在具有ISE的Arista交換機上配置TACACS+身份驗證

目錄

簡介

本文檔介紹如何將Cisco ISE TACACS+與Arista交換機整合以實現集中式AAA管理員訪問。

必要條件

思科建議您瞭解以下主題：

- Cisco ISE和TACACS+通訊協定。
- Arista交換機

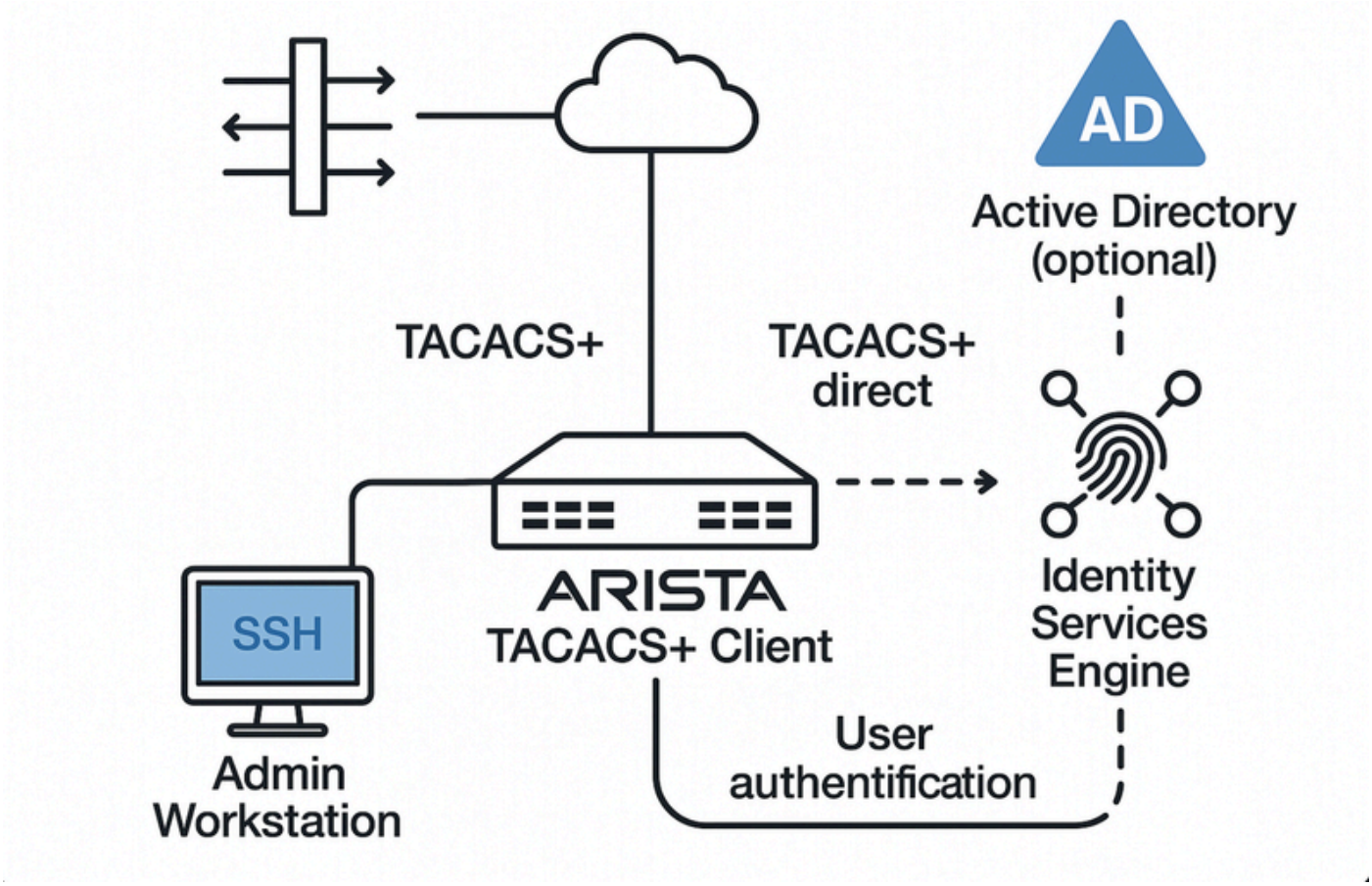
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Arista switch軟體映像版本：4.33.2F
- 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

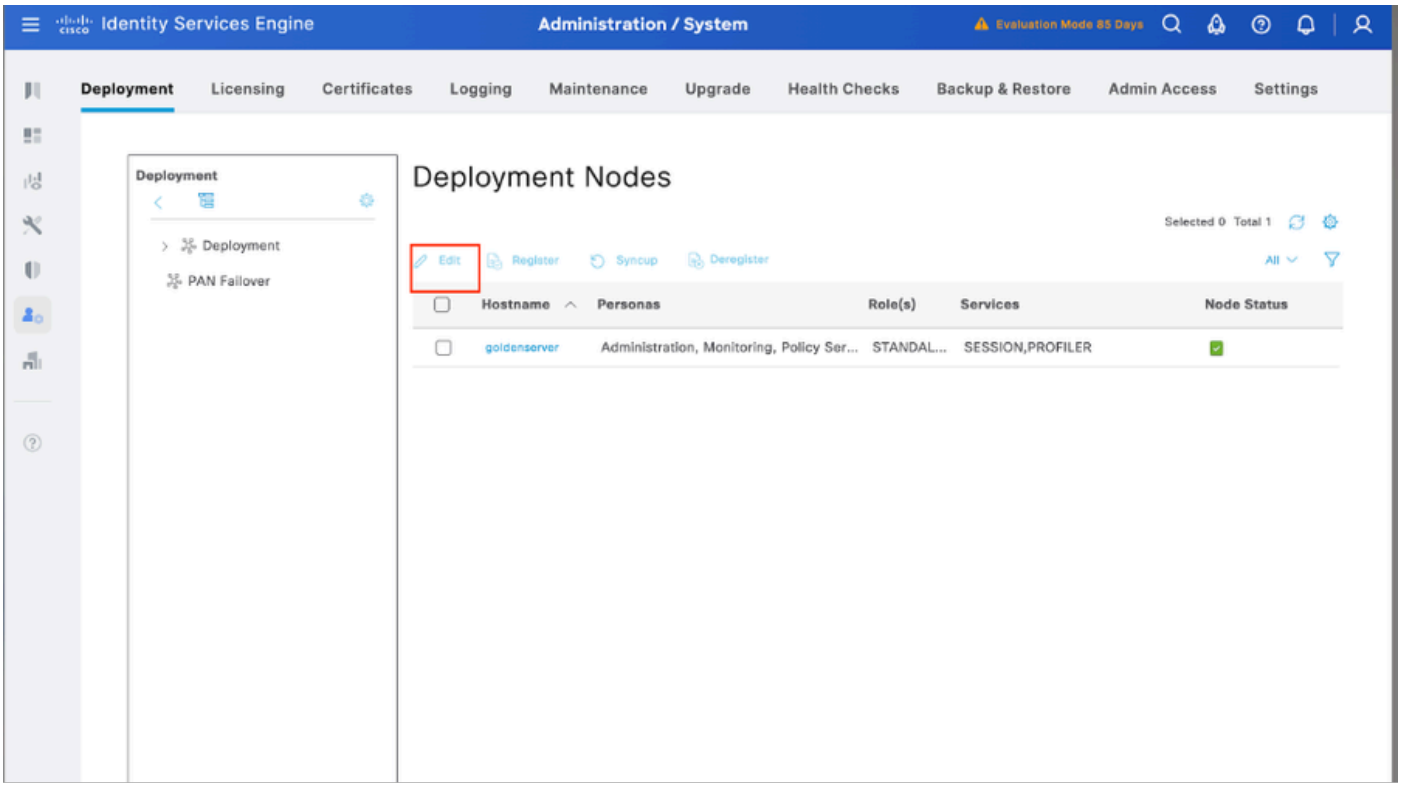


組態

ISE上的TACACS+配置

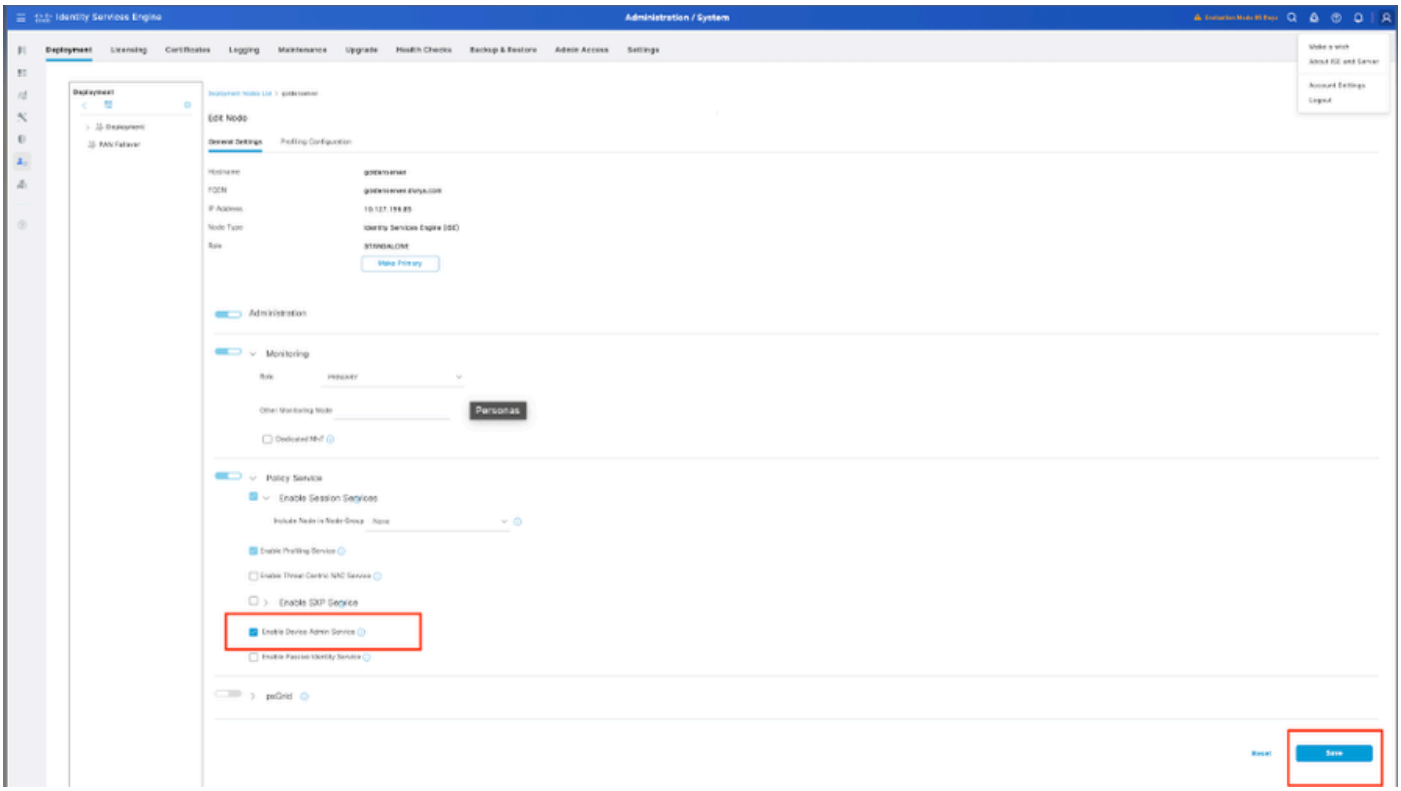
步驟1。初始步驟是驗證思科ISE是否具備處理TACACS+身份驗證的必要能力。為此，請確認所需的策略服務節點(PSN)已啟用裝置管理服務功能。

導覽至Administration > System > Deployment，選擇ISE處理TACACS+身份驗證的相應節點，然後點選Edit以檢視其配置。



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。



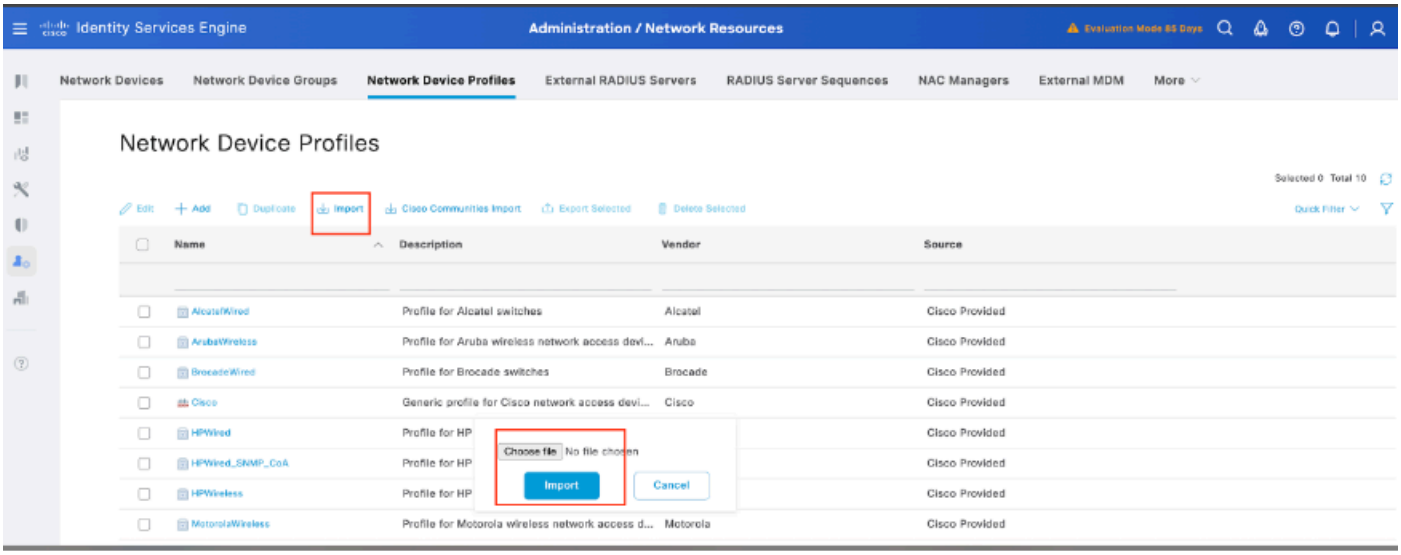
步驟3.獲取Cisco ISE的Arista網路裝置配置檔案。

思科社群已共用Arista裝置的專用NAD配置檔案。此配置檔案以及必要的字典檔案，可在Arista

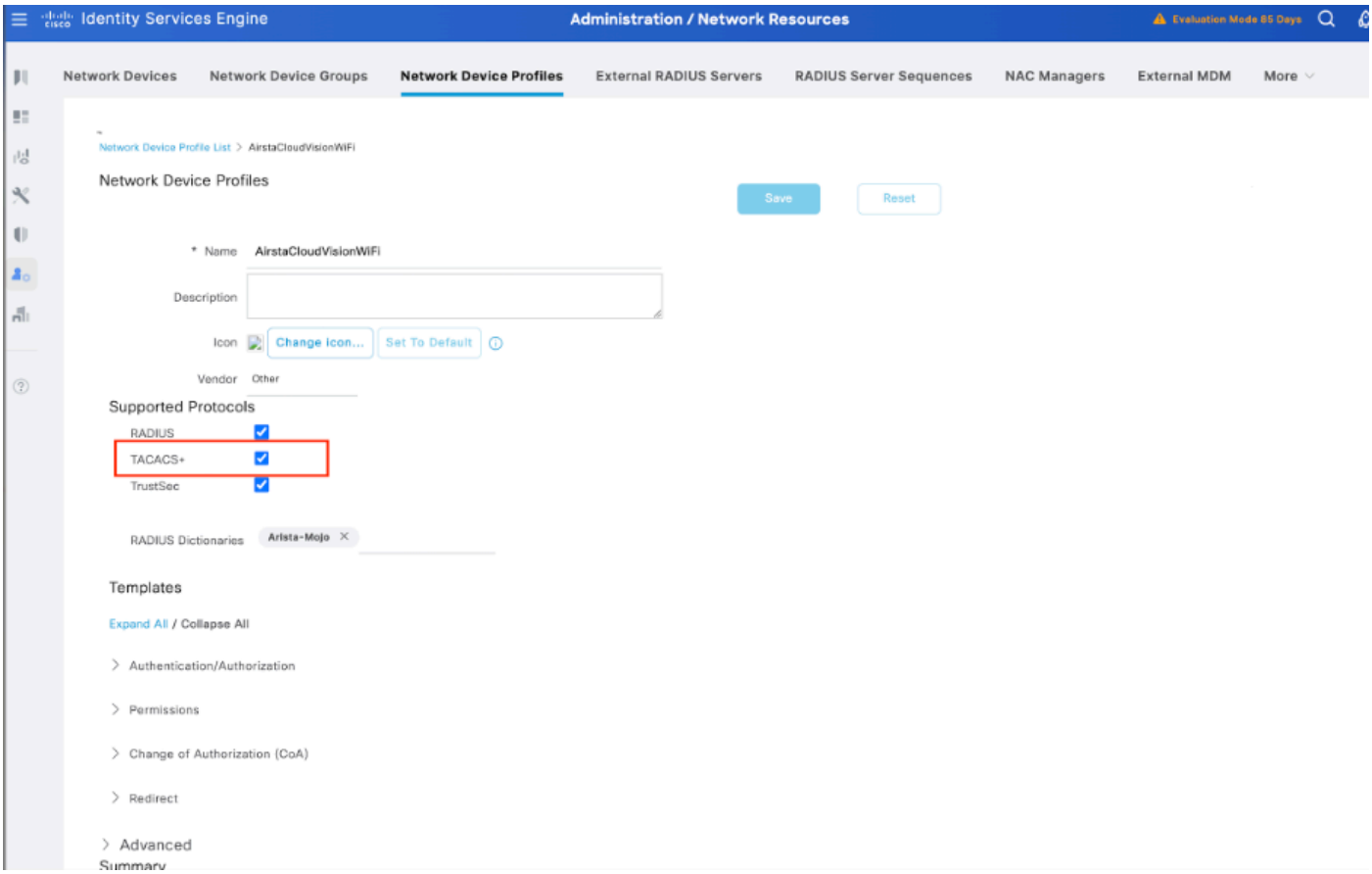
CloudVision WiFi Dictionary and NAD Profile for ISE Integration一文中找到。將此配置檔案下載並匯入到ISE設定有助於更順利的整合。

將Arista NAD配置檔案匯入思科ISE的步驟：

1. 下載設定檔：
    - 從上面提供的思科社群連結獲取Arista NAD配置檔案。
2. 訪問思科ISE:
    - 登入到您的Cisco ISE管理控制檯。
3. 匯入NAD配置檔案：
    - 導覽至Administration > Network Resources > Network Device Profiles。
    - 按一下「匯入」按鈕。
    - 上傳下載的Arista NAD配置檔案。

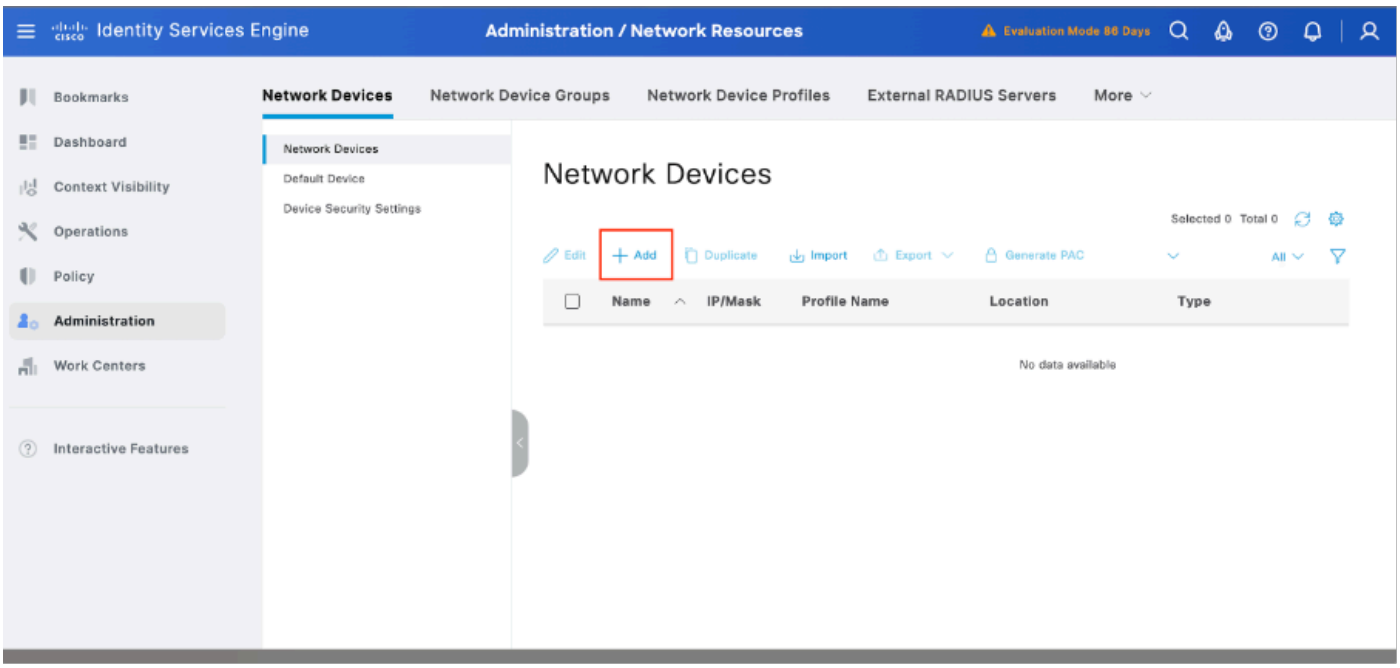


上傳完成後，導覽至Edit選項，並啟用TACACS+作為支援的通訊協定。



步驟 2:新增Arista Switch作為網路裝置。

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

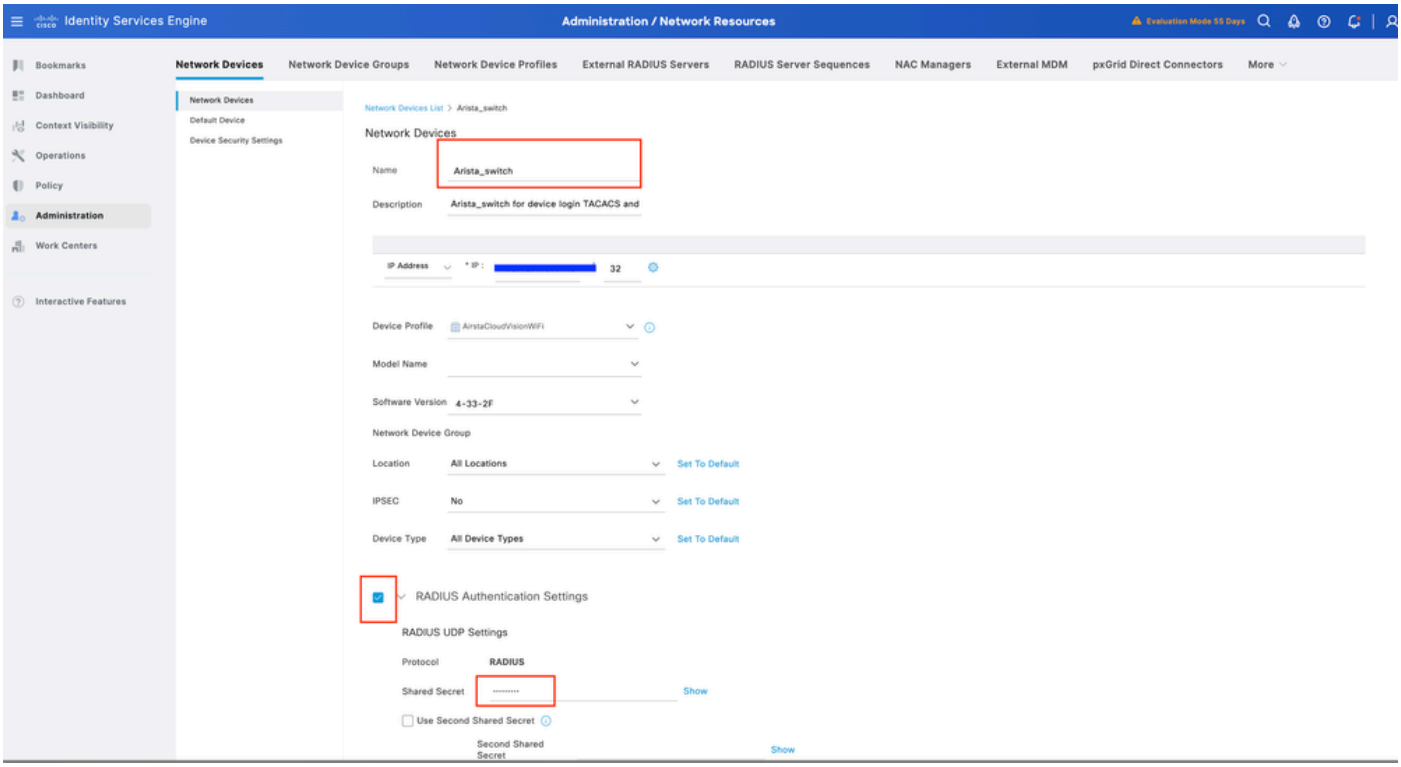


2.按一下Add並輸入以下詳細資訊：

- IP 位址:<Switch-IP>
- 裝置型別:選擇其他有線
- 網路裝置配置檔案:選擇AirstaCloudVisionWiFi。

- RADIUS驗證設定:
  - 啟用RADIUS身份驗證。
  - 輸入Shared Secret（必須與交換機配置匹配）。

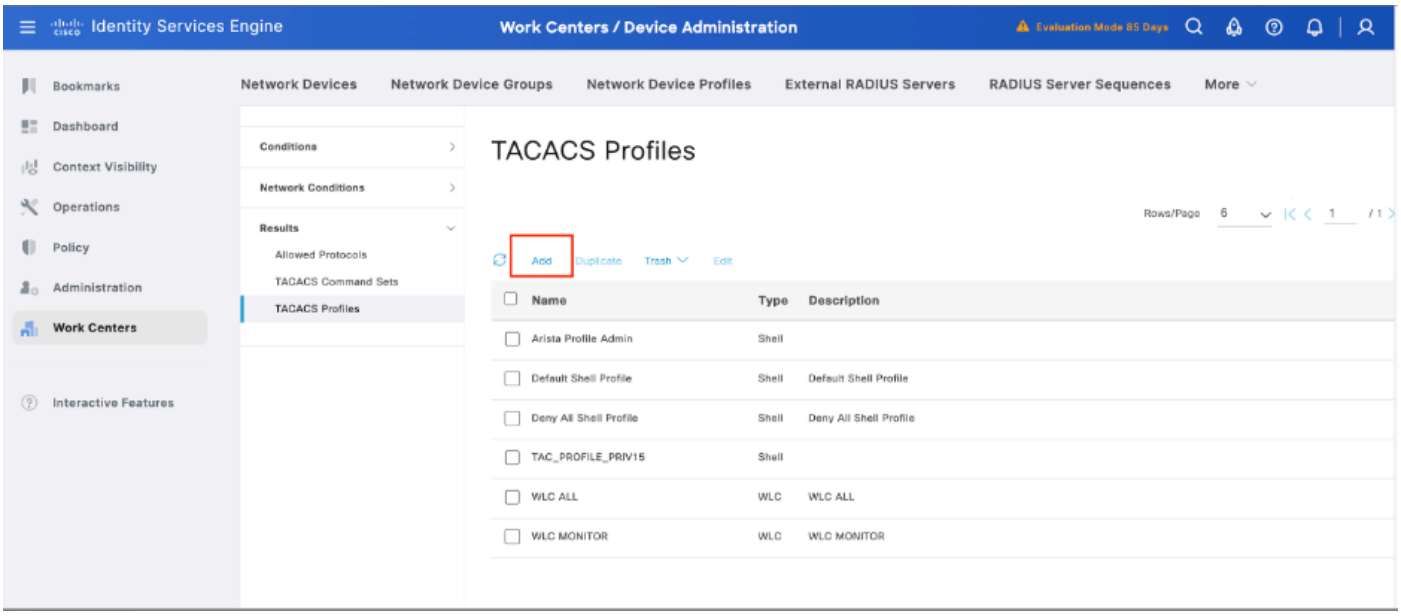
3.按一下Save:



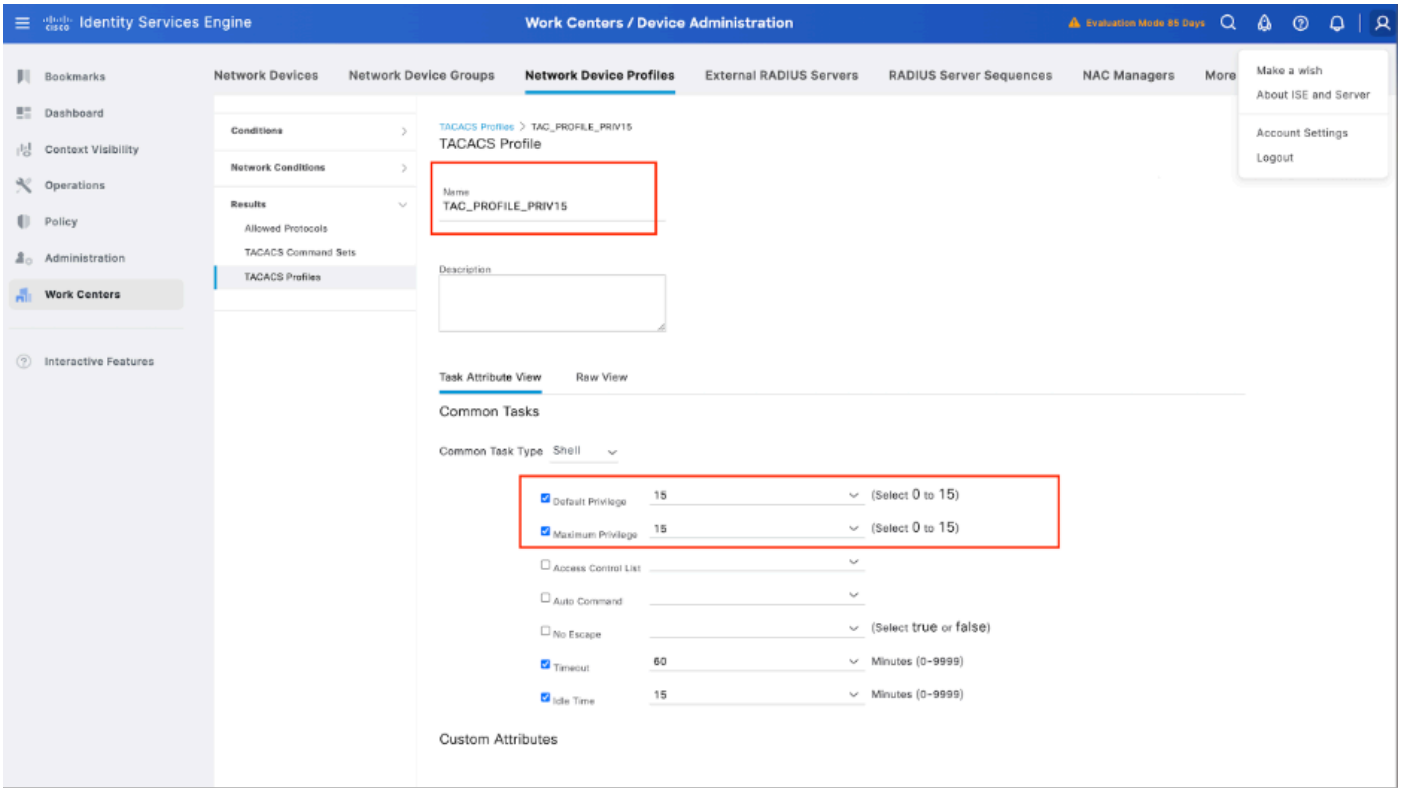
步驟3.驗證新裝置顯示在Network Devices(網絡裝置)下:

步驟4.配置TACACS配置檔案。

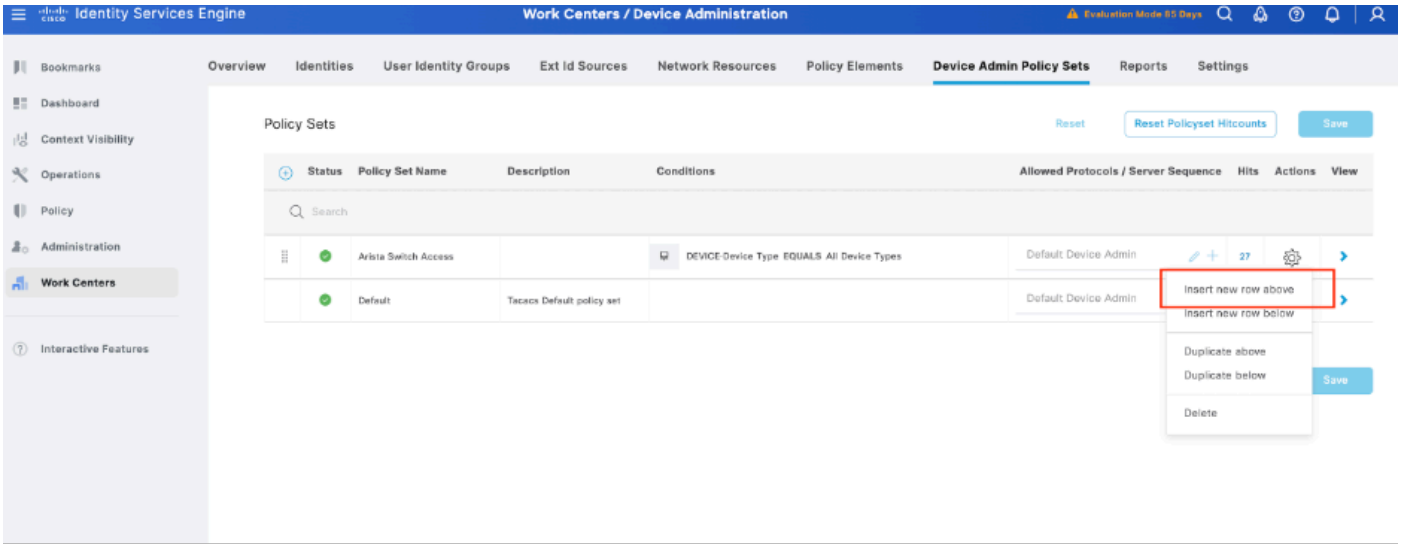
建立TACACS配置檔案，導航到選單Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles，然後選擇Add:



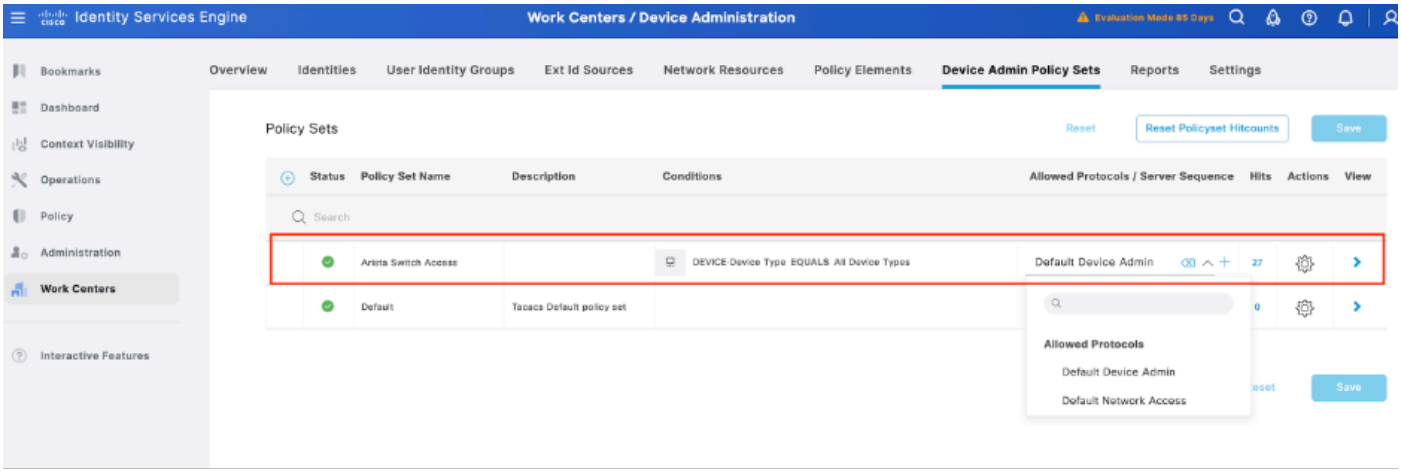
輸入名稱，選中預設許可權覈取方塊，然後將值設定為15。此外，選擇「最大許可權」，將其值設定為15，然後按一下提交:



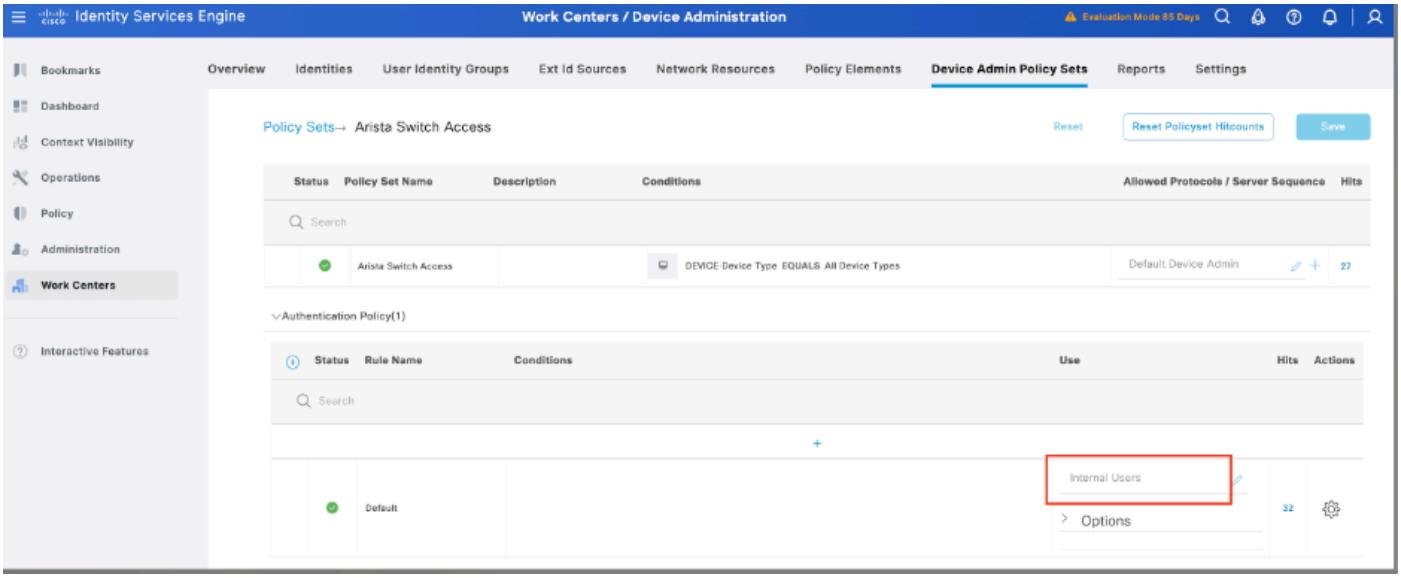
步驟5.建立用於Arista Switch的Device Admin Policy Set，導航到選單Work Centers > Device Administration > Device Admin Policy Sets，然後從現有策略集中選擇齒輪圖示，然後選擇上面的Insert new row。



步驟6.命名此新策略集，根據Arista交換機上正在進行的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。

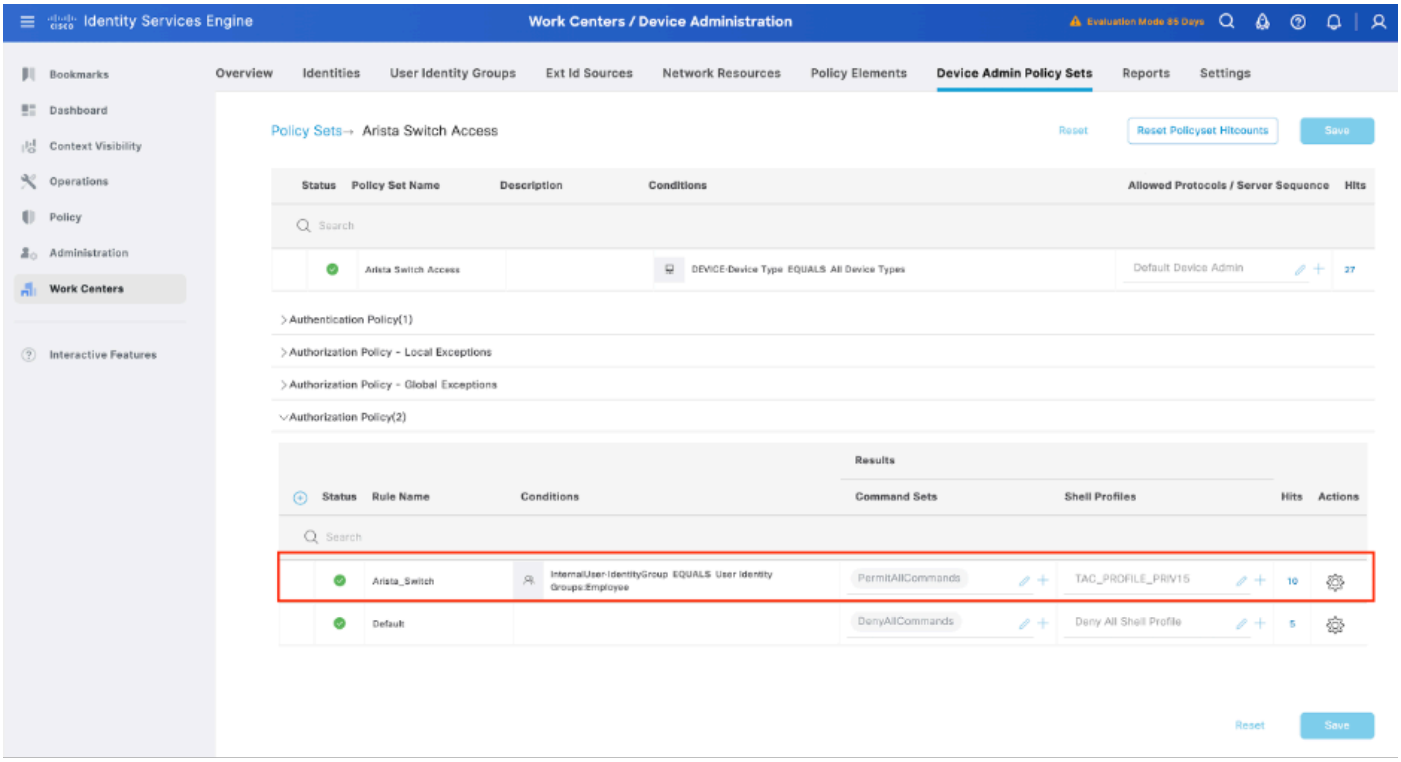


步驟7.在 > view選項中選擇，然後在Authentication Policy部分中選擇Cisco ISE用於在Arista交換機上查詢身份驗證的使用者名稱和憑據的外部身份源。在此示例中，憑證對應於ISE中儲存的內部使用者。



步驟8.向下滾動直到名為Authorization Policy to Default policy的部分，選擇齒輪圖示，然後在上面插入一個規則。

步驟9.命名新的授權規則，新增與已經驗證為組成員身份的使用者有關的條件，並在外殼配置檔案部分新增您先前配置的TACACS配置檔案，儲存配置。



配置Arista交換機

步驟1.啟用TACACS+身份驗證

登入到Arista交換機並進入配置模式：

設定

!

tacacs-server host <ISE-IP> key <TACACS-SECRET>

!

aaa群組伺服器tacacs+ ISE_TACACS

   伺服器<ISE-IP>

!

aaa authentication login default group ISE_TACACS local

aaa authorization exec預設組ISE_TACACS本地

aaa accounting commands 15 default start-stop group ISE_TACACS

!

End

步驟2.儲存組態

要在重新啟動後保留配置，請執行以下操作：

寫入記憶體數量

或

copy running-config startup-config

驗證

ISE稽核

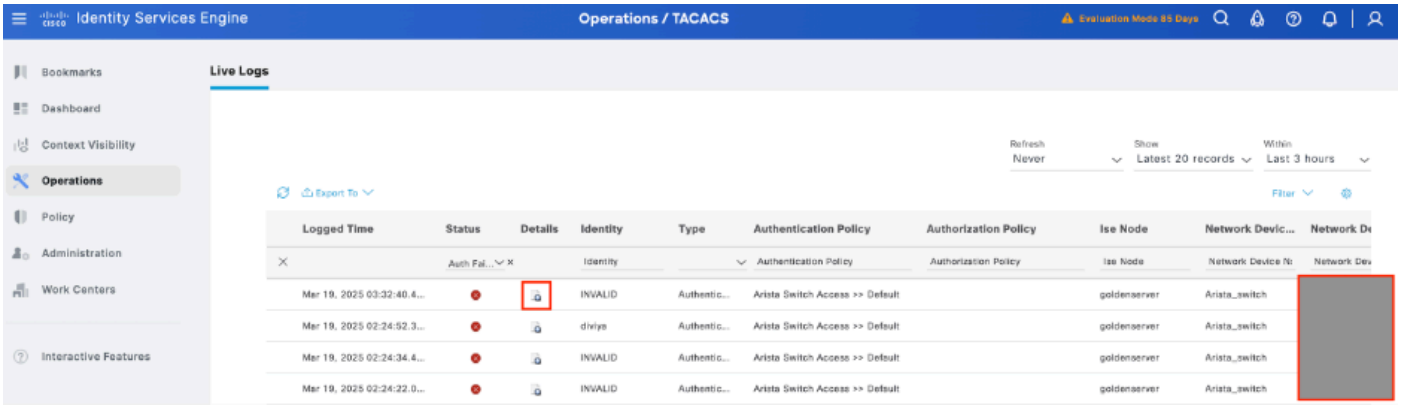
步驟1.檢查TACACS+可維護性是否正在運行，可以簽入：

- GUI:如果節點在System > Deployment中列出了DEVICE ADMIN服務，請參閱該節點。
- CLI:執行命令show ports | include 49以確認TCP連線埠中有屬於TACACS+的連線

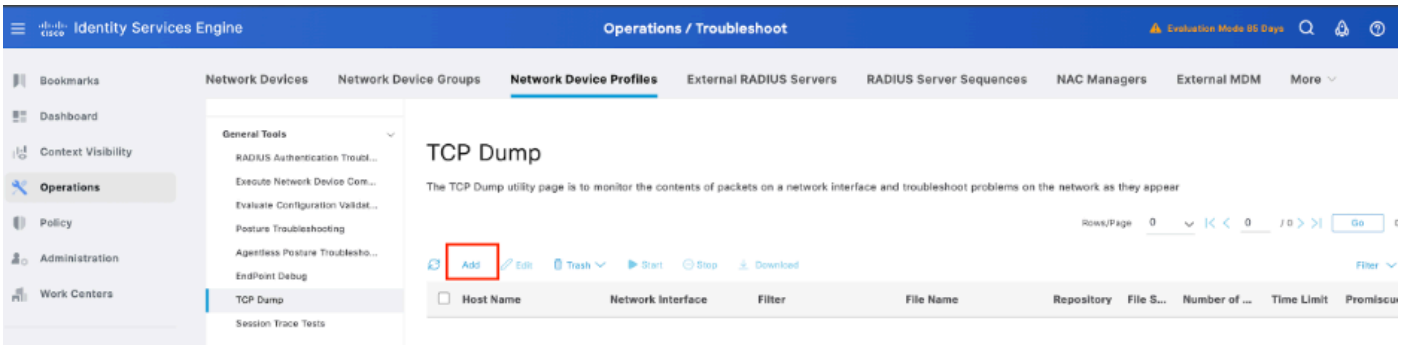
```
goldenserver/admin#show ports | include 49
tcp: [redacted]
```

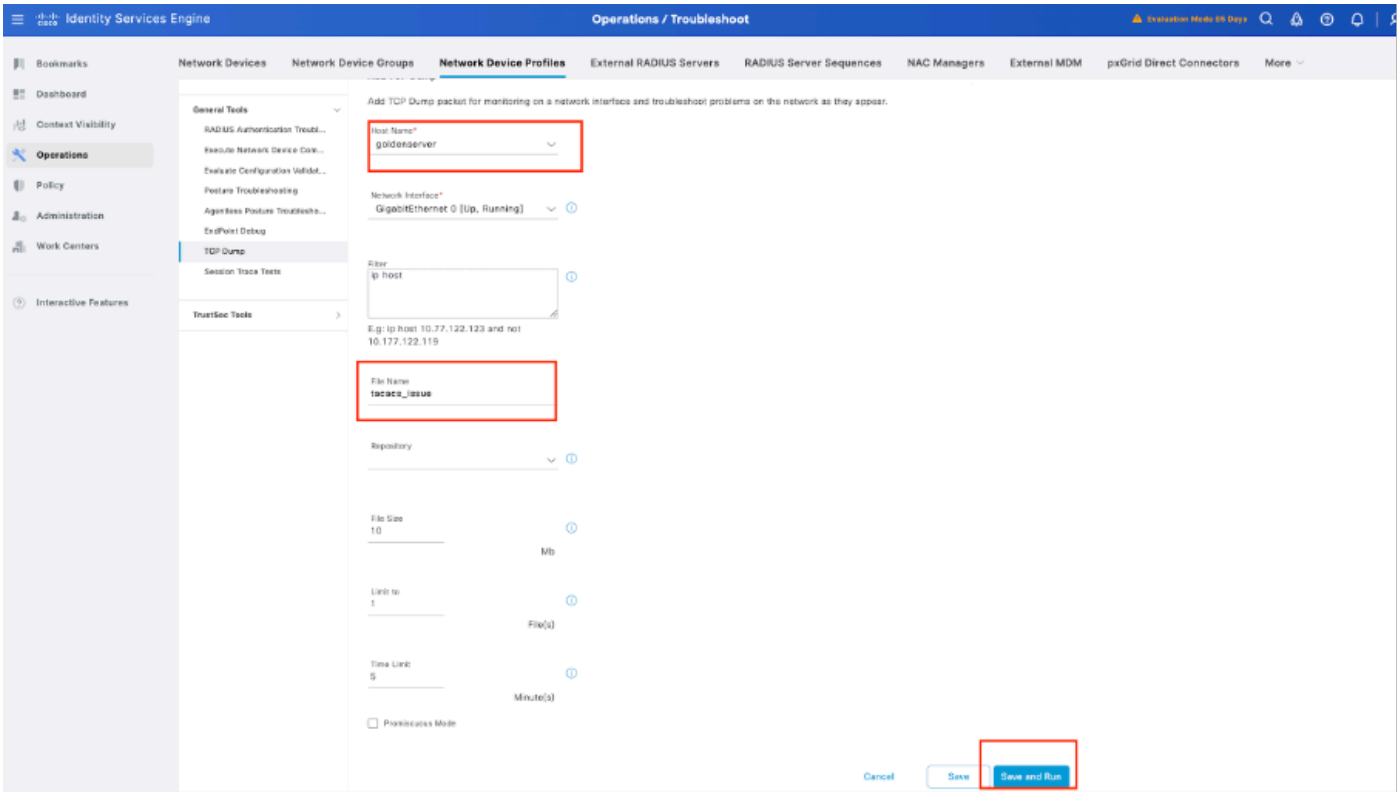
步驟2.確認是否存在有關TACACS+身份驗證嘗試的即時日誌：您可以在Operations > TACACS > Live logs選單中選中此項，

根據故障原因，您可以調整配置或解決故障原因。

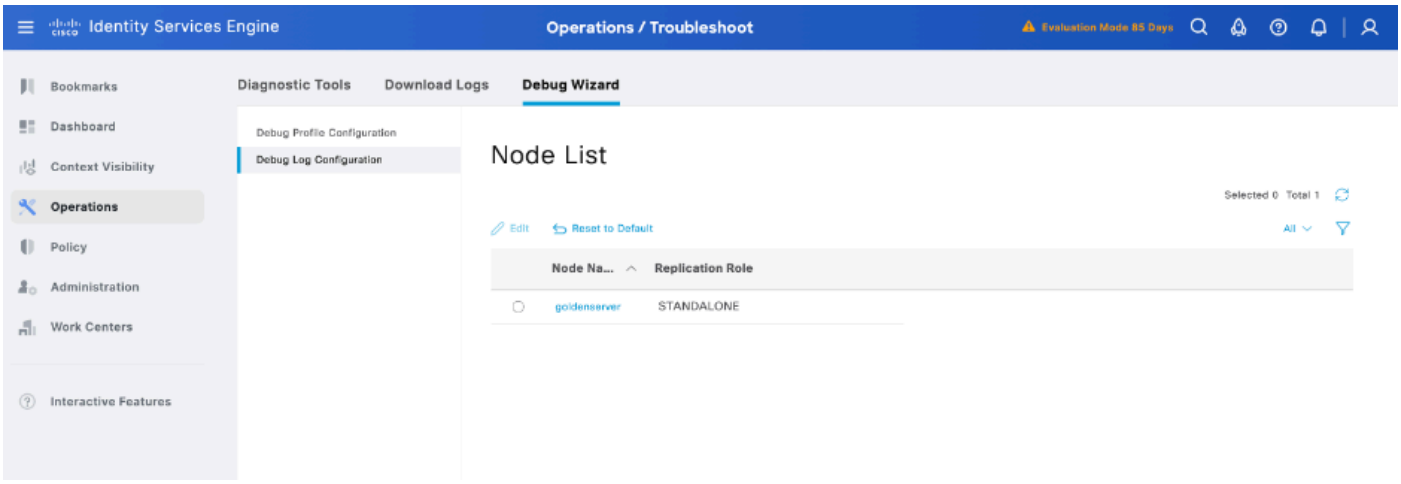


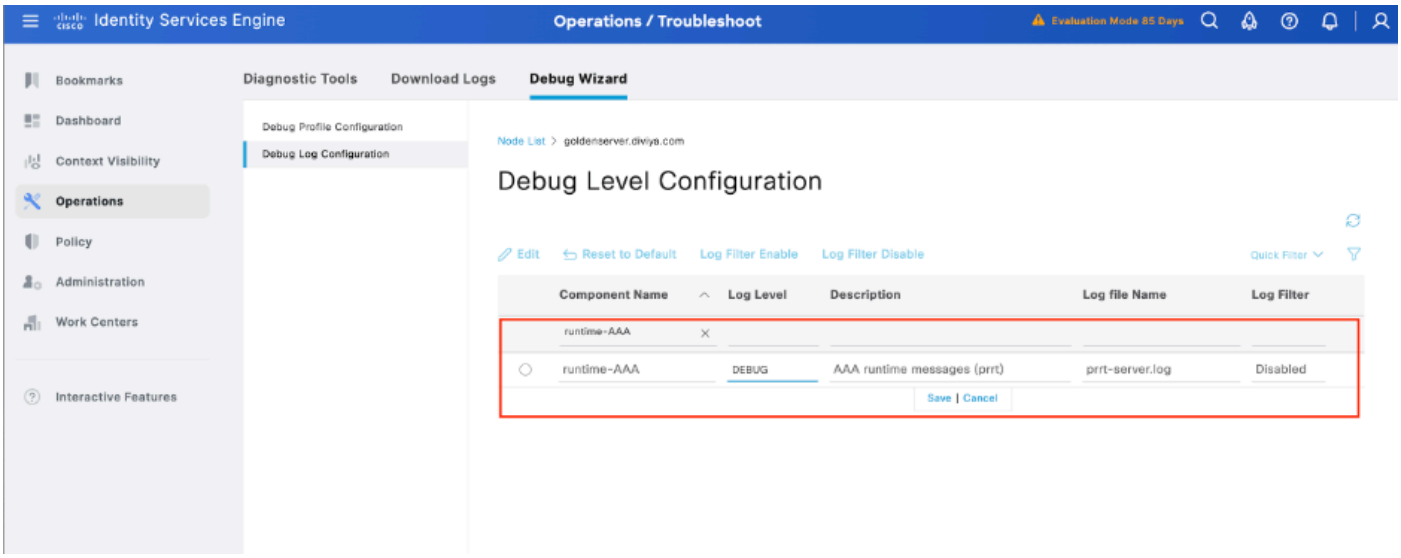
步驟3.如果您沒有看到任何即時日誌，請繼續捕獲資料包。導航到選單Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump，選擇Add:





步驟4.在Operations > Troubleshoot > Debug Wizard > Debug log configuration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，然後選擇Edit按鈕：





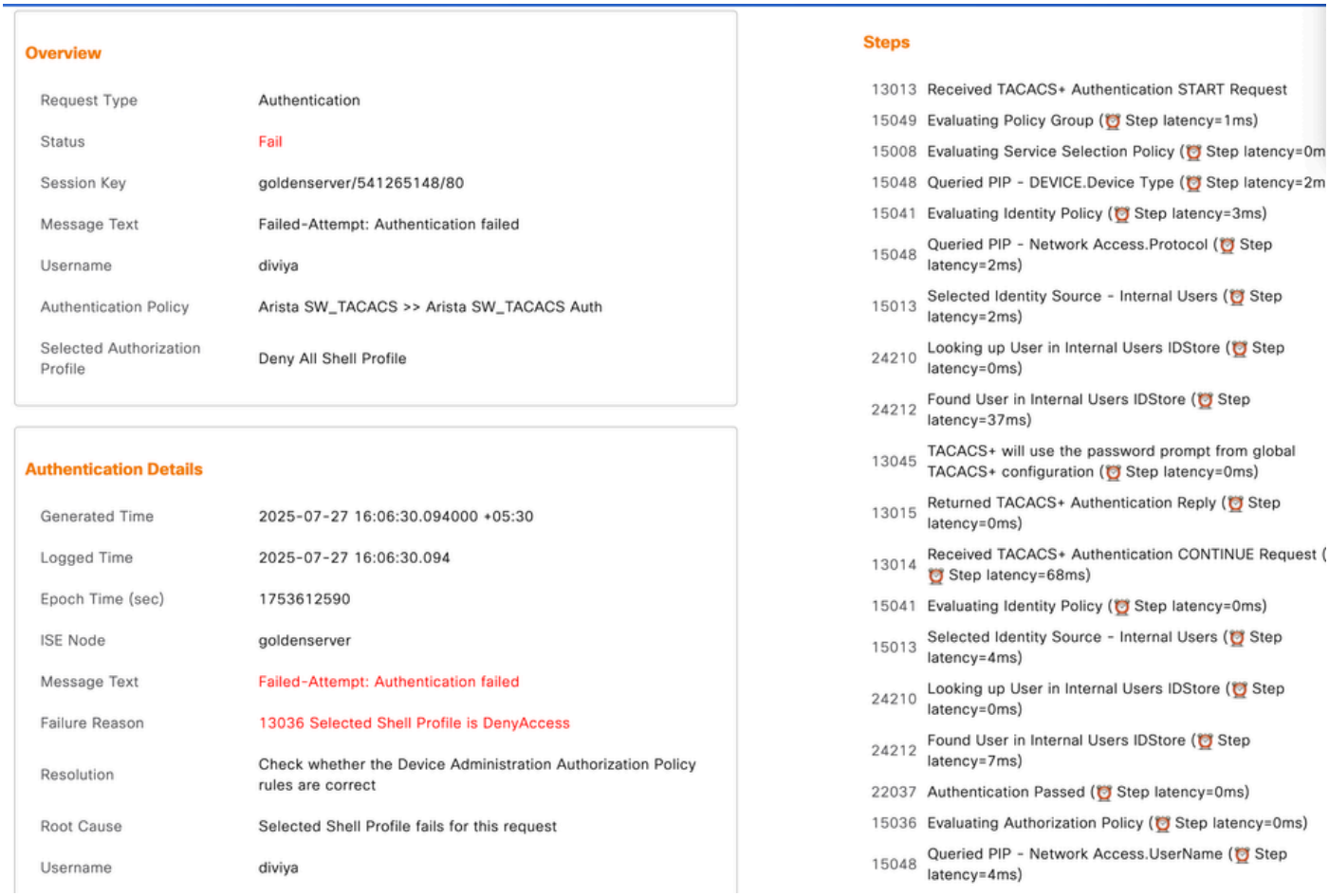
確定運行時AAA元件，將其日誌記錄級別設定為debug，重現問題，並分析日誌以進行進一步調查。

疑難排解

問題1

思科ISE和Arista交換機（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：

"選13036的Shell配置檔案是DenyAccess"



Overview

Request Type	Authentication
Status	Fail
Session Key	goldenserver/541265148/80
Message Text	Failed-Attempt: Authentication failed
Username	diviya
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth
Selected Authorization Profile	Deny All Shell Profile

Authentication Details

Generated Time	2025-07-27 16:06:30.094000 +05:30
Logged Time	2025-07-27 16:06:30.094
Epoch Time (sec)	1753612590
ISE Node	goldenserver
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13036 Selected Shell Profile is DenyAccess
Resolution	Check whether the Device Administration Authorization Policy rules are correct
Root Cause	Selected Shell Profile fails for this request
Username	diviya

Steps

13013	Received TACACS+ Authentication START Request
15049	Evaluating Policy Group (Step latency=1ms)
15008	Evaluating Service Selection Policy (Step latency=0m
15048	Queried PIP - DEVICE.Device Type (Step latency=2m
15041	Evaluating Identity Policy (Step latency=3ms)
15048	Queried PIP - Network Access.Protocol (Step latency=2ms)
15013	Selected Identity Source - Internal Users (Step latency=2ms)
24210	Looking up User in Internal Users IDStore (Step latency=0ms)
24212	Found User in Internal Users IDStore (Step latency=37ms)
13045	TACACS+ will use the password prompt from global TACACS+ configuration (Step latency=0ms)
13015	Returned TACACS+ Authentication Reply (Step latency=0ms)
13014	Received TACACS+ Authentication CONTINUE Request (Step latency=68ms)
15041	Evaluating Identity Policy (Step latency=0ms)
15013	Selected Identity Source - Internal Users (Step latency=4ms)
24210	Looking up User in Internal Users IDStore (Step latency=0ms)
24212	Found User in Internal Users IDStore (Step latency=7ms)
22037	Authentication Passed (Step latency=0ms)
15036	Evaluating Authorization Policy (Step latency=0ms)
15048	Queried PIP - Network Access.UserName (Step latency=4ms)

思科ISE中的錯誤「13036 Selected Shell Profile is DenyAccess」通常意味著在TACACS+裝置管理嘗試期間，授權策略與設定為DenyAccess的Shell配置檔案相匹配。這通常不是錯誤配置的外殼配置檔案本身導致的結果，而是表明配置的授權規則均未與傳入的使用者屬性（如組成員身份、裝置型別或位置）匹配。 因此，ISE回退到預設規則或顯式拒絕規則，導致訪問被拒絕。

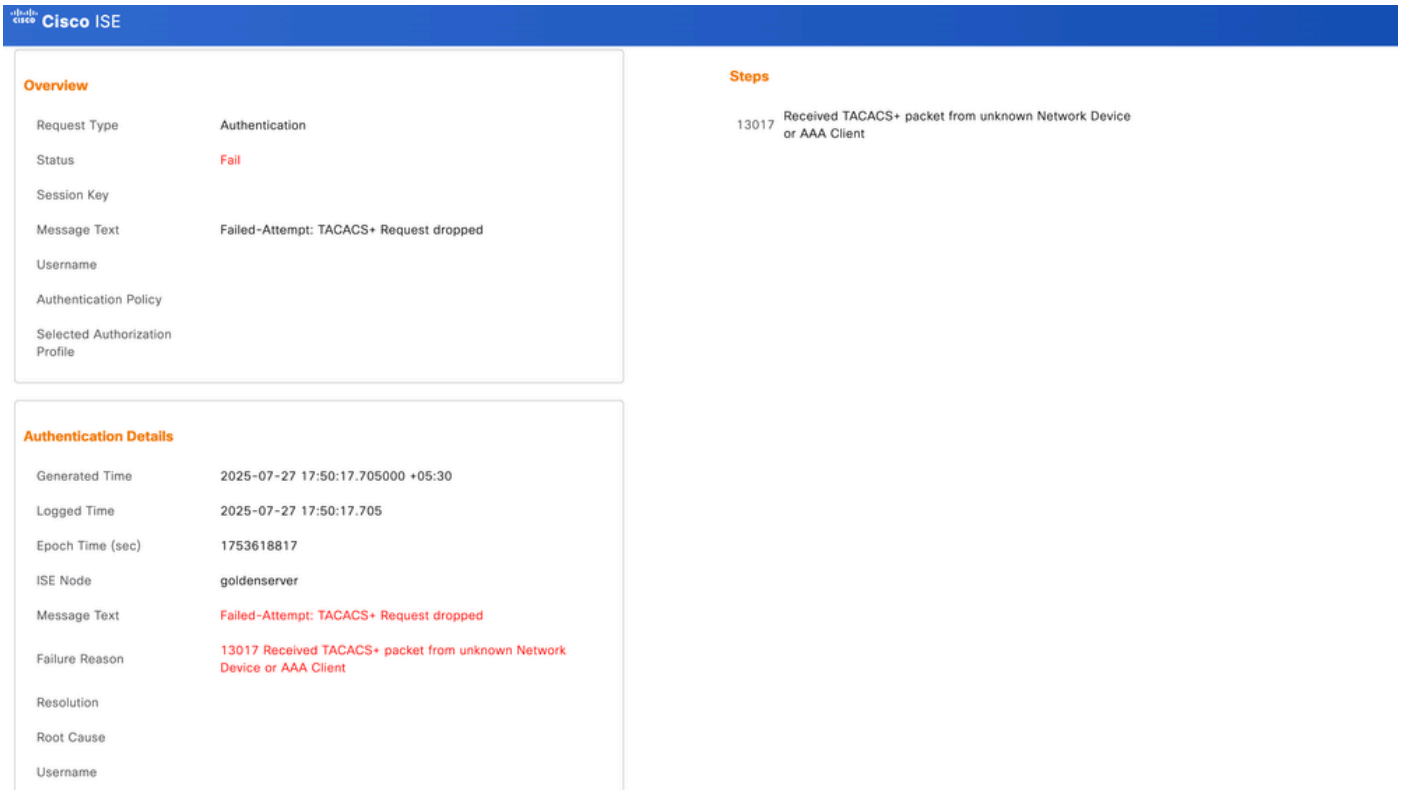
可能原因

- 檢查ISE中的授權策略規則。確認使用者或裝置與分配預期外殼配置檔案的正確規則（例如允許適當訪問的規則）匹配。
- 確保AD或內部使用者組對映正確，並且策略條件（如使用者組成員資格、裝置型別和協定）被準確指定。
- 使用ISE即時日誌和失敗嘗試的詳細資訊，確切瞭解匹配的規則及其原因。

問題2

思科ISE和Arista交換機（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：

"已13017未知網路裝置或AAA客戶端收到TACACS+資料包"



可能原因

- 最常見的原因是，交換機的IP地址沒有新增為ISE中的網路裝置（在Administration > Network Resources > Network Devices下）。
- 確保IP地址或範圍與Arista交換機用於傳送TACACS+資料包的源IP完全匹配。
- 如果您的交換機使用管理介面，請確認其確切的IP（不只是子網/範圍）已新增到ISE中。

解決方案

- 在ISE GUI中轉至Administration > Network Resources > Network Devices。
- 驗證Arista交換機上的確切源IP地址是否用於TACACS+通訊（通常為管理介面IP）。
- 指定共用金鑰（必須與Arista交換機上的設定匹配）。

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）。