

在具有ISE的IOS XR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 — 用於裝置管理的ISE配置](#)

[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 XR RW — 管理員設定檔](#)

[IOS XR RO — 運算子配置檔案](#)

[配置TACACS+命令集](#)

[CISCO IOS XR RW — 管理員命令集](#)

[CISCO IOS XR RO — 操作員命令集](#)

[配置裝置管理策略集](#)

[第2部分 — 為TLS 1.3上的TACACS+配置Cisco IOS XR](#)

[初始配置](#)

[配置信任點](#)

[使用TLS配置TACACS和AAA](#)

[證書續訂](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹使用思科身份服務引擎(ISE)作為伺服器，使用思科IOS® XR裝置作為客戶端的TACACS+通過TLS的示例。

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 XR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 XR

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
- 思科8201路由器，版本25.3.1

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。

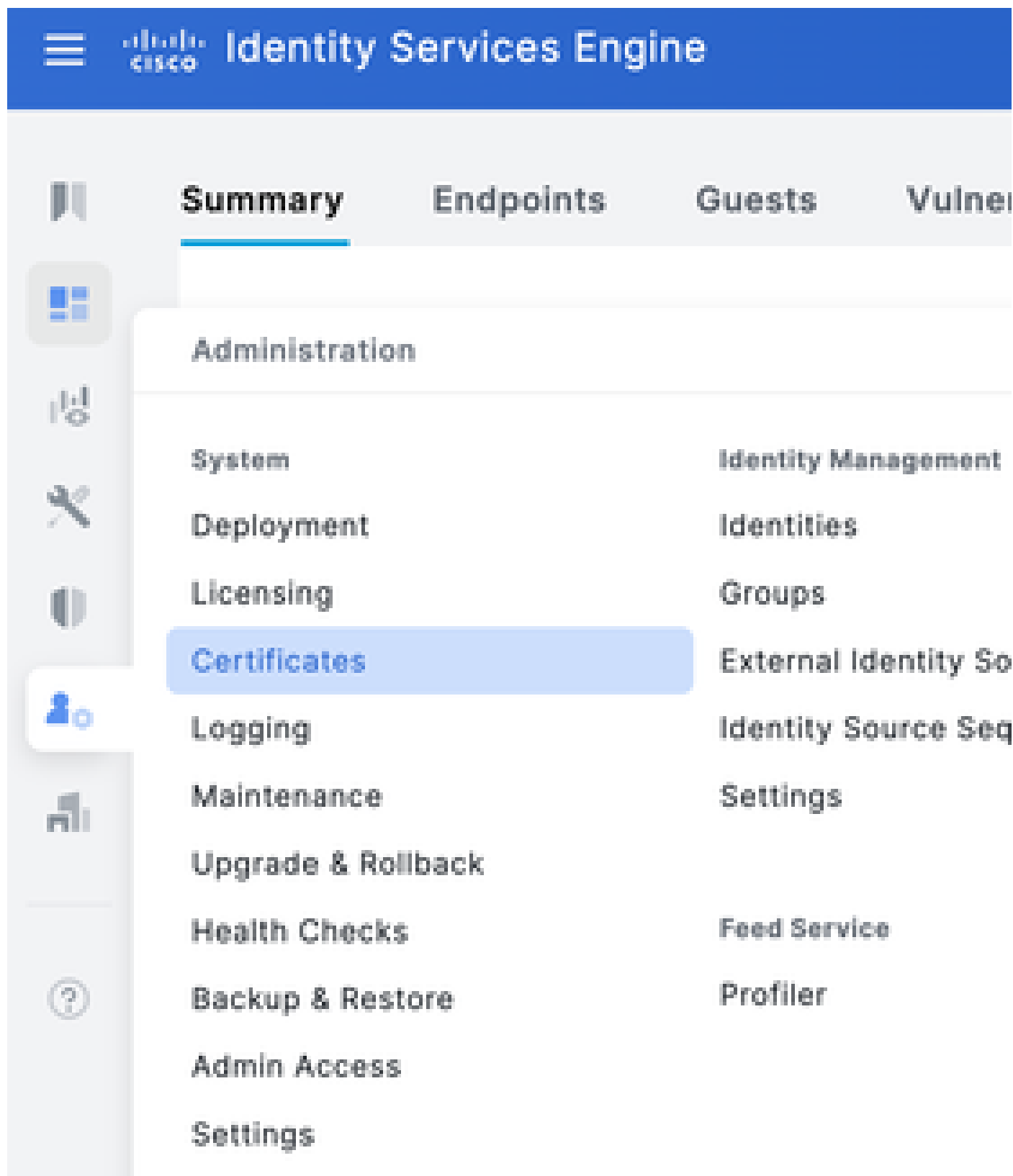
第1部分 — 用於裝置管理的ISE配置

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Administration > System > Certificates。



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



步驟4. SelectTACACS inUsage。

Usage

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

Allow Wildcard Certificates ☐ 

步驟5.選擇已啟用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

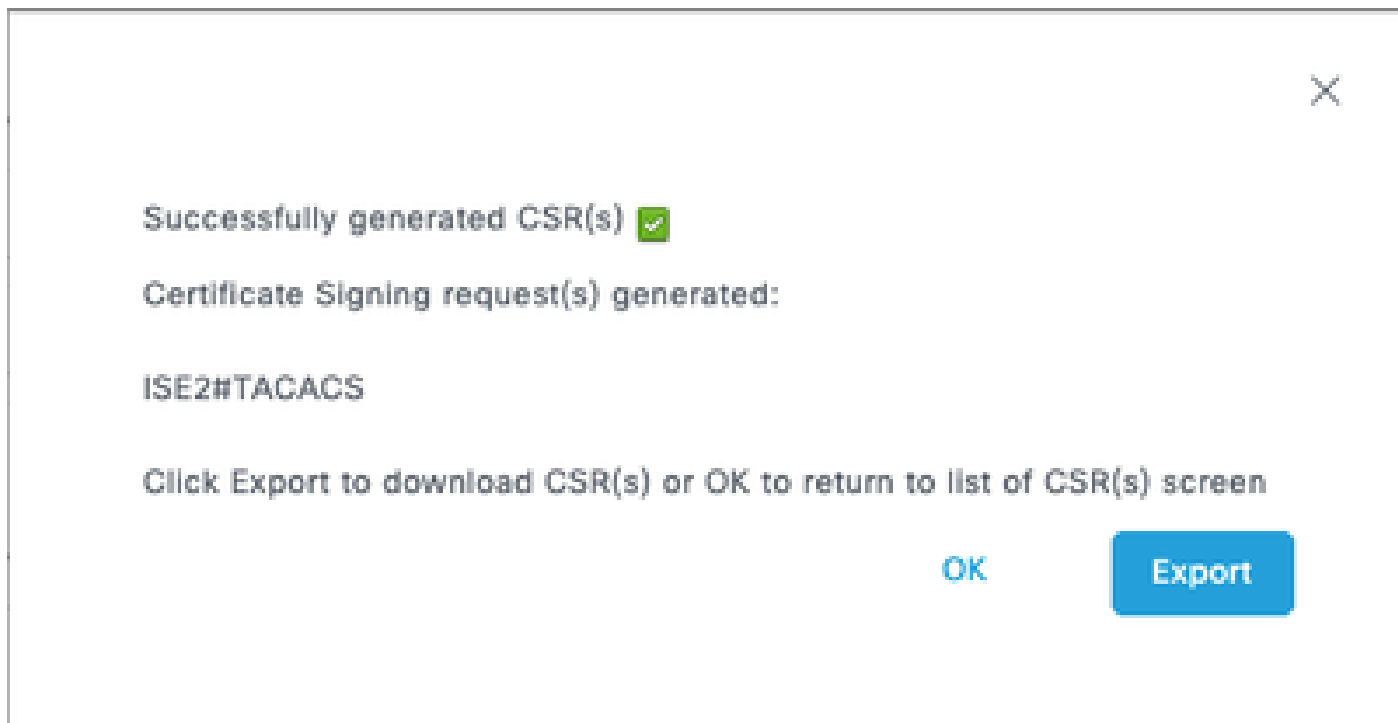
Country (C)
US

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，然後按一下Export。



現在，您可以讓憑證授權單位(CA)簽署憑證(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。

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

[Edit](#) [+ Import](#) [Export](#) [Delete](#) [View](#) [show internal CA certificates](#)

☐	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.選擇由簽署您的TACACS憑證簽署請求(CSR)的憑證授權單位(CA)頒發的憑證。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

按一下提交。現在，證書必須出現在受信任證書下。

Identity Services Engine Administration / System Evaluation Mode 27 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

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

Table Headers: Friendly Name, Trusted For, Serial Number, Issued To, Issued By, Valid From, Expiration Date, Sta

Table Row 1: CN=SVS LabCA, OU=SVS, O=Cisco, L=..., Infrastructure Cisco Services Endpoints AdminAuth, 20 CD 74 02 ..., SVS LabCA, SVS LabCA, Mon, 28 Apr 2025, Sat, 28 Apr 2...

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。

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 Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

View Export Delete **Bind Certificate**

Table Headers: Friendly Name, Certificate Subject, Key Length, Portal gro..., Timestamp, Host

步驟2.選擇已簽名的證書，並確保Usage底下的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.

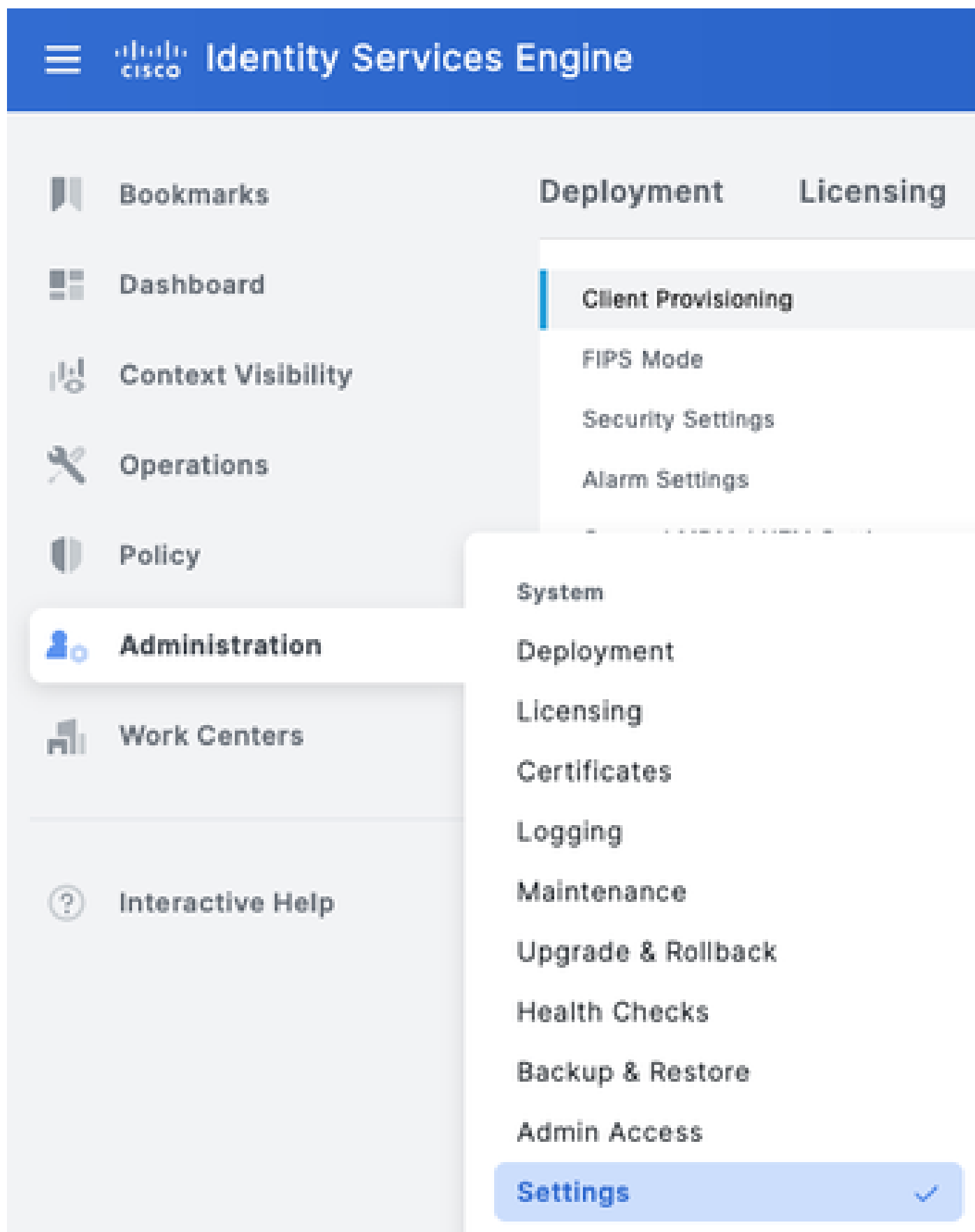
[Edit](#) [Generate Self Signed Certificate](#) [Import](#) [Export](#) [Delete](#) [View](#)

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=I SE1.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。必須手動啟用它。

步驟1.導覽至Administration > System > Settings。



步驟2.按一下Security Settings，選中TLS1.3 旁的「TLS版本設定」下的覈取方塊，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 ⓘ



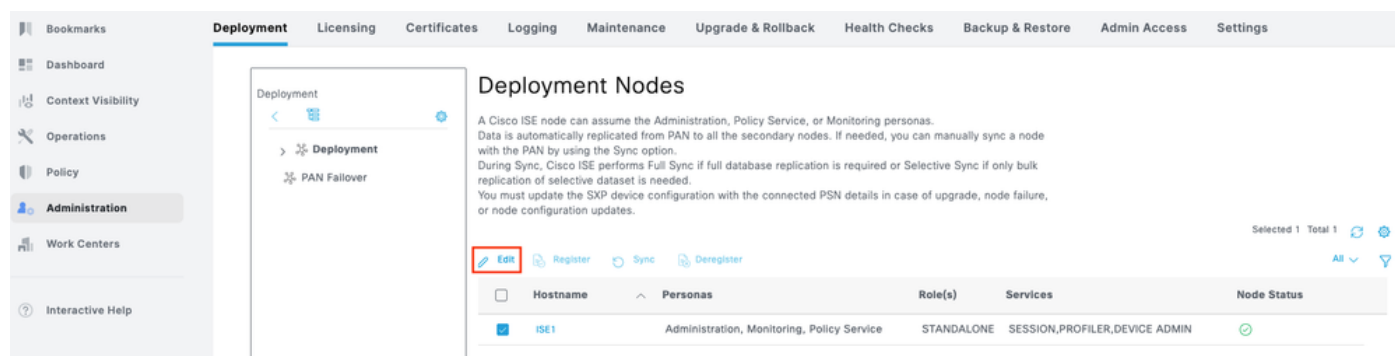
警告：當您更改TLS版本時，思科ISE應用伺服器在所有思科ISE部署電腦上重新啟動。

在ISE上啟用裝置管理

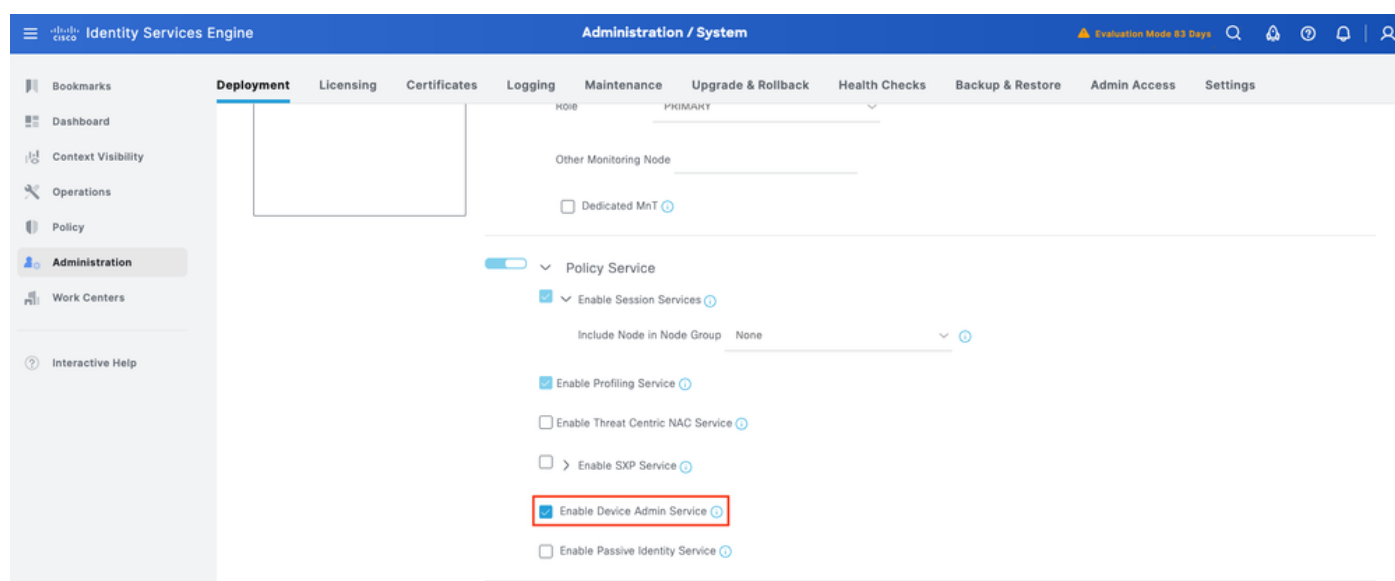
裝置管理服務(TACACS+)在ISE節點上預設未啟用。要在PSN節點上啟用TACACS+，請執行以下

操作：

步驟1. 導覽至管理>系統>部署。選中ISE節點旁邊的覈取方塊，然後按一下Edit。



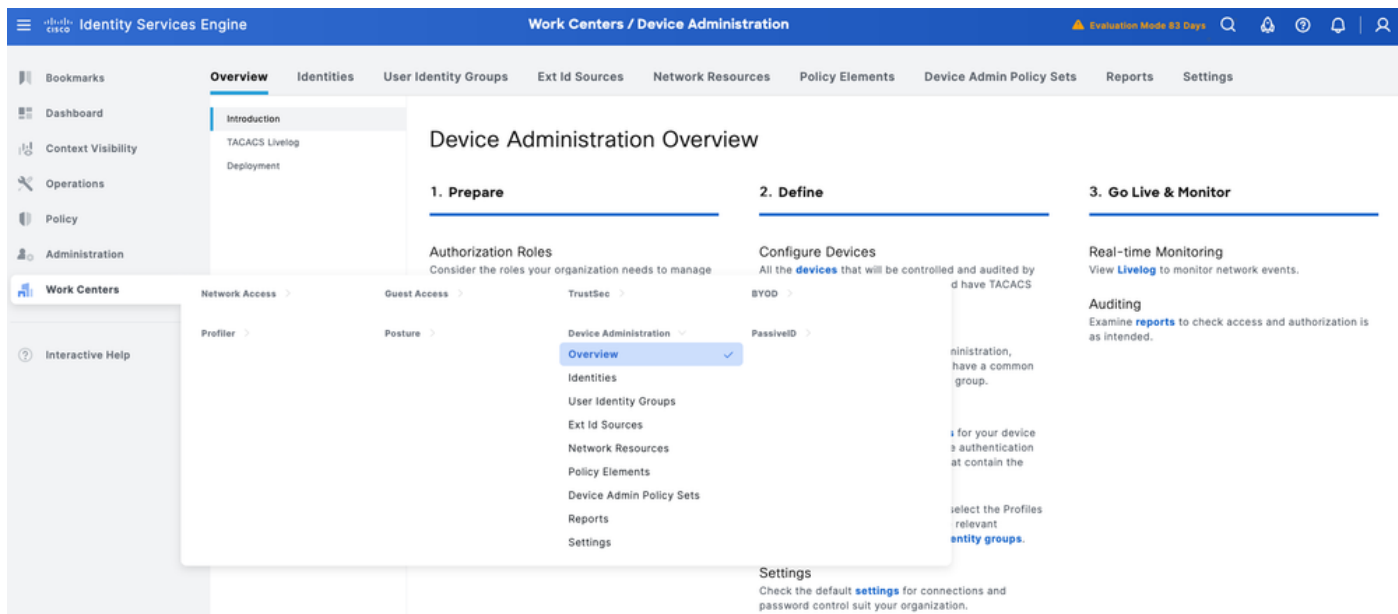
步驟2. 在General Settings下，向下滾動並選擇Enable Device Admin Service旁邊的覈取方塊。



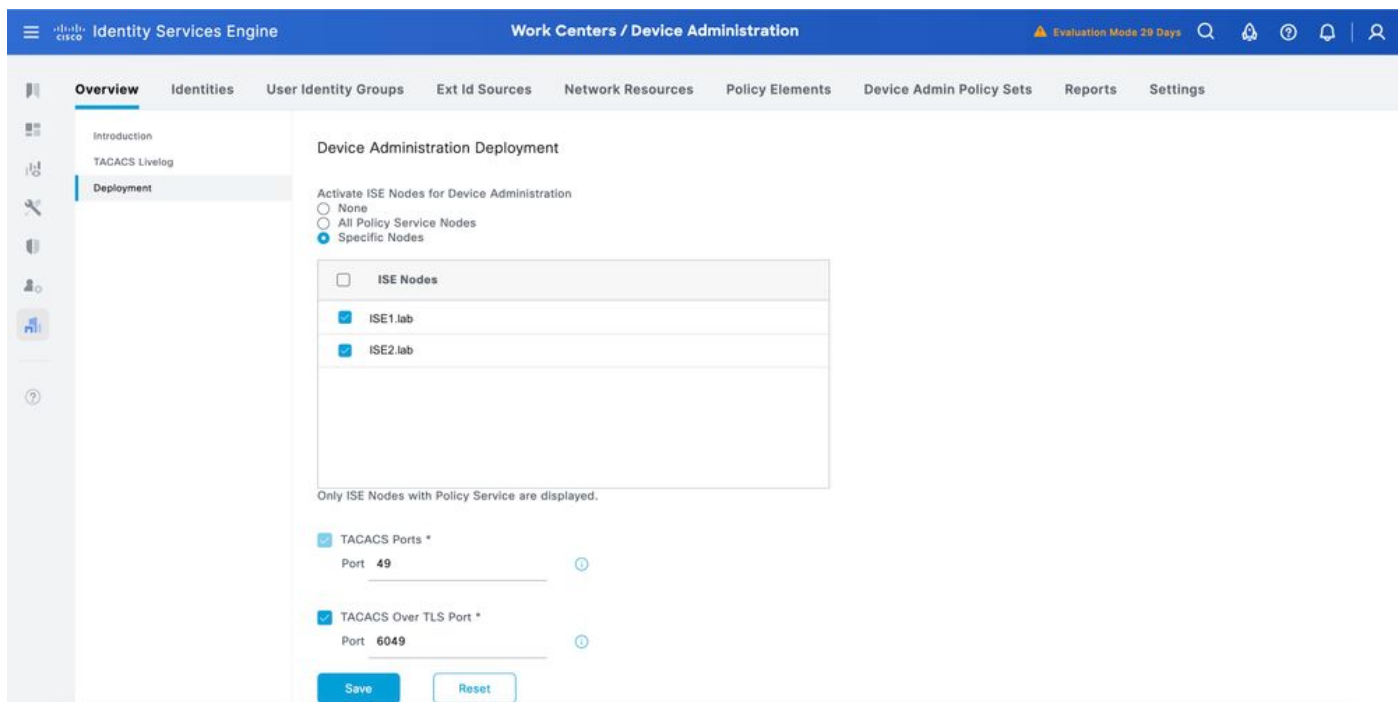
步驟3. 儲存組態。裝置管理服務現在在ISE上啟用。

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.導航到工作中心>裝置管理>網路資源。按一下網路裝置組，建立名稱為IOS XR的組。

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 93 Days

OverviewIdentitiesUsers

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Admin Policy Sets

More

✕

Edit Group

Name*

IOS-XR

Description

Group Hierarchy

Device Type > All Device Types > IOS-XR

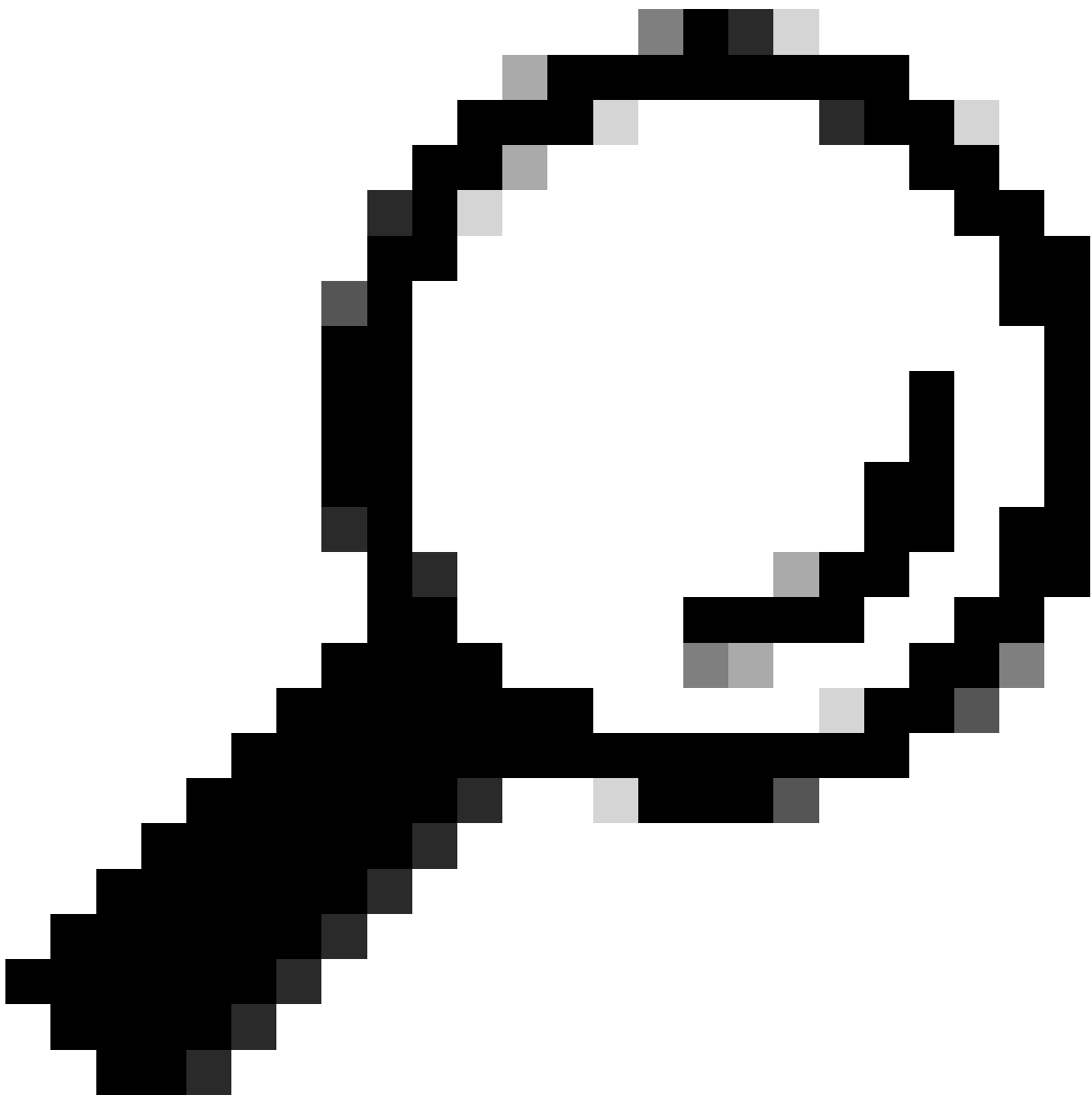
Cancel

Save

☐ ADVA

ADVA SyncDirector Network Time Monitoring

243



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 XR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。

Identity Services Engine

Administration / Network Resources

Evaluation Mode 11 Days

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

External MDM

pxGrid Direct Connectors

Network Devices

Default Device

Device Security Settings

Network Devices List > BRC-8201-1

Network Devices

Name

BRC-8201-1

Description

IP Address

* IP :

10.225.253.167

/

32

IP Address

* IP :

/

Device Profile

Cisco

Model Name

Software Version

Network Device Group

Location

All Locations

Set To Default

IPSEC

No

Set To Default

Device Type

IOS-XR

Set To Default

步驟3.輸入裝置的IP地址，並確保對映裝置的Location和Device Type(IOS XR)。最後，啟用TACACS+over TLS身份驗證設定。

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 67 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

More

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

☐

>

RADIUS Authentication Settings

☐

>

TACACS Authentication Settings

☒

>

TACACS over TLS Authentication Settings

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

Subject Alternative Name (SAN)^{*}

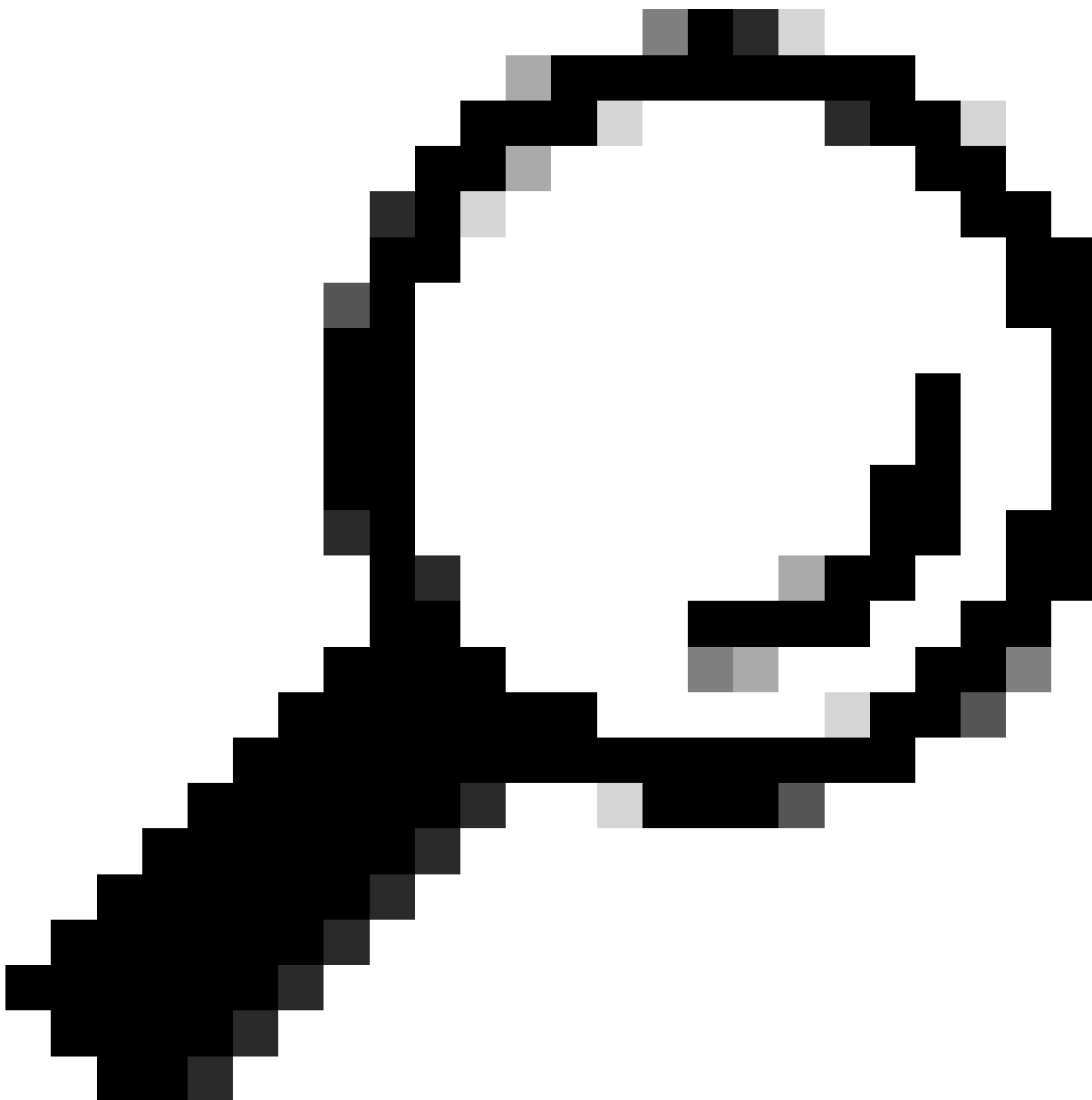
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When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

☐ IP Address

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

Additional SAN attribute details [Show](#)

Additional SAN Attributes

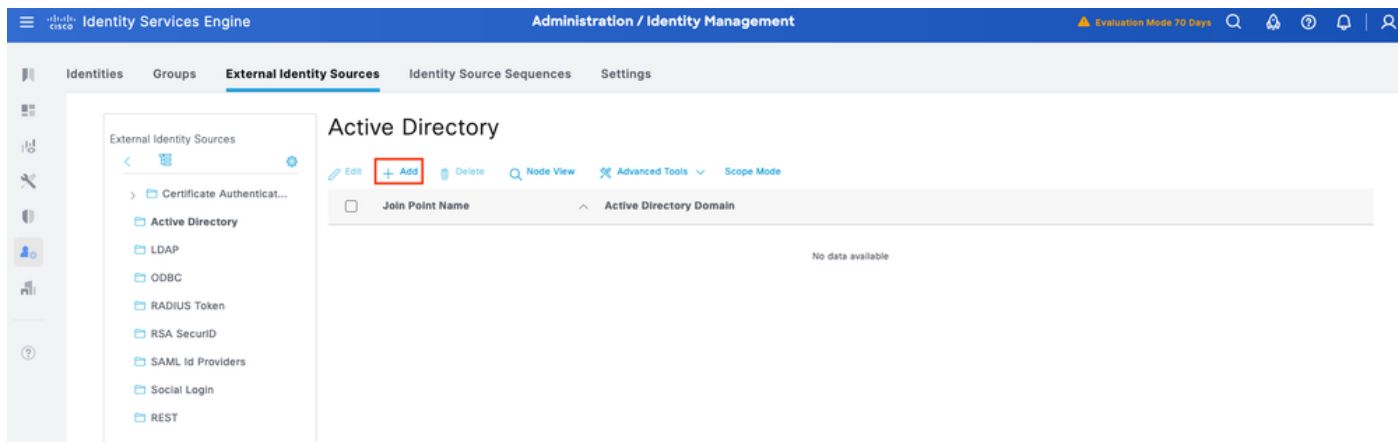


提示：建議啟用單一連線模式，以避免每次向裝置傳送命令時重新啟動TCP會話。

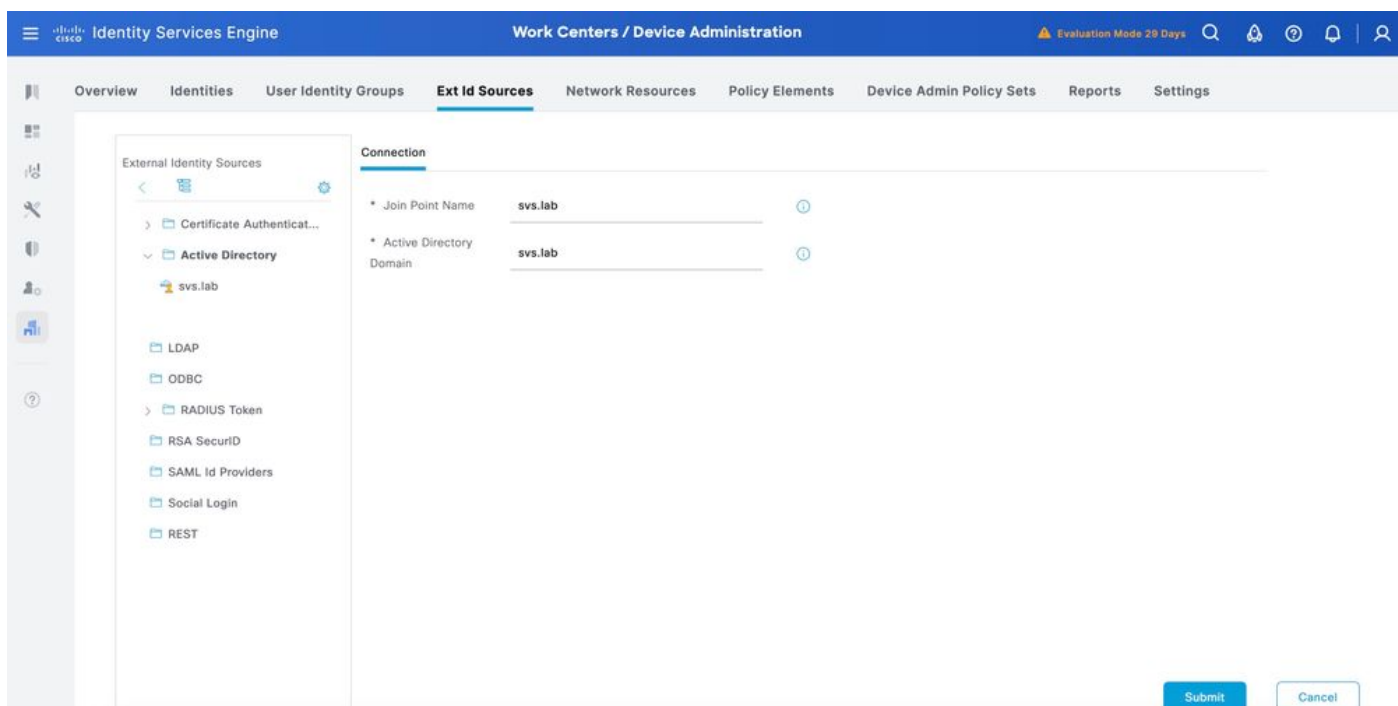
配置身份庫

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)。

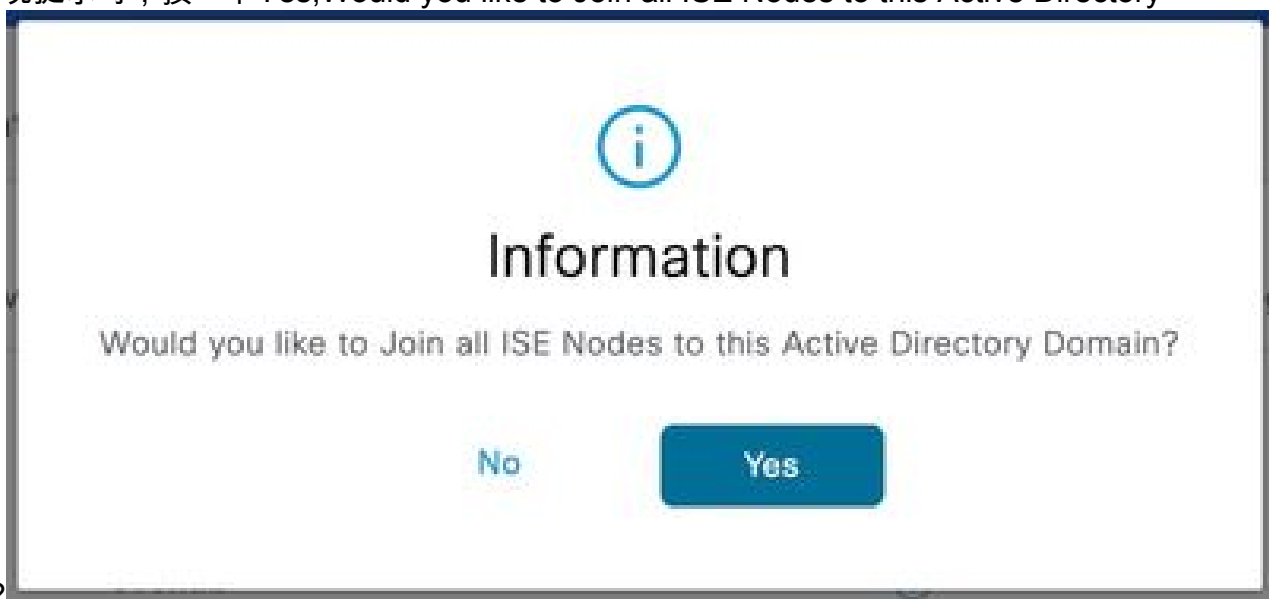
步驟1.導航到管理>身份管理>外部身份庫> Active Directory。按一下新增以定義新的AD關節點。



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，然後將ISE加入到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

×

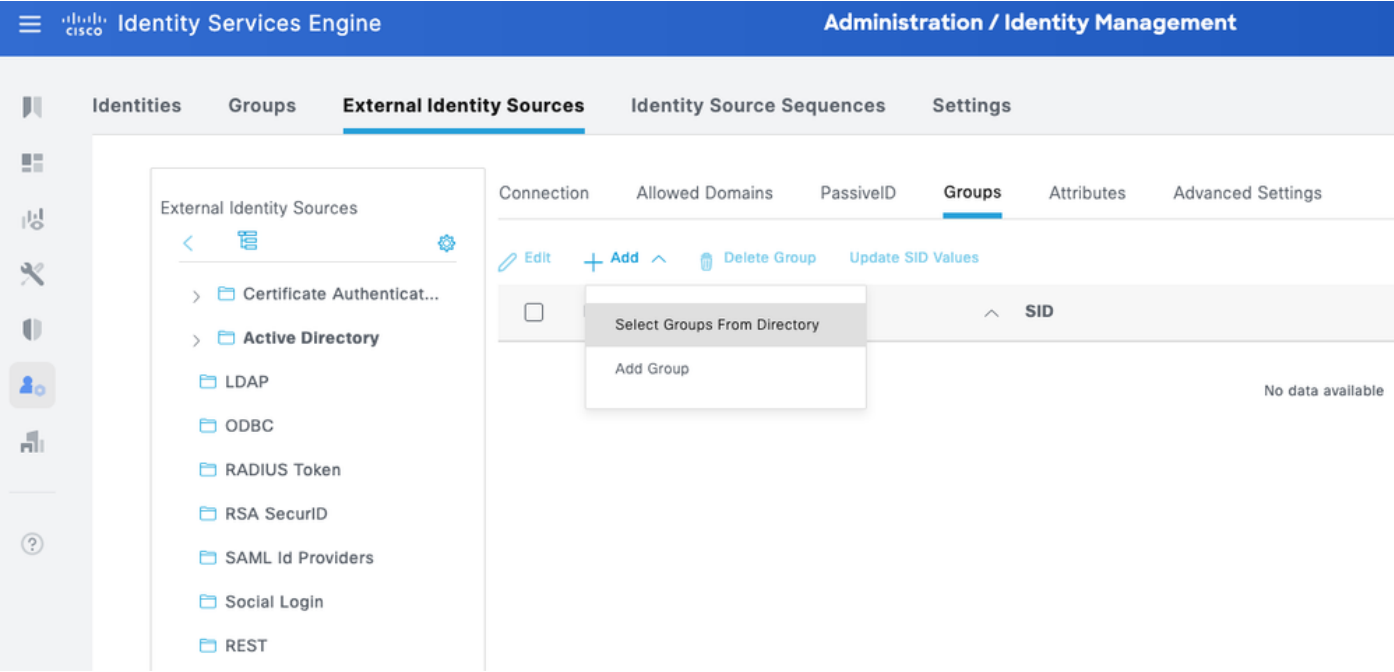
Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ISE1.lab	✔ Completed.

Close

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。此示例顯示了授權策略中使用的組。



Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

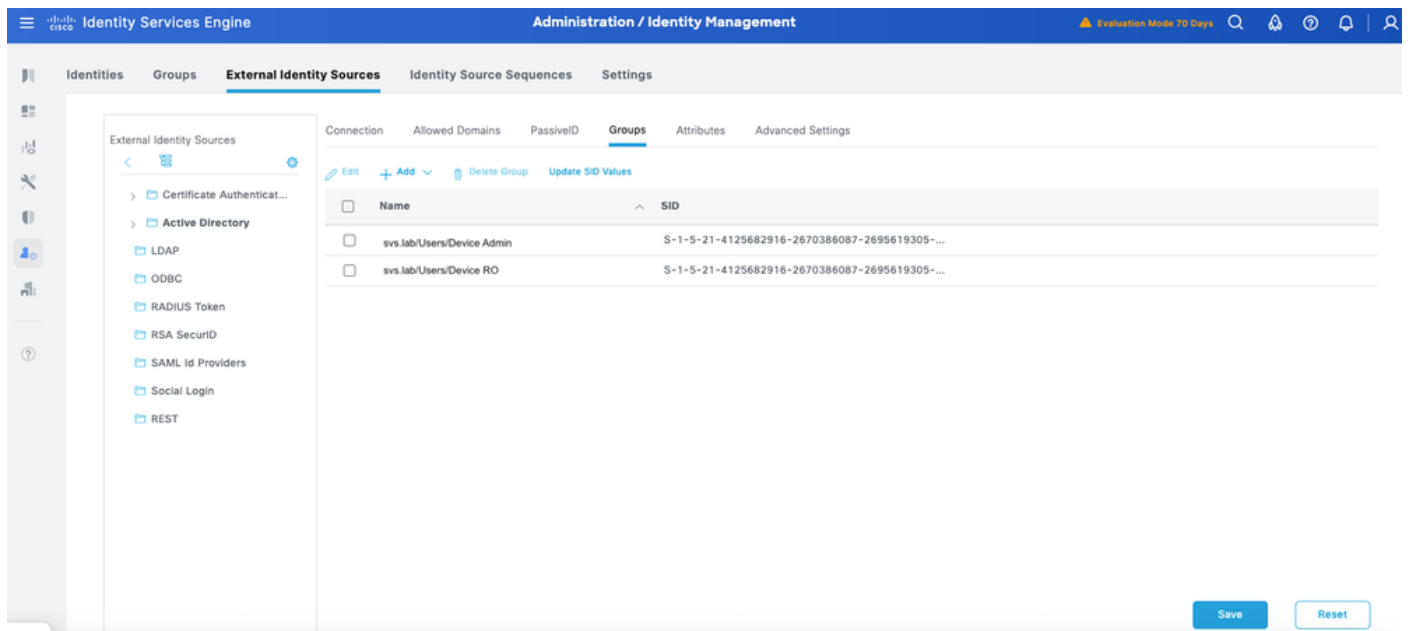
Name SID

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

將TACACS+配置檔案對映到Cisco IOS XR裝置上的使用者角色。在此範例中定義以下專案：

- 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。

定義兩個TACACS+設定檔：IOSXR_RW和IOSXR_RO。

IOS XR_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IOSXR_RW。

步驟2. 檢查並設定預設許可權和最大許可權為15。

步驟3. 確認設定並儲存。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', 'Work Centers / Device Administration', and a status indicator 'Evaluation Mode 63 Days'. The main navigation tabs are Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, Reports, and Settings. The left sidebar contains icons for various functions. The main content area is titled 'TACACS Profiles > IOSXR_RW TACACS Profile'. It includes a 'Name' field with the value 'IOSXR_RW' and a 'Description' text area. Below these are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Task Attribute View', there is a 'Common Tasks' section with a 'Common Task Type' dropdown set to 'Shell'. A list of task attributes is shown: 'Default Privilege' (checked, value 15), 'Maximum Privilege' (checked, value 15), 'Access Control List' (unchecked), 'Auto Command' (unchecked), and 'No Escape' (unchecked). Each attribute has a dropdown menu to select a value from 0 to 15, except for 'No Escape' which is a boolean (true/false).

IOS XR_RO — 運算子配置檔案

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IOSXR_RO。

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。

This screenshot shows the same ISE interface as the first one, but for a new TACACS profile named 'IOSXR_RO'. The breadcrumb trail is 'TACACS Profiles > New TACACS Profile'. The 'Name' field contains 'IOSXR_RO'. The 'Description' field is empty. The 'Task Attribute View' tab is selected. In the 'Common Tasks' section, the 'Common Task Type' is 'Shell'. The task attributes are: 'Default Privilege' (checked, value 1), 'Maximum Privilege' (checked, value 1), 'Access Control List' (unchecked), 'Auto Command' (unchecked), and 'No Escape' (unchecked). The dropdown menus for 'Default Privilege' and 'Maximum Privilege' show a range from 0 to 15.

配置TACACS+命令集

定義TACACS+命令集：在此範例中，這些是CISCO_IOSXR_RW和CISCO_IOSXR_RO。

CISCO IOS XR 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_IOSXR_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', 'Work Centers / Device Administration', and a status indicator 'Evaluation Mode 63 Days'. The left sidebar contains a menu with 'Overview', 'Identities', 'User Identity Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements' (selected), 'Device Admin Policy Sets', 'Reports', and 'Settings'. The main content area is titled 'TACACS Command Sets > CISCO_IOSXR_RW Command Set'. It includes fields for 'Name' (CISCO_IOSXR_RW) and 'Description'. Under the 'Commands' section, the checkbox 'Permit any command that is not listed below' is checked. Below this, there are buttons for 'Add', 'Trash', 'Edit', 'Move Up', and 'Move Down'. A table with columns 'Grant', 'Command', and 'Arguments' is shown, but it is empty with the message 'No data found.' at the bottom. At the bottom right, there are 'Cancel' and 'Save' buttons.

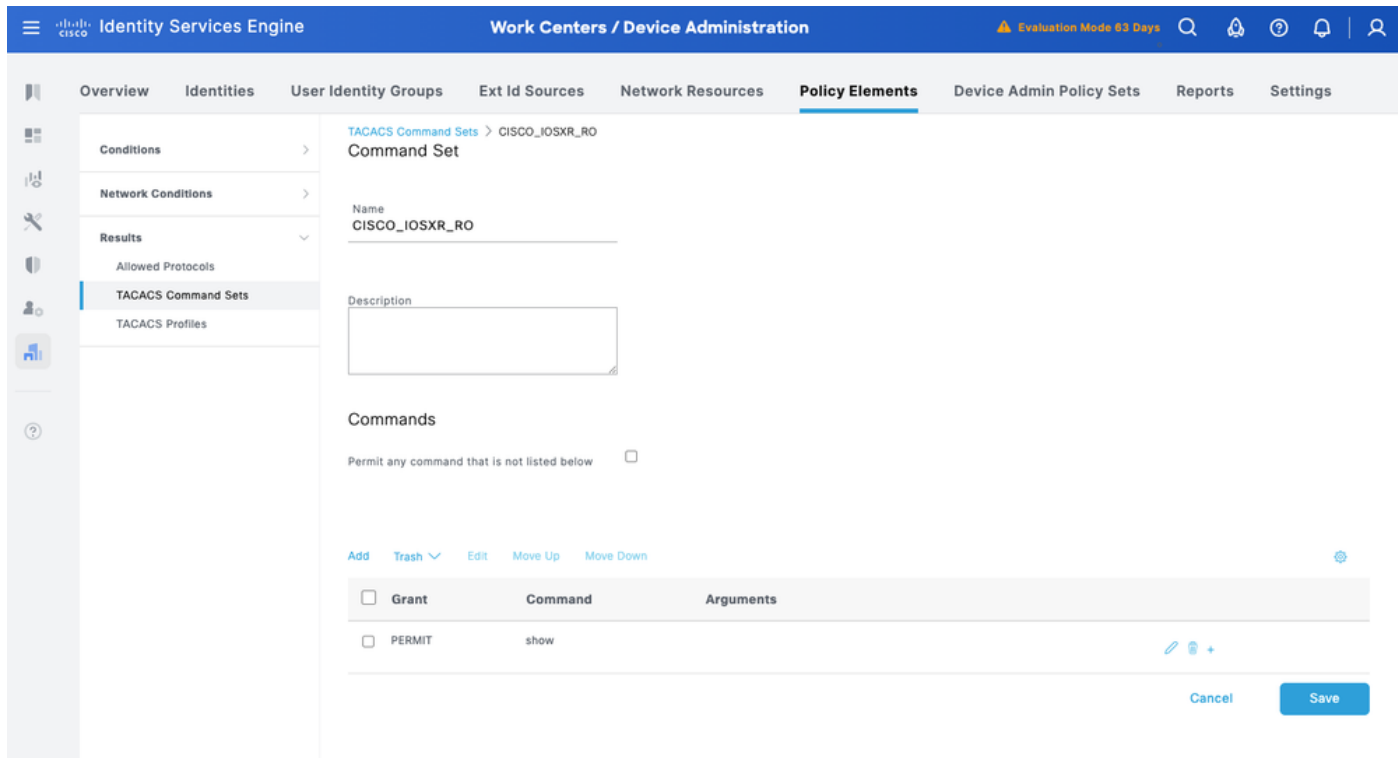
CISCO IOS XR RO — 操作員命令集

步驟1. 從ISE UI導航到工作中心>裝置管理>策略元素>結果> TACACS命令集。新增新的TACACS命令集並將其命名為CISCO_IOSXR_RO。

步驟2. 在Commands 一節中，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。

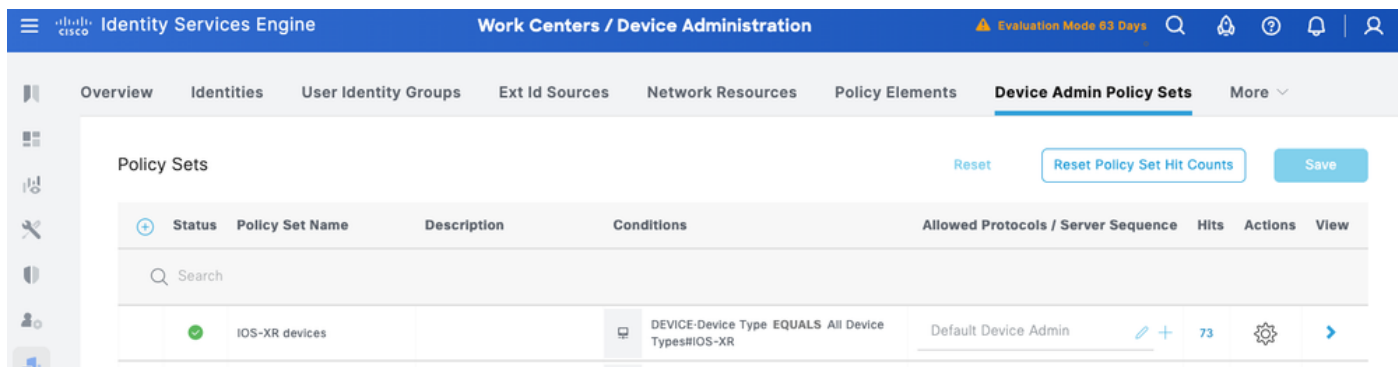
步驟4. 確認資料，然後按一下Save。



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 XR裝置。在條件下，指定DEVICE:Device Type EQUALS All Device Types#IOS XR。在Allowed Protocols下，選擇Default Device Admin。



步驟2.按一下儲存，然後單擊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 63 Days

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

More

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

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
Search					
	Default				

svs.lab

Options

If Auth fail
REJECT

If User not found
REJECT

If Process fail
DROP

85

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：

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

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 62 Days

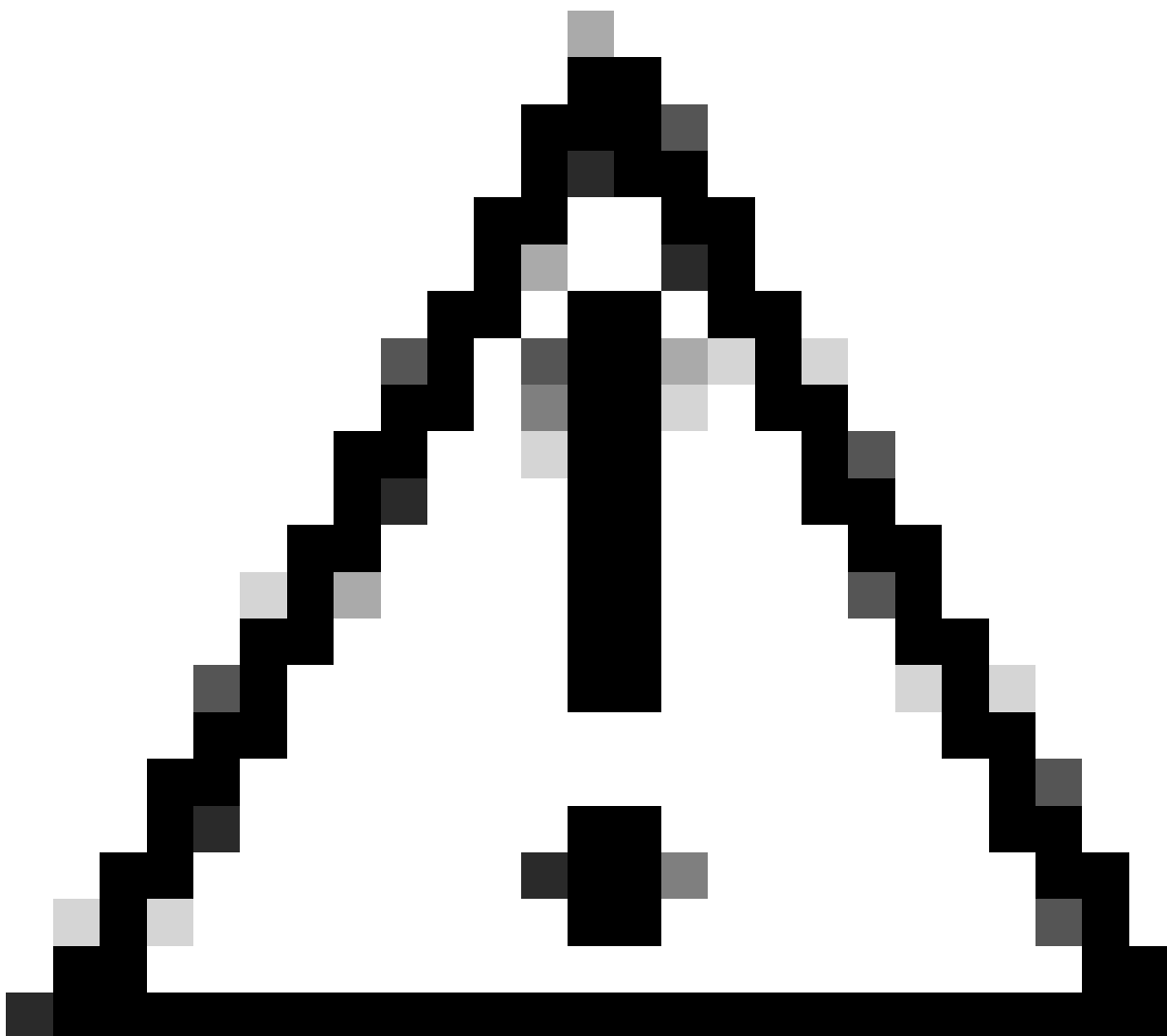
Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets → IOS-XR devices

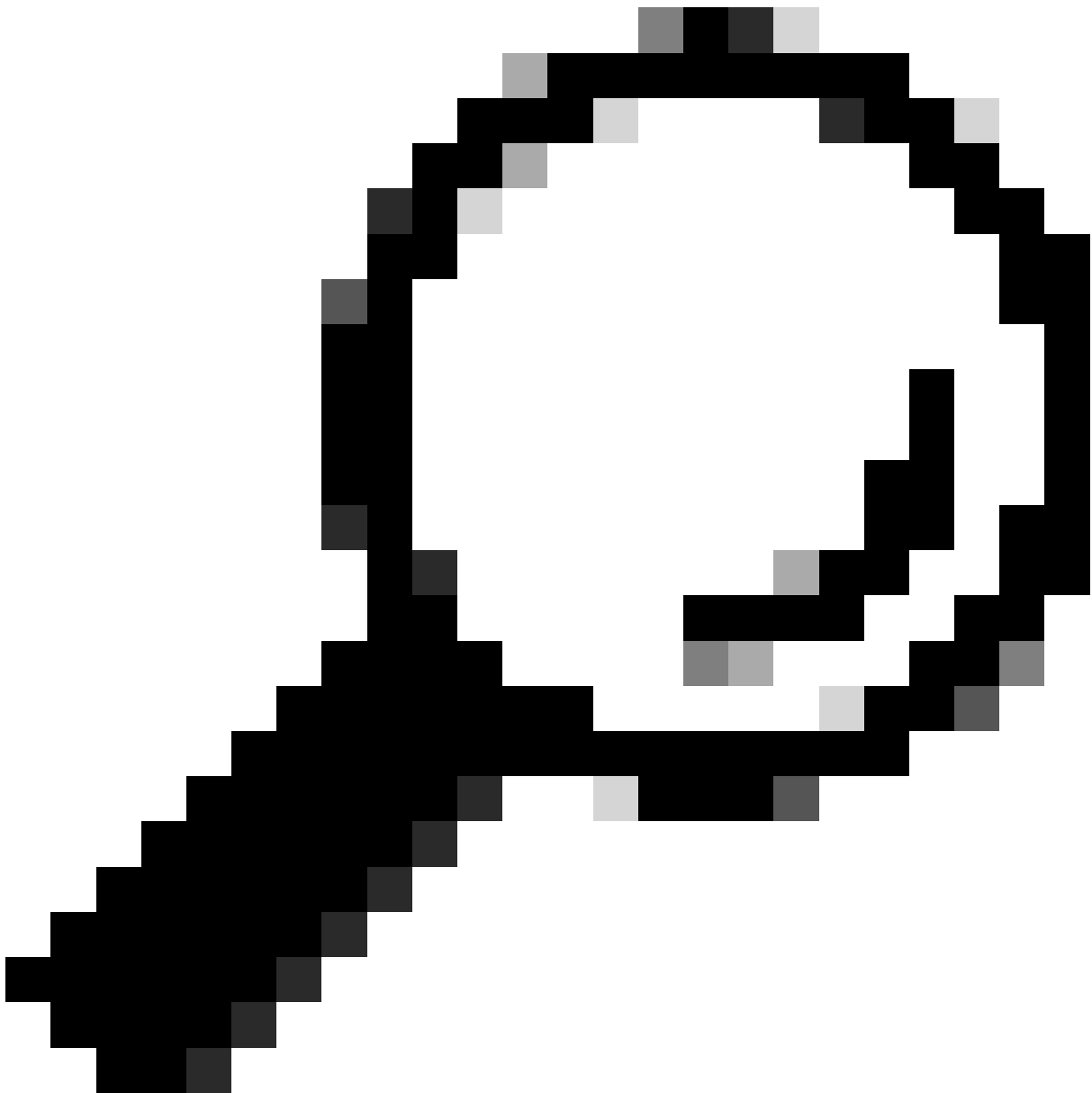
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
🔍 Search					
✅	IOS-XR devices		DEVICE=Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	77
> Authentication Policy(1)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global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

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

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



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。

初始配置

步驟1.確保配置了名稱伺服器(DNS)，並且路由器能夠成功解析頻繁限定的域名(FQDN)，特別是ISE伺服器FQDN。

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

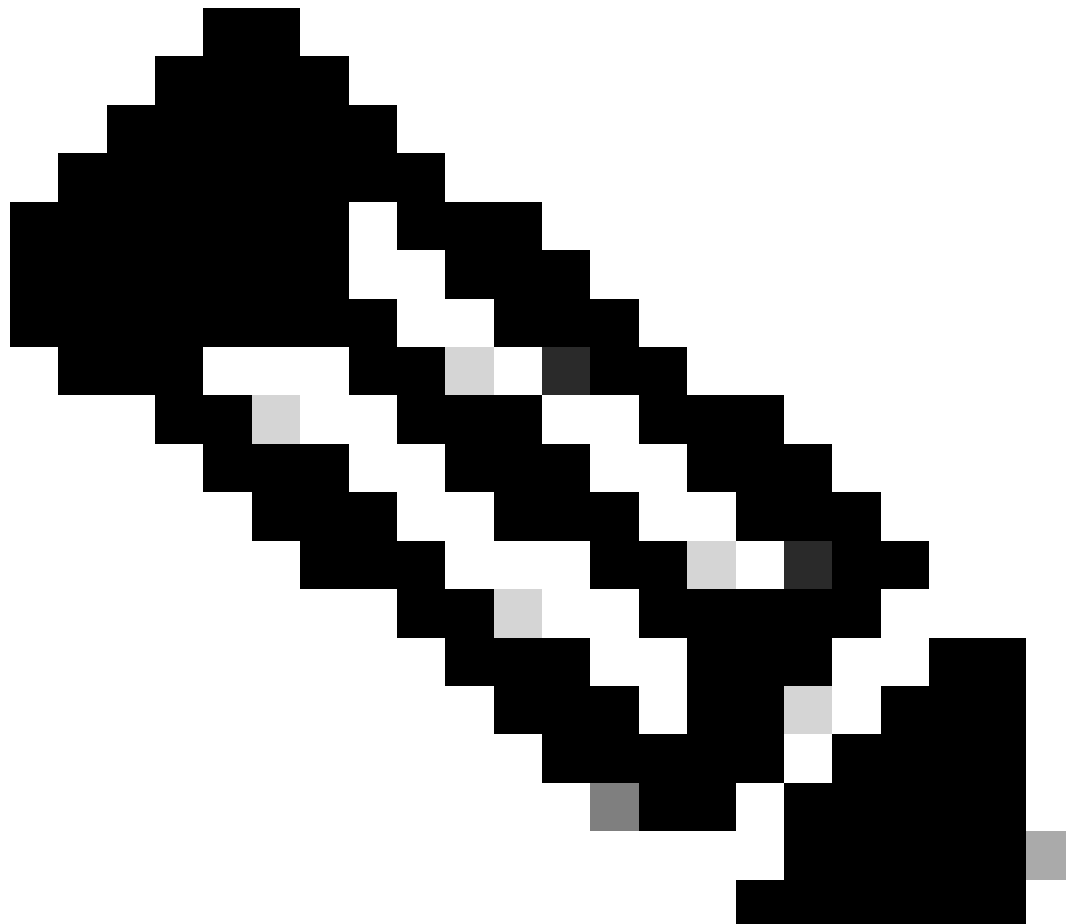
```
RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
Type escape sequence to abort.
```

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

步驟2.清除所有舊/未使用的信任點和證書。確保不存在舊信任點和證書。如果您看到任何舊條目，請將其刪除/清除。

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

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



附註：您可以手動建立新的RSA金鑰對，並將其附加到信任點下。如果不建立金鑰對，則使用預設金鑰對。當前不支援在信任點下定義ECC金鑰對。

配置信任點

步驟1.金鑰對配置 (可選)。

```
<#root>
```

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

```
crypto key generate rsa
```

```
4096
```

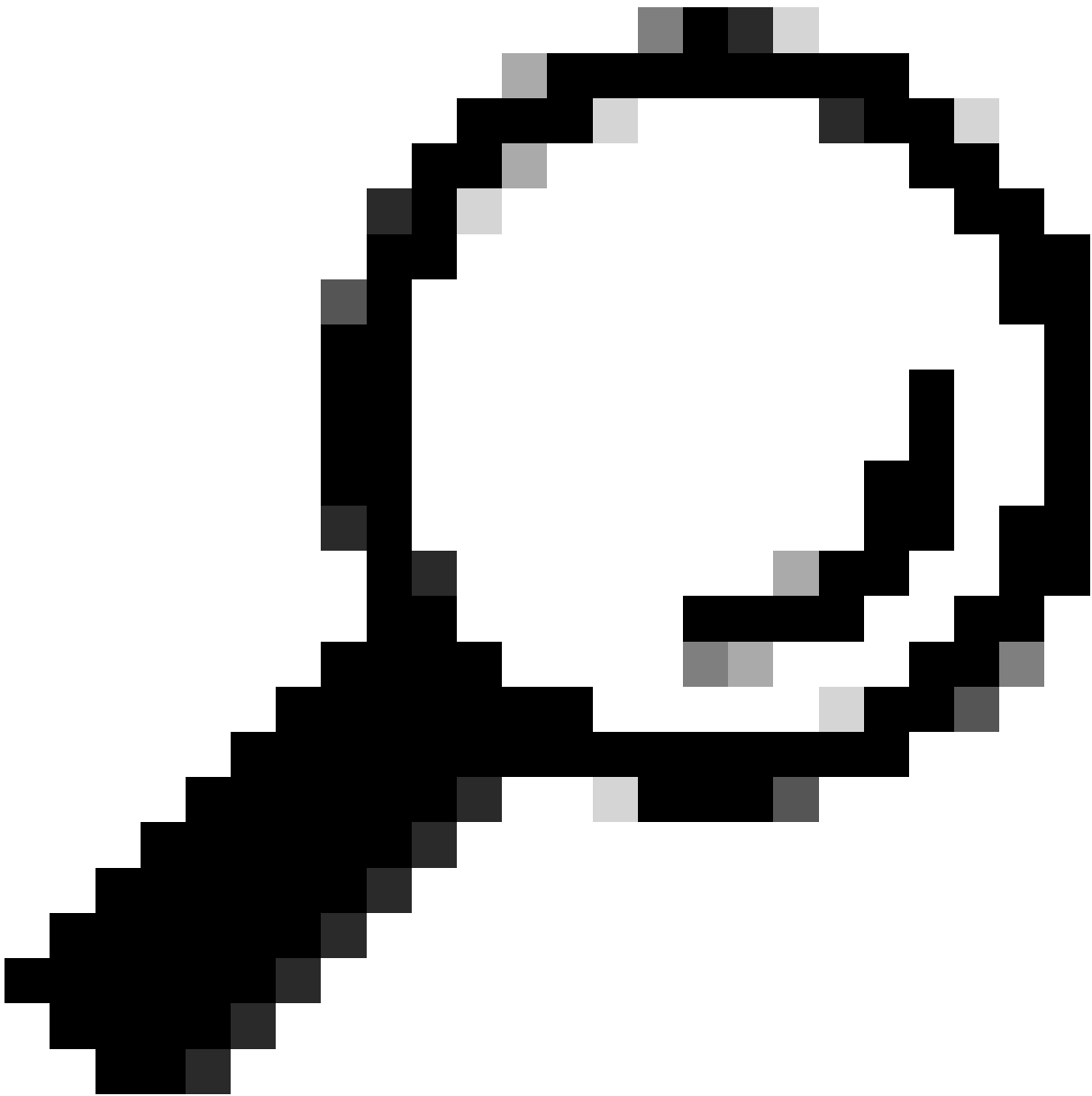
```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto ca trustpoint
```

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

```
rsakeypair
```

步驟2.建立信任點。



提示：使用者替代名稱的DNS配置是可選的（如果在ISE上啟用），但建議使用。

```
<#root>
```

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

```
crypto ca trustpoint svs
```

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

```
vrf mgmt
```

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

```
crl optional
```

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

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

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

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

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

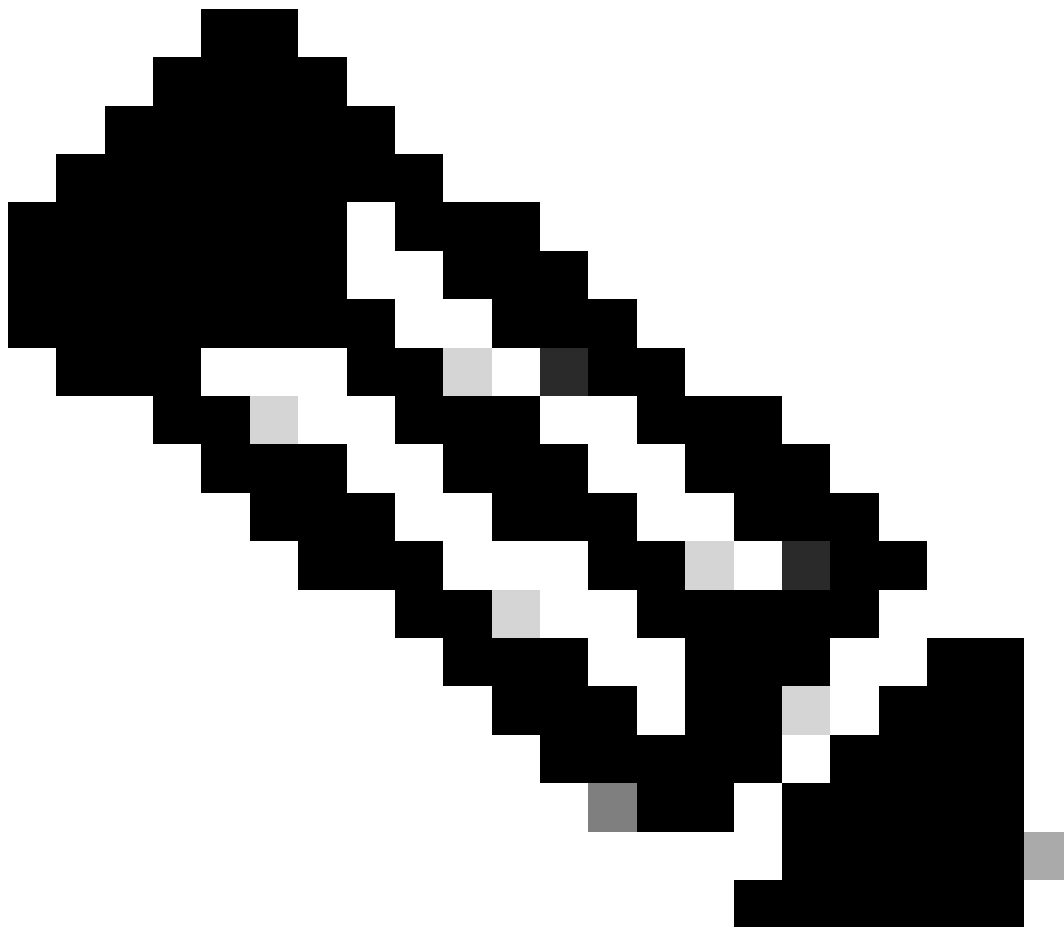
enrollment url terminal

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

rsa-keypair svs-4096

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

commit



附註：如果您需要在O或OU中使用逗號，您可以在逗號之前使用反斜線(\)。舉例來說：
：O=思科系統公司

步驟3.通過安裝CA證書驗證信任點。

<#root>

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

crypto ca authenticate svcs

Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

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

```
MIIFDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBYWJJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTty+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBBjHfM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULo/wxMHdTbtPBf11HRHTkNIto3qy04UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjREONyT973MCbVAAxtNVU6bEBROz+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpl334rTixy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XC0NX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCSAGG+EIBDQMFgptV1MgTGFiIENBMAOGCSqGSIb3DQEB
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
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

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

quit

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

Subject:

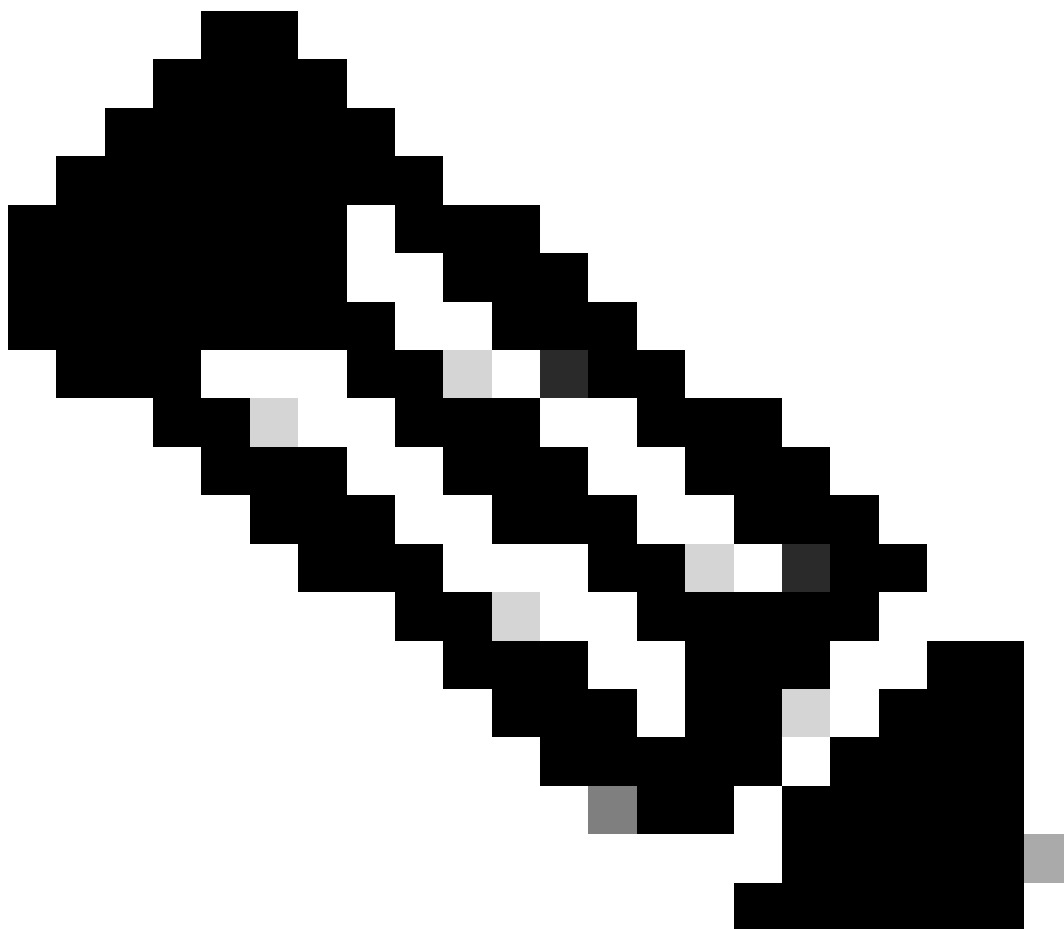
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US

Issued By :

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

```
Validity Start : 17:05:00 UTC Mon Apr 28 2025
Validity End   : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
SHA1 Fingerprint:
0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
yes
```

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



附註：如果您有從屬CA系統，則需要匯入根CA和子CA證書。使用頂部有子CA，底部有根CA的相同命令。

步驟4. 產生憑證簽署請求(CSR)。

<#root>

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

crypto ca enroll svcs

Fri May 9 14:52:44.030 UTC

% Start certificate enrollment ...

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

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

% Please make a note of it.

Password:

Re-enter Password:

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167

% The subject name in the certificate will include: BRC-8201-1.svs.lab

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

yes

% The serial number in the certificate will be: 4090843b

% Include an IP address in the subject name? [yes/no]:

yes

Enter IP Address[]

10.225.253.167

Fingerprint: 36354532 38324335 43434136 42333545

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

yes

Certificate Request follows:

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

MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAk5DMQwwCgYDVQQQH
DANSVFAXDjAMBGNVBAoMBUNpc2NmMQwwCgYDVQQQLDANTVlMxZzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtr1oDH9iOZxPvEDARwN0t4WrPEjaQc1ZUA
6ax6Cqx/0JlQiUf2+eQv+4rKZqAZ1xDhiaIMGqETn00LKpwmtx10IqXL7UYMHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRwMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkKwI0cb1X2HgtbVQdCXTAwJDmr209
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAACBiTAYBgqhkiG
9w0BCQcxCMJQzFzY28uMTIzMG0GCSqGSIb3DQEJJDJFgMF4wDgYDVROPAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCSqGSIb3DQEJJDJFgMF4wDgYDVROPAQH/BAQD
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBbX0eWF5ZUz701GFjuQHBBdgYb+3lhF0xbYm9psIWfv1uwjKkOL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswj1YpO+IxxUM971Ejwg2rj+jABDR7I8SU
06Y06mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTI1jdgVxB+Xyz0FJMckI05US3j
T/3aw/115RcXerdrh360MUHEepUjIx/15u9s1c7e1mxACoQE6f90A+fdg2zYt0ME
Z6VAw64cY+YF6iLbYv7c4l1z05Zj2NJBkUpeqijkFAKY/1rIXTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZN00

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

no
```

步驟5.匯入CA簽名的證書。

```
<#root>
```

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

```
crypto ca import svcs certificate
```

```
Fri May 9 15:00:35.426 UTC
```

```
Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
MIIE3zCCAsegAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA5MTQ1NzAwWWhcNMjUwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkxMDDAKBgNVBACMA1JUUEDEOMAwGA1UECgwFQ21zY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAUMjI1LjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMiIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOd02uW
gMf2I5nE+8QMBHA3S3has8SNpByV1QDprHoLGr/QmVCJR/b55C/7ispmoBnXE0GJ
qIwaoR0c7QsqnCa3HXQipcvrtRgwcFAX29Egjnboi aRYDxrddbHrpSQTfpeh5dp/k
eQuio07rxfdzTss+8x7WwzC+artGbLYMC7fQcH819iVAIeZNUXPcz18G3zrHHI3W
fFMVT/iVFYwLvdR0v1h0okuMykFPa00TemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTajRxvVfYeC1tVB0JdMDAK0avY73N3Zk Jr16dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0
ZTA0BgNVHQ8BAf8EBAMCBaAwIAyDVR01AQH/BBYwFAYIKwYBBQUHAWEGCCsGAQUF
BwMCMAMkGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAUMjI1LjI1My4xNjcxETAPBgNV
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+oj012106WxedDQ8Vdu0bBtrn0H+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTzRQ93tb9mMTZg7exqN89ZU
V1XoB2U0Tri5K10/+izEGgyNq42/ytAP8Y007HR/2jf7gfhovwvCR5QNOEHv4o61
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV81RGXxxgyt1mwNmb7EiAc81odRcgyp7FNh3
F/k9cMMMr51M4Ysvo1tx1k9AeLjb2syv5/fG6Qu0ZdWwTaaQh0Y2h/cVDiV97wg
0D1mEfDsv6QrxQSujZr22RzVykKH1tuiV2B74pthUuGRBtFHS5Xfy7uTTbfGX8M6
ZJw8rX1SADr8tDp1rf1ZIrPmv3ZPP7woTB22yWzyd0use+5Ia1b0w70twN4t/Iiw
8CJu6HfnDXLDPZ0jsC8steffrS1opwGccp3j6aZKPFz+I/Purb44a9WxEwa2TA7H
+r1oynBcGMet0HxVlnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF5370w+uNHok8Bdt8mqadUT40oUSqY8ArV0Bom05tzbemreVPmQAZ/IahZ7TqKo
3dGNontAFTTESM1iujQ81iRKsikdHysnwcCM2ni1CKZrhVq5IB8NK6jKRJZ0eQAX
vMt1
-----END CERTIFICATE-----
```

```
quit
```

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

```
Subject:
```

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

```
Issued By :
```

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

Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792

驗證是否已註冊路由器身份證書。

<#root>

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

show crypto ca trustpoint svcs detail

Trustpoint :svs-new
=====

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

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

show crypto ca certificates svcs

Wed May 14 14:55:58.173 UTC

Trustpoint : svcs-new
=====

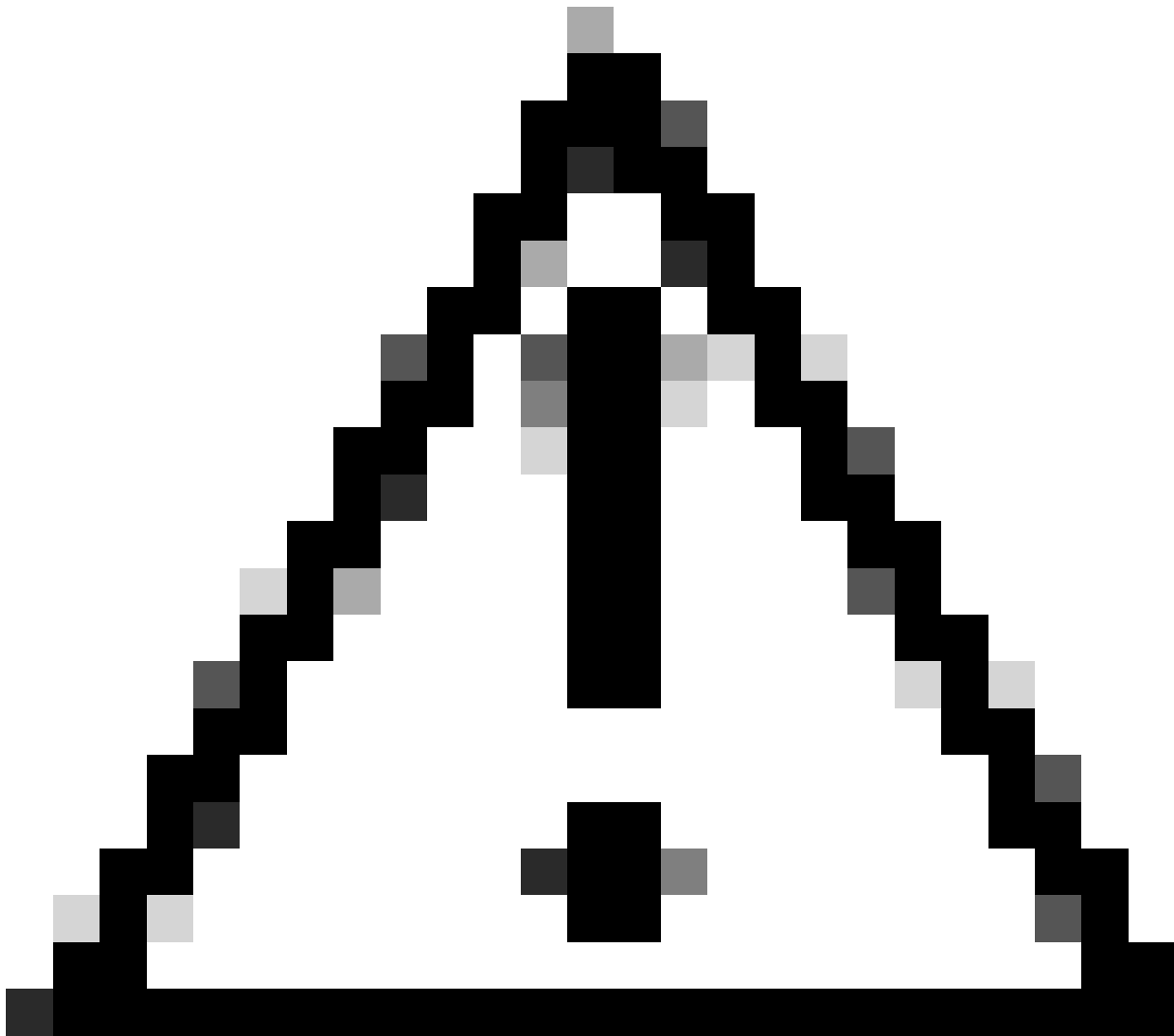
CA certificate
Serial Number : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
Subject:
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 17:05:00 UTC Mon Apr 28 2025
Validity End : 17:05:00 UTC Sat Apr 28 2035
SHA1 Fingerprint:
0EB181E95A3ED7803BC5A8059A854A95C83AC737

Router certificate

Key usage : General Purpose
Status : Available
Serial Number : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
Subject:
serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 19:59:00 UTC Fri May 09 2025
Validity End : 19:59:00 UTC Sat May 09 2026
SHA1 Fingerprint:
AC17E4772D909470F753BDBFA463F2DF522CC2A6

Associated Trustpoint: svcs

使用TLS配置TACACS和AAA



注意：通過具有本地憑據的控制檯執行配置更改。

步驟1.配置TACACS+伺服器。

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

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

步驟2.配置AAA組。

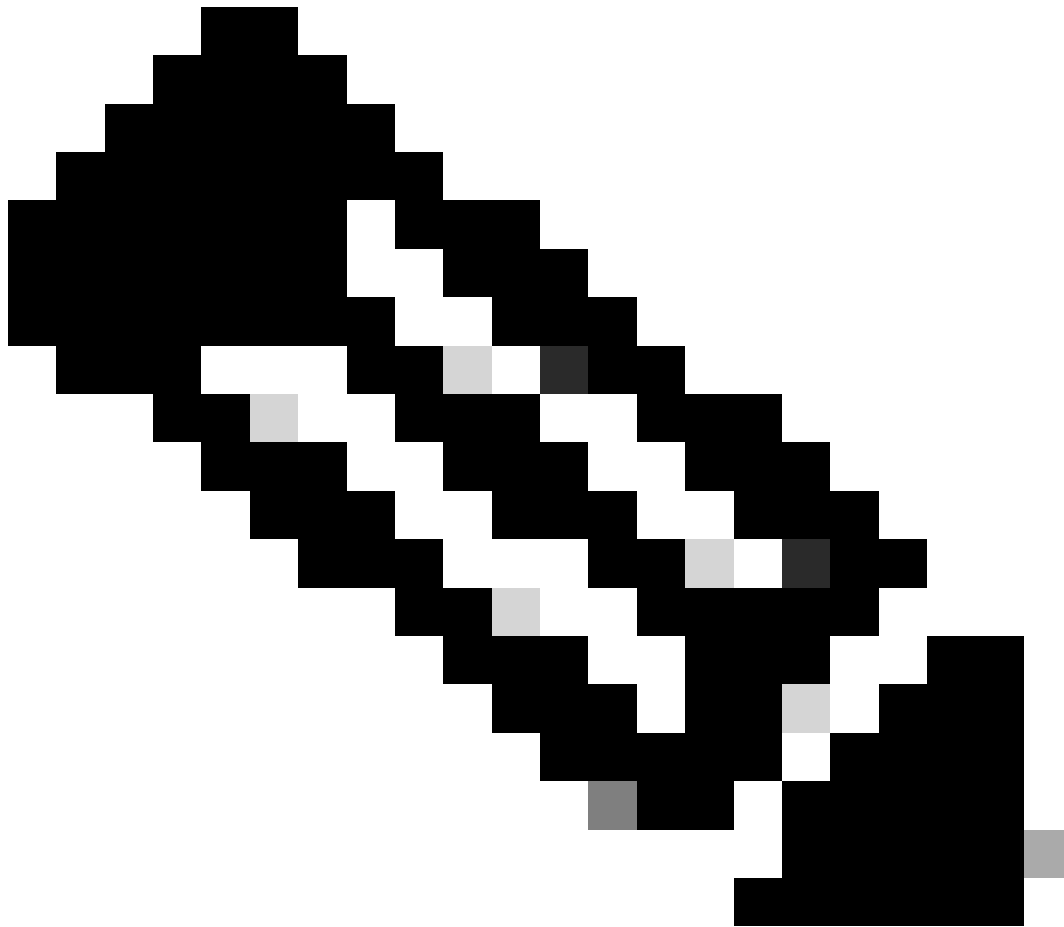
```
aaa group server tacacs+ tac_tls_sc
```

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

步驟2.配置AAA。

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

證書續訂



附註：續訂期間，無需從TACACS+配置中刪除信任點。

步驟1.驗證當前證書的有效日期。

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

```
Trustpoint : svcs-new
```

```
=====
```

```
CA certificate
```

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

```
Subject:
```

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

```
Issued By :
```

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

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

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

```
CRL Distribution Point
```

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

```
SHA1 Fingerprint:
    EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
Subject:
    CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
    CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Sun Jun 24 2035
SHA1 Fingerprint:
    E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
Key usage : General Purpose
Status : Available
Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E
Subject:
    CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
    CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 16:38:36 UTC Wed Jul 30 2025
Validity End : 16:38:35 UTC Thu Jul 30 2026
CRL Distribution Point
```

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

```
SHA1 Fingerprint:
    B562F3CF507CE7F97893F28BC896794CFF6995C1
Associated Trustpoint: svb-new
```

步驟2.刪除現有信任點證書。

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
Thu Aug 14 15:25:26.286 UTC
certificates cleared for trustpoint KF_TP
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database updated
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:25:37.270 UTC
RP/0/RP0/CPU0:BRC-8201-1#
```

步驟3.按照信任點配置下的步驟所述重新驗證並註冊信任點。

步驟4.驗證證書有效日期是否已更新。

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:31:28.309 UTC
```

```
Trustpoint : KF_TP
=====
CA certificate
```

Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Tue Jun 25 2030

CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uB1QsZDYy6wxomiFWB5Gv0AZM
SHA1 Fingerprint:
EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2

Trusted Certificate Chain

Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
Subject:
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Sun Jun 24 2035
SHA1 Fingerprint:
E225647FF9BDA176D2998D5A3A9770270F37D2A7

Router certificate

Key usage : General Purpose
Status : Available
Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
Subject:
CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 15:17:29 UTC Thu Aug 14 2025
Validity End : 15:17:28 UTC Fri Aug 14 2026

CRL Distribution Point

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

驗證

驗證設定.

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

TACACS+調試

```
debug tacacs tls
```

調試TLS

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

在配置AAA身份驗證之前測試遠端使用者。

```
<#root>
```

```
test aaa group tacacs2
```

```
user has been authenticated
```

疑難排解

清除憑證 (這將刪除與信任點關聯的所有憑證) 。

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

TACACS進程重新啟動 (如有必要)

```
process restart tacacsd
```

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）。