

# 在使用ISE的Nexus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](#)

### [为设备管理员配置ISE](#)

[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](#)

[网络设备和网络设备组](#)

[配置身份库](#)

[配置TACACS+外壳配置文件](#)

[NX-OS管理员](#)

[NX-OS帮助台](#)

[配置设备管理策略集](#)

### [配置基于TLS的TACACS+的Cisco NX-OS](#)

[TACACS+服务器配置](#)

[信任点配置](#)

[TACACS+ TLS配置](#)

[AAA 配置](#)

### [对NX-OS的用户访问进行测试和故障排除](#)

[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NX-OS设备作为客户端的基于TLS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 NX-OS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 — 配置基于TLS的TACACS+的Cisco NX-OS

## 先决条件

### 要求

通过TLS配置TACACS+的必备条件：

- 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。
- Nexus 9000交换机型号C9364D-GX2A，Cisco NX-OS版本10.5(3t)。

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。

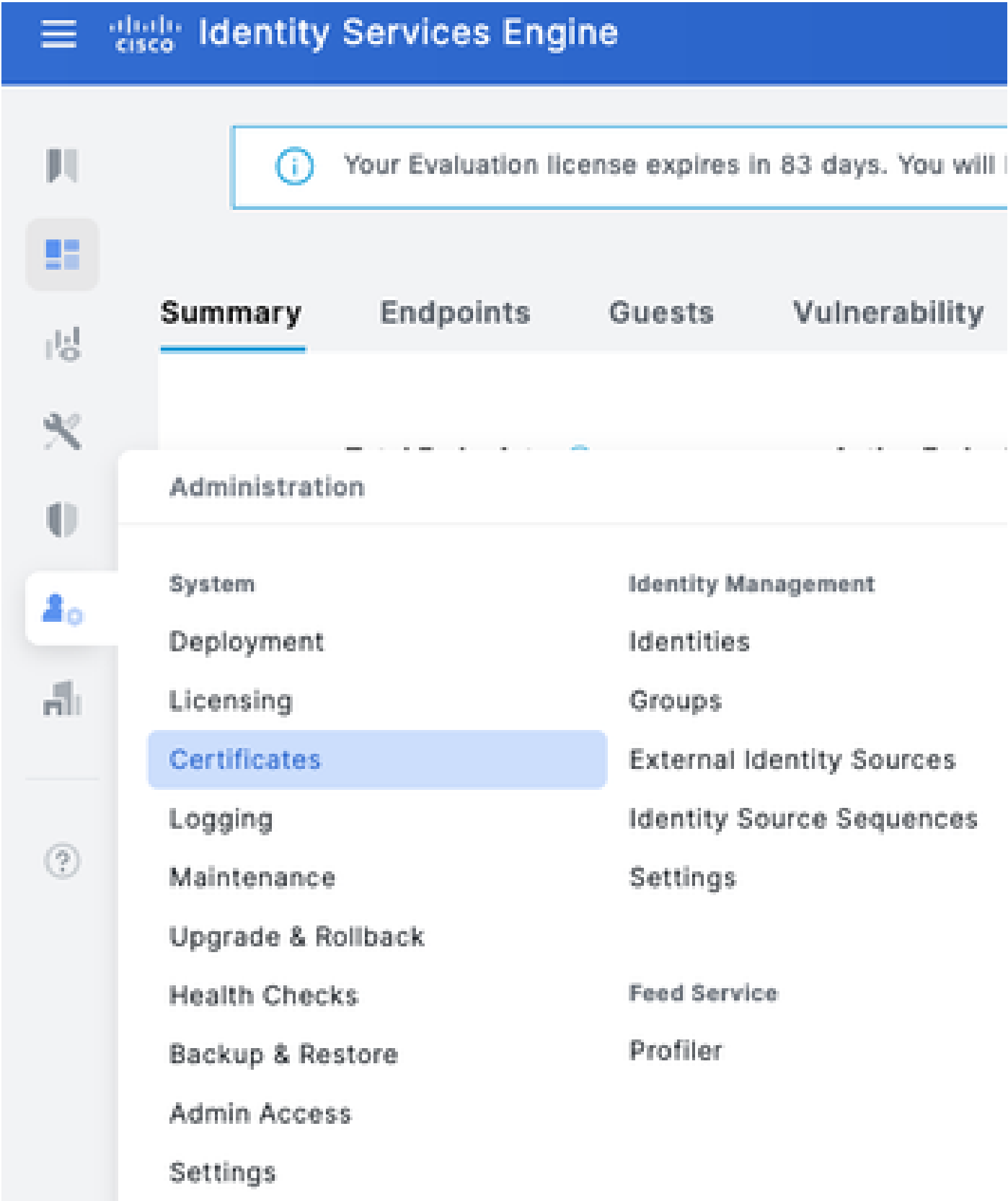
## 为设备管理员配置ISE

### 为TACACS+服务器身份验证生成证书签名请求

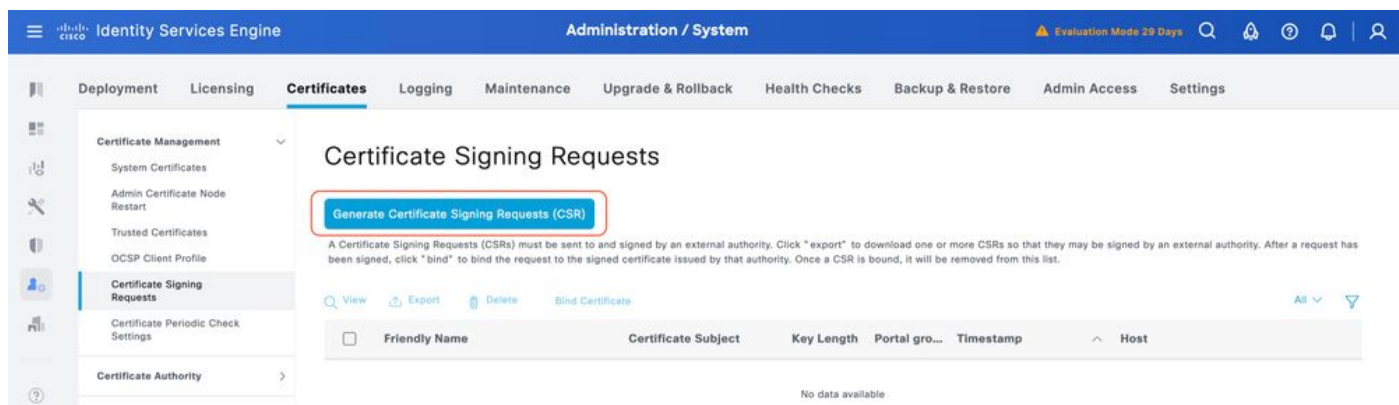
第1步：使用受支持的浏览器之一登录ISE管理员Web门户。

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。

步骤2.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Usage中的TACACS。

## Usage

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

Allow Wildcard Certificates ☐ i

步骤5.选择已启用TACACS+的PSN。

## Node(s)

Generate CSR's for these Nodes:

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

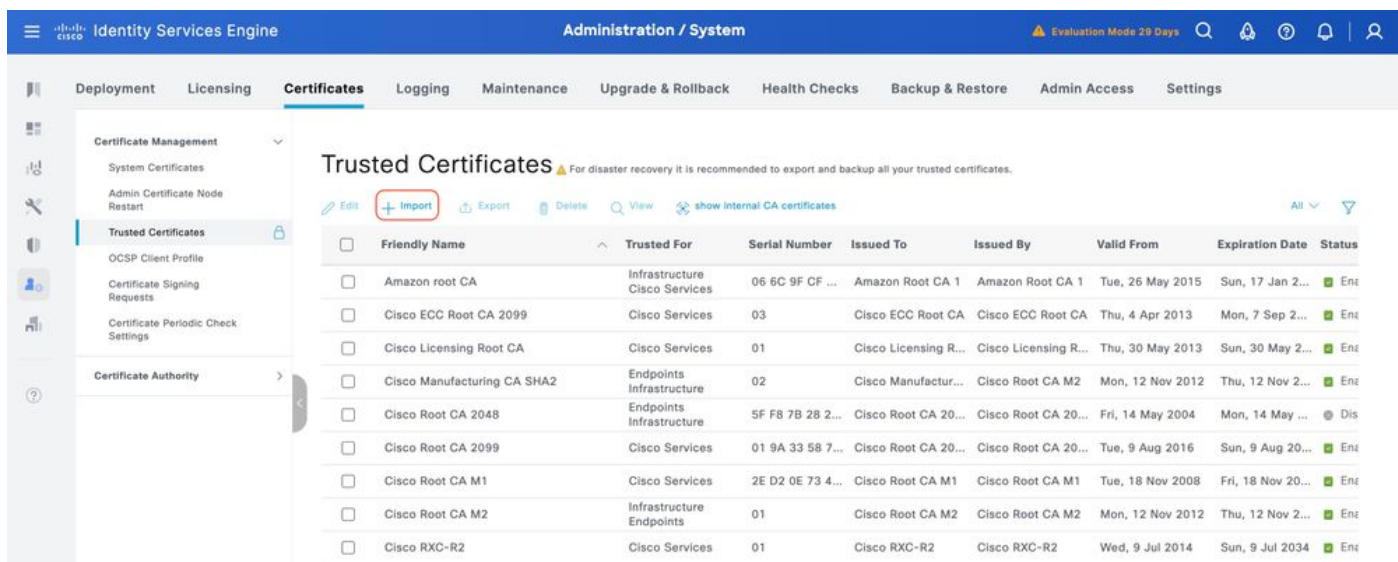
步骤8.单击Generate，然后单击Export。



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

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



第2步：选择由证书颁发机构(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。确保启用ISE内身份验证的信任选项。

## Import a new Certificate into the Certificate Store

\* Certificate File  ISE SVSLab CA.crt

Friendly Name

Trusted For: ☐

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

Description

Submit

Cancel

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

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

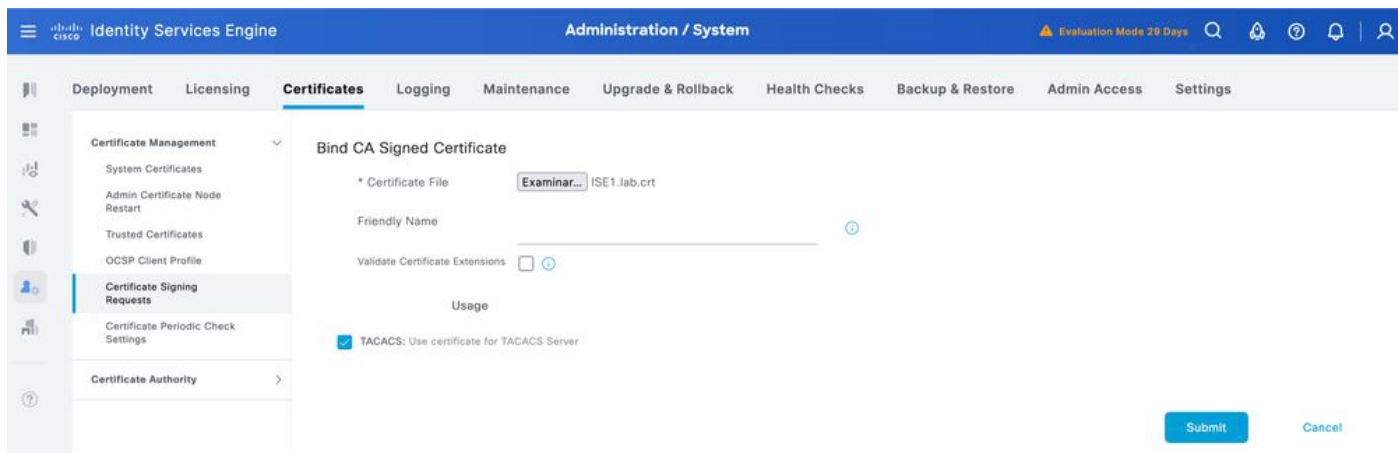
## 将签名证书签名请求(CSR)绑定到ISE

签名证书签名请求(CSR)后，您可以在ISE上安装已签名的证书。

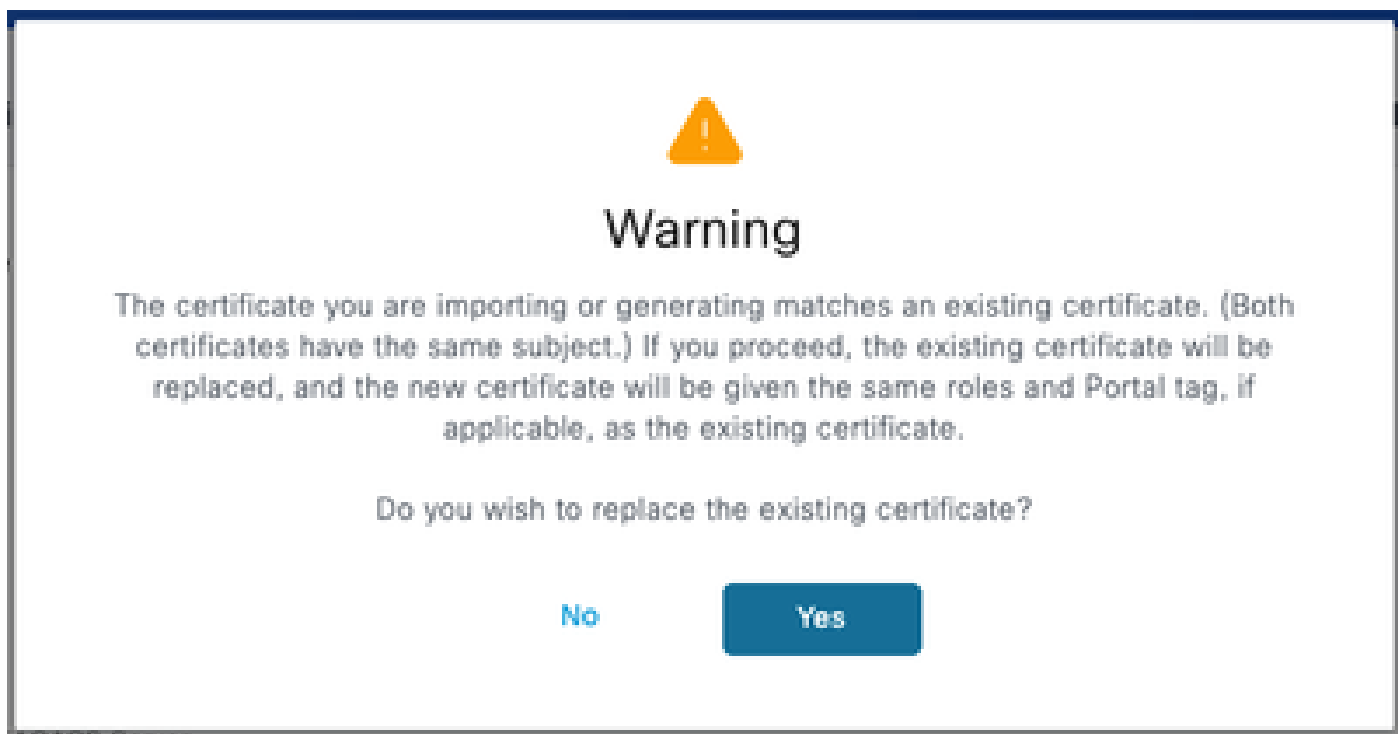
步骤1.导航到管理>系统>证书。在Certificate Signing Requests下，选择上一步中生成的TACACS CSR，然后单击Bind Certificate。

| Friendly Name | Certificate Subject | Key Length | Portal gro... | Timestamp | Host |
|---------------|---------------------|------------|---------------|-----------|------|
|---------------|---------------------|------------|---------------|-----------|------|

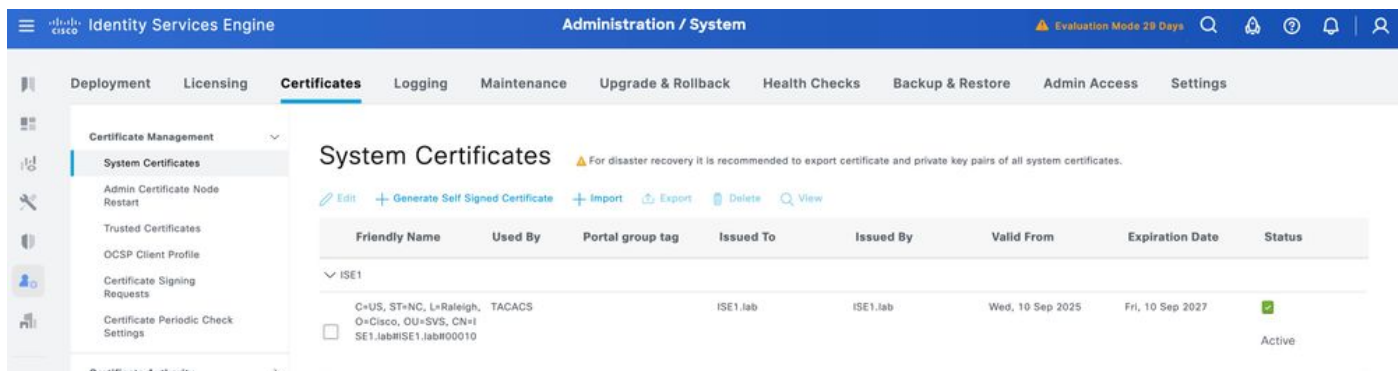
步骤2.选择签名证书，并确保使用(Usage)下的TACACS复选框保持选中。



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以继续。



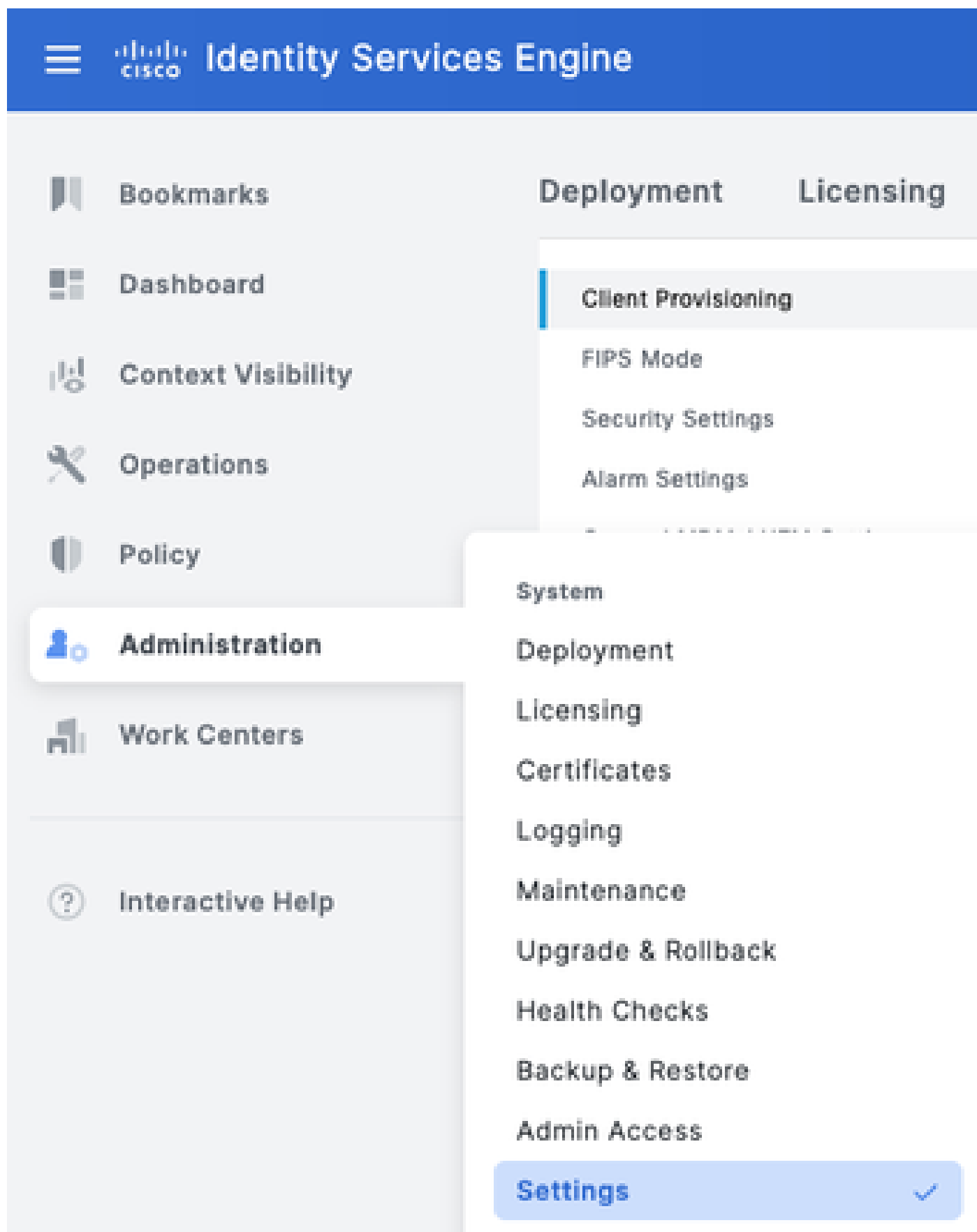
现在必须正确安装证书。您可以在System Certificates下验证这一点。



## 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。

步骤1.导航到管理>系统>设置。



步骤2.单击Security Settings，在TLS Version Settings下选中TLS1.3旁的复选框，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

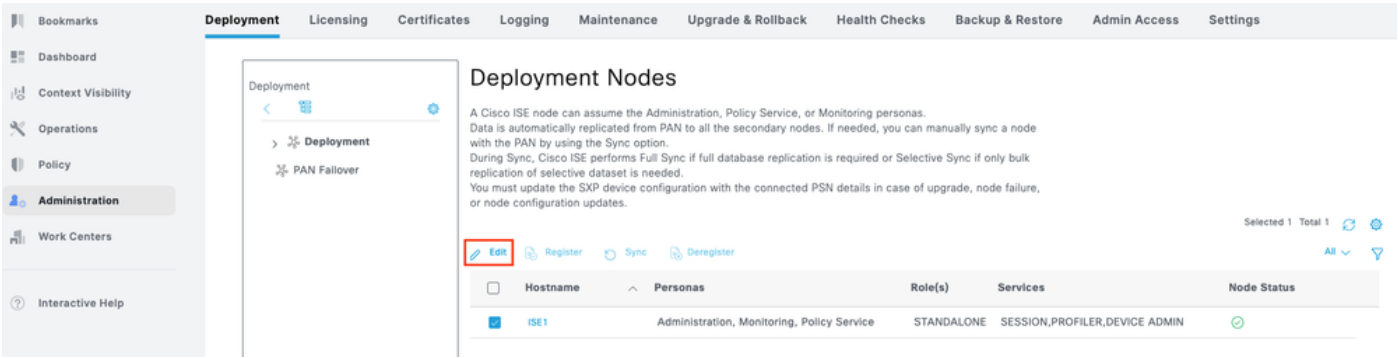


警告：当您更改TLS版本时，思科ISE应用服务器在所有思科ISE部署计算机上重新启动。

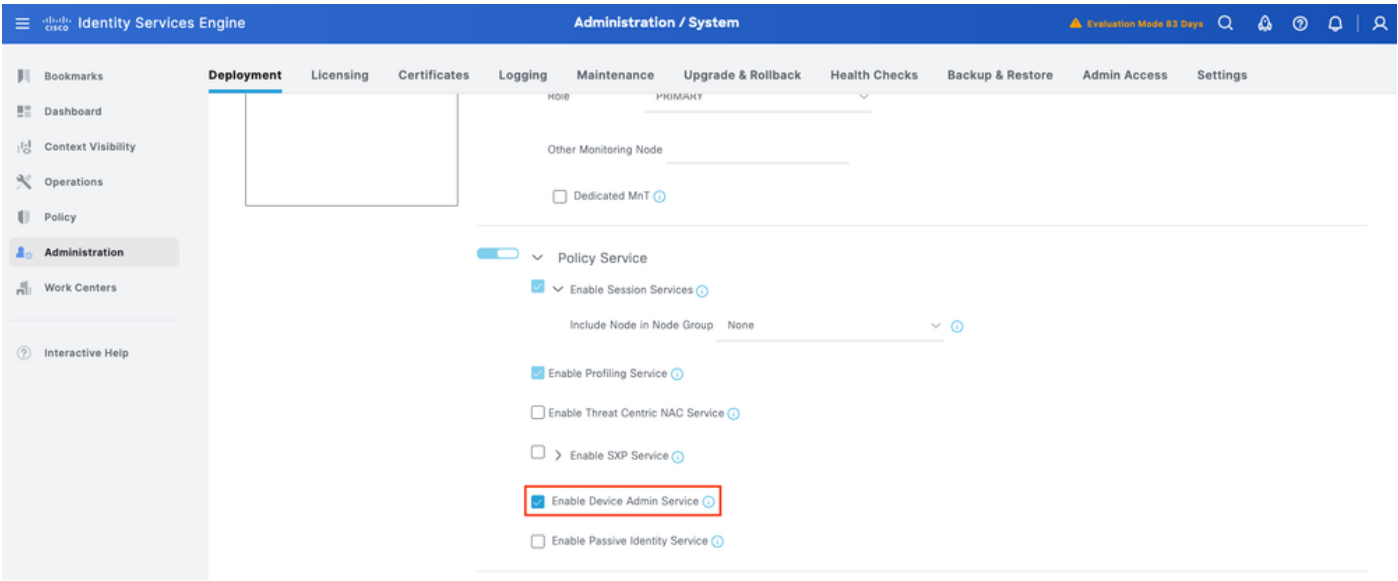
## 在ISE上启用设备管理

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

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。



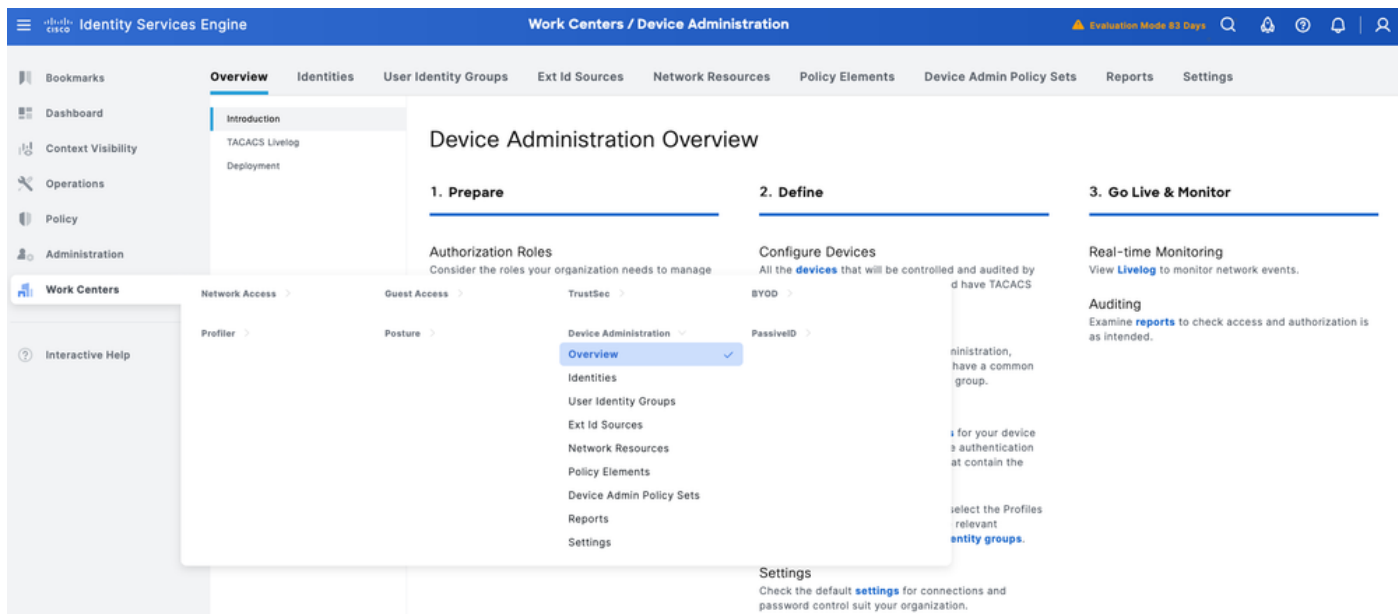
步骤2.在General Settings下，向下滚动并选中Enable Device Admin Service旁边的复选框。



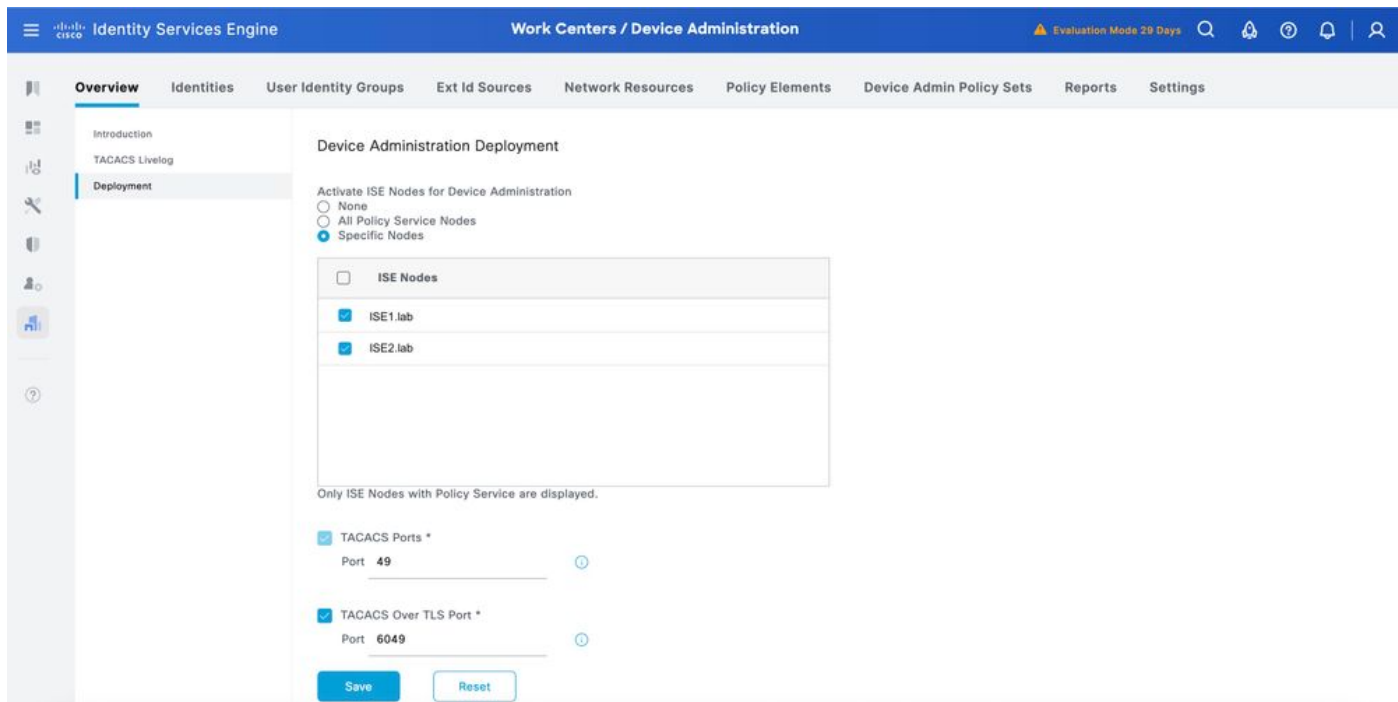
步骤3.保存配置。设备管理服务现在在ISE上启用。

## 启用TLS上的TACACS

步骤1.导航到工作中心>设备管理>概述。



步骤2.单击部署。选择要通过TLS启用TACACS的PSN节点。

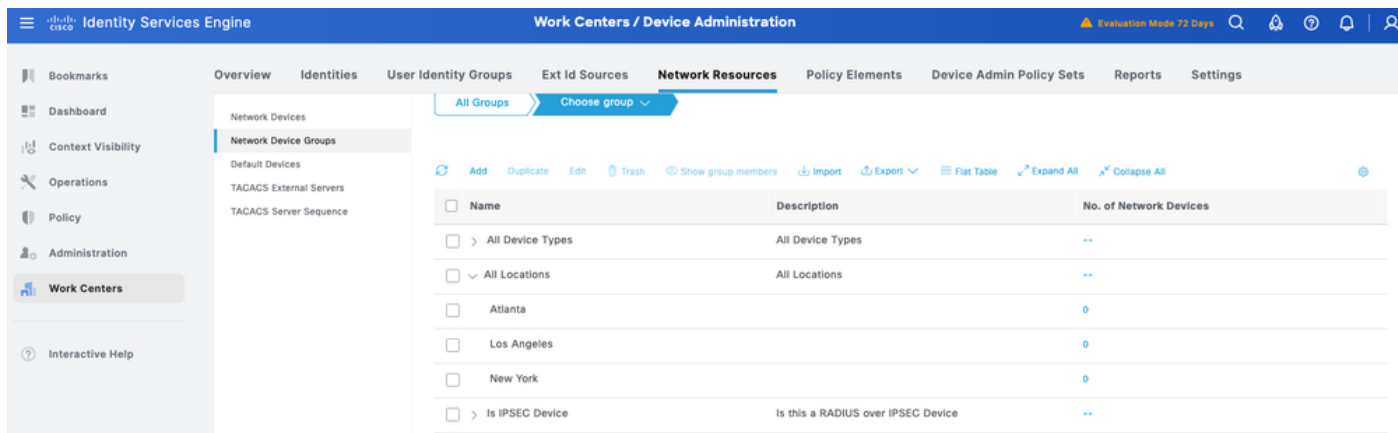


步骤3.保留默认端口6049或为TLS上的TACACS指定不同的TCP端口，然后单击Save。

## 网络设备和网络设备组

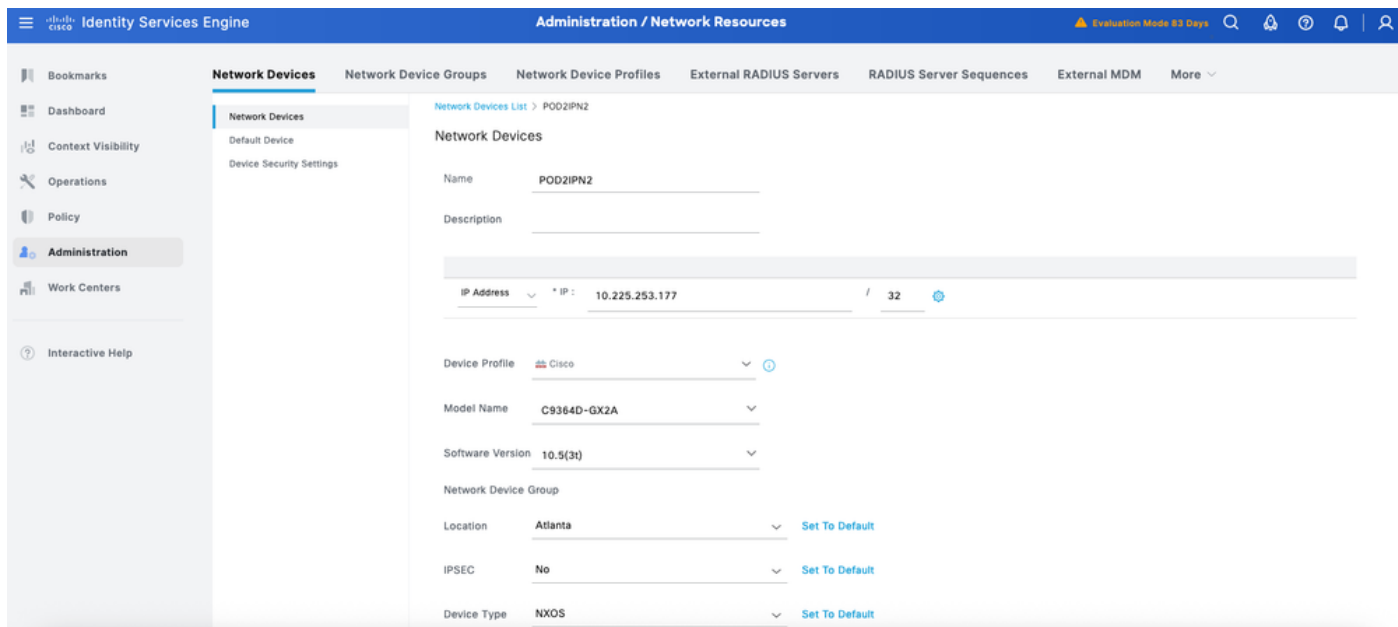
ISE提供具有多个设备组层次结构的强大设备分组。每个分层结构代表网络设备不同的独立分类。

步骤1.导航到工作中心>设备管理>网络资源。单击Network Device Groups。



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NS-OX设备作为网络设备。导航到工作中心>设备管理>网络资源。单击Add添加新的网络设备POD2IPN2。



步骤3.输入设备的IP地址，并确保映射设备的位置和设备类型。最后，启用TLS身份验证设置上的TACACS+。

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

External MDM

More

Network Devices

Default Device

Device Security Settings

☐ RADIUS Authentication Settings

☐ TACACS Authentication Settings

☒ TACACS over TLS Authentication Settings

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

Subject Alternative Name (SAN) \*

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

☐ IP Address

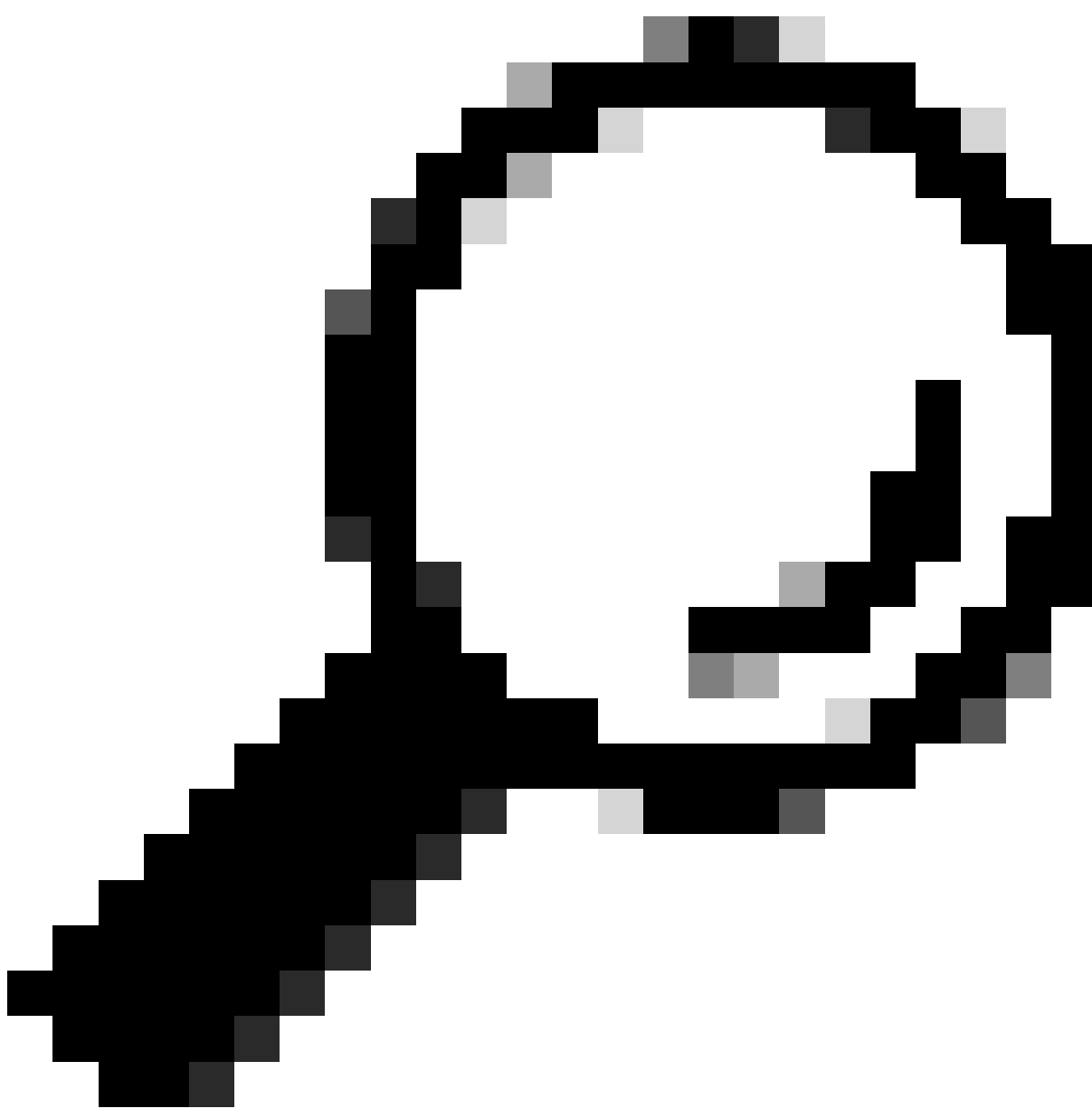
The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details [Show](#)

Additional SAN Attributes

☒ Enable Single Connect Mode

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

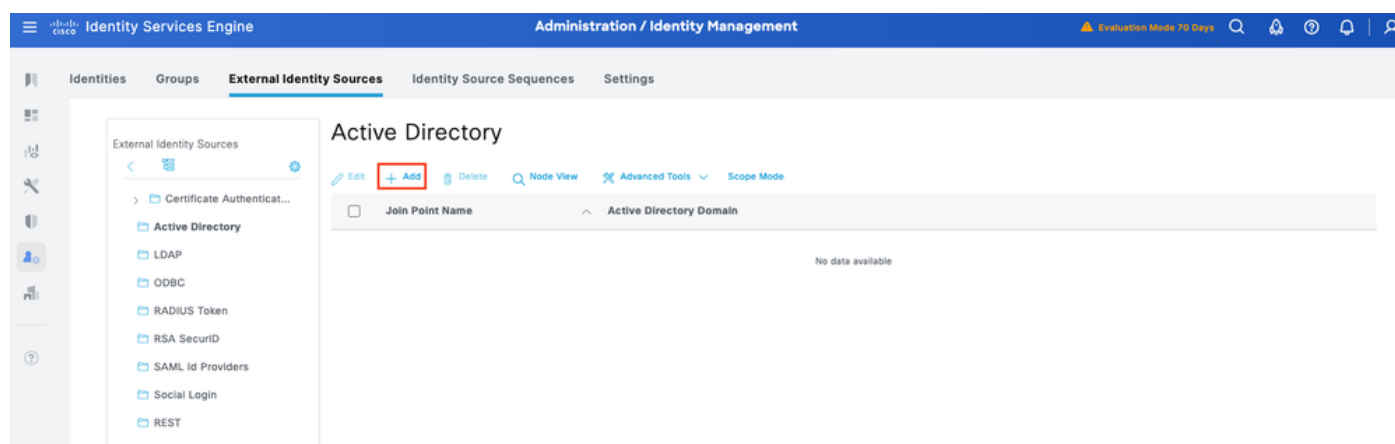


提示：建议启用单一连接模式，以避免每次向设备发送命令时重新启动TCP会话。

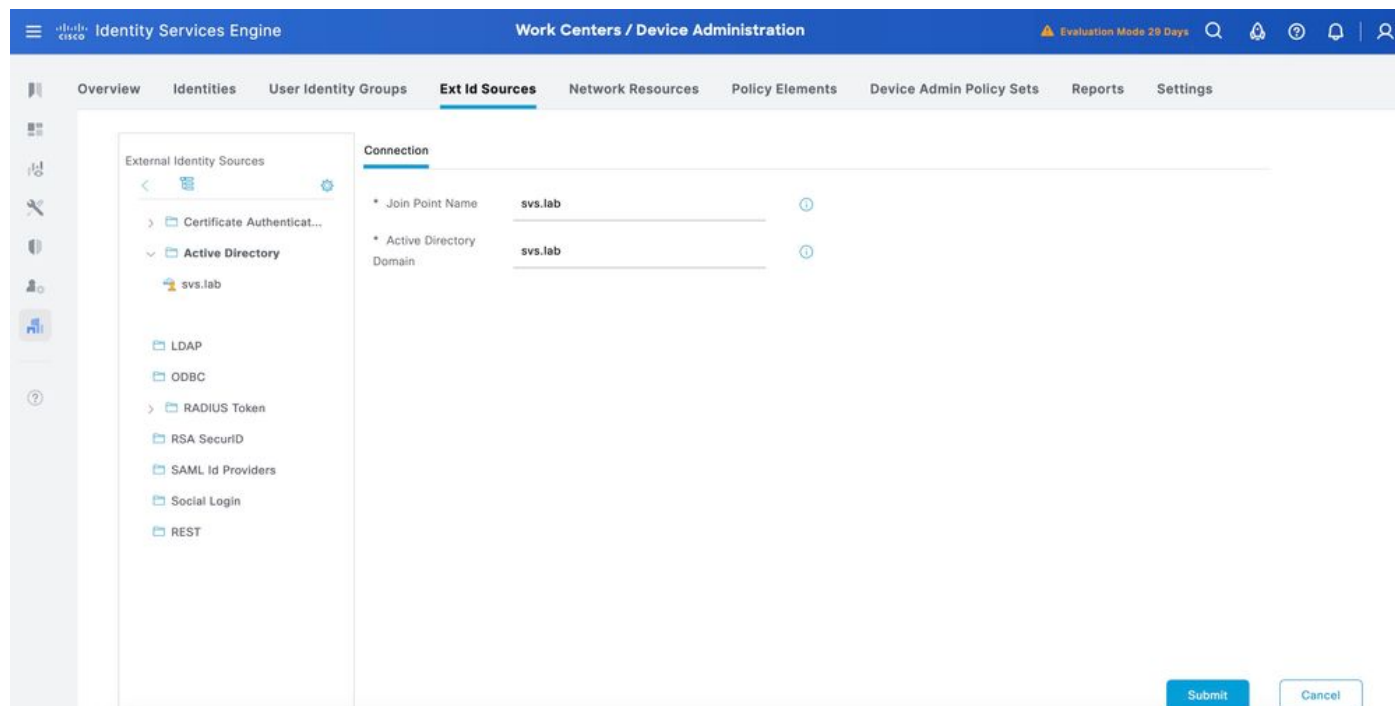
## 配置身份库

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.指定加入点名和AD域名，然后单击提交。



步骤3.当系统提示“是否要将所有ISE节点加入此Active Directory域？”时，单击Yes。



## Information

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

No

Yes

第4步：输入具有AD加入权限的凭证，将ISE加入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

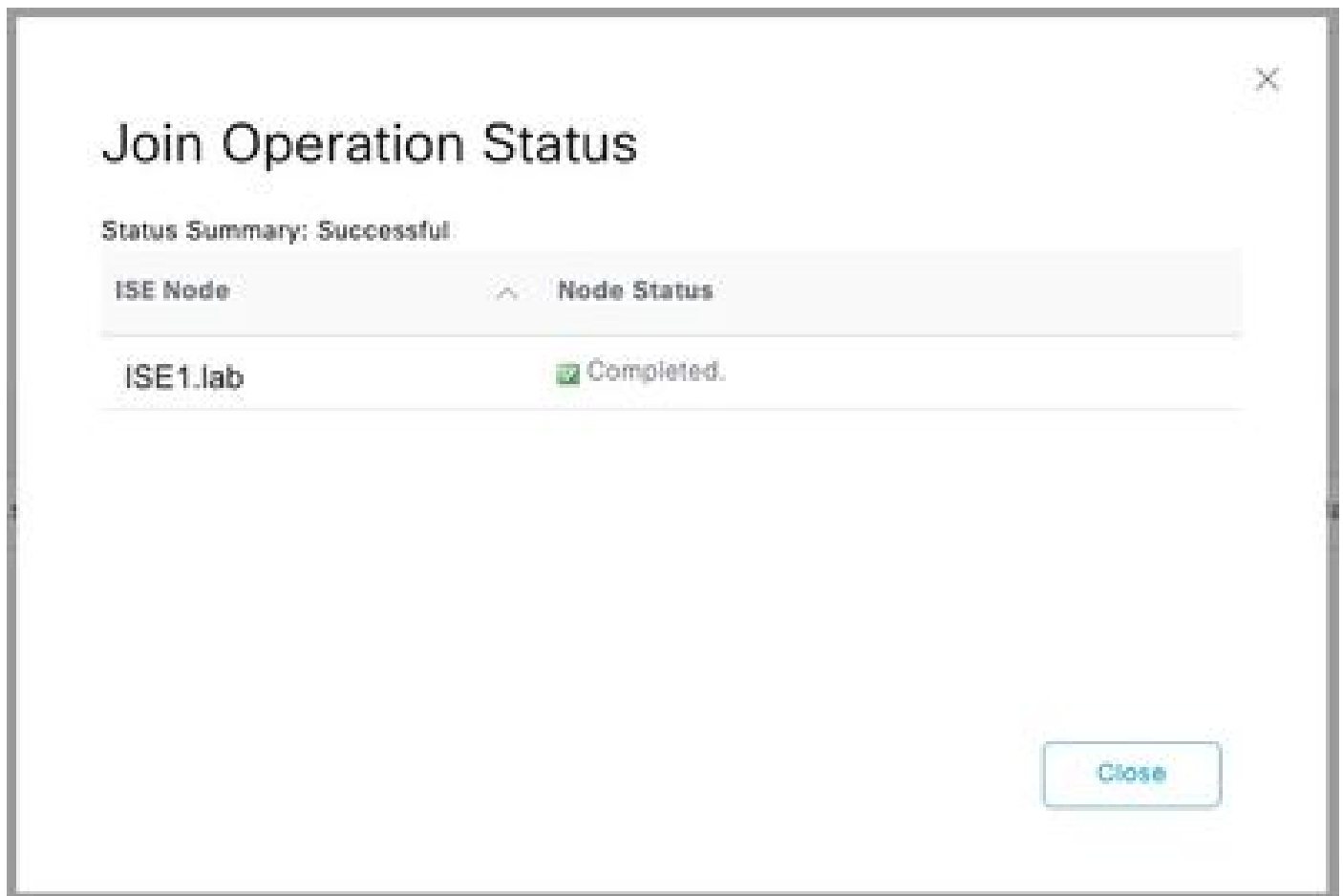
\* Password .....  
.....

☐ Specify Organizational Unit ⓘ

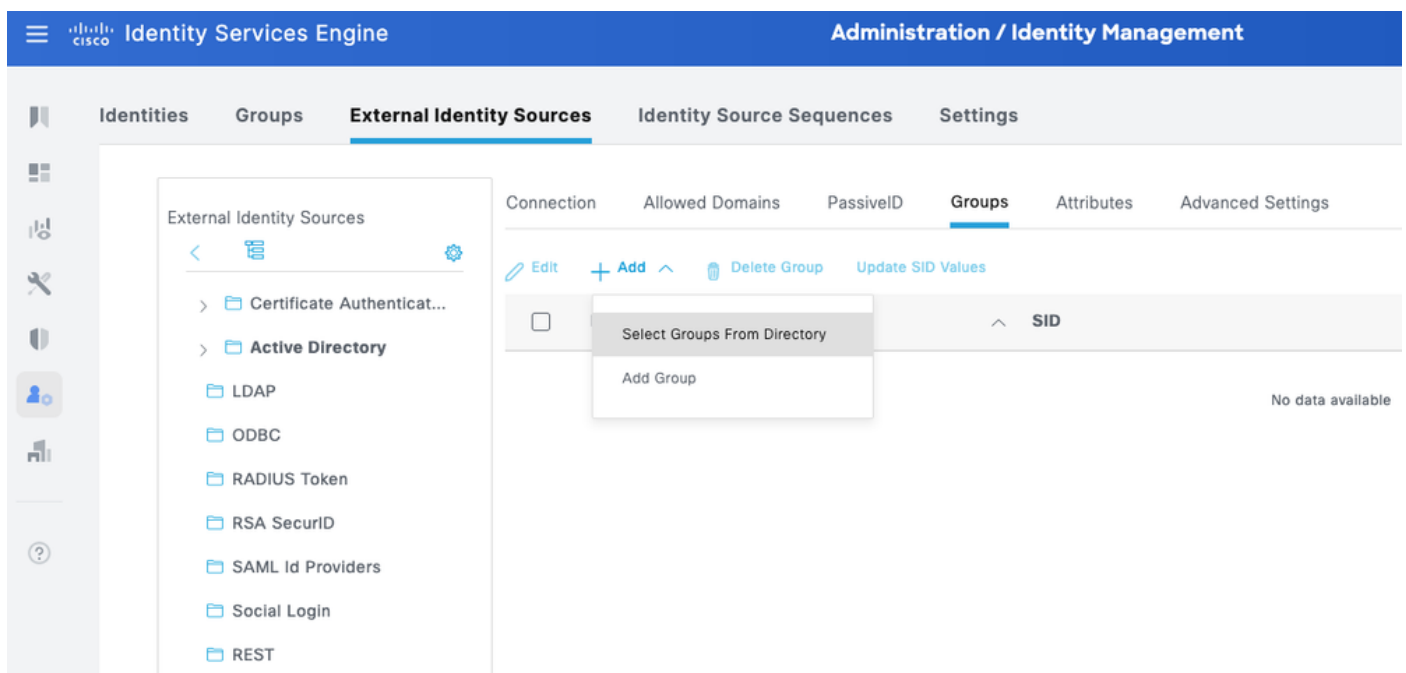
☒ Store Credentials ⓘ

Cancel

OK



第5步：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。



# Select Directory Groups

This dialog is used to select groups from the Directory.

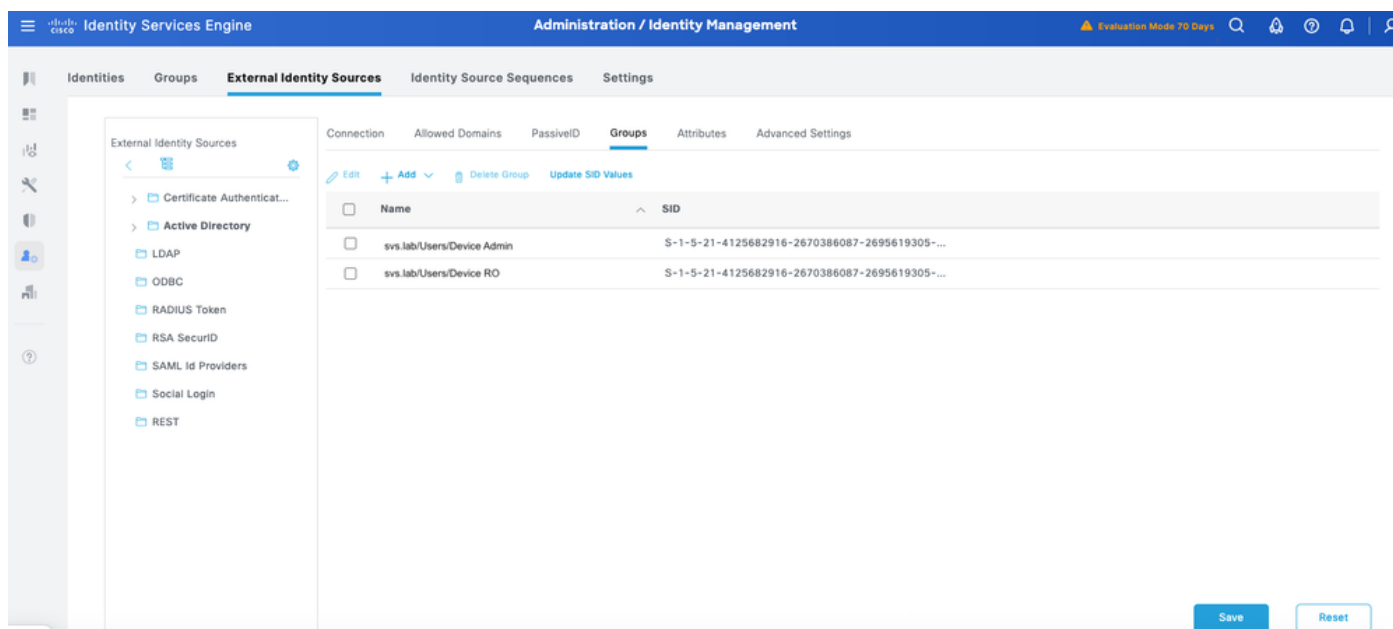
Domain

Name  SID

Filter  Type Filter

2 Groups Retrieved.

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



## 配置TACACS+外壳配置文件

与使用权限级别进行授权的Cisco IOS设备不同，Cisco NX-OS设备实施基于角色的访问控制 (RBAC)。在ISE中，您可以使用Nexus类型常见任务将TACACS+配置文件映射到思科NX-OS设备上的用户角色。

NX-OS设备上的预定义角色因NX-OS平台而异。两种常见方式是：

- network-admin — 预定义网络管理员角色对交换机上的所有命令具有完全读写访问权限；仅在设备（例如Nexus 7000）有多个VDC时可用于默认虚拟设备环境(VDC)。使用NX-OS CLI命令show cli syntax roles network-admin查看可用于此角色的完整命令列表。
- network-operator — 预定义网络管理员角色对交换机上的所有命令具有完全读取访问权限；仅在设备（例如Nexus 7000）有多个VDC时可用。使用NX-OS CLI命令show cli syntax roles network-operator查看可用于此角色的完整命令列表。

接下来，它定义了两个TACACS配置文件 — NXOS Admin和NXOS HelpDesk。

## NX-OS管理员

步骤1.添加另一个配置文件，并将其命名为NX-OS Admin。

步骤2.从Set attributes as下拉列表中选择Mandatory。在常见任务下，选择Network-role选项下的Administrator。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Device Administration'. The left sidebar shows a tree view with 'TACACS Profiles' selected. The main content area is titled 'TACACS Profile' and shows the configuration for a profile named 'NXOS Admin'. The 'Name' field is 'NXOS Admin'. The 'Description' field is empty. Below the 'Task Attribute View' tab, the 'Common Tasks' section shows 'Common Task Type' set to 'Nexus'. Under 'Set attributes as', 'Mandatory' is selected. Under 'Network role', 'Administrator (Read Write)' is selected. Under 'VDC role', 'None' is selected.

步骤3.单击Submit保存配置文件。

## NX-OS帮助台

第1步：从ISE UI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NXOS HelpDesk。转到Common Task Type ( 常见任务类型 ) 下拉菜单并选择 Nexus。

您可以看到特定于用户角色的模板更改。您可以选择与要配置的用户角色对应的这些选项。

步骤2.从Set attributes as下拉列表中选择Mandatory。在常见任务下，选择Network-role选项下的Operator。

**Identity Services Engine** | Work Centers / Device Administration | Evaluation Mode 89 Days

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

**TACACS Profiles** > NXOS HelpDesk

**TACACS Profile**

Name: NXOS HelpDesk

Description:

Task Attribute View | Raw View

**Common Tasks**

Common Task Type: Nexus

Set attributes as: Optional

**Network role**

☐ None

☒ Operator (Read Only)

☐ Administrator (Read Write)

**VDC role**

☒ None

☐ Operator (Read Only)

☐ Administrator (Read Write)

第 3 步：单击Save保存配置文件。

## 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。例如，Cisco IOS设备使用权限级别和/或命令集，而Cisco NX-OS设备使用自定义属性。

第1步：导航到工作中心(Work Centers)>设备管理(Device Administration)>设备管理策略集(Device Admin Policy Sets)。添加新的策略集NX-OS设备。在condition下，指定DEVICE:Device Type EQUALS All Device Types#NXOS。在Allowed Protocols下，选择Default Device Admin。

**Identity Services Engine** | Work Centers / Device Administration | Evaluation Mode 89 Days

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

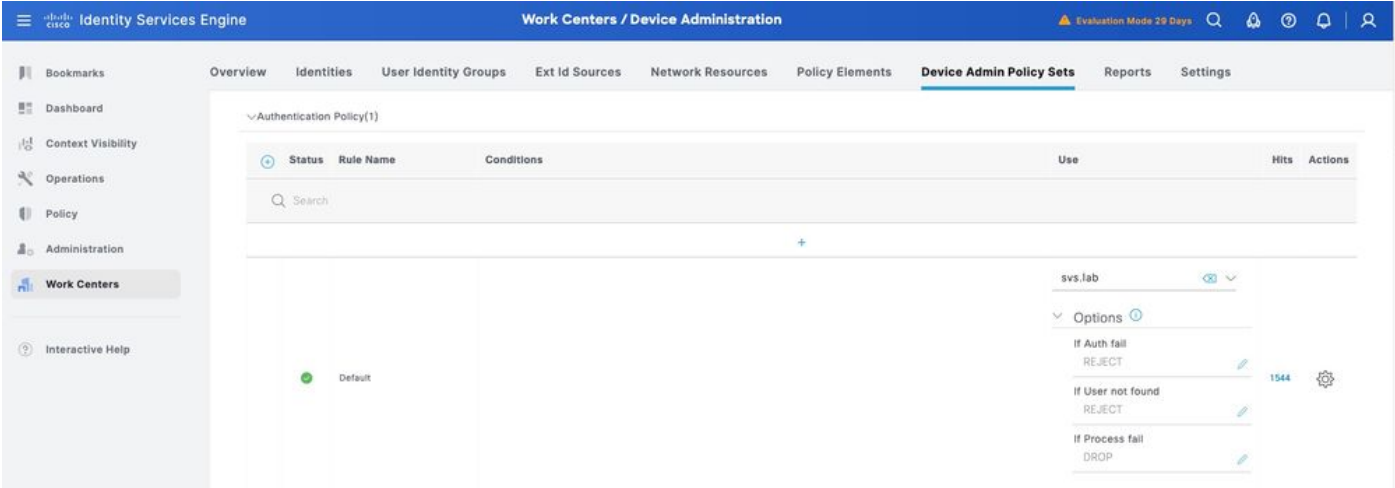
Policy Sets

Reset | Reset Policy Set Hit Counts | Save

| Status                           | Policy Set Name | Description | Conditions                                      | Allowed Protocols / Server Sequence | Hits | Actions | View |
|----------------------------------|-----------------|-------------|-------------------------------------------------|-------------------------------------|------|---------|------|
| <input checked="" type="radio"/> | NX-OS Devices   |             | DEVICE:Device Type EQUALS All Device Types#NXOS | Default Device Admin                |      |         |      |

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，将AD用作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。

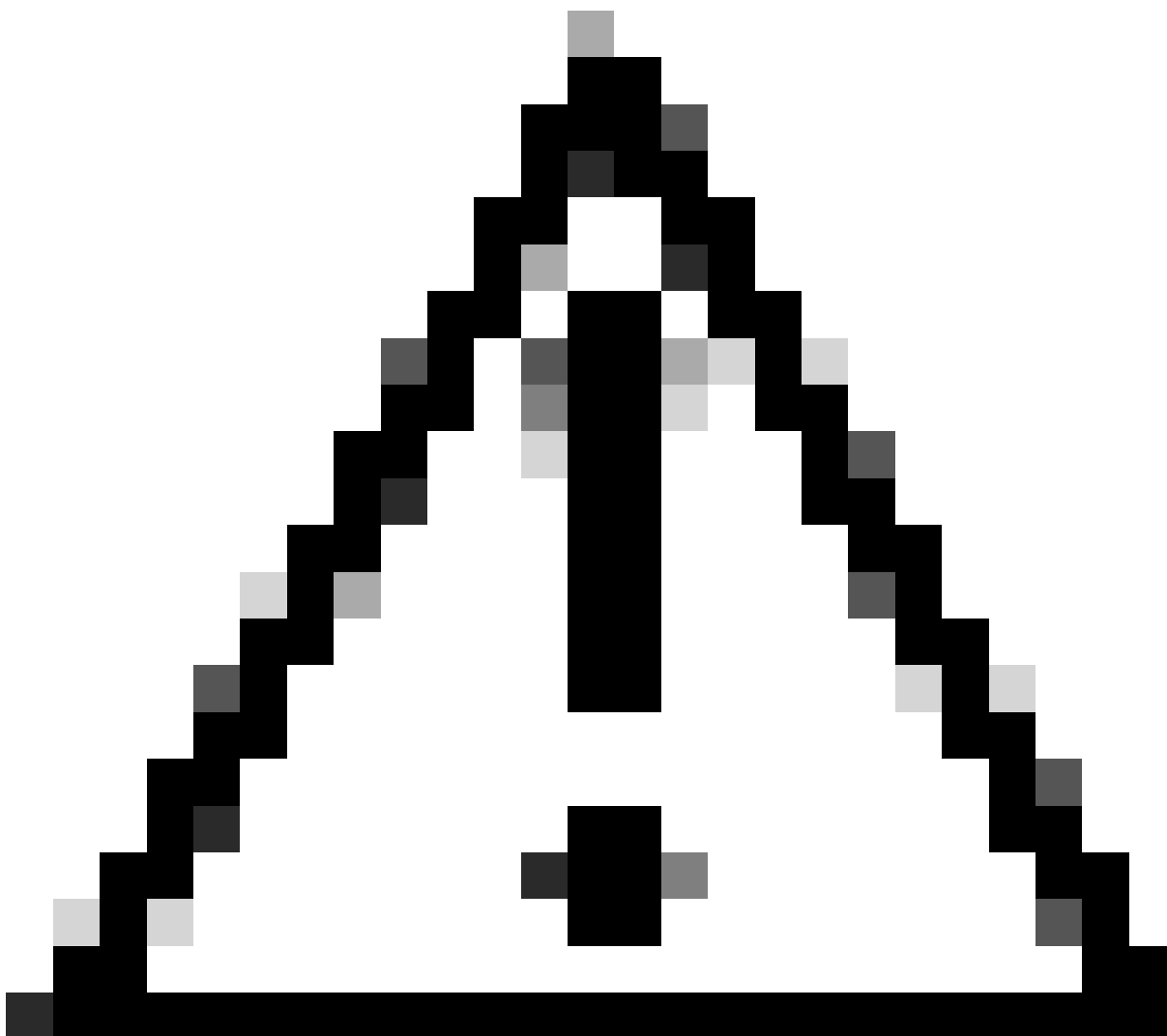
例如：

- AD组Device Admin中的用户分配有NXOS Admin TACACS配置文件。
- AD组设备RO中的用户分配了NXOS帮助台TACACS配置文件。

Authorization Policy(3)

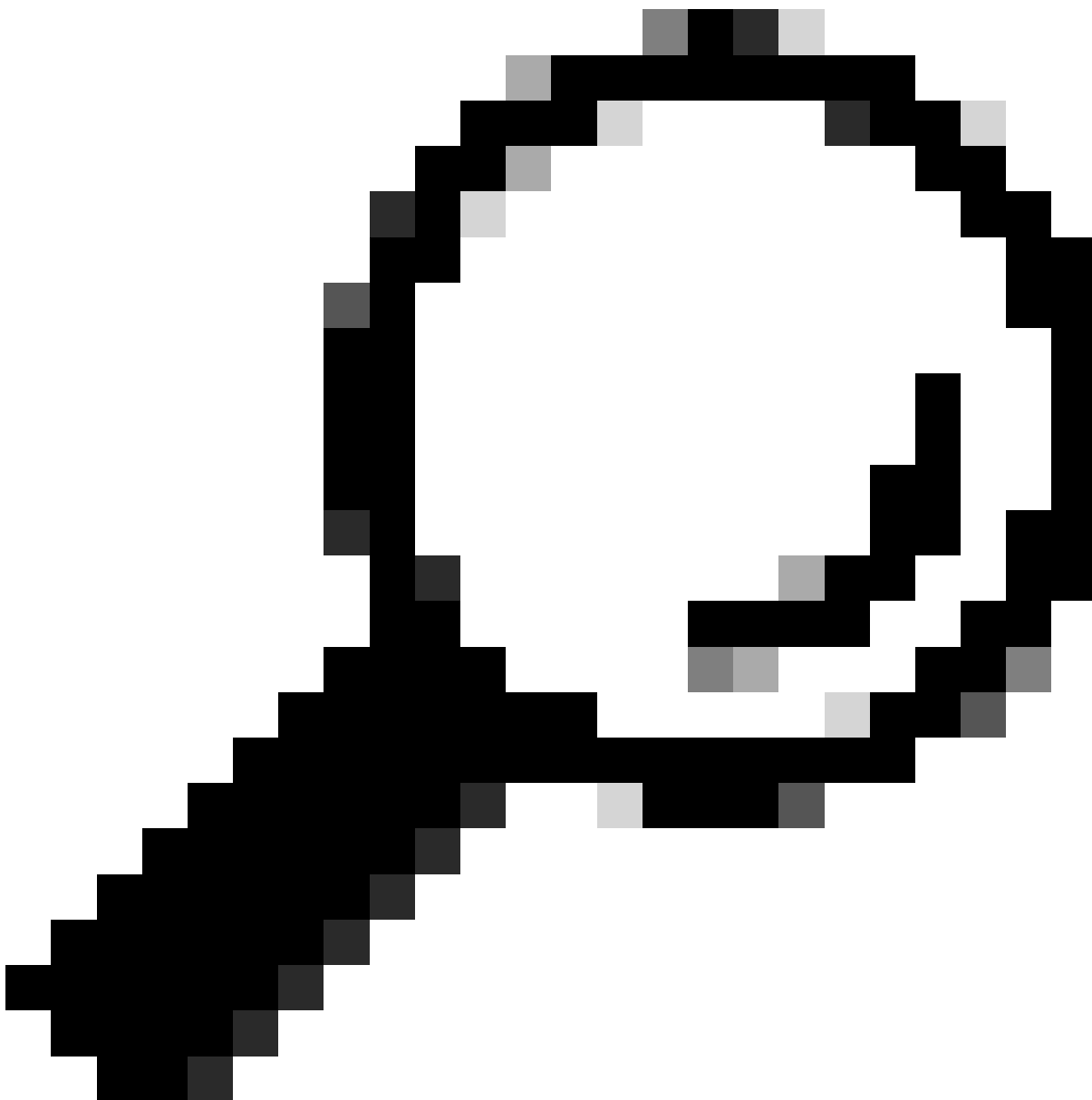
|                                                                                            |        |                       |                                                                                                                                              |  | Results          |                                                                                                                                                                             |                        |                                                                                                                                                                             |                                                                                       |
|--------------------------------------------------------------------------------------------|--------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|--|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
|         | Status | Rule Name             | Conditions                                                                                                                                   |  | Command Sets     |                                                                                                                                                                             | Shell Profiles         | Hits                                                                                                                                                                        | Actions                                                                               |
|  Search |        |                       |                                                                                                                                              |  |                  |                                                                                                                                                                             |                        |                                                                                                                                                                             |                                                                                       |
|         |        | Authorization Rule RO |  svs.lab-ExternalGroups EQUALS svs.lab/Users/Device RO    |  | Select from list |   | NXOS HelpDe            |   |  |
|         |        | Authorization Rule RW |  svs.lab-ExternalGroups EQUALS svs.lab/Users/Device Admin |  | Select from list |   | NXOS Admin             |   |  |
|         |        | Default               |                                                                                                                                              |  | DenyAllCommands  |   | Deny All Shell Profile |   |  |

## 配置基于TLS的TACACS+的Cisco NX-OS



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。

---

## TACACS+服务器配置

步骤1.初始配置。

```
POD2IPN2# sho run tacacs
```

```
feature tacacs+
```

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

use-vrf management

## 信任点配置

步骤1.创建密钥标签，对于您的情况，请使用ecc密钥对。

```
<#root>
```

```
POD2IPN2(config)#
```

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

步骤2.将此值与信任点关联。

```
<#root>
```

```
POD2IPN2(config)#
```

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

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

```
ecckeypair ec521-label
```

步骤3.安装CA公钥。

```
<#root>
```

```
POD2IPN2(config)#
```

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

```
input (cut & paste) CA certificate (chain) in PEM format;
```

```
end the input with a line containing only END OF INPUT :
```

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

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUgA1UECBM0Tm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJT+ykksFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatKXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULO/wxMhDTbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
```

```
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAAQDAgAHMBkGCWCGSAGG+EIBDQQMFGpTV1MgTGF iENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLFiNHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8tFITVmAzcX8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1POdsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOX E/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTwLlIt/9T1/F0b0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

**END OF INPUT**

Fingerprint(s): SHA1

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

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

POD2IPN2(config)#

POD2IPN2(config)#

**show crypto ca certificates ec521-tp**

Trustpoint: ec521-tp

CA certificate 0:

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

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

serial=20CD7402C4DA37F5

notBefore=Apr 28 17:05:00 2025 GMT

notAfter=Apr 28 17:05:00 2035 GMT

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

purposes: sslserver sslclient

POD2IPN2(config)#

步骤4.生成交换机身份证书请求。

<#root>

POD2IPN2(config)#

**crypto ca enroll ec521-tp**

Create the certificate request ..

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

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

Please make a note of it.

Password:C1sco.123

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

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

**yes**

The serial number in the certificate will be: FD026490P4T  
Include an IP address in the subject name [yes/no]:

**yes**

ip address:10.225.253.177

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

**no**

The certificate request will be displayed...

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

MIIBtjCCARcCAQAwKTERMA8GA1UEAwwIUE9EMk1QTjIxFDASBgNVBAUTC0ZETzI2NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw70vqIKQ/a22LkgNa9IhqWQvetjxKq485gqTSBEo6Lzpk0hPAGE4jBveNHxYeIA7PfnWvJ7xTBWjDNX/IYBm6E7Hd7q420mCe8Mef+bqJbDj9wzpyEjhI2lIIOxt4814nBxObkIWwYR5cZNiXtLk8P4IMZvPq8jRnELRxd8RGcSTAYBgkqhkiG9w0BCQcxCwwJQZfZy28uMTIzMC0GCSqGSIB3DQEJJDjEGMB4wHAYDVR0RAQH/BIwEIIIEUE9EMk1QTjKHBArh/bEwCgYIKoZIZj0EAwIDgYwAMIGIAkIAtzQ/knrW2ovCvohaUq1v2cr0n3NenS/44lu1+3H1y52vn4Rm4CGU3wkzXU3qG03YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfjb5rwPIC5tvXS/A8upqIzqc0yt30hpaDDOTWzzvZY7qFf1CO15p6pvUpHiqqoZNg59xhNdM1CQSyk0g==

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

步骤5.导入由CA签名的交换机身份证书。

&lt;#root&gt;

POD2IPN2(config)#

```
crypto ca import ec521-tp certificate
```

input (cut & paste) certificate in PEM format:

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

MIIDzTCCAbwgAwIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAKGA1UE  
BhMCVVMxZzFVbG9uVBAgTdk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo  
MQ4wDAYDVQQKEwVdaXNjbzEMMAoGA1UECxMDU1ZTRMRiEAYDVQQDEw1TV1MgTGFi  
Q0EwHhcNMjUwNTA3MTkxMDAwHhcNMjUwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ  
T0QySVBOMjEUMBIGA1UEBRMLRkRPMjY0OTBQNFQwZSwEYAHKCoZIZjOCAQYFK4EE  
ACMDgYYABAEZhPSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjov0mQ6E8  
AYTiMG940fFh4gDs981a8nvFMFaMM1f8hgGboTsd3urjY6YJ7wx5/5uokF0n3D0n  
ISOEjaUgihe3jzXiCHE5uQhZbJH1xk0iJdMuTw/ggxm8+ryNGcQtHF3xEaNAMD4w  
HgYJYIZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTACBgNVHREBAf8EEjAQgggQ  
T0QySVBOMocECuH9sTANBgbkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7  
8uai/pF7VQC8NSCd0Kqr4w4+695ZjJuzqFL3msod0QK0EdgxpQ4+pEa5msRtK0i8  
mms2X/Px3/ESHxoHrZ01PUXNTyZidXpGd/yTrdQA15JzpW4pEudrbCJMZEETqoP  
wD+40E8vKoYegyw1DrpRZ0ZG1usZczuUhLZ8orkjXmHC26Q5aqiCKkyg10Nt6nb  
1iToeYy2Q0cTesSZCKvRBv6Ewj5JuSLeMURyB4GHY+LT+A9UNmEUM2n+OSVEL329  
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61Ln1VxhXombiS6  
INoa0GvQONrl+1FT8ADIdZ/Ukd5UbhC9bh/sYzf4MWtkK1wV016Hv7vGpSMYonD6  
a271im+tJPyKnnezQ60yKz1GqSL/Ta6J0dip/fEYp8UmRq9InDh23gDjqrojlW7k  
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJT1nuk5KCqFx//4P7mAoyZYiTIDp1pkYS  
VK65fJKD+pYxIhSP9wN8rnwtzSCwb0Z78sg006Y6wIXyTP0UB3FWhd+GxtTkmEce  
ZnA0baxpqrg51hpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFiSnch

```
1fKuuebdZkbwz72r70yyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

验证交换机身份证书是否已注册。

```
<#root>
```

```
POD2IPN2(config)#
```

```
show crypto ca certificates ec521-tp
```

```
Trustpoint: ec521-tp
```

```
certificate:
```

```
subject=CN = POD2IPN2, serialNumber = FD026490P4T
```

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

```
serial=0BACD2EFA5D80E6F
```

```
notBefore=May 7 19:10:00 2025 GMT
```

```
notAfter=May 7 19:10:00 2026 GMT
```

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

```
purposes: sslserver sslclient
```

```
CA certificate 0:
```

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

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

```
serial=20CD7402C4DA37F5
```

```
notBefore=Apr 28 17:05:00 2025 GMT
```

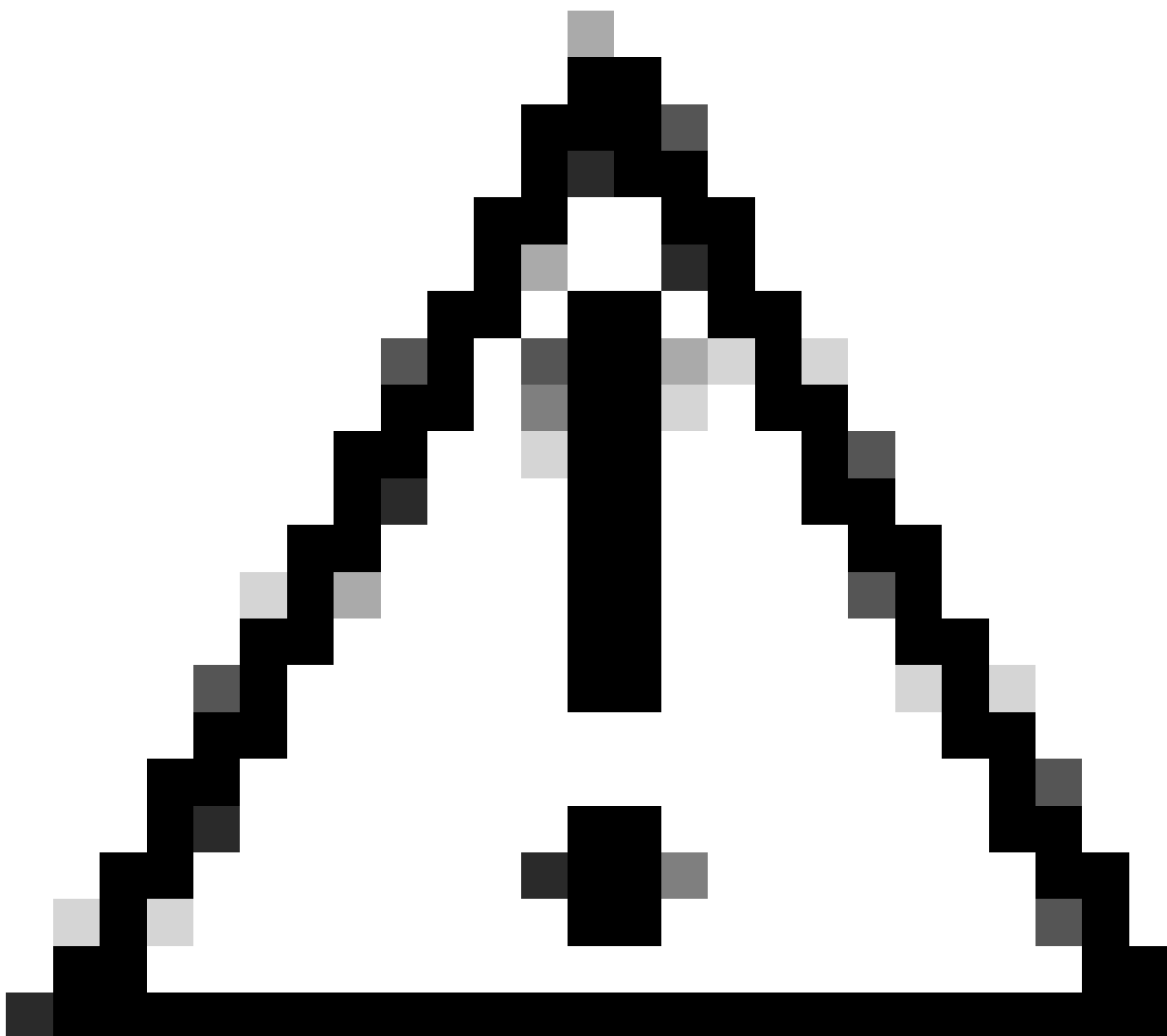
```
notAfter=Apr 28 17:05:00 2035 GMT
```

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

```
purposes: sslserver sslclient
```

```
POD2IPN2(config)#
```

## TACACS+ TLS配置



警告：使用本地凭证通过控制台执行这些配置更改。

---

步骤1.配置全局tacacs tls。

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server secure tls
```

步骤2.将ISE端口更改为ISE服务器配置的TLS端口。

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

步骤3.将交换机上配置的ISE服务器关联到TLS连接的信任点。

```
<#root>
```

```
POD2IPN2(config)#
```

```
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

步骤4.创建tacacs服务器组。

```
<#root>
```

```
POD2IPN2(config)#
```

```
aaa group server tacacs+ tacacs2
```

```
POD2IPN2(config-tacacs+)#
```

```
server 10.225.253.209
```

```
POD2IPN2(config-tacacs+)#
```

```
use-vrf management
```

步骤 5. 检验配置。

```
<#root>
```

```
POD2IPN2#
```

```
sho run tacacs
```

```
feature tacacs+
```

```
tacacs-server secure tls
```

```
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

```
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

```
aaa group server tacacs+ tacacs2
```

```
server 10.225.253.209
```

```
use-vrf management
```

步骤6.在配置AAA身份验证之前测试远程用户。

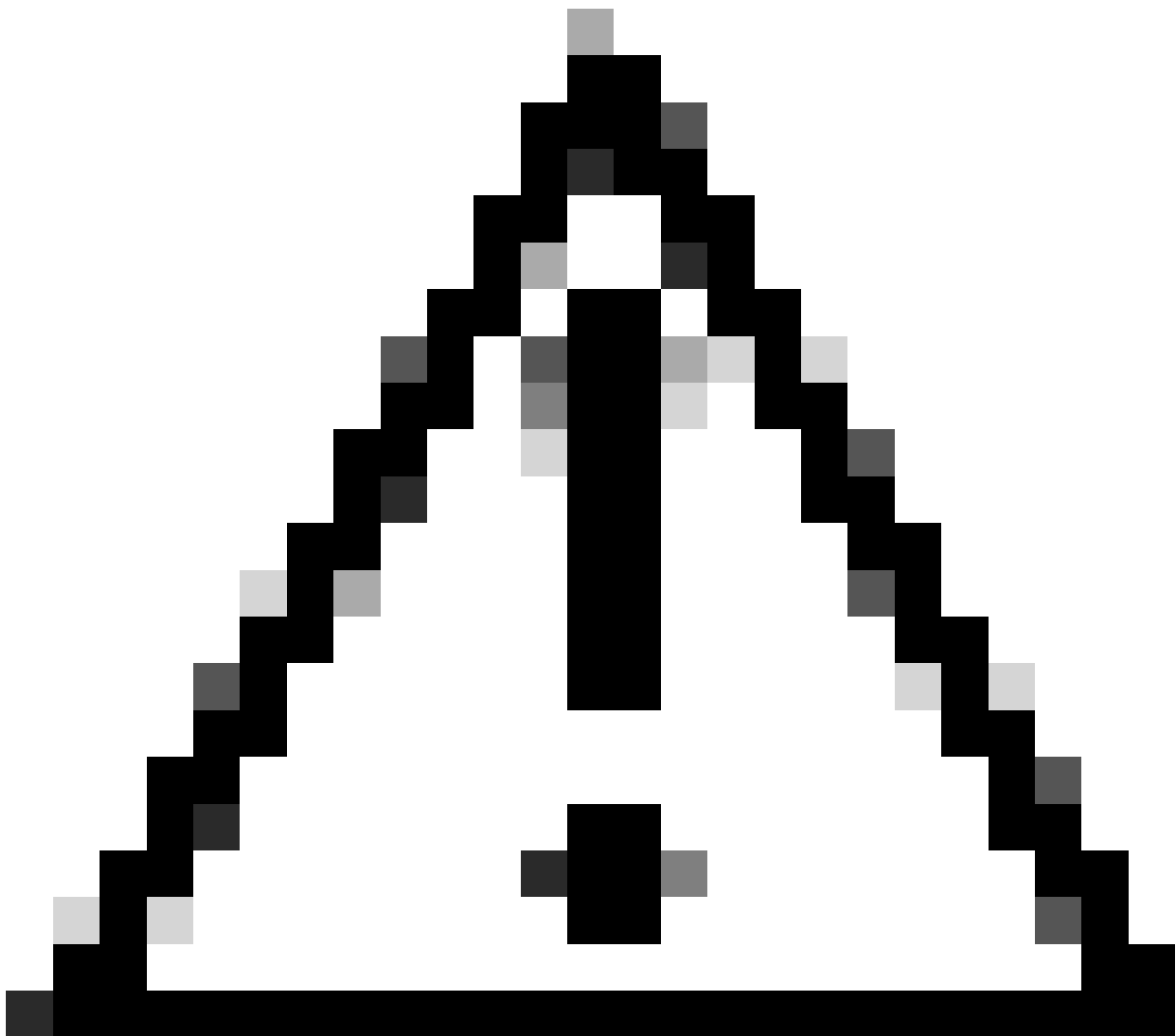
```
<#root>
```

```
POD2IPN2#
```

```
test aaa group tacacs2
```

```
user has been authenticated
POD2IPN2#
```

## AAA 配置



**警告：**在继续AAA配置之前，请确保远程用户身份验证成功。

步骤1.配置AAA远程身份验证。

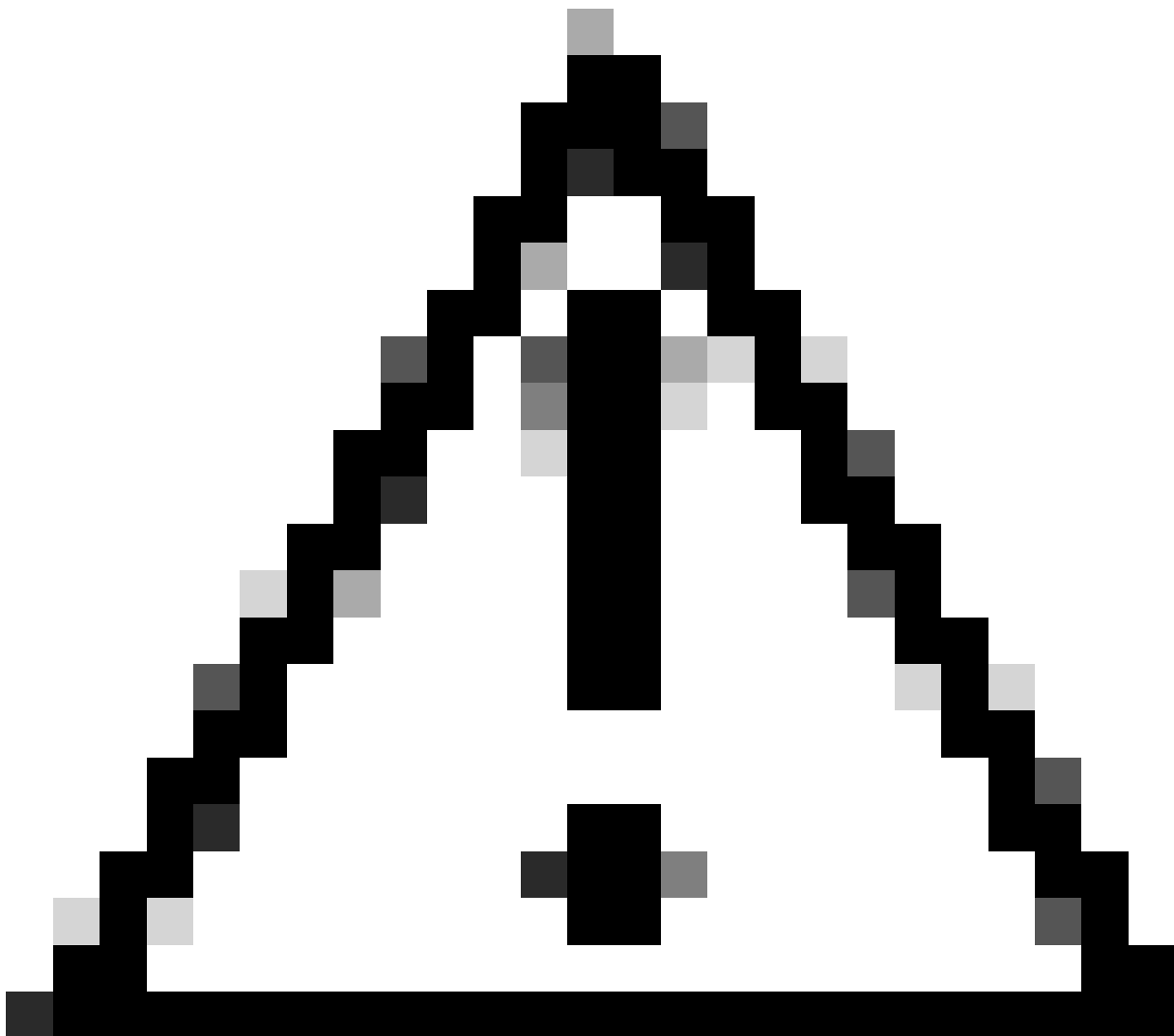
```
<#root>
```

```
POD2IPN2(config)#
```

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

步骤2.测试命令后配置AAA远程授权。

---



警告：确保将授权状态显示为“AAA\_AUTHOR\_STATUS\_PASS\_ADD”。

---

```
<#root>
```

```
POD2IPN2#
```

```
test aaa authorization command-type config-commands default user
```

```
command "feature bgp"
```

```
sending authorization request for: user: pamemart, author-type:3, cmd "feature bgp"  
user pamemart, author type 3, command: feature bgp, authorization-status:0x1(AAA_AUTHOR_STATUS_PASS_ADD)
```

步骤3.配置AAA命令和config-command授权。

```
<#root>
```

```
POD2IPN2(config)#
```

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

```
POD2IPN2(config)#
```

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

## 对NX-OS的用户访问进行测试和故障排除

### 确认

Cisco NX-OS的设备管理配置已完成。您需要验证配置。

步骤1.使用SSH作为各种角色登录到NX-OS设备。

步骤2.一旦进入设备命令行界面(CLI)，验证用户是否有权访问正确的命令。例如，帮助台用户必须能够ping通常IP地址（例如，10.225.253.129），但拒绝显示运行配置。

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

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

## 故障排除

NX-OS配置验证。

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

要显示用户连接和角色，请使用以下命令。

```
show users
show user-account [<user-name>]
A sample output is shown below:
POD2IPN1# show users
NAME LINE TIME IDLE PID COMMENT
Admin-ro pts/5 May 15 23:49 . 16526 (10.189.1.151) session=ssh *
POD2IPN1# show user-account Admin-ro
user:Admin-ro
roles:network-operator
account created through REMOTE authentication
Credentials such as ssh server key will be cached temporarily only for this user account
Local login not possible...
```

以下是TACACS+故障排除中非常有用的调试：

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

启用SSL调试。

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

显示调试文件内容。

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

从ISE GUI导航到操作> TACACS Livelog。此处捕获所有TACACS身份验证和授权请求，详细信息按钮提供关于特定事务通过/失败原因的详细信息。

Identity Services Engine

Operations / TACACS

Evaluation Mode 80 Days

Live Logs

Refresh Every 10 sec... Show Latest 20 reco... Within Last 3 hours

Export To

Filter

| Logged Time                  | Status | Details | Identity | Type           | Authentication Policy | Authorization Policy               | Ise Node | Network Device... | Network D    |
|------------------------------|--------|---------|----------|----------------|-----------------------|------------------------------------|----------|-------------------|--------------|
| ×                            | ▼      |         | Identity | ▼              | Authentication Policy | Authorization Policy               | Ise Node | Network Device N  | Network Dev  |
| May 15, 2025 07:39:57.081 PM | ✓      | 🔒       | Admin-ro | Authorization  |                       | Test NXOS >> Authorization Rule RO | ISE1     | POD2IPN1          | 10.225.253.1 |
| May 15, 2025 07:39:57.061 PM | ✓      | 🔒       | Admin-ro | Authentication | Test NXOS >> Default  |                                    | ISE1     | POD2IPN1          | 10.225.253.1 |
| May 15, 2025 07:39:54.462 PM | ✓      | 🔒       | pamemart | Authorization  |                       | Test NXOS >> Authorization Rule RW | ISE1     | POD2IPN1          | 10.225.253.1 |
| May 15, 2025 07:39:54.443 PM | ✓      | 🔒       | pamemart | Authentication | Test NXOS >> Default  |                                    | ISE1     | POD2IPN1          | 10.225.253.1 |

对于历史报告：导航到工作中心(Work Centers)>设备管理(Device Administration)>报告(Reports)>设备管理(Device Administration)以获取身份验证、授权和记帐报告。

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 80 Days

OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork ResourcesPolicy ElementsDevice Admin Policy SetsReportsSettings

Export SummaryMy Reports>Reports>Device Administration Reports>Authentication SummaryTACACS AccountingTACACS AuthenticationTACACS AuthorizationTACACS Command AccountingTop N Authentication by Failure ReasonTop N Authentication by Network DeviceTop N Authentication by UserScheduled Reports>

TACACS Authentication

From 2025-05-15 00:00:00.0 To 2025-05-15 20:00:45.0  
Reports exported in last 7 days 0

FilterRefresh

| Logged Time             | Status | Details | Identity | Authentication Policy | ISE Node | Network Device Name | Network Device IP | Failure |
|-------------------------|--------|---------|----------|-----------------------|----------|---------------------|-------------------|---------|
| ×                       | Today  | ×       | Identity | Authentication Policy | ISE Node | Network Device Name | Network Device IP | Failure |
| 2025-05-15 19:39:57.061 | ✓      | 🔒       | Admin-ro | Test NXOS >> Default  | ISE1     | POD2IPN1            | 10.225.253.176    |         |
| 2025-05-15 19:39:54.443 | ✓      | 🔒       | pamemart | Test NXOS >> Default  | ISE1     | POD2IPN1            | 10.225.253.176    |         |
| 2025-05-15 19:39:43.001 | ✓      | 🔒       | pamemart | Test NXOS >> Default  | ISE1     | POD2IPN1            | 10.225.253.176    |         |
| 2025-05-15 19:35:39.809 | ✓      | 🔒       | pamemart | Test NXOS >> Default  | ISE1     | POD2IPN1            | 10.225.253.176    |         |
| 2025-05-15 18:49:11.209 | ✓      | 🔒       | pamemart | Test NXOS >> Default  | ISE1     | POD2IPN1            | 10.225.253.176    |         |
| 2025-05-15 18:49:10.303 | ✓      | 🔒       | Admin-ro | Test NXOS >> Default  | ISE1     | POD2IPN1            | 10.225.253.176    |         |

## 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）。