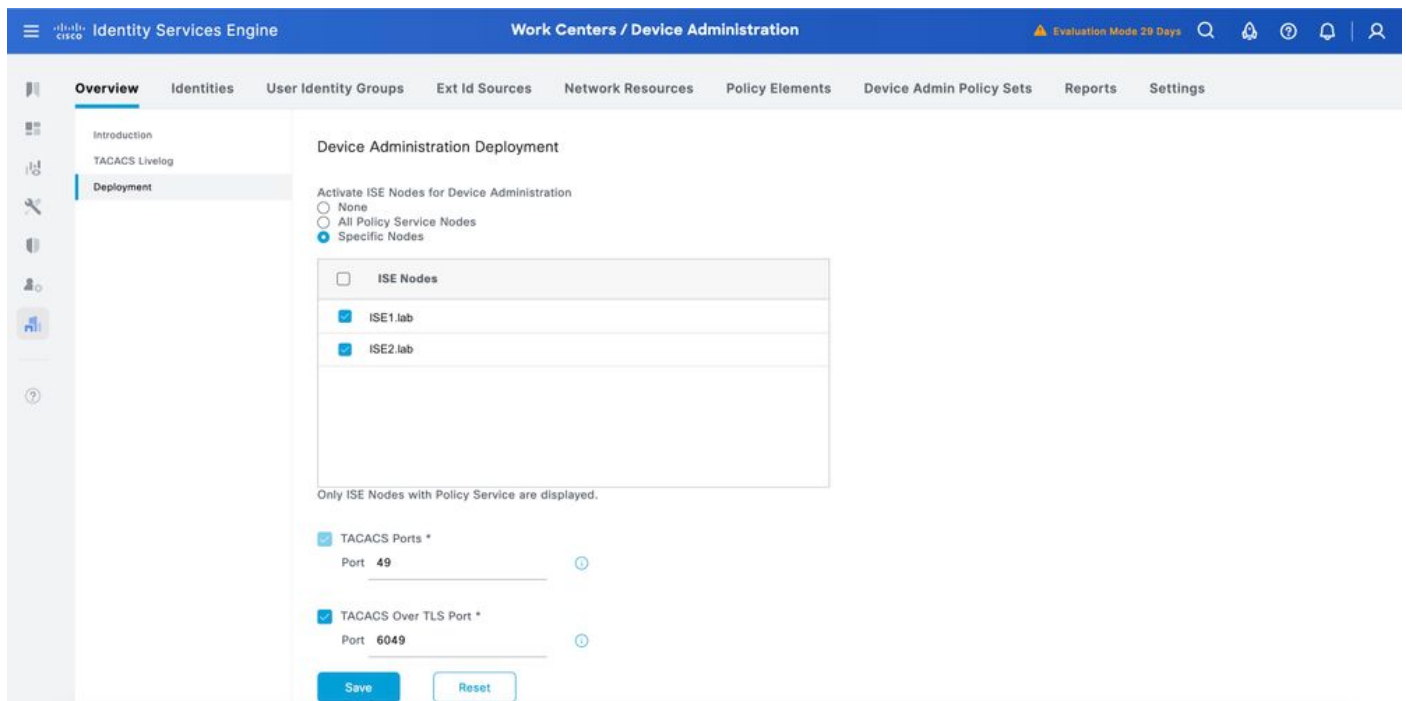
Step 3. **Save** the configuration. Device Admin Service is now enabled on ISE.

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 XR**.

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 93 Days

OverviewIdentitiesUsers

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Admin Policy Sets

More

✕

Edit Group

Name*

IOS-XR

Description

Group Hierarchy

Device Type > All Device Types > IOS-XR

Cancel

Save

☐ ADVA

ADVA SyncDirector Network Time Monitoring

No. of Network Device

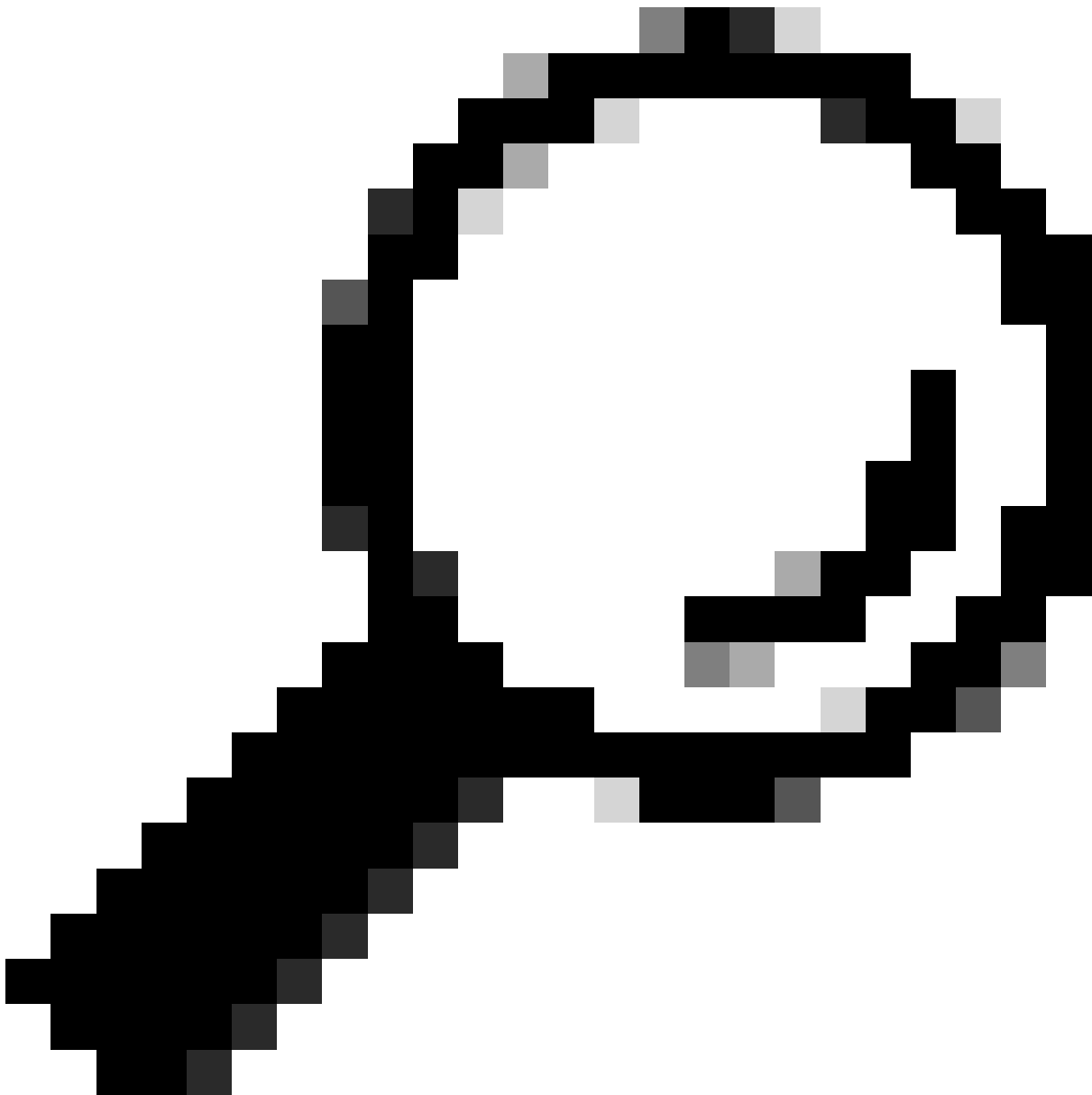
--

702

0

11

243



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 XR device as a Network Device. Navigate to **Work Centers > Device Administration > Network Resources > Network Devices**. Click **Add** to add a new Network Device.

Identity Services Engine Administration / Network Resources Evaluation Mode 11 Days

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxGrid Direct Connectors

Network Devices

Network Devices List > BRC-8201-1

Network Devices

Name

Description

IP Address /

IP Address /

Device Profile

Model Name

Software Version

Network Device Group

Location [Set To Default](#)

IPSEC [Set To Default](#)

Device Type [Set To Default](#)

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

Identity Services Engine Work Centers / Device Administration Evaluation Mode 87 Days

Bookmarks Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements More

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

☐ 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)

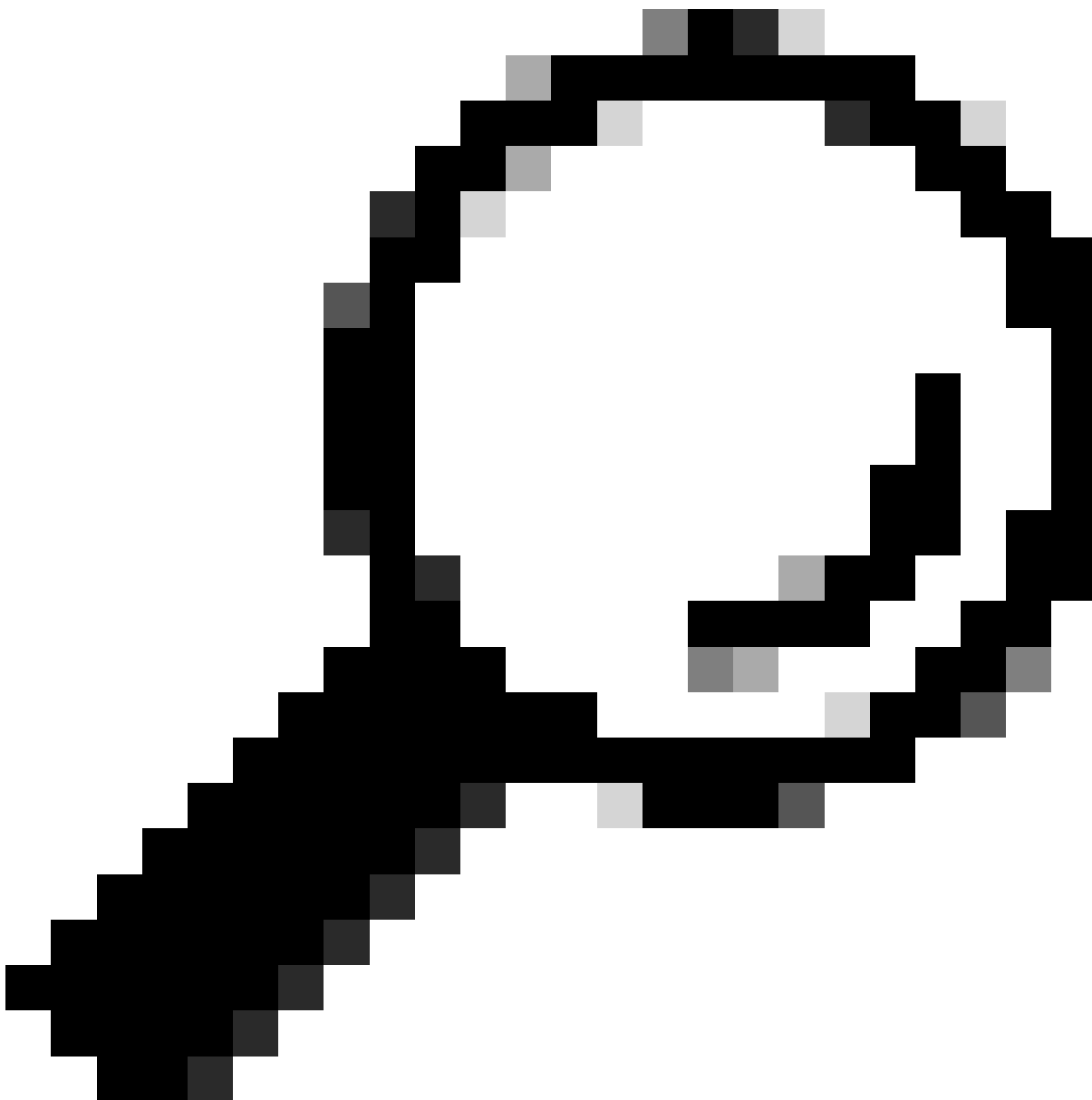
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When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

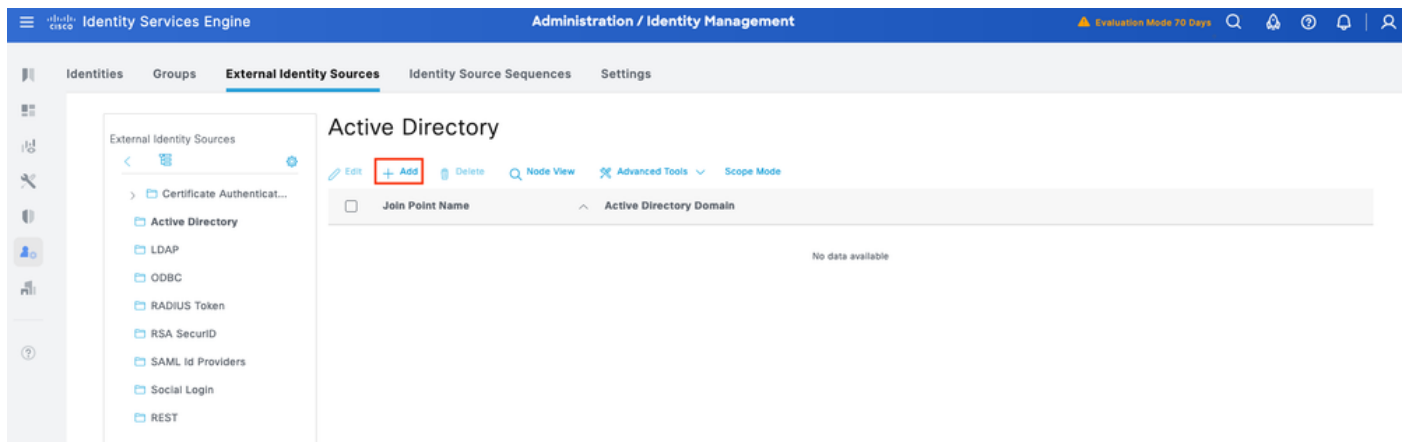


Tip: It is recommended to Enable Single Connect Mode to avoid restarting the TCP session each time a command is sent to the device.

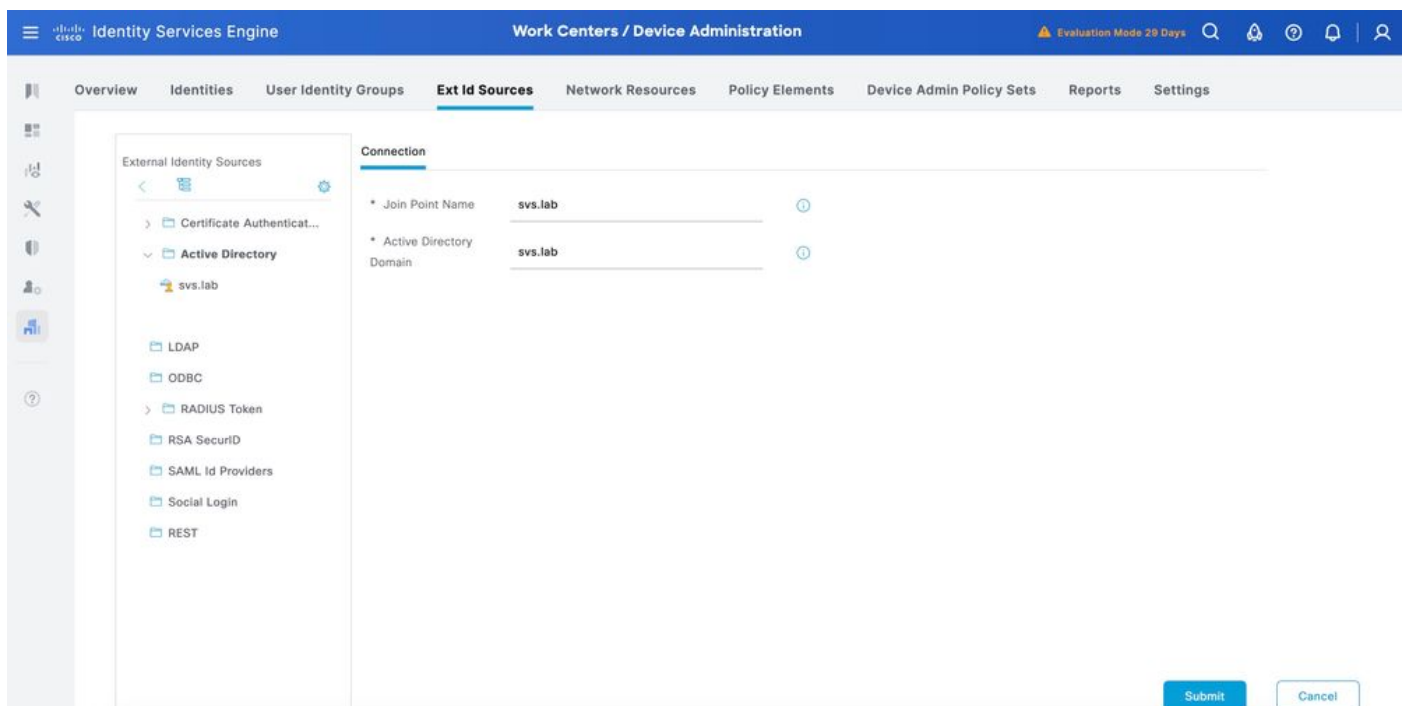
Configure Identity Stores

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.

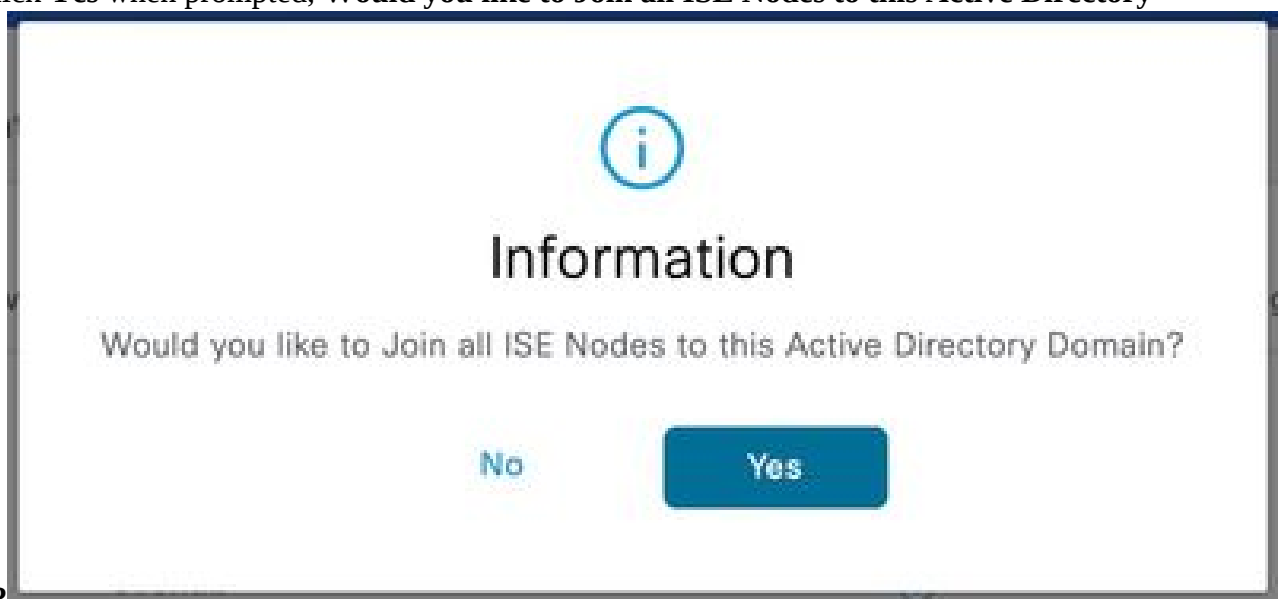
Step 1. Navigate to **Administration > Identity Management > External Identity Stores > Active Directory**. Click **Add** to define a new AD Joint Point.



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

×

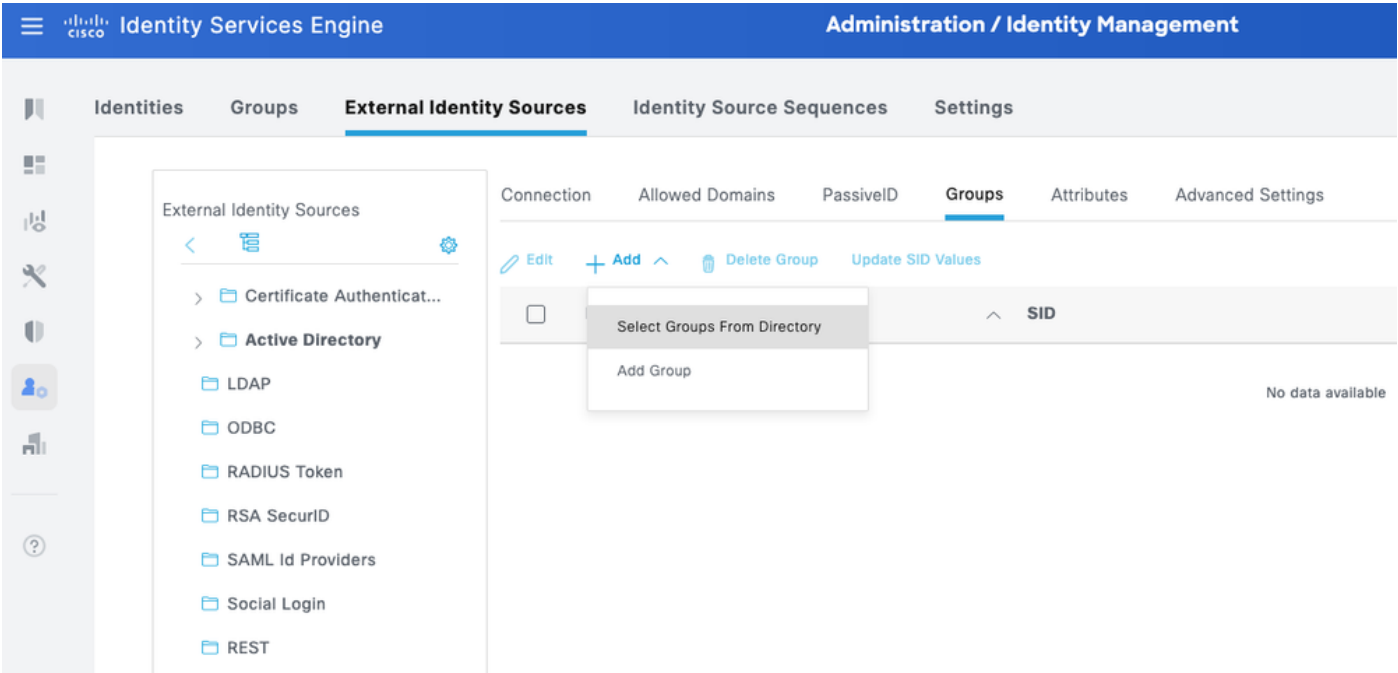
Join Operation Status

Status Summary: Successful.

ISE Node	Node Status
ISE1.lab	✔ Completed.

Close

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.



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

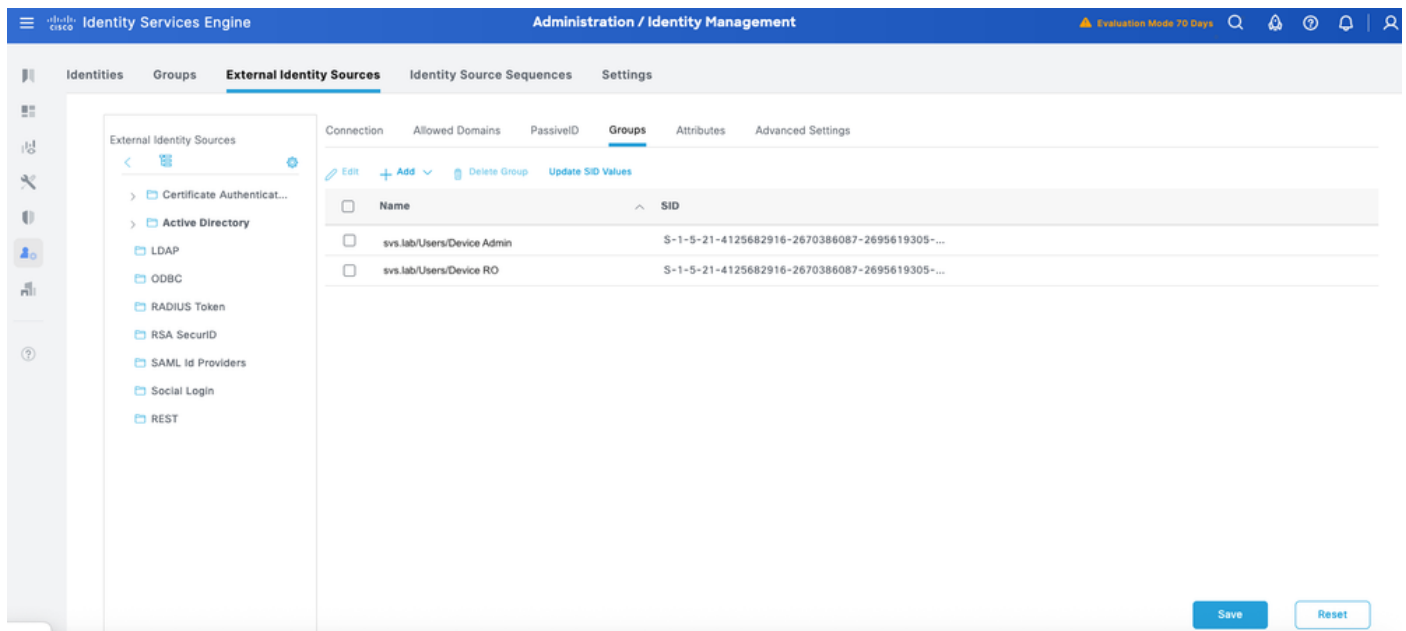
Name SID

Filter Filter

Type

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



Configure TACACS+ Profiles

Map the TACACS+ Profiles to user roles on the Cisco IOS XR devices. In this example these are defined:

- 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.

Define two TACACS+ Profiles: IOSXR_RW and IOSXR_RO.

IOS XR_RW - Administrator Profile

Step 1. Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**. Add a new TACACS Profile and name it **IOSXR_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 Evaluation Mode 63 Days

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

Conditions > Network Conditions > Results > Allowed Protocols > TACACS Command Sets > **TACACS Profiles**

TACACS Profiles > IOSXR_RW
TACACS Profile

Name: IOSXR_RW

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☒ Default Privilege: 15 (Select 0 to 15)

☒ Maximum Privilege: 15 (Select 0 to 15)

☐ Access Control List:

☐ Auto Command:

☐ No Escape: (Select true or false)

IOS XR_RO - Operator Profile

Step 1. Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**. Add a new **TACACS Profile** and name it **IOSXR_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 Evaluation Mode 62 Days

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

Conditions > Network Conditions > Results > Allowed Protocols > TACACS Command Sets > **TACACS Profiles**

TACACS Profiles > New
TACACS Profile

Name: IOSXR_RO

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☒ Default Privilege: 1 (Select 0 to 15)

☒ Maximum Privilege: 1 (Select 0 to 15)

☐ Access Control List:

☐ Auto Command:

☐ No Escape: (Select true or false)

Configure TACACS+ Command Sets

Define the TACACS+ Commands Sets: In this example, these are defined CISCO_IOSXR_RW and CISCO_IOSXR_RO.

CISCO IOS XR 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_IOSXR_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'. A right-hand navigation bar shows 'Evaluation Mode 63 Days' and various icons. The main navigation menu on the left includes 'Overview', 'Identities', 'User Identity Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements' (selected), 'Device Admin Policy Sets', 'Reports', and 'Settings'. The 'Policy Elements' section is expanded, showing 'Conditions', 'Network Conditions', 'Results' (expanded), 'Allowed Protocols', 'TACACS Command Sets' (selected), and 'TACACS Profiles'. The 'TACACS Command Sets' page shows a breadcrumb 'TACACS Command Sets > CISCO_IOSXR_RW' and a 'Command Set' section. The 'Name' field is 'CISCO_IOSXR_RW'. The 'Description' field is empty. The 'Commands' section has a checkbox 'Permit any command that is not listed below' which is checked. Below this are buttons: 'Add', 'Trash' (with a dropdown arrow), 'Edit', 'Move Up', and 'Move Down'. A table with columns 'Grant', 'Command', and 'Arguments' is shown, but it is empty with the message 'No data found.' at the bottom. At the bottom right are 'Cancel' and 'Save' buttons.

CISCO IOS XR 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_IOSXR_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**.

The screenshot shows the 'Policy Elements' configuration page in the Cisco ISE interface. The breadcrumb trail is 'TACACS Command Sets > CISCO_IOSXR_RO'. The page is divided into a left sidebar with navigation options (Conditions, Network Conditions, Results, Allowed Protocols, TACACS Command Sets, TACACS Profiles) and a main content area. In the main area, the 'Name' is 'CISCO_IOSXR_RO'. There is a 'Description' text area. Under the 'Commands' section, there is a checkbox for 'Permit any command that is not listed below'. Below this is a table with columns 'Grant', 'Command', and 'Arguments'. The table contains one entry: 'PERMIT' for the command 'show'. At the bottom right, there are 'Cancel' and 'Save' buttons.

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.

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

The screenshot shows the 'Device Admin Policy Sets' configuration page in the Cisco ISE interface. The breadcrumb trail is 'Work Centers / Device Administration > Device Admin Policy Sets'. The page has a top bar with 'Reset', 'Reset Policy Set Hit Counts', and 'Save' buttons. Below this is a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The table contains one entry: 'IOS-XR devices' with a status of 'On'. The 'Conditions' column shows 'DEVICE-Device Type EQUALS All Device Types#IOS-XR'. The 'Allowed Protocols / Server Sequence' column shows 'Default Device Admin'. The 'Hits' column shows '73'. At the bottom right, there is a right arrow button.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	IOS-XR devices		DEVICE-Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	73		

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**.

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 62 Days

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Policy Sets→ IOS-XR devices

Reset

Reset Policy Set Hit Counts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search	✓ IOS-XR devices		DEVICE-Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	77

> Authentication Policy(1)

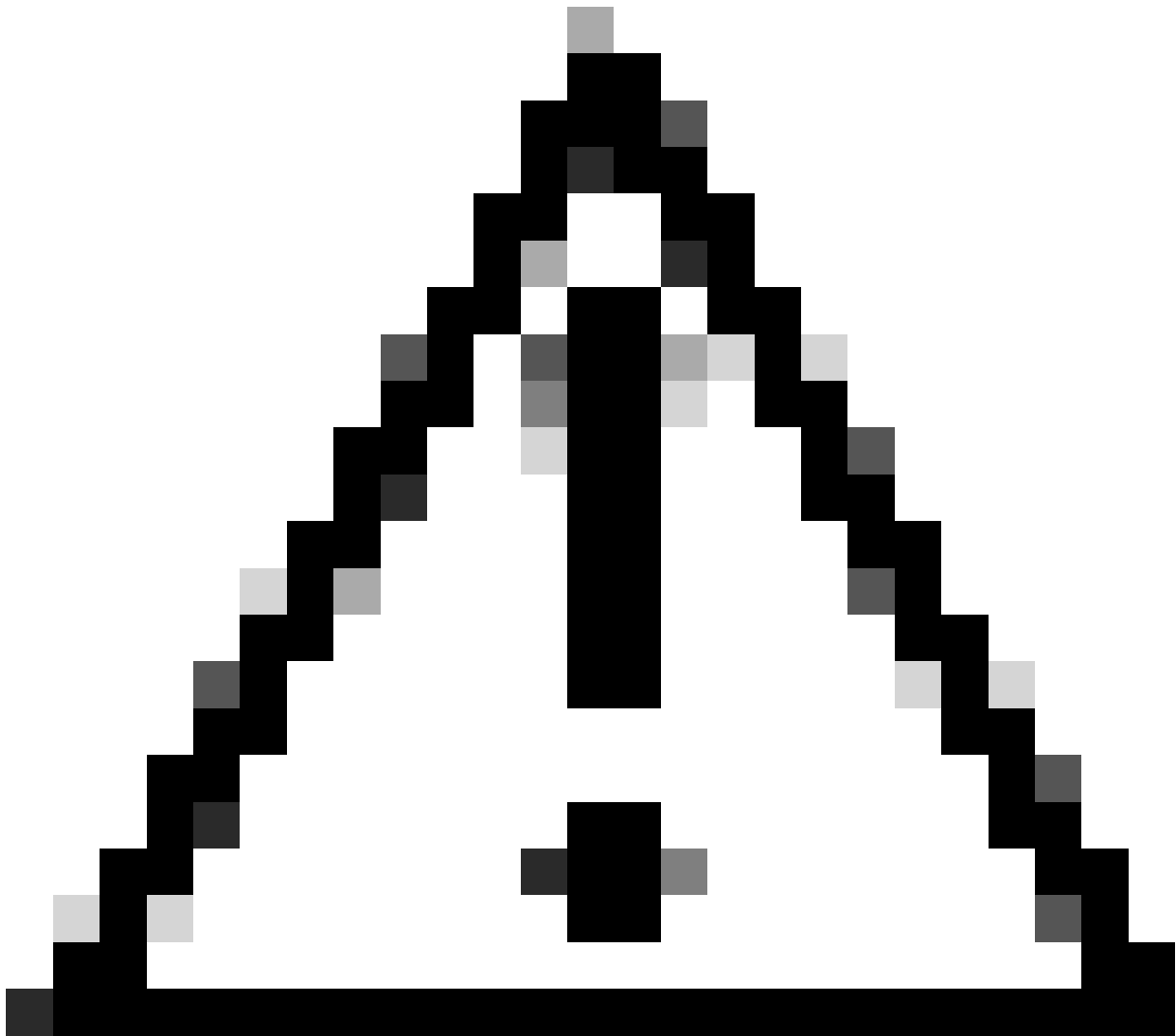
> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

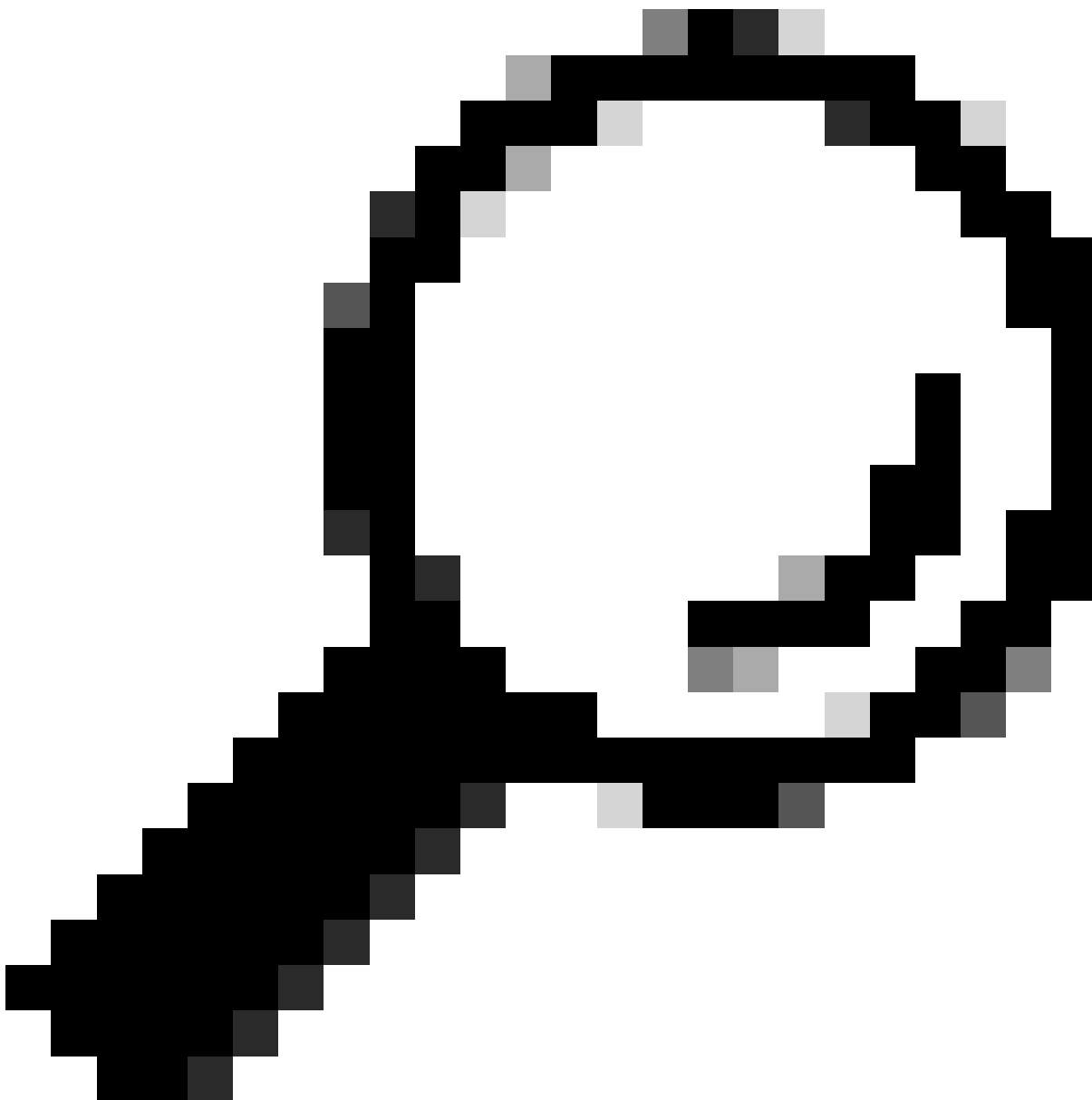
> Authorization Policy(3)

	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
Search	✓ Authorization Rule RO		svs.lab-ExternalGroups EQUALS svs.lab /Users/Device RO	CISCO_IOSXR_RO	IOSXR_RO	0	
✓ Authorization Rule RW		svs.lab-ExternalGroups EQUALS svs.lab /Users/Device Admin	CISCO_IOSXR_RW	IOSXR_RW	77		
✓ Default			DenyAllCommands	Deny All Shell Profile	0		

Part 2 - Configure Cisco IOS XR 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.

Initial Configurations

Step 1. Ensure name-server (DNS) is configured and the router is successfully able to resolve Frequently Qualified Domain Names (FQDNs), especially the ISE server FQDN.

```
domain vrf mgmt name svcs.lab
domain vrf mgmt name-server 10.225.253.247
no domain vrf mgmt lookup disable
```

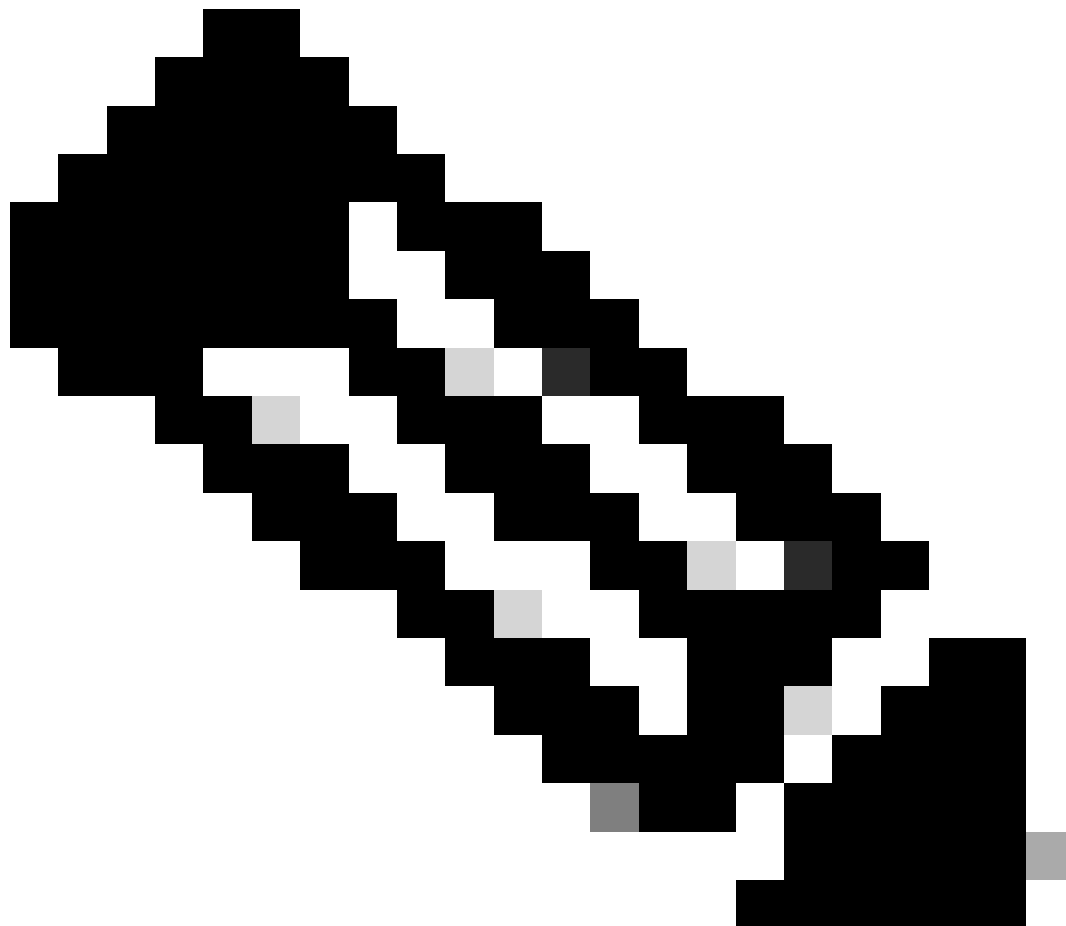
```
RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
Type escape sequence to abort.
```

Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Step 2. Clear any old/unused trustpoints and certificates. Ensure that there are no old trustpoints and certificates present. If you see any old entries, remove/clear them.

```
show crypto ca trustpoint
show crypto ca certificates
```

```
(config)# no crypto ca trustpoint <tp-name>
# clear crypto ca certificates <tp-name>
```



Note: You can manually create a new RSA keypair and attach it under trustpoint. If you do not create one, the default keypair is used. Defining ECC keypair under trustpoint is not currently supported.

Configure Trustpoint

Step 1. Keypair configuration (optional).

```
<#root>
```

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto key generate rsa <key-label> 4096
```

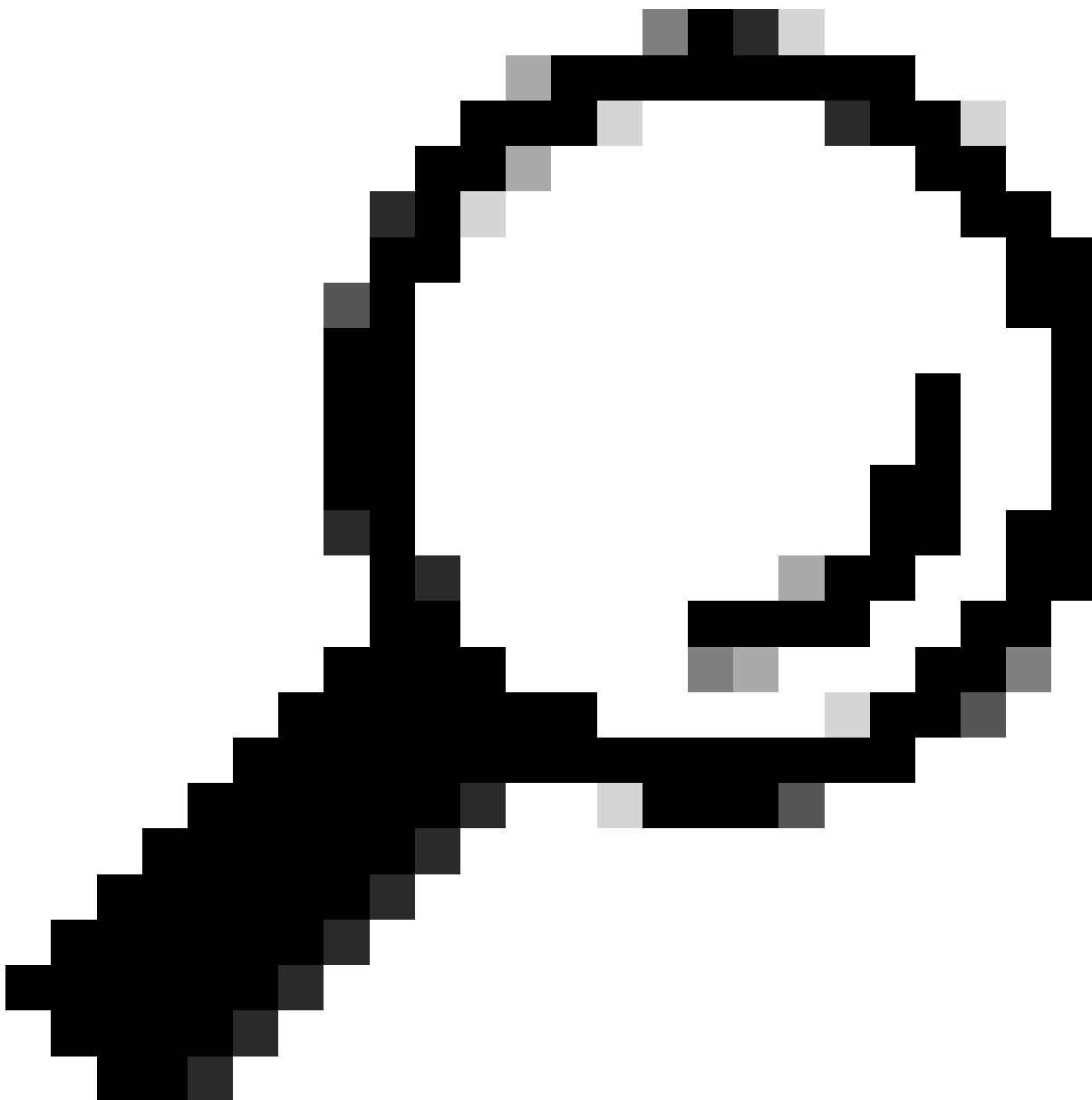
```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto ca trustpoint <tp-name>
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
rsakeypair <key-label>
```

Step 2. Create **trustpoint**.



Tip: DNS configuration for subject-alternative name is optional (if being enabled on ISE), but recommended.

```
<#root>
```

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto ca trustpoint sv
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
vrf mgmt
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
crl optional
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

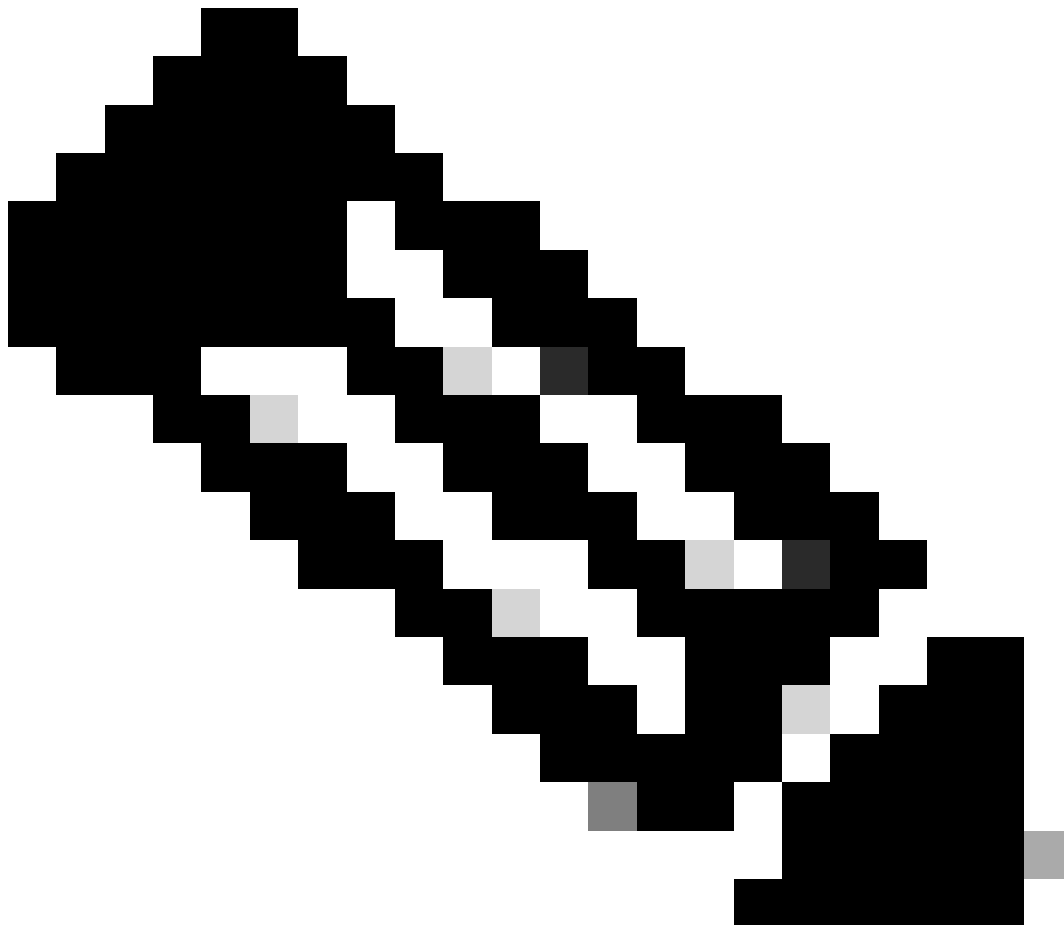
```
enrollment url terminal
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
rsakeypair svs-4096
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
commit
```



Note: If you need to use comma in O or OU, you can use a backslash (\) before the comma. For example: O=Cisco Systems\, Inc.

Step 3. Authenticate Trustpoint by installing **CA certificate**.

```
<#root>
```

```
RP/0/RP0/CPU0:BRC-8201-1#
```

```
crypto ca authenticate svcs
```

Enter the base64/PEM encoded certificate/certificates.

Please note: for multiple certificates use only PEM.

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

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

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwaajELMAkGA1UE
BhMCVVMxZmFzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUUA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLZWNTV1MxEjAQBgNVBAMTCVNWUyBYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBBjHfM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatKXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVPL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuaOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH1OrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQGMFgpTV1MgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXR67X+v
0+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCkoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfPiyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgrU8
8ggz1POdsS/i6Lo7ypYX0eB9HgVDckzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOX/AJHQQ7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGua==
```

```
-----END CERTIFICATE-----
```

```
quit
```

```
Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5
```

```
Subject:
```

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

```
Issued By :
```

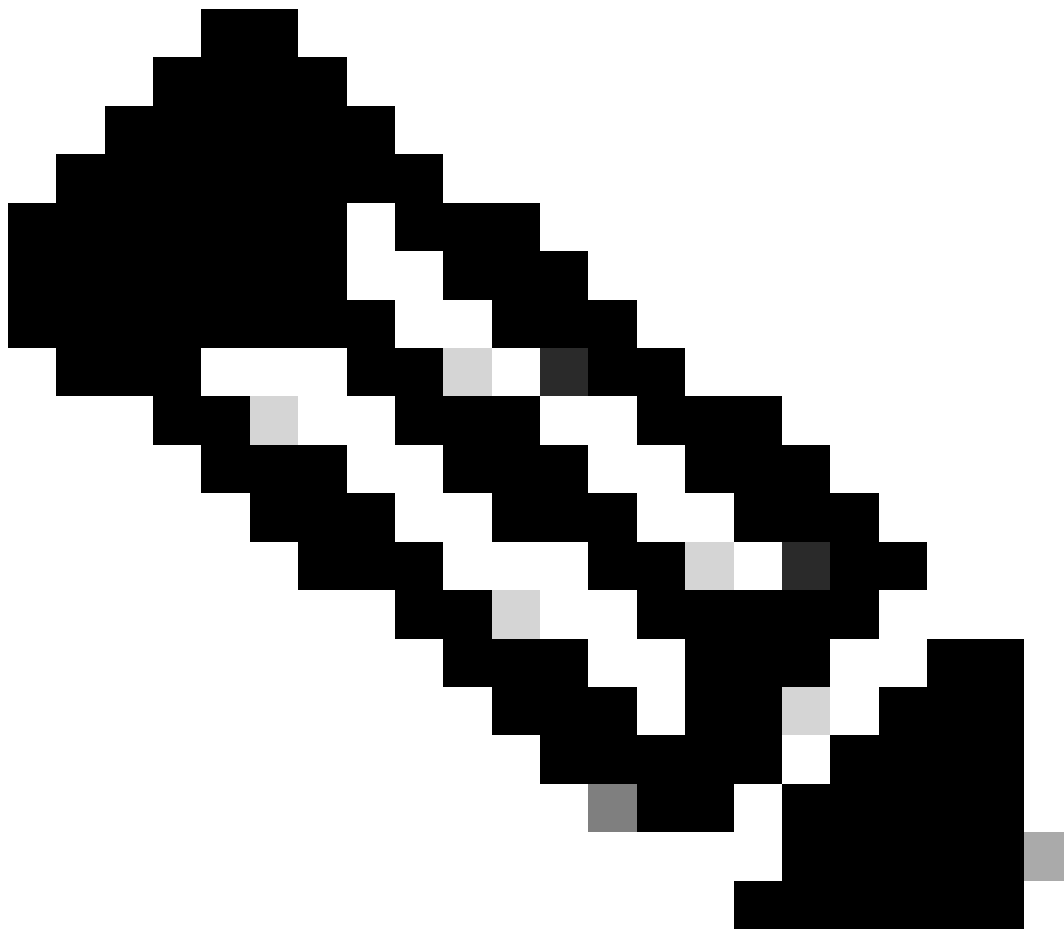
```
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
Validity Start : 17:05:00 UTC Mon Apr 28 2025
```

Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
SHA1 Fingerprint:
0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:

yes

RP/0/RP0/CPU0:May 9 14:52:23.437 UTC: cepki[153]: %SECURITY-CEPKI-6-INFO : certificate database updated



Note: If you have a Subordinate CA system, you need to import both Root CA and Sub CA certificates. Use the same command with Sub CA on top and Root CA at the bottom.

Step 4. Generate **Certificate Signing Request (CSR)**.

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

crypto ca enroll svcs

```
Fri May 9 14:52:44.030 UTC
% Start certificate enrollment ...
% 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:

Re-enter Password:

```
% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167
% The subject name in the certificate will include: BRC-8201-1.svs.lab
% Include the router serial number in the subject name? [yes/no]:
```

yes

```
% The serial number in the certificate will be: 4090843b
% Include an IP address in the subject name? [yes/no]:
```

yes

Enter IP Address[]

10.225.253.167

```
Fingerprint: 36354532 38324335 43434136 42333545
Display Certificate Request to terminal? [yes/no]:
```

yes

Certificate Request follows:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAK5DMQwwCgYDVQQH
DANSVFAXDjAMBGNVBAoMBUNpc2NmQwwCgYDVQQLDANTVlMxZzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTYzMRERDwYDVQQFEWg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtrloDH9iOZxPvEDARwN0t4WrPEjaQc1ZUA
6ax6Cqx/0JlQiUf2+eQv+4rKZqAZ1xDhiaIMGqETn00LKpwmTx10IqXL7UYMHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/41RwMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkKwIOcb1X2HgtbVQdCXTAwJDMr2O9
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAACBiTAYBgqhkiG
9w0BCQcxCMJQzFzY28uMTIzMG0GCSqGSIb3DQEJDDjFgMF4wDgYDVR0PAQH/BAQD
AgWgMCAgA1UdJQEB/wQwMBQGCSsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBbX0eWF5ZUz701GFjuQHBBdgYb+3lhFOxbYm9psIWfv1uwjKkoL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswjlyp0+IxxUM971Ejwg2rj+jABDR7I8SU
06Y06mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTIljdgVxB+Xyz0FJMckI05US3j
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f90A+fdg2zYtOME
Z6VAw64cY+YF6iLbYv7c4liz05Zj2NJBuKpeqijkFAkY/1rIxTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZN00
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
```

Redisplay enrollment request? [yes/no]:

no

Step 5. Import CA signed certificate.

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

crypto ca import svcs certificate

Fri May 9 15:00:35.426 UTC

Enter the base64/PEM encoded certificate/certificates.

Please note: for multiple certificates use only PEM.

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

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

```
MIIE3zCCAsEgAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA5MTQ1NzAwWWhcNMjUwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkxMxDDAKBgNVBACMA1JUUEDEOMAwGA1UECgwFQ21zY28xDDAK
BgNVBASMA1NWUzEXMBUGA1UEAwwOMTAuMjU1ZjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3Dg0d02uW
gMf2I5nE+8QMBHA3S3has8SNpByVlQDprHoLGr/QmVCJR/b55C/7i spmoBnXEOGJ
qIwaoROc7QsqnCa3HXQipcvrtGwcfAX29EgjnboiaRYDxrrdbHrpSQTfpeh5dp/k
eQuio07rxfdzTss+8x7WwzC+artGbLYMC7fQCH819iVAIeZNUXPcz18G3zrHHi3W
fFMVT/iVFYwLvdR0v1h0okuMykFPA00TemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTajRxxvfyE1tVB0JdMDAK0avY73N3Zkjr16dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0
ZTA0BgNVHQ8BAf8EBAMCBaAwIAyDVR01AQH/BBYwFAYIKwYBBQUHAWEGCCsGAQUF
BwMCMakGA1UdEwQCAAwHwYDVR0RBBgwFoIOMTAuMjU1ZjI1My4xNjcxETAPBgNV
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+oj012106WxedDQ8Vdu0bBtrnOH+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTZrQ93tb9mMTZg7exqN89ZU
VlXoB2UOTri5Kl0/+izEGgyNq42/ytAP8Y007HR/2jf7gfhoRvwcR5QNOEHv4o6l
Zma5Xio1sBbkA7JB2mpzzG4ZjsyV81RGXxxgyt1mwNmb7EiAc8lodRcgyp7FNh3
F/k9cMMMr51M4Ysvo1tx1k9AeLjzb2syv5/fG6Qu0ZdWwTaaQh0Y2h/cVDiV97wg
OD1mEfdsV6QrxQSujZr22RzVykKH1tuiV2B74pthUuGRBtfHS5XFy7uTTbfGX8M6
ZJw8rX1SADR8tDp1rf1ZIrPmv3ZPP7woTB22yWzyd0use+5Ia1b0w70twN4t/IIw
8CJu6HfndXLDLPZ0jsC8steffrSlopwGccp3j6aZKPFz+I/Purb44a9WxEwa2TA7H
+r1oynBcGmetOHxVLnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF5370w+uNHok8Bdt8mqadUT40oUSqY8ArV0Bom05tzbemreVPmQAZ/IahZ7TqKo
3dGNontAFTTESM1iujQ81iRKsikdHySnwcCM2ni1CKZrhVq5IB8NK6jKRJZ0eQAX
vMt1
```

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

quit

Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5

Subject:

serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US

Issued By :

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

Validity Start : 14:57:00 UTC Fri May 09 2025

Validity End : 14:57:00 UTC Sat May 09 2026

SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792

Verify the router identity certificate is enrolled.

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

show crypto ca trustpoint svcs detail

```
Trustpoint          :svcs-new
=====
KeyPair Label: the_default
CRL:optional
enrollment: terminal
subject name: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab
```

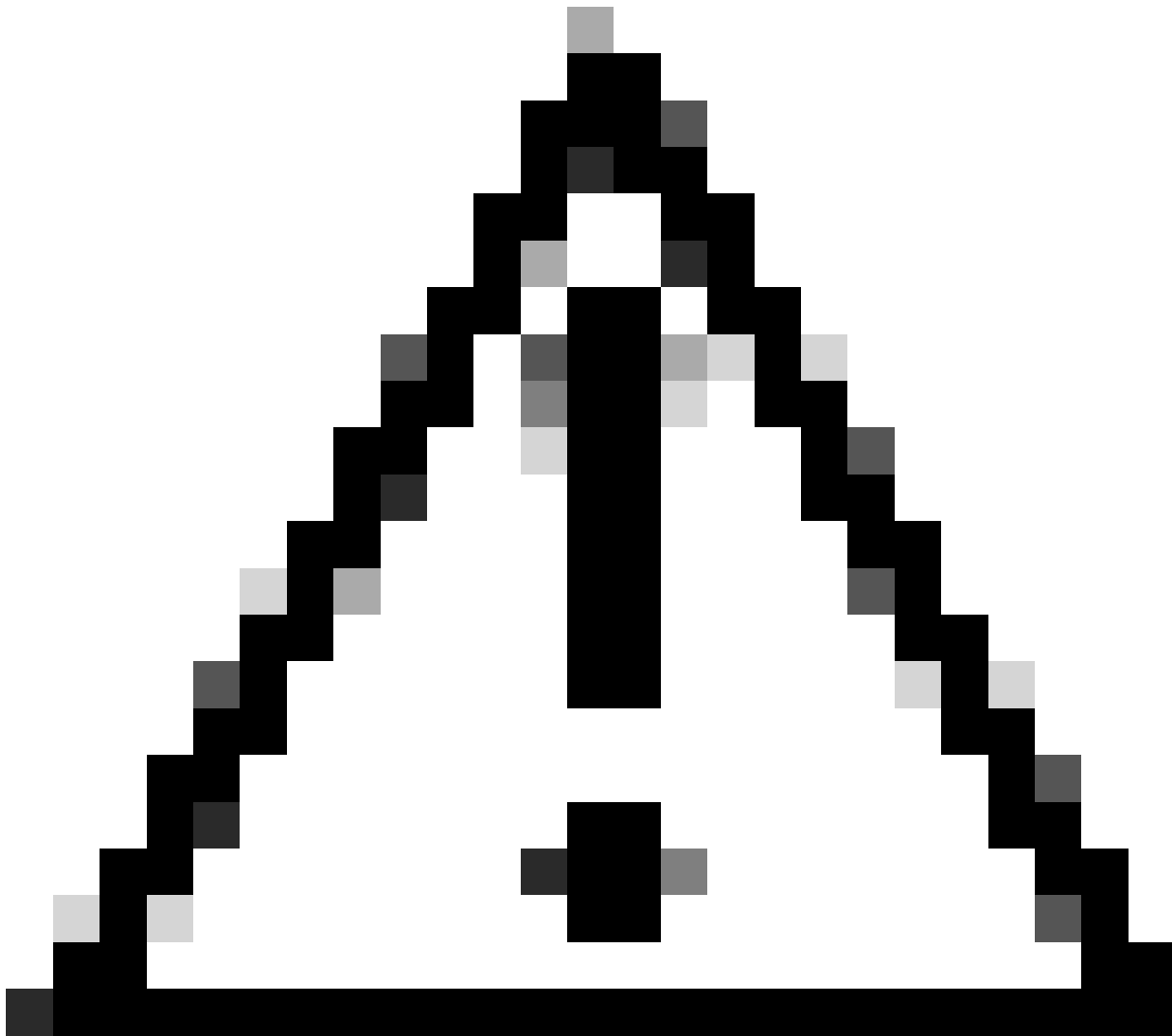
RP/0/RP0/CPU0:BRC-8201-1#

show crypto ca certificates svcs

Wed May 14 14:55:58.173 UTC

```
Trustpoint          : svcs-new
=====
CA certificate
  Serial Number   : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
  Subject:
    CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Issued By      :
    CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 17:05:00 UTC Mon Apr 28 2025
  Validity End   : 17:05:00 UTC Sat Apr 28 2035
  SHA1 Fingerprint:
    0EB181E95A3ED7803BC5A8059A854A95C83AC737
Router certificate
  Key usage       : General Purpose
  Status          : Available
  Serial Number   : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
  Subject:
    serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By      :
    CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 19:59:00 UTC Fri May 09 2025
  Validity End   : 19:59:00 UTC Sat May 09 2026
  SHA1 Fingerprint:
    AC17E4772D909470F753BDBFA463F2DF522CC2A6
Associated Trustpoint: svcs
```

Configure TACACS & AAA with TLS



Caution: Perform the configuration changes through console with local credentials.

Step 1. Configure **TACACS+ server**.

```
tacacs source-interface MgmtEth0/RP0/CPU0/0 vrf mgmt
tacacs-server host 10.225.253.209 port 49
  key 7 072C705F4D0648574453
```

```
aaa group server tacacs+ tacacs2
  server 10.225.253.209
  vrf mgmt
```

Step 2. Configure **AAA group**.

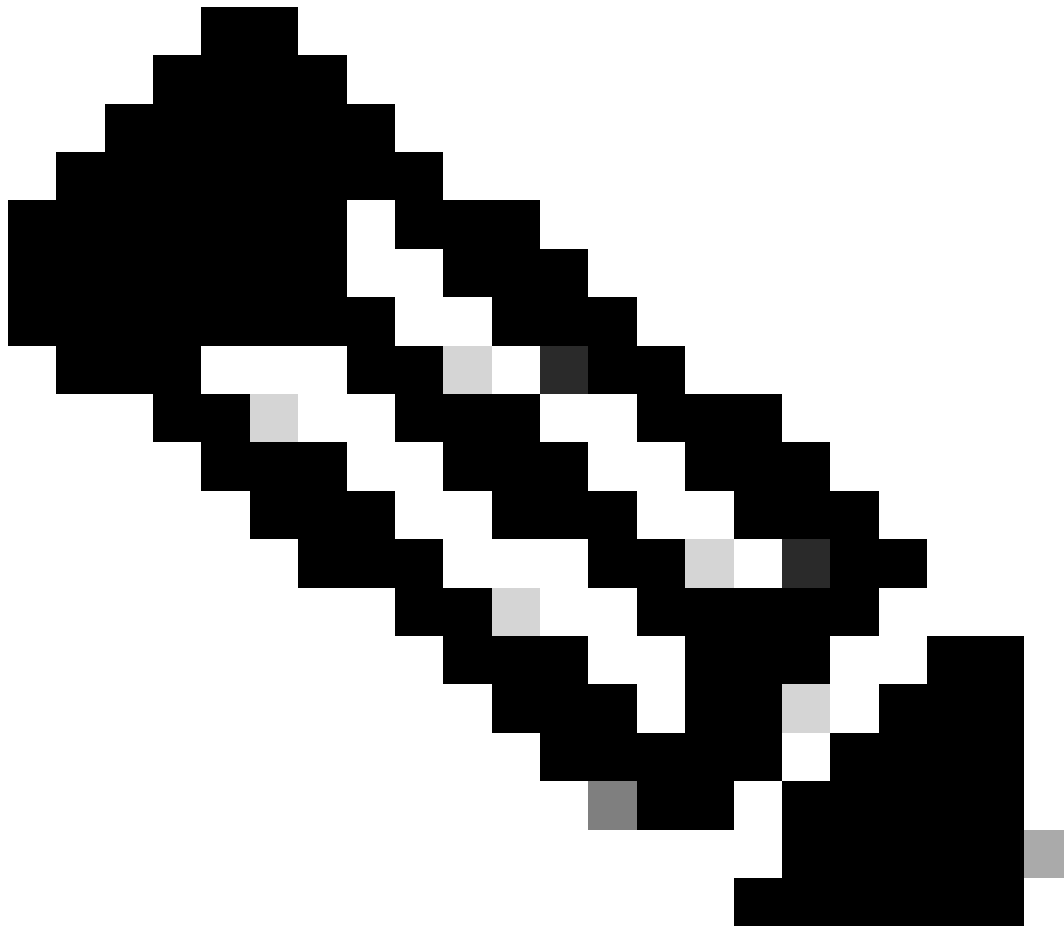
```
aaa group server tacacs+ tac_tls_sc
  vrf mgmt
```

```
server-private 10.225.253.209 port 6049
timeout 10
tls
  trustpoint svcs
!
single-connection
```

Step 2. Configure **AAA**.

```
aaa accounting exec default start-stop group tac_tls_sc
aaa accounting system default start-stop group tac_tls_sc
aaa accounting network default start-stop group tac_tls_sc
aaa accounting commands default stop-only group tac_tls_sc
aaa authorization exec default group tac_tls_sc local
aaa authorization commands default group tac_tls_sc none
aaa authentication login default group tac_tls_sc local
```

Certificate Renewal



Note: Trust point does not need to be removed from TACACS+ configuration during renewal.

Step 1. Verify current certificate validity dates.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svcs-new
Thu Aug 14 15:13:37.465 UTC
```

```
Trustpoint : svcs-new
```

```
=====
```

```
CA certificate
```

```
Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
```

```
Subject:
```

```
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
```

```
Issued By :
```

```
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
```

```
Validity Start : 22:13:17 UTC Thu Jun 26 2025
```

```
Validity End : 22:13:16 UTC Tue Jun 25 2030
```

```
CRL Distribution Point
```

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uB1QsZDYy6wxomiFWB5Gv0AZM

SHA1 Fingerprint:

EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2

Trusted Certificate Chain

Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96

Subject:

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Issued By :

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 22:13:17 UTC Thu Jun 26 2025

Validity End : 22:13:16 UTC Sun Jun 24 2035

SHA1 Fingerprint:

E225647FF9BDA176D2998D5A3A9770270F37D2A7

Router certificate

Key usage : General Purpose

Status : Available

Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E

Subject:

CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US

Issued By :

CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 16:38:36 UTC Wed Jul 30 2025

Validity End : 16:38:35 UTC Thu Jul 30 2026

CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4Qg1Qa8g1xoH8GY

SHA1 Fingerprint:

B562F3CF507CE7F97893F28BC896794CFF6995C1

Associated Trustpoint: svb-new

Step 2. Delete existing trustpoint certificate.

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
```

```
Thu Aug 14 15:25:26.286 UTC
```

```
certificates cleared for trustpoint KF_TP
```

```
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database updated
```

```
RP/0/RP0/CPU0:BRC-8201-1#
```

```
RP/0/RP0/CPU0:BRC-8201-1#
```

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
```

```
Thu Aug 14 15:25:37.270 UTC
```

```
RP/0/RP0/CPU0:BRC-8201-1#
```

Step 3. Re-authenticate and enroll trust point as described in the steps under **Trustpoint Configuration**.

Step 4. Verify certificate validity dates are updated.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
```

```
Thu Aug 14 15:31:28.309 UTC
```

```
Trustpoint : KF_TP
```

```
=====
```

```
CA certificate
```

```
Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
```

Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Tue Jun 25 2030

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uB1QsZDYy6wxomiFWB5Gv0AZM>
SHA1 Fingerprint:
EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
Subject:
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Sun Jun 24 2035
SHA1 Fingerprint:
E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
Key usage : General Purpose
Status : Available
Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
Subject:
CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 15:17:29 UTC Thu Aug 14 2025
Validity End : 15:17:28 UTC Fri Aug 14 2026

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4Qg1Qa8g1xoH8GY>
SHA1 Fingerprint:
D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE
Associated Trustpoint: KF_TP

Verification

Verify the configuration.

```
show crypto ca certificates [detail]  
show crypto ca trustpoint detail  
show tacacs details
```

Debug for TACACS+

```
debug tacacs tls
```

Debug TLS

```
debug ssl error  
debug ssl events
```

Test the remote user before configuring AAA authentication.

```
<#root>
```

```
test aaa group tacacs2 <username> <password>
```

```
user has been authenticated
```

Troubleshooting

Clearing the certificates (this deletes all certificates associated with a trust point).

```
clear crypto ca certificate <trustpoint name>
```

TACACS process restart (if necessary)

```
process restart tacacsd
```