使用ISE在Palo Alto上配置TACACS+裝置管理

目錄

簡介

本文檔介紹使用Cisco ISE的Palo Alto上的TACACS+配置。

必要條件

思科建議您瞭解以下主題：

- Cisco ISE和TACACS+通訊協定。
- 帕洛阿爾托防火牆。

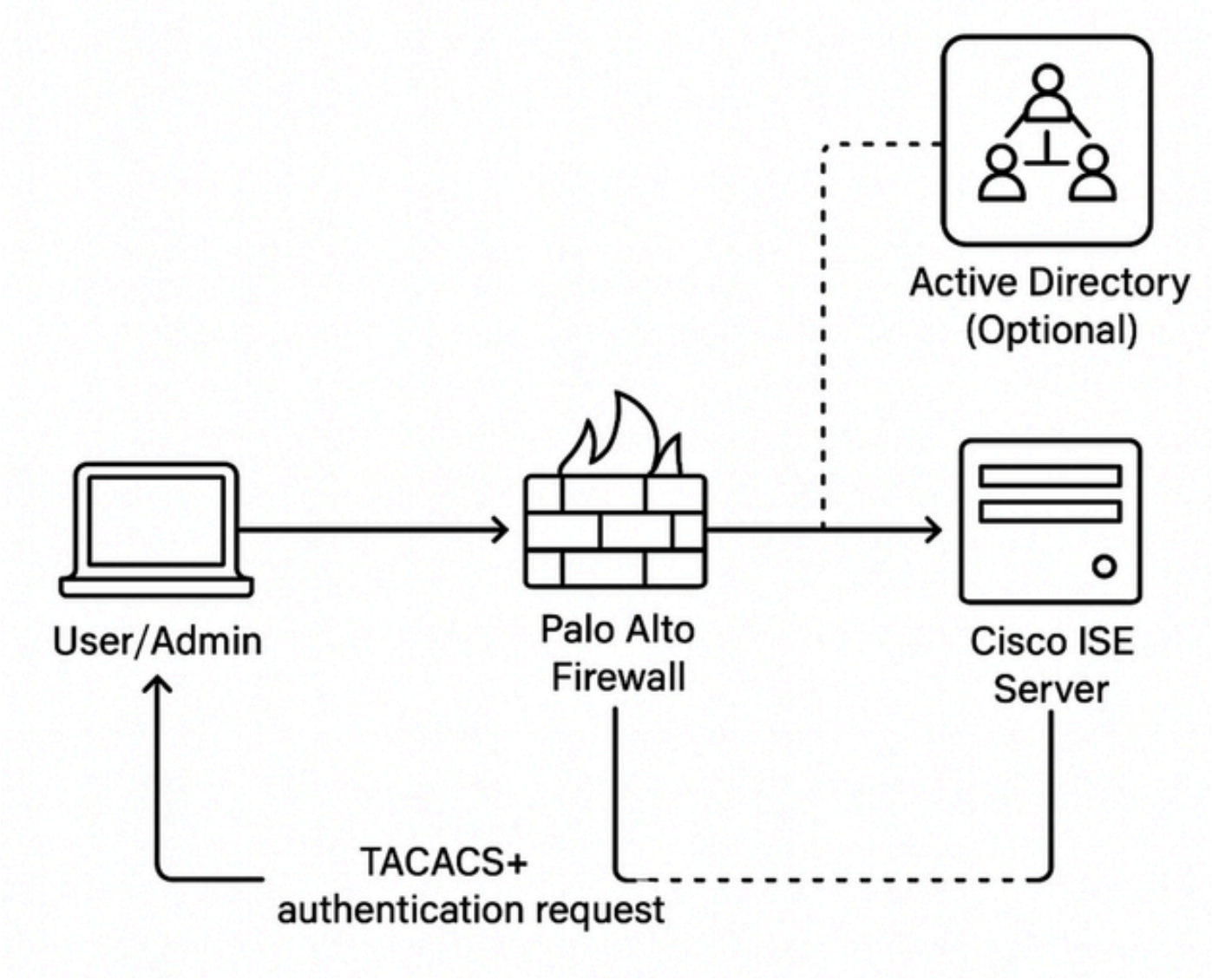
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Palo Alto防火牆版本10.1.0
- 思科身分識別服務引擎(ISE)版本3.3補丁4

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。

網路圖表



身份驗證流程

1.管理員登入到Palo Alto防火牆。

2. Palo Alto向Cisco ISE傳送TACACS+身份驗證請求。

3.思科ISE:

- 如果AD是整合的，它將查詢AD以進行身份驗證和授權。
- 如果沒有AD，則使用本地身份儲存區或策略。
- 思科ISE根據配置的策略向Palo Alto傳送授權響應。
- 管理員獲得具有適當許可權級別的訪問許可權。

設定

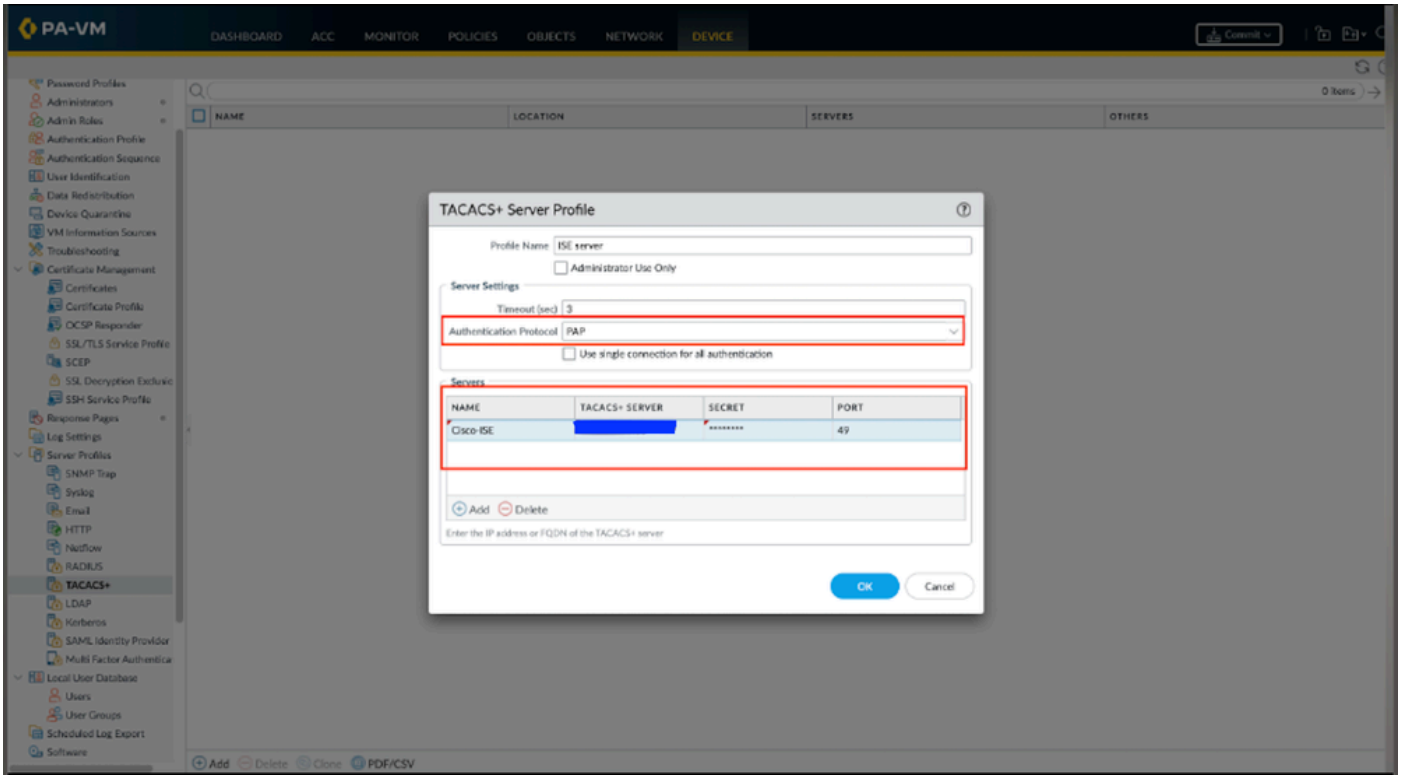
第1部分：為TACACS+配置Palo Alto防火牆

步驟1.新增TACACS+伺服器配置檔案。

該配置檔案定義了防火牆如何連線到TACACS+伺服器。

1. 選擇Device > Server Profiles > TACACS+或Panorama > Server Profiles > TACACS+ on Panorama和Add a profile。
2. 輸入配置檔名稱以標識伺服器配置檔案。
3. （可選）選擇Administrator Use Only以限制對管理員的訪問。
4. 輸入身份驗證請求超時前的超時時間間隔（以秒為單位）(預設值為3;範圍為1-20)。
5. 選擇防火牆用於向TACACS+伺服器進行身份驗證的身份驗證協定（預設為CHAP）。
6. 新增每個TACACS+伺服器並執行以下步驟：
    1. 用於標識伺服器的名稱。
    2. TACACS+伺服器IP地址或FQDN。如果使用FQDN地址對象標識伺服器，並且隨後更改了該地址，則必須提交更改，以使新伺服器地址生效。
    3. 用於加密使用者名稱和密碼的加密和確認金鑰。
    4. 用於身份驗證請求的伺服器埠（預設值為49）。 按一下確定儲存伺服器配置檔案。

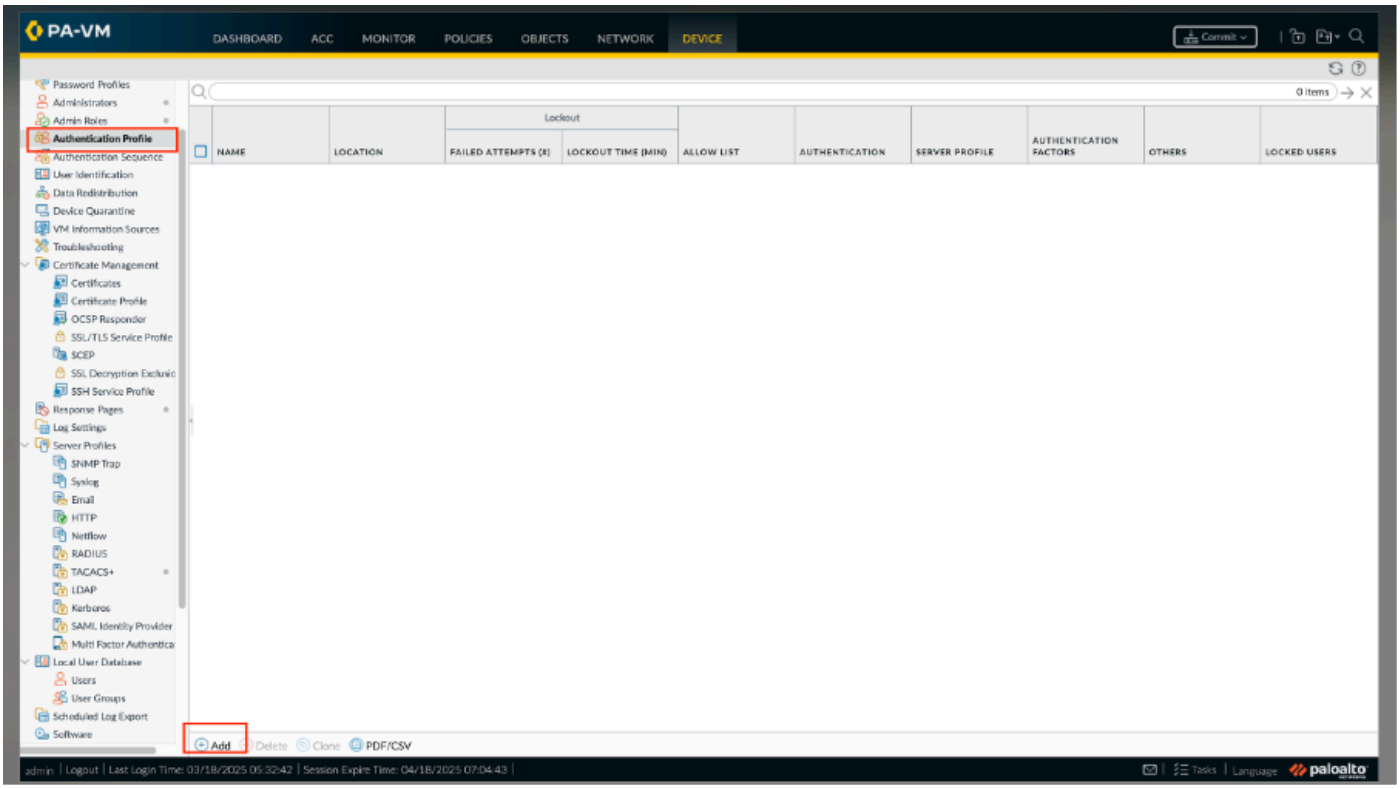
7.按一下「確定」儲存伺服器配置檔案。

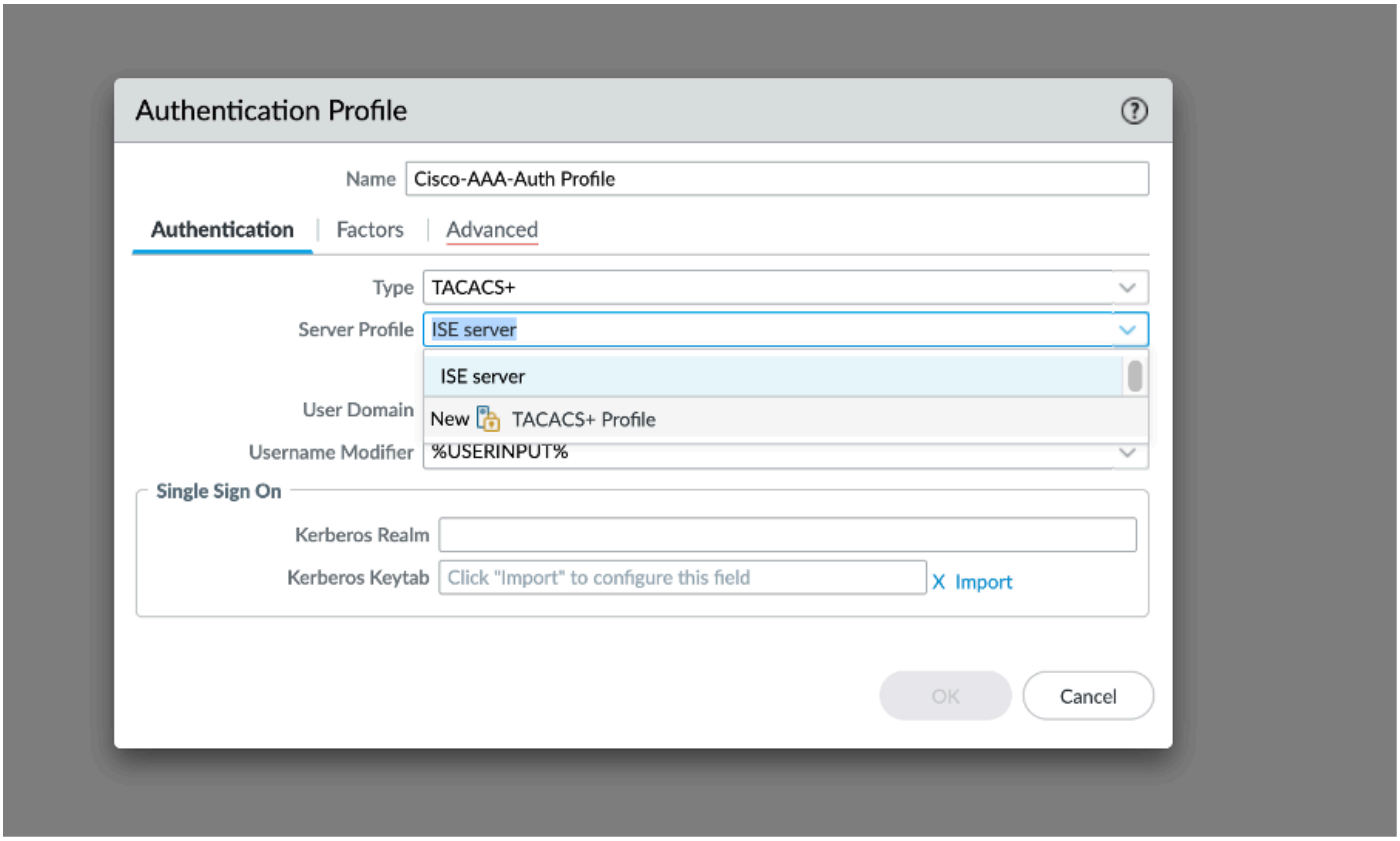


步驟2.將TACACS+伺服器配置檔案分配到身份驗證配置檔案。

身份驗證配置檔案定義一組使用者通用的身份驗證設定。

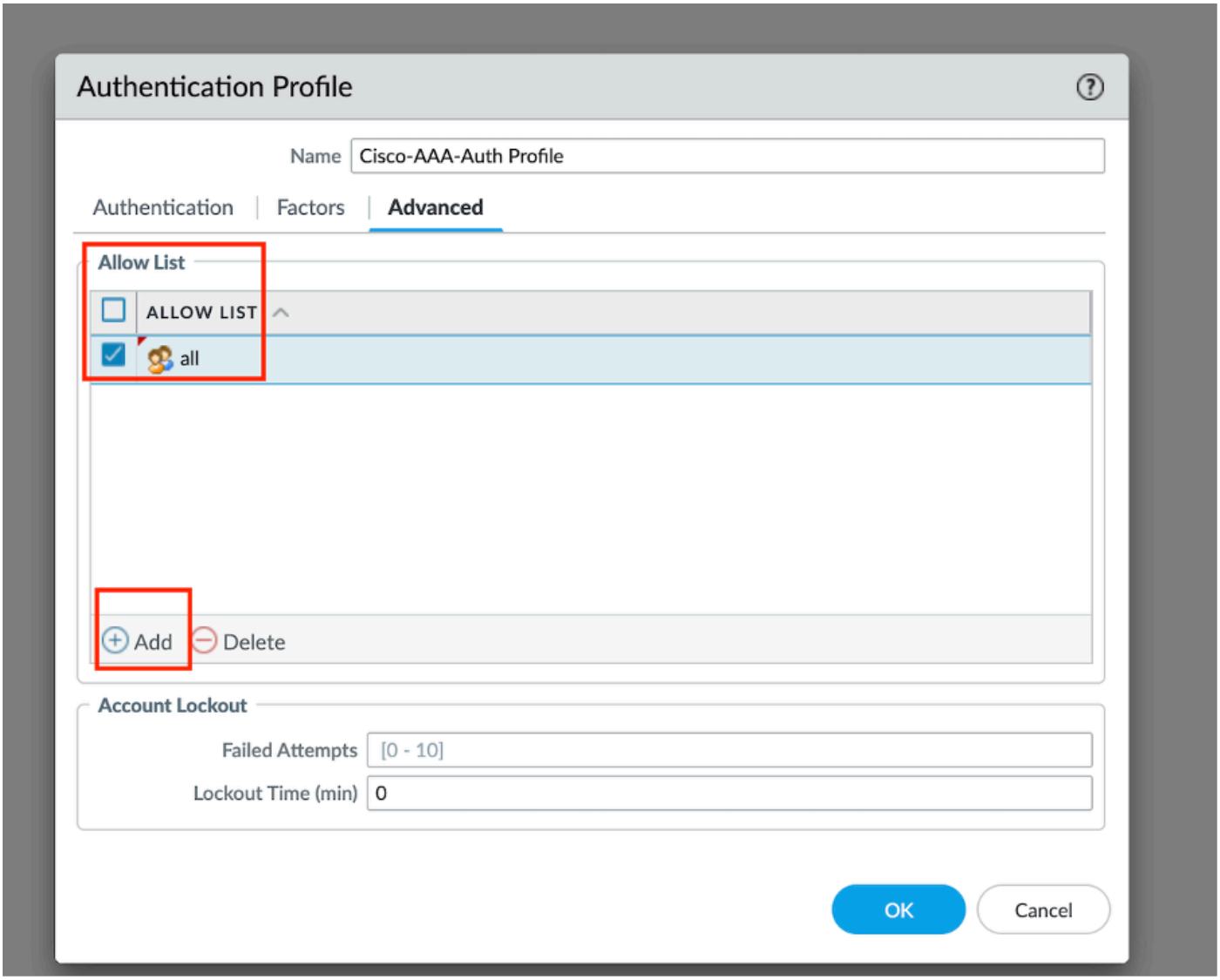
1. 選擇Device > Authentication Profile 和Add配置檔案。
    1. 輸入用於標識配置檔案的名稱
    2. 將「Type（型別）」設定為TACACS+。
    3. 選擇已配置的伺服器配置檔案。
    4. 選擇Retrieve user group from TACACS+以從TACACS+伺服器上定義的VSA收集使用者組資訊。





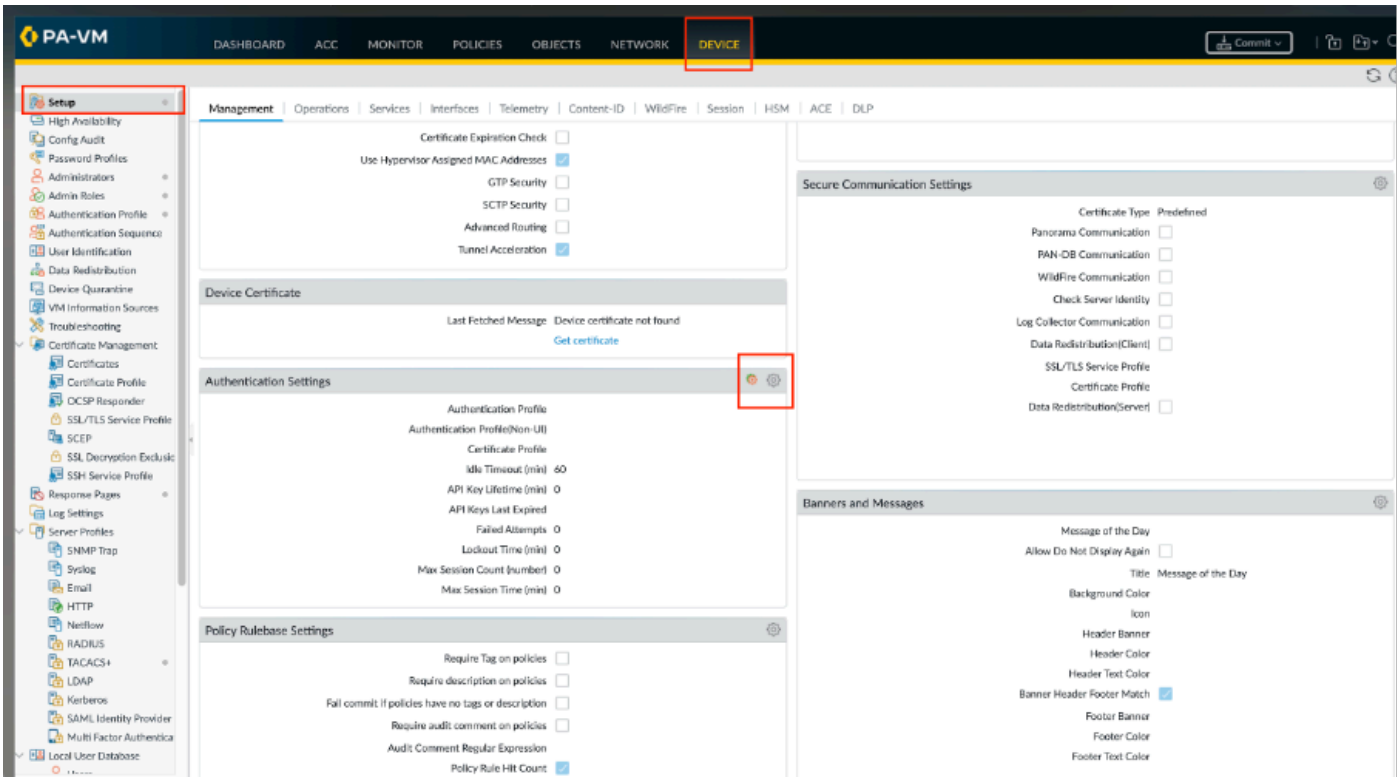
防火牆使用您在身份驗證配置檔案的允許清單中指定的組來匹配組資訊。

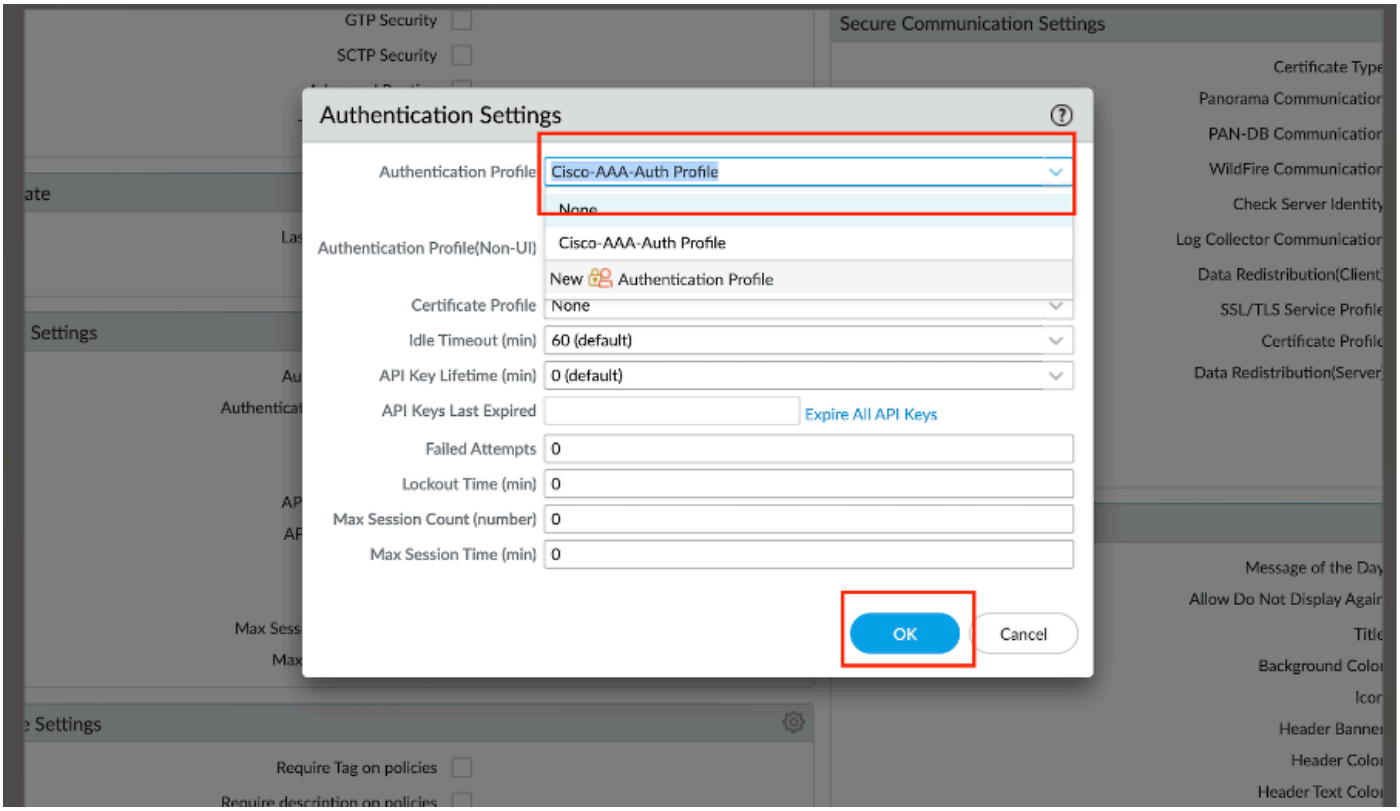
1. 選擇Advanced，然後在Allow List中選擇Add，以新增可使用此身份驗證配置檔案進行身份驗證的使用者和組。
2. 按一下「OK」以儲存驗證設定檔。



步驟3.將防火牆配置為對所有管理員使用身份驗證配置檔案。

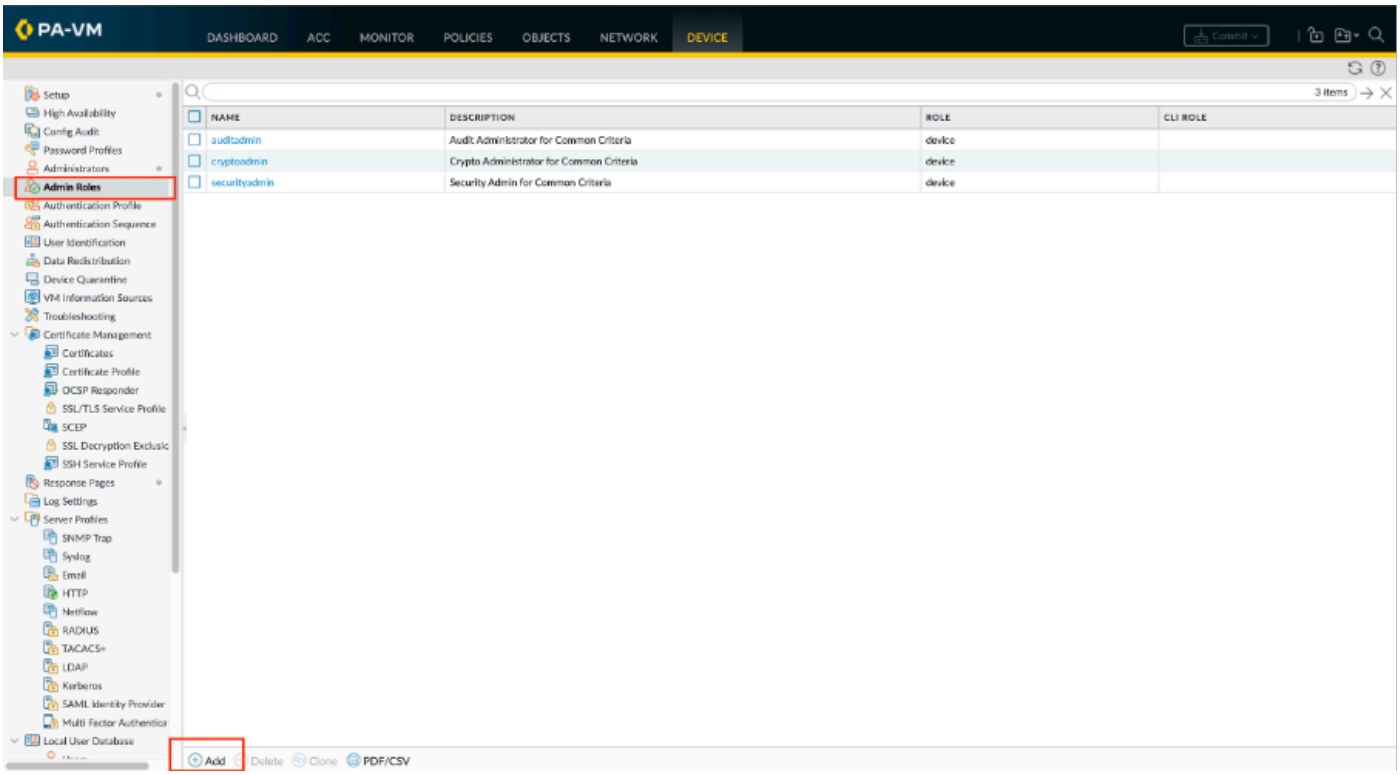
1. 選擇Device > Setup > Management，然後編輯Authentication Settings。
2. 選擇您配置的身份驗證配置檔案，然後單擊OK。



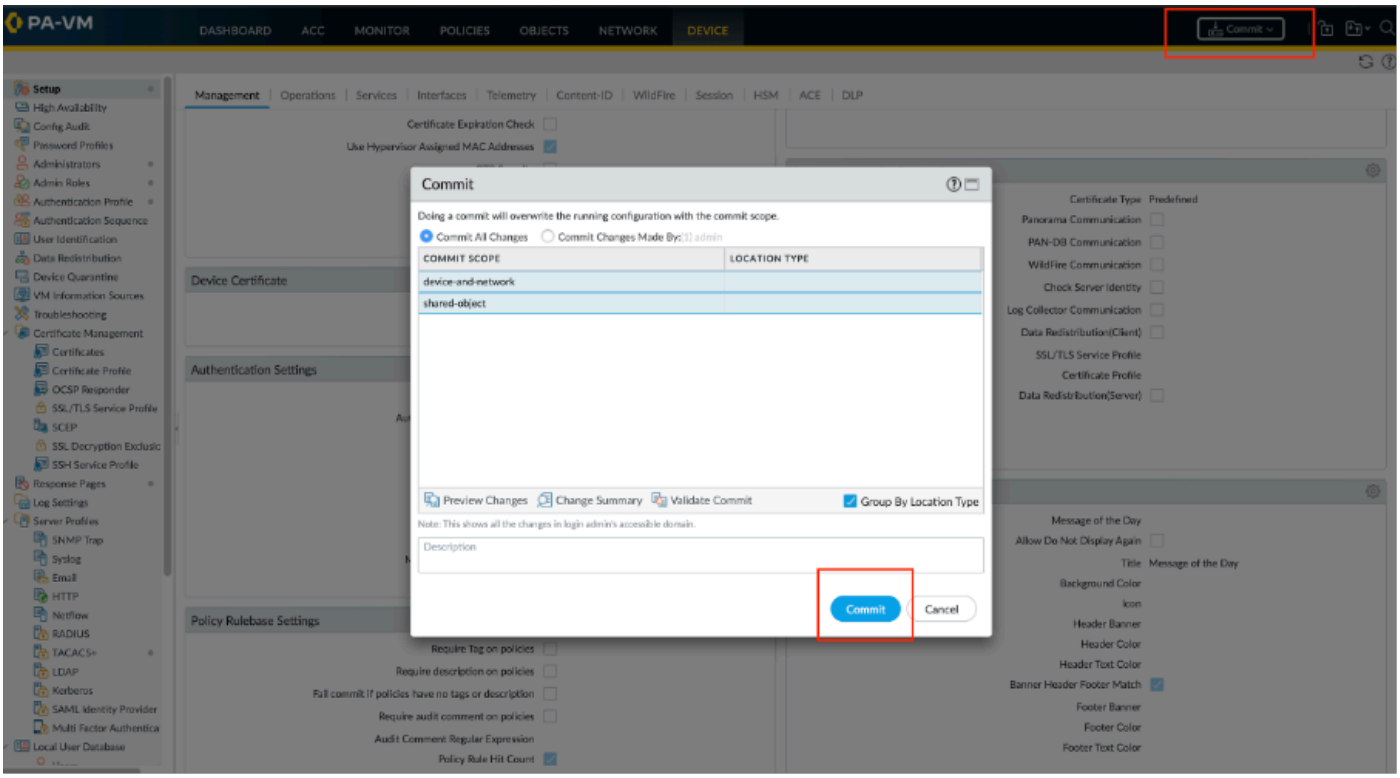


步驟4.配置管理員角色配置檔案。

選擇Device > Admin Roles，然後按一下Add。輸入名稱以標識角色。

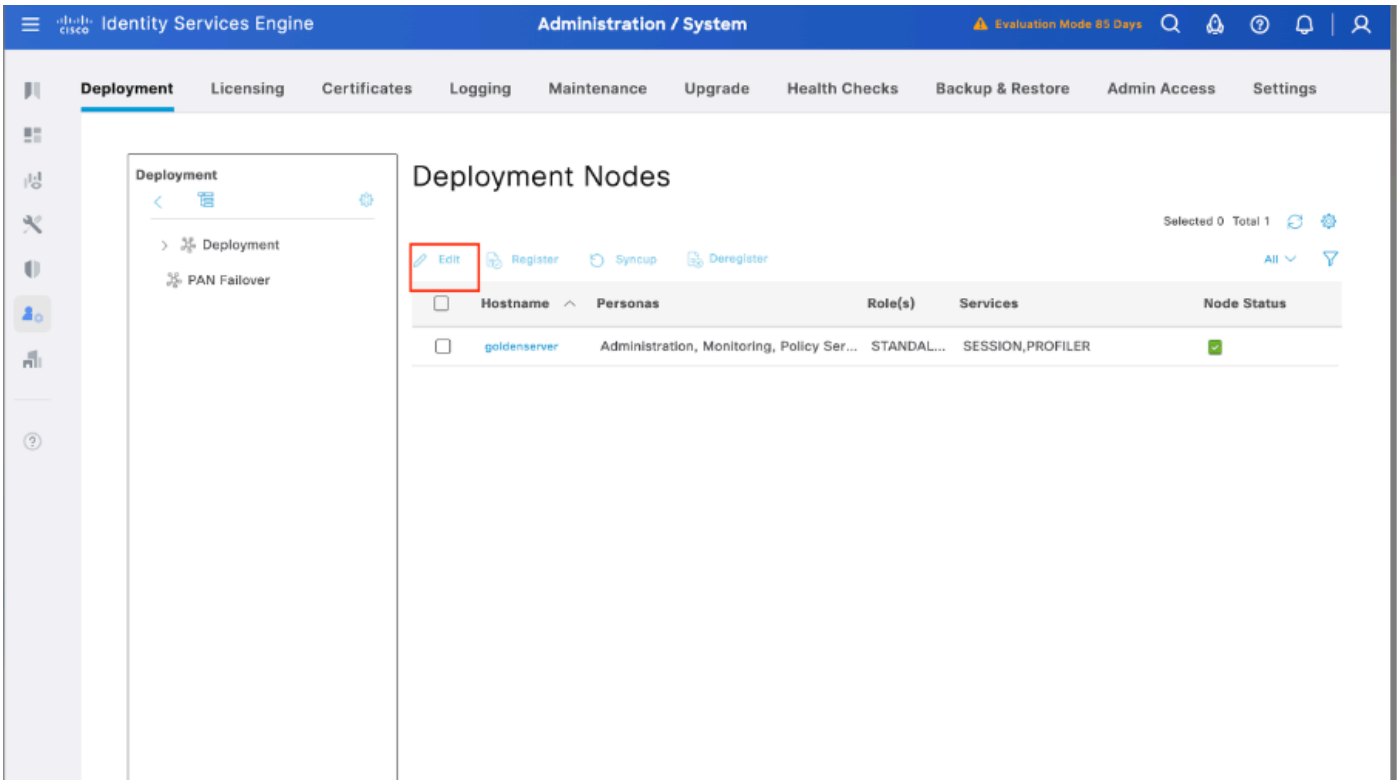


步驟5.提交更改以在防火牆上啟用這些更改。

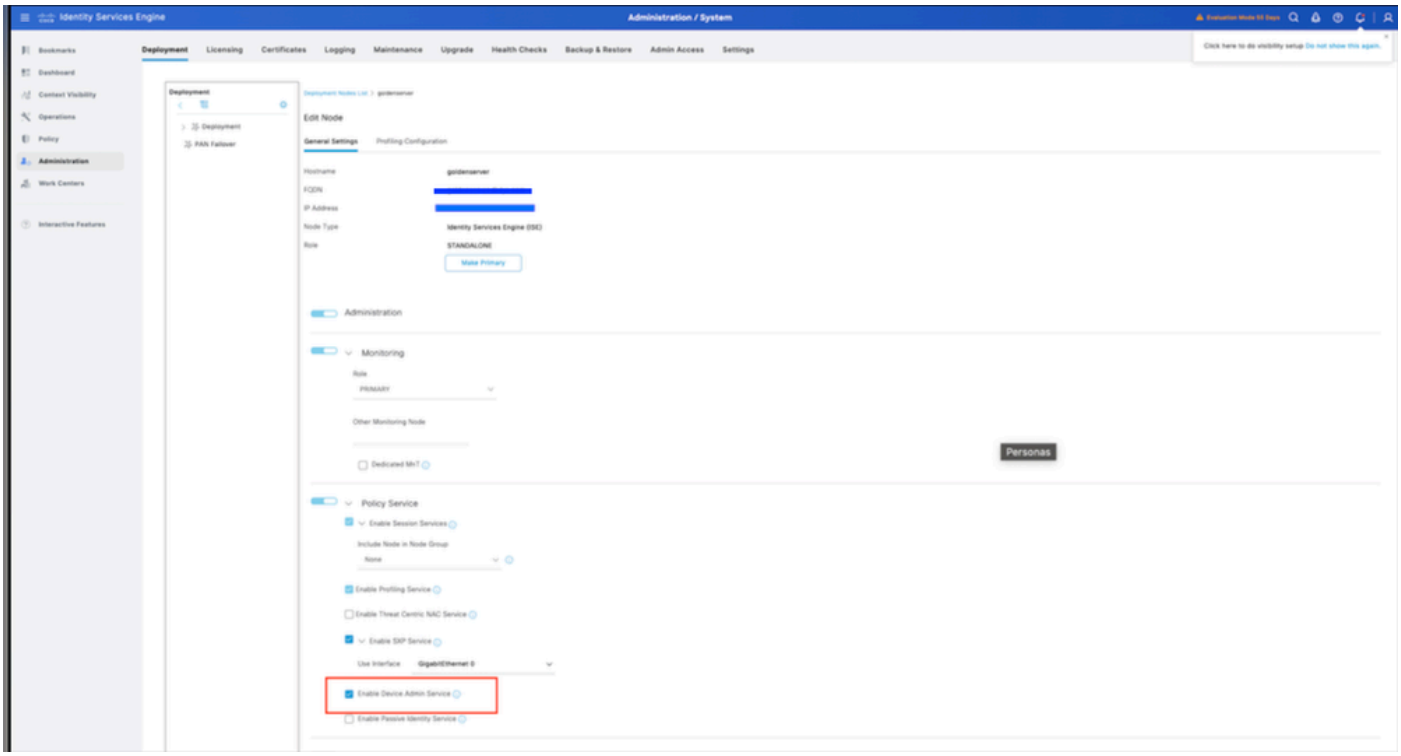


第2部分：ISE上的TACACS+配置

步驟1。初始步驟是驗證思科ISE是否具備處理TACACS+身份驗證的必要能力。為此，請確認所需的策略服務節點(PSN)已啟用裝置管理服務功能。導航到Administration > System > Deployment，選擇ISE處理TACACS+身份驗證的相應節點，然後點選Edit檢視其配置。

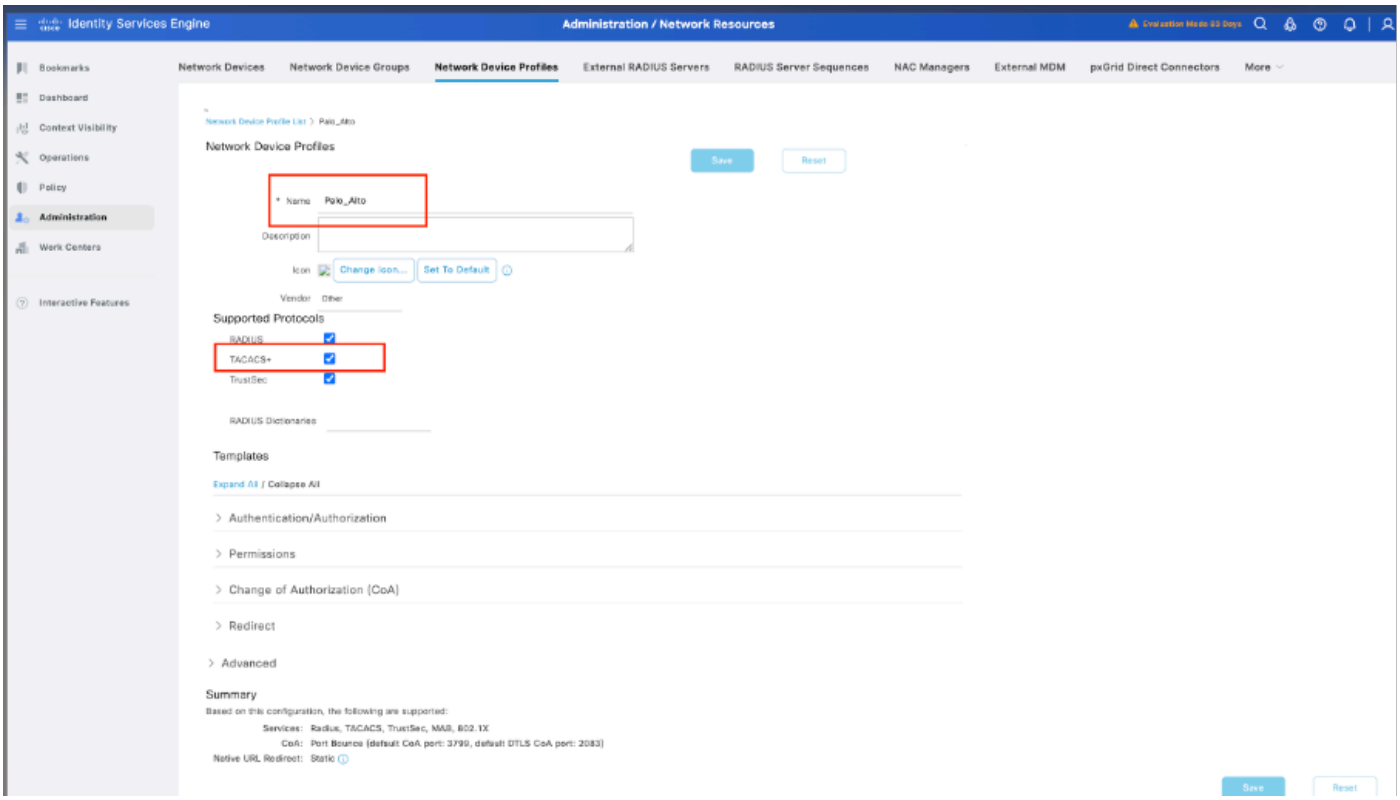


步驟2.向下滾動以找到Device Administration Service功能。請注意，啟用此功能需要策略服務角色在節點上處於活動狀態，同時還需要部署中的可用TACACS+許可證。選中該覈取方塊以啟用該功能，然後儲存配置。



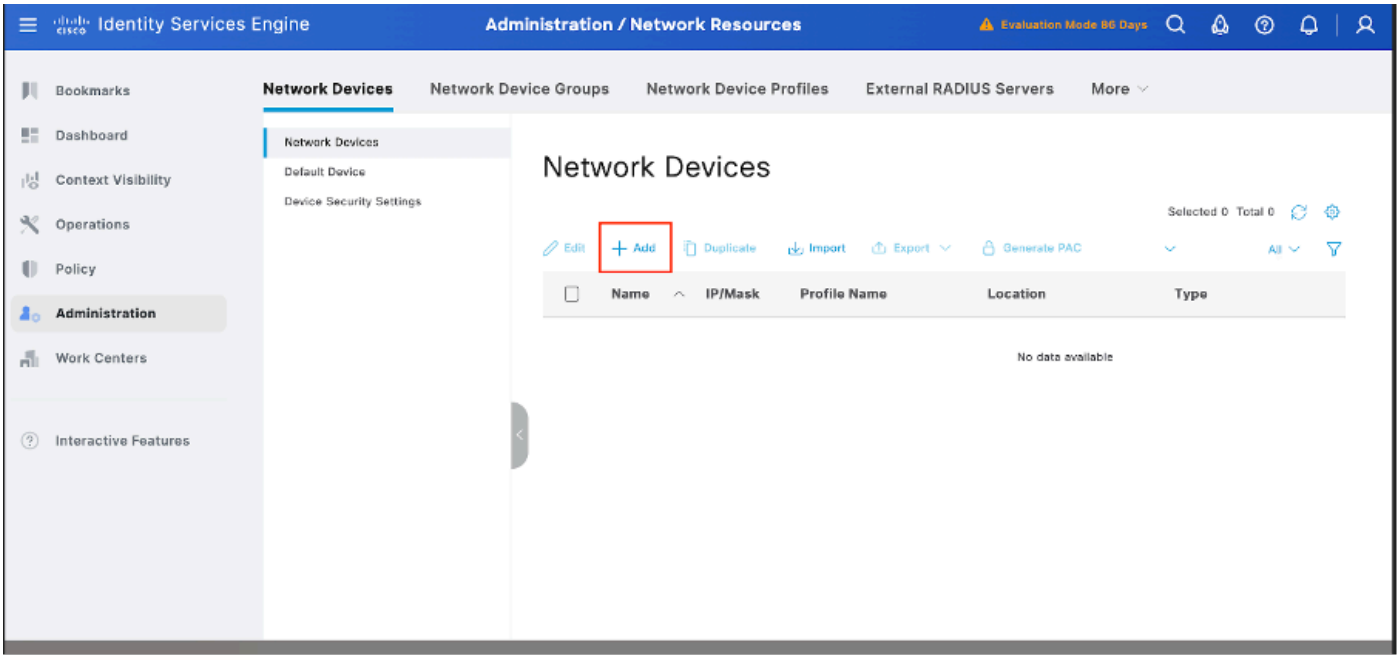
步驟3.為Cisco ISE配置Palo Alto網路裝置配置檔案。

導覽至Administration > Network Resources > Network device profile。按一下Add並提及名稱(Palo Alto)並在受支援的協定下啟用TACACS+。



步驟4.新增Palo Alto作為網路裝置。

1. 導覽至Administration > Network Resources > Network Devices > +Add。



2.按一下Add並輸入以下詳細資訊：

名稱:帕洛阿爾托

IP 位址:<Palo-Alto IP>

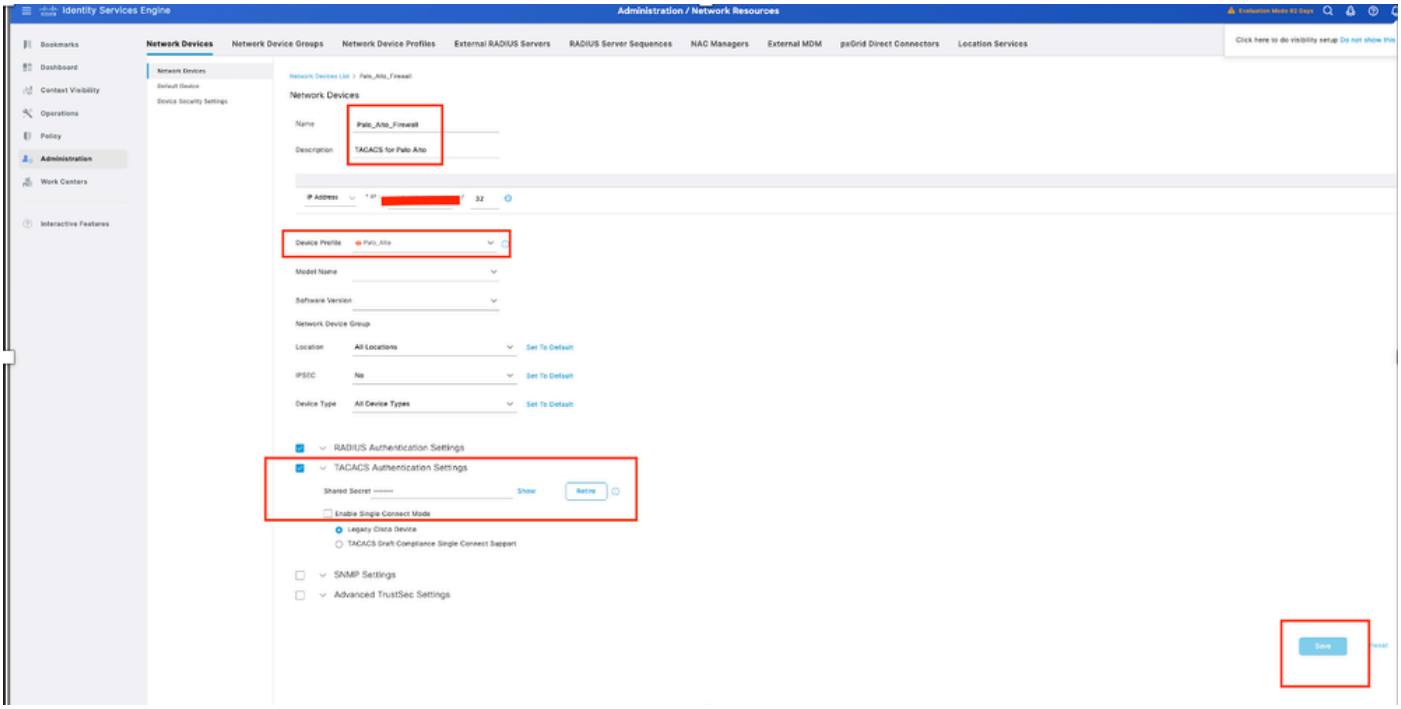
網路裝置配置檔案：選擇Palo Alto

TACACS身份驗證設定：

啟用TACACS+身份驗證

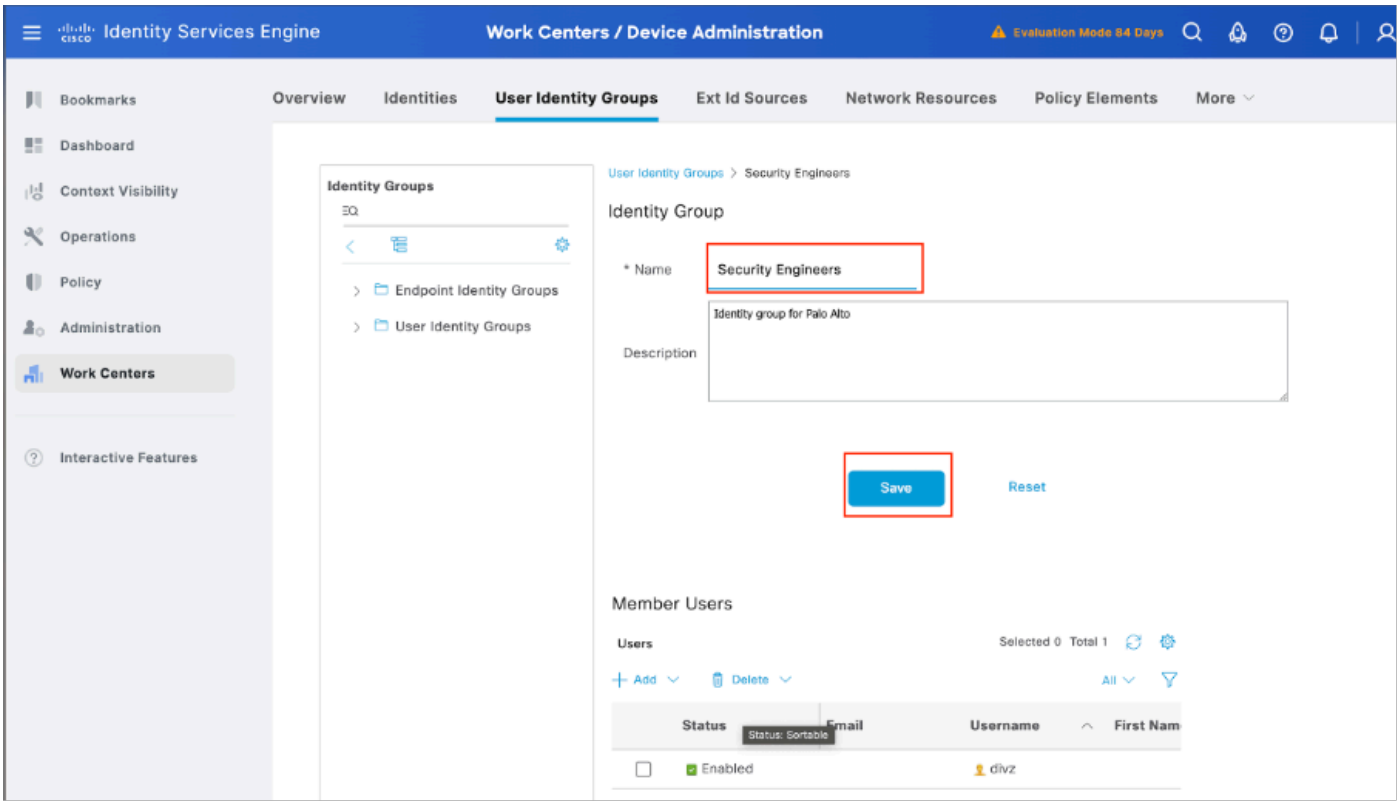
輸入共用金鑰（必須與Palo Alto配置匹配）

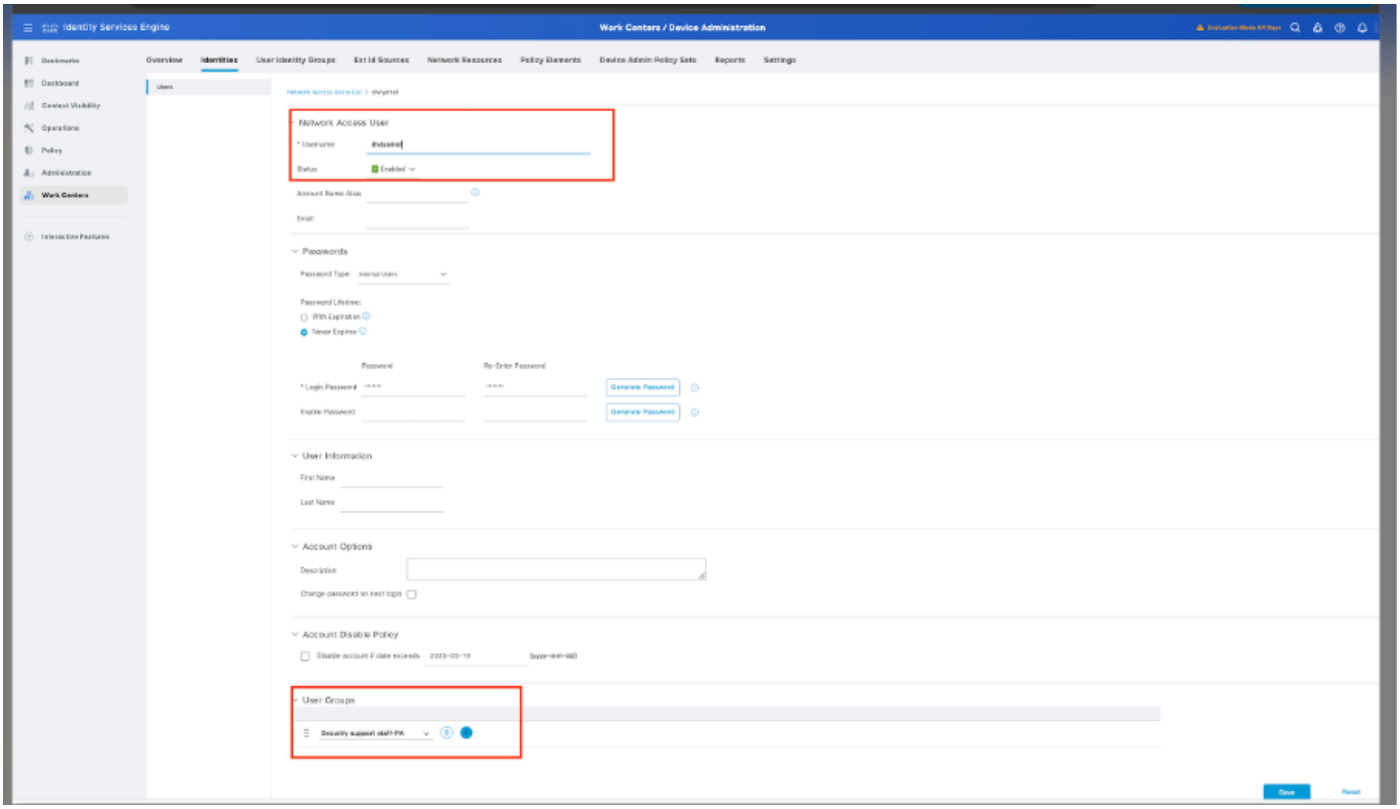
按一下「Save」。

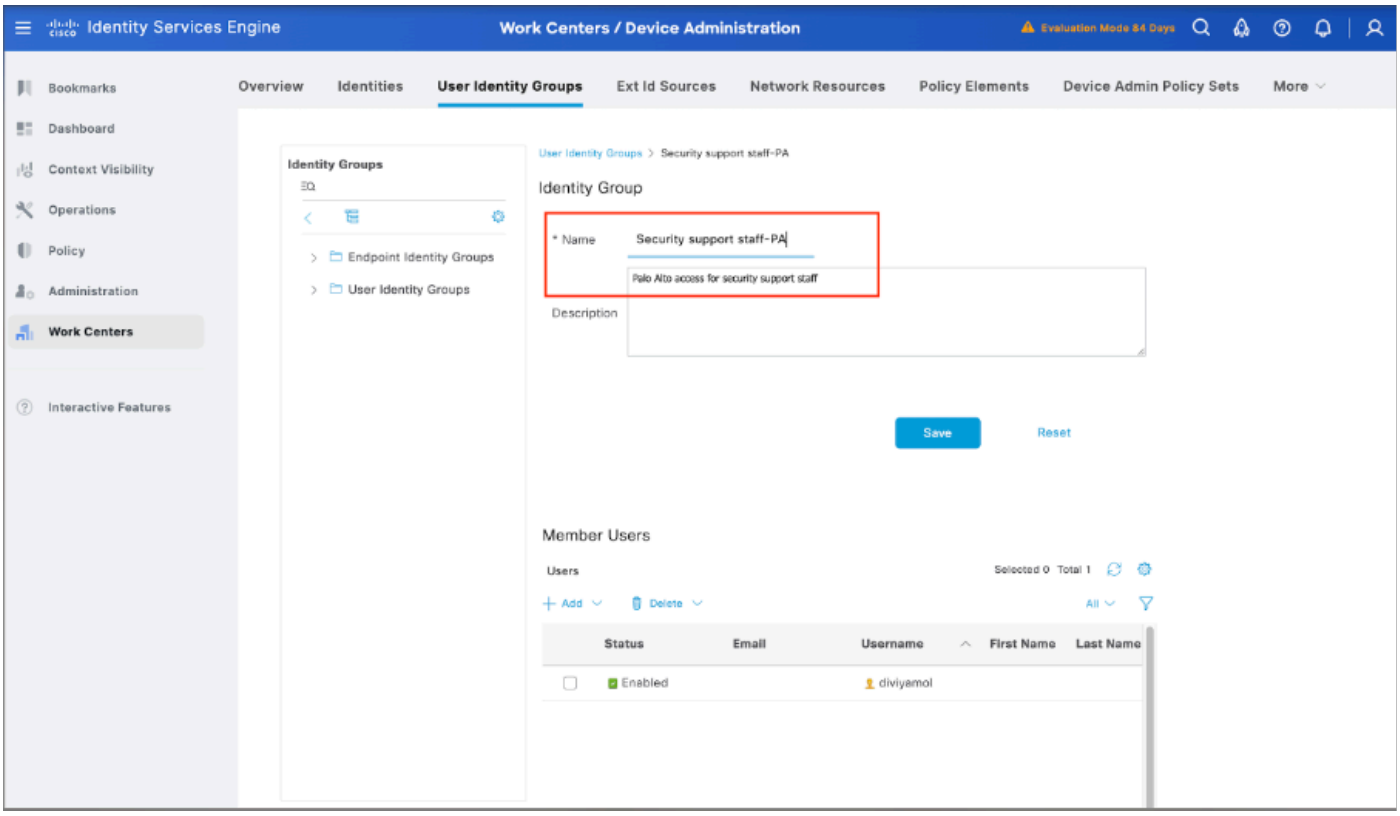


步驟5.建立使用者身份組。

導航到工作中心(Work Centers)>裝置管理(Device Administration)>使用者身份組(User Identity Groups)，然後點選新增(Add)並指定使用者組的名稱。


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 84 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
More
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Security Engineers
Identity Group
* Name
Security Engineers
Description
Identity group for Palo Alto
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Nam
Status: Sortable
Enabled
divz

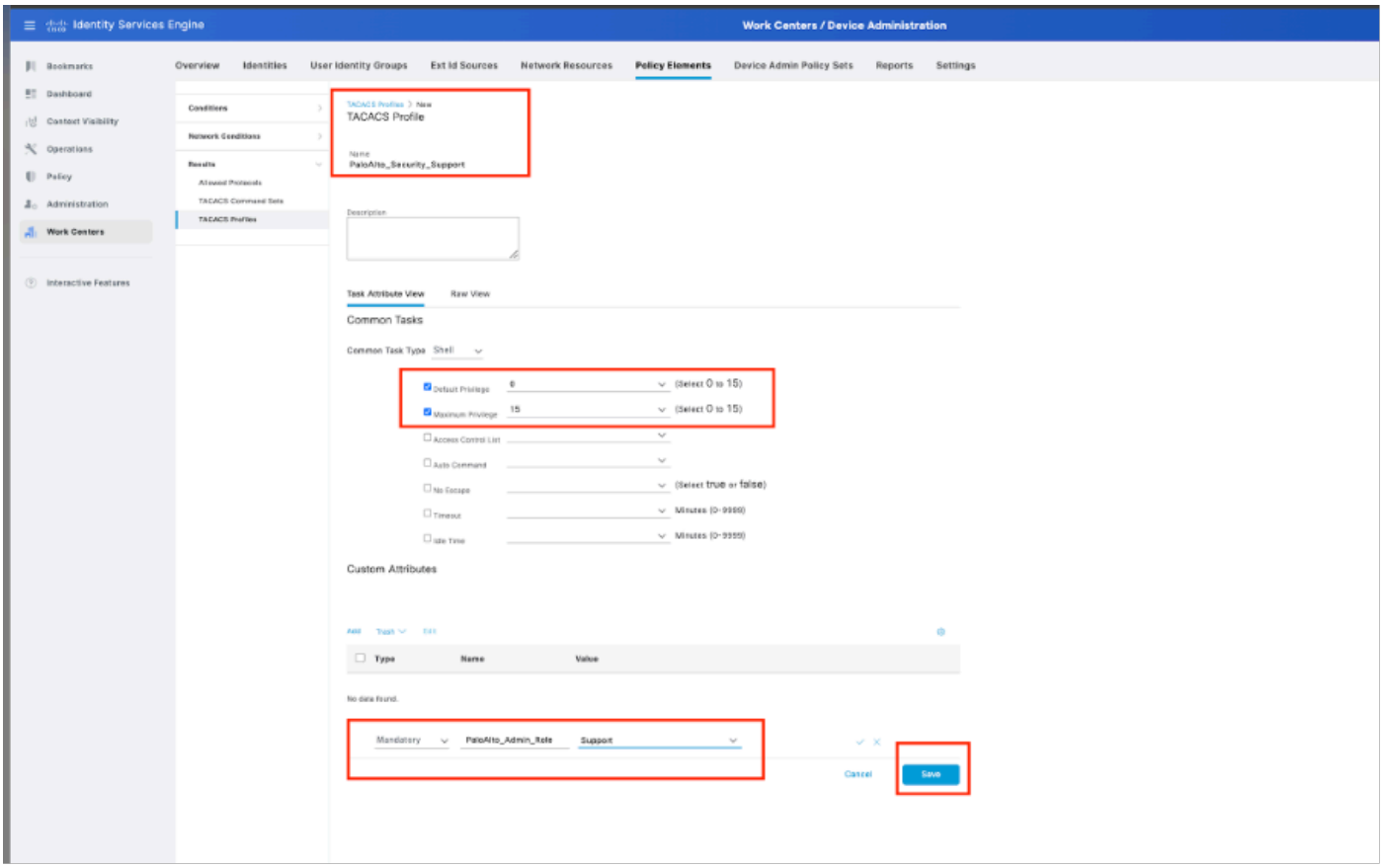

Identity Services Engine
Work Centers / Device Administration
Network Access User
Passwords
User Information
Account Options
Account Disable Policy
User Groups

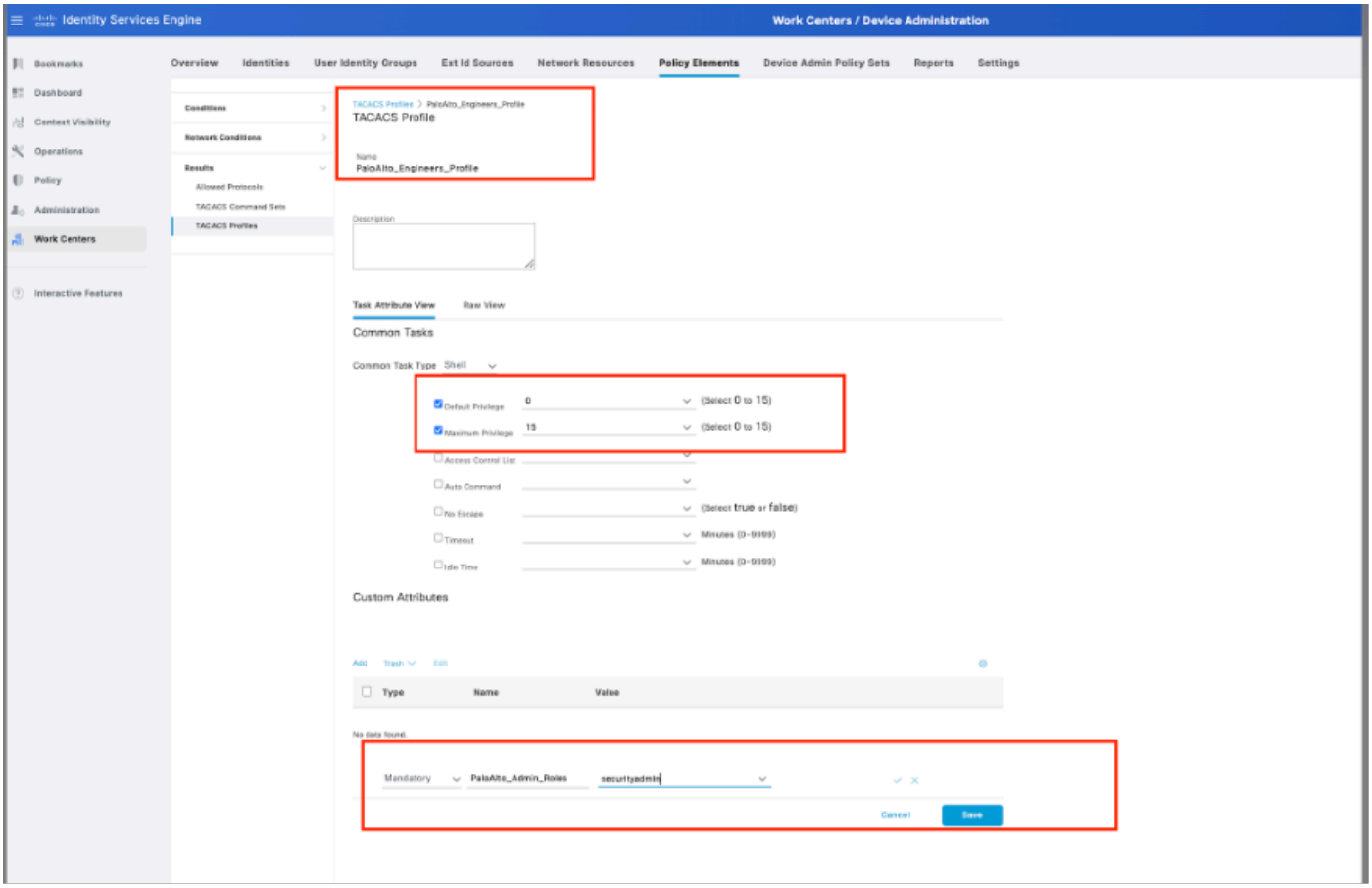


步驟6.配置TACACS配置檔案。

下一步是配置TACACS配置檔案，您可以在此配置許可權級別和超時設定等設定。導航至工作中心(Work Centers)>裝置管理(Device Administration)->策略元素(Policy Elements)->結果(Results)->TACACS配置檔案(TACACS Profiles)。

按一下Add以建立新的TACACS配置檔案。為配置檔案取個好名字。





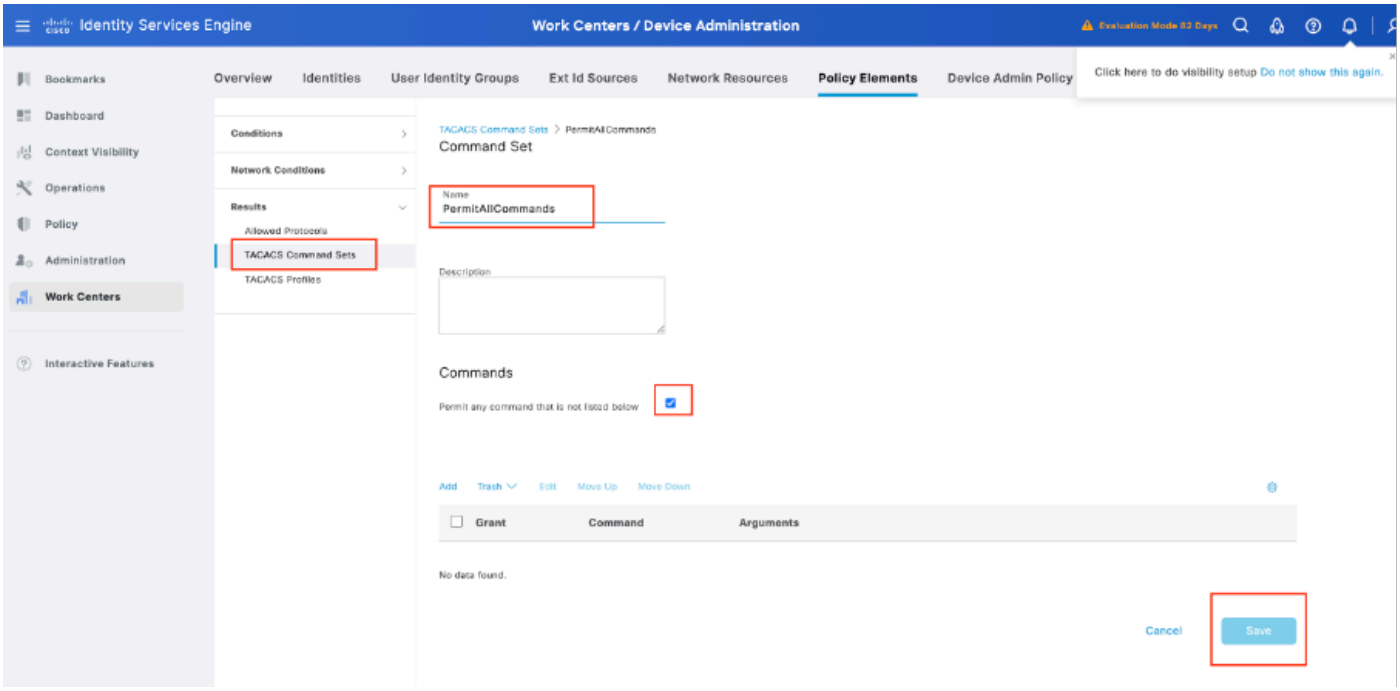
步驟6.配置TACACS命令集。

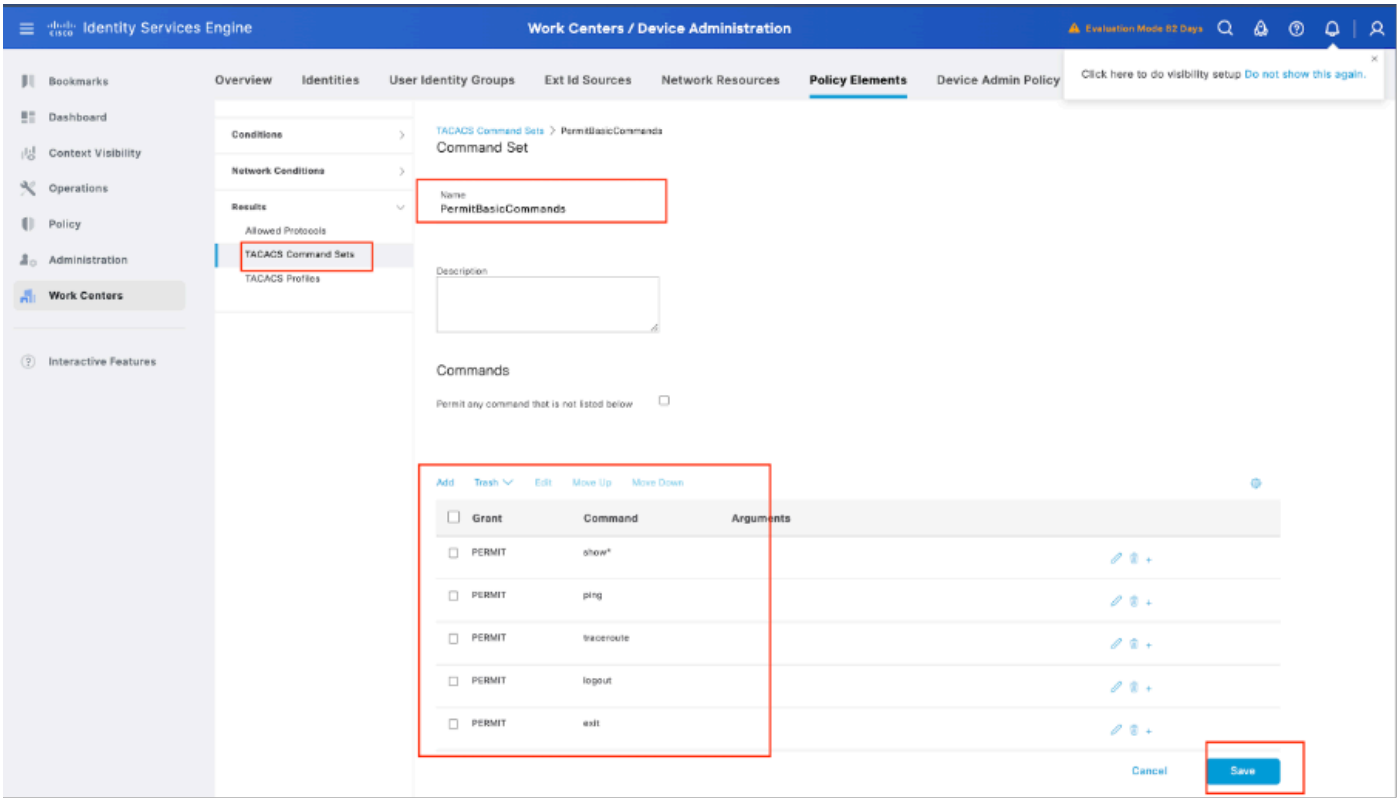
現在，應該配置允許使用者使用的命令。由於您可以授予這兩個使用案例的15級許可權（授予訪問

每個可用命令的許可權），因此使用TACACS命令集來限制可以使用哪些命令。

導覽至Work Centers > Device Administration > Policy Elements > Results -> TACACS Command Sets。按一下Add建立新的TACACS命令集並將其命名為PermitAllCommands。將此TACACS命令集應用於安全支援。

在此TACACS命令集中唯一需要配置的是選中Permit any command that not listed below覈取方塊。

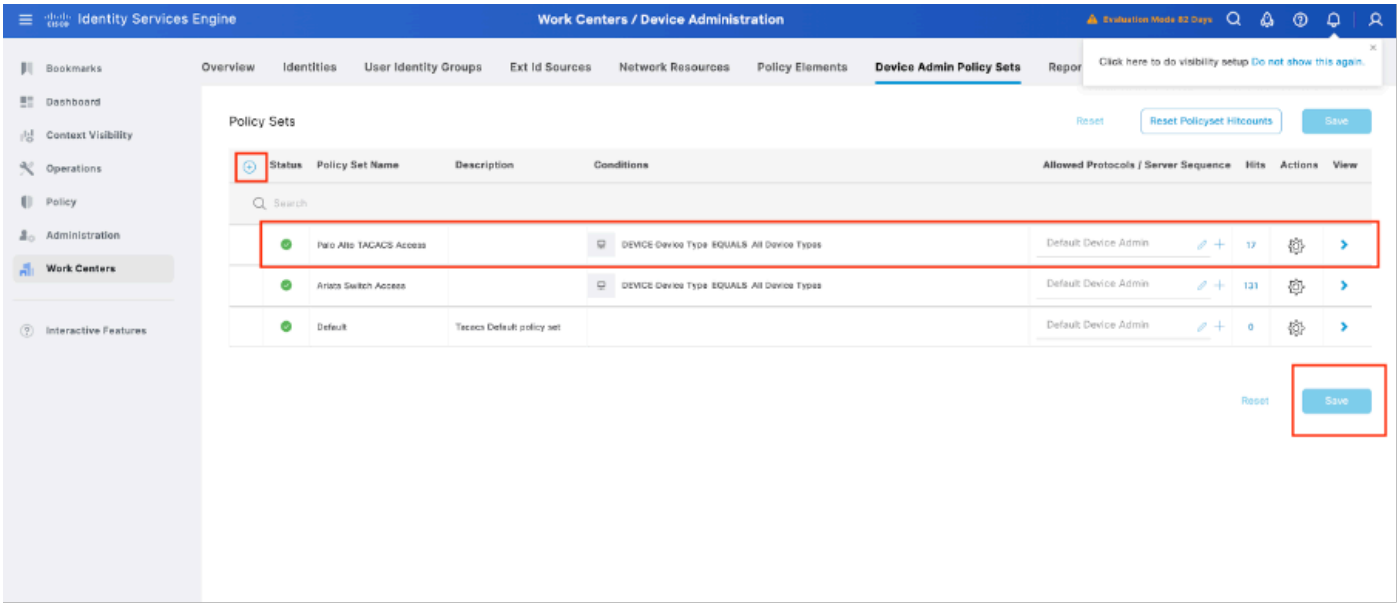




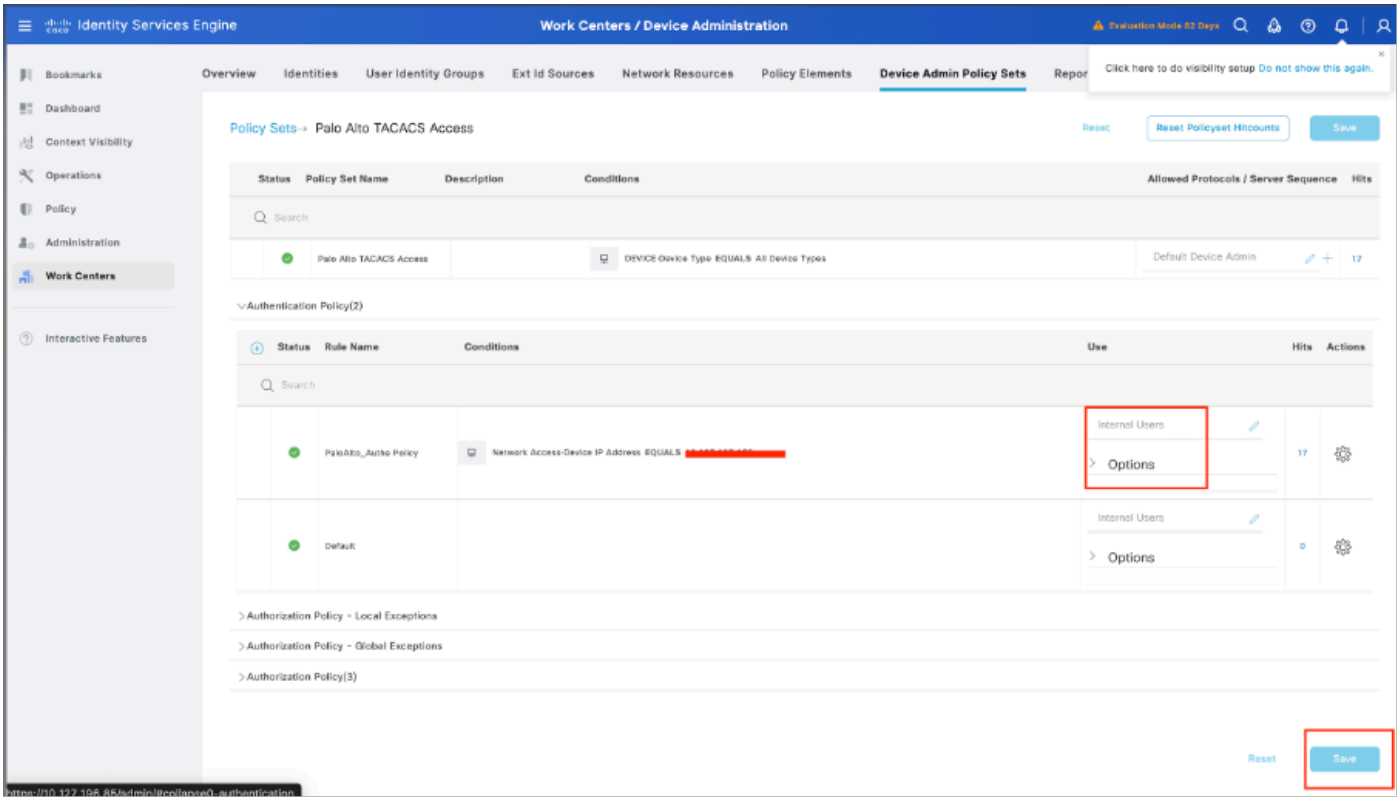
步驟7.建立用於Palo Alto的裝置管理策略集，導航選單Work Centers > Device Administration >

Device Admin Policy Sets，點選Add +圖示。

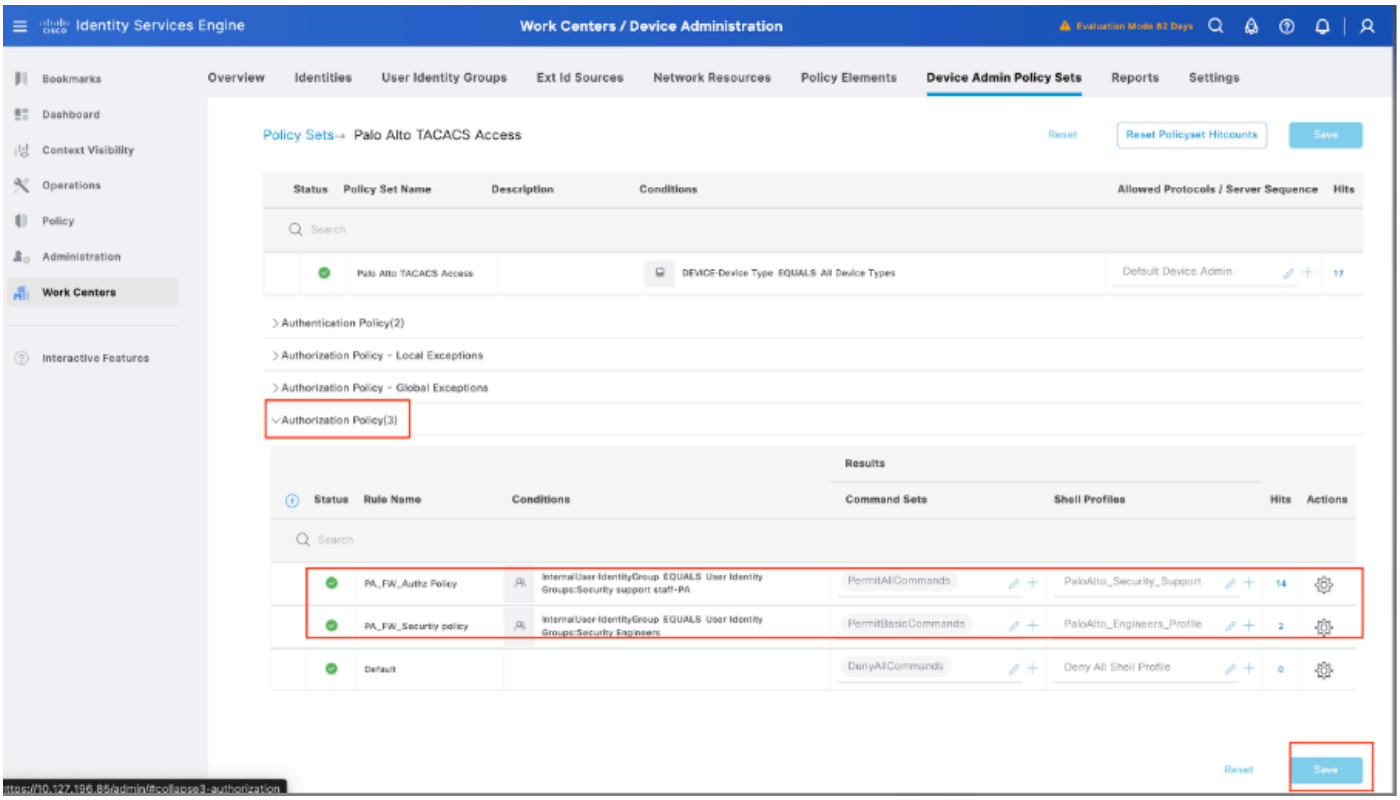
步驟8.命名此新策略集，根據Palo Alto防火牆進行中的TACACS+身份驗證的特徵新增條件，然後選擇Allowed Protocols > Default Device Admin。儲存您的配置。



步驟9.在 > view選項中選擇，然後在Authentication Policy部分，選擇Cisco ISE用於在Palo Alto防火牆上查詢身份驗證的使用者名稱和憑據的外部身份源。在此示例中，憑證對應於ISE中儲存的內部使用者。



步驟10.向下滾動直到名為Authorization Policy的部分直到Default策略，選擇齒輪圖示，然後在上面插入一個規則。



步驟11.命名新的授權規則，新增與已經驗證為組成員資格的使用者有關的條件，並在Shell Profiles部分新增您先前配置的TACACS配置檔案，儲存配置。

驗證

ISE稽核

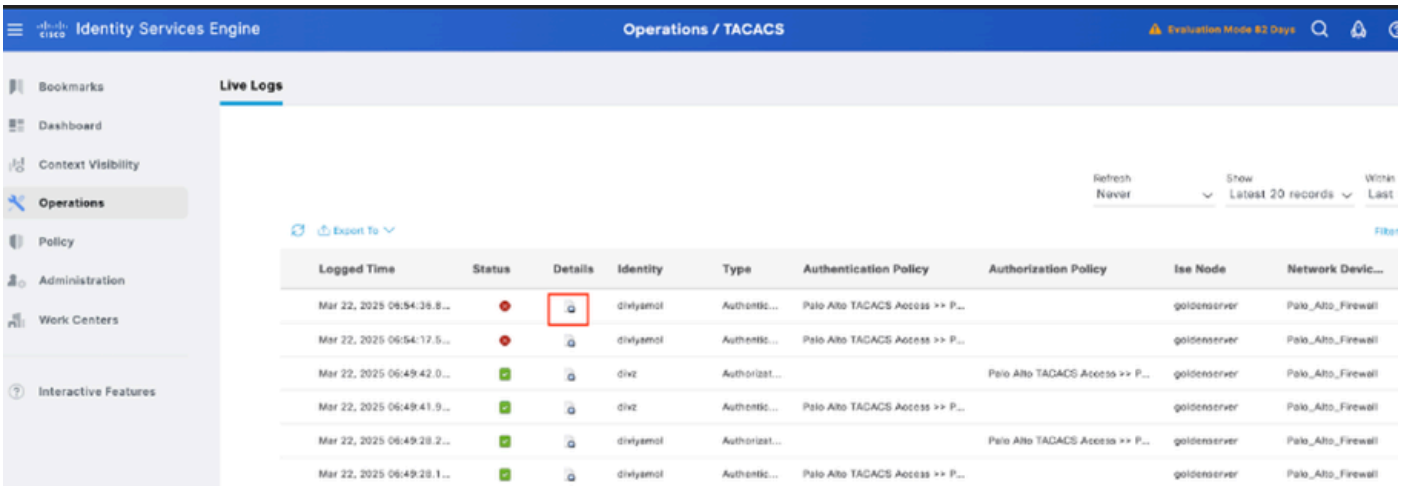
步驟1.檢查TACACS+可維護性是否正在運行，可以簽入：

- GUI:如果節點在Administration -> System -> Deployment中以DEVICE ADMIN服務列出，請檢視。
- CLI:執行命令show ports | include 49以確認TCP連線埠中有屬於TACACS+的連線

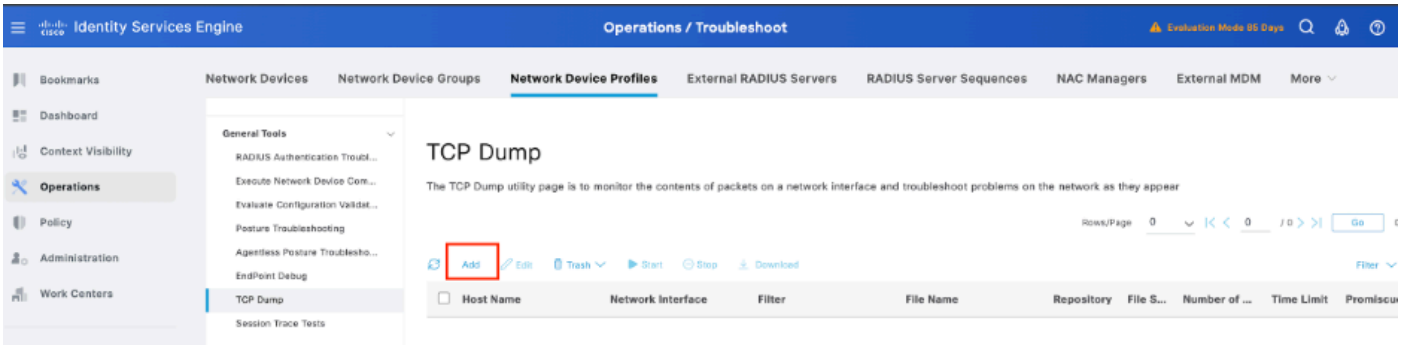
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

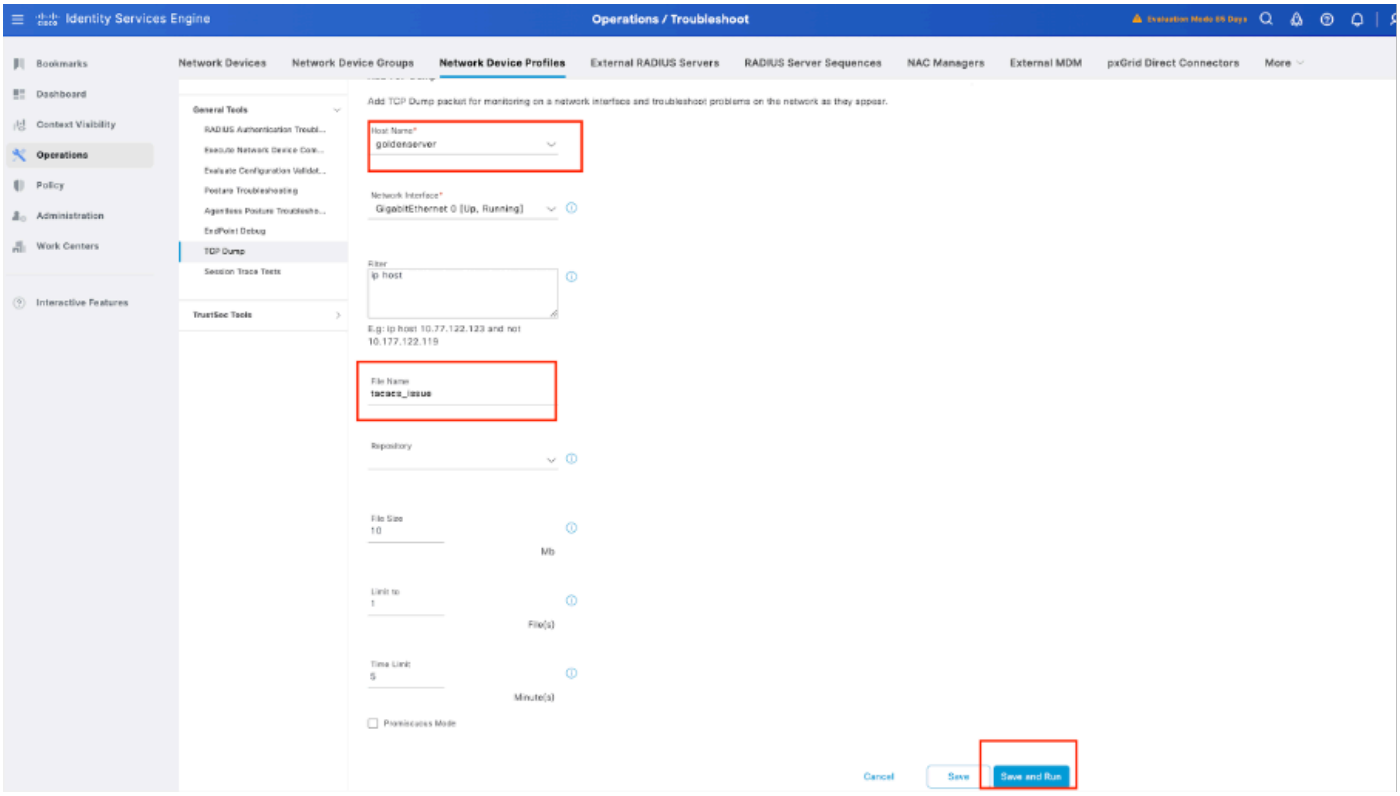
步驟2.確認是否存在有關TACACS+身份驗證嘗試的即時日誌：可在Operations -> TACACS -> Live logs選單中選中此項。

根據故障原因，您可以調整配置或解決故障原因。

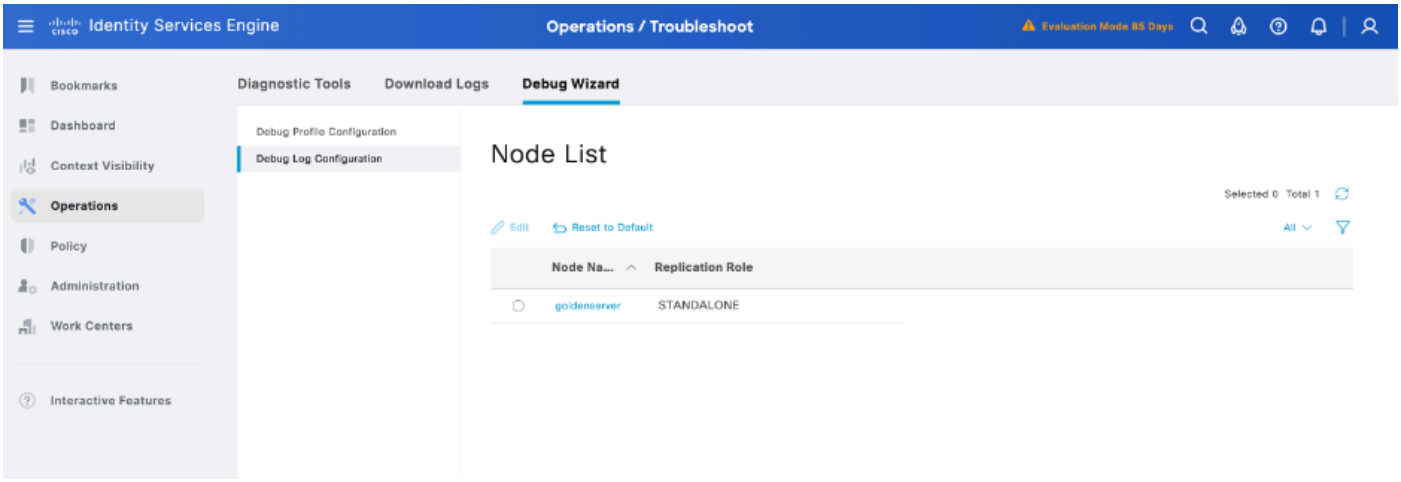


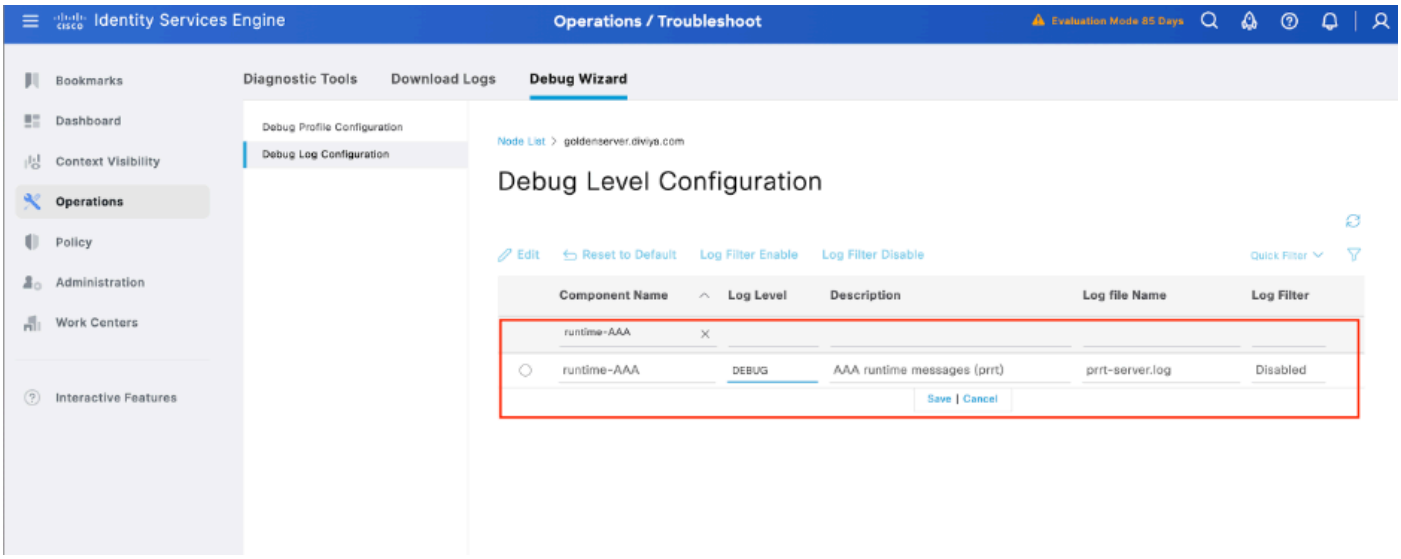
步驟3.如果您沒有看到任何即時日誌，請繼續執行資料包捕獲操作，導航到選單Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump，選擇Add。





步驟4.在操作>故障排除>調試嚮導>調試日誌配置中執行身份驗證的PSN內，啟用調試中的元件runtime-AAA，選擇PSN節點，然後在編輯按鈕中選擇「下一步」。





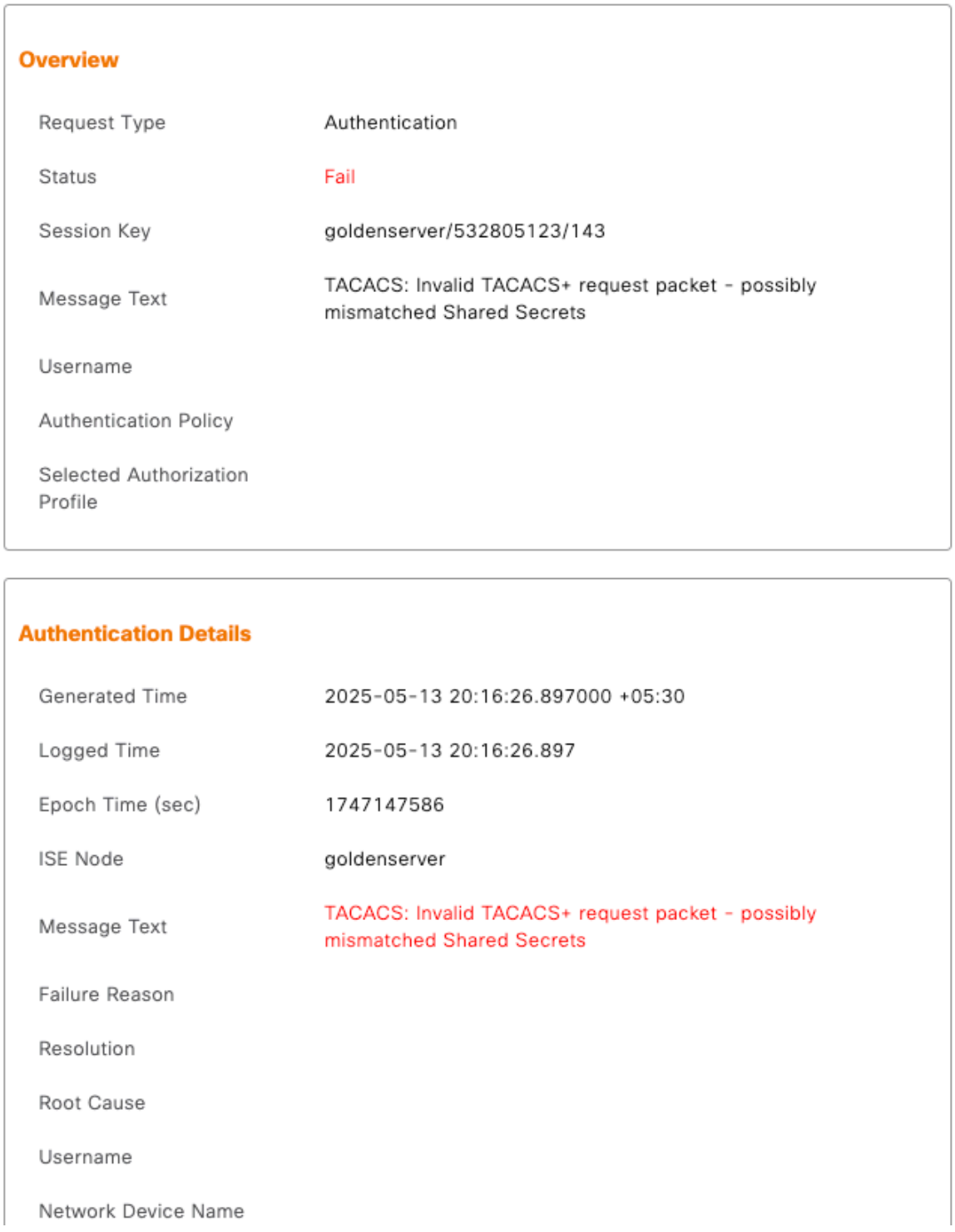
確定運行時AAA元件，將其日誌記錄級別設定為debug，重現問題，並分析日誌以進行進一步調查。

疑難排解

TACACS:無效的TACACS+請求資料包 — 可能共用金鑰不匹配

問題

思科ISE和Palo Alto防火牆（或任何網路裝置）之間的TACACS+身份驗證失敗，並顯示以下錯誤消息：
"無效TACACS+請求資料包 — 可能共用金鑰不匹配"



Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/532805123/143
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-05-13 20:16:26.897000 +05:30
Logged Time	2025-05-13 20:16:26.897
Epoch Time (sec)	1747147586
ISE Node	goldenserver
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Failure Reason	
Resolution	
Root Cause	
Username	
Network Device Name	

這可以阻止成功的管理登入嘗試，並且可能會通過集中身份驗證影響裝置訪問控制。

可能原因

- 思科ISE和Palo Alto防火牆或網路裝置上配置的共用金鑰不匹配。
- 裝置上的TACACS+伺服器配置不正確（例如IP地址、埠或協定錯誤）。

解決方案

此問題有幾種可能的解決方案：

1.驗證共用金鑰：

- 在Cisco ISE上：
  導航到Administration > Network Resources > Network Devices，選擇受影響的裝置，然後確認共用金鑰。

- 在Palo Alto防火牆上：
  轉至Device > Server Profiles > TACACS+，並確保共用金鑰完全匹配，包括大小寫和特殊字元。

2.檢查TACACS+伺服器設定：

- 確保在防火牆的TACACS+配置檔案中配置思科ISE的正確IP地址和埠（預設為49）。

- 確認通訊協定型別是TACACS+（不是RADIUS）。

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）。