在带有ISE的IOS XE设备上通过TLS 1.3配置TACACS+

目录

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® XE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 XE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 — 为TLS上的TACACS+配置Cisco IOS XE

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 IOS XE软件，版本17.15+

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。

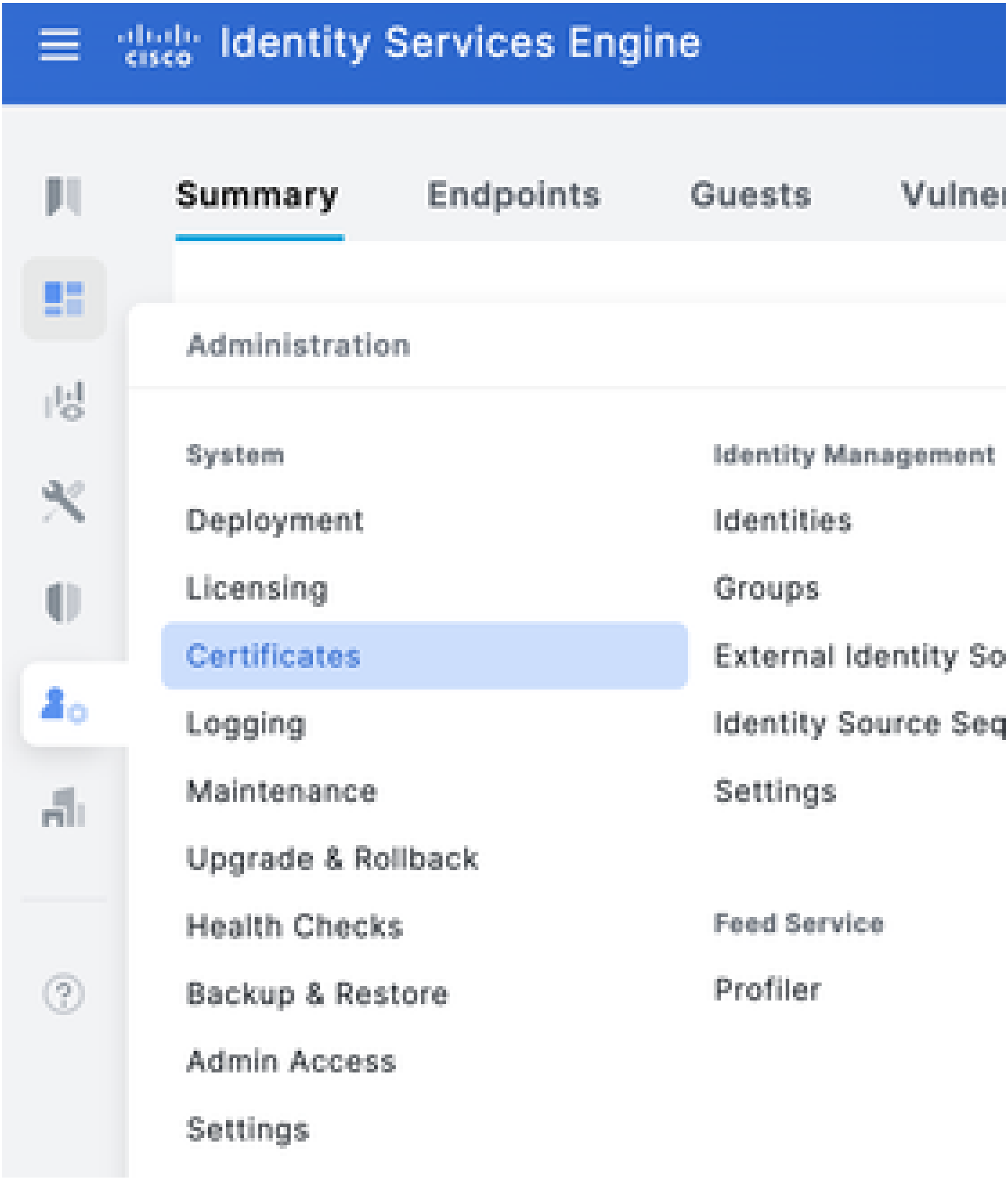
第1部分 — 配置ISE进行设备管理

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。

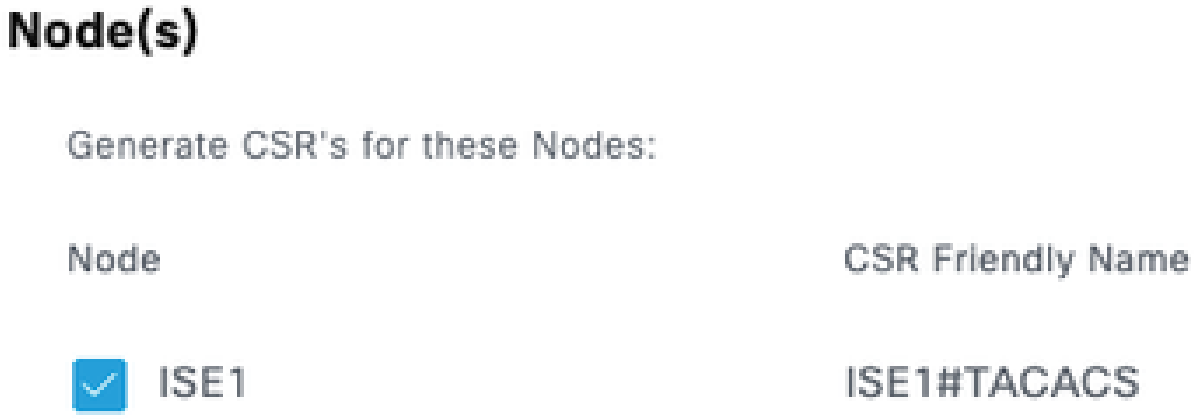
第2步：导航到Administration > System > Certificates。



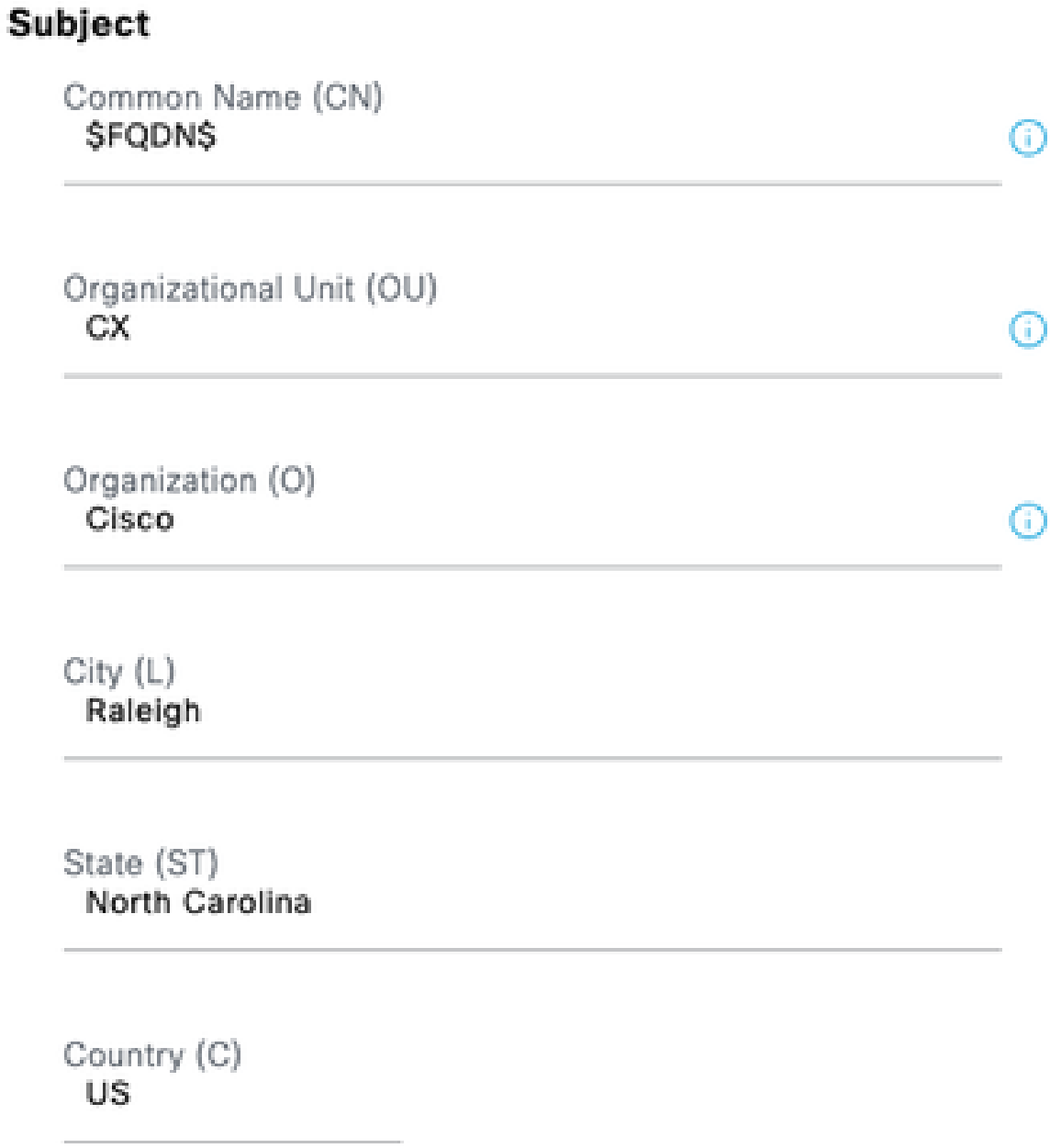
第 3 步： 在Certificate Signing Requests下，单击Generate Certificate Signing Request。

第4步：选择TACACS inUsage。

第5步：选择将启用TACACS+的PSN。

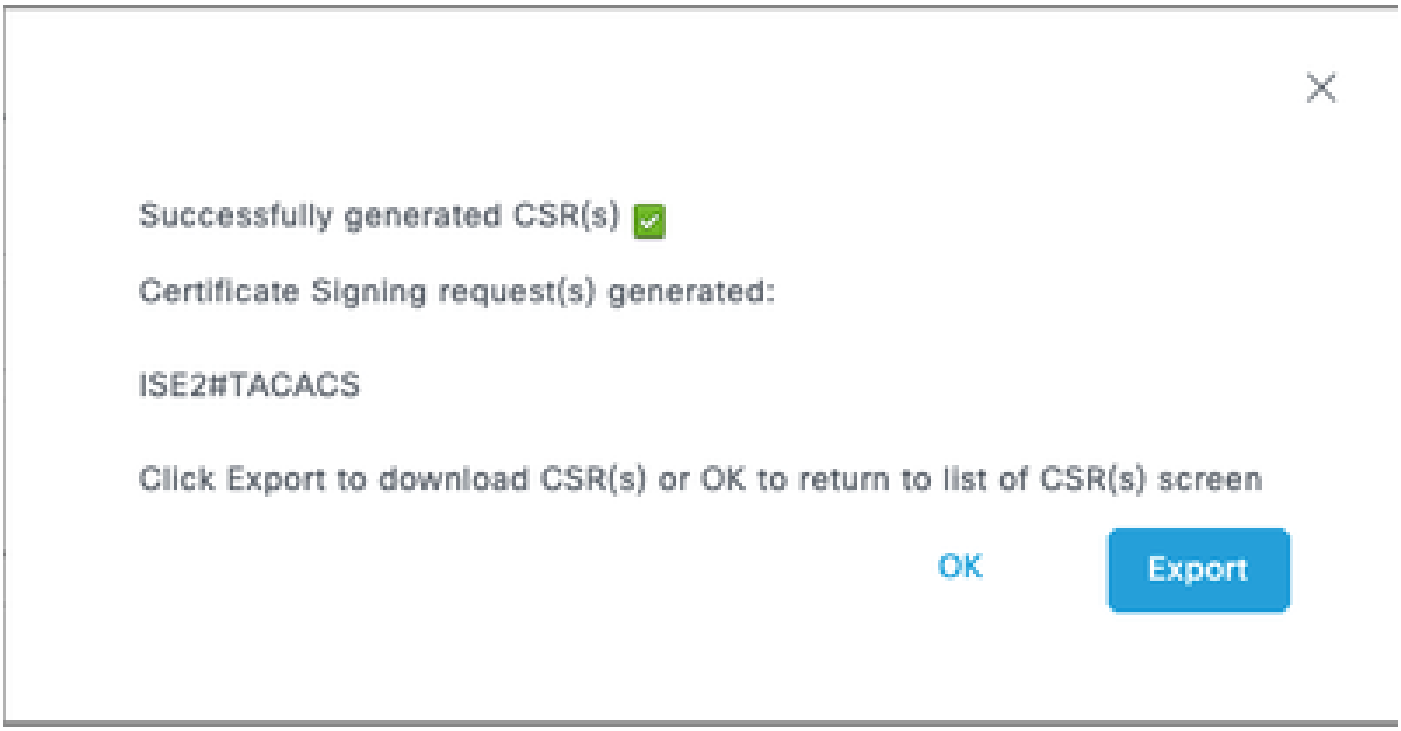


步骤6.使用适当的信息填充Subject字段。



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

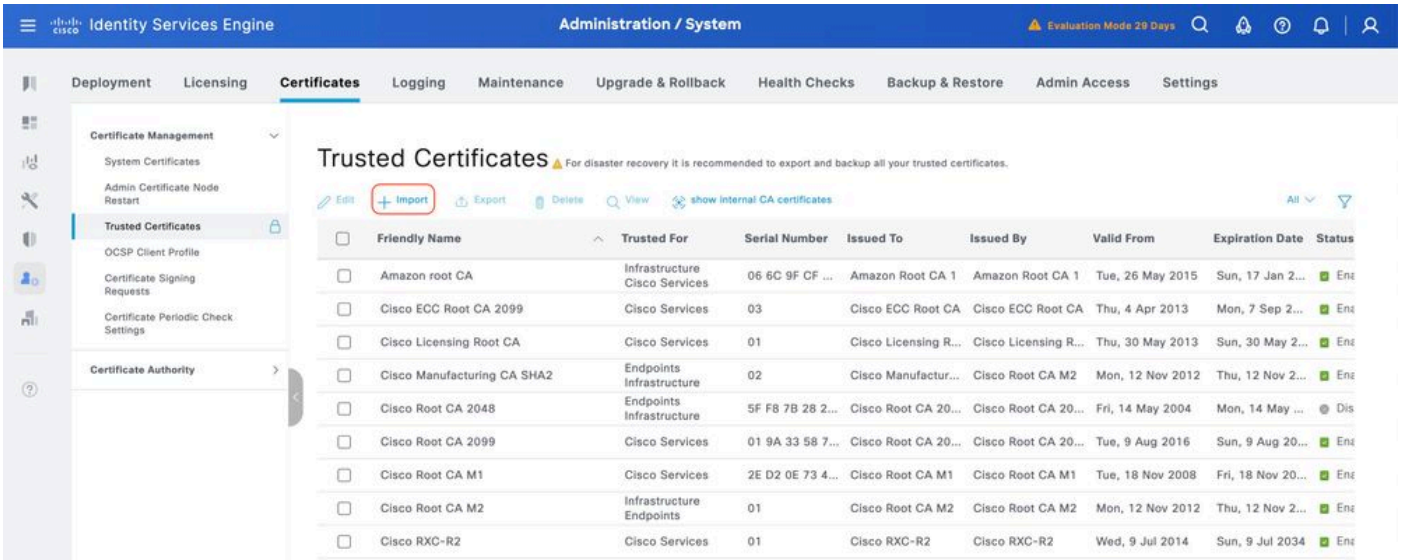
步骤8.单击Generate，然后单击Export。



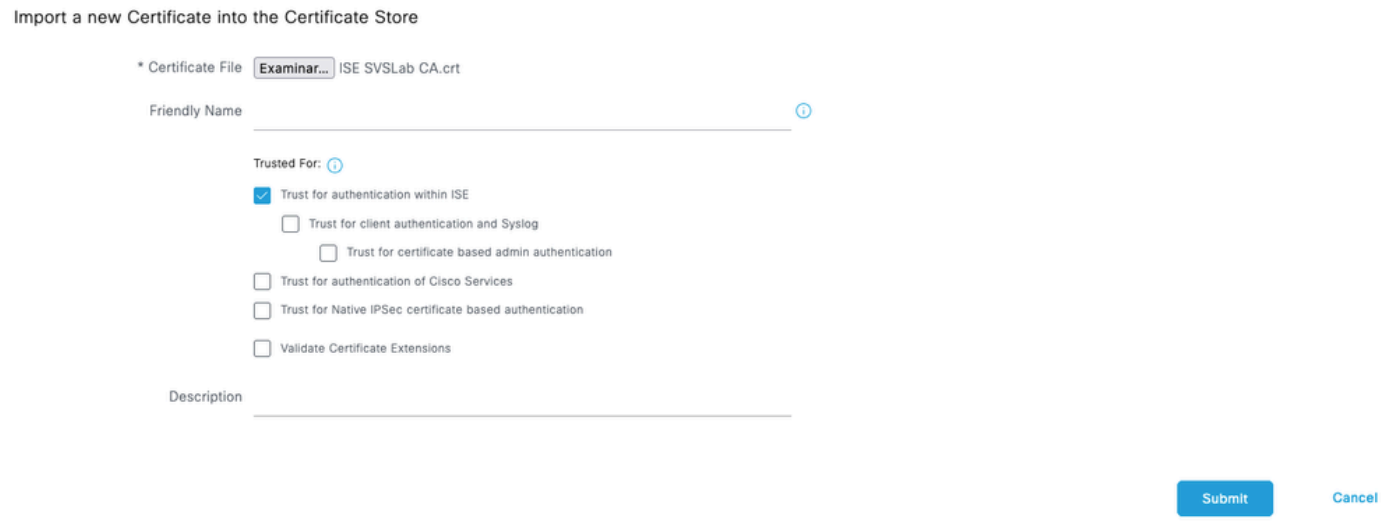
现在，您可以让证书颁发机构(CA)签署证书(CRT)。

上传用于TACACS+服务器身份验证的根CA证书

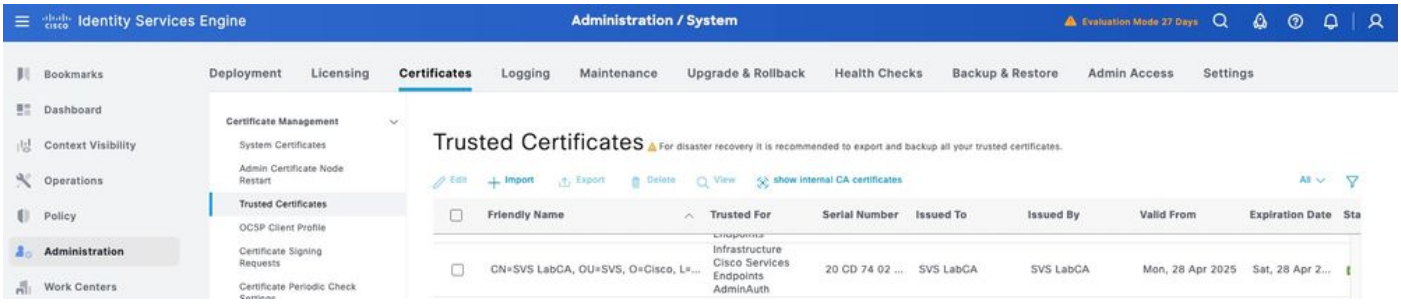
步骤1.导航到管理>系统>证书。在Trusted Certificates下，单击Import。



第2步：选择证书颁发机构(CA)颁发的证书，该证书颁发机构对您的TACACS证书签名请求(CSR)签名。 确保信任ISE内的身份验证 选项已启用。



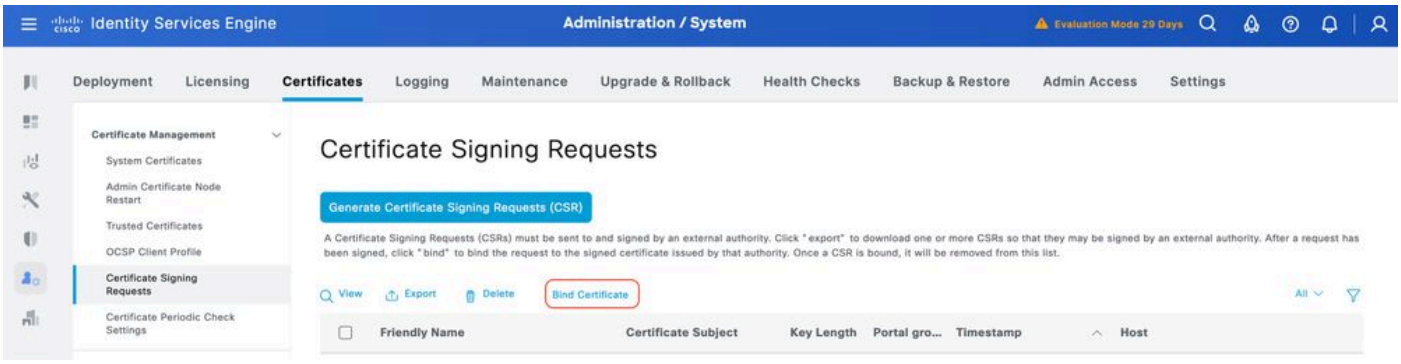
步骤3.单击Submit。证书现在必须出现在Trusted Certificates下。



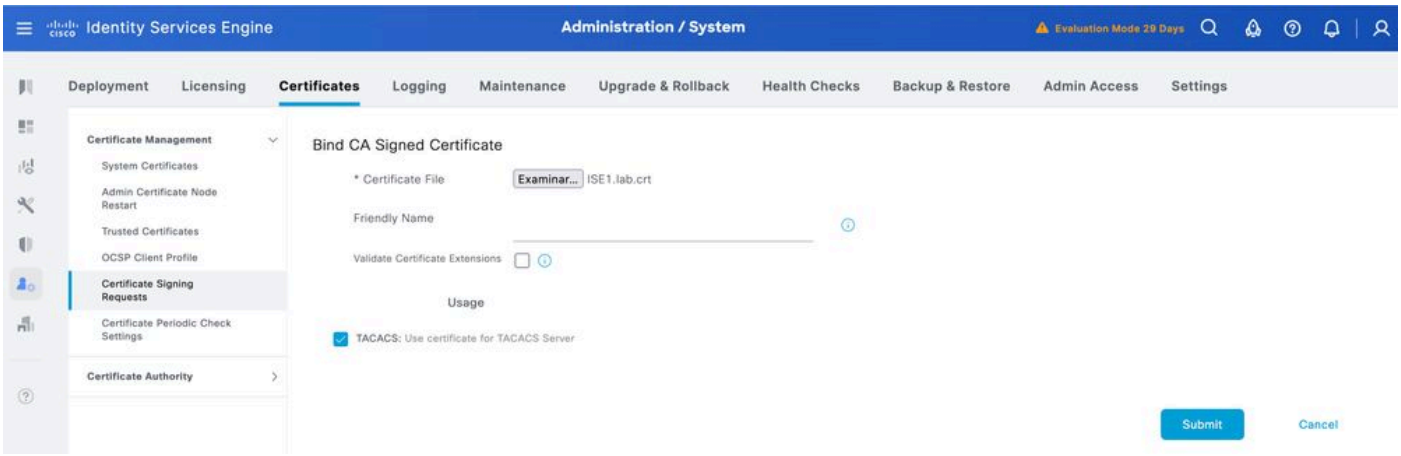
将签名证书签名请求(CSR)绑定到ISE

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。

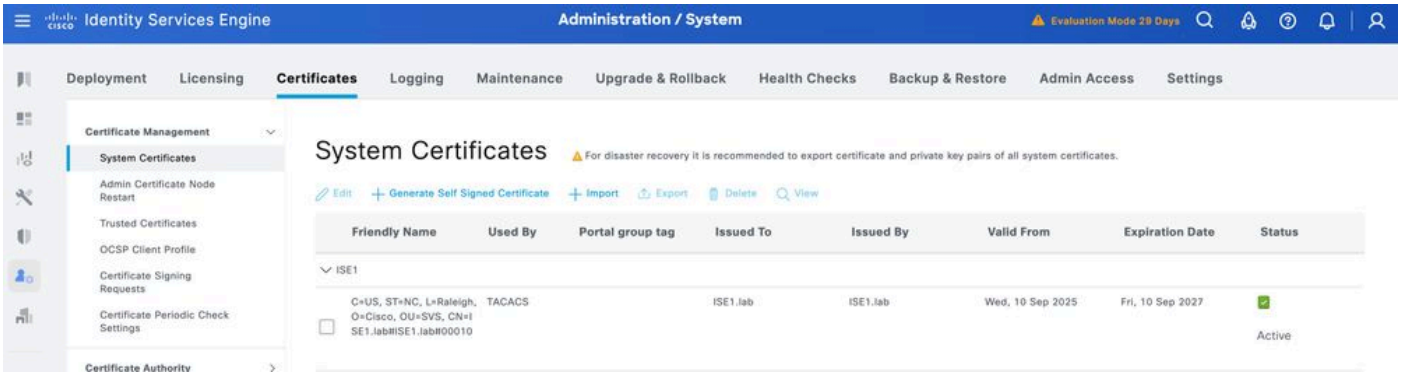


第2步：选择签名证书，并确保使用下的TACACS复选框保持选中。



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。

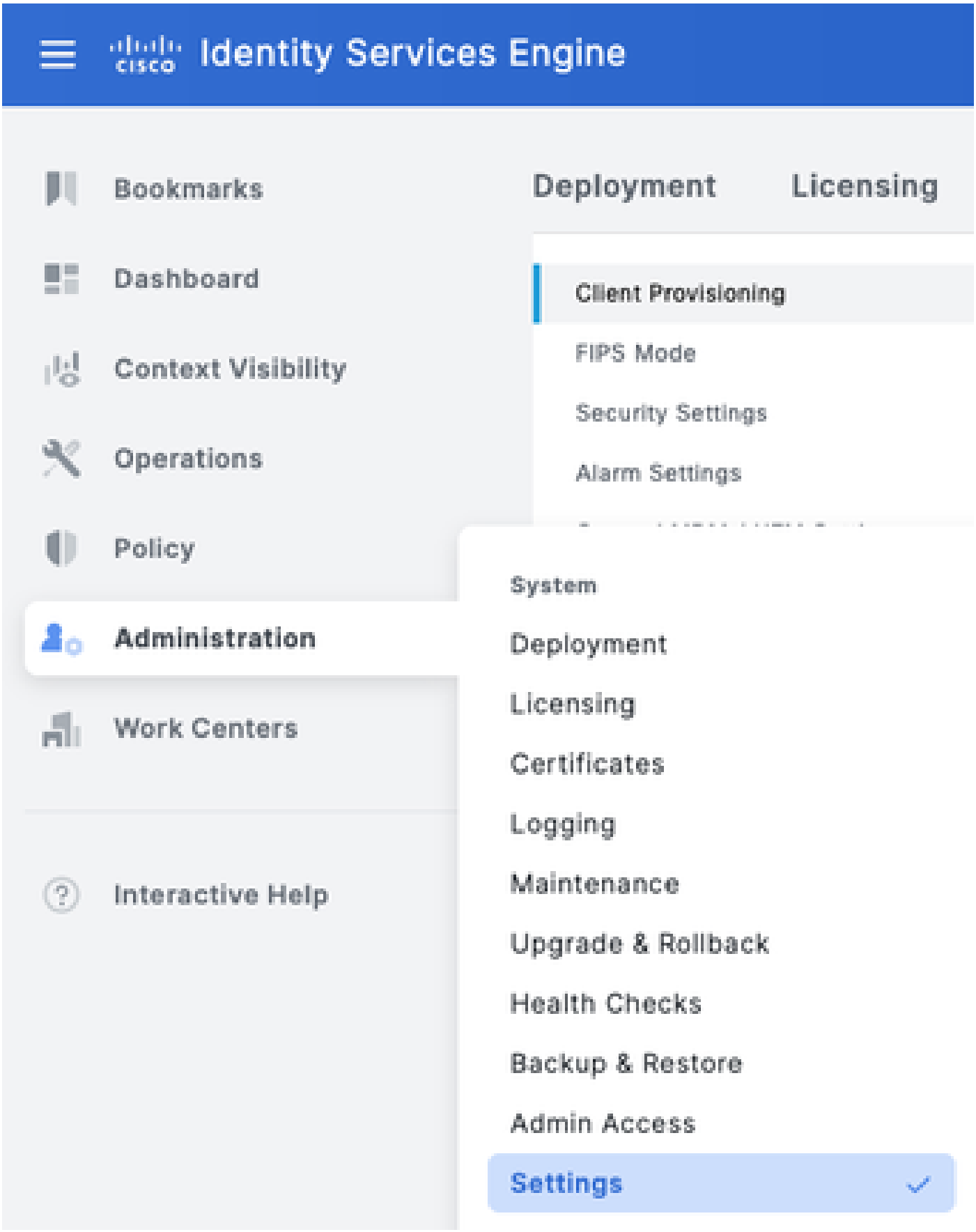
现在必须正确安装证书。您可以在System Certificates下验证这一点。



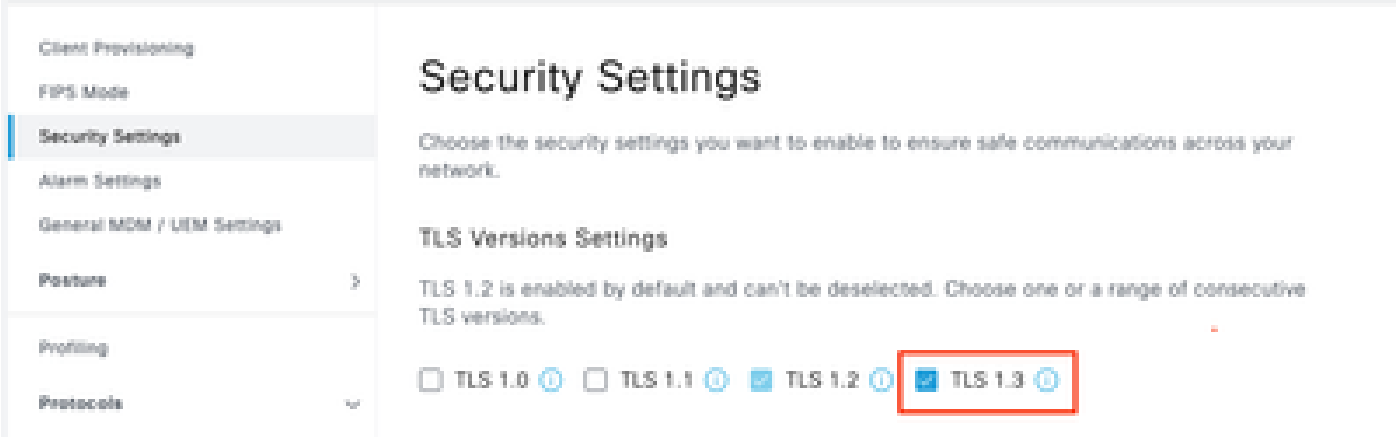
启用TLS 1.3

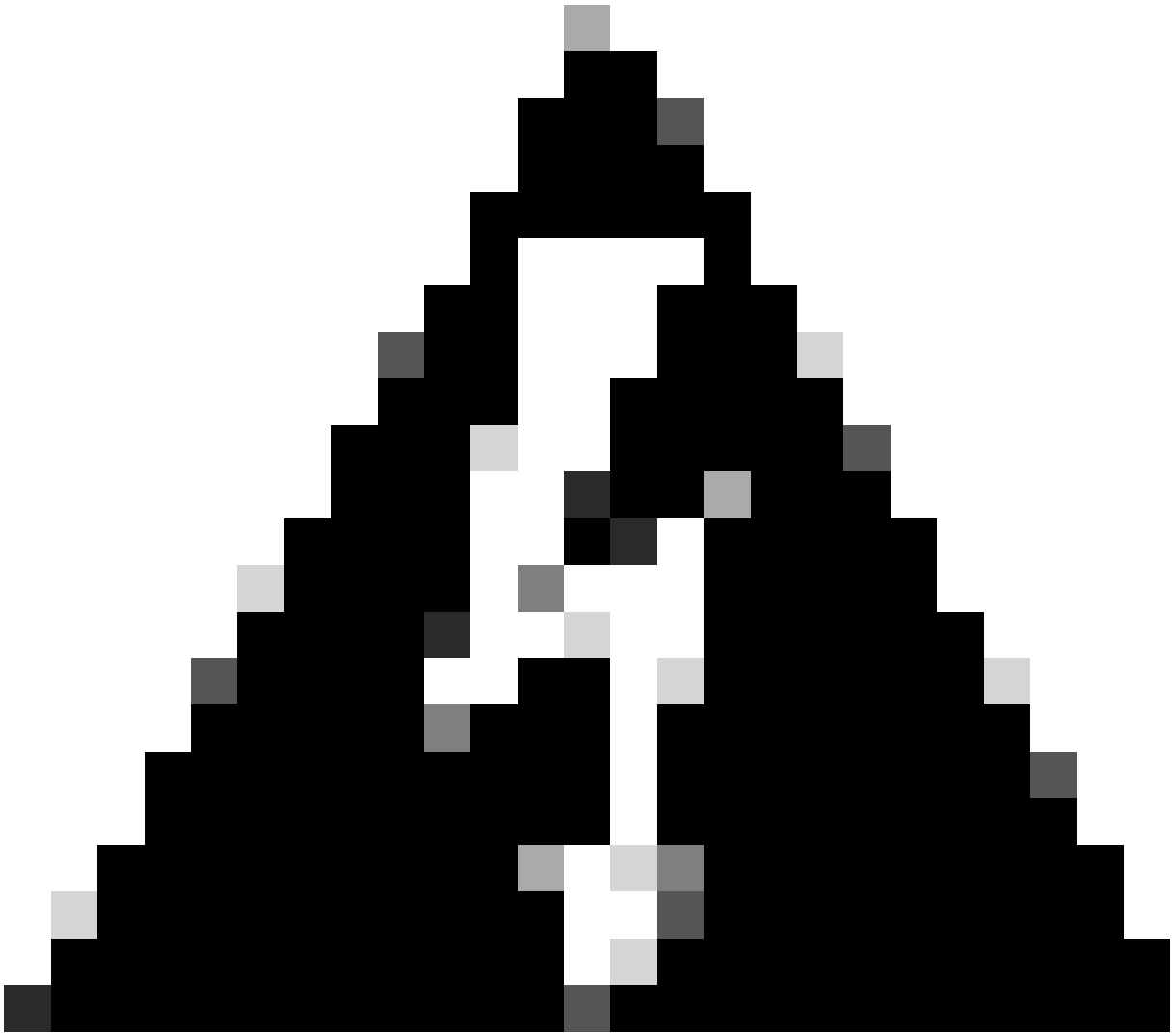
默认情况下，TLS 1.3在ISE 3.4.x中未启用。必须手动启用它。

第1步：导航到Administration > System > Settings。



第2步：单击Security Settings，在TLS Version Settings下选中TLS1.3 旁的复选框，然后单击Save。



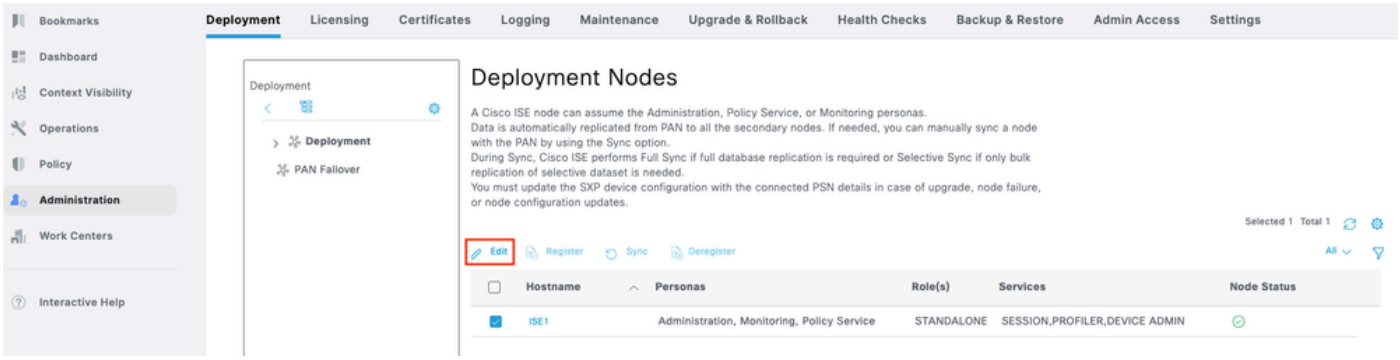


警告：当您更改TLS版本时，思科ISE应用服务器在所有思科ISE部署计算机上重新启动。

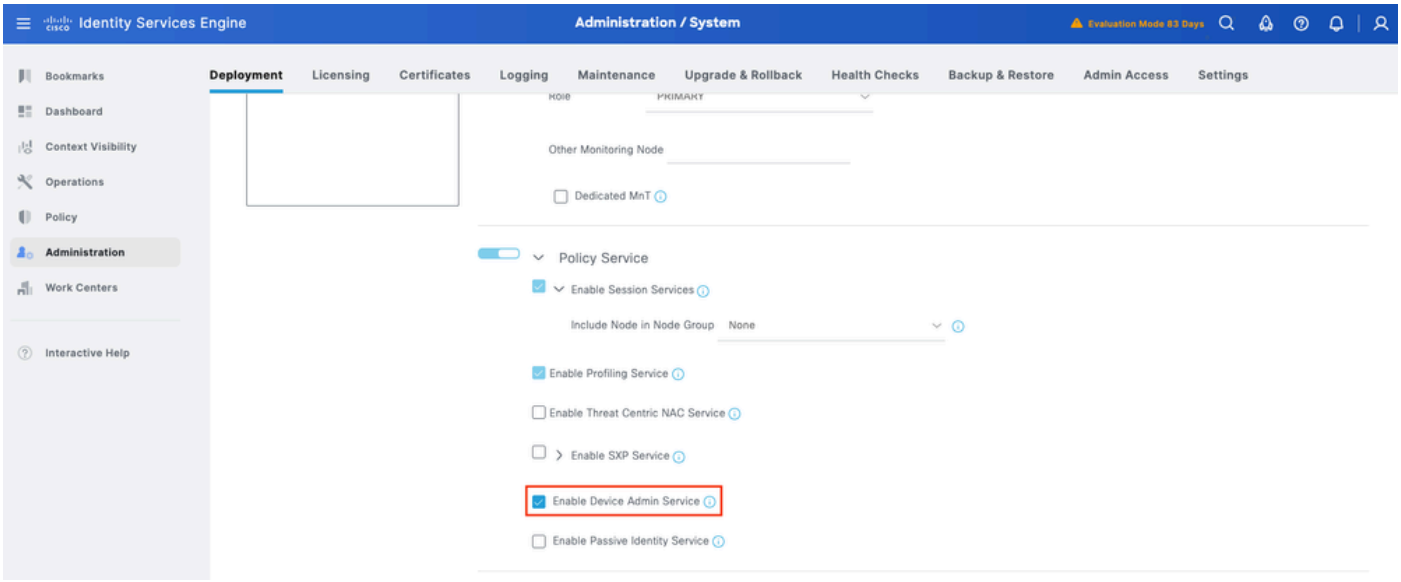
在ISE上启用设备管理

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

第1步：导航到Administration > System > Deployment。选中ISE节点旁边的复选框，然后点击Edit。



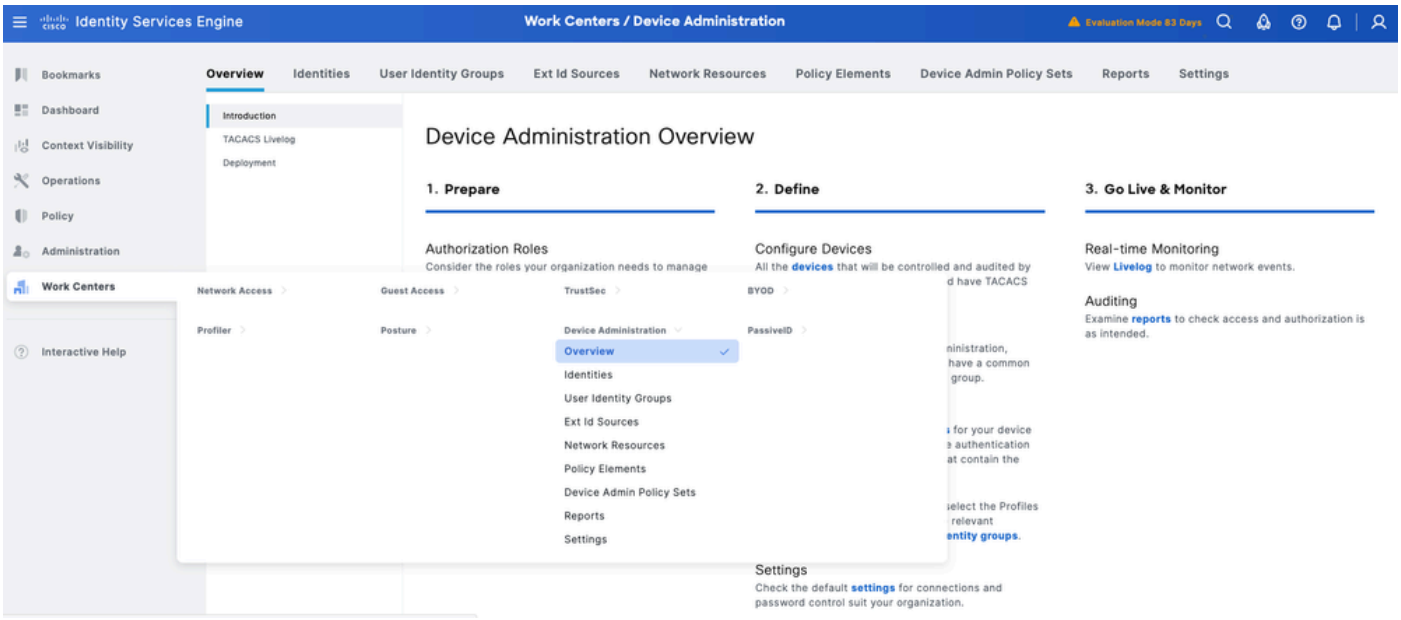
第2步：在GeneralSettings下，向下滚动并选中Enable Device Admin Service旁边的复选框。



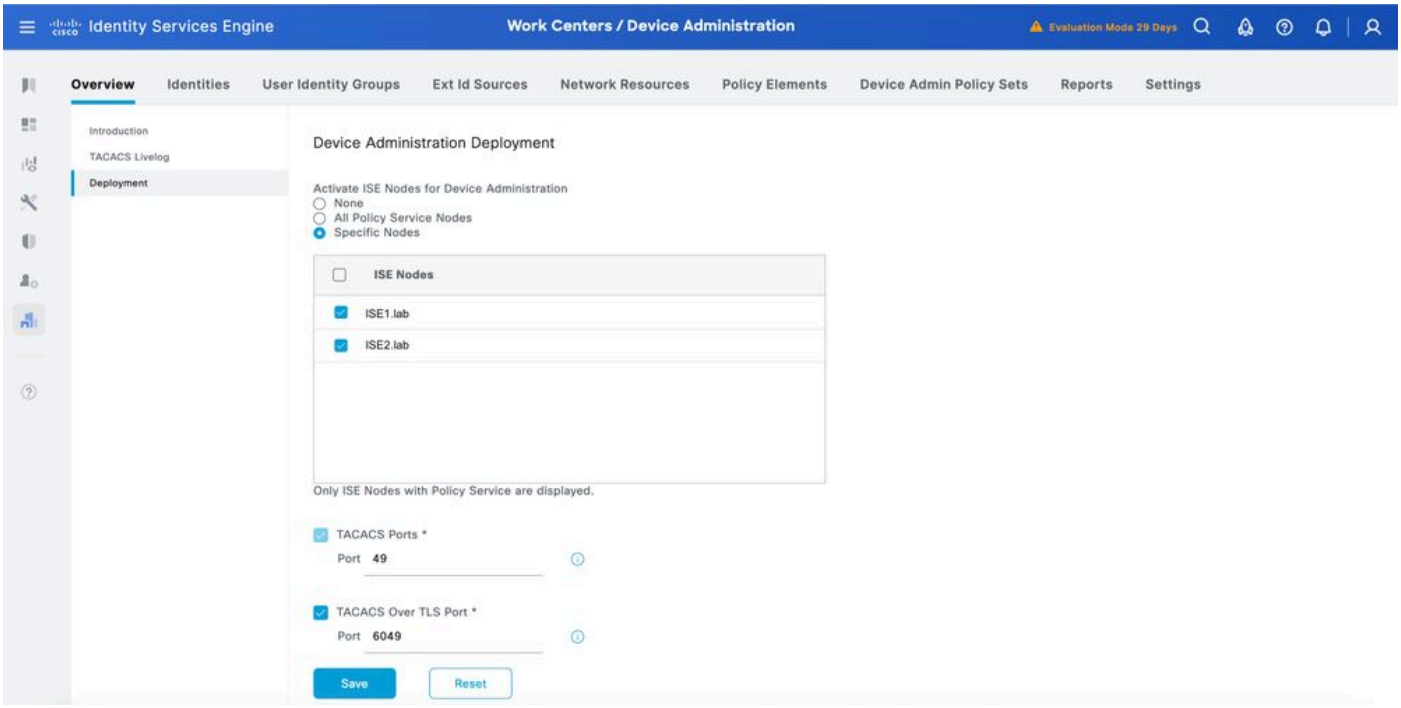
步骤3.保存配置。设备管理服务现在在ISE上启用。

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。

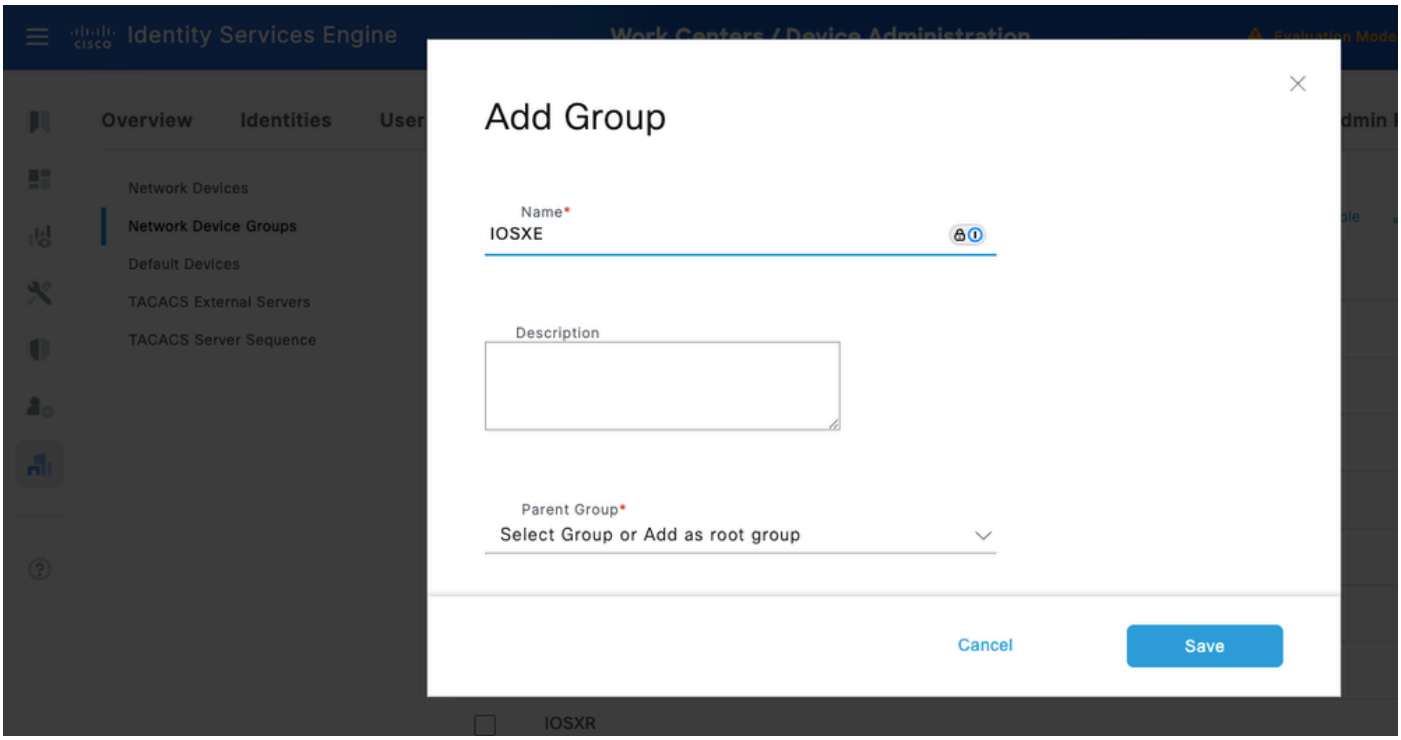


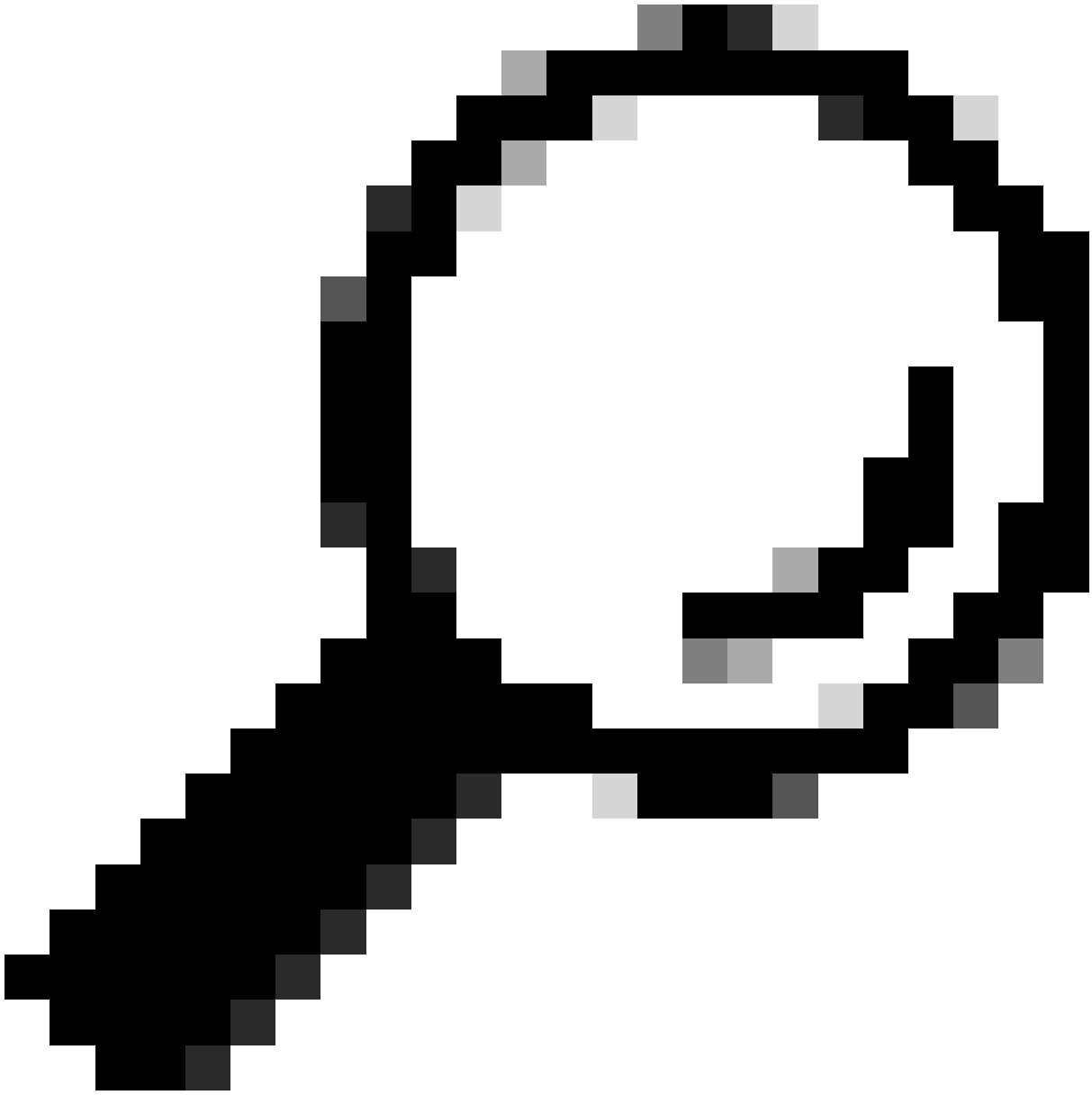
步骤3.保留默认端口6049或为TLS上的TACACS指定不同的TCP端口，然后单击Save。

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。

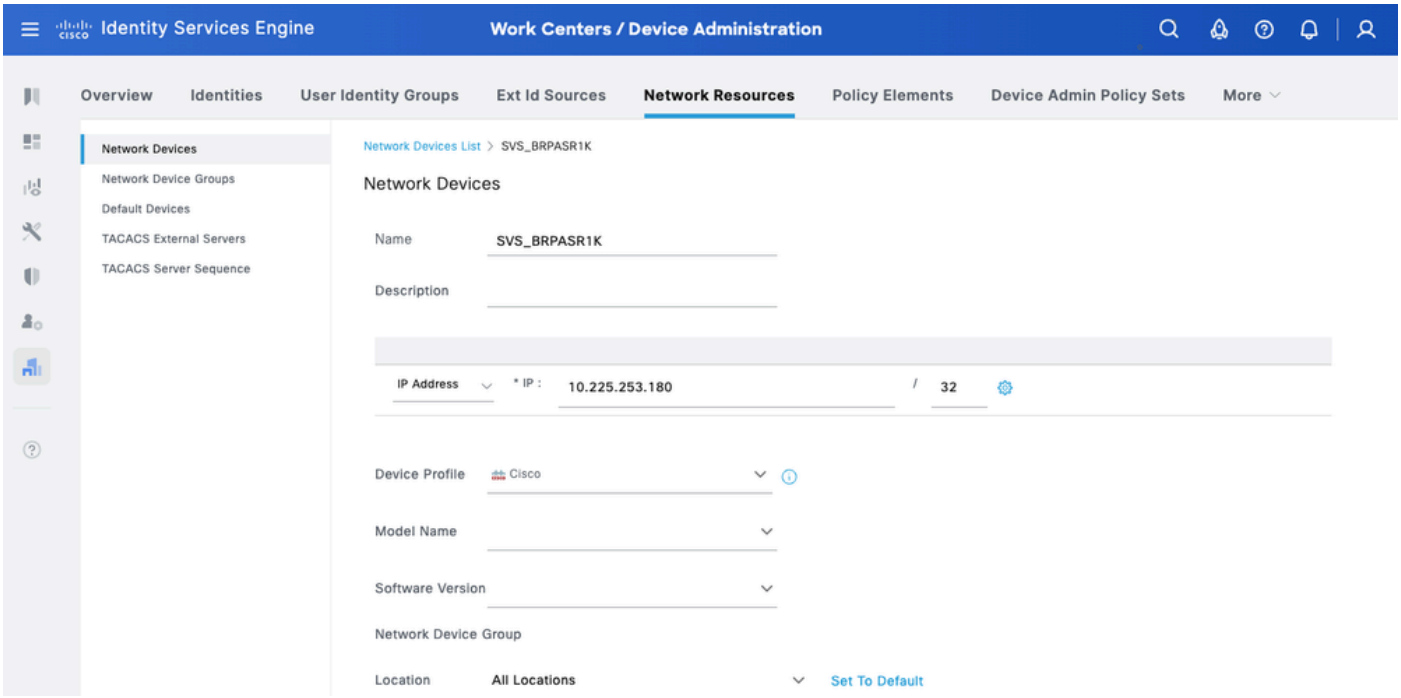
步骤1.导航到工作中心>设备管理>网络资源。单击网络设备组，创建名称为IOS XE的组。


Identity Services Engine
Overview
Identities
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Add Group
Name*
IOSXE
Description
Parent Group*
Select Group or Add as root group
Cancel
Save
IOSXR

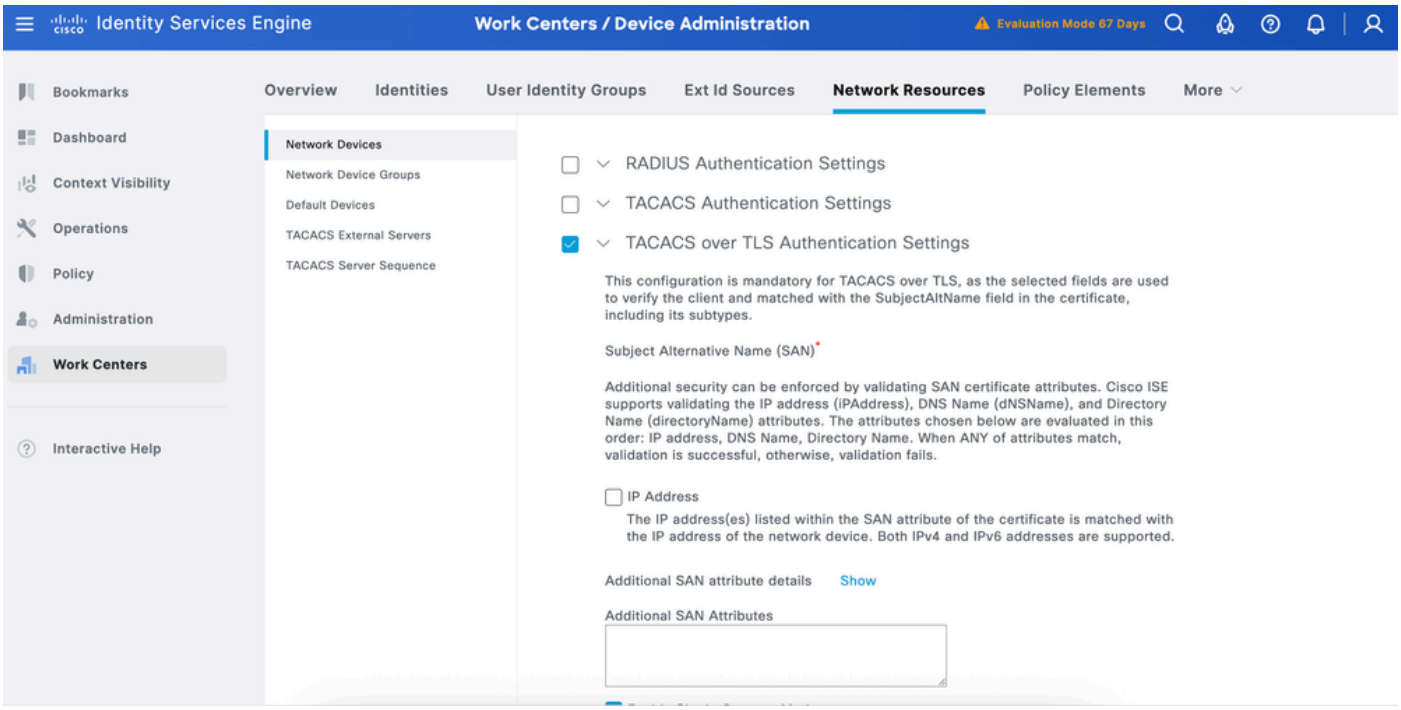


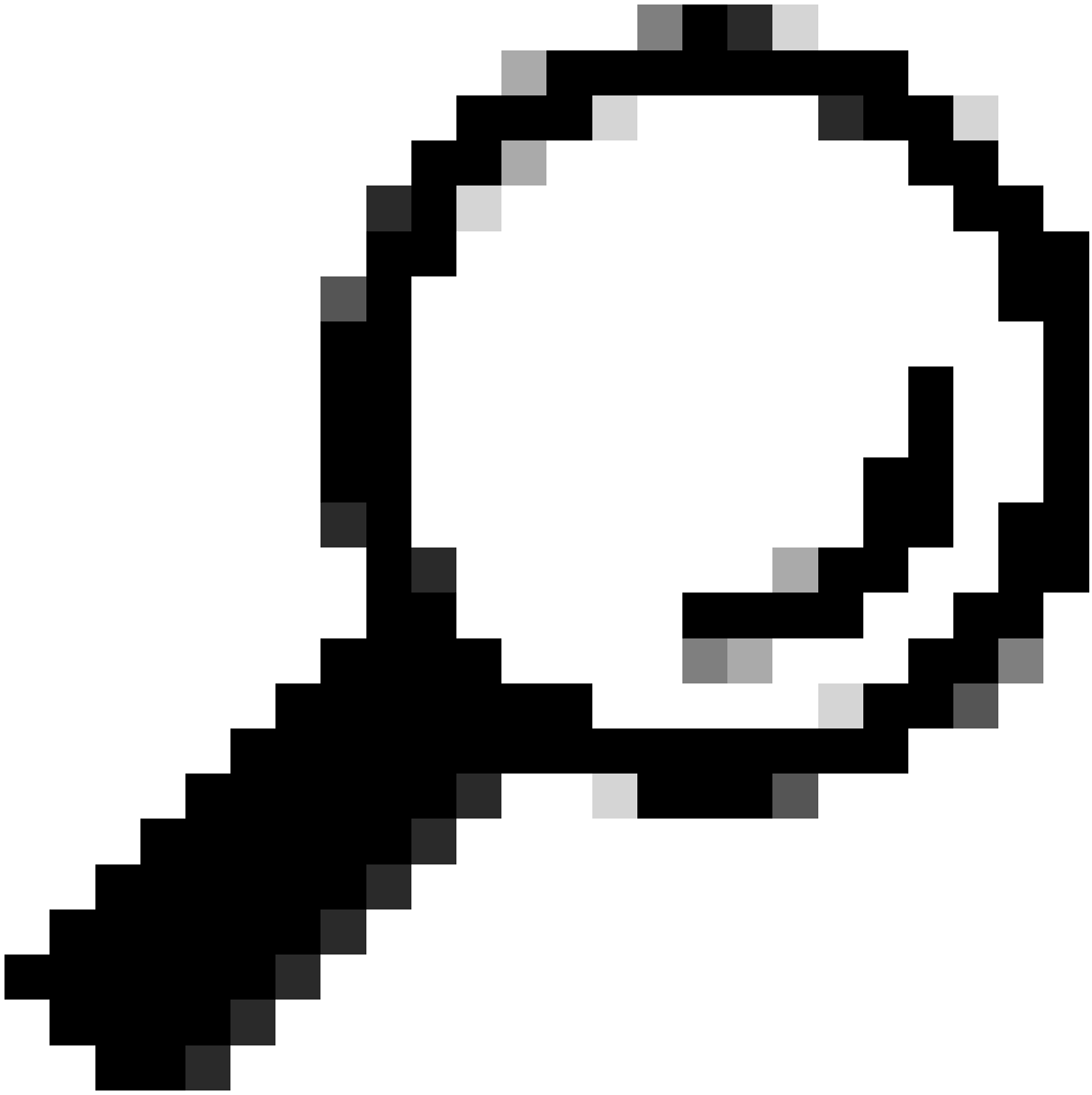
提示：所有设备类型和所有位置是ISE提供的默认层次结构。您可以添加自己的层次结构并定义识别网络设备中的各种组件，稍后可以在“策略条件”中使用

第2步：现在添加Cisco IOS XE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。对于此测试，它是SVS_BRPASR1K。



第3步：输入设备的IP地址，并确保映射设备的位置和设备类型(IOS XE)。最后，启用基于TLS身份验证设置的TACACS+。



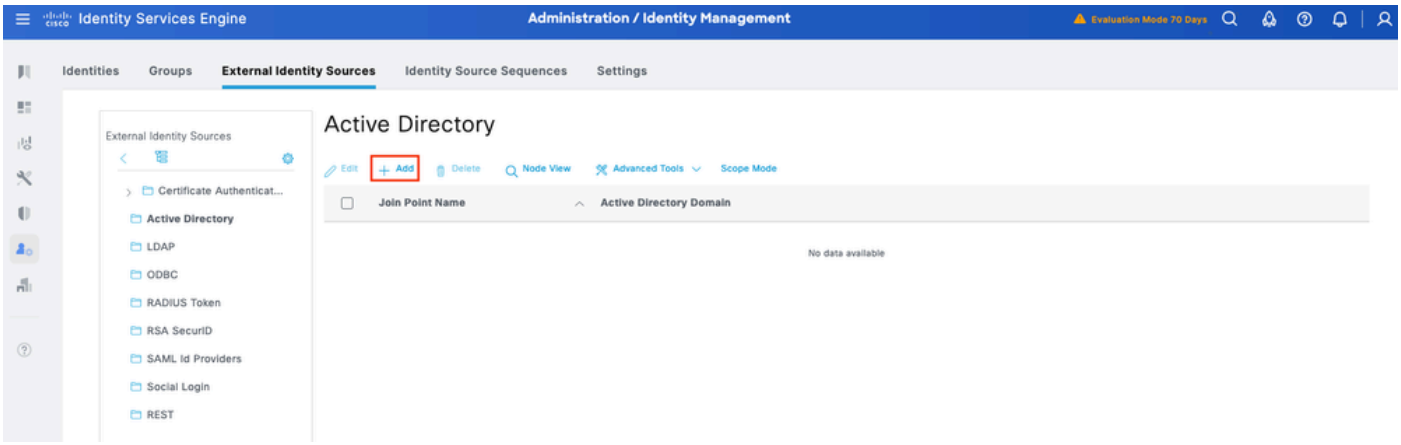


提示：建议启用单一连接模式，以避免每次向设备发送命令时重新启动TCP会话。

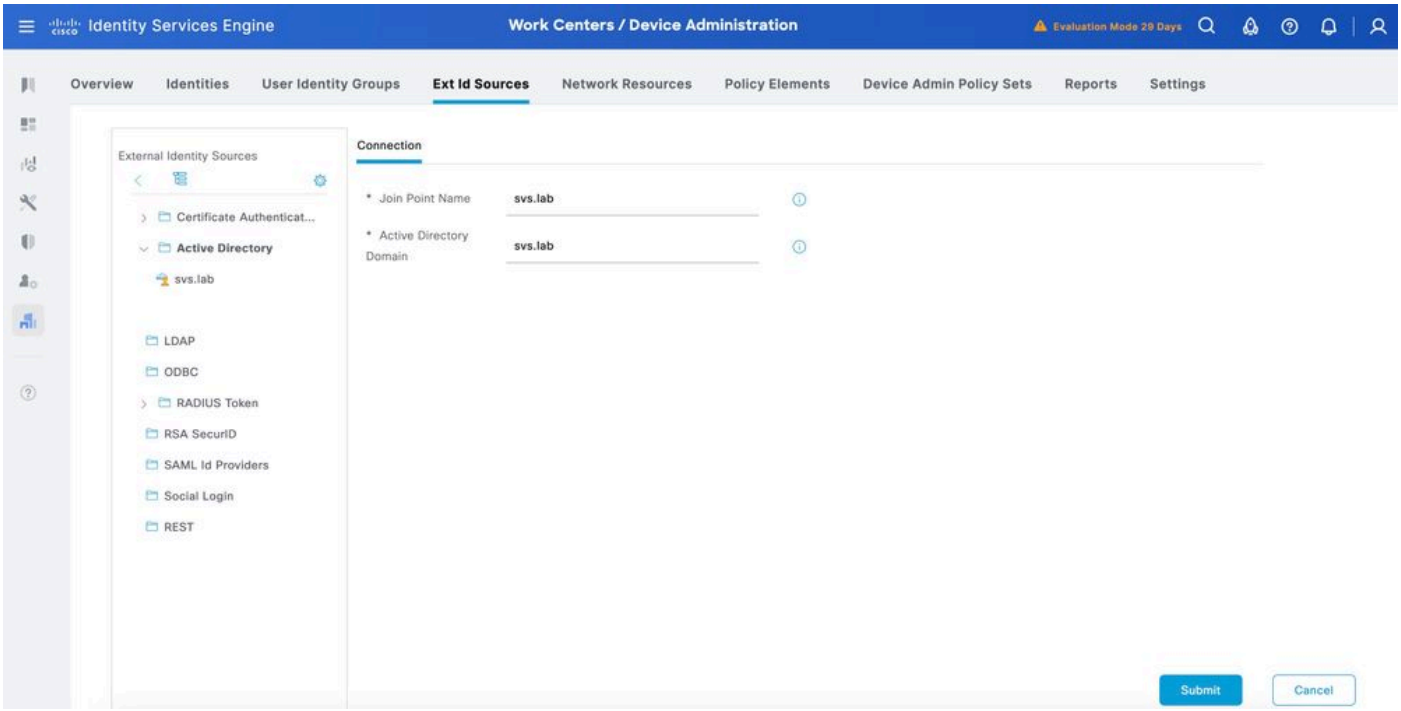
配置身份库

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)。

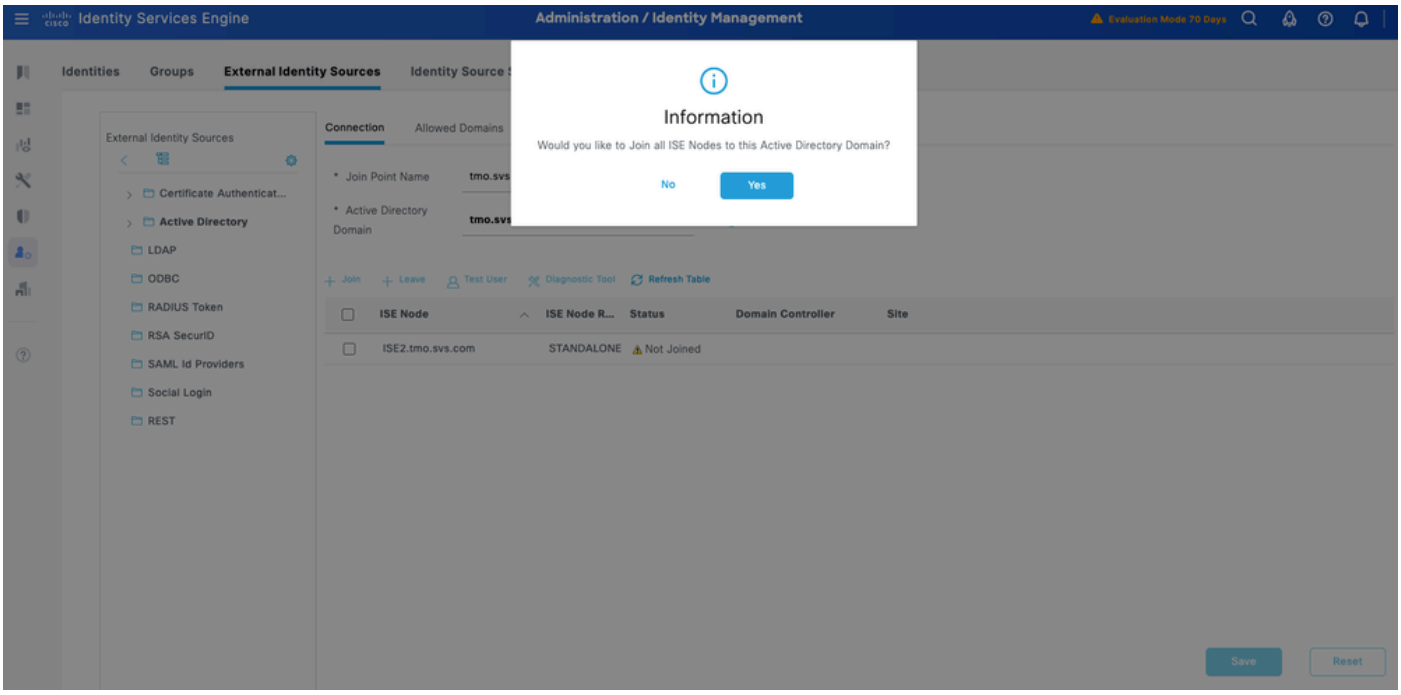
步骤1.导航到管理>身份管理>外部身份库> Active Directory。单击Add以定义新的AD接点。



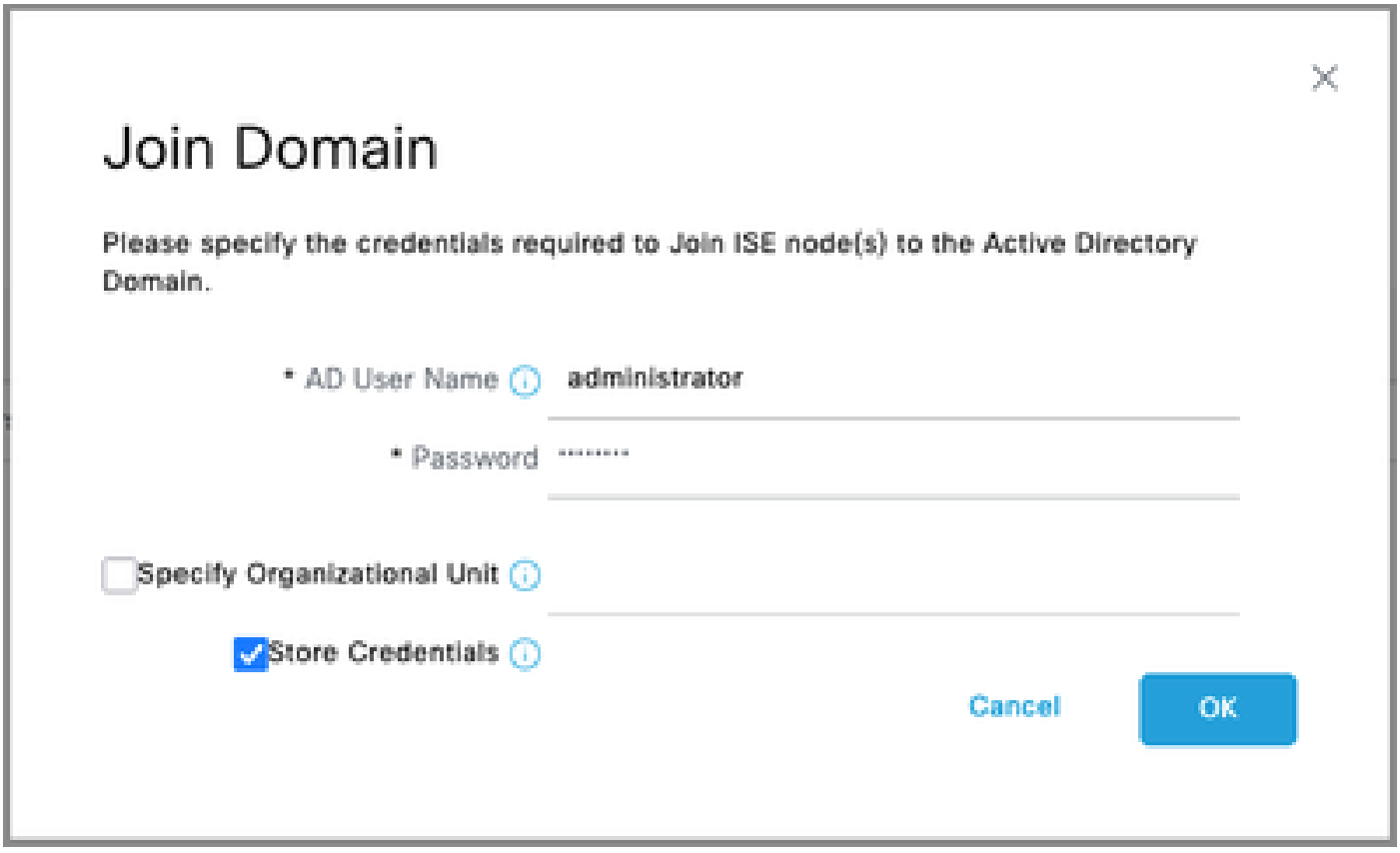
步骤2.指定加入点名称和AD域名，然后单击提交。

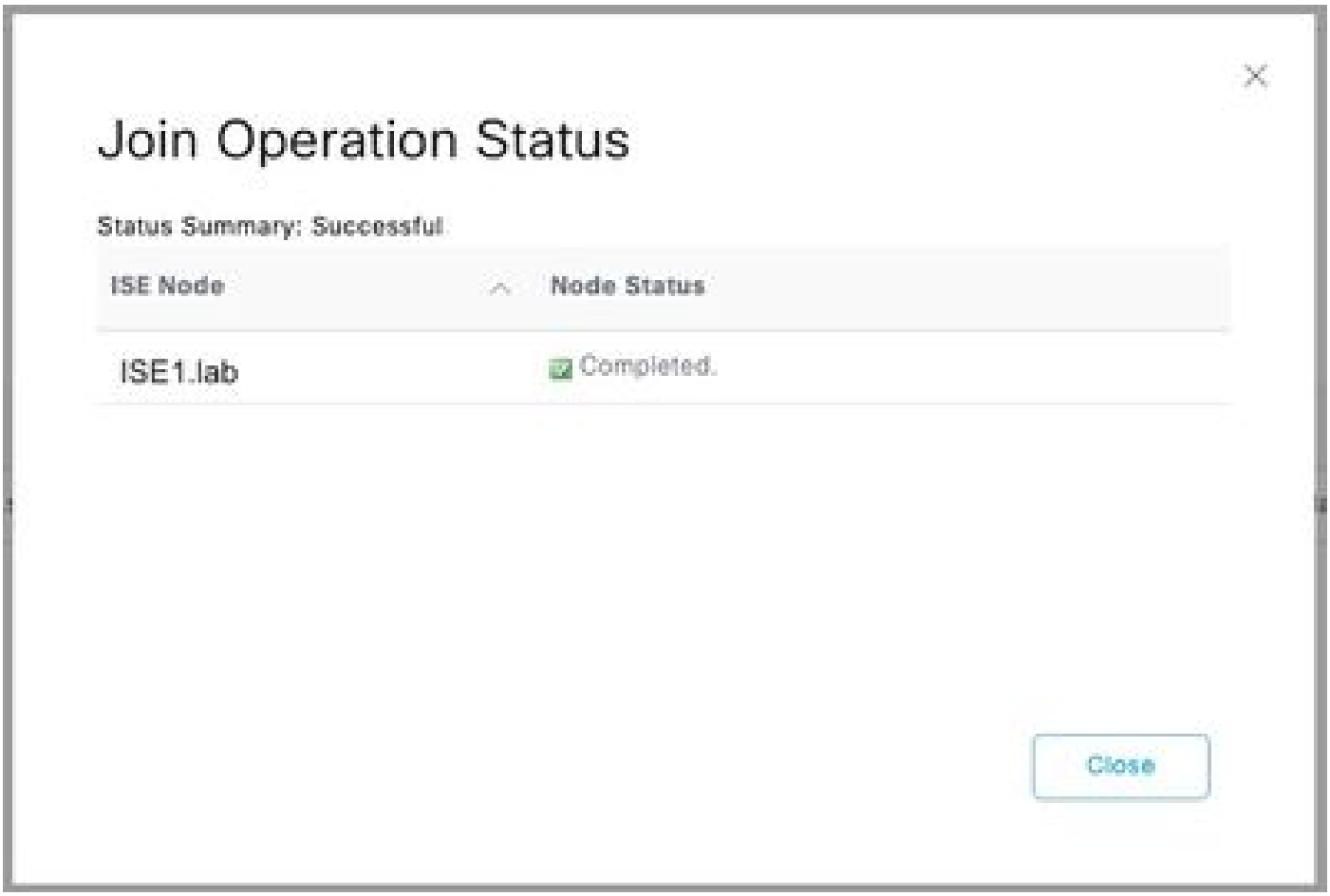


步骤3.出现提示时是否要将所有ISE节点加入此Active Directory域时，单击Yes?

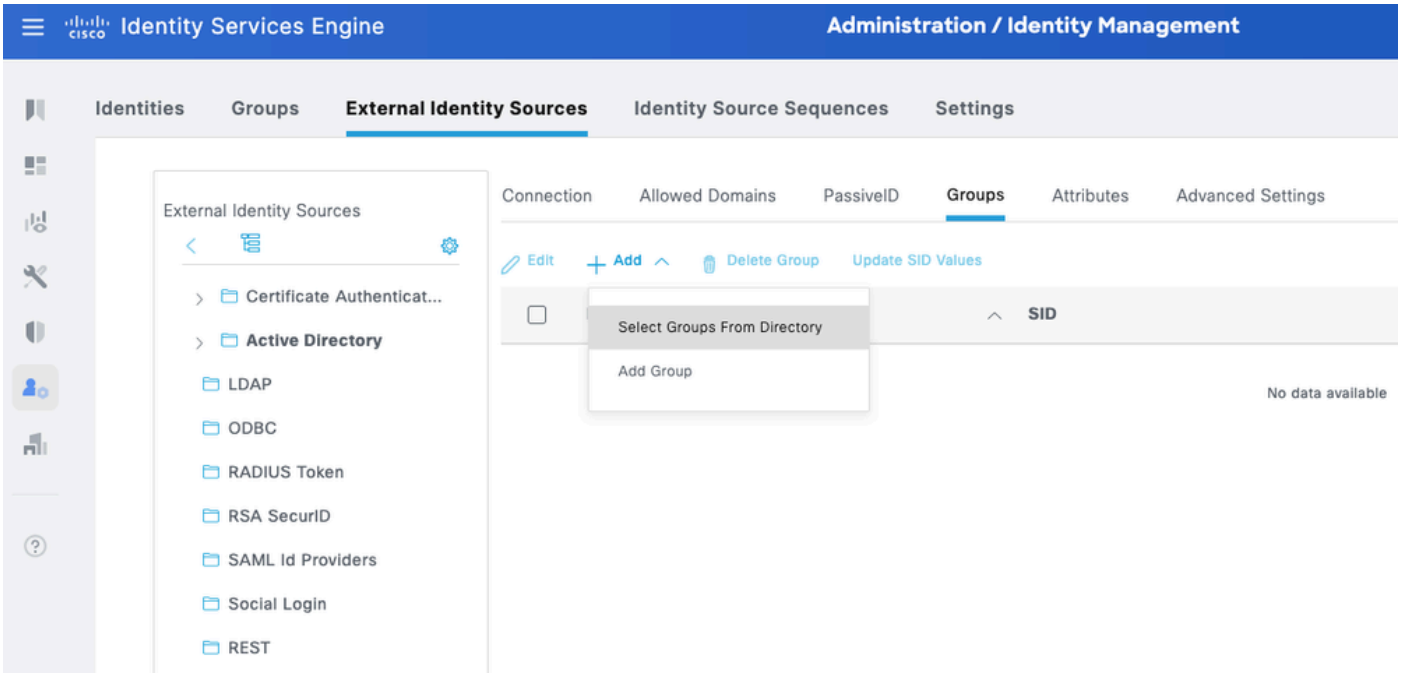


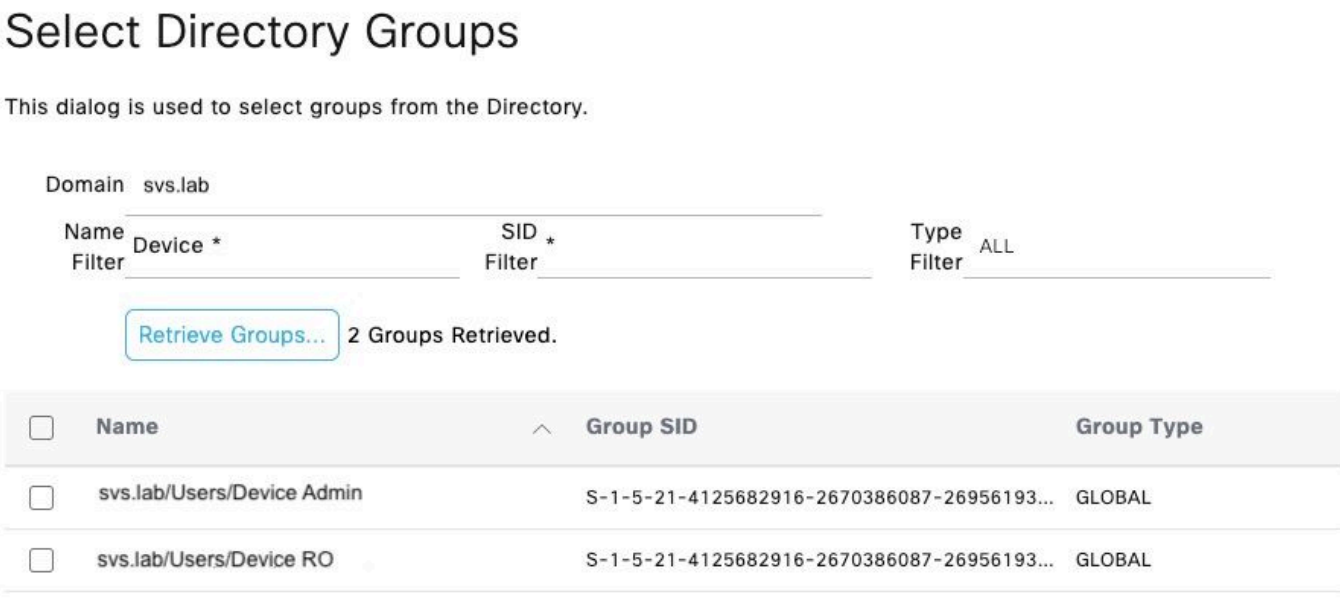
第4步：输入具有AD加入权限的凭证，并将ISE加入AD。检查状态以验证其是否正常运行。

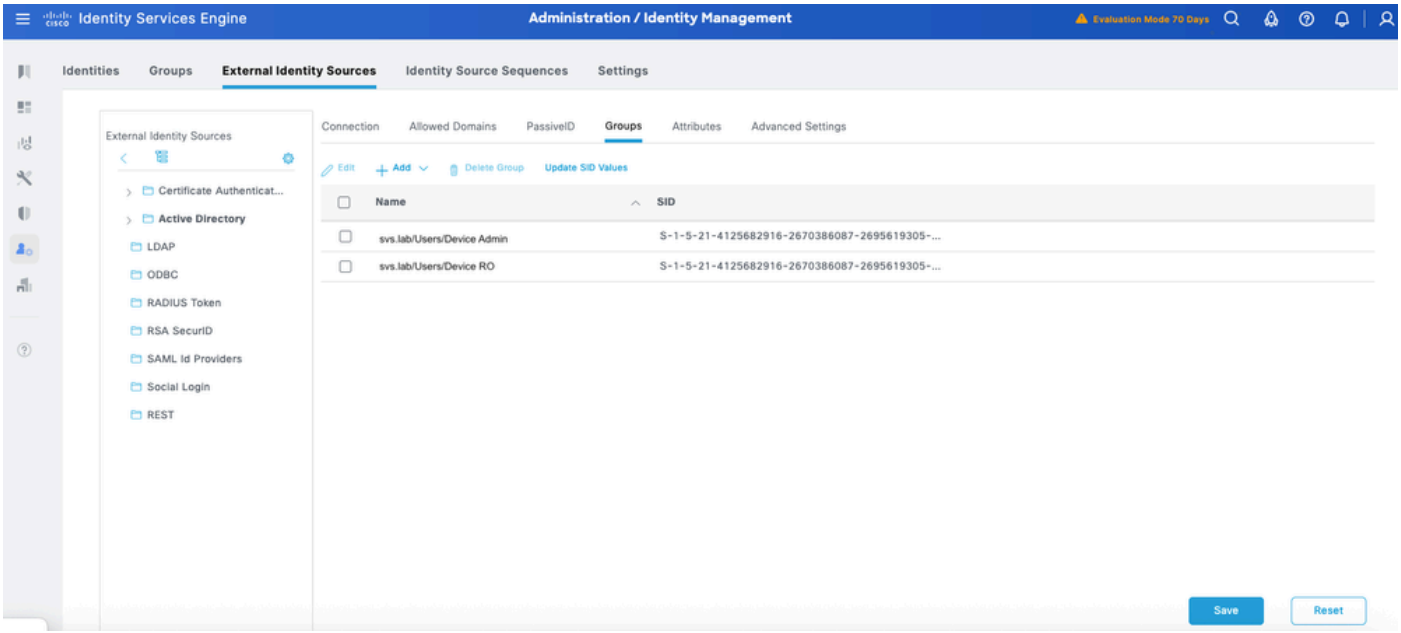




步骤5.导航到Groups选项卡，然后单击Add获取根据哪些用户有权访问设备而需要的所有组。本示例显示本指南的授权策略中使用的组







配置TACACS+配置文件

您将将TACACS+配置文件映射到Cisco IOS XE设备上的两个主要用户角色：

- 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。

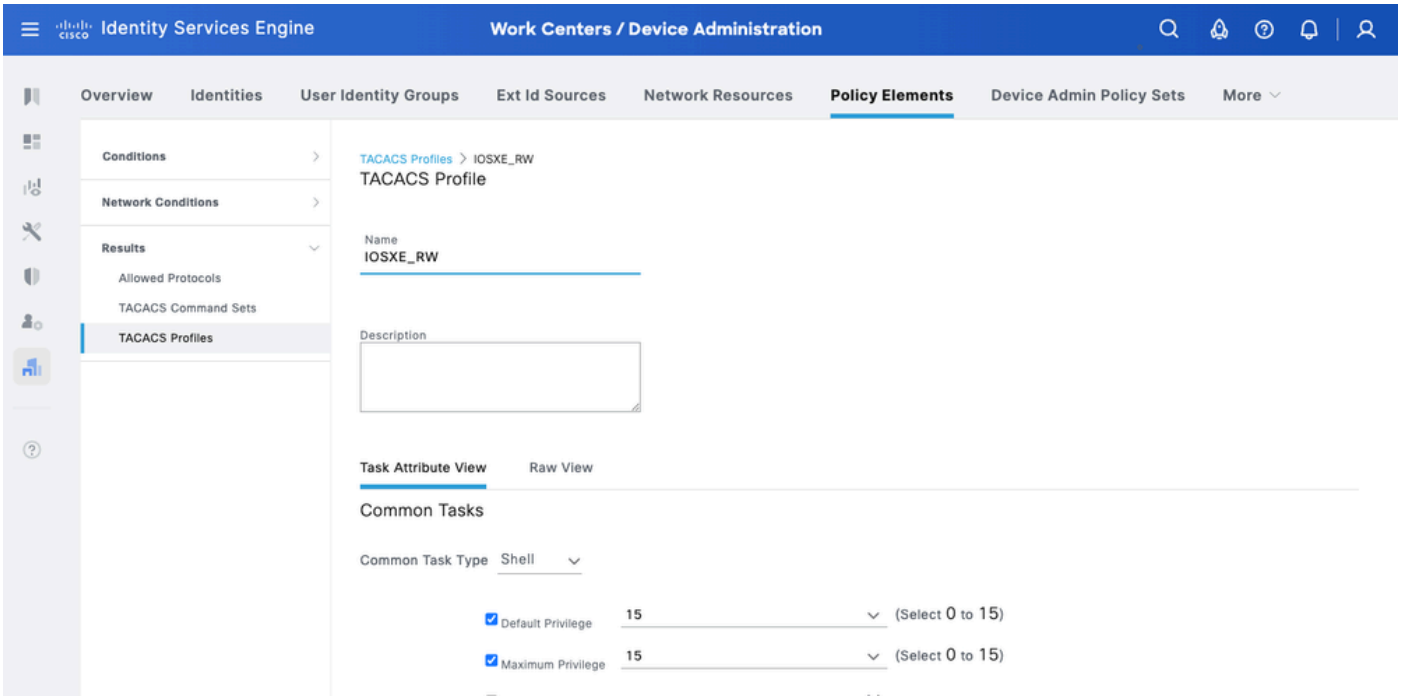
这些配置文件定义为两个TACACS+配置文件：IOS XE_RW和IOSXR_RO。

IOS XE_RW — 管理员配置文件

第1步导航到工作中心>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IOS XE_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。

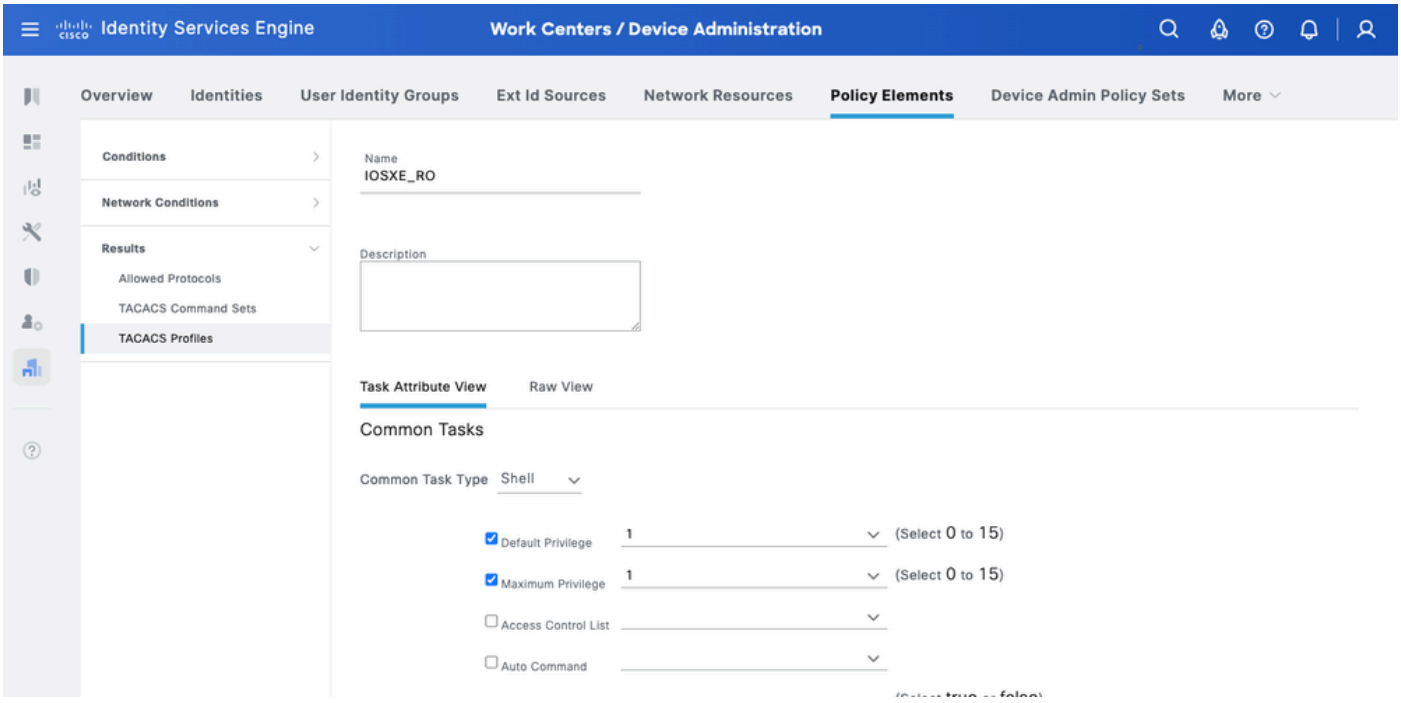


IOS XE_RO — 运营商配置文件

第1步导航到工作中心>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IOS XE_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。



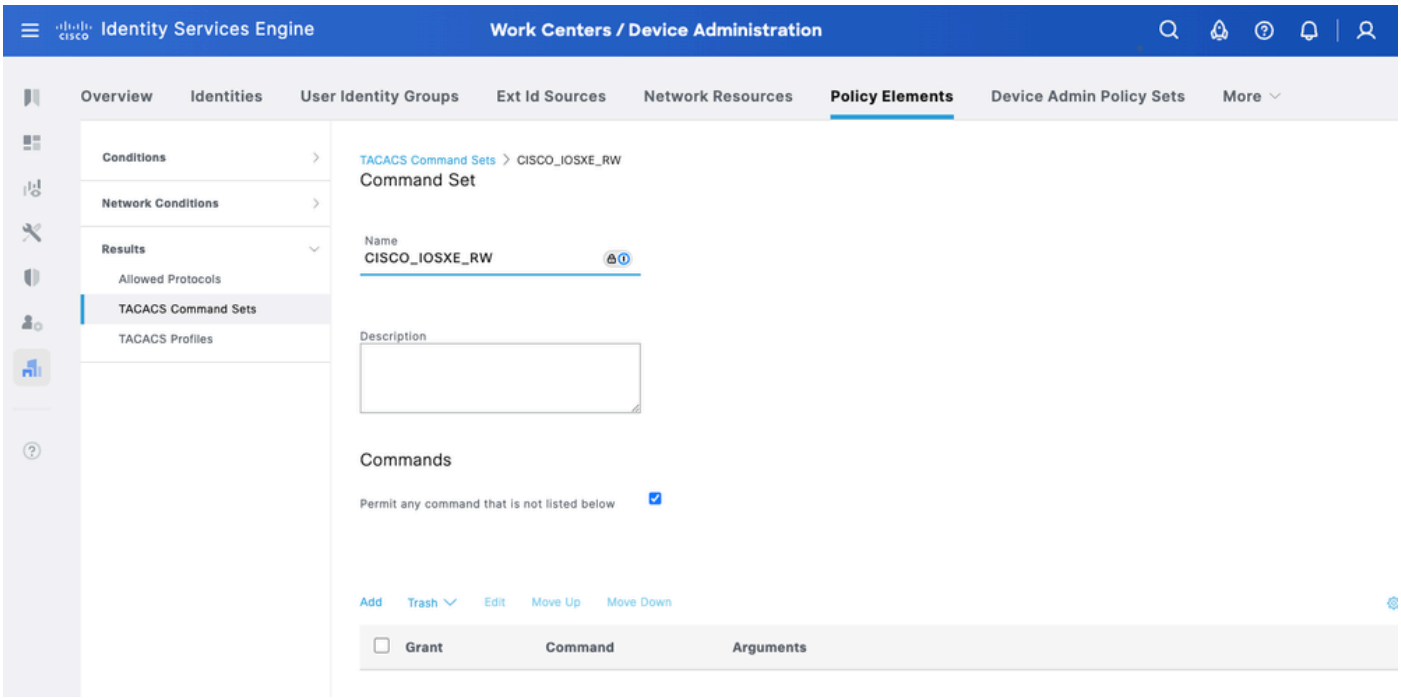
配置TACACS+命令集

以下命令集定义为两个TACACS+命令集：CISCO_IOS XE_RW和CISCO_IOS XE_RO。

CISCO_IOS XE_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_IOS XE_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。



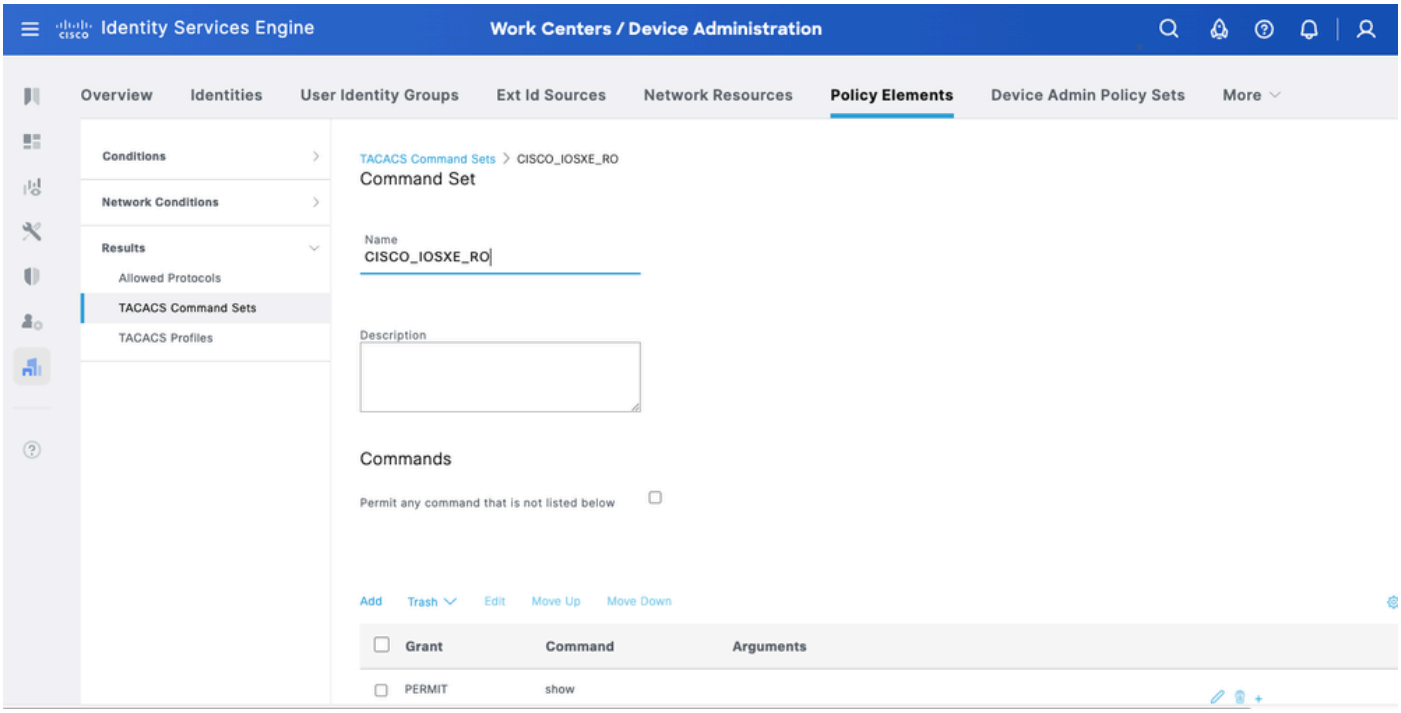
CISCO_IOS XE_RO — 运算符命令集

第1步从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_IOS XE_RO。

步骤2.在Commands部分中，添加新的命令。

步骤3.从Grant 列的下拉列表中选择Permit ，然后在Command 列中输入show ;并点击复选箭头。

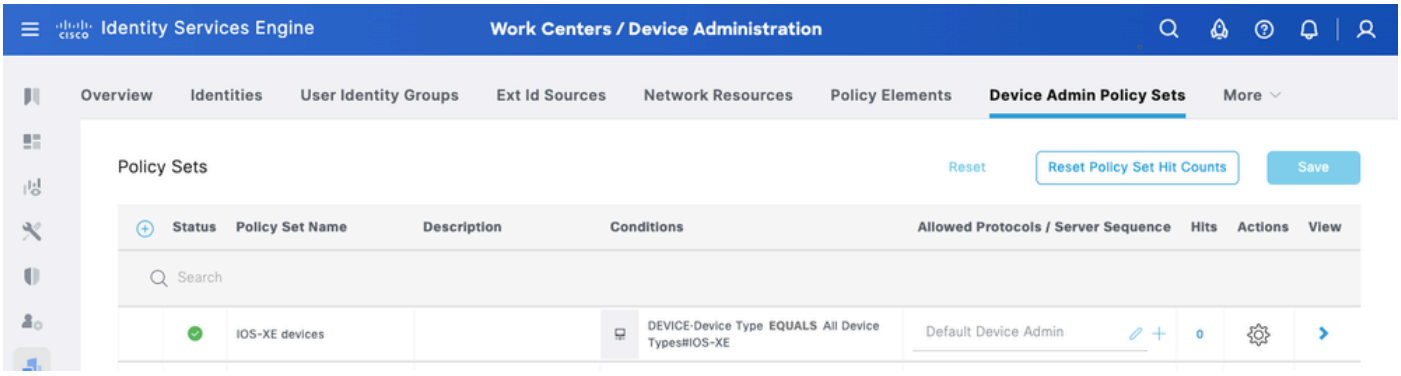
步骤4.确认数据并点击保存。



配置设备管理策略集

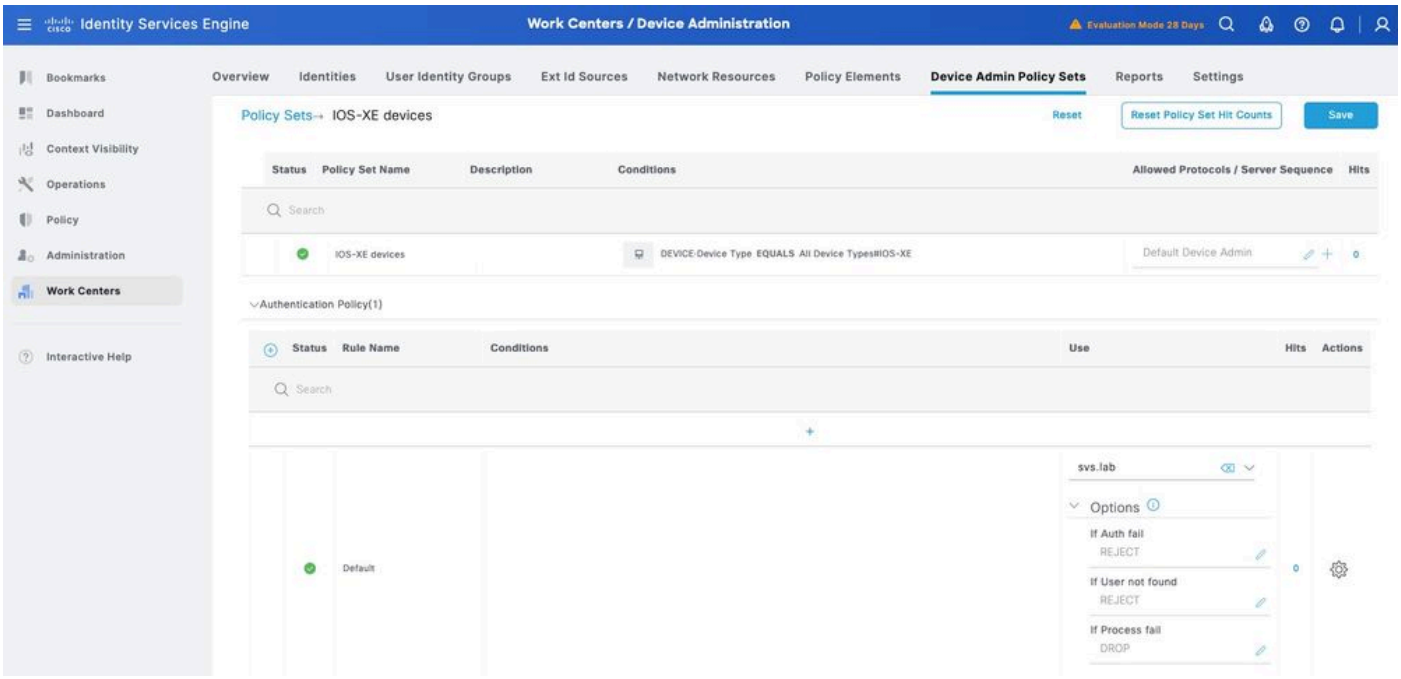
默认情况下，为设备管理启用策略集。策略集可以根据设备类型划分策略，以简化TACACS配置文件的应用。

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



步骤2.单击Save，然后单击向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。



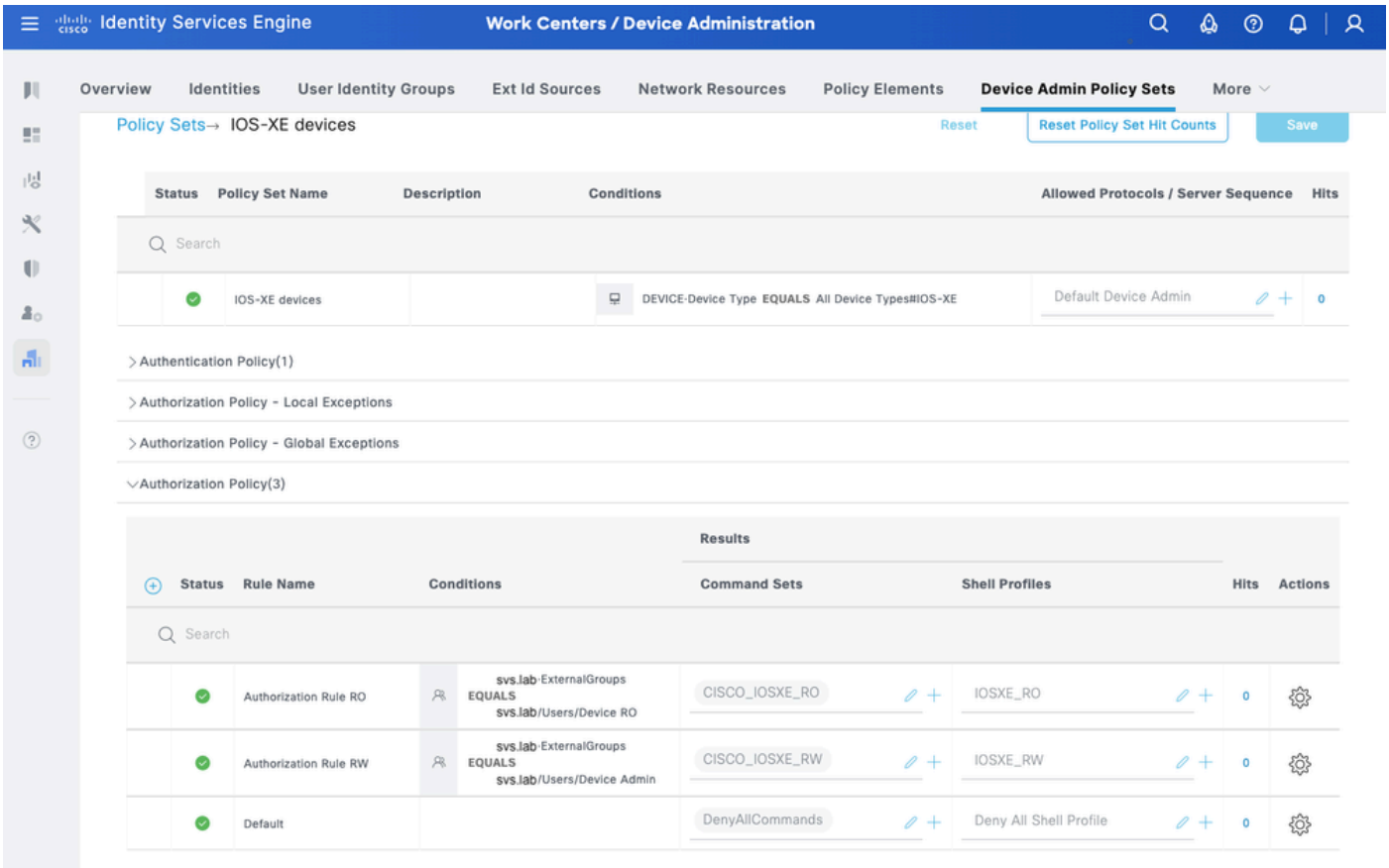
步骤4.定义授权策略。

根据Active Directory(AD)中的用户组创建授权策略。

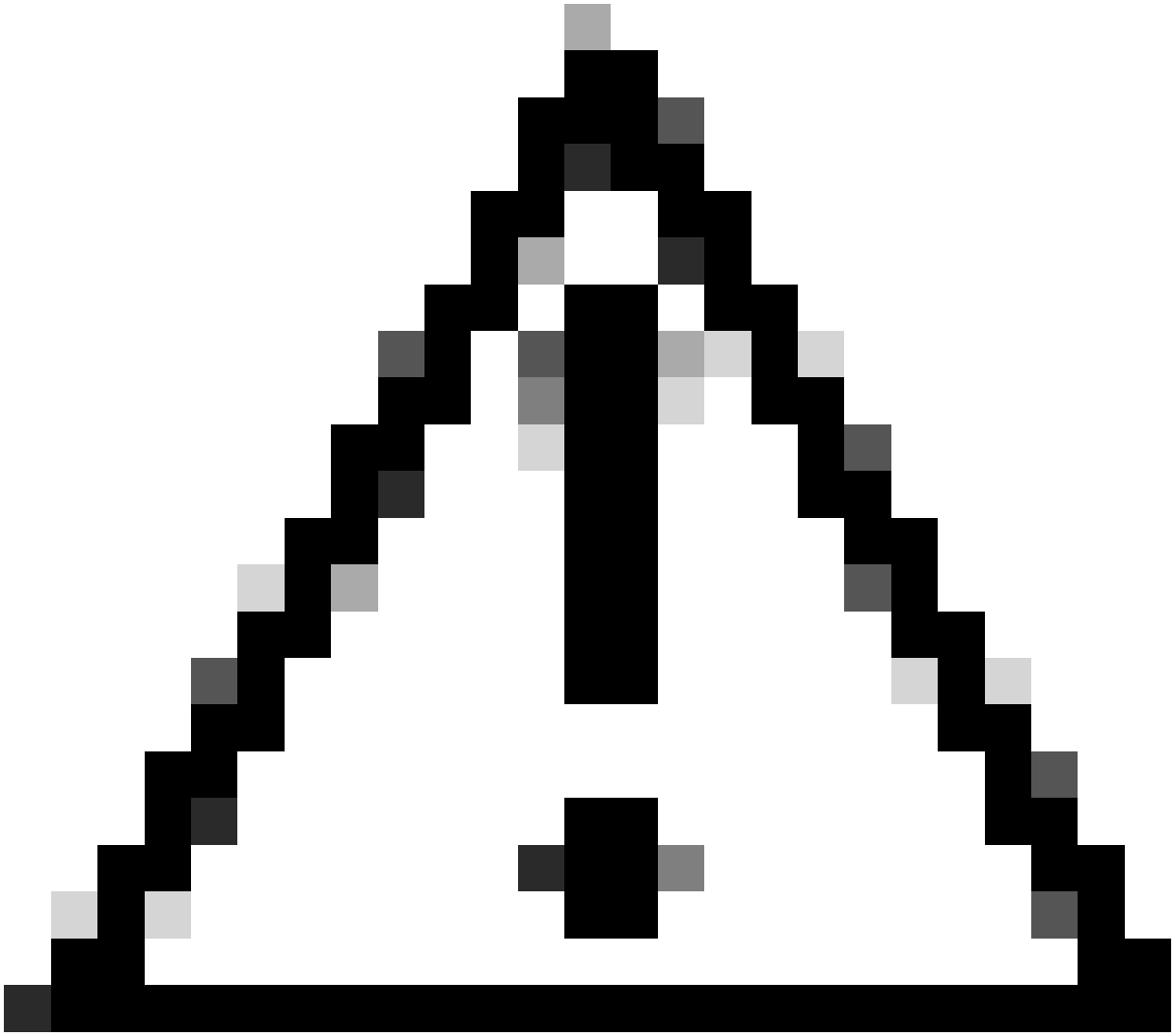
例如:

· AD组设备RO 中的用户分配有CISCO_IOSXR_RO 命令集和IOSXR_RO 外壳配置文件。

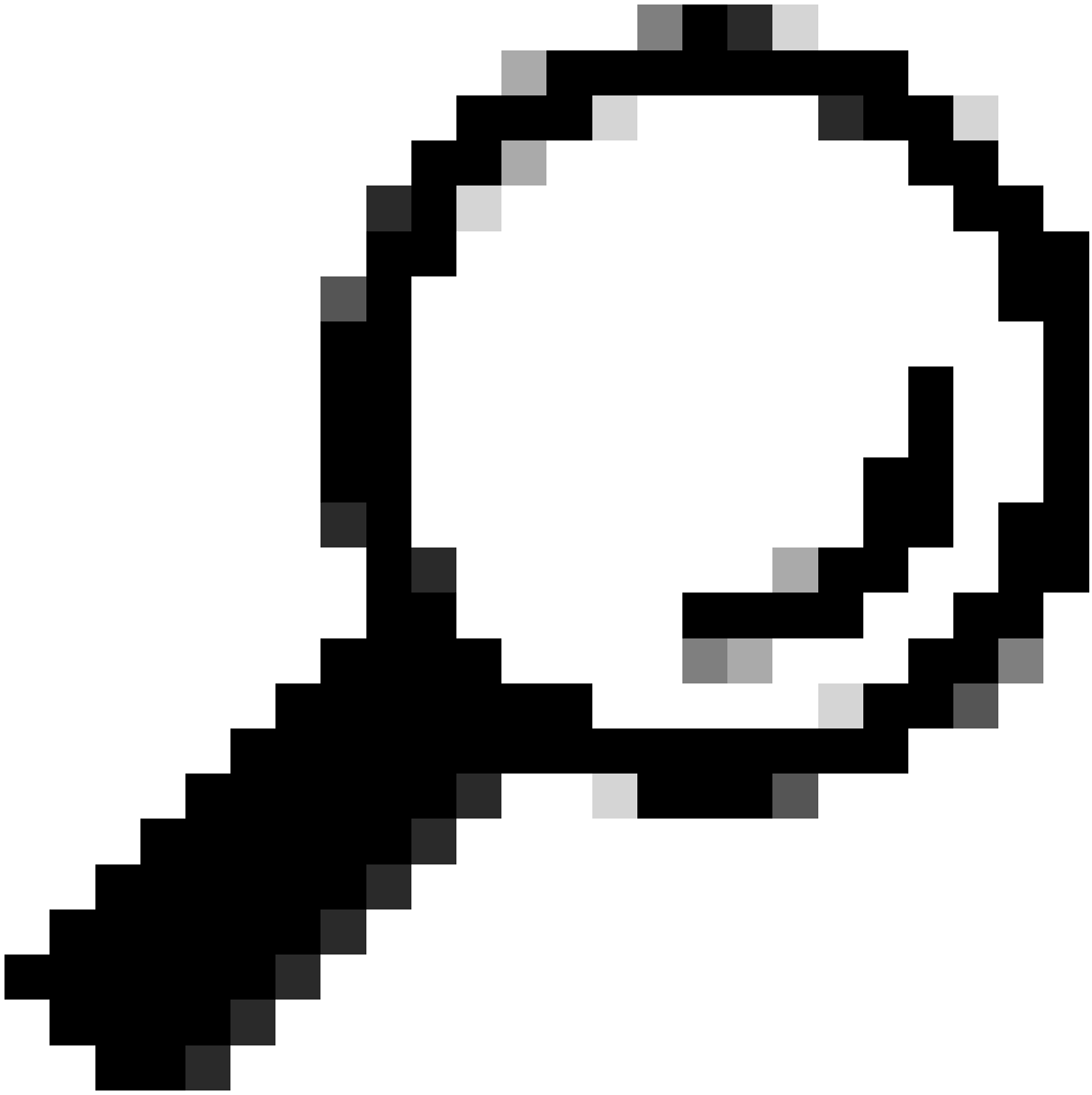
· AD组Device Admin 中的用户分配有CISCO_IOSXR_RW 命令集和IOSXR_RW 外壳配置文件。



第2部分 — 为基于TLS 1.3的TACACS+配置Cisco IOS XE



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。

配置方法1 — 设备生成的密钥对

TACACS+服务器配置

第1步配置域名并生成用于路由器信任点的密钥对。

```
ip domain name svs.lab

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

信任点配置

第1步创建路由器信任点并关联密钥对。

```
crypto pki trustpoint svs_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 svs-256ec-key
```

步骤2.通过安装CA证书对信任点进行身份验证。

<#root>

cat9k(config)#

crypto pki authenticate svs_cat9k

Enter the base 64 encoded CA certificate.

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

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

MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4

```
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==

-----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)#
```

步骤3.生成证书签名请求(CSR)。

<#root>

```
cat9k(config)#
```

crypto pki enroll svs_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-----
MIIBfDCCASMCAQAwgYQxGjAYBgNVBAMTEWNhdDlrLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAxCzAJBgNVBAgT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2F0OWsudG1vLnN2cy5j
b20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATpYE7atscrtl4ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMS0wKzAcBgNVHREEFTATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTwM3ZZrmIphJ7+jSTER
4OkTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----
```

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

Redisplay enrollment request? [yes/no]:
```

no

```
cat9k(config)#
```

步骤4.导入CA签名证书。

<#root>

```
cat9k(config)#
```

crypto pki import svs_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
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTE0MTUxMjAwWhcNMjYwNTE0MTUxMjAwWjCBhDEaMBgGA1UEAxMR
Y2FOOWsudG1vLnN2cy5jb2OxDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ2lzY28x
DDAKBgNVBAcTA1JUUDELMAkGA1UECBMCTkMxCzAJBgNVBAYTAlVTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay5ObW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABOlgTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFyOrLiyjxXmLpFcO3uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2Vy
dGlmaWNhdGUwHAYDVR0RBBUwE4IRY2FOOWsudG1vLnN2cy5jb2OwCwYDVR0PBAQD
AgeAMA0GCSqGSIb3DQEBCwUAA4ICAQBObgKVykeyVC9UsvuuOAUsGaZHGwy2H9Yd
m5vIaui6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAhzY
RtmIM5KIojiDHLtifPayxv9juDuOZRx+wYR2PIQ5eLv1bafg7K8E82sqOCfOtcPr
OcONU8UCxqObdOgu4XsdBN1+wcWFqeQSDLmP7nxvhOOm/LXwCWUHwgVioOAuU2Fe
k5NthtvdxNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
lxCSoLtYOdUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUhQSY+4m
Qq2Sn3iqf4mGh/AO8T4iXfWDWfNezh7ZxMsCSCK/ZRlELZ2hj6OfzwX1H27Uf8XU
ecrOWx+WzRn7LVRCaGQzFkukfi8S4DLLNtxnNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVrPitwN3ZbO9poZyWiRLTnBsb42xNaWiL9bjQznAOiTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+4lOTMawDgGiEv7iaiJ6xWc95EC+AdmOx3FvBXMtIM9qr7WwHW6
3C2hVYHJH254elV5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
-----END CERTIFICATE-----

% Router Certificate successfully imported

cat9k(config)#
```

采用TLS配置的TACACS和AAA

步骤1.创建TACACS服务器和AAA组，关联客户端（路由器）信任点。

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

步骤2.配置AAA方法。

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

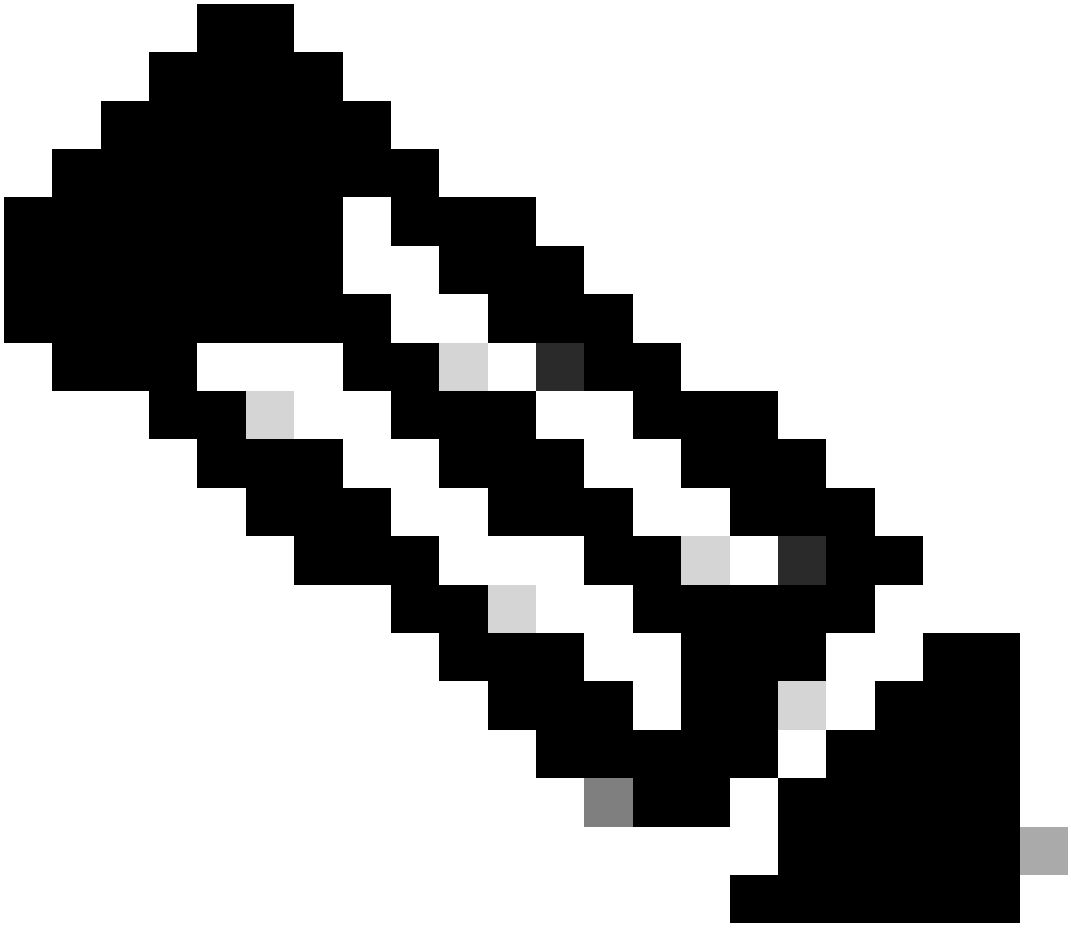
配置方法2 - CA生成的密钥对

如果直接以PKCS#12格式而不是CSR方法导入密钥以及设备和CA证书，则可以使用此方法。

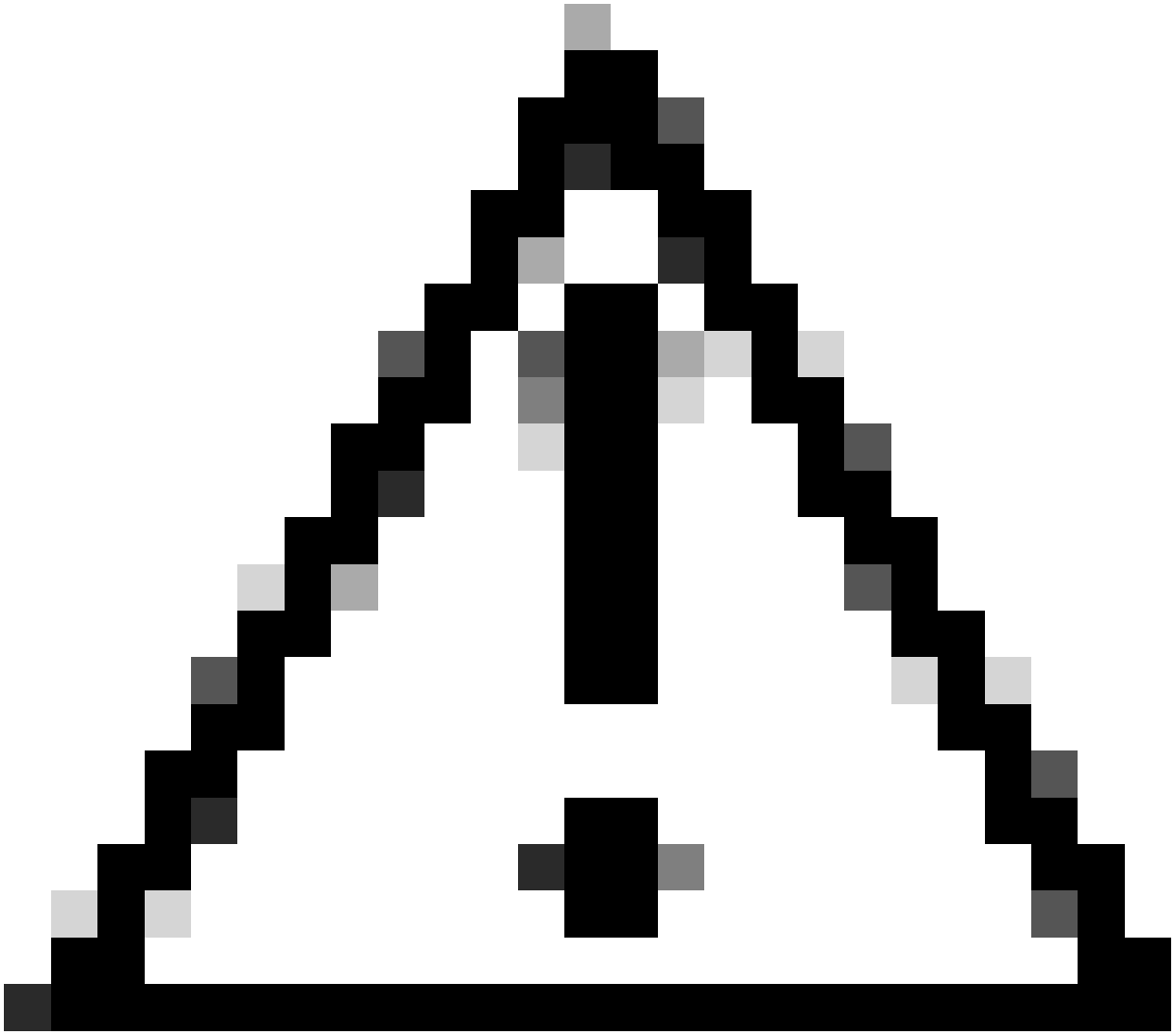
步骤1.创建客户端信任点。

```
cat9k(config)#crypto pki trustpoint svs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

步骤2.将PKCS#12文件复制到bootflash中。



注意：确保PKCS#12文件包含完整的证书链和作为加密文件的私钥。



警告：导入的PKCS#12中的密钥必须是RSA(例如：RSA 2048)类型，而不是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)
```

步骤3.使用import命令导入PKCS#12文件。

<#root>

```
cat9k#

crypto pki import svs_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 svs_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: svs_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: svs_cat9k_25jun17 svs_cat9k
  Storage: nvram:SVSLabCA#37F5CA.cer
```

采用TLS配置的TACACS和AAA

步骤1.创建TACACS服务器和AAA组，关联客户端（路由器）信任点。

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

步骤2.配置AAA方法。

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

确认

验证配置。

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

调试AAA和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
```

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）。