在具有ISE的Nexus裝置上通過TLS 1.3配置TACACS+

目錄

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NX-OS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 NX-OS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 — 配置基於TLS的TACACS+的Cisco NX-OS

必要條件

需求

通過TLS配置TACACS+的先決條件：

- 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

本檔案中的資訊是根據以下軟體和硬體版本：

- ISE VMware虛擬裝置，版本3.4補丁2。
- Nexus 9000交換機型號C9364D-GX2A，Cisco NX-OS版本10.5(3t)。

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。

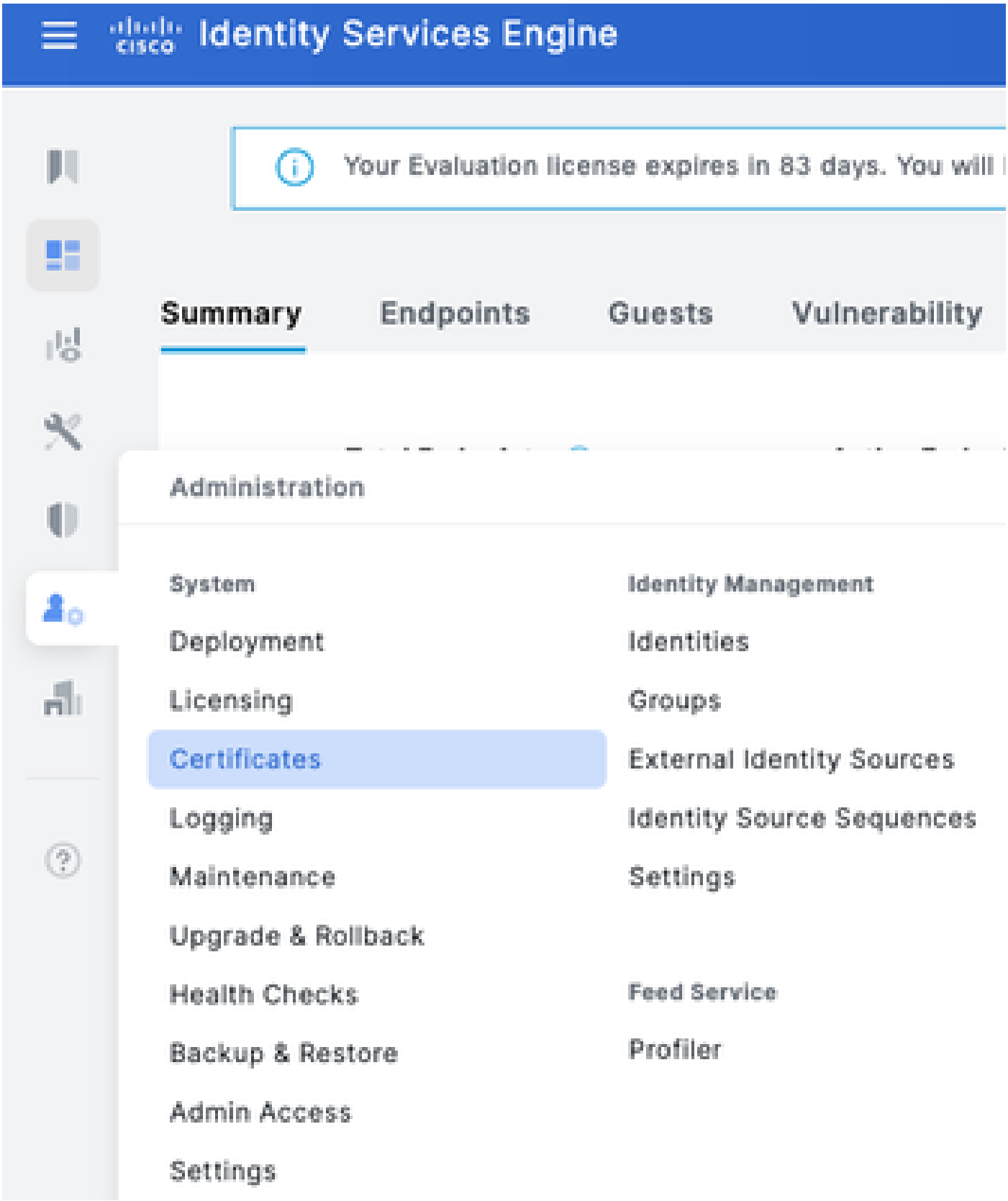
為裝置管理員配置ISE

生成TACACS+伺服器身份驗證的證書簽名請求

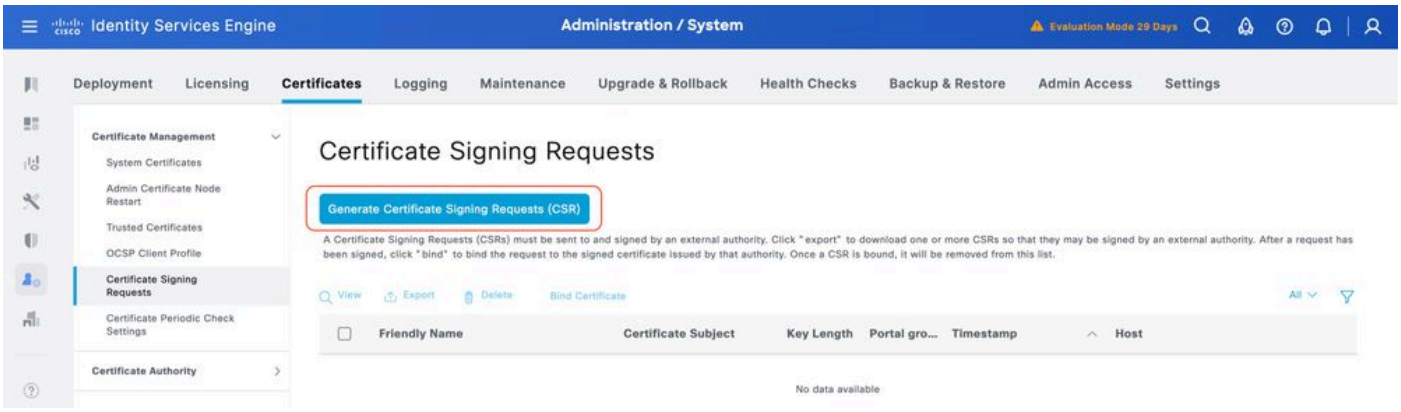
步驟1.使用其中一個受支援的瀏覽器登入ISE管理員Web門戶。

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。

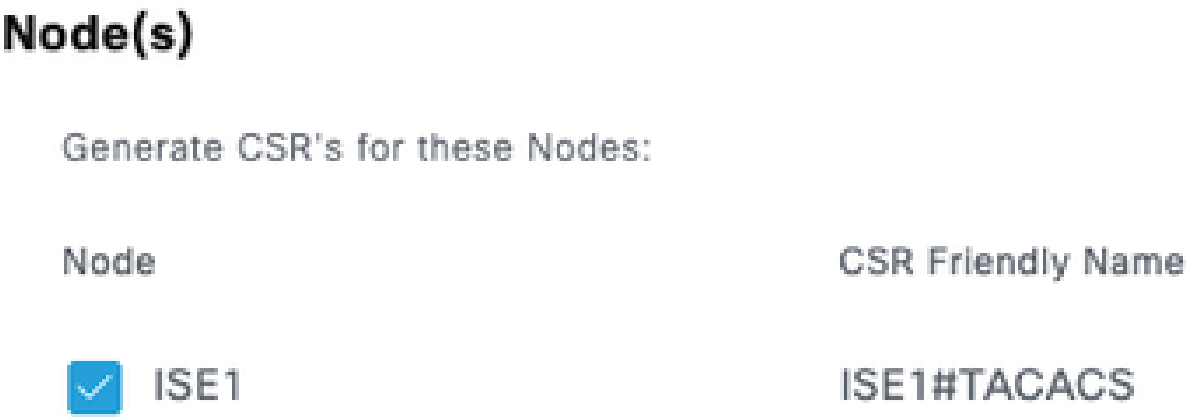


步驟 3. 在Certificate Signing Requests下，按一下Generate Certificate Signing Request。

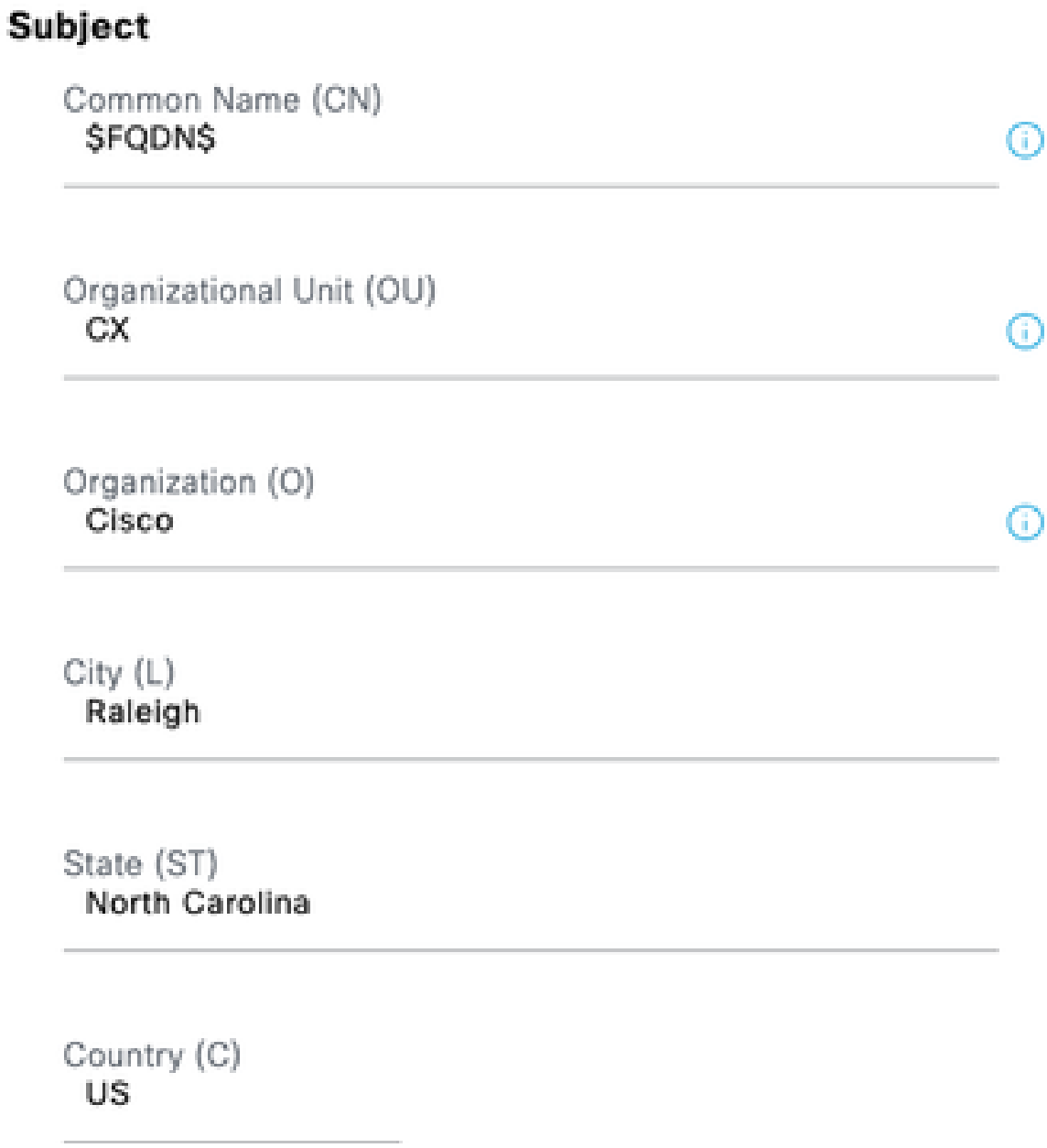


步驟4.在Usage中選擇TACACS。

步驟5.選擇已啟用TACACS+的PSN。



步驟6.使用適當的資訊填充Subject欄位。



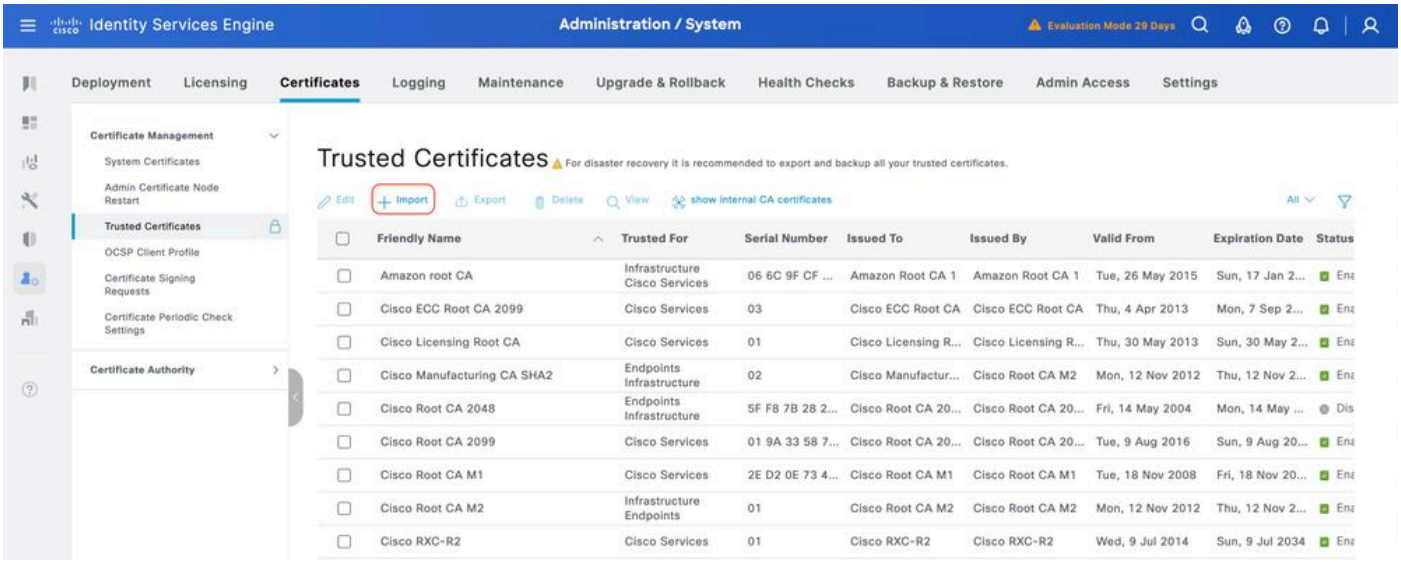
步驟7.在使用者替代名稱(SAN)下新增DNS Name和IP Address。

步驟8.按一下Generate，然後Export。

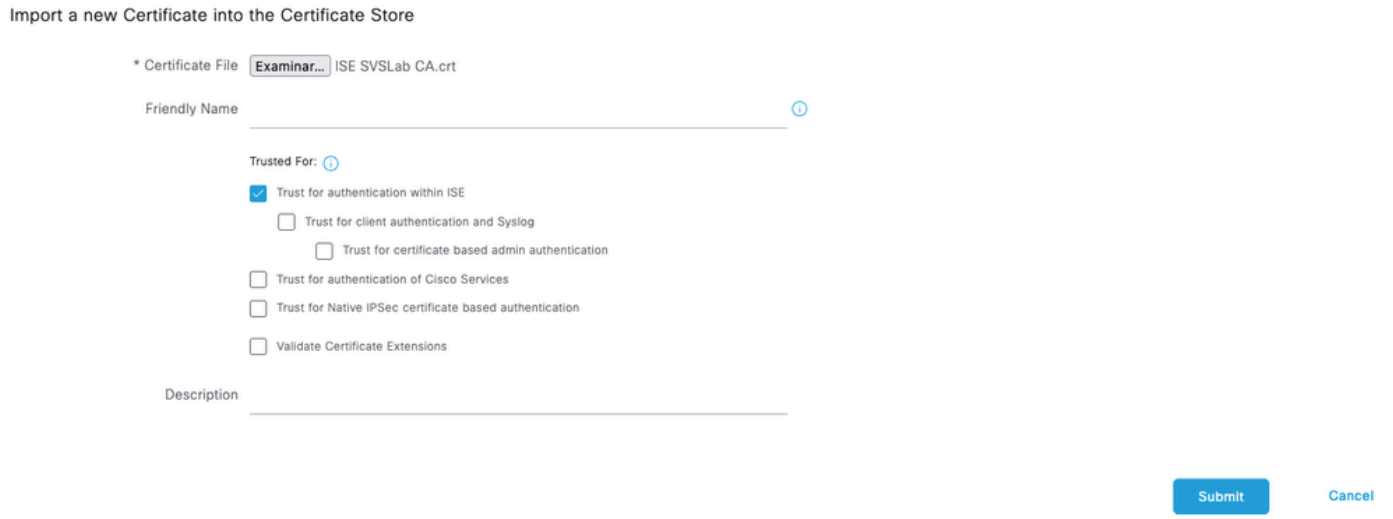
現在，您可以讓證書頒發機構(CA)簽署證書(CRT)。

上傳用於TACACS+伺服器身份驗證的根CA證書

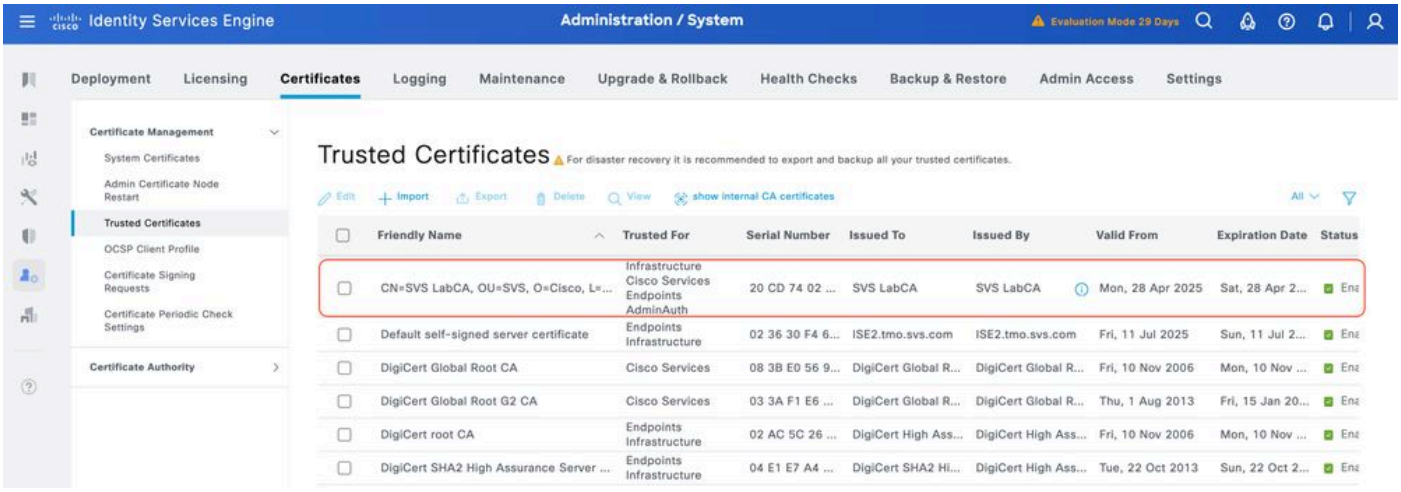
步驟1.導覽至Administration > System > Certificates。在Trusted Certificates下，按一下Import。



步驟2.選擇由證書頒發機構(CA)頒發的證書，該證書頒發機構對您的TACACS證書簽名請求(CSR)進行簽名。確保啟用ISE中的身份驗證信任選項。



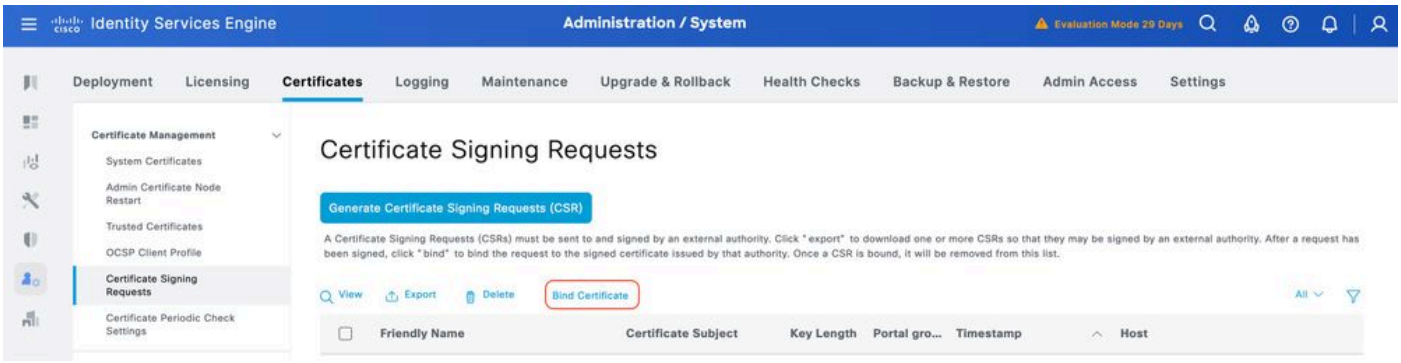
按一下提交。證書現在必須出現在受信任證書下。



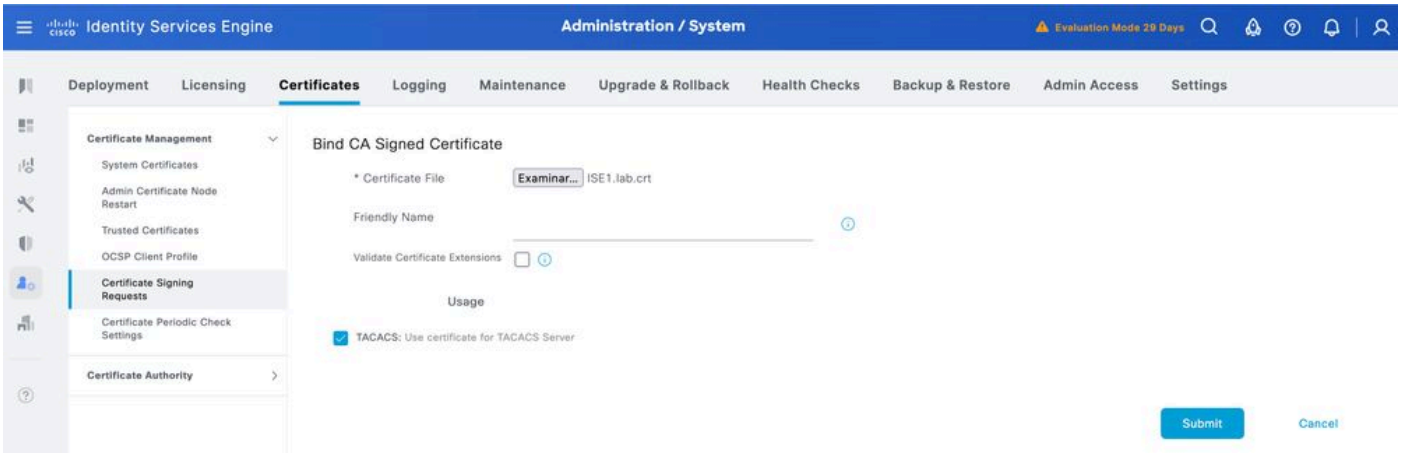
將簽名證書簽名請求(CSR)繫結到ISE

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，選擇上一步中產生的TACACS CSR，然後按一下Bind Certificate。

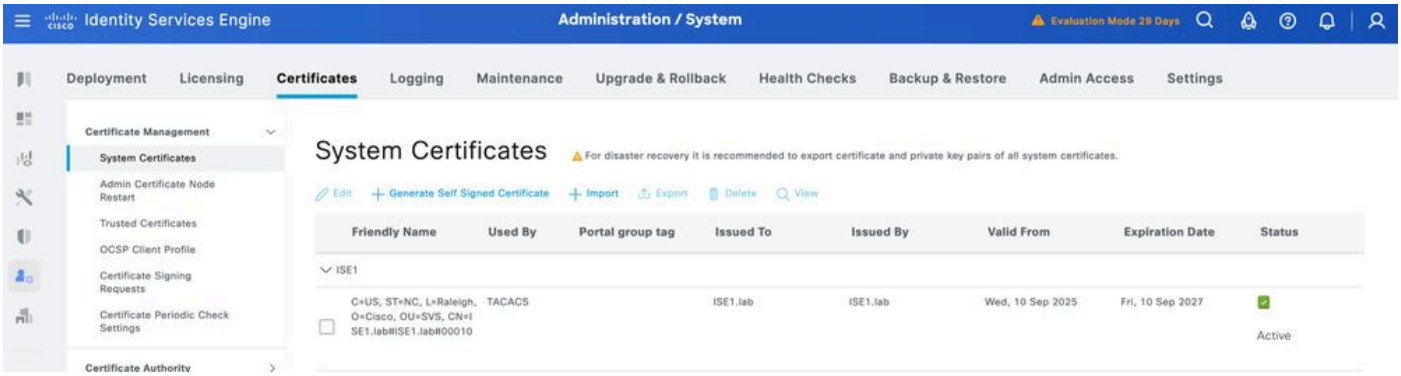


步驟2.選擇已簽名的證書，並確保「用法」下的「TACACS」覈取方塊保持選中狀態。



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。

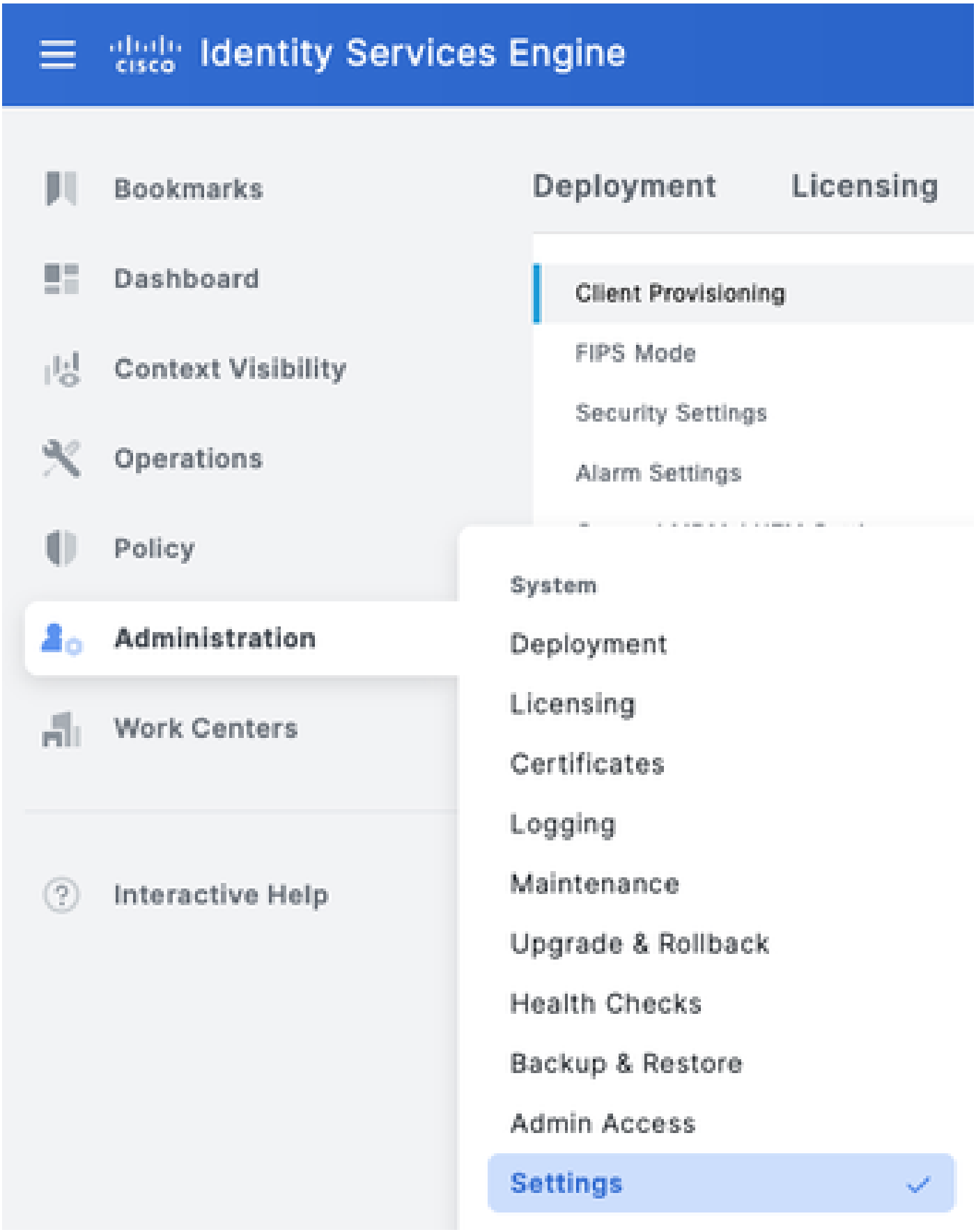
現在必須正確安裝證書。您可以在系統憑證下驗證這一點。



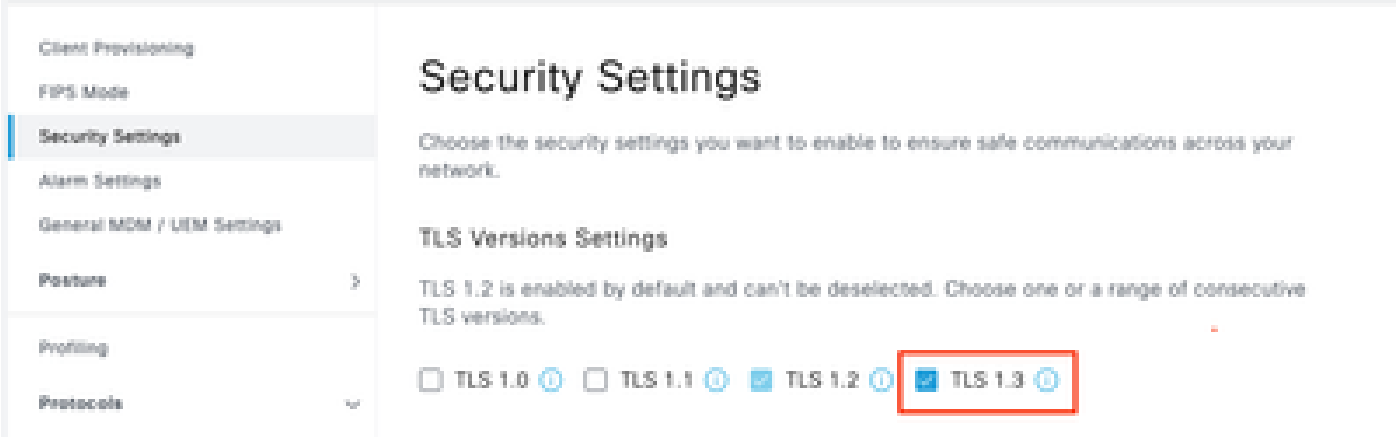
啟用TLS 1.3

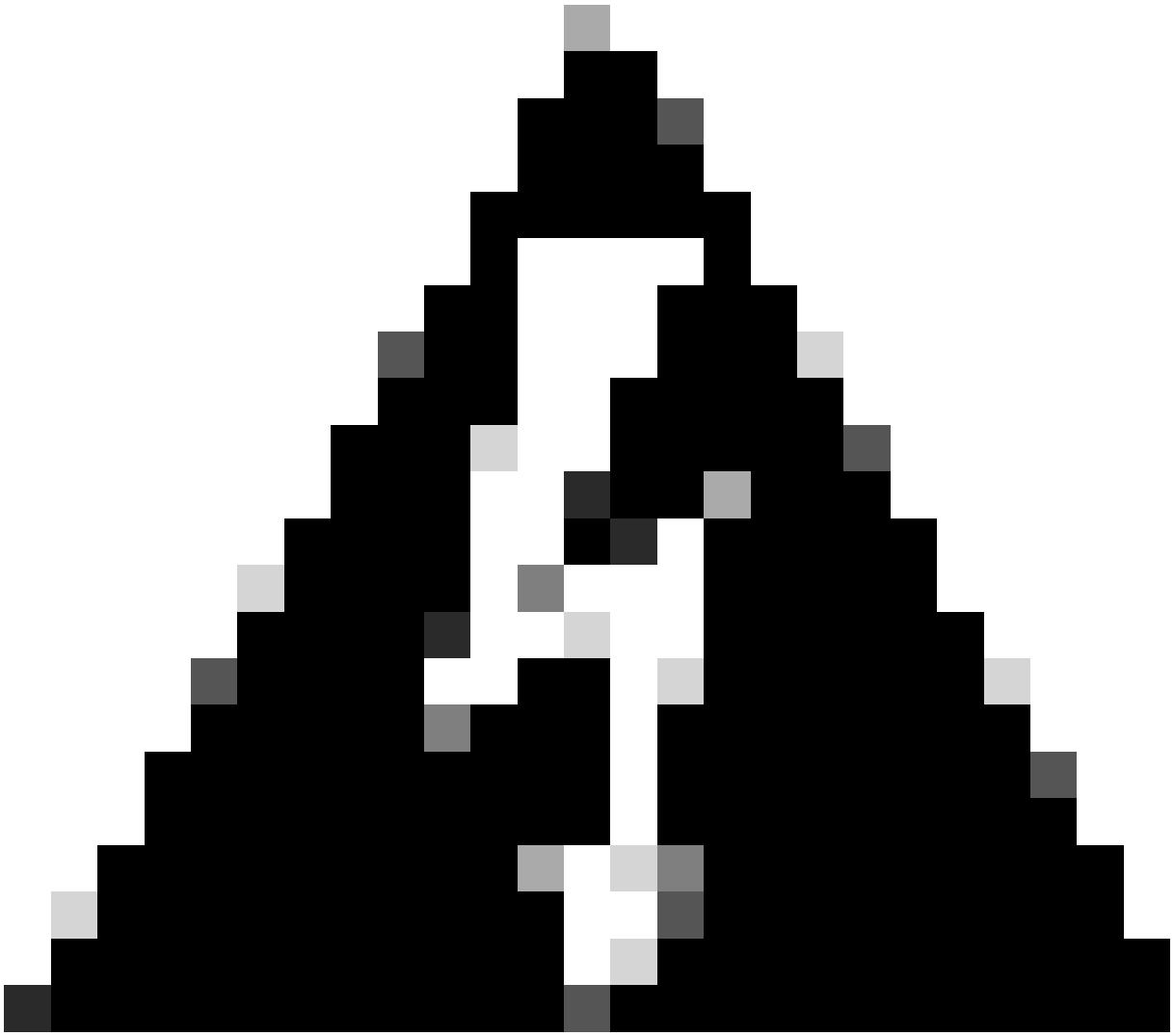
ISE 3.4.x中預設未啟用TLS 1.3。必須手動啟用。

步驟1.導覽至Administration > System > Settings。



步驟2.按一下Security Settings，選中TLS1.3（在TLS版本設定下）旁的覈取方塊，然後按一下Save。



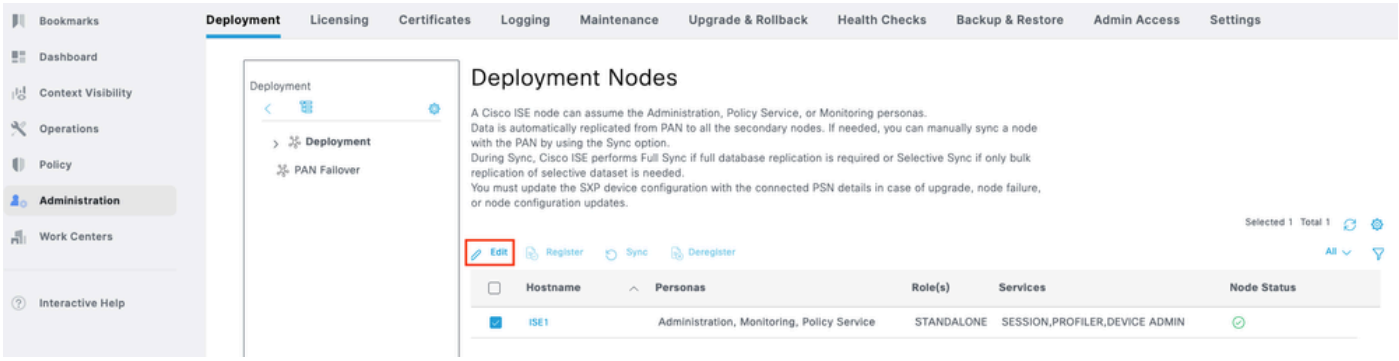


警告：當您更改TLS版本時，思科ISE應用伺服器在所有思科ISE部署電腦上重新啟動。

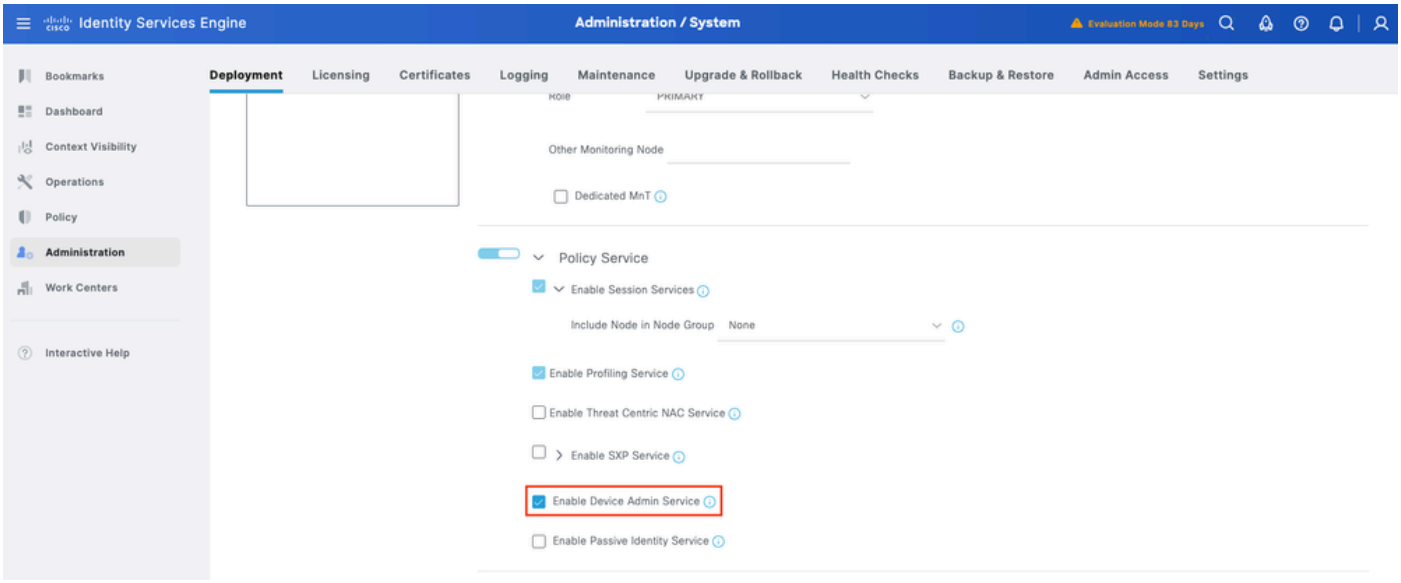
在ISE上啟用裝置管理

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。



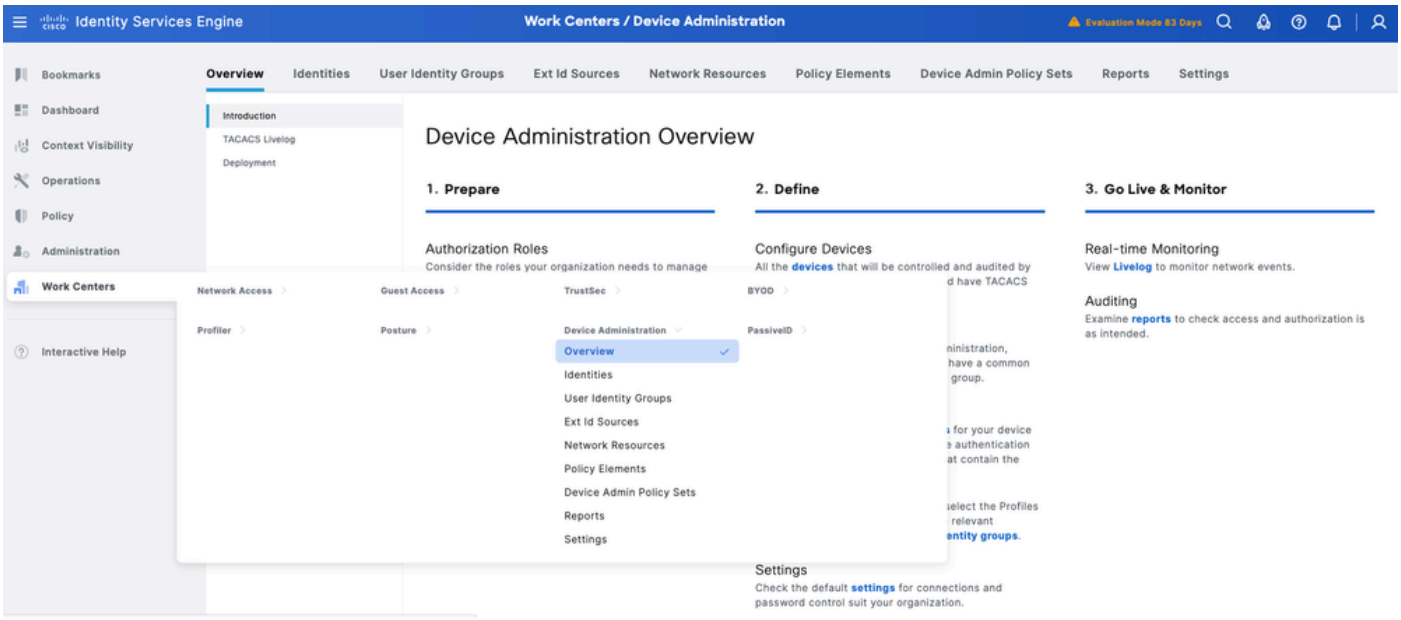
步驟2.在General Settings下，向下滾動並選中Enable Device Admin Service旁邊的覈取方塊。



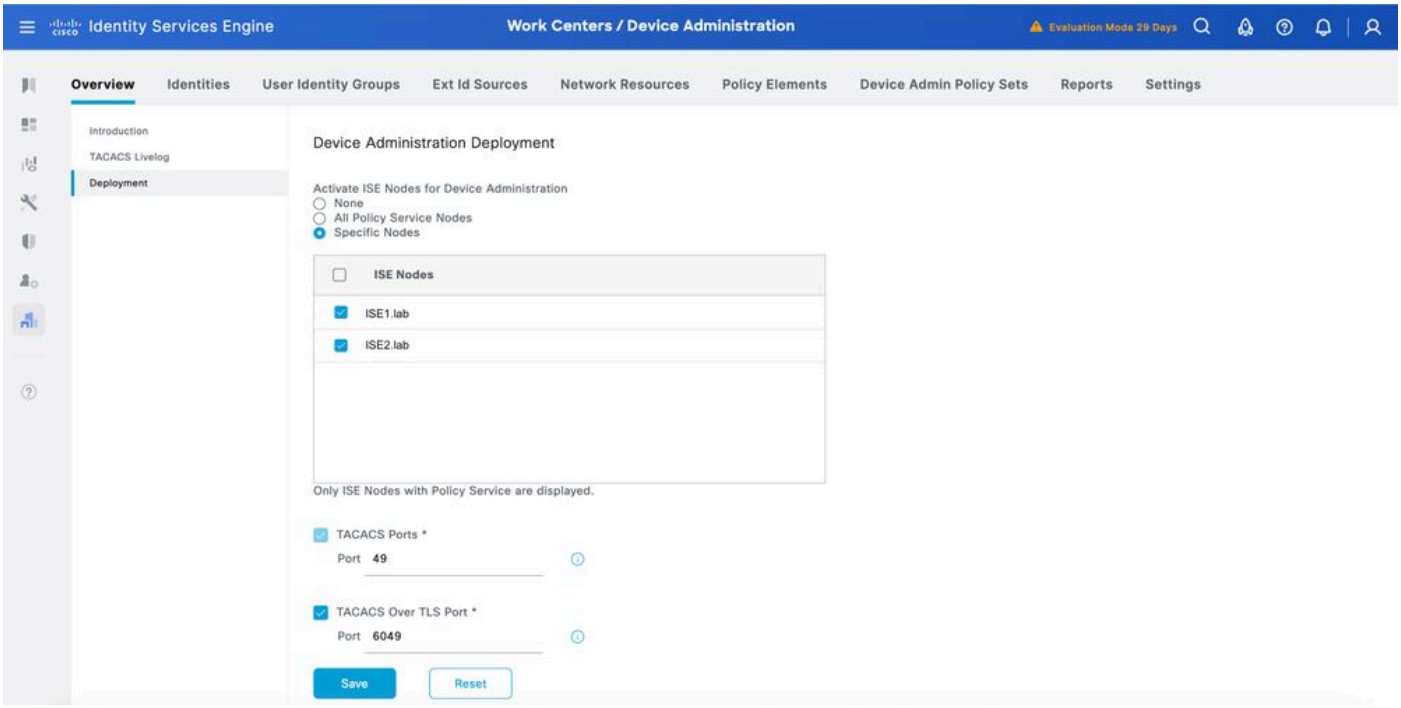
步驟3. 儲存組態。裝置管理服務現在在ISE上啟用。

啟用TLS上的TACACS

步驟1.定位至工作中心>裝置管理>概覽。



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

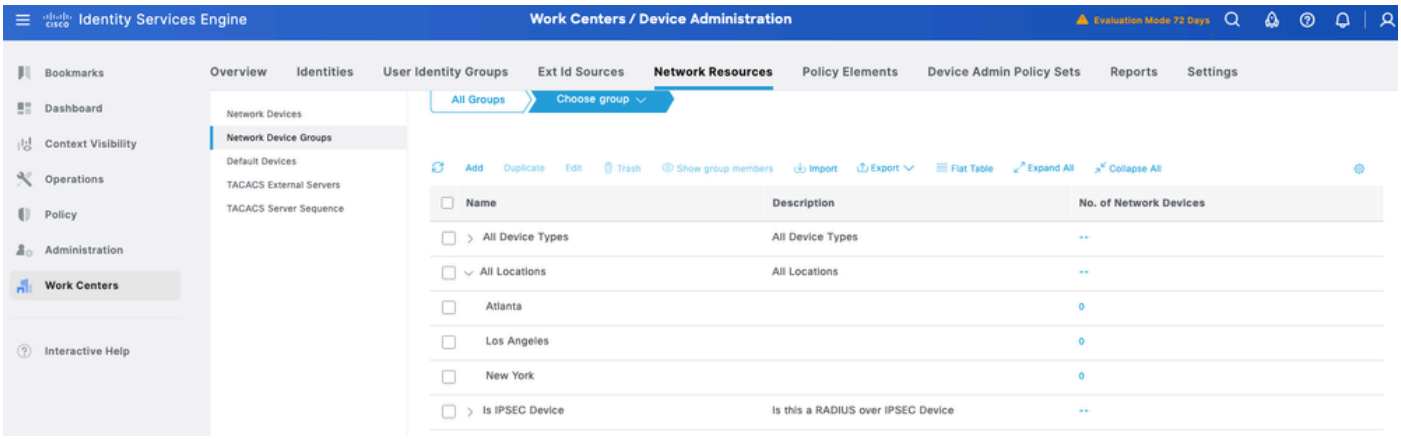


步驟3.保留預設埠6049，或者為TLS上的TACACS指定不同的TCP埠，然後按一下Save。

網路裝置和網路裝置組

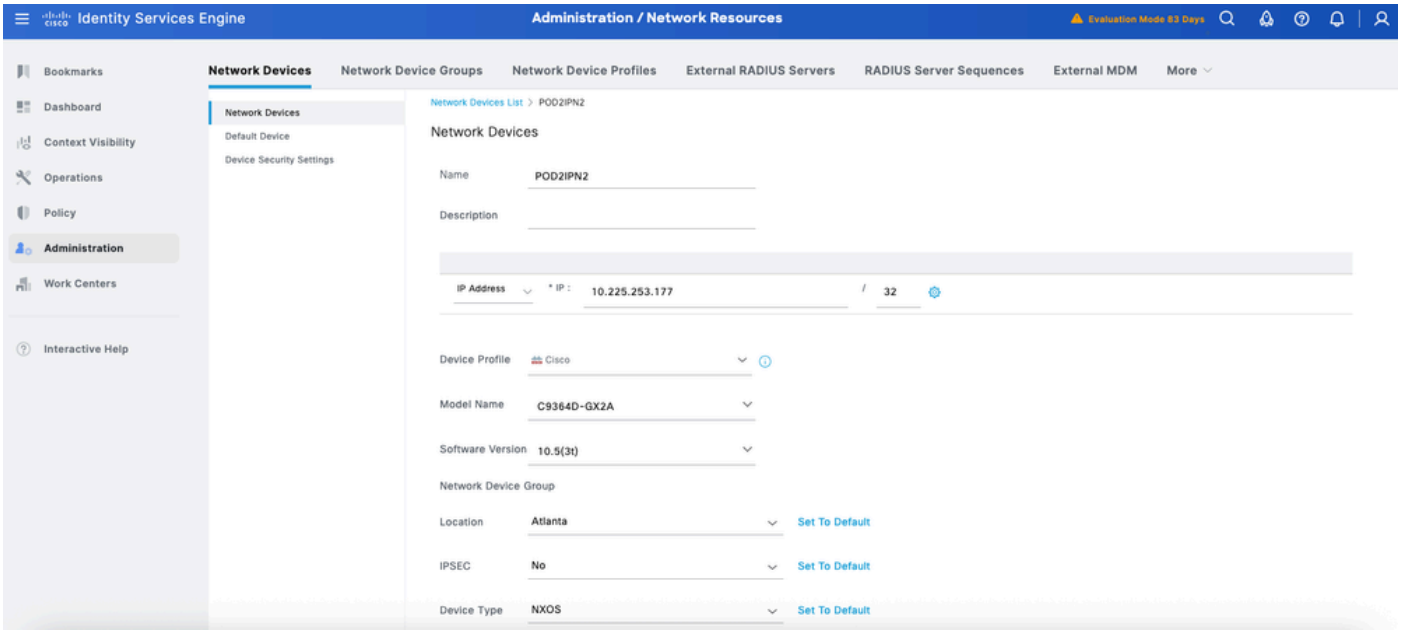
ISE提供具有多個裝置組層次結構的強大裝置分組。每個層次代表網路裝置的不同、獨立的分類。

步驟1。導覽至工作中心>裝置管理>網路資源。按一下Network Device Groups。

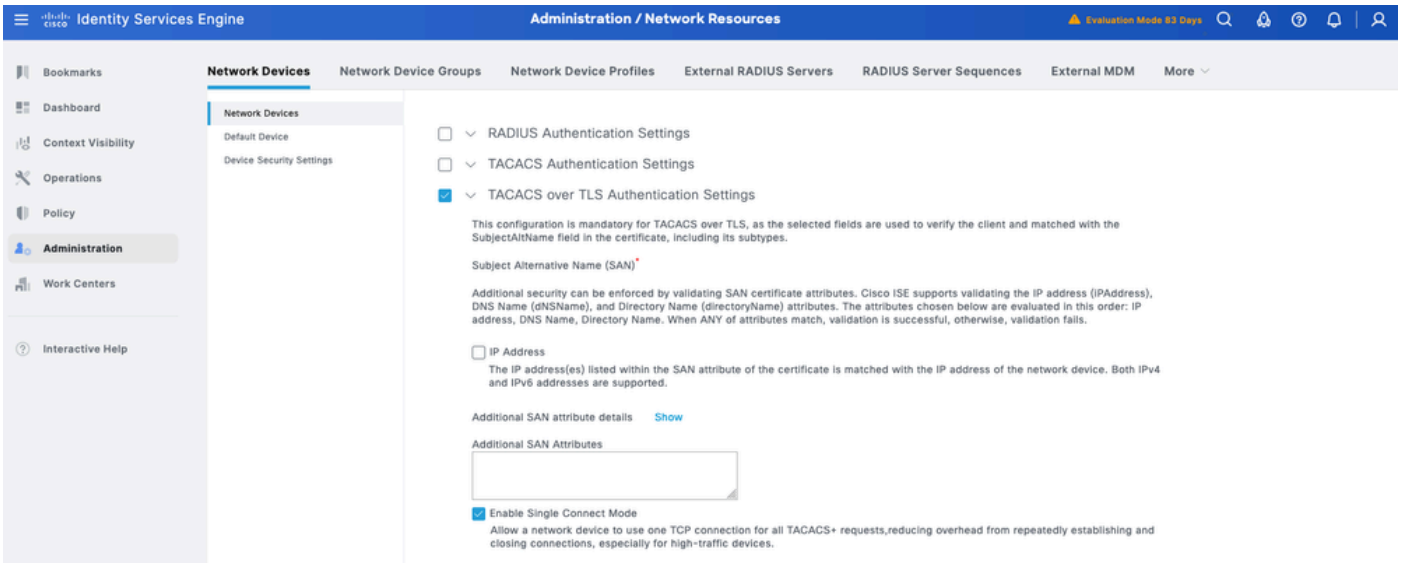


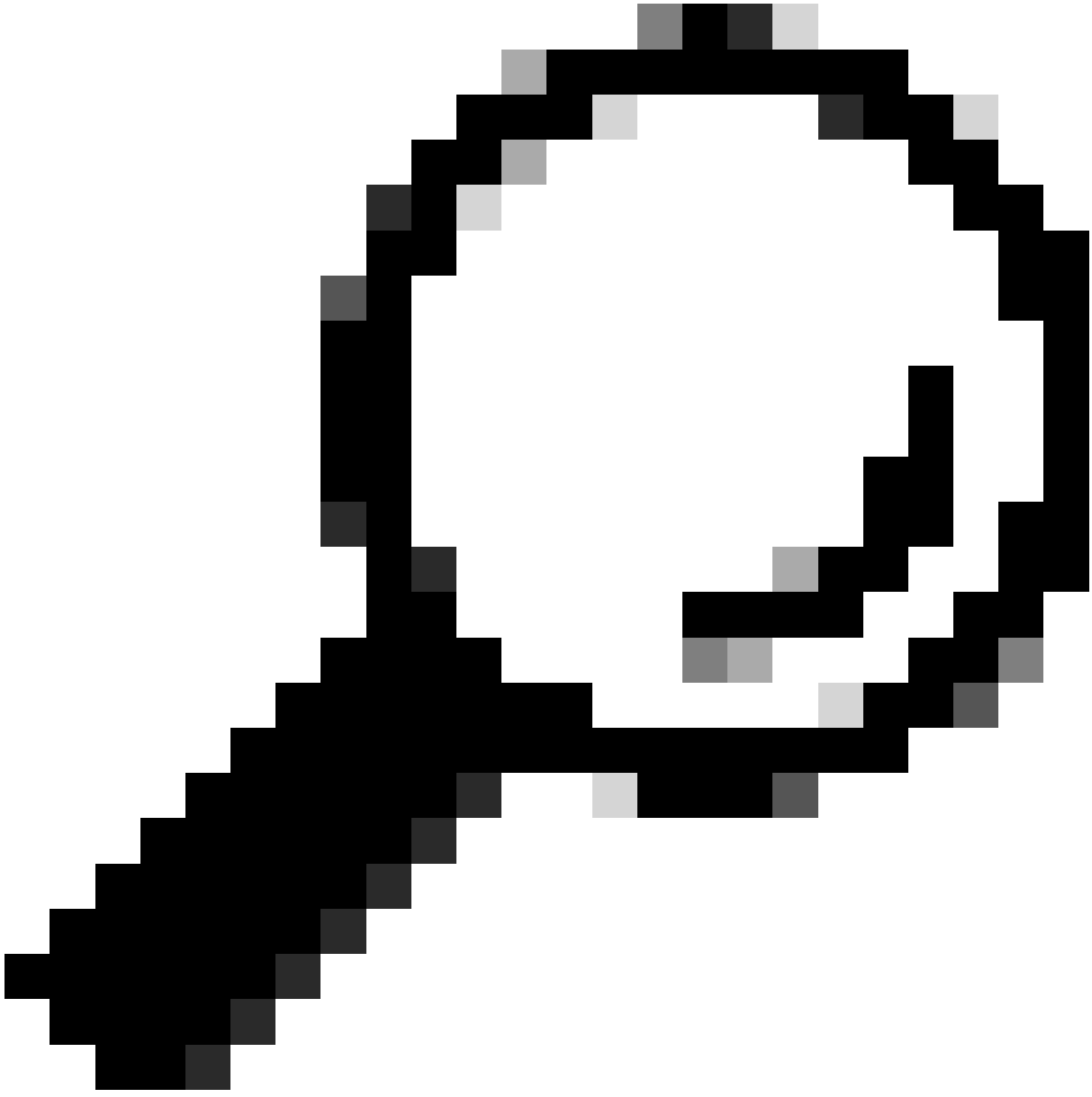
所有裝置型別和所有位置是ISE提供的預設層次結構。您可以新增自己的層次結構並在標識網路裝置時定義各種元件，這些元件以後可以在「策略條件」中使用。

步驟2.現在新增NS-OX裝置作為網路裝置。導航至工作中心>裝置管理>網路資源。按一下Add新增新的網路裝置POD2IPN2。



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


Identity Services Engine
Administration / Network Resources
Evaluation Mode 83 Days
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.

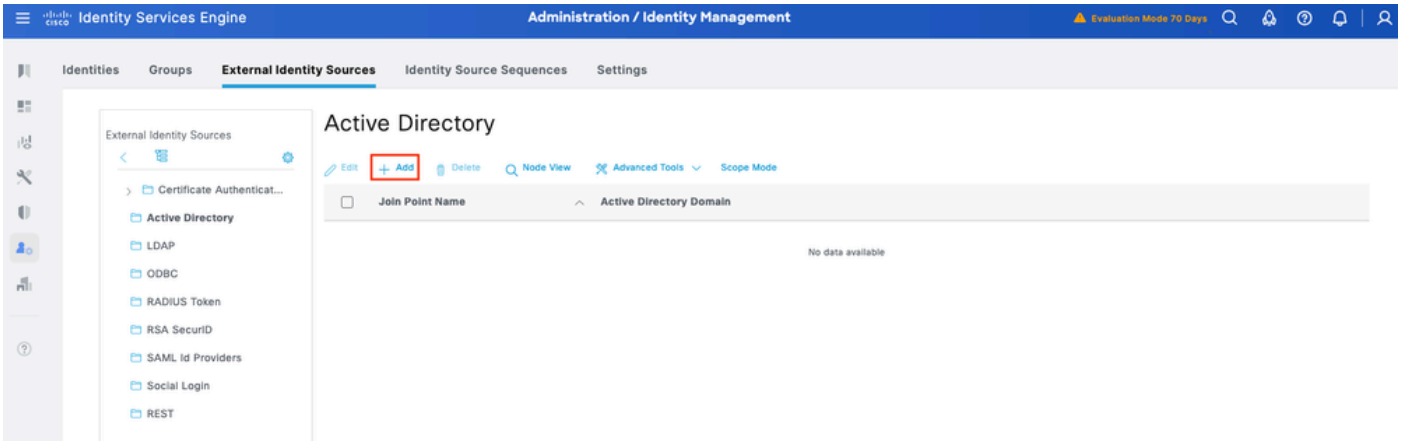


提示：建議啟用單一連線模式，以避免每次向裝置傳送命令時重新啟動TCP會話。

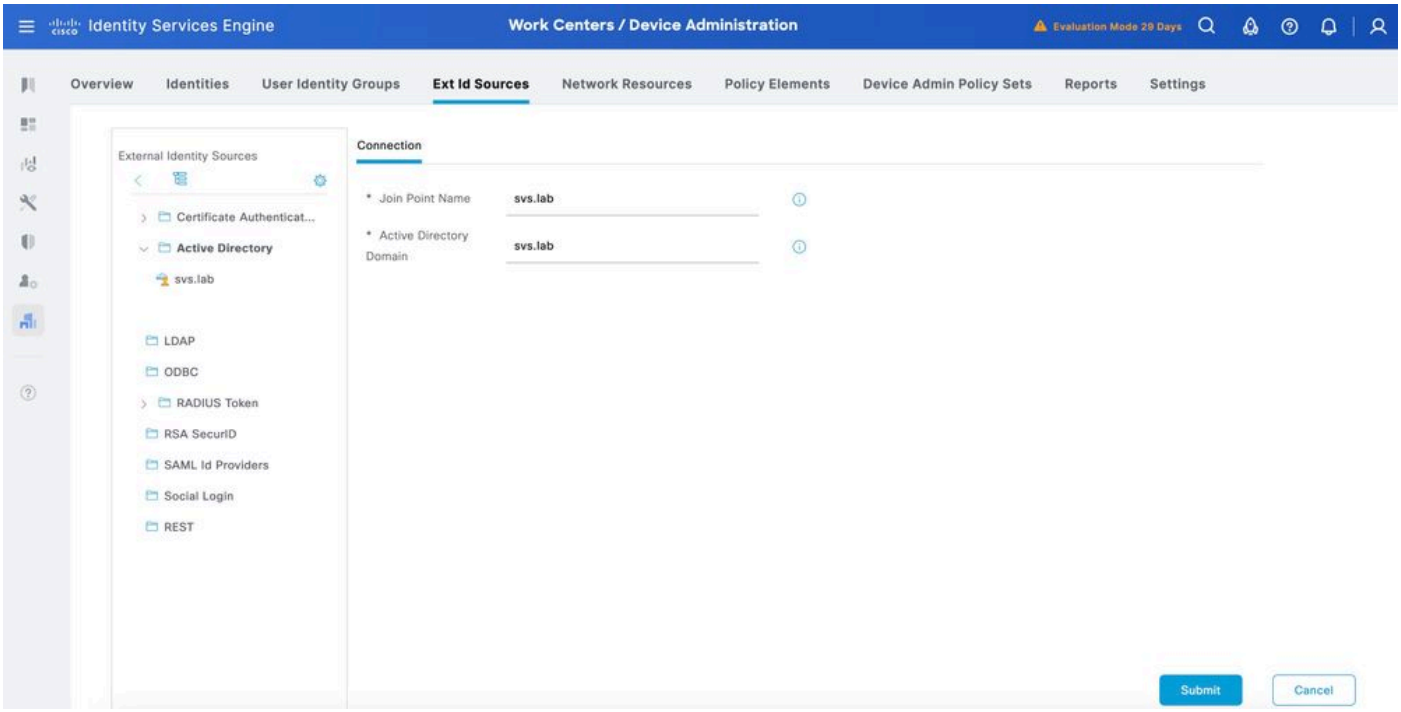
配置身份庫

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Add以定義新的AD關節點。

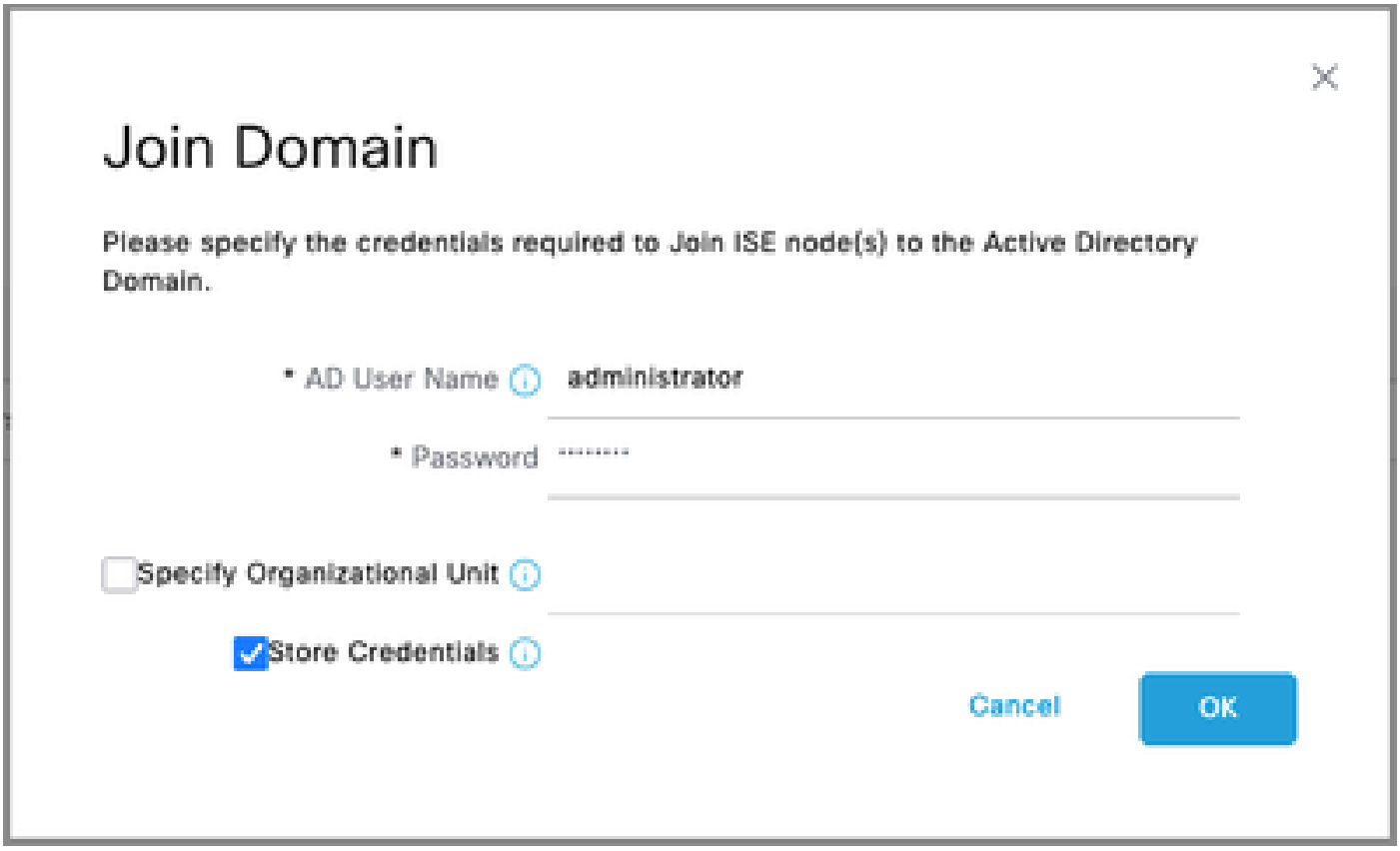


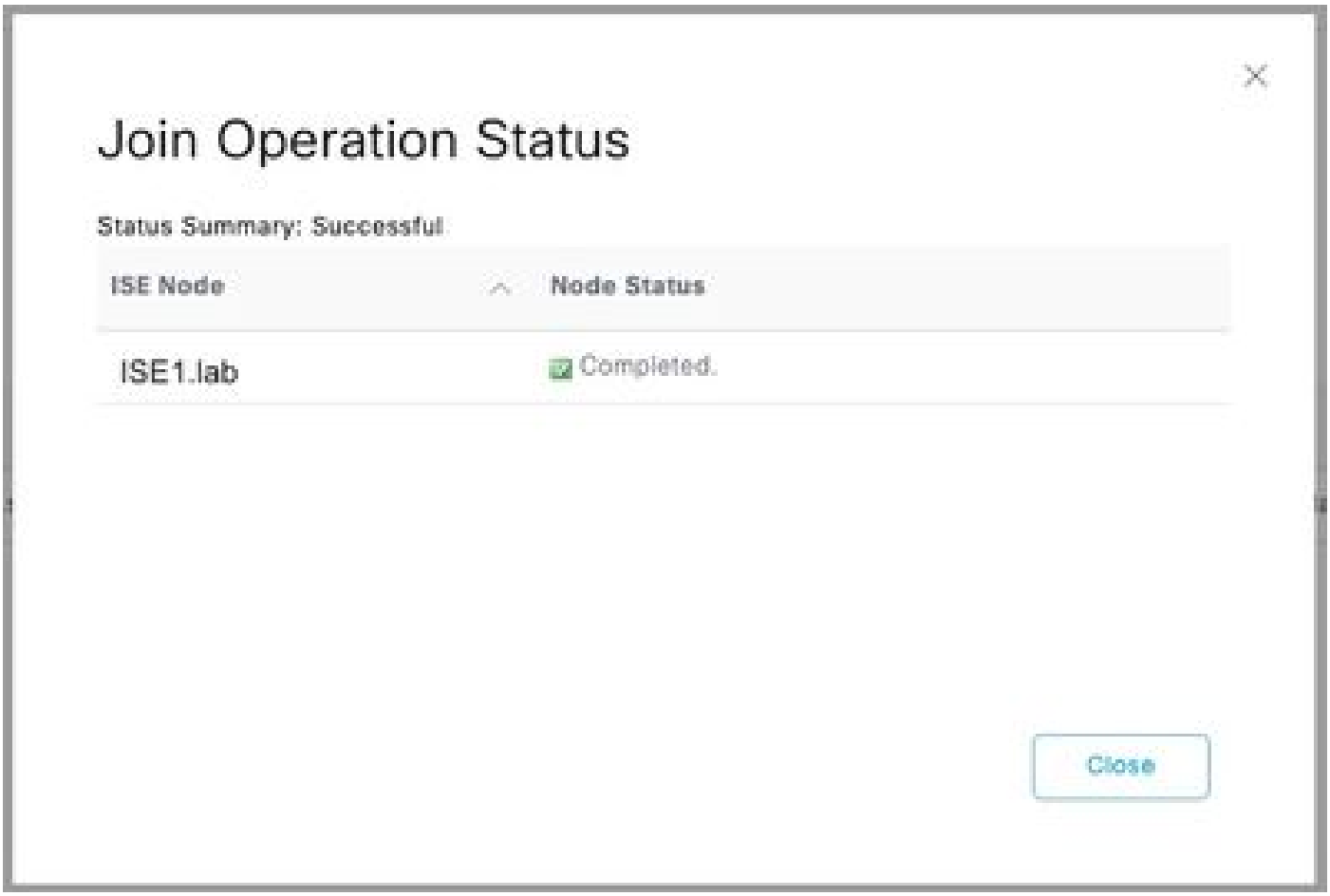
步驟2.指定加入點名和AD域名，然後按一下提交。



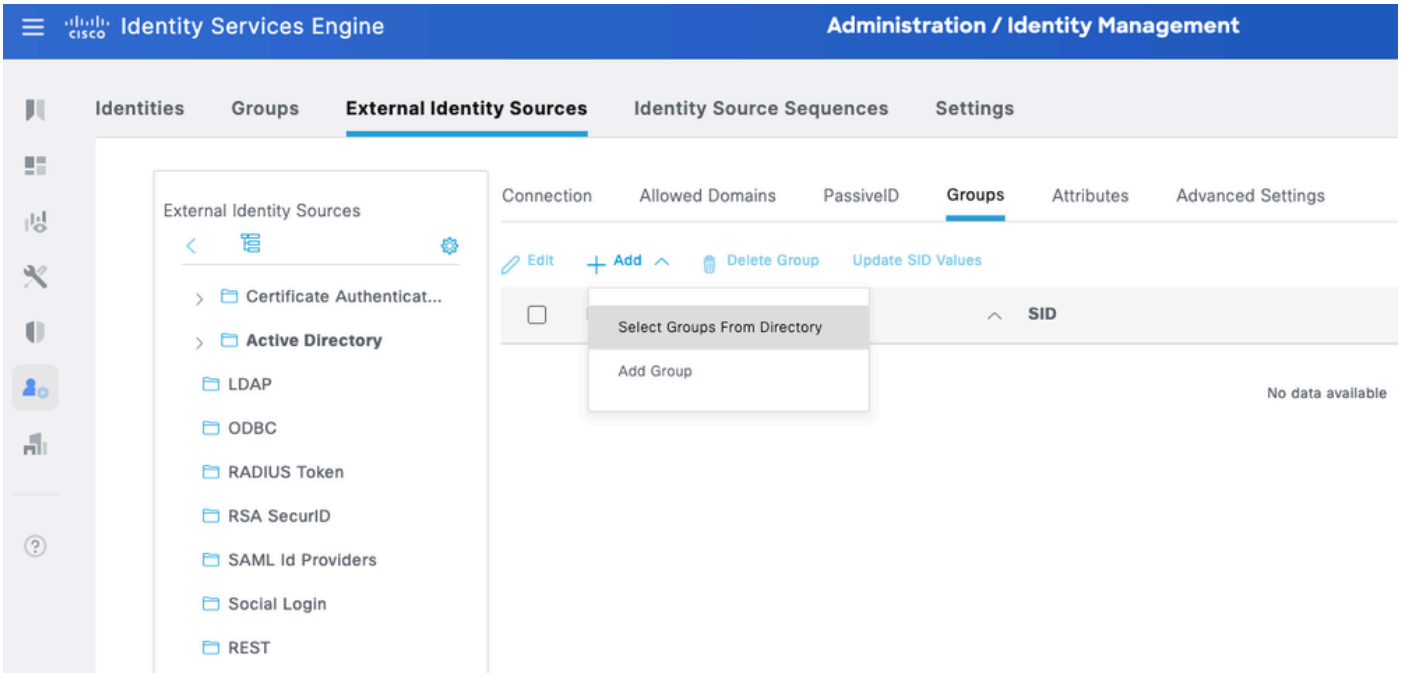
步驟3.出現提示「Would you like to Join all ISE Nodes to this Active Directory Domain？（是否要將所有ISE節點加入此Active Directory域？）」時，按一下Yes。

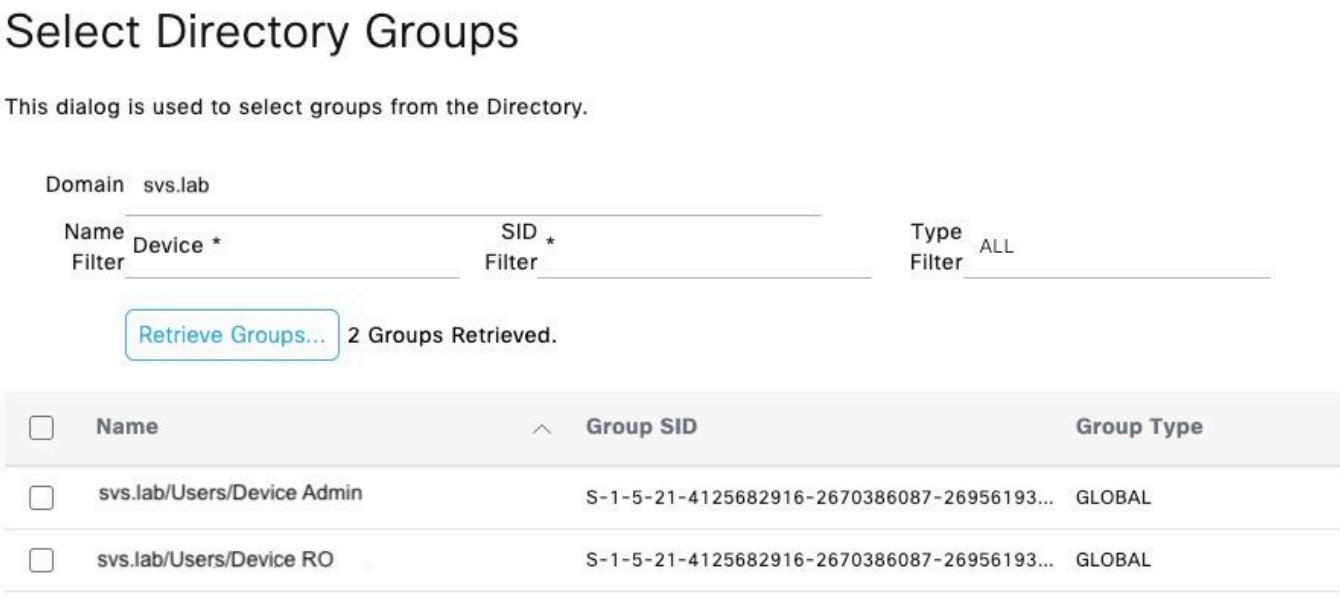
步驟4.輸入具有AD加入許可權的憑證，並輸入將ISE加入AD。檢查「Status（狀態）」以驗證其是否可操作。

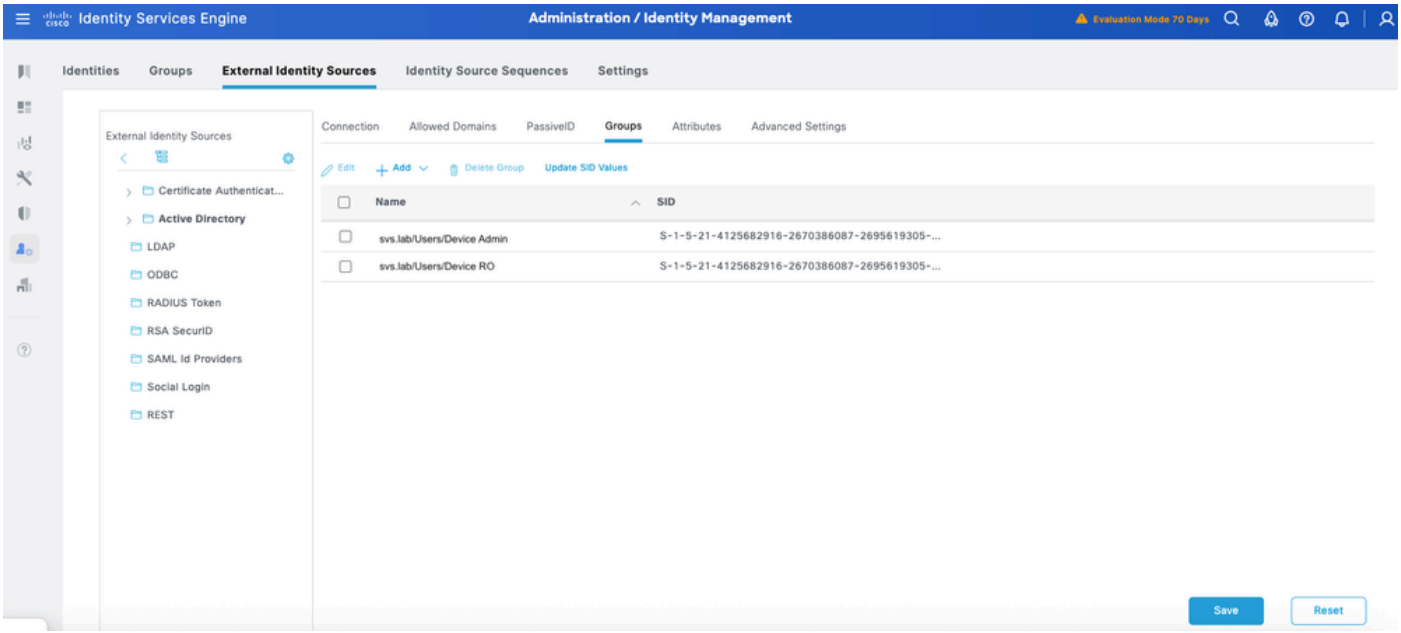




步驟5.導航到Groups頁籤，然後點選Add以獲取授權使用者訪問裝置所需的所有組。此示例顯示本指南的授權策略中使用的組。







設定TACACS+外殼設定檔

與使用許可權級別進行授權的Cisco IOS裝置不同，Cisco NX-OS裝置實施基於角色的訪問控制(RBAC)。 在ISE中，可以使用Nexus型別的常見任務將TACACS+配置檔案對映到思科NX-OS裝置上的使用者角色。

NX-OS裝置上的預定義角色在NX-OS平台上有所不同。兩種常見情況是：

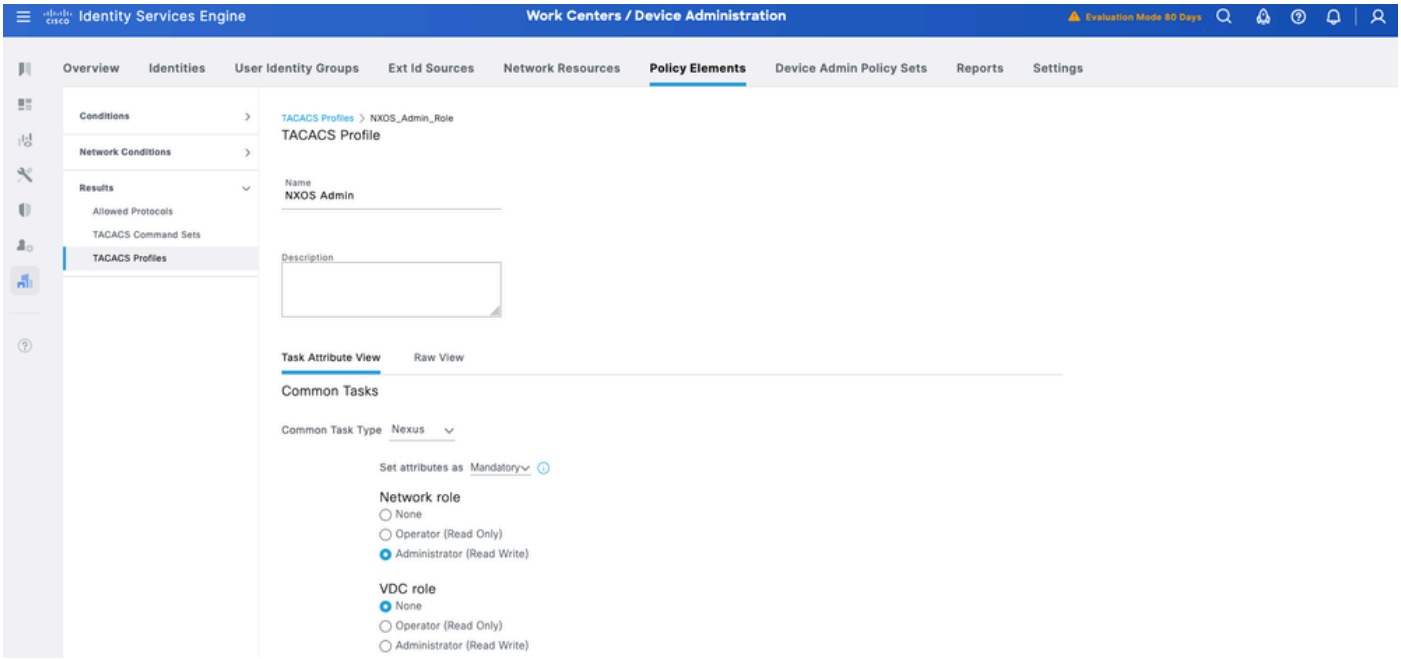
- network-admin — 預定義的網路管理員角色對交換機上的所有命令具有完全的讀寫訪問許可權；僅當裝置（例如Nexus 7000）具有多個VDC時，在預設虛擬裝置環境(VDC)中可用。使用NX-OS CLI命令show cli syntax roles network-admin檢視可用於此角色的完整命令清單。
- network-operator — 預定義的網路管理員角色對交換機上的所有命令具有完全讀取訪問許可權；僅在裝置（例如Nexus 7000）有多個VDC時可用。使用NX-OS CLI命令show cli syntax roles network-operator檢視可用於此角色的完整命令清單。

接下來，定義兩個TACACS配置檔案 — NXOS管理員和NXOS幫助台。

NX-OS管理員

步驟1.新增另一個配置檔案，並將其命名為NX-OS Admin。

步驟2.從Set attributes as下拉選單中選擇Mandatory。在常見任務下選擇Network-role選項中的Administrator。



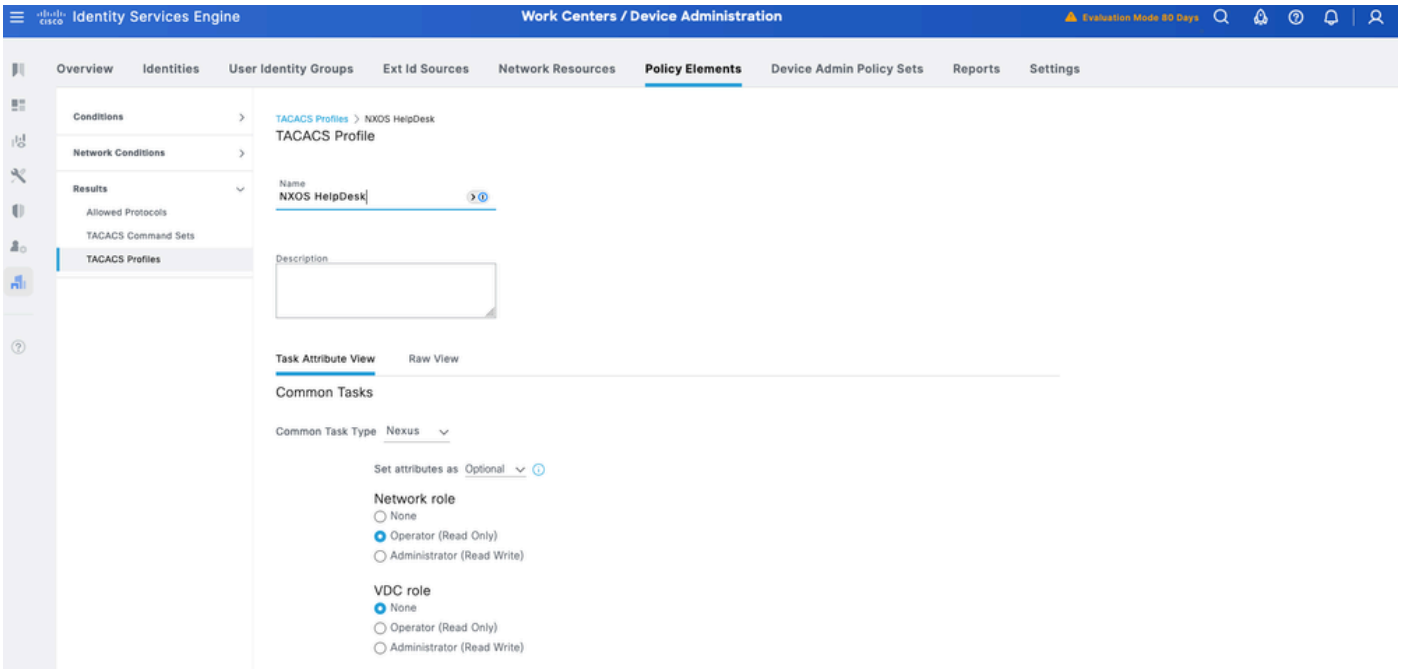
步驟3.按一下Submit以儲存設定檔。

NX-OS幫助台

步驟1.從ISE UI導航至工作中心>裝置管理>策略元素>結果> TACACS配置檔案。新增新的TACACS配置檔案，並將其命名為NXOS HelpDesk。轉到「常見任務型別」下拉選單並選擇Nexus。

您可以看到特定於使用者角色的模板更改。您可以選擇與要配置的使用者角色對應的這些選項。

步驟2.從Set attributes as下拉選單中選擇Mandatory。在常見任務下選擇Network-role選項中的Operator。

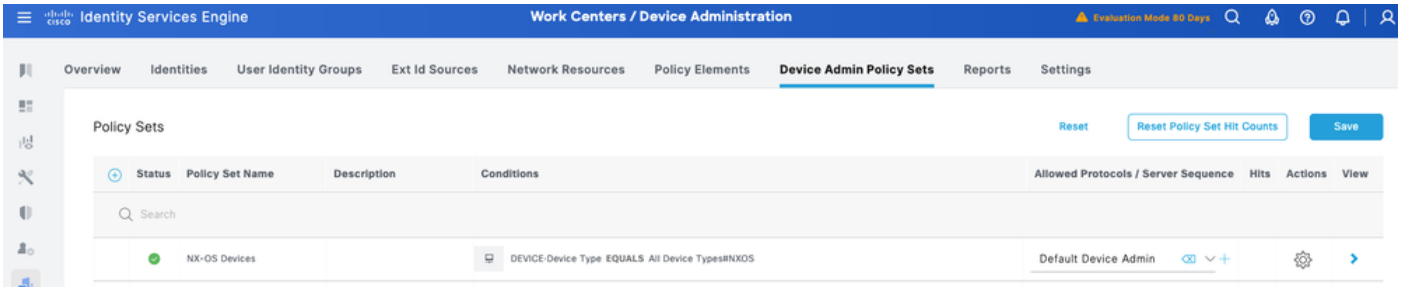


步驟 3. 按一下Save儲存配置檔案。

配置裝置管理策略集

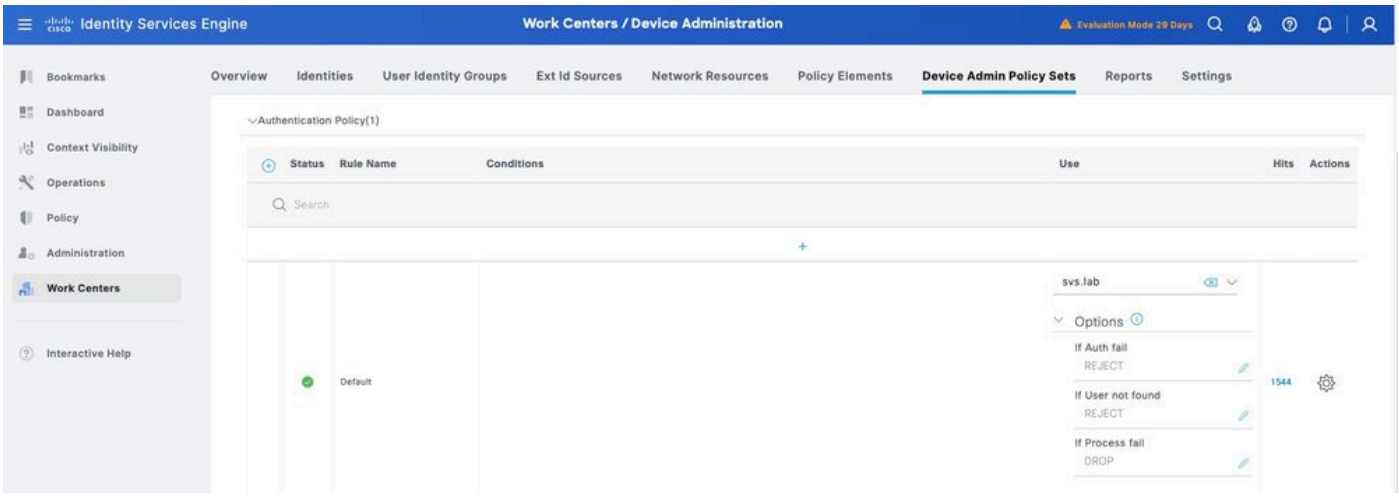
預設情況下會啟用「裝置管理」策略集。策略集可以根據裝置型別劃分策略，以簡化TACACS配置檔案的應用。例如，Cisco IOS裝置使用許可權級別和/或命令集，而Cisco NX-OS裝置使用自定義屬性。

步驟1.導航到工作中心>裝置管理>裝置管理策略集。新增新的策略集NX-OS裝置。在condition下，指定DEVICE:Device Type EQUALS All Device Types#NXOS。在Allowed Protocols下，選擇Default Device Admin。



步驟2.按一下Save，然後按一下右箭頭以配置此策略集。

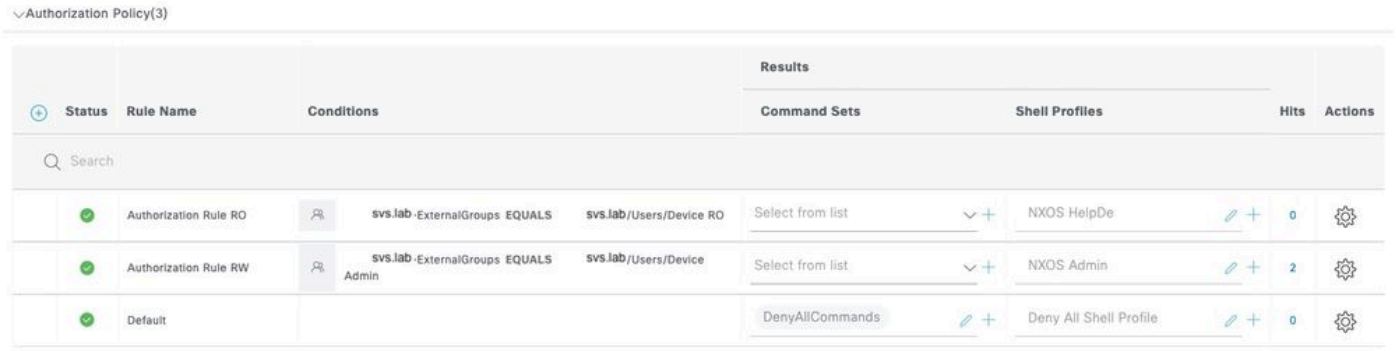
步驟3.建立身份驗證策略。對於身份驗證，您將AD用作ID Store。保留If Auth fail、If User not found和If Process fail下的預設選項。



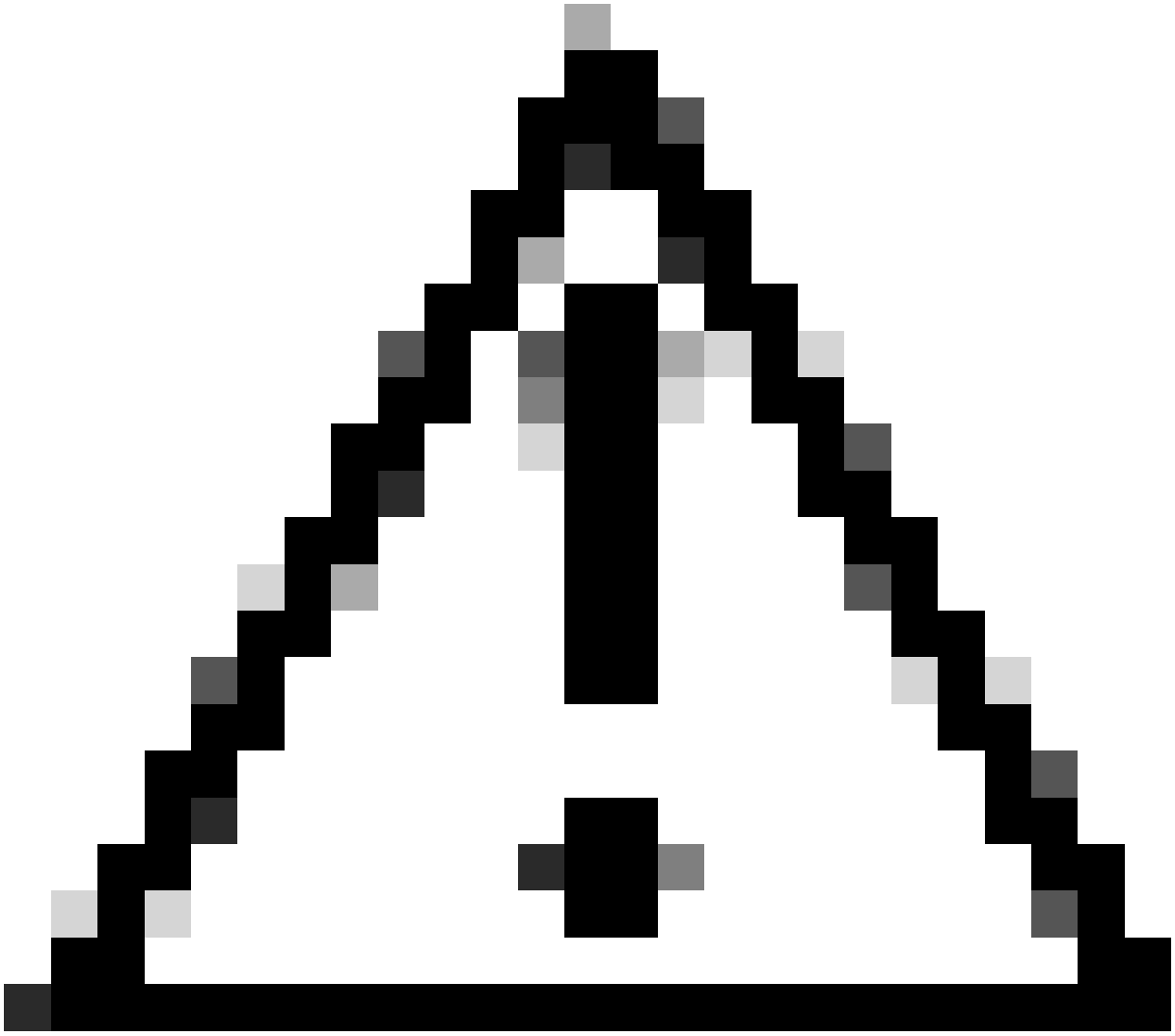
步驟4.定義授權策略。

根據Active Directory(AD)中的使用者組建立授權策略。

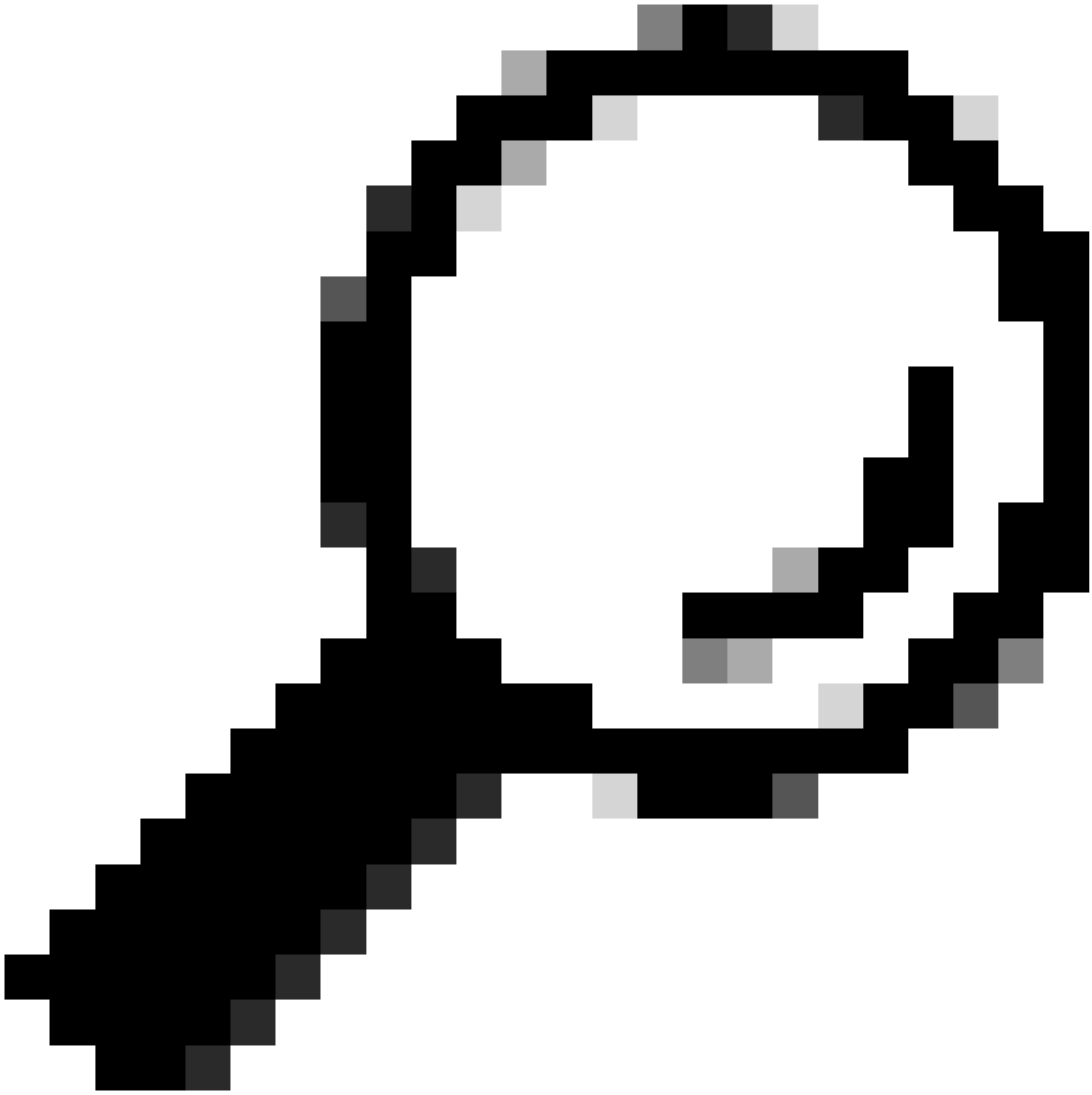
舉例來說：
·為AD組Device Admin中的使用者分配NXOS Admin TACACS配置檔案。
·為AD組裝置RO中的使用者分配NXOS幫助台TACACS配置檔案。



配置通過TLS的TACACS+的Cisco NX-OS



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。

TACACS+伺服器組態

步驟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
```

信任點配置

步驟1.建立密鑰標籤，在您的情況下使用ecc金鑰對。

<#root>

POD2IPN2(config)#

crypto key generate ecc label ec521-label exportable modulus 521

步驟2.將此值與信任點關聯。

<#root>

POD2IPN2(config)#

crypto ca trustpoint ec521-tp

POD2IPN2(config-trustpoint)#

ecckeypair ec521-label

步驟3.安裝CA公鑰。

<#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-----
MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3sOJ/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
```

```
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh6OI4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMA0GCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----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)#
```

步驟4. 產生交換器身分識別憑證請求。

<#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: FDO2649OP4T
 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-----
MIIBtjCCARcCAQAwKTERMA8GA1UEAwwIUE9EMklQTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYTOiw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6LzpkOhPAGE4jBveNHxYeIA7PfNWvJ7xTBWjDNX
/IYBm6E7Hd7q42OmCe8Mef+bqJBdJ9wzpyEjhI2lIIoXt4814nBxObkIWWyR5cZN
IiXTLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MC0GCSqGSIb3DQEJDjEgMB4wHAYDVR0RAQH/BBIwEIIIUE9EMklQTjKHBArh/bEw
CgYIKoZIzj0EAwIDgYwAMIGIAkIAtzQ/knrW2ovCVoHAuq1v2cr0n3NenS/44lul
+3H1y52vn4Rm4CGU3wkzXU3qGO3YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt3OhpaDDOTWzzvZY7qFflCOl5p6pvUpHigqoZNg5
9xhNdM1CQSykOg==
-----END CERTIFICATE REQUEST-----
```

步驟5.匯入由CA簽名的交換機身份證書。

<#root>

```
POD2IPN2(config)#
```

crypto ca import ec521-tp certificate

```
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIDzTCCAbWgAwIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA3MTkxMDAwWhcNMjYwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
TOQySVBOMjEUMBIGA1UEBRMLRkRPMjYOOTBQNFQwgZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhPSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMFaMM1f8hgGboTsd3urjY6YJ7wx5/5uokFOn3DOn
ISOEjaUgihe3jzXicHE5uQhZbJHlxk0iJdMuTw/ggxm8+ryNGcQtHF3xEaNAMD4w
HgYJYIZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAcBgNVHREBAf8EEjAQgghQ
TOQySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msodOQK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZO1PUXNTyZidXpGd/yTrdQAl5JzpW4pEudrbCJMZEEYtqoP
wD+4OE8vKoYEgyWlDrpRZOZG1usZczuUhLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
liToeYy2Q0cTesSZCKvRBv6Ewj5JuSLemURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61LnlVxhXombiS6
INoa0GvQONrl+lFT8ADIdZ/Ukd5Ubhc9bh/sYzf4MWtkK1wVO16Hv7vGpSMYonD6
a271im+tJPyKnnezQ6OykzlGqsL/Ta6JOdip/fEYp8UmRq9InDh23gDjqrojWL7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJTlnuk5KCqFx//4P7mAoyZYiTIDp1pkYS
VK65fJKD+pYxIhSP9wN8rnwtzSCWb0Z78sgO06Y6wIXyTP0UB3FWhD+GxtTkmEce
ZnAQbgxpgrg5lhpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
```

```
lfKuuebdZkbwz72r7OyyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

驗證交換機身份證書是否已註冊。

<#root>

```
POD2IPN2(config)#
```

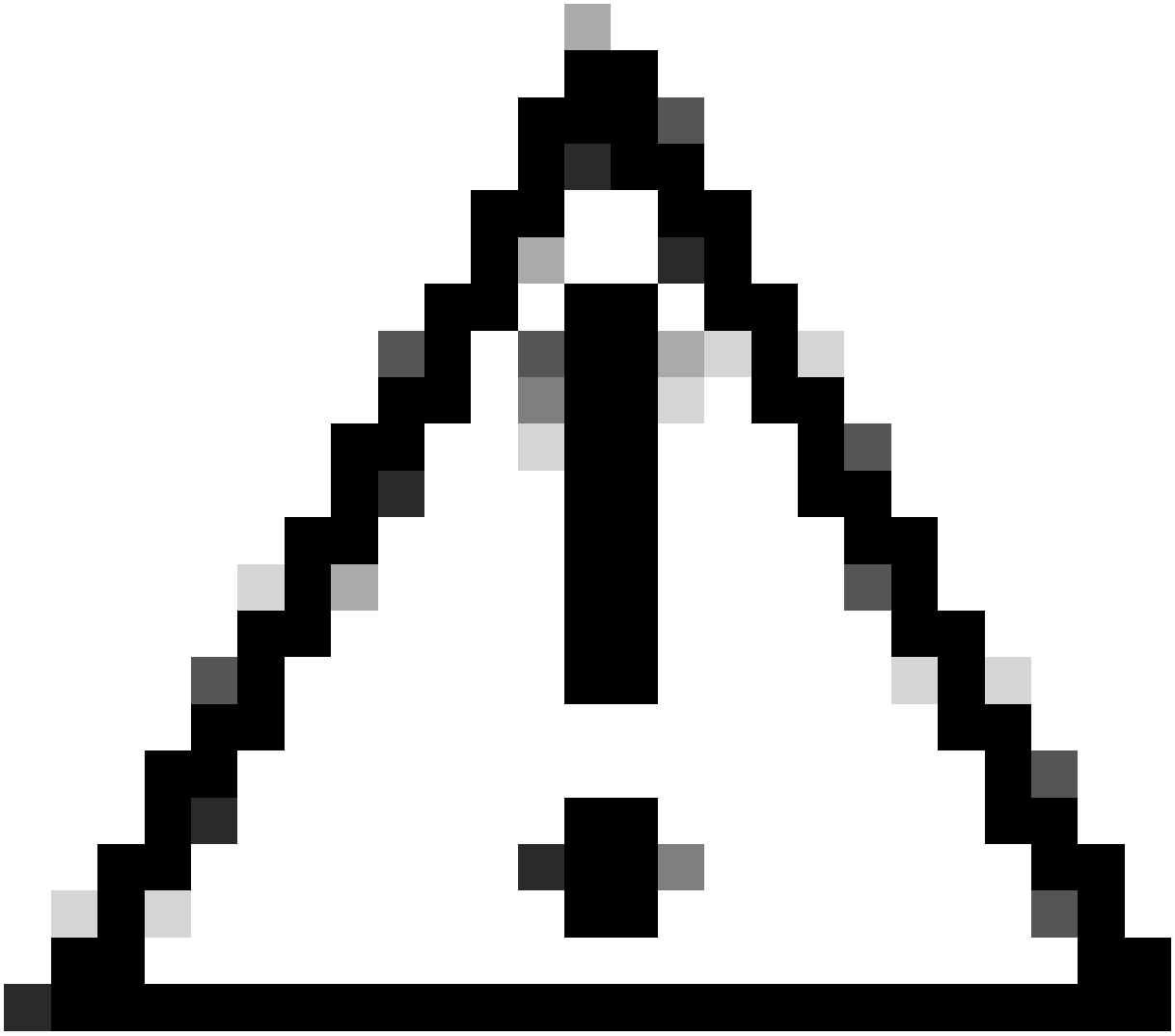
show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
certificate:
subject=CN = POD2IPN2, serialNumber = FDO2649OP4T
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



注意：通過具有本地憑據的控制檯執行這些配置更改。

步驟1. 設定全域tacacs tls。

<#root>

POD2IPN2(config)#

tacacs-server secure tls

步驟2.將ISE埠更改為ISE伺服器配置的TLS埠。

<#root>

POD2IPN2(config)#

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

步驟3.將交換機上配置的ISE伺服器與TLS連線的信任點相關聯。

<#root>

POD2IPN2(config)#

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

步驟4.建立tacacs伺服器組。

<#root>

POD2IPN2(config)#

aaa group server tacacs+ tacacs2

POD2IPN2(config-tacacs+)#

server 10.225.253.209

POD2IPN2(config-tacacs+)#

use-vrf management

步驟5.驗證設定。

<#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
```

步驟6.在配置AAA身份驗證之前測試遠端使用者。

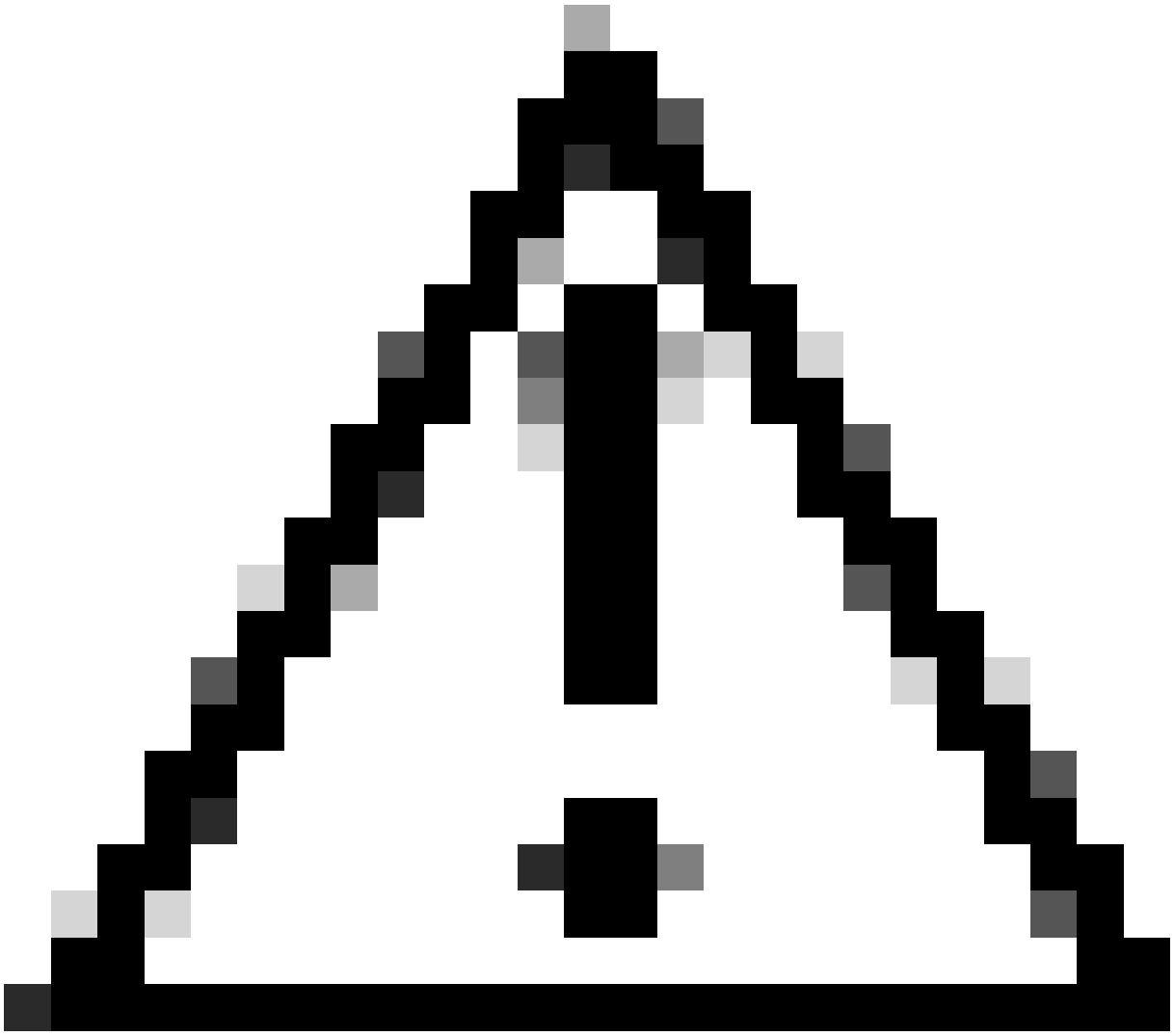
<#root>

POD2IPN2#

```
test aaa group tacacs2
```

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

AAA組態



注意：在繼續AAA配置之前，請確保遠端使用者身份驗證成功。

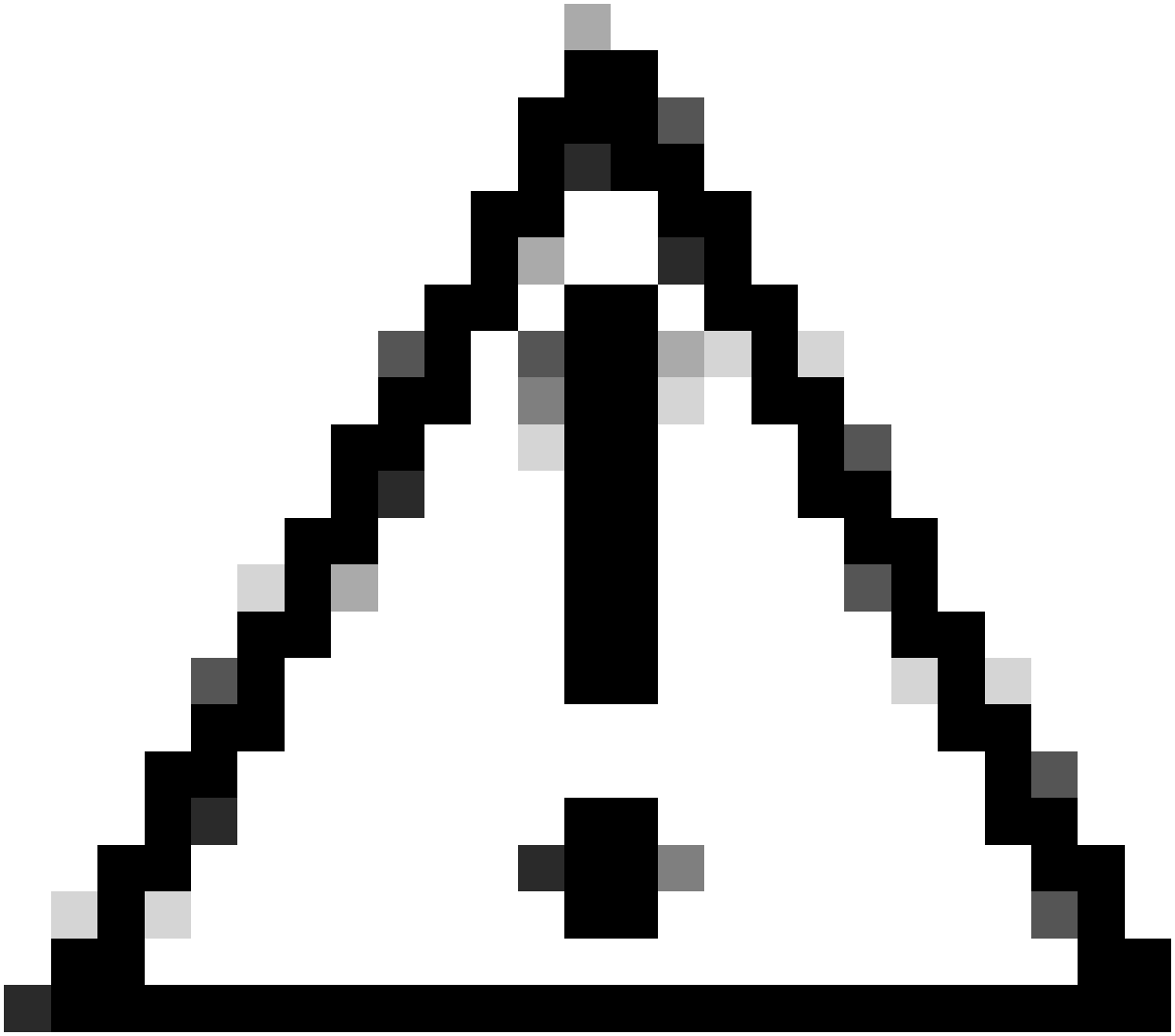
步驟1.配置AAA遠端身份驗證。

<#root>

POD2IPN2(config)#

aaa authentication login default group tacacs2

步驟2.測試命令後配置AAA遠端授權。



注意：確保您看到authorization-status為「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)
```

步驟3.配置AAA命令和config-command授權。

```
<#root>
POD2IPN2(config)#
aa authorization config-commands default group tacacs2 local

POD2IPN2(config)#
aaa authorization commands default group tacacs2 local
```

測試NX-OS使用者訪問並對其進行故障排除

驗證

Cisco NX-OS裝置管理配置已完成。您需要驗證設定。

步驟1.使用SSH作為各種角色登入到NX-OS裝置。

步驟2.在裝置命令列介面(CLI)上，驗證使用者是否有權訪問正確的命令。例如，幫助台使用者必須能夠ping通常規IP地址（例如10.225.253.129），但拒絕顯示運行配置。

```
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
```

疑難排解

NX-OS配置驗證。

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

要顯示使用者連線和角色，請使用以下命令。

```
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...
```

以下是疑難排解TACACS+的有用偵錯：

```
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
```

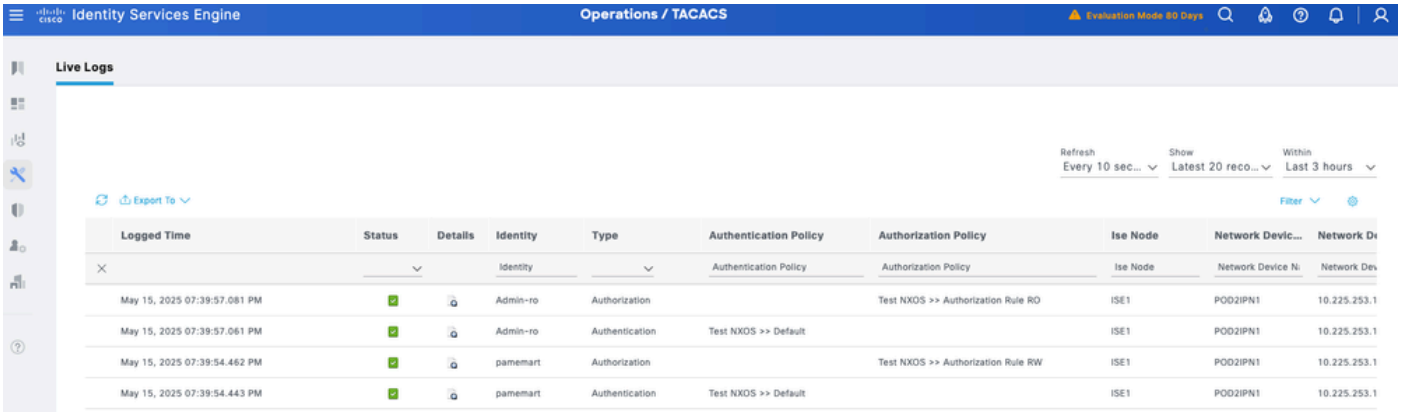
啟用SSL調試。

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

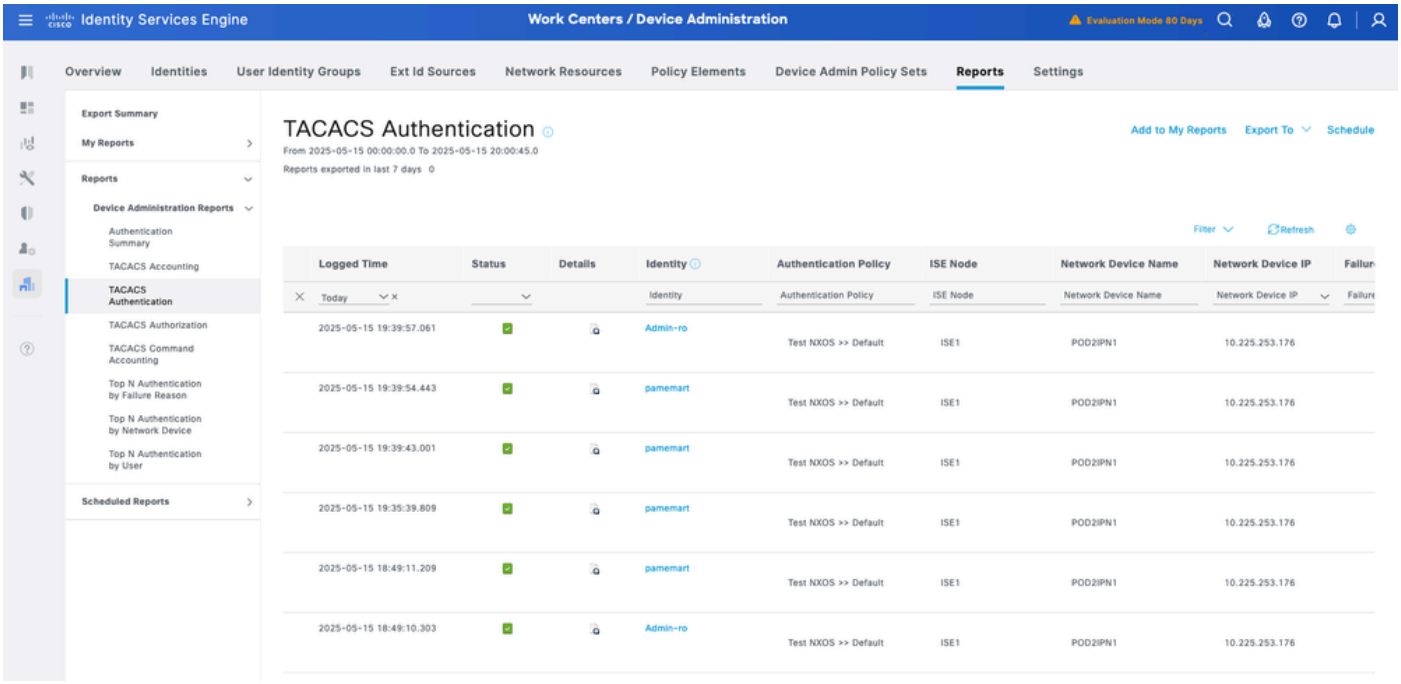
顯示調試檔案內容。

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

在ISE GUI中，導航到Operations > TACACS Livelog。此處捕獲所有TACACS身份驗證和授權請求，而details按鈕提供關於特定事務通過/失敗原因的詳細資訊。



對於歷史報表：導航到工作中心(Work Centers)>裝置管理(Device Administration)>報告(Reports)>裝置管理(Device Administration)，獲取身份驗證、授權和記帳報告。



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）。