

在带有ISE的IOS XR设备上通过TLS 1.3配置TACACS+

目录

[简介](#)

[概述](#)

[使用本指南](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[许可](#)

[第1部分 — 设备管理的ISE配置](#)

[为TACACS+服务器身份验证生成证书签名请求](#)

[上传用于TACACS+服务器身份验证的根CA证书](#)

[将签名证书签名请求\(CSR\)绑定到ISE](#)

[启用TLS 1.3](#)

[在ISE上启用设备管理](#)

[启用TLS上的TACACS](#)

[创建网络设备和网络设备组](#)

[配置身份库](#)

[配置TACACS+配置文件](#)

[IOS XR RW — 管理员配置文件](#)

[IOS XR RO — 运营商配置文件](#)

[配置TACACS+命令集](#)

[CISCO IOS XR RW — 管理员命令集](#)

[CISCO IOS XR RO — 操作员命令集](#)

[配置设备管理策略集](#)

[第2部分 — 配置Cisco IOS XRfor TACACS+ over TLS 1.3](#)

[初始配置](#)

[配置信任点](#)

[使用TLS配置TACACS和AAA](#)

[证书续订](#)

[确认](#)

[故障排除](#)

简介

本文档介绍使用思科身份服务引擎(ISE)作为服务器，使用思科IOS® XR设备作为客户端的TLS上的TACACS+示例。

概述

增强型终端访问控制器访问控制系统(TACACS+)协议[RFC8907]通过一台或多台TACACS+服务器实现对路由器、网络访问服务器和其他联网设备的集中设备管理。它提供身份验证、授权和记帐(AAA)服务，专为设备管理使用案例量身定制。

基于TLS 1.3的TACACS+ [RFC8446]通过引入安全传输层来增强协议，从而保护高度敏感的数据。此集成可确保TACACS+客户端与服务器之间的连接和网络流量的机密性、完整性和身份验证。

使用本指南

本指南将活动分为两部分，使ISE能够管理基于Cisco IOS XR的网络设备的管理访问。

- 第1部分 — 为设备管理员配置ISE
- 第2部分 — 配置Cisco IOS XR for TACACS+ over TLS

先决条件

要求

通过TLS配置TACACS+的要求：

- 证书颁发机构(CA)，用于签署TLS上TACACS+用于签署ISE和网络设备证书的证书。
- 来自证书颁发机构(CA)的根证书。
- 网络设备和ISE具有DNS可达性并可解析主机名。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ISE VMware虚拟设备，版本3.4补丁2
- Cisco 8201路由器，版本25.3.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

许可

设备管理许可证允许您在策略服务节点上使用TACACS+服务。在高可用性(HA)独立部署中，设备管理许可证允许您在HA对中的单个策略服务节点上使用TACACS+服务。

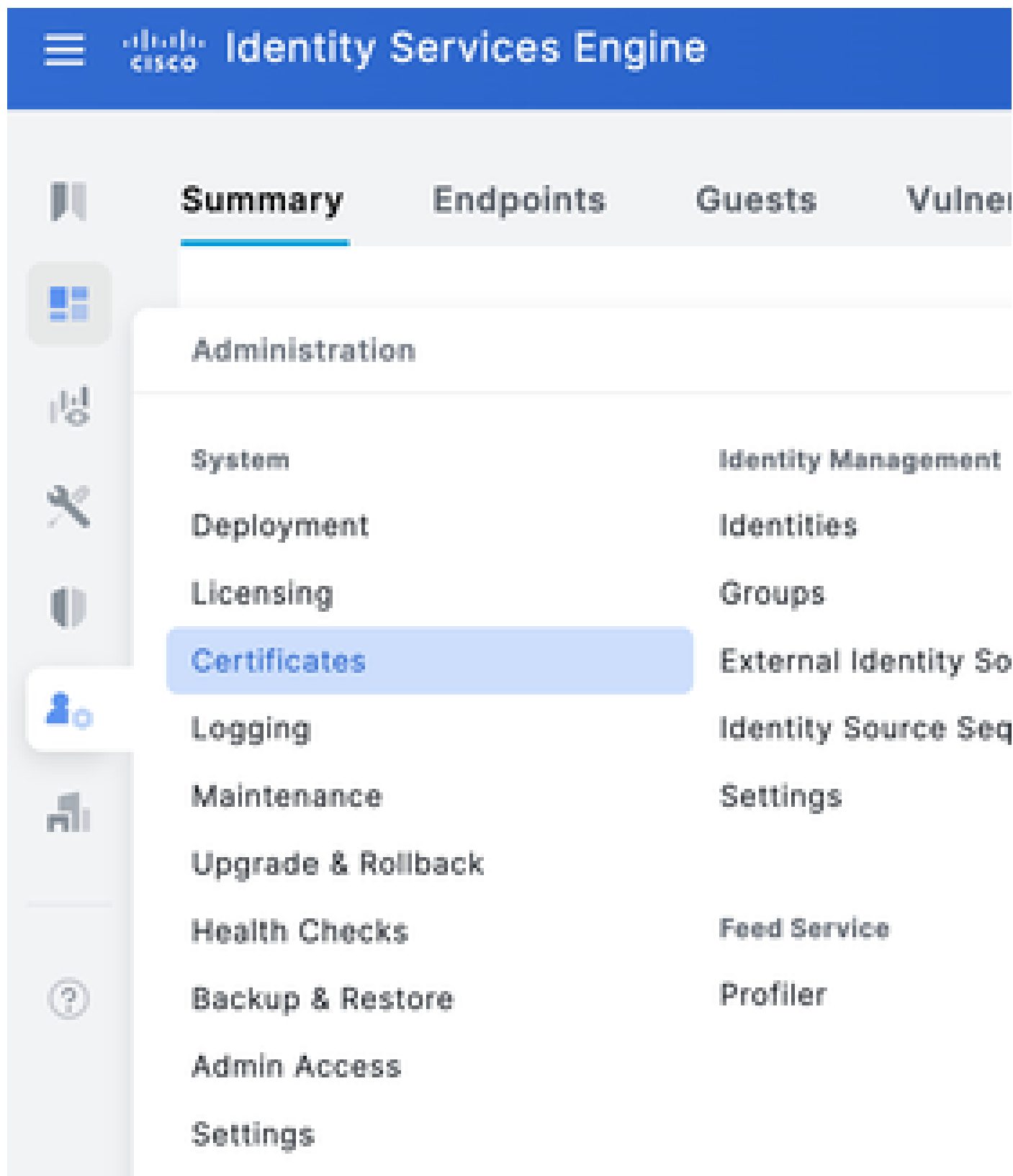
第1部分 — 设备管理的ISE配置

为TACACS+服务器身份验证生成证书签名请求

第1步：使用受支持的浏览器之一登录ISE管理员Web门户。

默认情况下，ISE对所有服务使用自签名证书。第一步是生成证书签名请求(CSR)，以便由我们的证书颁发机构(CA)签名。

第2步：导航到管理>系统>证书。



第 3 步：在Certificate Signing Requests下，单击Generate Certificate Signing Request。



步骤4.选择TACACS inUsage。

Usage

Certificate(s) will be used forTACACS

Allow Wildcard Certificates☐ ⓘ

步骤5.选择已启用TACACS+的PSN。

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ ISE1	ISE1#TACACS

步骤6.使用适当的信息填充Subject字段。

Subject

Common Name (CN)
\$FQDN\$



Organizational Unit (OU)
CX



Organization (O)
Cisco



City (L)
Raleigh

State (ST)
North Carolina

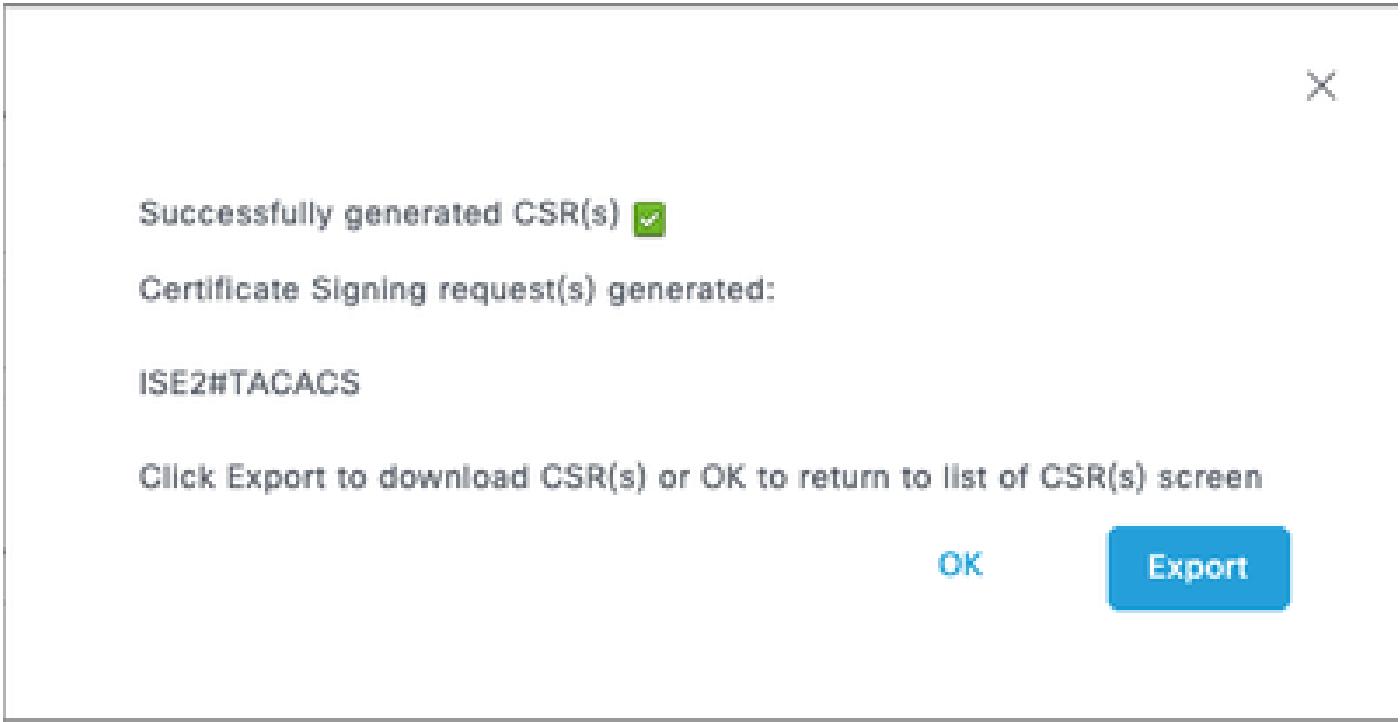
Country (C)
US

步骤7.在Subject Alternative Name(SAN)下添加DNS Name和IP Address。

Subject Alternative Name (SAN)

⋮	DNS Name	✓	ISE1.lab	—	+	
⋮	IP Address	✓	10.225.253.209	—	+	①

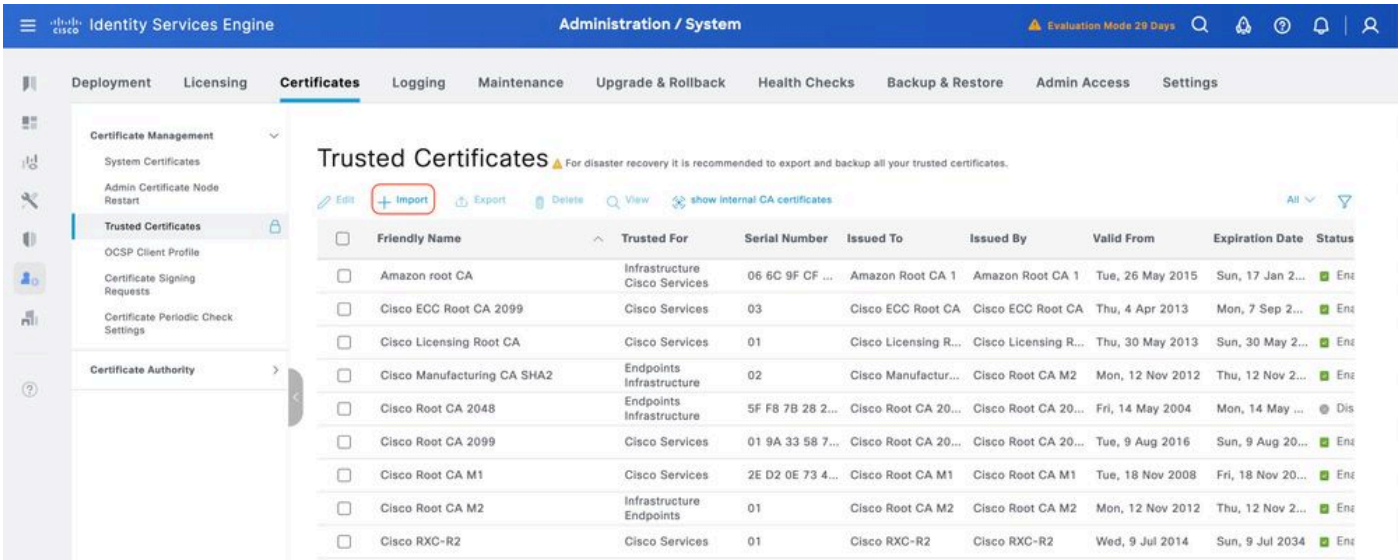
步骤8.单击Generate，然后单击Export。



现在，您可以让证书颁发机构(CA)签署证书(CRT)。

上传用于TACACS+服务器身份验证的根CA证书

第1步：导航到管理>系统>证书。在Trusted Certificates下，单击Import。



步骤2.选择由签署TACACS证书签名请求(CSR)的证书颁发机构(CA)颁发的证书。 确保 信任ISE内的身份验证 选项已启用。

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

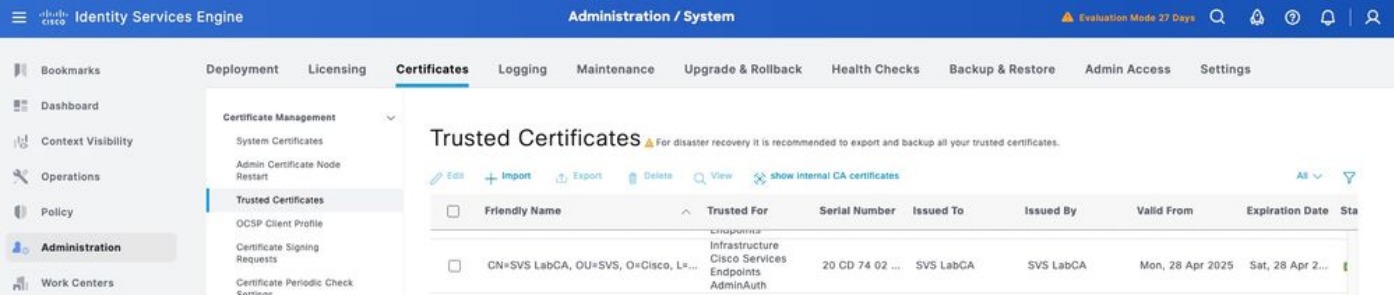
☐ Validate Certificate Extensions

Description

Submit

Cancel

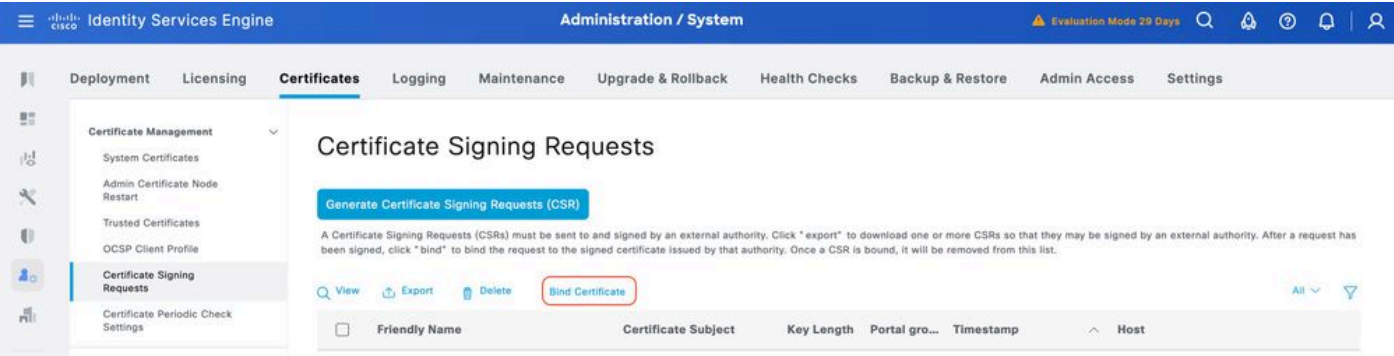
点击Submit。证书现在必须出现在受信任证书下。



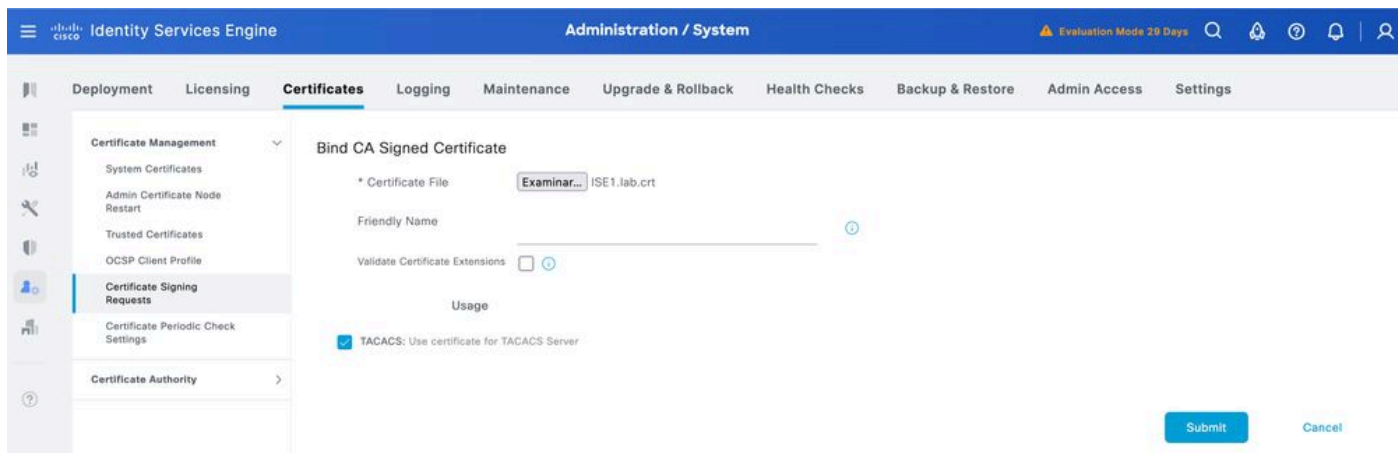
将签名证书签名请求(CSR)绑定到ISE

签名证书签名请求(CSR)后，您可以在ISE上安装已签名的证书。

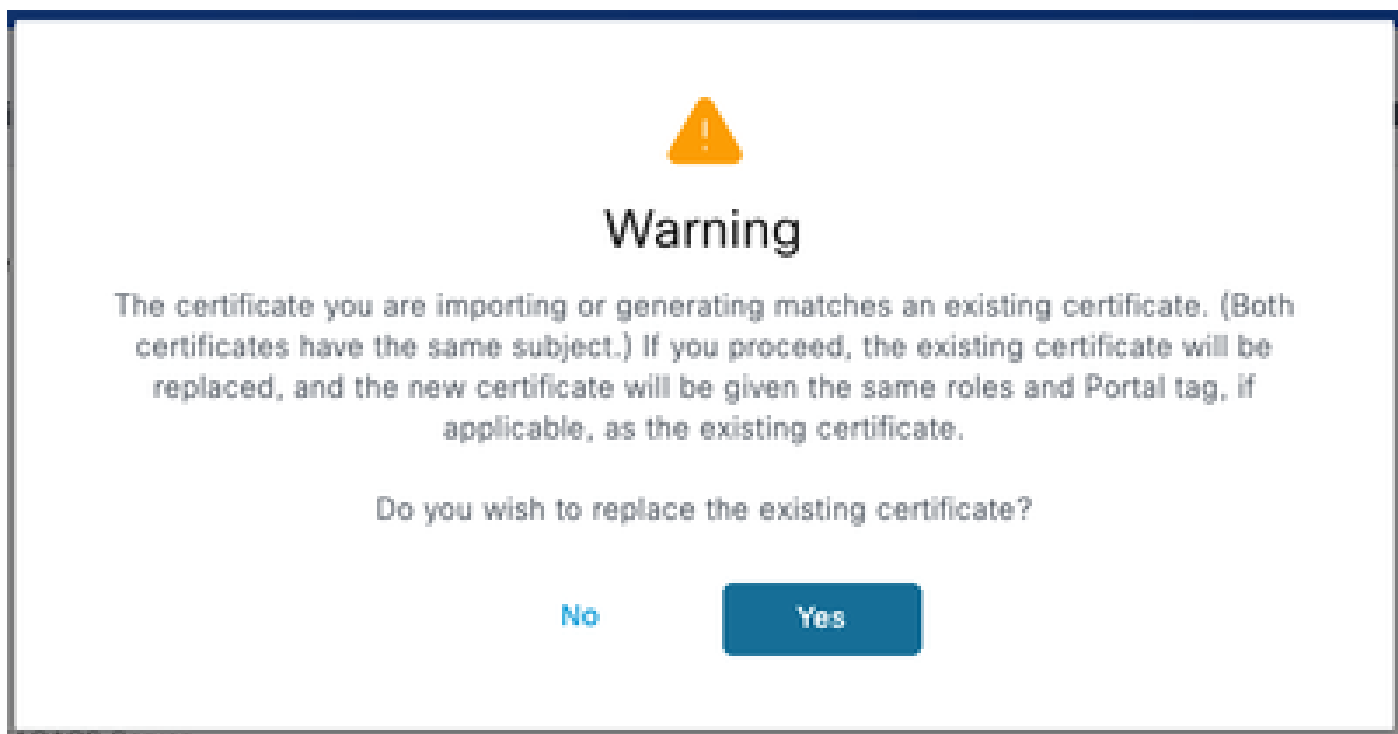
第1步：导航到Administration > System > Certificates。在Certificate Signing Requests下，选择在上一步中生成的TACACS CSR，然后单击Bind Certificate。



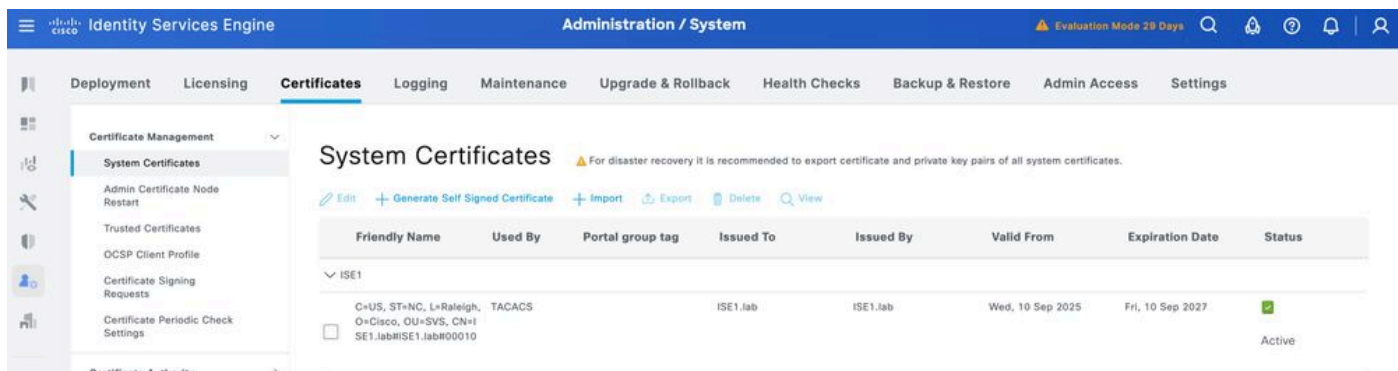
第2步：选择签名证书，并确保使用下的TACACS复选框保持选中。



步骤3.单击Submit。如果收到有关替换现有证书的警告，请单击Yes继续。



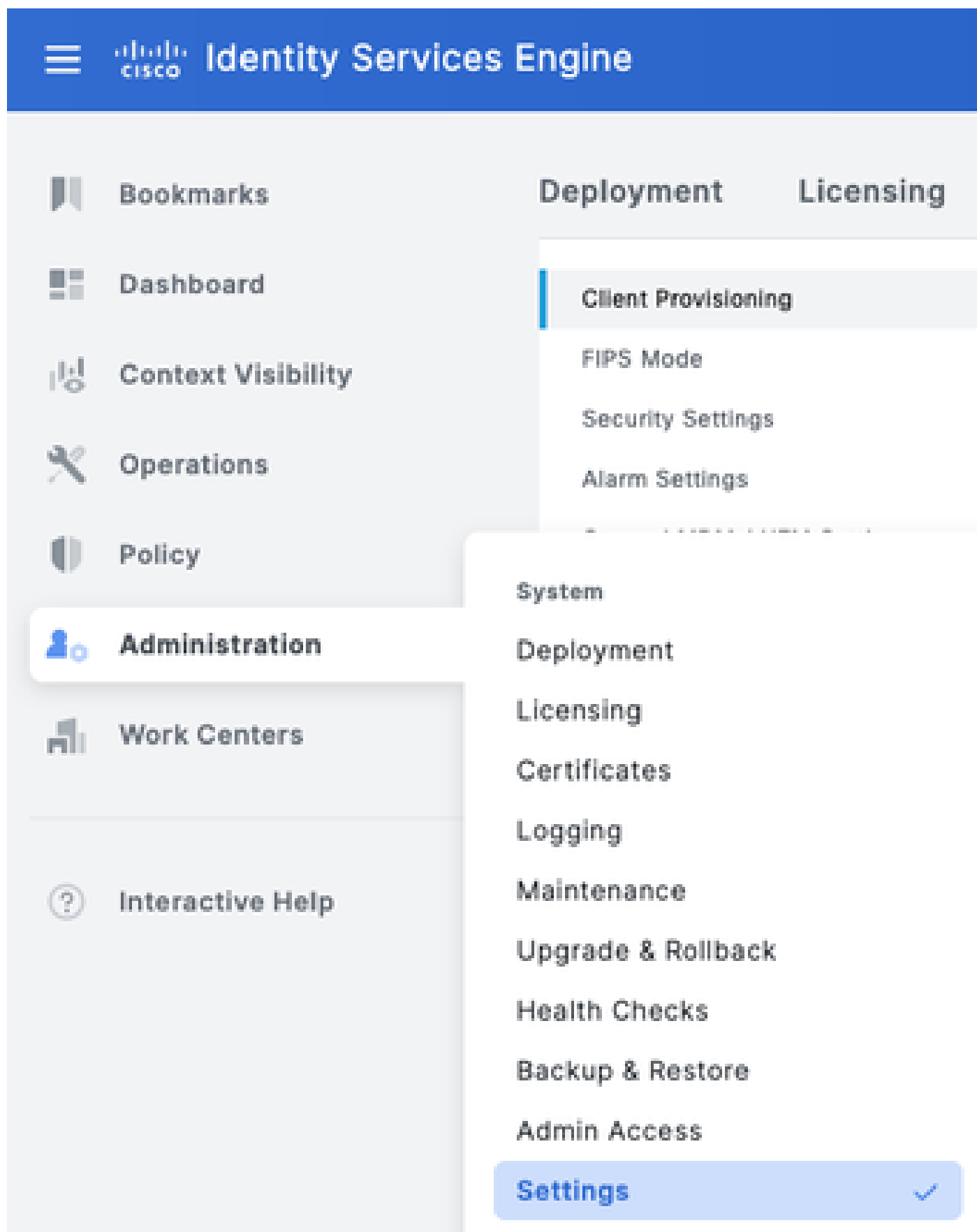
现在必须正确安装证书。您可以在System Certificates下验证这一点。



启用TLS 1.3

ISE 3.4.x中，默认情况下未启用TLS 1.3。必须手动启用它。

第1步：导航到管理>System >设置。



步骤2.单击Security Settings，选中TLS1.3 下面的TLS Version Settings复选框，然后单击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 ?



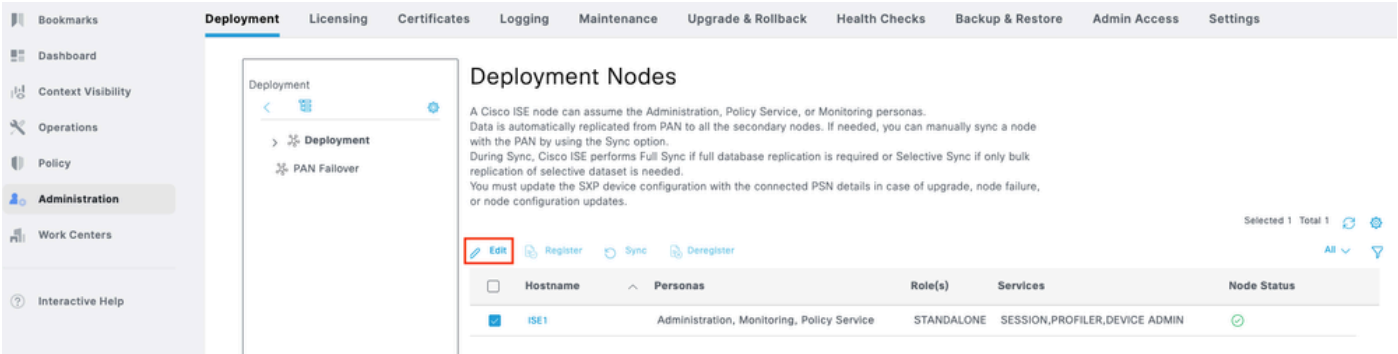
警告：当您更改TLS版本时，思科ISE应用服务器在所有思科ISE部署计算机上重新启动。

在ISE上启用设备管理

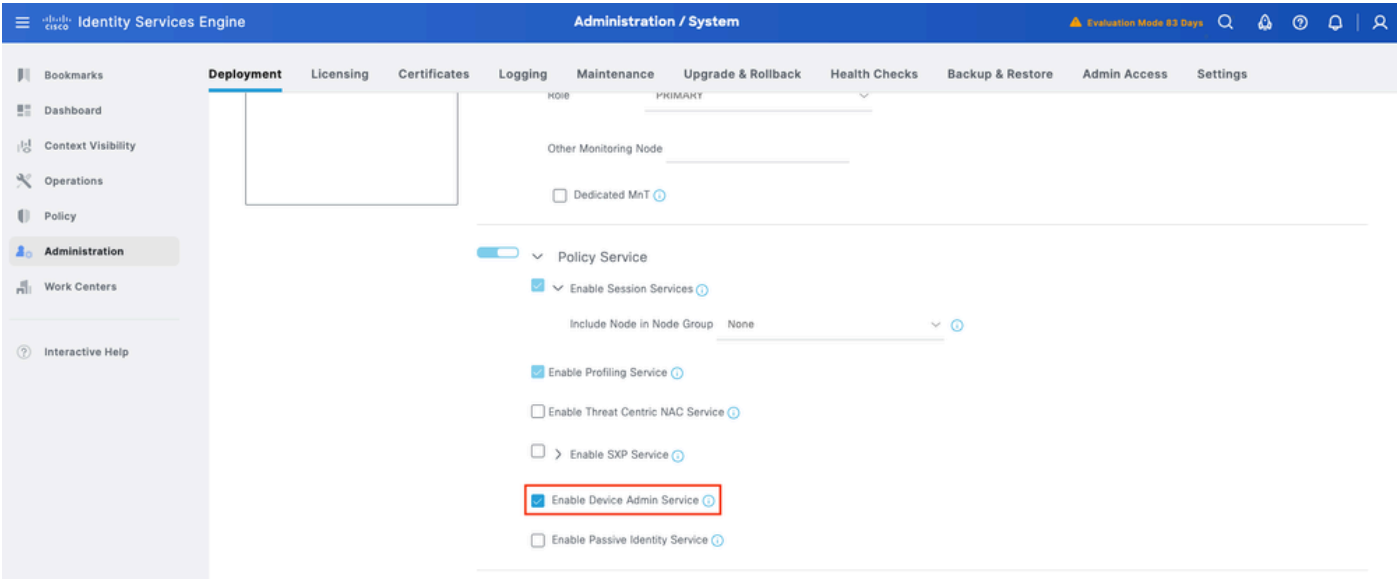
默认情况下，设备管理服务(TACACS+)未在ISE节点上启用。要在PSN节点上启用TACACS+，请

执行以下操作：

步骤1.导航到管理>系统>部署。选中ISE节点旁边的复选框，然后点击Edit。



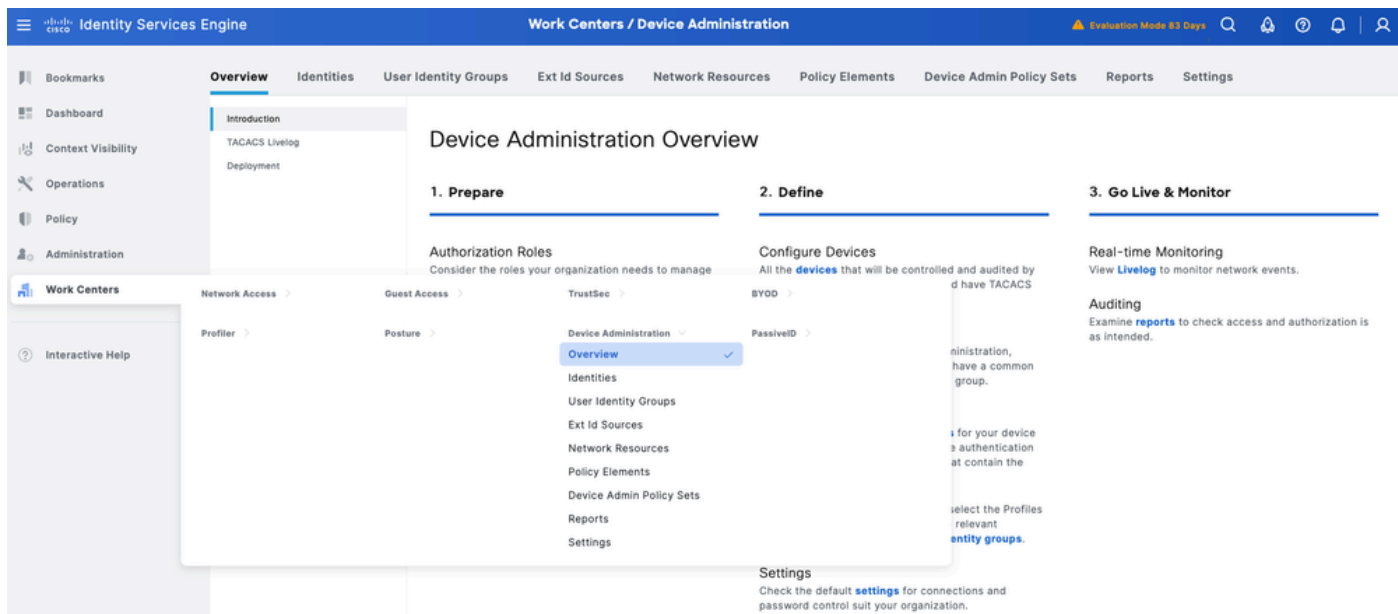
第2步：在GeneralSettings下，向下滚动并选中Enable Device Admin Service旁边的复选框。



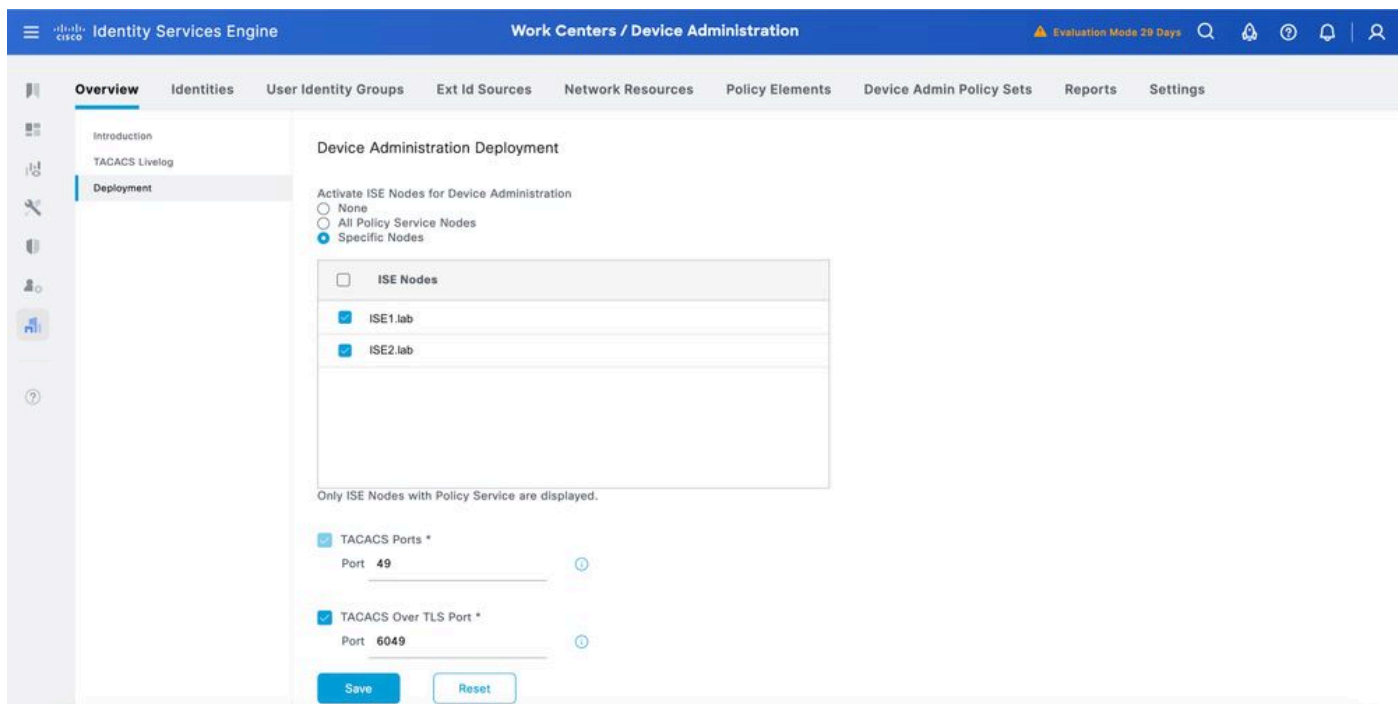
步骤3.保存配置。设备管理服务现在在ISE上启用。

启用TLS上的TACACS

第1步：导航到工作中心(Work Centers)>设备管理(Device Administration)>概述(Overview)。



步骤2.单击Deployment。选择要通过TLS启用TACACS的PSN节点。



步骤3.保留默认端口6049或为TLS上的TACACS指定不同的TCP端口，然后单击Save。

创建网络设备和网络设备组

ISE提供具有多个设备组层次结构的强大设备分组。每个分层结构代表网络设备不同的独立分类。

第1步：导航到工作中心(Work Centers)>设备管理(Device Administration)>网络资源(Network Resources)。单击网络设备组(Network Device Groups)，创建名称为IOS XR的组。

Identity Services Engine

Work Centers / Device Administration

Resolution 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

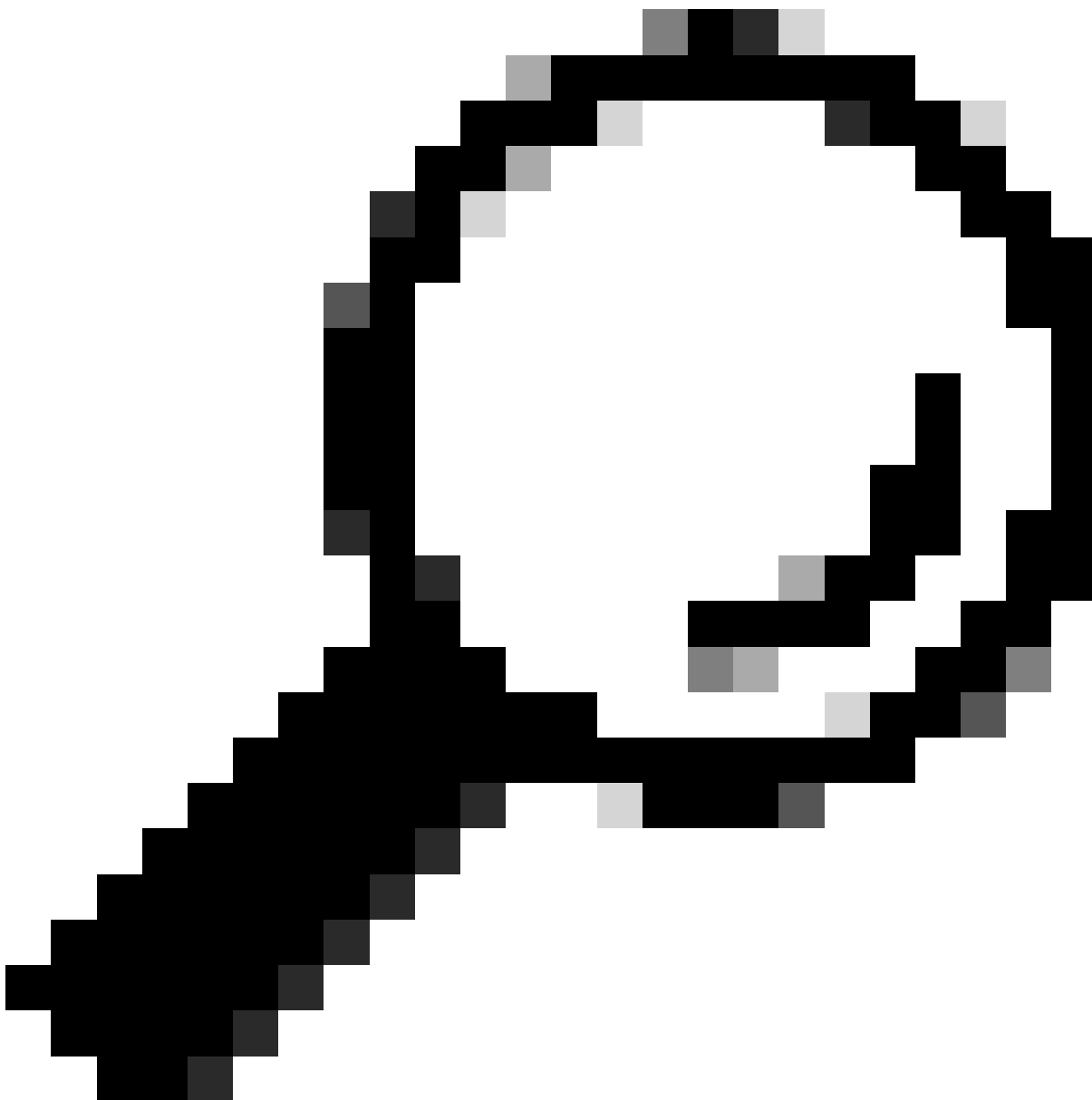
--

702

0

11

243



提示：所有设备类型和所有位置是ISE提供的默认层次结构。您可以添加自己的层次结构并定义识别网络设备中的各种组件，稍后可以在“策略条件”中使用

步骤2.现在添加Cisco IOS XR设备作为网络设备。导航至工作中心(Work Centers)>设备管理(Device Administration)>网络资源(Network Resources)>网络设备(Network Devices)。单击Add添加新的网络设备。

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

Default Device

Device Security Settings

Network Devices List > BRC-8201-1

Network Devices

NameBRC-8201-1

Description

IP Address * IP : 10.225.253.167 / 32

IP Address * IP :

Device ProfileCisco

Model Name

Software Version

Network Device Group

LocationAll Locations Set To Default

IPSECNo Set To Default

Device TypeIOS-XR Set To Default

步骤3.输入设备的IP地址，并确保映射设备的Location和Device Type(IOS XR)。最后，启用TLS身份验证设置上的TACACS+。

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 67 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

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)*

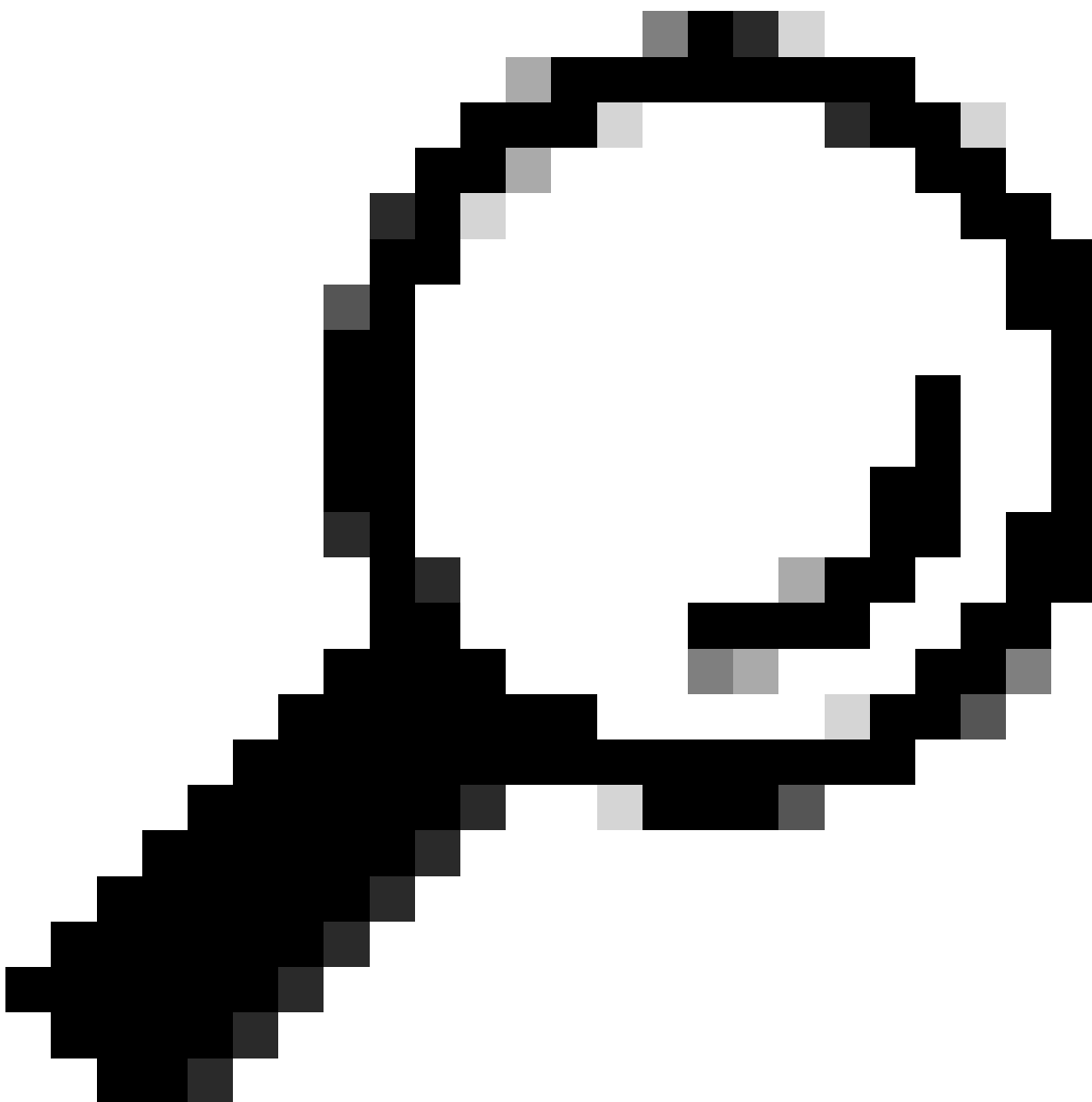
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When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

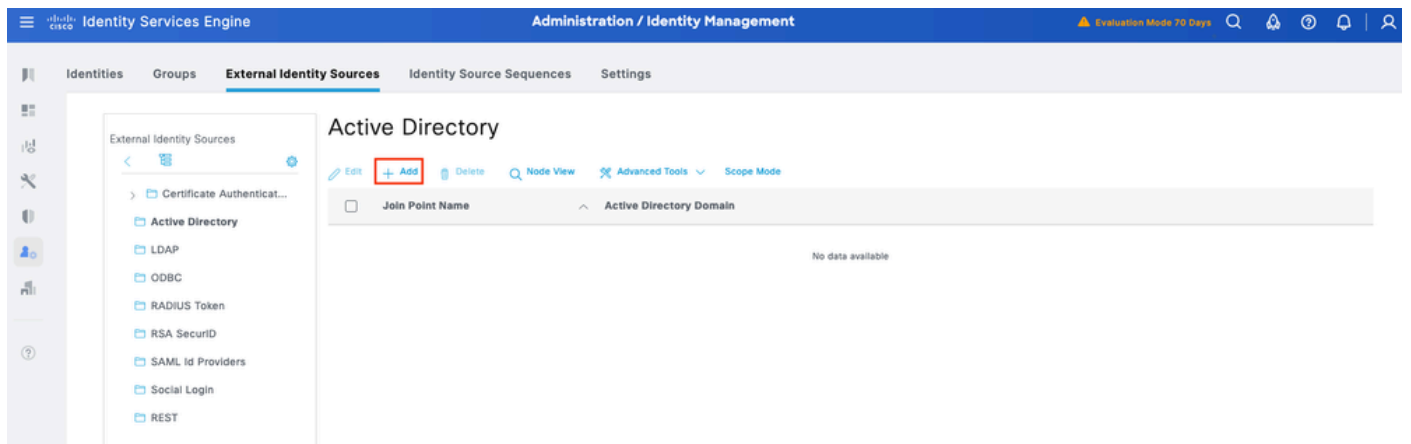


提示：建议启用单一连接模式，以避免每次向设备发送命令时重新启动TCP会话。

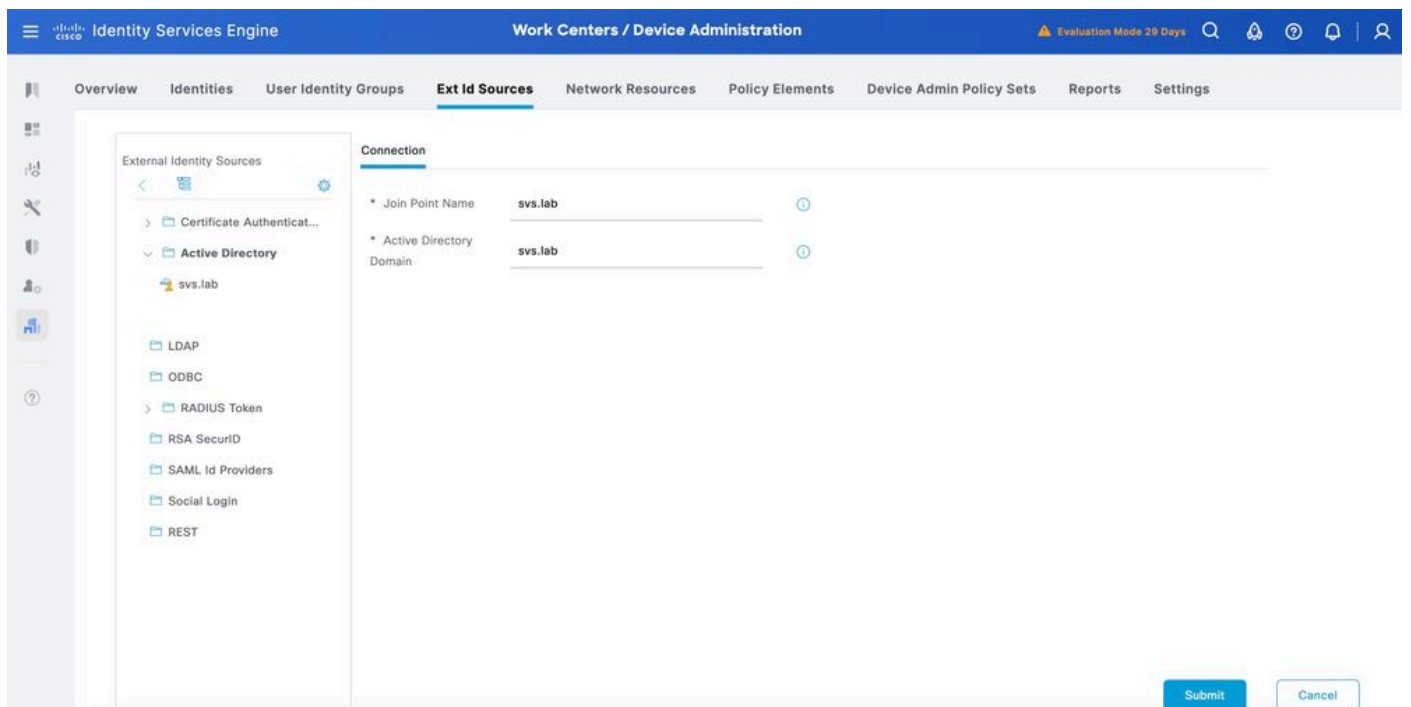
配置身份库

此部分定义设备管理员的身份库，可以是ISE内部用户和任何支持的外部身份源。此处使用外部身份源Active Directory(AD)。

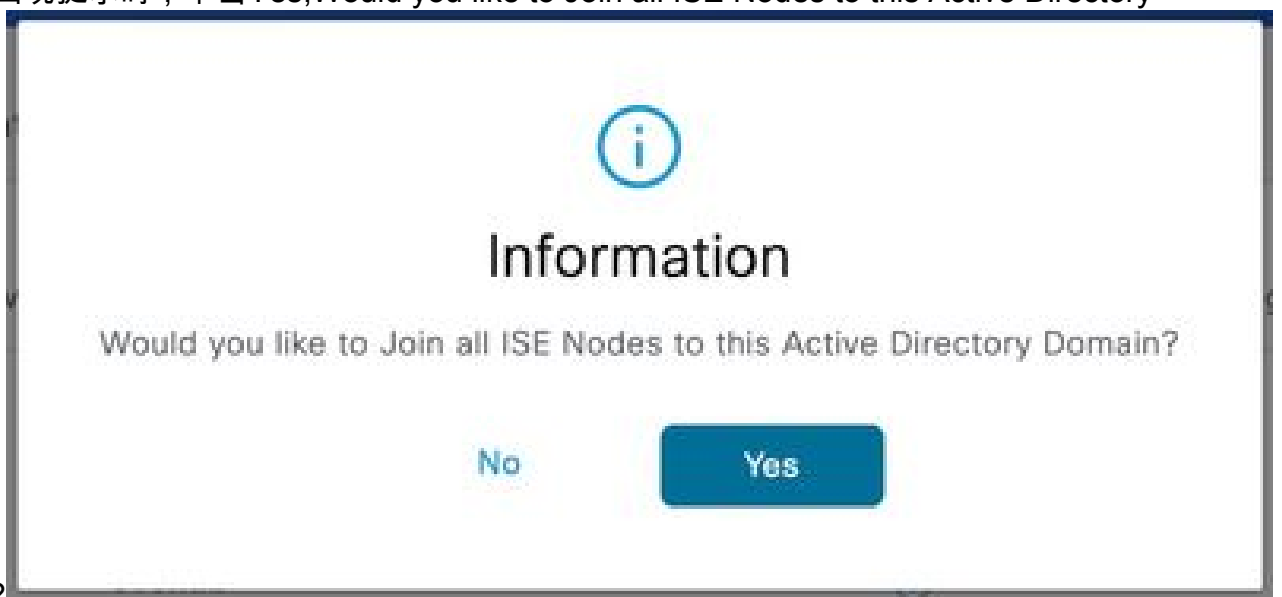
第1步：导航到管理>身份管理>外部身份库> Active Directory。单击Add以定义新的AD接点。



步骤2.指定加入点名称和AD域名，然后单击提交。



第3步：出现提示时，单击Yes,Would you like to Join all ISE Nodes to this Active Directory



Domain?

第4步：输入具有AD加入权限的凭证，然后将ISE加入到AD。检查状态以验证其是否正常运行。

×

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

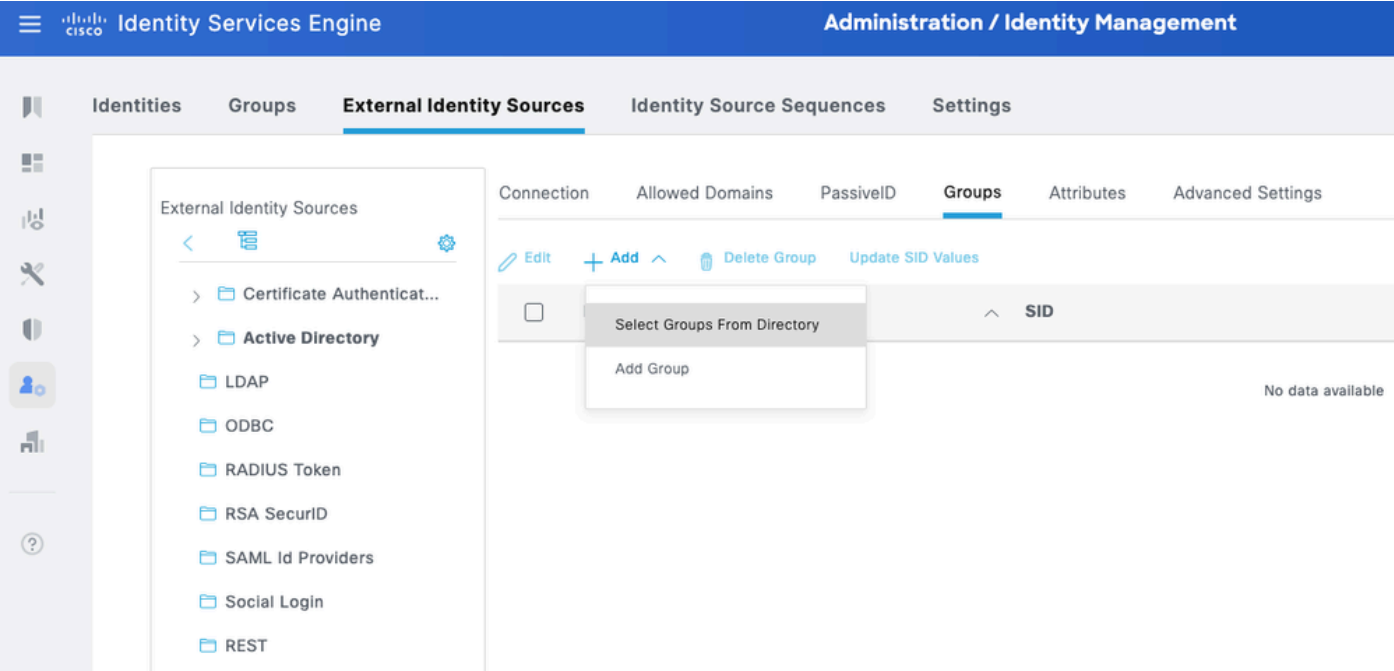
Status Summary: Successful.

ISE Node	Node Status
ISE1.lab	✔ Completed.

Close

第5步：导航到Groups选项卡，然后点击Add获取根据哪些用户有权访问设备而需要的所有组。此

示例显示授权策略中使用的组。



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

svs.lab

Name

Device *

SID *

Type

ALL

Filter

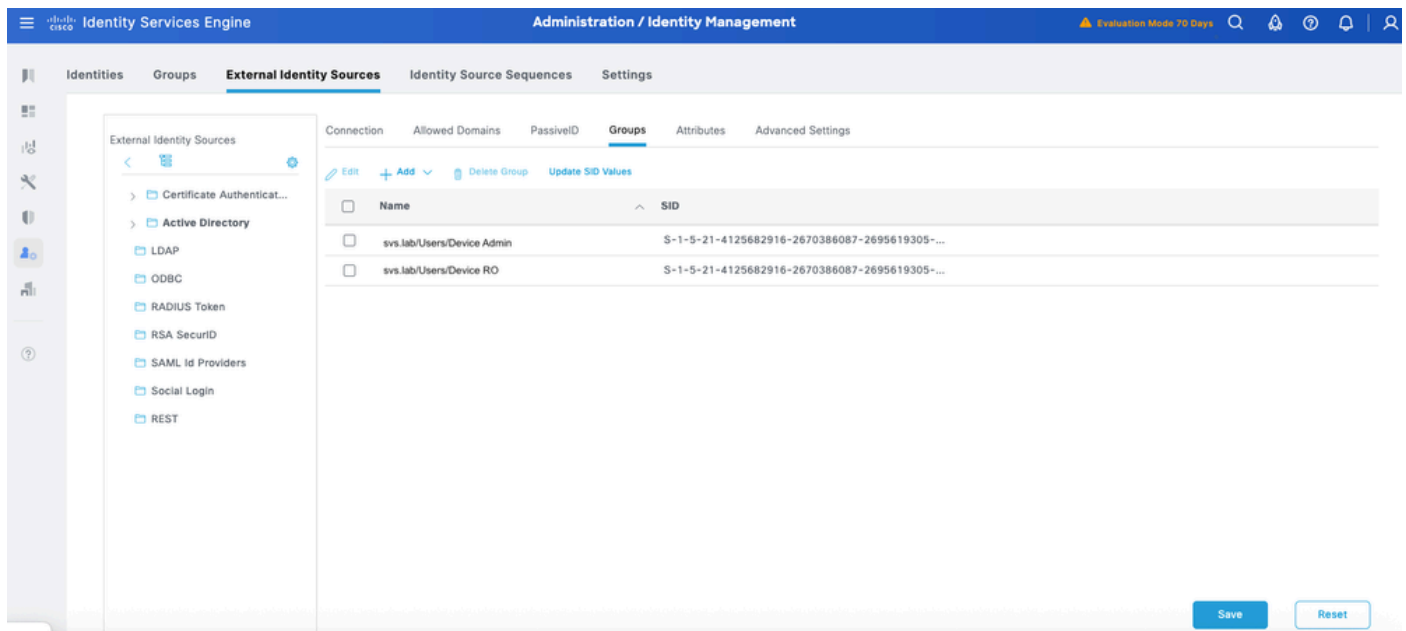
Filter

Filter

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



配置TACACS+配置文件

将TACACS+配置文件映射到思科IOS XR设备上的用户角色。在本示例中，定义以下内容：

- 根系统管理员 — 这是设备中的最高特权角色。具有root系统管理员角色的用户对所有系统命令和配置功能具有完全管理访问权限。
- 操作员 — 此角色适用于出于监控和故障排除目的而需要对系统进行只读访问的用户。

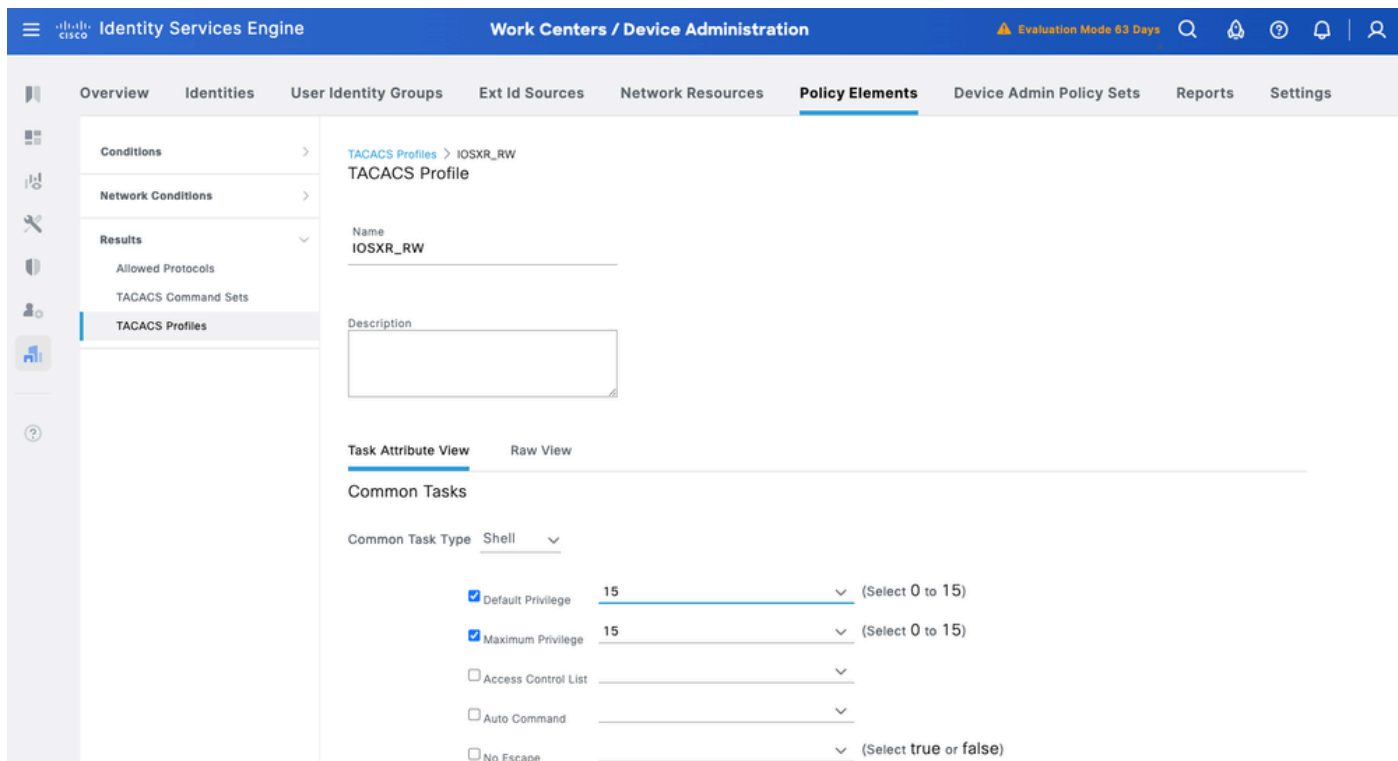
定义两个TACACS+配置文件：IOSXR_RW和IOSXR_RO。

IOS XR_RW — 管理员配置文件

步骤1.导航到工作中心>设备管理>策略元素>结果> TACACS配置文件。添加新的TACACS配置文件并将其命名为IOSXR_RW。

步骤2.检查并将Default Privilege和Maximum Privilege设置为15。

步骤3.确认配置并保存。

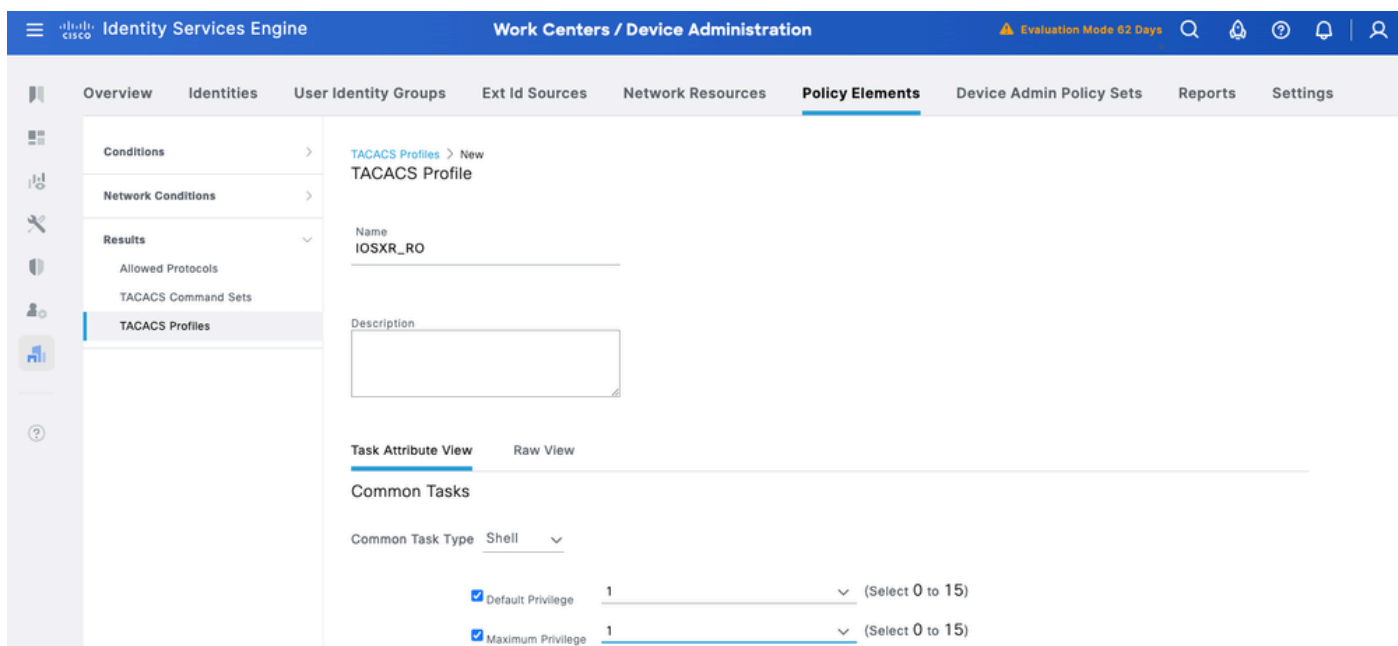


IOS XR_RO — 运营商配置文件

步骤1.导航到工作中心>设备管理>策略元素>结果> TACACS配置文件。添加新的TACACS配置文件，并将其命名为IOSXR_RO。

步骤2.检查并将Default Privilege和Maximum Privilege设置为1。

步骤3.确认配置并保存。



配置TACACS+命令集

定义TACACS+命令集：在本例中，这些命令定义为CISCO_IOSXR_RW和CISCO_IOSXR_RO。

CISCO IOS XR RW — 管理员命令集

步骤1.导航到工作中心>设备管理>策略元素>结果> TACACS命令集。添加新的TACACS命令集并将其命名为CISCO_IOSXR_RW。

步骤2.选中Permit any command that not listed below复选框（这将允许管理员角色使用任何命令），然后单击Save。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', 'Work Centers / Device Administration', and an 'Evaluation Mode 63 Days' warning. The left sidebar contains a menu with '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 Command Sets > CISCO_IOSXR_RW Command Set'. It includes a 'Name' field with 'CISCO_IOSXR_RW', a 'Description' text area, and a 'Commands' section with a checked checkbox for 'Permit any command that is not listed below'. Below this are buttons for 'Add', 'Trash', 'Edit', 'Move Up', and 'Move Down'. A table with columns 'Grant', 'Command', and 'Arguments' is shown, currently empty with the message 'No data found.' At the bottom right are 'Cancel' and 'Save' buttons.

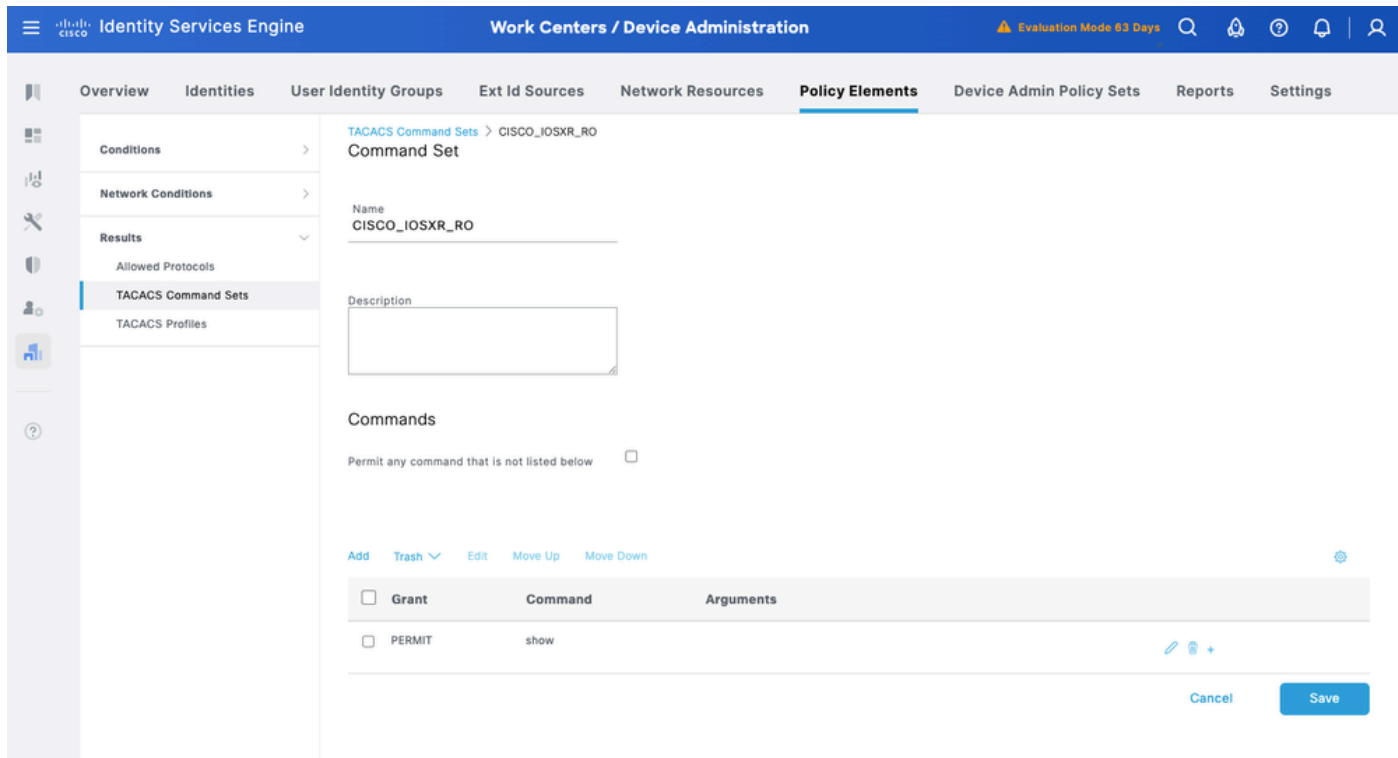
CISCO IOS XR RO — 操作员命令集

步骤1.从ISE UI导航到工作中心>设备管理>策略元素>结果> TACACS命令集。添加新的TACACS命令集并将其命名为CISCO_IOSXR_RO。

步骤2.在命令部分，添加一个新命令。

步骤3.从Grant 列的下拉列表中选择Permit，然后在Command 列中输入show;然后单击check箭头。

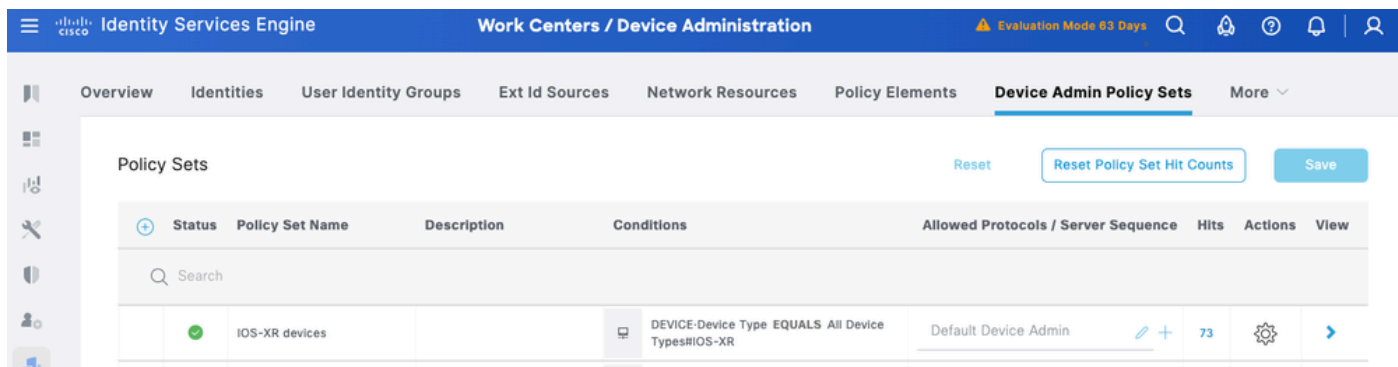
步骤4.确认数据并单击保存。



配置设备管理策略集

默认情况下，为设备管理启用策略集。策略集可以根据设备类型划分策略，以简化TACACS配置文件的应用。

第1步：导航到Work Centers > Device Administration > Device Admin Policy Sets。添加新的策略集IOS XR设备。在条件下，指定DEVICE:Device Type EQUALS All Device Types#IOS XR。在允许的协议下，选择默认设备管理。



步骤2.点击保存，然后点击右箭头配置此策略集。

步骤3.创建身份验证策略。对于身份验证，使用AD作为ID存储。保留If Auth fail，If User not found和If Process fail下的默认选项。

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

More

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	73

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
Search					
	Default		svs.iab	85	

Options

If Auth fail
REJECT

If User not found
REJECT

If Process fail
DROP

步骤4.定义授权策略。

根据Active Directory(AD)中的用户组创建授权策略。

例如：

- 为AD组设备中的用户分配CISCO_IOSXR_RO 命令集和IOSXR_RO 外壳配置文件。
- AD组Device Admin中的用户被分配为CISCO_IOSXR_RW 命令集和IOSXR_RW Shell配置文件。

Identity Services Engine **Work Centers / Device Administration** ⚠️ Evaluation Mode 62 Days 🔍 🛎️ ⓘ 📧 | 👤

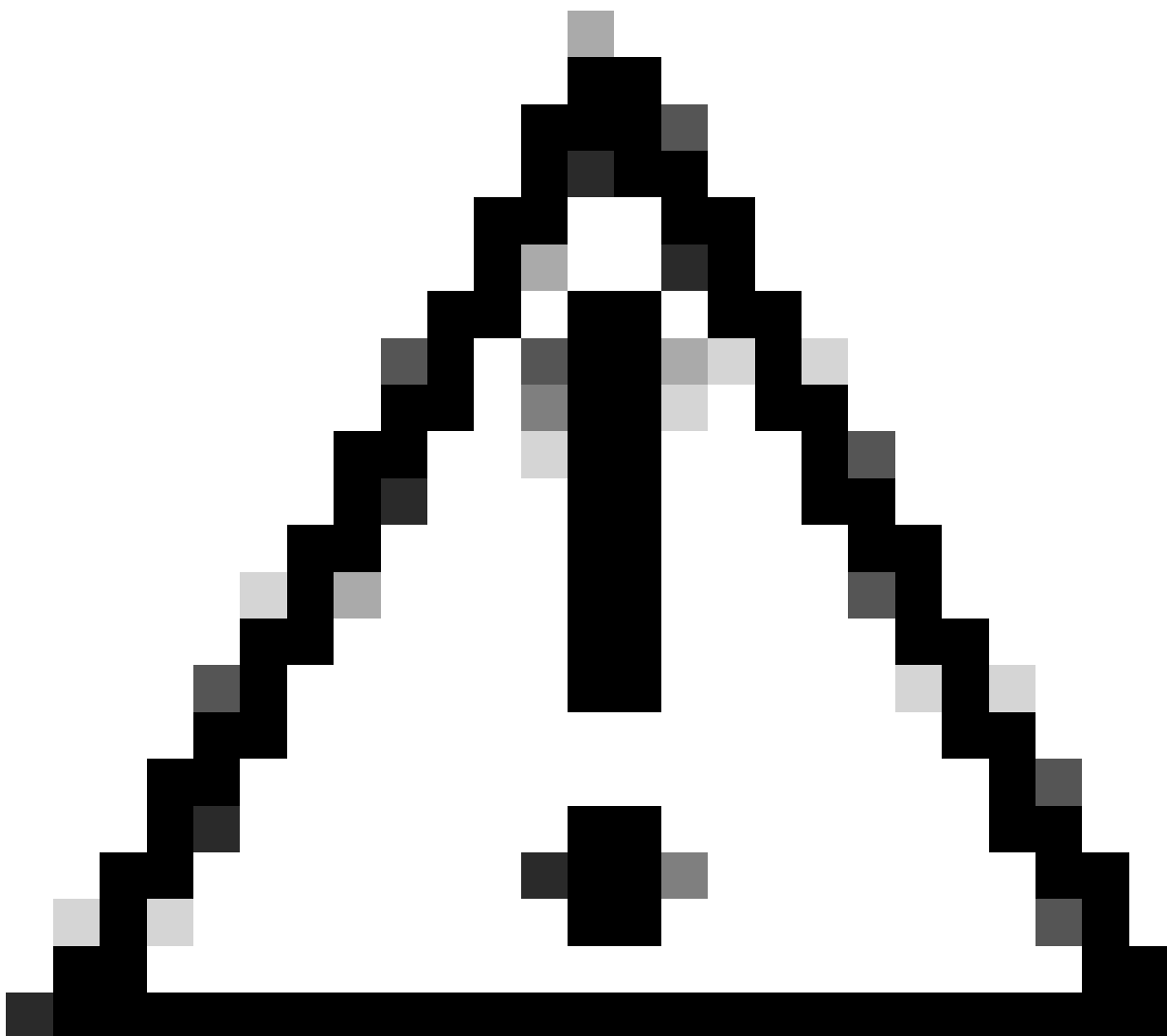
Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets → IOS-XR devices [Reset](#) [Reset Policy Set Hit Counts](#) [Save](#)

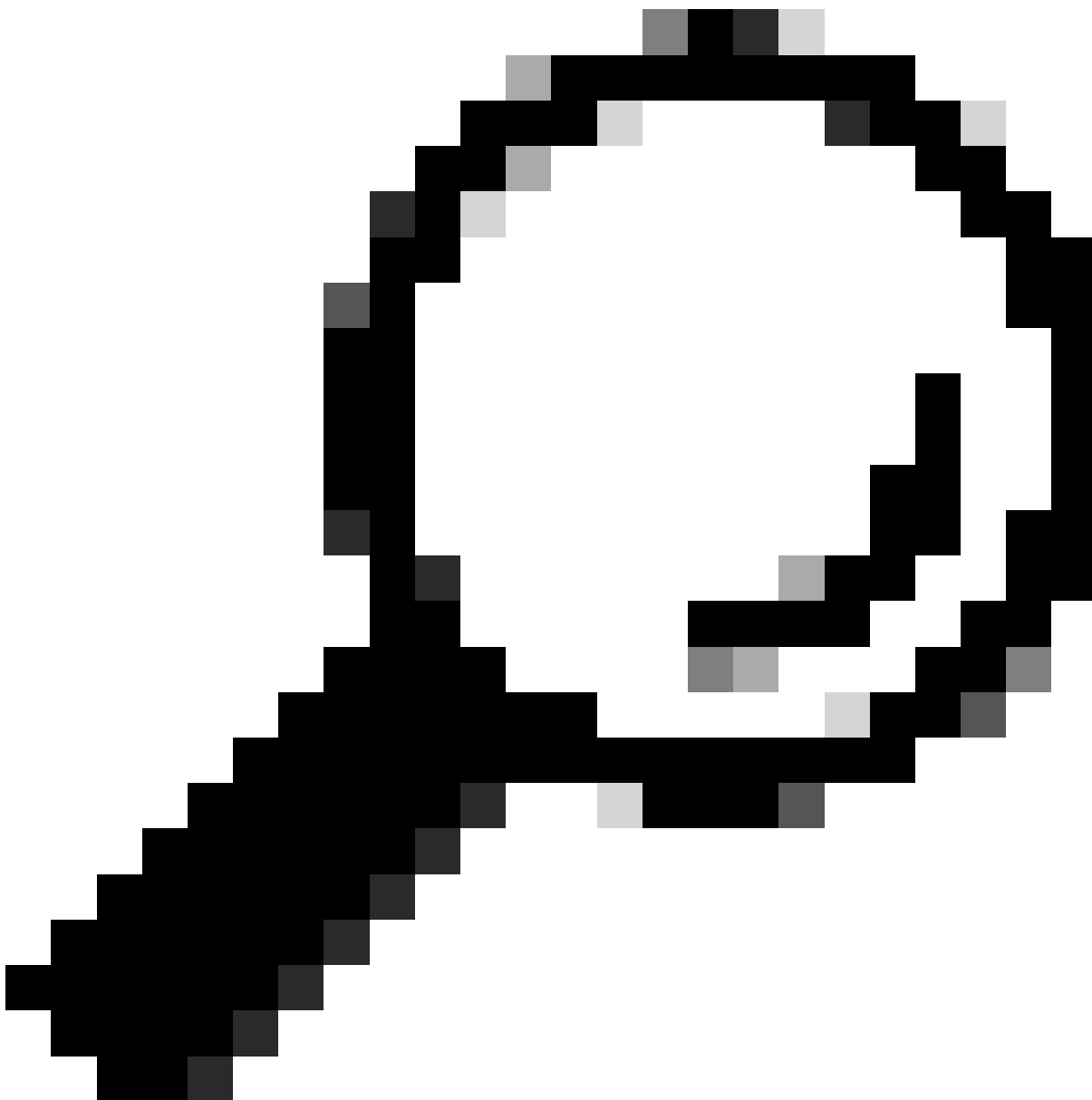
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search					
🟢	IOS-XR devices		DEVICE=Device Type EQUALS All Device Types#IOS-XR	Default Device Admin ✏️ +	77
> Authentication Policy(1)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
∨ Authorization Policy(3)					

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

第2部分 — 配置Cisco IOS XR，使其适用于TLS 1.3上的TACACS+



警告：确保控制台连接可达且运行正常。



提示：建议配置临时用户，并更改AAA身份验证和授权方法，以便在更改配置时使用本地凭证而非TACACS，以免被设备锁定。

初始配置

步骤1.确保配置名称服务器(DNS)，并且路由器能够成功解析频繁限定域名(FQDN)，特别是ISE服务器FQDN。

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

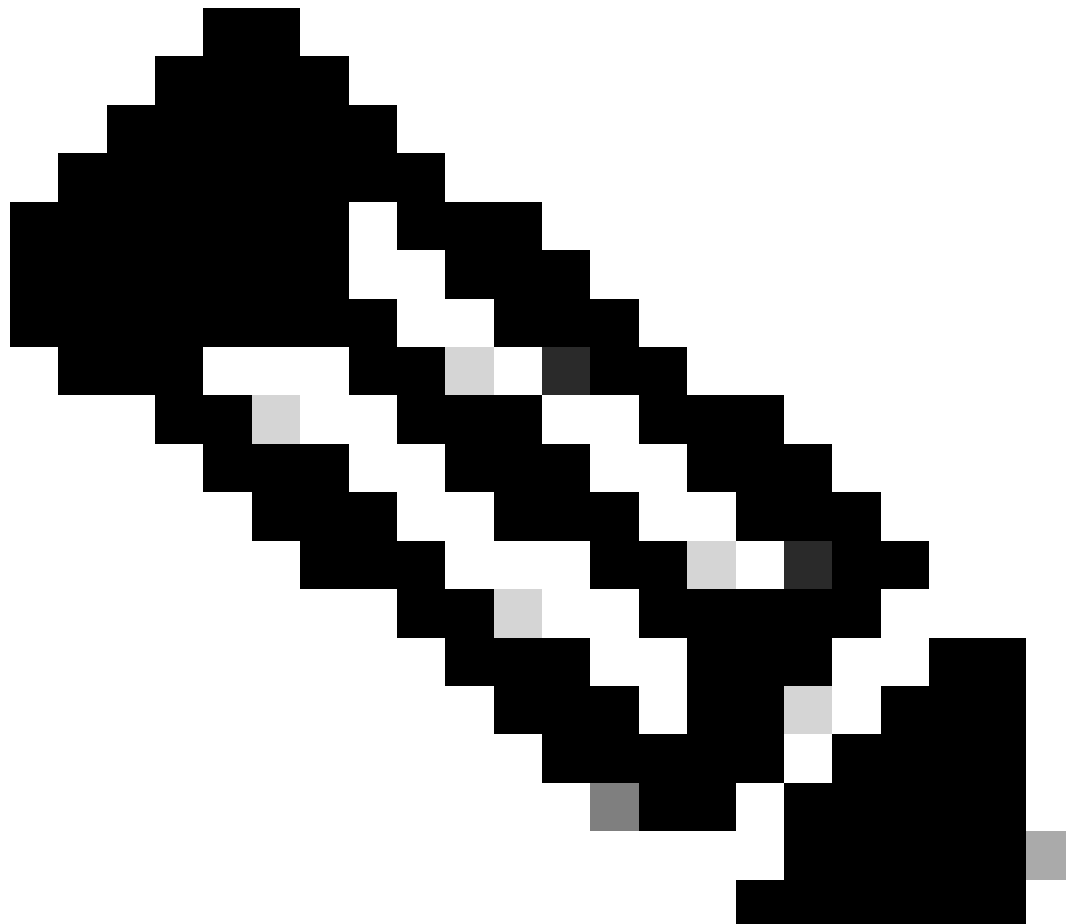
```
RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
Type escape sequence to abort.
```

```
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
```

步骤2.清除所有旧/未使用的信任点和证书。请确保不存在旧的信任点和证书。如果看到任何旧条目，请将其删除/清除。

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

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



注意：您可以手动创建新的RSA密钥对并将其附加到信任点下。如果不创建密钥对，则使用默认密钥对。当前不支持在信任点下定义ECC密钥对。

配置信任点

步骤1.密钥对配置 (可选)。

```
<#root>
```

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

```
crypto key generate rsa
```

```
4096
```

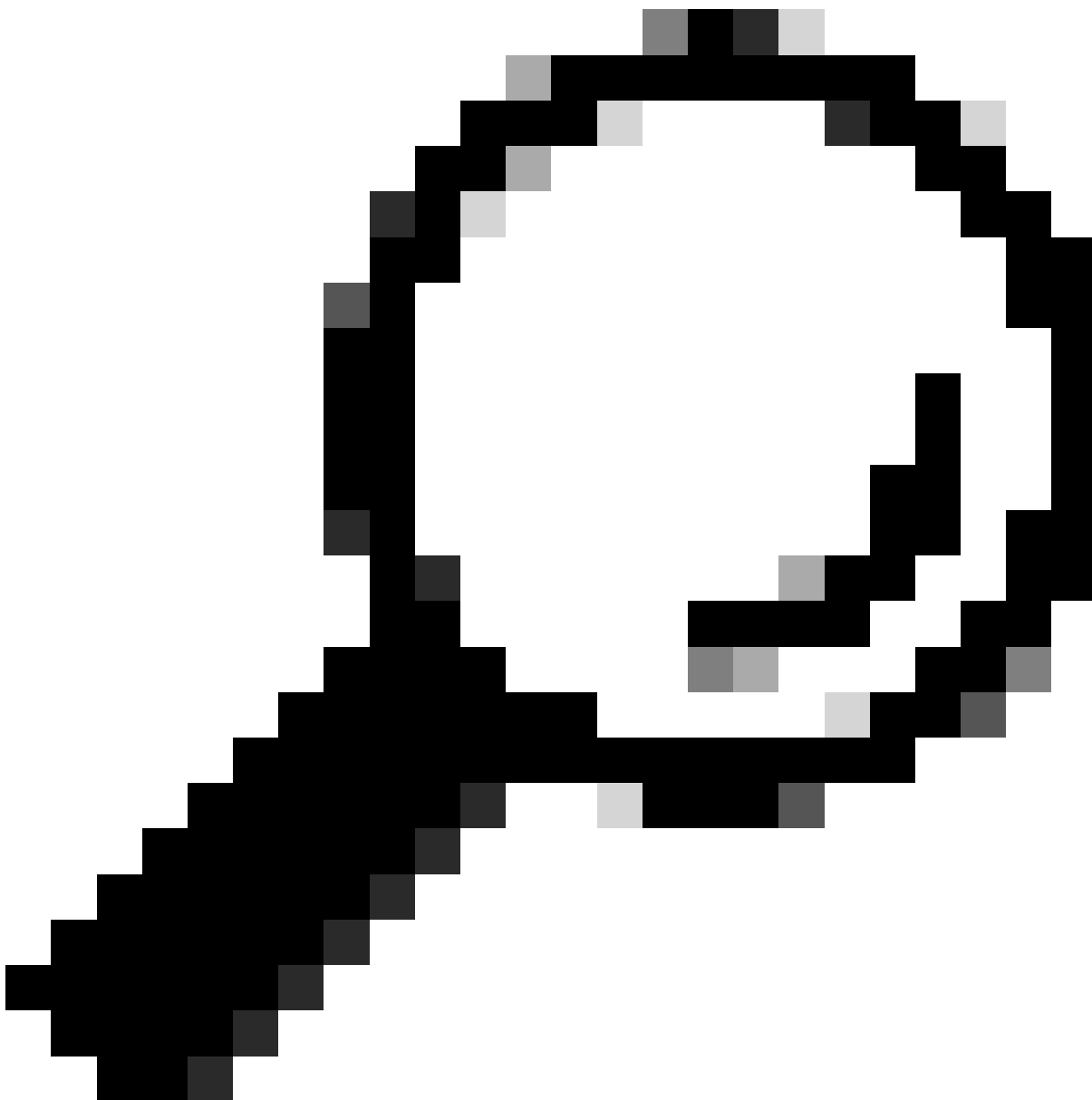
```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto ca trustpoint
```

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

```
rsakeypair
```

步骤2.创建信任点。



提示：主题备用名称的DNS配置是可选的（如果在ISE上启用），但建议使用。

```
<#root>
```

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

```
crypto ca trustpoint svs
```

```
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)#

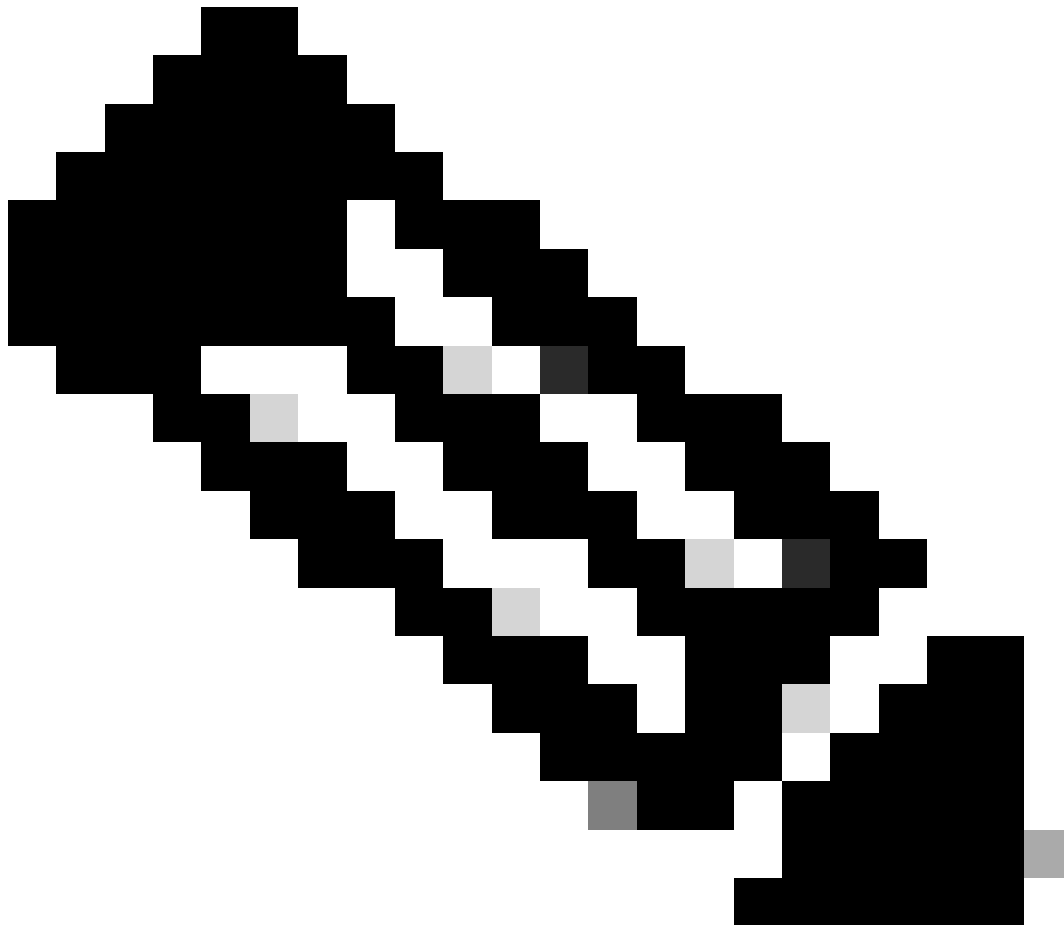
enrollment url terminal

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

rsakeypair svs-4096

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

commit



注意：如果需要在O或OU中使用逗号，可以在逗号前使用反斜线(\)。例如：O=思科系统公司

步骤3.通过安装CA证书对信任点进行身份验证。

<#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-----

```
MIIFDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMjUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBMWJDQTC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTty+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBBjHfM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULo/wxMHdTbtPBf11HRHTkNIO3qy04UADL2
WpoGhGT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpl334rTixy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XC0NX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCSAGG+EIBDQMFgptV1MgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAITA08oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
0+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpiYtprokz1UvZBZ8v1oI7YzmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

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

quit

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

Subject:

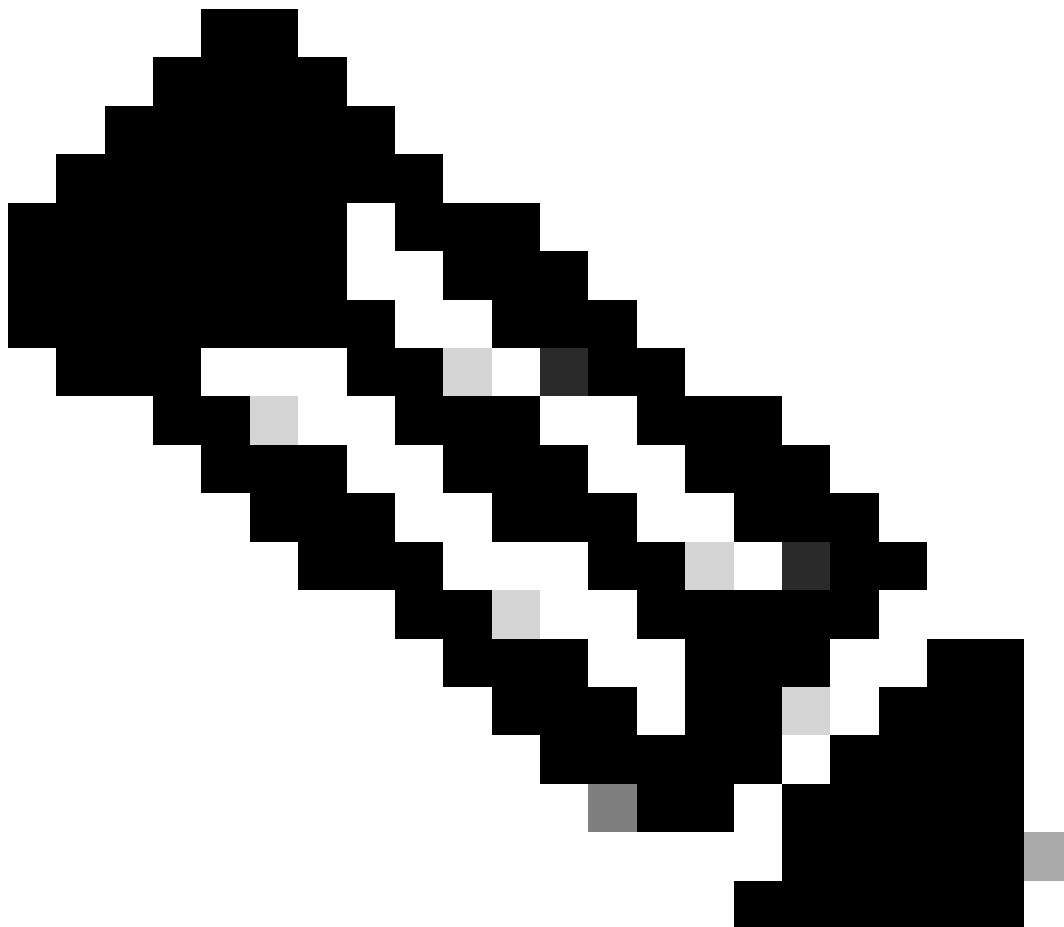
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US

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
```



注意：如果您有从属CA系统，则需要导入根CA和子CA证书。使用相同的命令，其中Sub CA位于顶部，Root CA位于底部。

步骤4.生成证书签名请求(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-----

MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAk5DMQwwCgYDVQQQH
DANSVFAXDjAMBGNVBAoMBUNpc2NmMQwwCgYDVQQQLDANTVlMxZzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtr1oDH9iOZxPvEDARwN0t4WrPEjaQc1ZUA
6ax6Cxq/0JlQiUf2+eQv+4rKZqAZ1xDhiaIMGqETn00LKpwmtx10IqXL7UYMHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRwMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkKwI0cb1X2HgtbVQdCXTAwJDmr209
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAACBiTAYBgqhkiG
9w0BCQcxCMJQzFzY28uMTIzMG0GCSqGSIb3DQEJJDJFgMF4wDgYDVROPAQH/BAQD
AgWgMCAGA1UdJQEB/wQwMBQGCSqGSIb3DQEJJDJFgMF4wDgYDVROPAQH/BAQD
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBbX0eWF5ZUz701GFjuQHBBdgYb+3lhF0xbYm9psIWfv1uwjKkOL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswj1YpO+IxxUM971Ejwg2rj+jABDR7I8SU
06Y06mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTI1jdgVxB+Xyz0FJMckI05US3j
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f90A+fdg2zYt0ME
Z6VAw64cY+YF6iLbYv7c4l1z05Zj2NJBkUpeqijkFAKY/1rIXTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZN00

```
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:

no
```

步骤5.导入CA签名证书。

```
<#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
BhMCVVMxZmZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA5MTQ1NzAwWWhcNMjUwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkMxDDAKBgNVBACMA1JUUEDEOMAwGA1UECgwFQ21zY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAuMjUwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
OTA4NDNiMiIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOd02uW
gMf2I5nE+8QMBHA3S3has8SNpByV1QDprHoLGr/QmVCJR/b55C/7ispmoBnXE0GJ
qIwaoR0c7QsqnCa3HXQipcvrtRgwcFAX29Egjnboi aRYDxrddbHrpSQTfpeh5dp/k
eQuio07rxfdzTss+8x7WwzC+artGbLYMC7fQcH819iVAIeZNUXPcz18G3zrHHI3W
fFMVT/iVFYwLvdR0v1h0okuMykFPa00TemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTajRxxvFyEC1tVB0JdMDAK0avY73N3Zkjr16dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0
ZTA0BgNVHQ8BAf8EBAMCBaAwIAyDVR01AQH/BBYwFAYIKwYBBQUHAWEGCCsGAQUF
BwMCMAMkGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAuMjUwDQYJKoZIhvcNAQELBQADggIBAARpS5bEck+oj012106WxedDQ8Vdu0bBtrn0H+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTzrQ93tb9mMTZg7exqN89ZU
V1XoB2U0Tri5K10/+izEGgyNq42/ytAP8Y007HR/2jf7gfhovwR5QN0EHv4o61
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV81RGXxxgyt1mwNmb7EiAc81odRcgyp7FNh3
F/k9cMMMr51M4Ysvo1tx1k9AeLjb2syv5/fG6Qu0ZdWwTaaQh0Y2h/cVDiV97wg
0D1mEfDsv6QrxQSujZr22RzVykKH1tuiV2B74pthUuGRBtFHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDp1rf1ZIrPmv3ZPP7woTB22yWzyd0use+5Ia1b0w70twN4t/Iiw
8CJu6HfnDXLDPZ0jsC8steffrS1opwGccp3j6aZKPFz+I/Purb44a9WxEwa2TA7H
+r1oynBcGMet0HxVLnptlsC7Q4mN/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

验证路由器身份证书是否已注册。

<#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
```

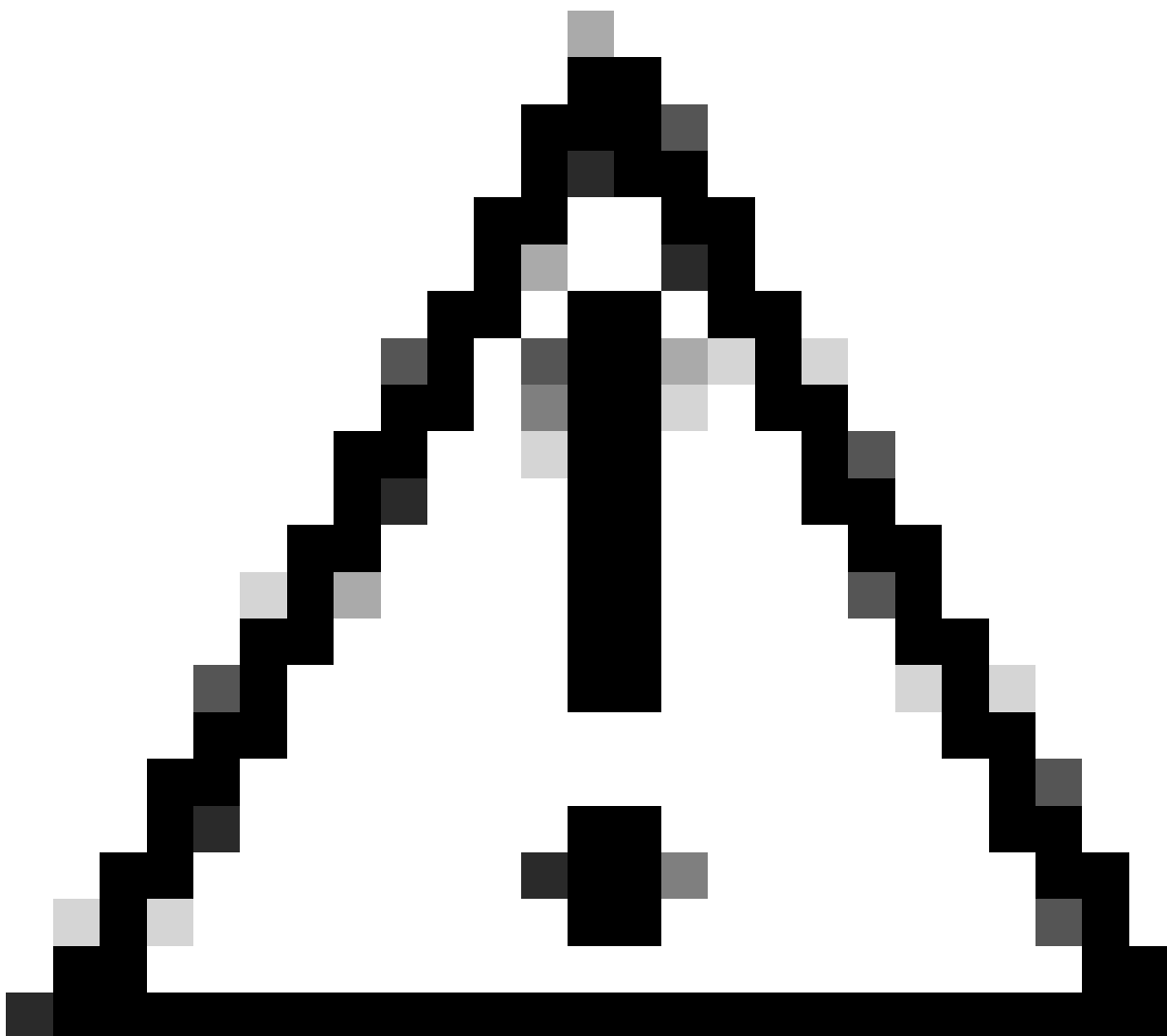
RP/0/RP0/CPU0:BRC-8201-1#

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
```

使用TLS配置TACACS和AAA



警告：使用本地凭证通过控制台执行配置更改。

步骤1.配置TACACS+服务器。

```
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
```

步骤2.配置AAA组。

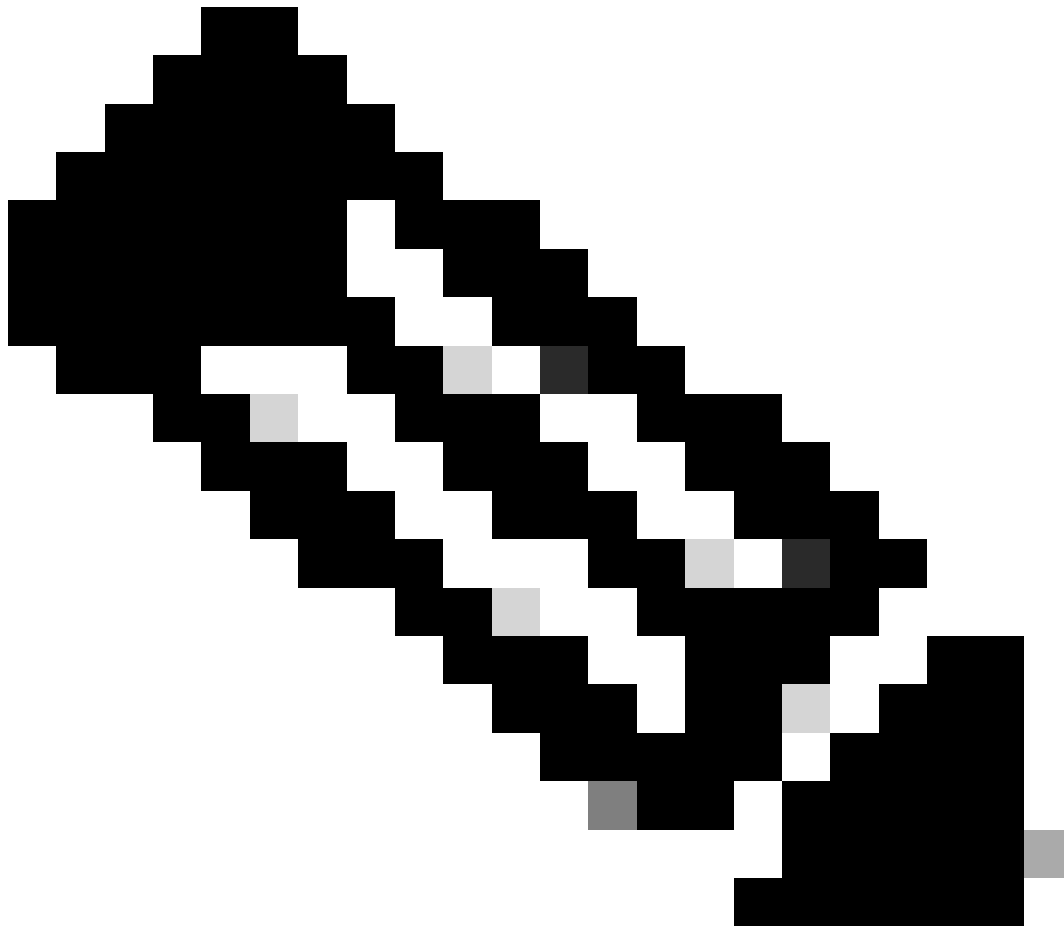
```
aaa group server tacacs+ tac_tls_sc
```

```
vrf mgmt
server-private 10.225.253.209 port 6049
timeout 10
tls
  trustpoint sv
  !
single-connection
```

步骤2.配置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
```

证书续订



注意：续订期间无需从TACACS+配置中删除信任点。

步骤1.验证当前证书有效日期。

```
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
```

步骤2.删除现有信任点证书。

```
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#
```

步骤3.按照Trustpoint Configuration下的步骤中所述重新验证并注册信任点。

步骤4.验证证书有效日期是否已更新。

```
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

确认

验证配置。

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

TACACS+调试

```
debug tacacs tls
```

调试TLS

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

在配置AAA身份验证之前测试远程用户。

```
<#root>
```

```
test aaa group tacacs2
```

```
user has been authenticated
```

故障排除

清除证书（这将删除与信任点关联的所有证书）。

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

TACACS进程重新启动（如有必要）

```
process restart tacacsd
```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。