

在具有ISE的IOS XE裝置上通過TLS 1.3配置TACACS+

目錄

[簡介](#)

[概觀](#)

[使用本指南](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[授權](#)

[第1部分 — 為裝置管理配置ISE](#)

[生成TACACS+伺服器身份驗證的證書簽名請求](#)

[上傳用於TACACS+伺服器身份驗證的根CA證書](#)

[將簽名證書簽名請求\(CSR\)繫結到ISE](#)

[啟用TLS 1.3](#)

[在ISE上啟用裝置管理](#)

[啟用TLS上的TACACS](#)

[建立網路裝置和網路裝置組](#)

[配置身份庫](#)

[設定TACACS+設定檔](#)

[IOS XE RW — 管理員設定檔](#)

[IOS XE RO — 操作員配置檔案](#)

[配置TACACS+命令集](#)

[CISCO IOS XE RW — 管理員命令集](#)

[CISCO IOS XE RO — 運算子命令集](#)

[配置裝置管理策略集](#)

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

[配置方法1 — 裝置生成的金鑰對](#)

[TACACS+伺服器組態](#)

[信任點配置](#)

[採用TLS配置的TACACS和AAA](#)

[組態方法2 - CA產生的金鑰對](#)

[採用TLS配置的TACACS和AAA](#)

[驗證](#)

簡介

本檔案將介紹以思科身份服務引擎(ISE)作為伺服器、以思科IOS® XE裝置作為使用者端的TACACS+通過TLS的範例。

概觀

終端存取控制器存取控制系統Plus(TACACS+)通訊協定[RFC8907]透過一個或多個TACACS+伺服器，啟用路由器、網路存取伺服器和其他網路裝置的集中化裝置管理。它提供專為裝置管理使用案例定製的身份驗證、授權和記帳(AAA)服務。

使用TLS 1.3的TACACS+ [RFC8446]通過引入安全傳輸層來增強協定，從而保護高度敏感的資料。此整合可確保TACACS+客戶端和伺服器之間的連線和網路流量的機密性、完整性和身份驗證。

使用本指南

本指南將活動分為兩部分，使ISE能夠管理基於Cisco IOS XE的網路裝置的管理訪問。

- 第1部分 — 為裝置管理員配置ISE
- 第2部分 — 為使用TLS的TACACS+配置Cisco IOS XE

必要條件

需求

通過TLS配置TACACS+的要求：

- 證書頒發機構(CA)，用於簽署TLS上TACACS+用於簽署ISE和網路裝置證書的證書。
- 來自證書頒發機構(CA)的根證書。
- 網路裝置和ISE具有DNS可達性並可解析主機名。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ISE VMware虛擬裝置，版本3.4補丁2
- Cisco IOS XE軟體版本17.15+

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

授權

「裝置管理」許可證允許您在策略服務節點上使用TACACS+服務。在高可用性(HA)獨立部署中，裝置管理許可證允許您在HA對中的單個策略服務節點上使用TACACS+服務。

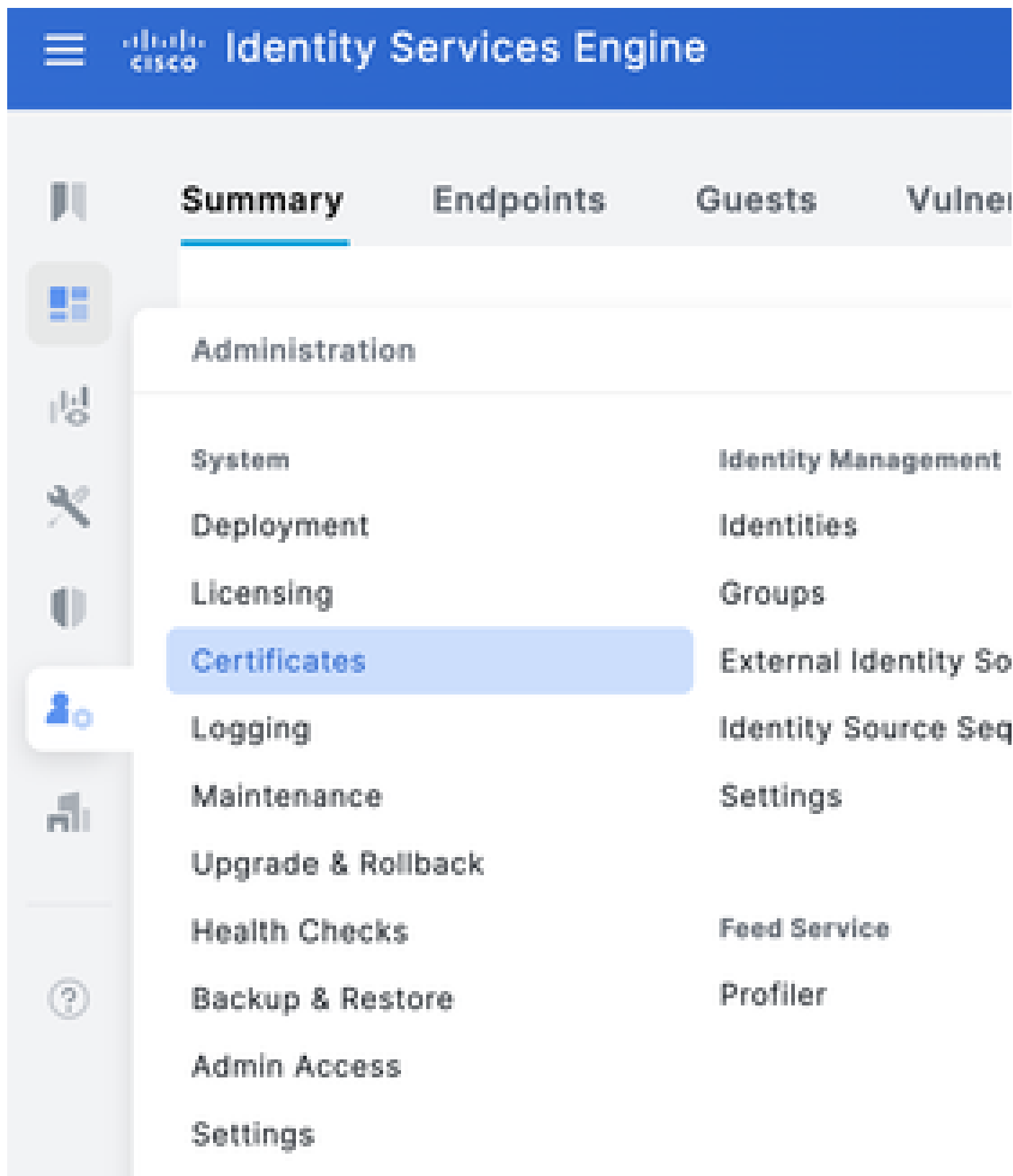
第1部分 — 為裝置管理配置ISE

生成TACACS+伺服器身份驗證的證書簽名請求

步驟1.使用其中一個受支援的瀏覽器登入ISE管理員Web門戶。

預設情況下，ISE對所有服務使用自簽名證書。第一步是產生憑證簽署請求(CSR)，讓我們的憑證授權單位(CA)簽署該請求。

步驟2.導覽至管理>系統>憑證。



步驟 3. 在Certificate Signing Requests下，按一下Generate Certificate Signing Request。



步驟4.選擇TACACS inUsage。

Usage

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

Allow Wildcard Certificates ☐ 

步驟5.選擇將啟用TACACS+的PSN。

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ ISE1	ISE1#TACACS

步驟6.使用適當資訊填充Subject欄位。

Subject

Common Name (CN)
\$FQDN\$



Organizational Unit (OU)
CX



Organization (O)
Cisco



City (L)
Raleigh

State (ST)
North Carolina

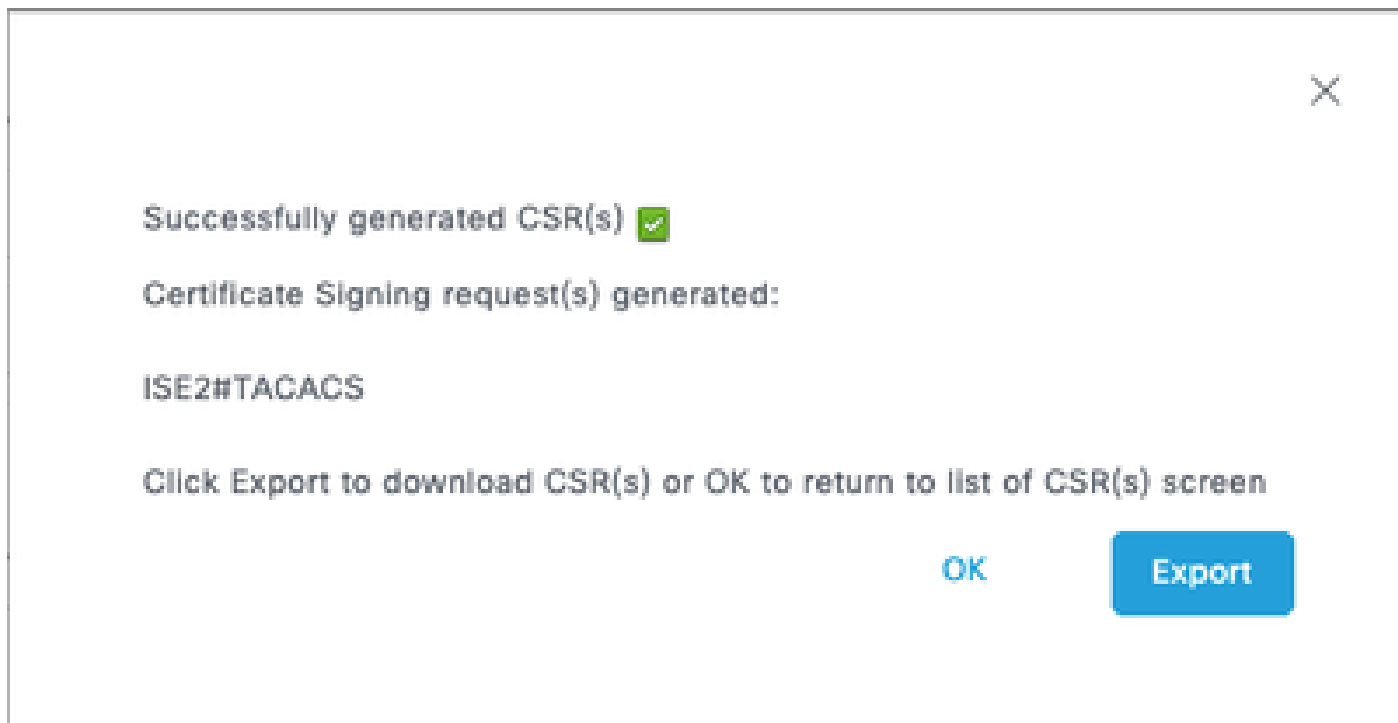
Country (C)
US

步驟7.在使用者替代名稱(SAN)下新增DNS名稱和IP位址。

Subject Alternative Name (SAN)

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

步驟8.按一下Generate，然後Export。



現在，您可以讓證書頒發機構(CA)簽署證書(CRT)。

上傳用於TACACS+伺服器身份驗證的根CA證書

步驟1.導覽至Administration > System > Certificates。在Trusted Certificates下，按一下Import。

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐	Amazon root CA	Infrastructure Cisco Services	06 6C 9F CF ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2015	Sun, 17 Jan 2...	Enr
☐	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2...	Enr
☐	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	Enr
☐	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Enr
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 20...	Cisco Root CA 20...	Fri, 14 May 2004	Mon, 14 May ...	Dis
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 20...	Cisco Root CA 20...	Tue, 9 Aug 2016	Sun, 9 Aug 20...	Enr
☐	Cisco Root CA M1	Cisco Services	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20...	Enr
☐	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Enr
☐	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034	Enr

步驟2.選擇簽署TACACS憑證簽署請求(CSR)的憑證授權單位(CA)發出的憑證。確保信任在ISE內進行身份驗證 選項已啟用。

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

步驟3.按一下Submit。憑證現在必須出現在Trusted Certificates下。

The screenshot shows the 'Trusted Certificates' section in the Cisco ISE Administration console. The left sidebar contains navigation links like 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area shows a table of trusted certificates. The table has columns for 'Friendly Name', 'Trusted For', 'Serial Number', 'Issued To', 'Issued By', 'Valid From', 'Expiration Date', and 'Status'. One certificate is listed with the friendly name 'CN=SVS LabCA, OU=SVS, O=Cisco, L=...', serial number '20 CD 74 02 ...', issued to 'SVS LabCA', issued by 'SVS LabCA', valid from 'Mon, 28 Apr 2025', and expires on 'Sat, 28 Apr 2025'.

將簽名證書簽名請求(CSR)繫結到ISE

簽名證書簽名請求(CSR)後，您可以在ISE上安裝已簽名的證書。

步驟1.導覽至Administration > System > Certificates。在Certificate Signing Requests下，選擇在上一步中產生的TACACS CSR，然後按一下「Bind Certificate」。

The screenshot shows the 'Certificate Signing Requests' section in the Cisco ISE Administration console. The left sidebar contains navigation links like 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area shows a table of certificate signing requests. The table has columns for 'Friendly Name', 'Certificate Subject', 'Key Length', 'Portal gro...', 'Timestamp', and 'Host'. A 'Generate Certificate Signing Requests (CSR)' button is visible at the top. Below the table, there is a 'Bind Certificate' button highlighted with a red box.

步驟2.選擇已簽名的證書，並確保使用下的TACACS覈取方塊保持選中狀態。

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

Bind CA Signed Certificate

* Certificate File

Friendly Name

Validate Certificate Extensions ☐

Usage

☒ TACACS: Use certificate for TACACS Server

步驟3.按一下「Submit」。如果您收到有關替換現有證書的警告，請按一下Yes繼續。

Warning

The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

Do you wish to replace the existing certificate?

現在必須正確安裝證書。您可以在系統憑證下驗證這一點。

Identity Services Engine Administration / System Evaluation Mode 29 Days

Deployment Licensing **Certificates** Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates**
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- Certificate Authority

System Certificates For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

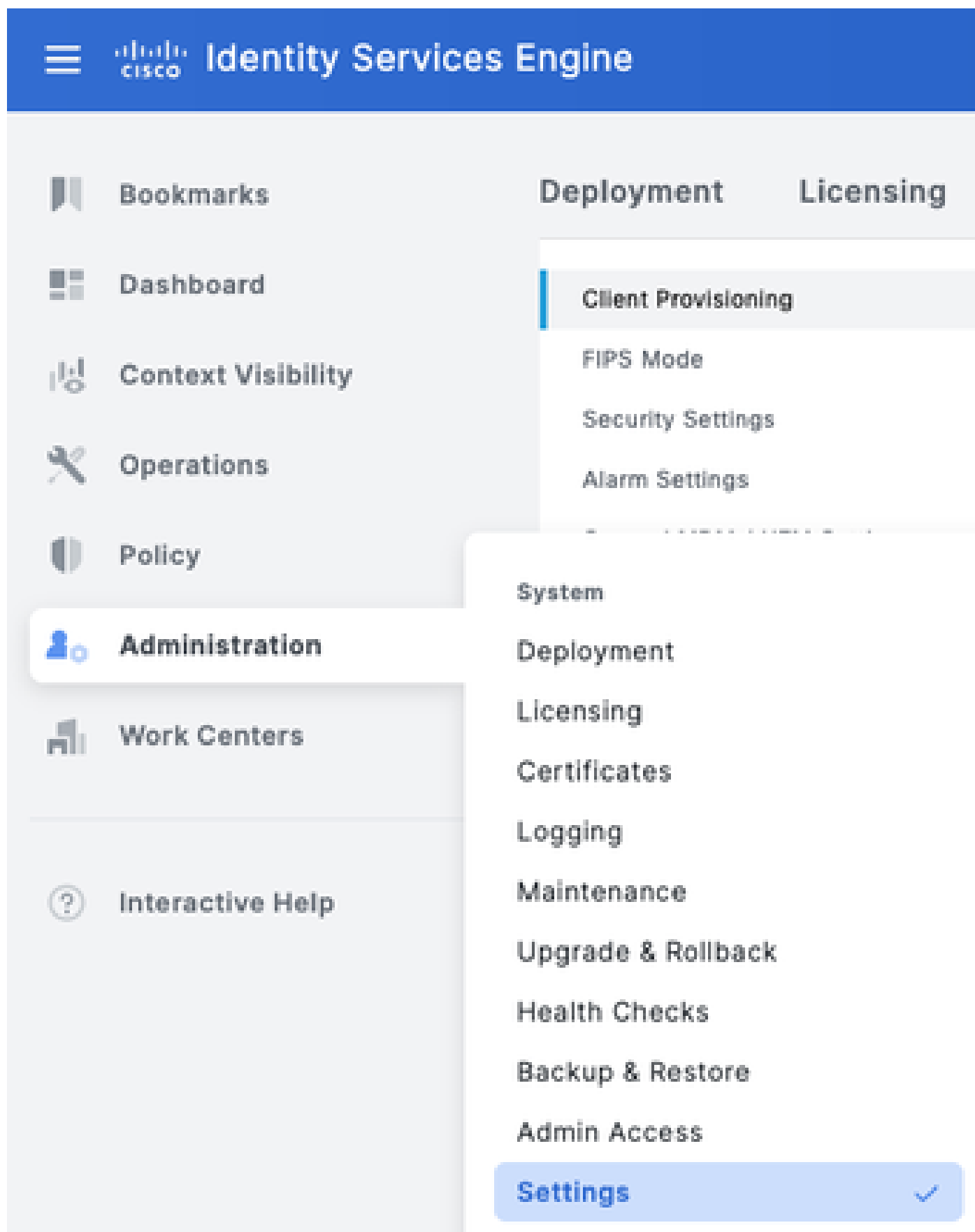
[Edit](#) [+ Generate Self Signed Certificate](#) [+ Import](#) [Export](#) [Delete](#) [View](#)

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
ISE1	C=US, ST=NC, L=Raleigh, O=Cisco, OU=SVS, CN=ISE1.lab@ISE1.lab#00010	TACACS	ISE1.lab	ISE1.lab	Wed, 10 Sep 2025	Fri, 10 Sep 2027	Active

啟用TLS 1.3

ISE 3.4.x中預設未啟用TLS 1.3。必須手動啟用。

步驟1.導覽至Administration > System > Settings。



步驟2.按一下Security Settings，選中TLS Version Settings下的TLS1.3旁的覈取方塊，然後按一下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

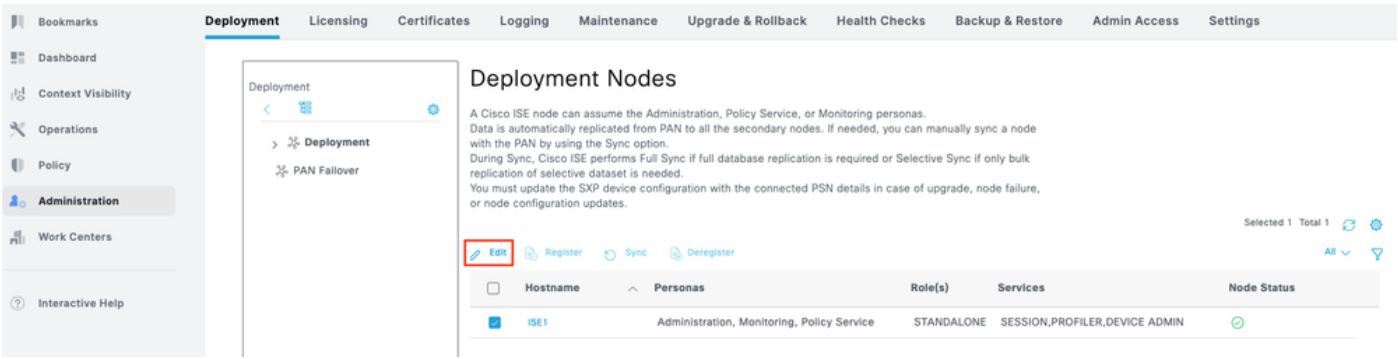


警告：當您更改TLS版本時，思科ISE應用伺服器在所有思科ISE部署電腦上重新啟動。

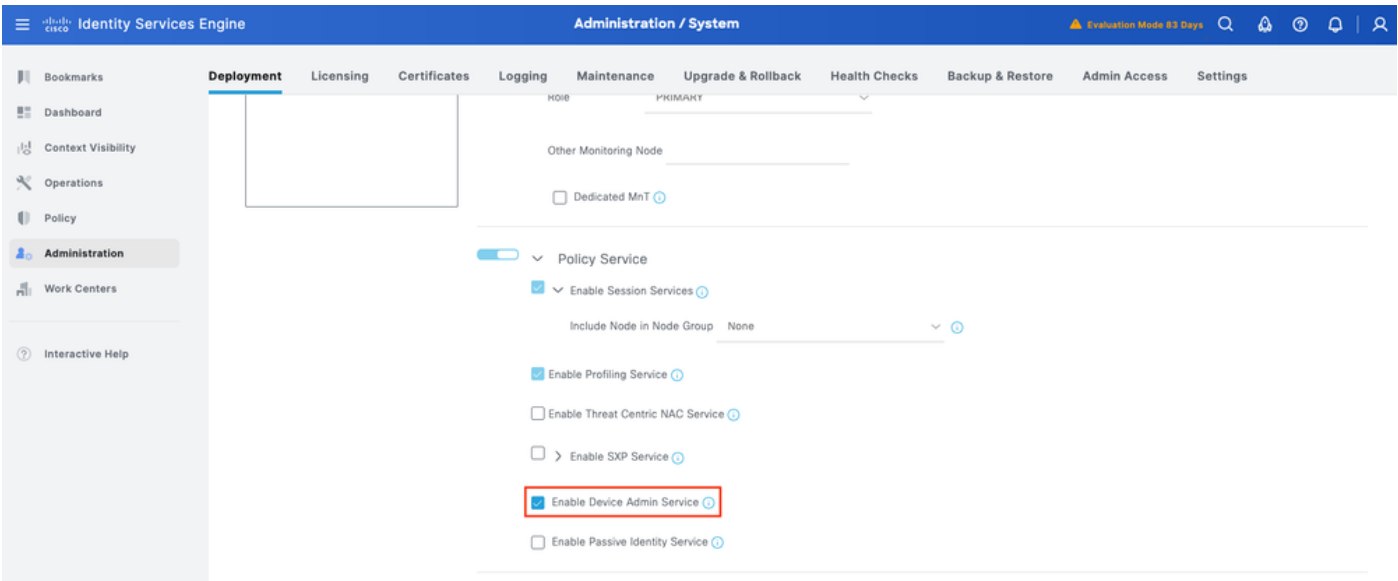
在ISE上啟用裝置管理

裝置管理服務(TACACS+)在ISE節點上預設未啟用。在PSN節點上啟用TACACS+。

步驟1.導航到Administration > System > Deployment。選中ISE節點旁邊的覈取方塊，然後單擊Edit。



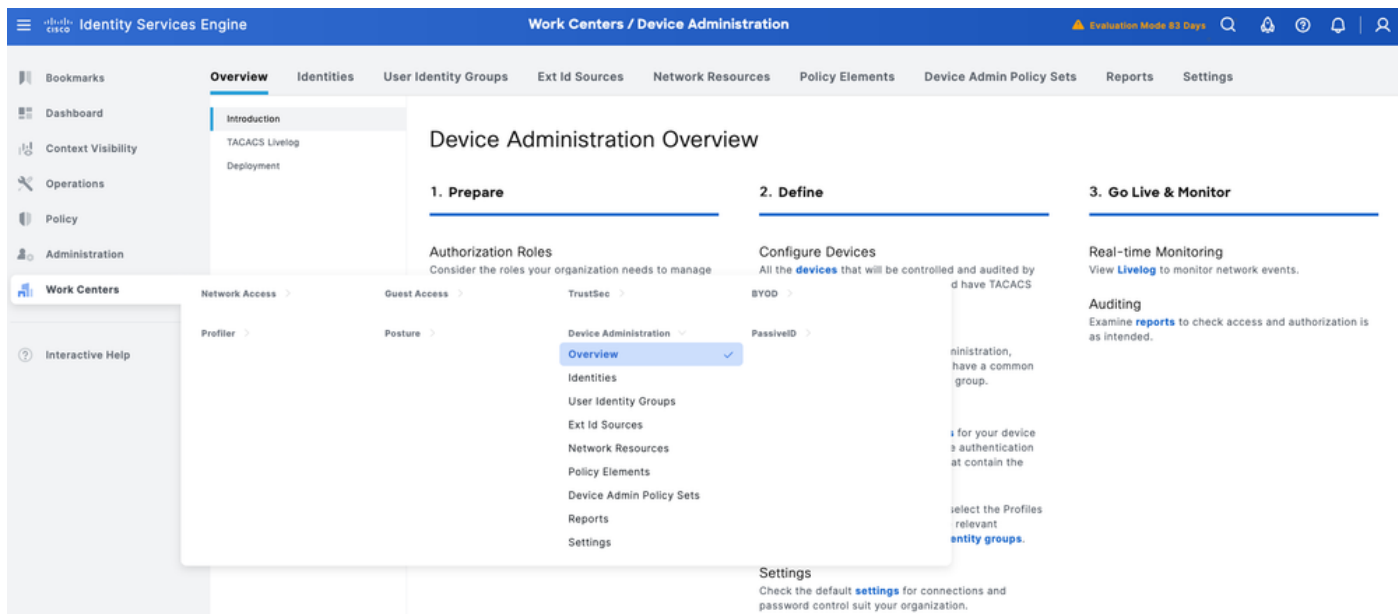
步驟2.在GeneralSettings下，向下滾動並選擇Enable Device Admin Service旁邊的覈取方塊。



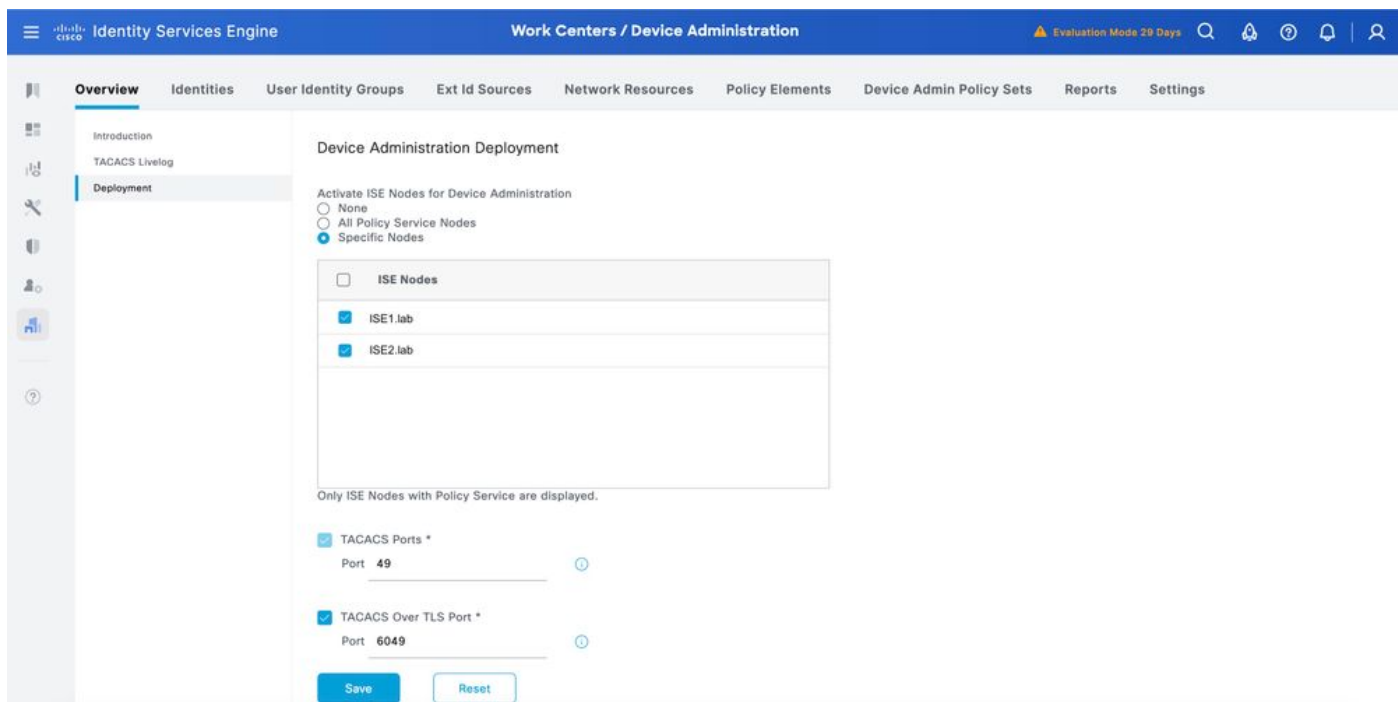
步驟3. 儲存組態。裝置管理服務現在在ISE上啟用。

啟用TLS上的TACACS

步驟1.導航至工作中心>裝置管理>概述。



步驟2. 按一下Deployment。選擇要通過TLS啟用TACACS的PSN 節點。



步驟3. 保留預設埠6049，或者為TLS上的TACACS指定不同的TCP埠，然後按一下Save。

建立網路裝置和網路裝置組

ISE提供具有多個裝置組層次結構的強大裝置分組。每個層次代表網路裝置的不同、獨立的分類。

步驟1. 導覽至工作中心>裝置管理>網路資源。按一下Network Device Groups，然後建立一個名稱為IOS XE的群組。

Add Group

Name*

IOSXE



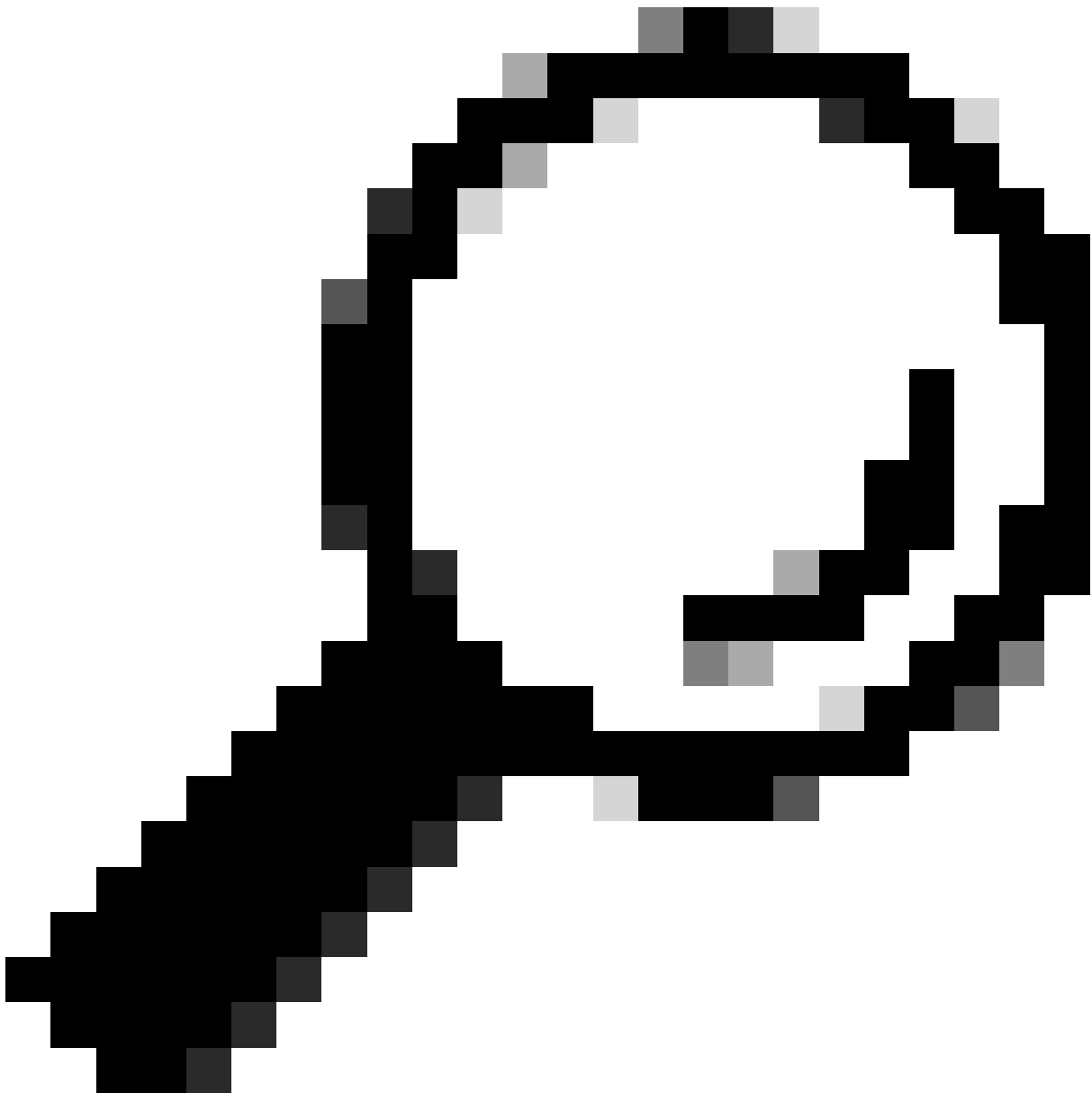
Description

Parent Group*

Select Group or Add as root group

Cancel

Save



提示：所有裝置型別和所有位置是ISE提供的預設層次結構。您可以新增自己的層次結構並定義各種元件，以標識稍後可在「策略條件」中使用的網路裝置

步驟2.現在將Cisco IOS XE裝置新增為網路裝置。導航至工作中心(Work Centers)>裝置管理(Device Administration)>網路資源(Network Resources)>網路裝置(Network Devices)。按一下Add新增新的網路裝置。對於此測試，它是SVS_BRPASR1K。

Identity Services Engine

Work Centers / Device Administration

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

More

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices List > SVS_BRPASR1K

Network Devices

NameSVS_BRPASR1K

Description

IP Address

* IP : 10.225.253.180

/ 32

Device ProfileCisco

Model Name

Software Version

Network Device Group

LocationAll Locations

Set To Default

步驟3.輸入裝置的IP地址，並確保對映裝置的位置和裝置型別(IOS XE)。最後，啟用TACACS+通過TLS身份驗證設定。

Identity Services Engine

Work Centers / Device Administration

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)^{*}

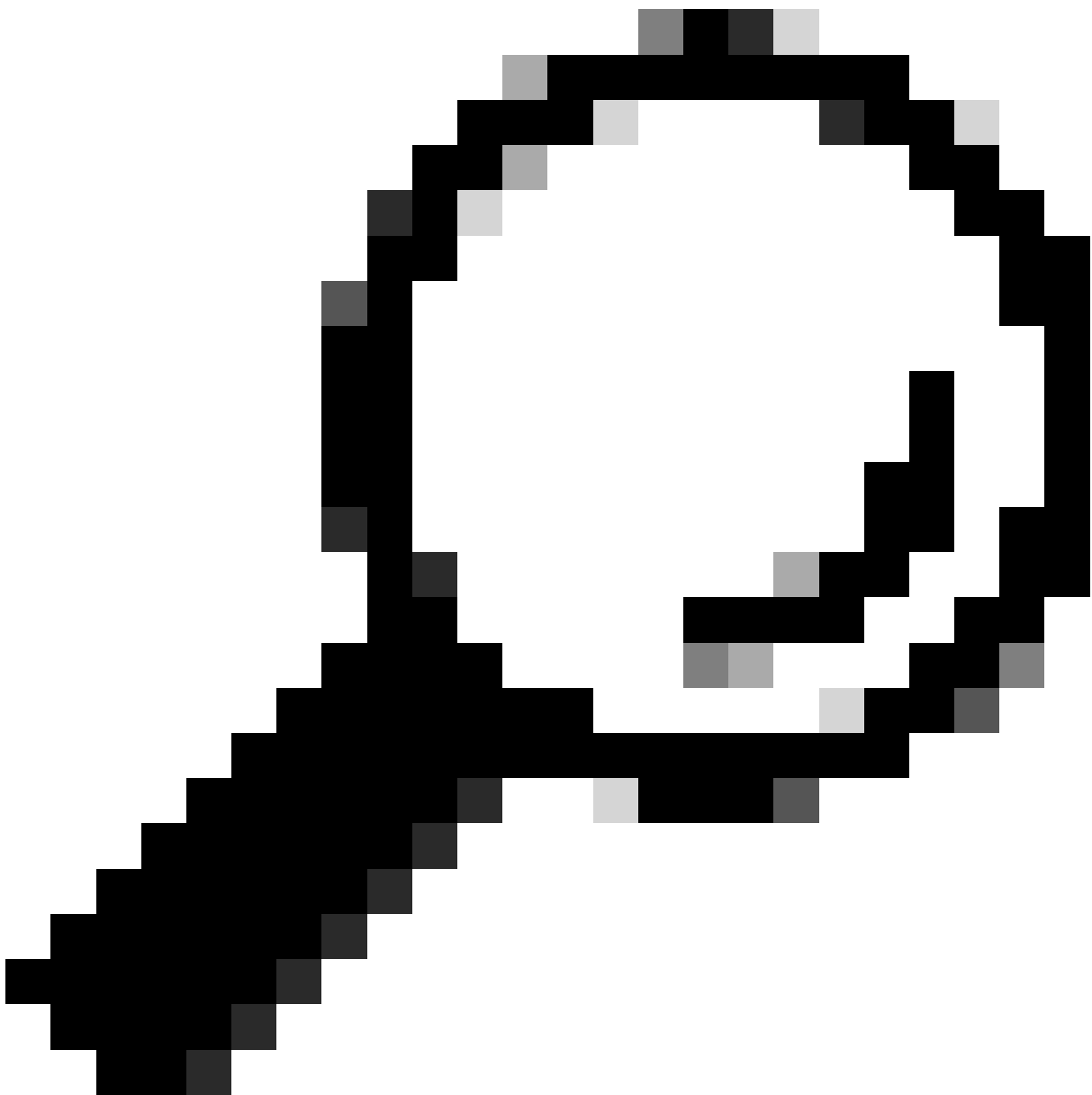
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When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

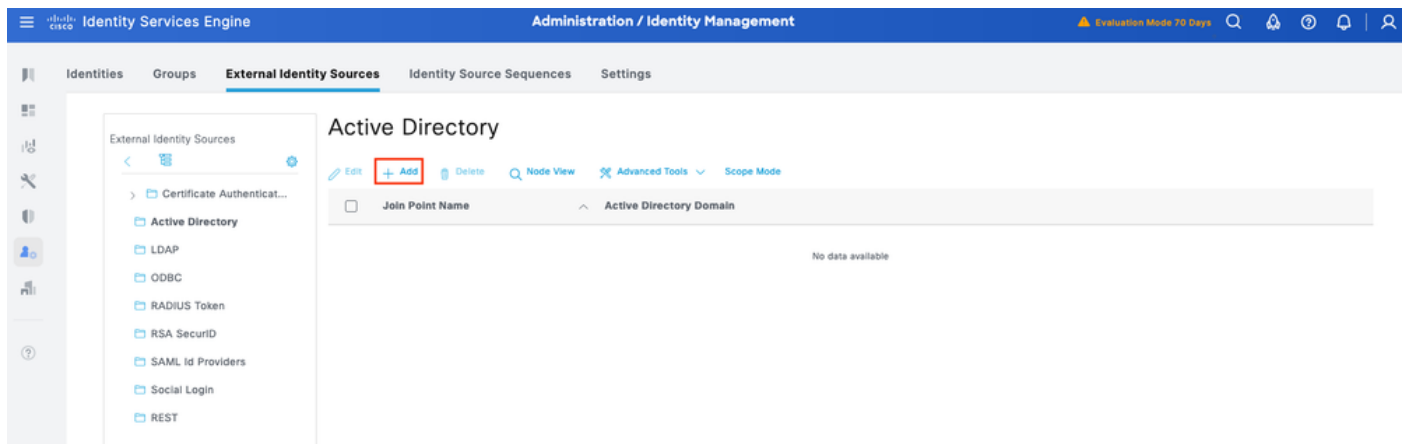


提示：建議啟用單一連線模式，以避免每次向裝置傳送命令時重新啟動TCP會話。

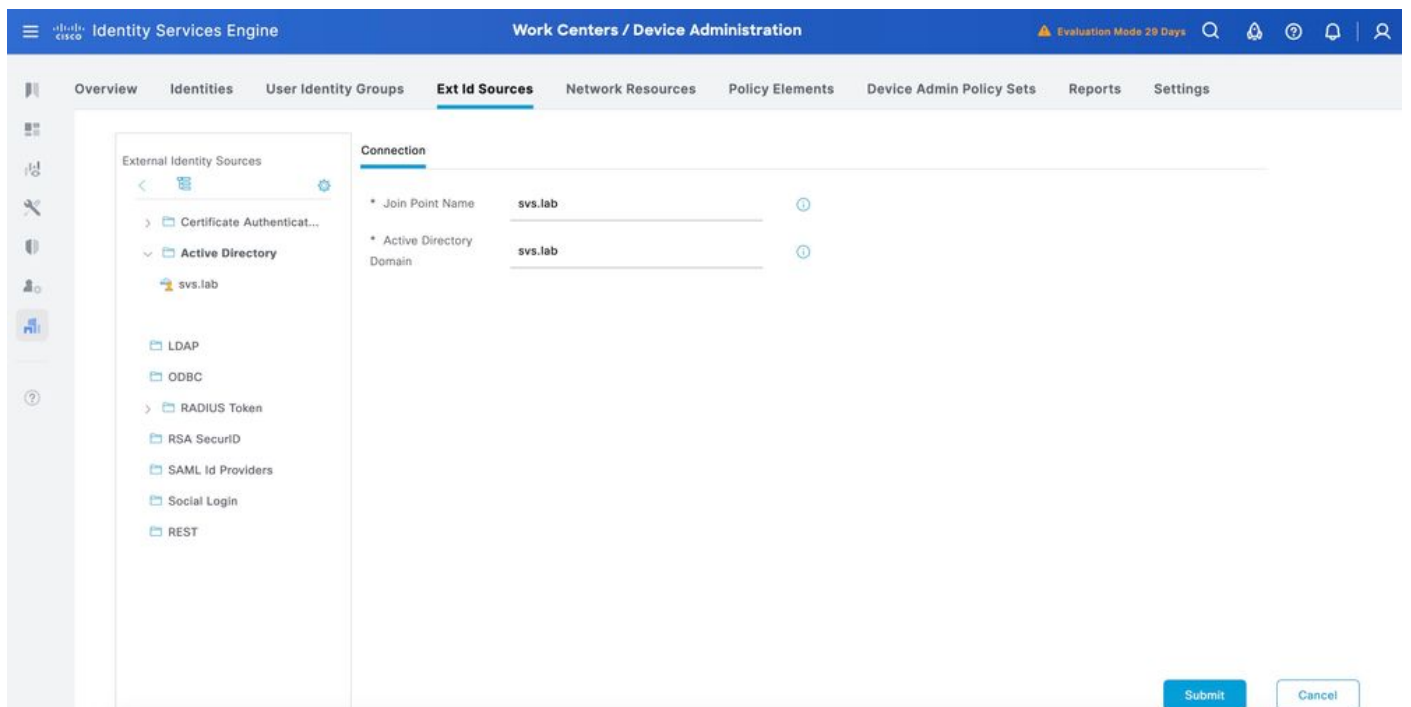
配置身份庫

本節為裝置管理員定義身份儲存，可以是ISE內部使用者和任何支援的外部身份源。此處使用Active Directory(AD) (外部身份源)。

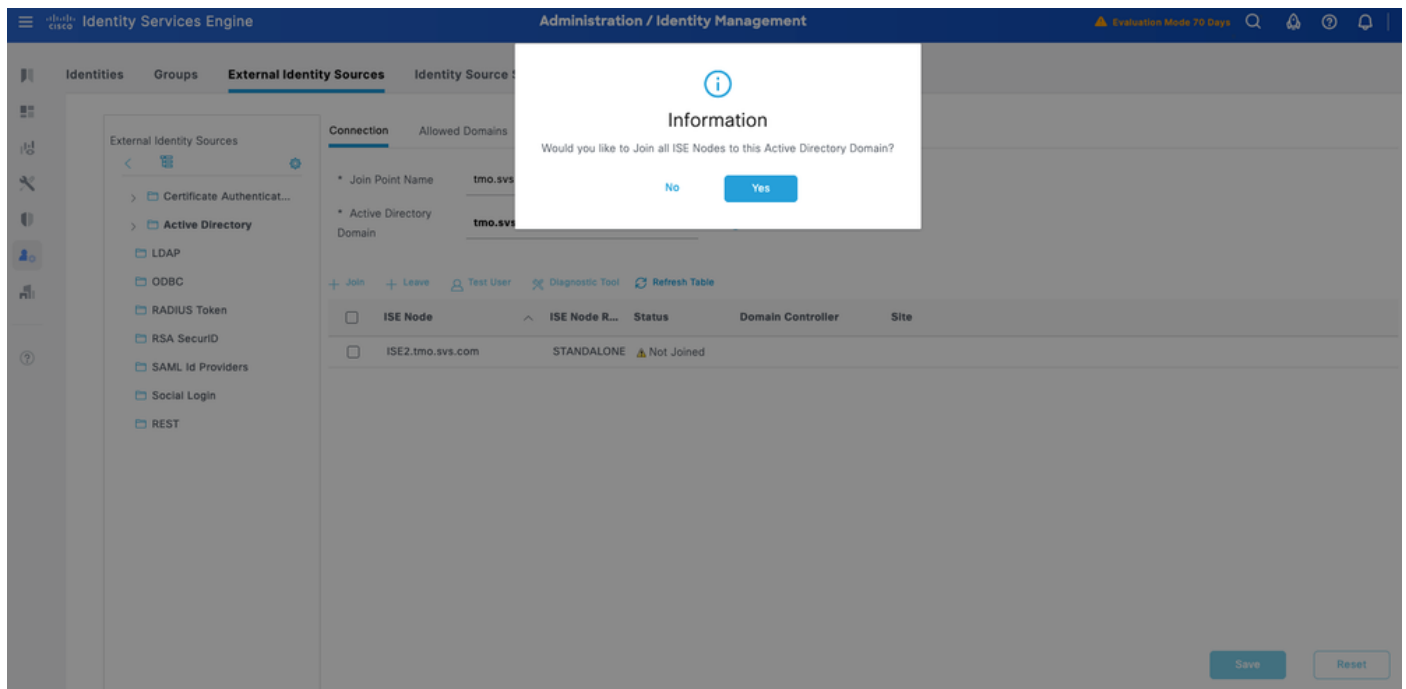
步驟1.導航到管理>身份管理>外部身份庫> Active Directory。按一下新增以定義新的AD關節點。



步驟2.指定加入點名稱和AD域名，然後按一下Submit。



步驟3.出現提示時，按一下Yes Would you like to Join all ISE Nodes to this Active Directory Domain?



步驟4.輸入具有AD加入許可權的憑證，並輸入Join ISE到AD。檢查「Status (狀態)」以驗證其是否可操作。

×

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

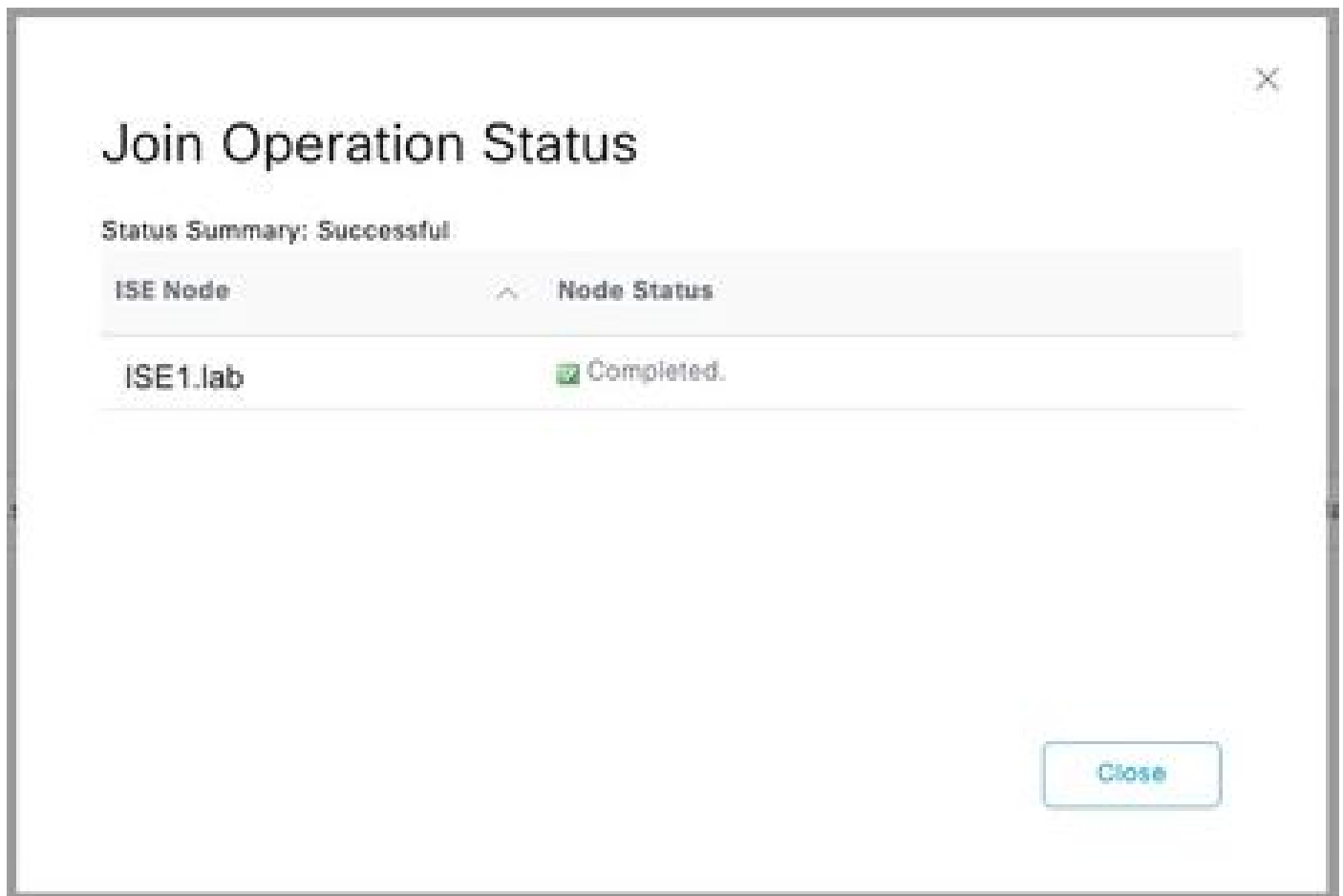
* AD User Name ⓘ administrator

* Password
.....

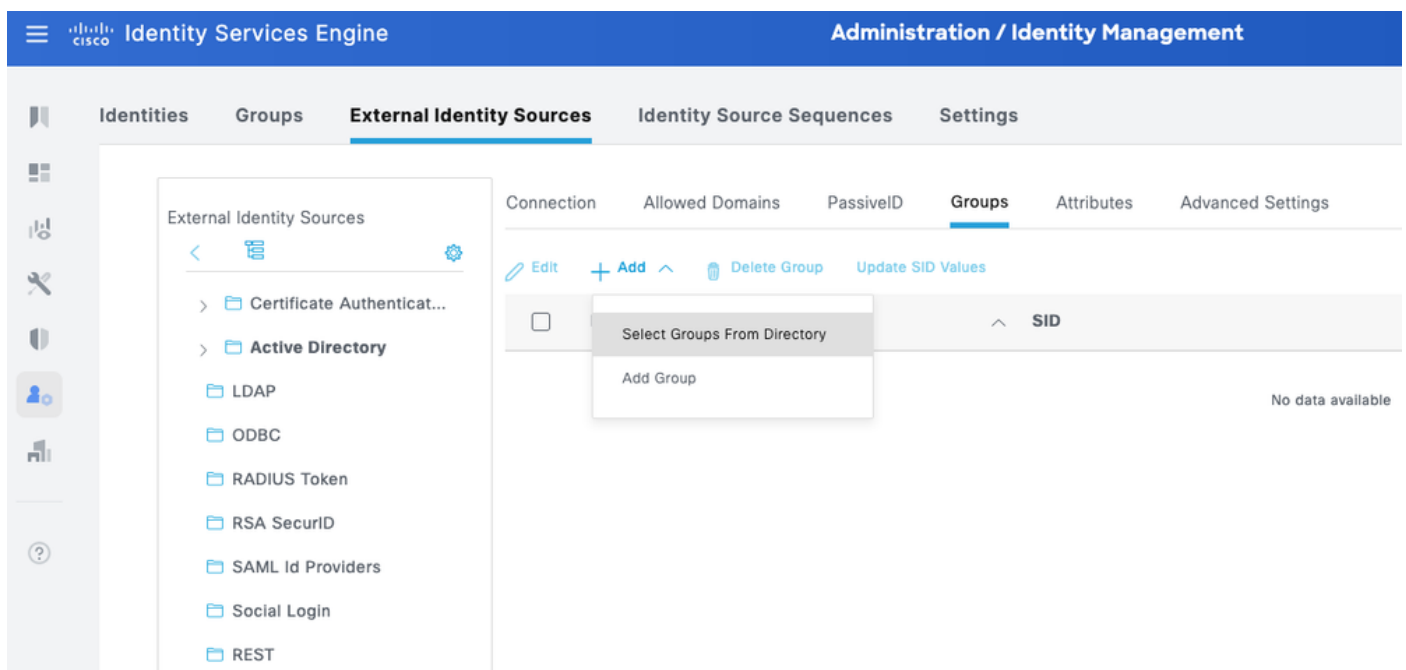
☐ Specify Organizational Unit ⓘ

☒ Store Credentials ⓘ

Cancel OK



步驟5.導航到Groups頁籤，然後點選Add以獲取授權使用者訪問裝置所需的所有組。此示例顯示本指南的授權策略中使用的組



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

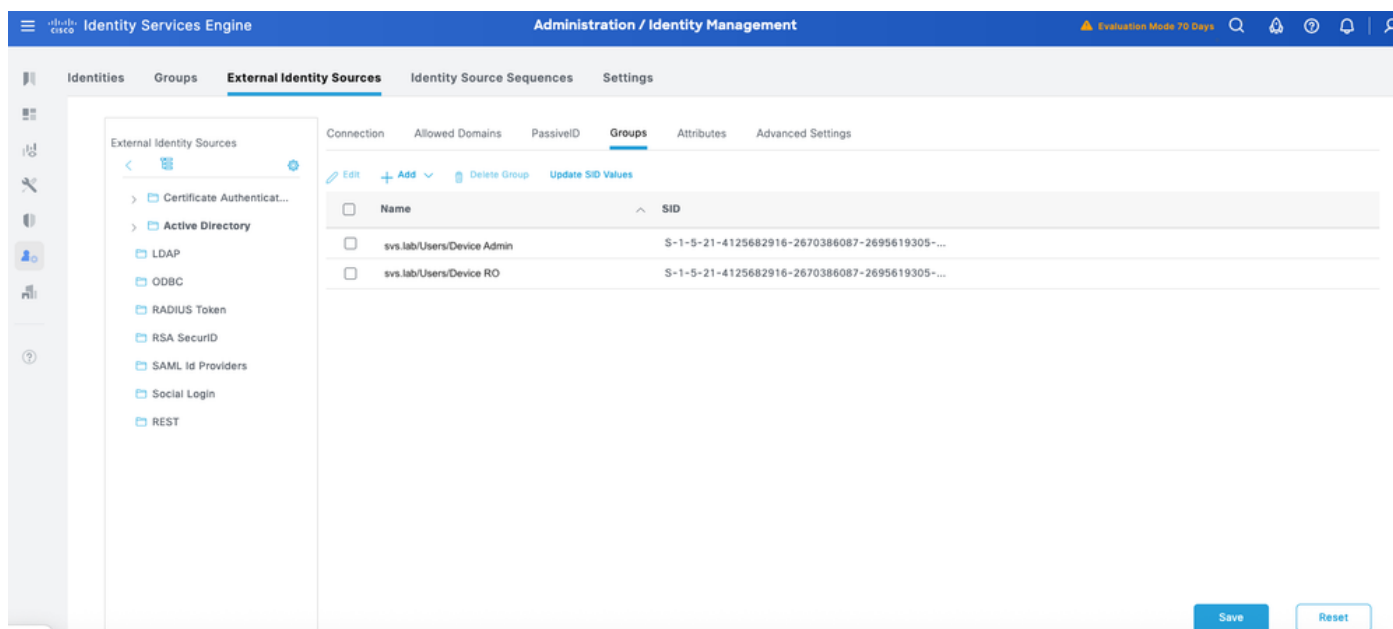
Name SID

Filter Filter

Type

2 Groups Retrieved.

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



設定TACACS+設定檔

您將將TACACS+配置檔案對映到Cisco IOS XE裝置上的兩個主要使用者角色：

- Root System Administrator — 這是裝置中的最高特權角色。具有root系統管理員角色的使用者對所有系統命令和配置功能具有完全管理訪問許可權。
- 操作員 — 此角色適用於出於監控和故障排除目的而需要系統只讀訪問許可權的使用者。

以下內容定義為兩個TACACS+設定檔：IOS XE_RW和IOSXR_RO。

IOS XE_RW — 管理員設定檔

步驟1導覽至工作中心>裝置管理>原則元素>結果> TACACS設定檔。新增一個TACACS設定檔，並將其命名為IOS XE_RW。

步驟3.確認設定並儲存。

IOS XE_RO — 操作員配置檔案

步驟2.檢查並設定預設許可權和最大許可權為1。

步驟3.確認設定並儲存。

Identity Services Engine

Work Centers / Device Administration

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

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

Name
IOSXE_RO
Description
Task Attribute View Raw View
Common Tasks
Common Task Type Shell ▾
☒ Default Privilege 1 ▾ (Select 0 to 15)
☒ Maximum Privilege 1 ▾ (Select 0 to 15)
☐ Access Control List ▾
☐ Auto Command ▾

配置TACACS+命令集

以下內容定義為兩個TACACS+命令集：CISCO_IOS XE_RW 和CISCO_IOS XE_RO。

CISCO_IOS XE_RW — 管理員命令集

步驟1. 導覽至工作中心>裝置管理>原則元素>結果> TACACS命令集。新增一個TACACS命令集，並將其命名為CISCO_IOS XE_RW。

步驟2. 勾選Permit any command that not listed below 覈取方塊（這將允許管理員角色使用任何命令），然後按一下Save。

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

CISCO_IOS XE_RO — 運算子命令集

第1步從ISE UI導航至工作中心>裝置管理>策略元素>結果> TACACS命令集。新增一個TACACS命令集，並將其命名為CISCO_IOS XE_RO。

步驟2. 在Commands區段中，新增一個命令。

步驟3. 從Grant列的下拉選單中選擇Permit，然後在Command列中輸入show;然後按一下check箭頭。

步驟4. 確認資料，然後按一下Save。

Identity Services Engine Work Centers / Device Administration

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

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

TACACS Command Sets > CISCO_IOSXE_RO

Command Set

Name: CISCO_IOSXE_RO

Description:

Commands

Permit any command that is not listed below

Add Trash Edit Move Up Move Down

Grant	Command	Arguments
☐	PERMIT	show

配置裝置管理策略集

預設情況下會啟用「裝置管理」策略集。策略集可以根據裝置型別劃分策略，以簡化TACACS配置檔案的應用。

步驟1.導航至工作中心>裝置管理>裝置管理策略集。新增新的策略集IOS XE裝置。在條件下，指定DEVICE:Device Type EQUALS All Device Types#IOS XE。在Allowed Protocols下，選擇Default Device Admin。

Identity Services Engine Work Centers / Device Administration

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

Policy Sets

Reset Reset Policy Set Hit Counts Save

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

步驟2.按一下Save，然後按一下右箭頭配置此策略集。

步驟3.建立身份驗證策略。對於身份驗證，請使用AD作為ID儲存。保留If Auth fail、If User not found和If Process fail下的預設選項。

Identity Services Engine Work Centers / Device Administration Evaluation Mode 28 Days

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

Policy Sets → IOS-XE devices Reset Reset Policy Set Hit Counts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	IOS-XE devices		DEVICE:Device Type EQUALS All Device TypesIOS-XE	Default Device Admin	0

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default				

svs.lab

Options

- If Auth fail REJECT
- If User not found REJECT
- If Process fail DROP

步驟4.定義授權策略。

根據Active Directory(AD)中的使用者組建立授權策略。

舉例來說：

- AD組裝置RO中的使用者分配有CISCO_IOSXR_RO命令集和IOSXR_RO外殼配置檔案。
- AD組Device Admin 中的使用者分配有CISCO_IOSXR_RW 命令集和IOSXR_RW 外殼配置檔案。

Identity Services Engine Work Centers / Device Administration

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

Policy Sets → IOS-XE devices Reset Reset Policy Set Hit Counts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	IOS-XE devices		DEVICE:Device Type EQUALS All Device TypesIOS-XE	Default Device Admin	0

> Authentication Policy(1)

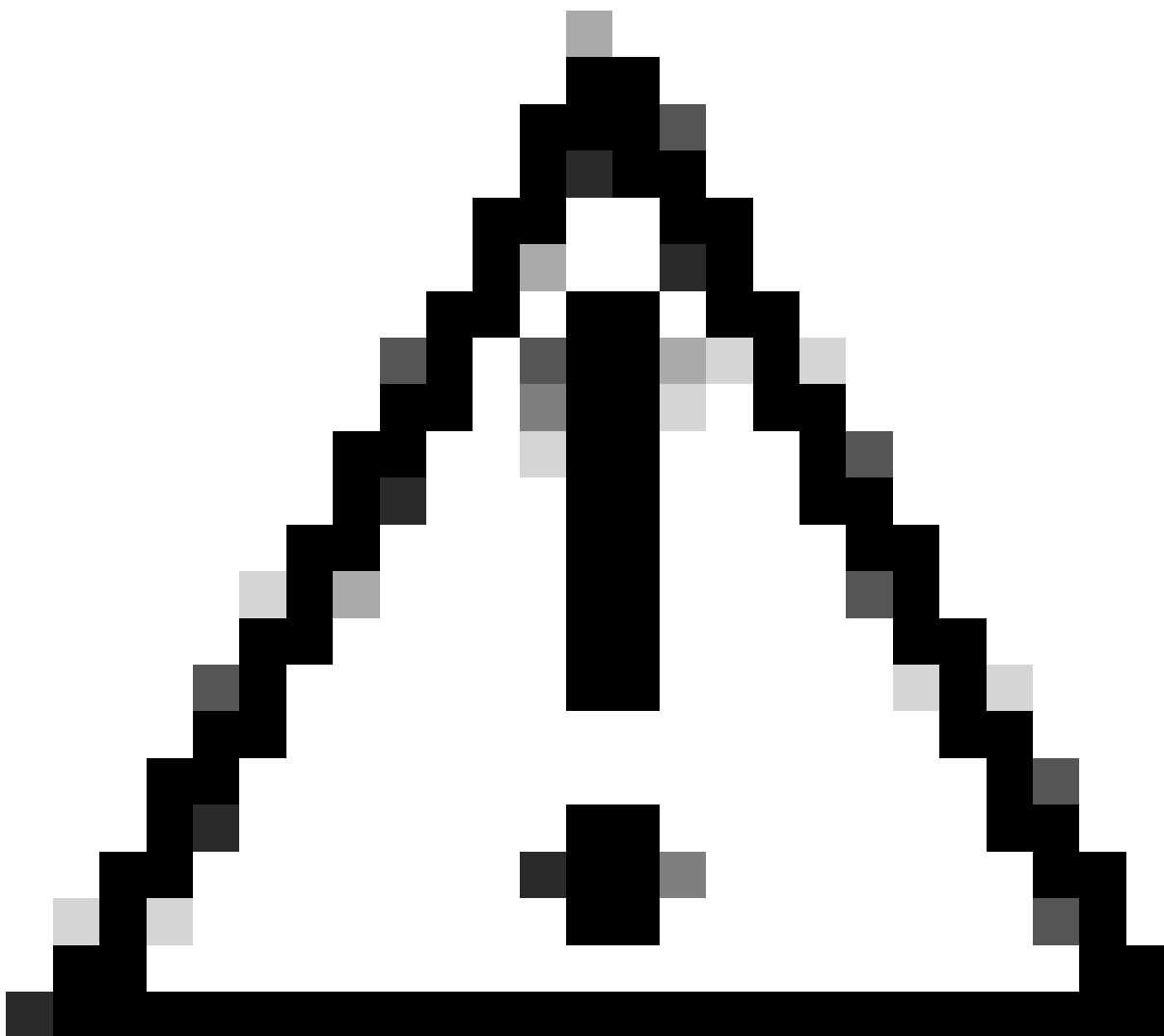
> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

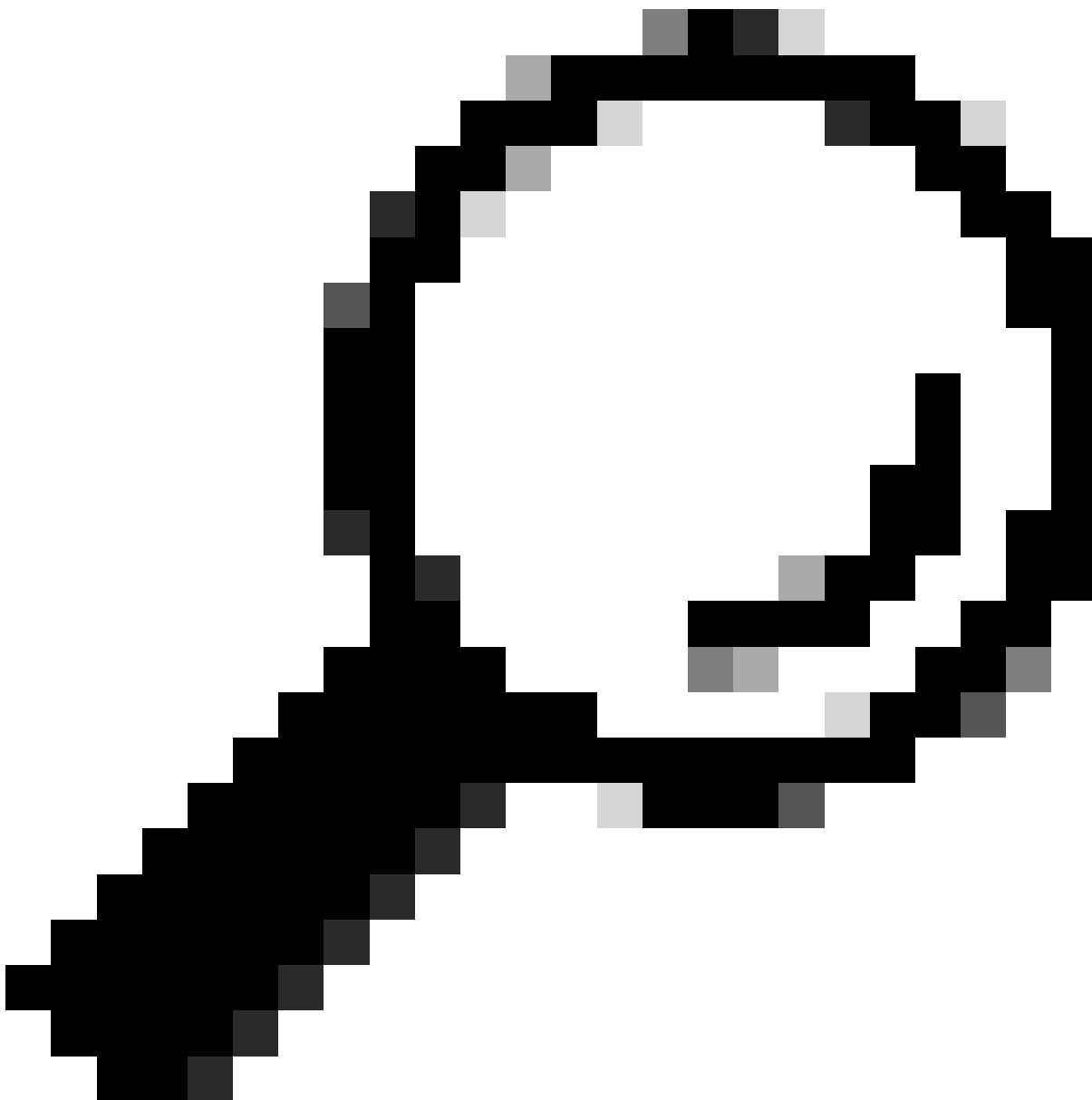
Authorization Policy(3)

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

第2部分 — 為使用TLS 1.3的TACACS+配置Cisco IOS XE



注意：確保控制檯連線可訪問且運行正常。



提示：建議配置臨時使用者並更改AAA身份驗證和授權方法，以便在更改配置時使用本地憑證而不是TACACS，以避免被鎖定在裝置之外。

配置方法1 — 裝置生成的金鑰對

TACACS+伺服器組態

步驟1設定網域名稱並產生用於路由器信任點的金鑰對。

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

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

信任點配置

步驟1 建立路由器信任點並關聯金鑰對。

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

步驟2.通過安裝CA證書驗證信任點。

</root>

cat9k(config)#

crypto pki authenticate svcs_cat9k

Enter the base 64 encoded CA certificate.

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

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

```
MIIF1DCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLZWNTV1MxEjAQBgNVBAMTCVNWUyBYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJT+y+kksifD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
Vwv4MBBjHFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULO/wxMHDtbtPBf11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzzFhwxn3chkW4JYhQ4AIwW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH1OrrurXsZummj9QBNkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
```

```
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQMMFgpTVlMgTGFiiENBMAOGCSqGSib3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
0+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOmN7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4l72a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXe/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGuA==
```

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

Certificate has the following attributes:

Fingerprint MD5: D9C404B2 EC08A260 EC3539E7 F54ED17D

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

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

yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

cat9k(config)#

步驟3. 產生憑證簽署請求(CSR)。

<#root>

cat9k(config)#

crypto pki enroll svcs_cat9k

% Start certificate enrollment ..

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

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

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

yes

Certificate Request follows:

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

```
MIIBfDCCASMAQAwgYQxGjAYBgNVBAMTEWdhD1rLnRtby5zdnMuY29tMQwwCgYD
VQQLewNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAXCzAJBgNVBAGT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCsqGSib3DQEJAhyRY2F0OWsudG1vLnN2cy5j
b20wWTATBgcqhkjOPQIBBggqhkJOPQMBBwNCAATpYE7atscrt14ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMSOwKzAcBgNVHREFTATghFjYXQ5ay50bw8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTWm3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
```

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

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

Redisplay enrollment request? [yes/no]:

no

cat9k(config)#

步驟4.匯入CA簽名的證書。

<#root>

cat9k(config)#

crypto pki import svcs_cat9k certificate

Enter the base 64 encoded certificate.

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

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

```
MIID8zCCAduGAWIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdu1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTE0MTUxMjAwWhcNMjUwNTE0MTUxMjAwWjCBhDEaMBGGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzE0MAwGA1UEChMFQ21zY28x
DDAKBgNVBAcTA1JUUEDEMAkGA1UECBMCTkMxCzAJBgNVBAYTA1VTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IAB01gTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFy0rLiYjXmLpFc03uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQRRFg94Y2EgY2Vy
dG1maWNhdGUwHAYDVR0RBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMAOGCSqGSIb3DQEBGwUAA4ICAQB0bgKVykeyVC9Usvuu0AUsGaZHGwy2H9Yd
m5vIau6PjczkCzIoAIGHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAHzY
RtmIM5KIojiDHLtiFpayxv9juDu0ZRx+wYR2PIQ5eLv1bafg7K8E82sq0Cf0tcPr
Oc0NU8UCxq0bd0gu4XsdBN1+wcWFqeQSDLP7nxvh00m/LXwCWUhwgVio0AuU2Fe
k5NthtvdXNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyZCsTBb6RvL+HsXqBgXGc5
1xCSolT0dUxFipJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUHQSY+4m
Qq2Sn3iqf4mGh/A08T4iXfWdWfNezh7ZxMsCSCK/ZR1ELZ2hj60fzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVRpitwN3Zb09poZyWiRLTnBsb42xNaWiL9bjQznA0iTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+41OTMawDgGiEv7iaiJ6xWc95EC+Adm0x3FvBXmtIM9qr7WwHW6
3C2hVYHJH254e1V5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
```

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

% Router Certificate successfully imported

cat9k(config)#

採用TLS配置的TACACS和AAA

步驟1.建立TACACS伺服器 and AAA組，關聯客戶端（路由器）信任點。

```
tacacs server sv_s_tacacs
address ipv4 10.225.253.209
single-connection
tls port 6049
tls idle-timeout 60
tls connection-timeout 60
tls trustpoint cli_s_cat9k
tls ip tacacs source-interface GigabitEthernet0/0
tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ sv_s_tls
server name sv_s_tacacs
ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

步驟2.配置AAA方法。

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

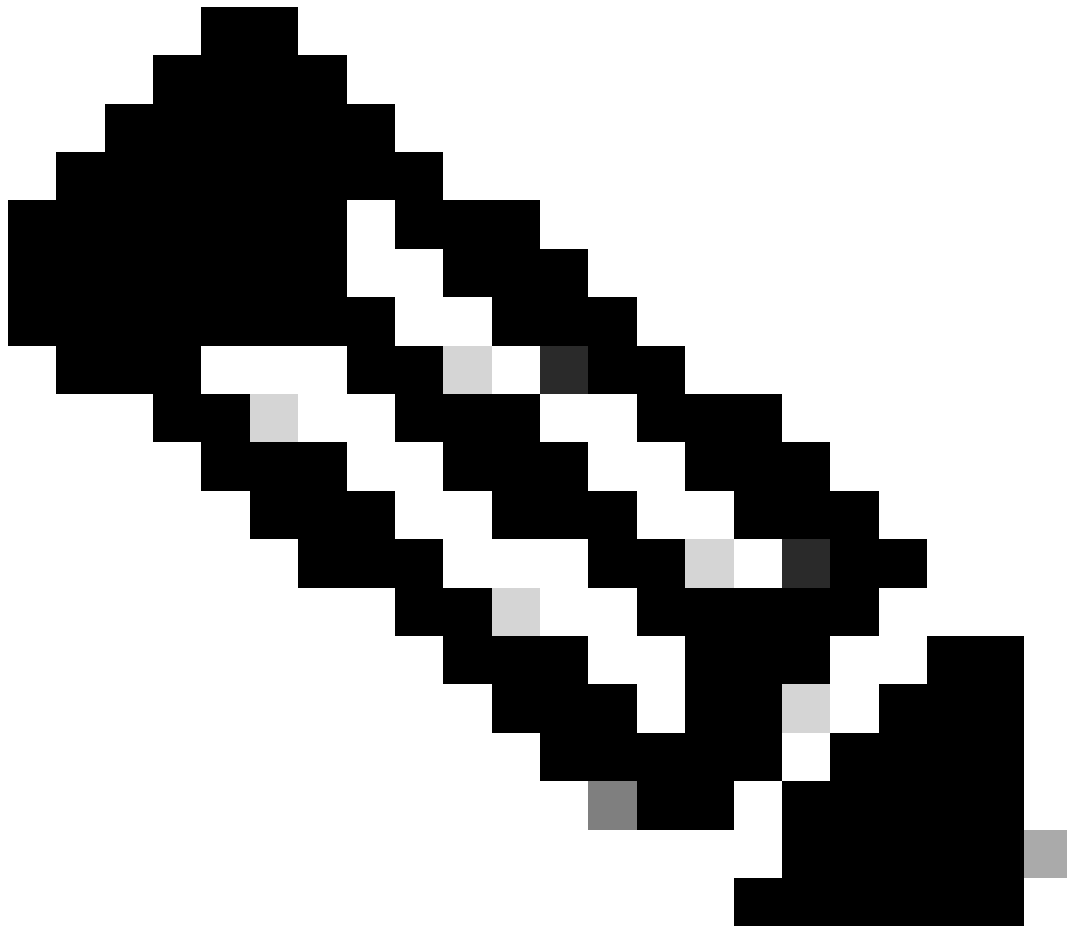
組態方法2 - CA產生的金鑰對

如果要以PKCS#12格式而不是CSR方法直接匯入金鑰以及裝置和CA證書，則可以使用此方法。

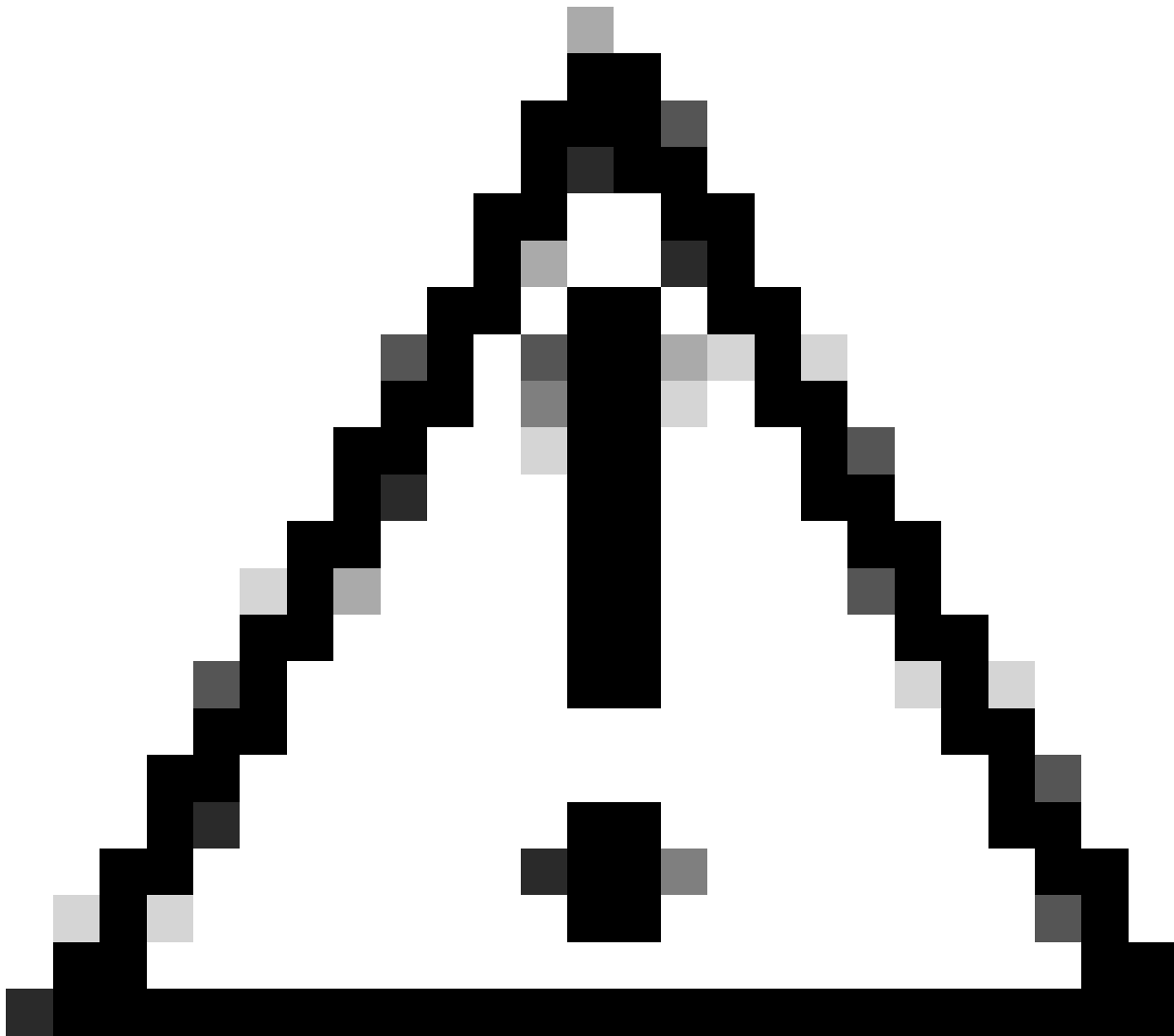
步驟1.建立客戶端信任點。

```
cat9k(config)#crypto pki trustpoint sv_s_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

步驟2.將PKCS#12檔案複製到bootflash中。



附註：確保PKCS#12檔案包含完整的證書鏈以及作為加密檔案的私鑰。



注意：匯入的PKCS#12中的金鑰必須是RSA金鑰(例如：RSA 2048)型別，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)
```

步驟3.使用import命令匯入PKCS#12檔案。

<#root>

cat9k#

crypto pki import svc_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 svc_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: svc_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: svc_cat9k_25jun17 svc_cat9k

Storage: nvram:SVSLabCA#37F5CA.cer

採用TLS配置的TACACS和AAA

步驟1.建立TACACS伺服器 and AAA組，關聯客戶端（路由器）信任點。

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

步驟2.配置AAA方法。

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

驗證

驗證設定.

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

AAA和TACACS+的調試。

```
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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。