使用ISE和TACACS+配置裝置管理的APIC

目錄

簡介

本文檔介紹將APIC與ISE整合以便管理員使用者通過TACACS+協定進行身份驗證的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 應用程式原則基礎架構控制器(APIC)
- 身分識別服務引擎 (ISE)
- TACACS通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- APIC 4.2(7u)版
- ISE版本3.2補丁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。

設定

網路圖表

整合圖表

驗證程式

步驟1.使用管理員使用者憑據登入APIC應用程式。

步驟2.身份驗證過程觸發和ISE在本地或通過Active Directory驗證憑證。

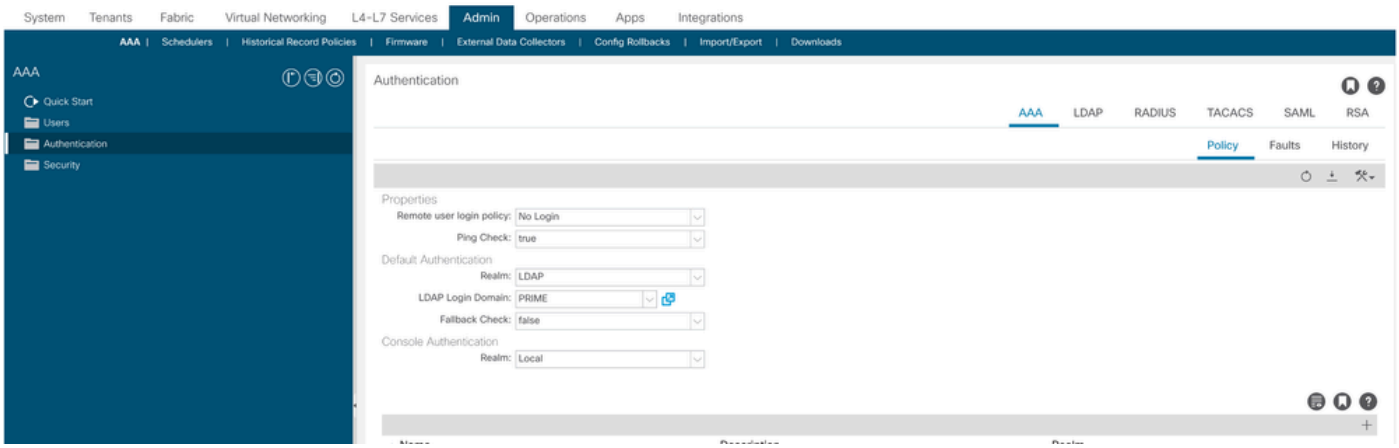
步驟3.身份驗證成功後，ISE傳送允許資料包以授權對APIC的訪問。

步驟4. ISE顯示成功的身份驗證即時日誌。

附註：APIC將TACACS+配置複製到屬於交換矩陣的枝葉交換機。

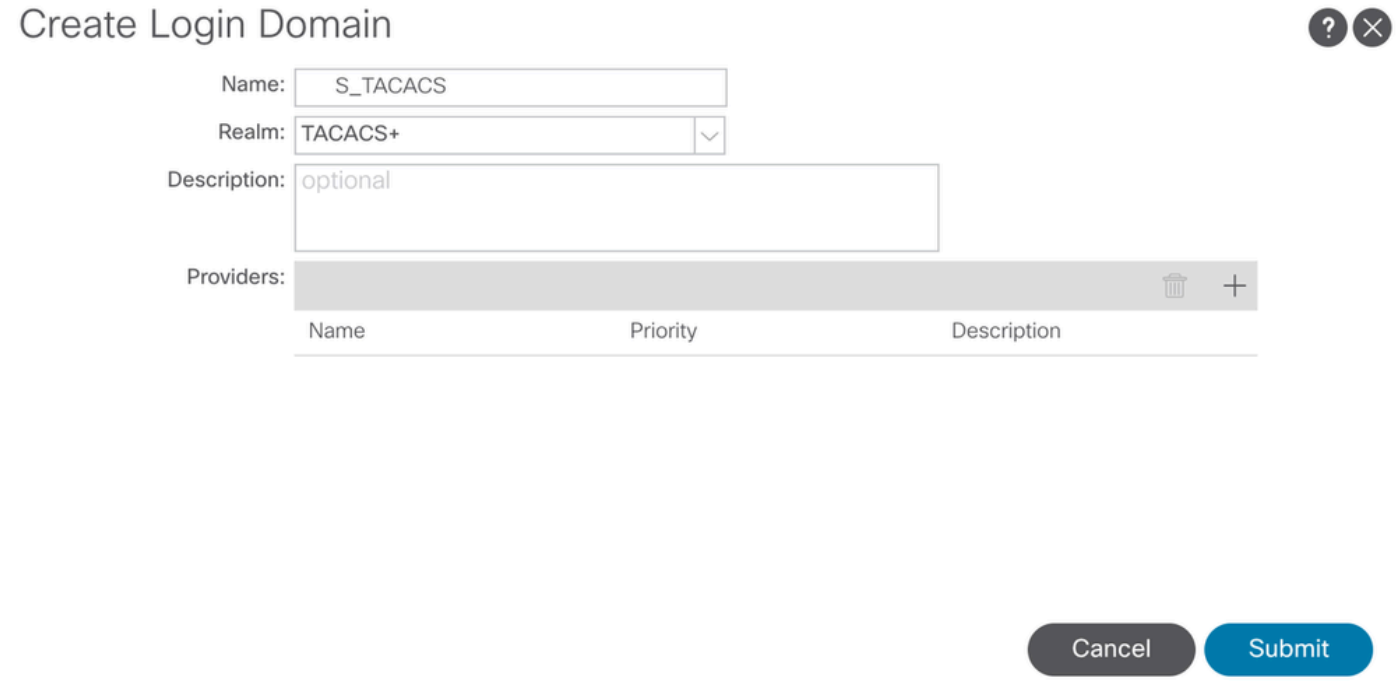
APIC配置

步驟1。導覽至Admin > AAA > Authentication > AAA，然後選擇+ icon，以便建立新的登入網域。

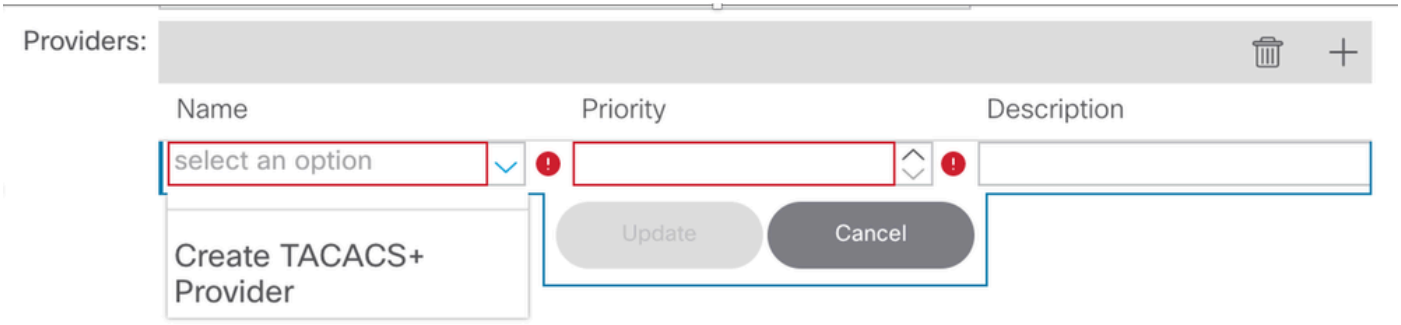


APIC登入管理員配置

步驟2.定義新登入域的名稱和領域，然後按一下+「提供程式」下的以便建立新提供程式。

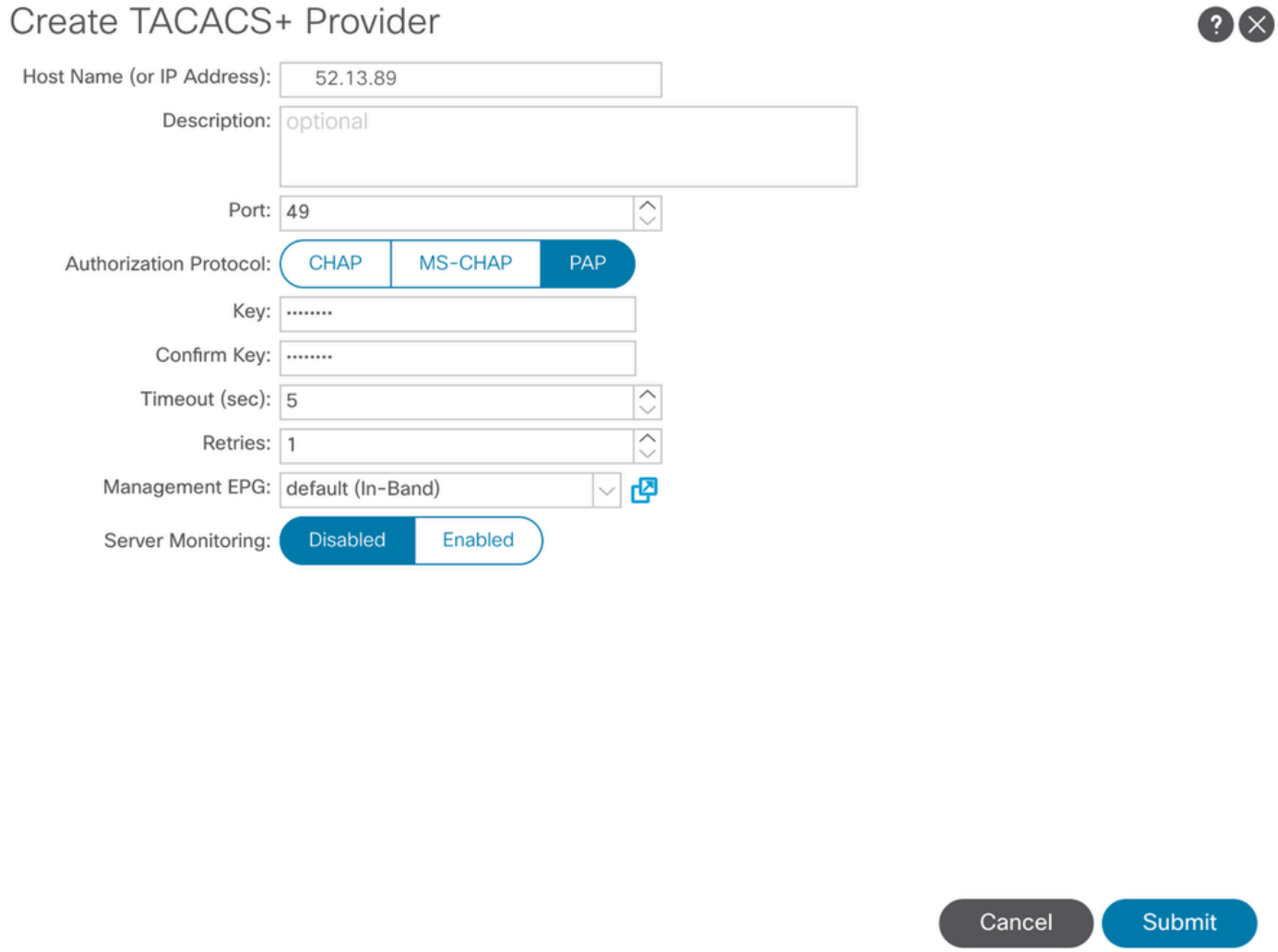


APIC登入管理員

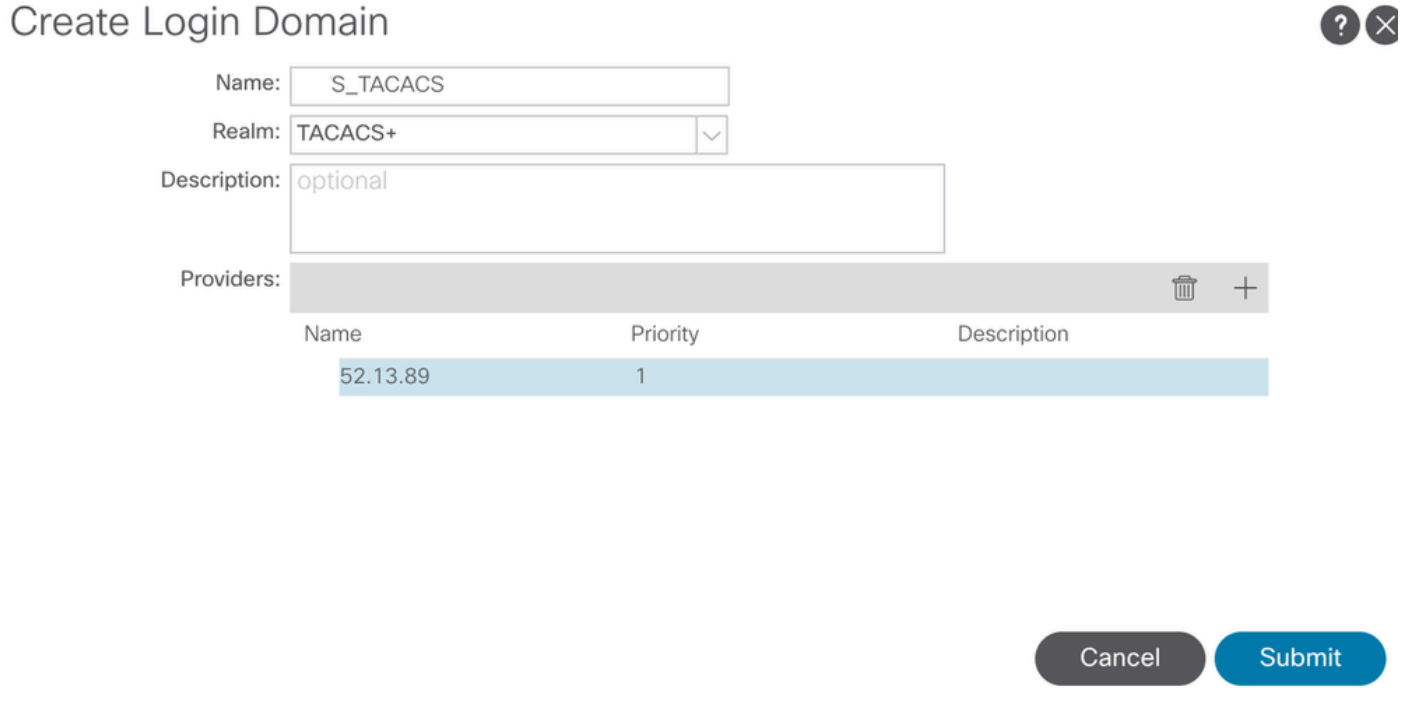


APIC TACACS提供程式

步驟3.定義ISE IP地址或主機名，定義共用金鑰，並選擇管理端點策略組(EPG)。 按一下Submit將TACACS+提供程式新增到登入管理員。



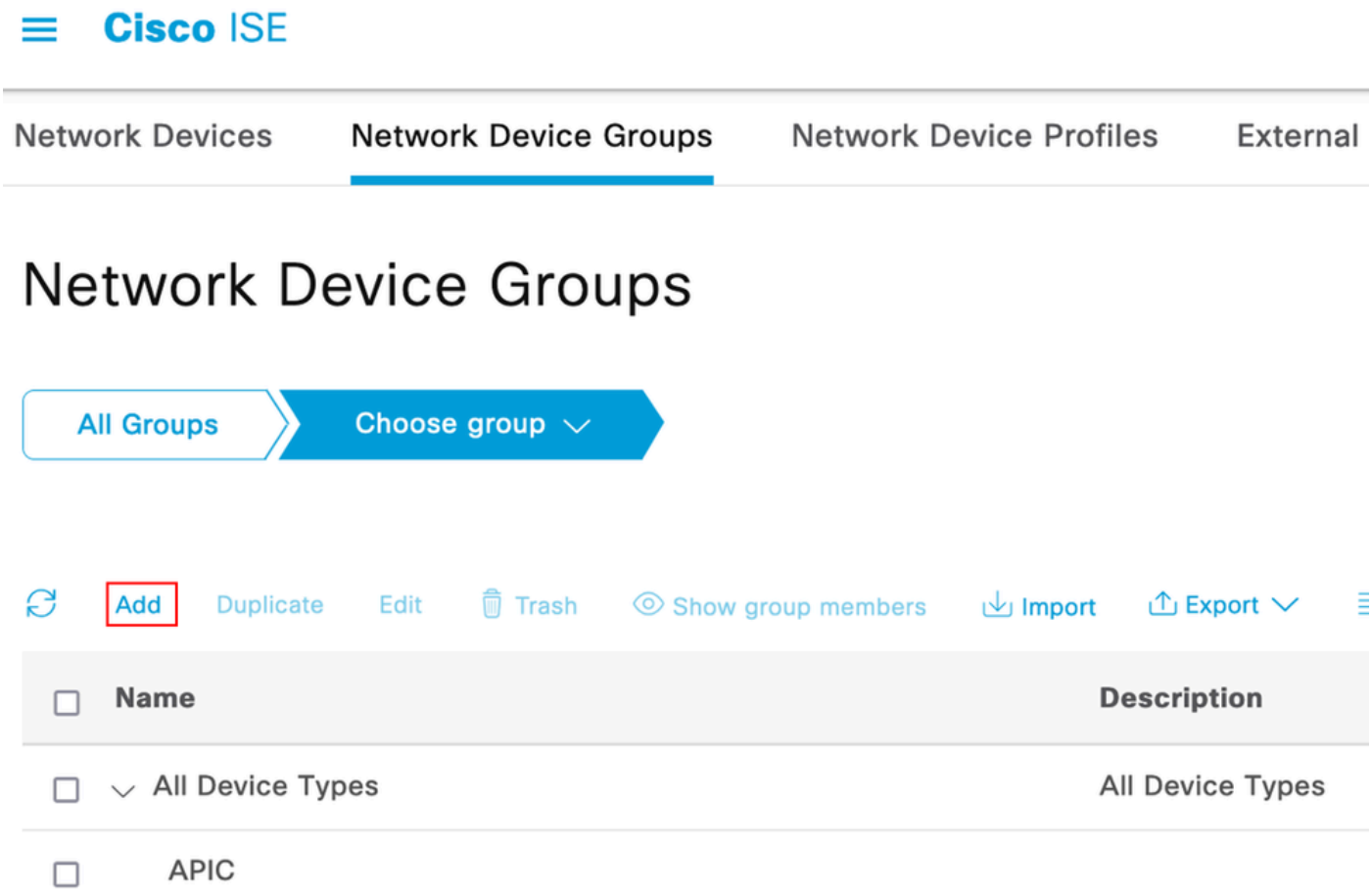
APIC TACACS提供程式設定



TACACS提供程式檢視

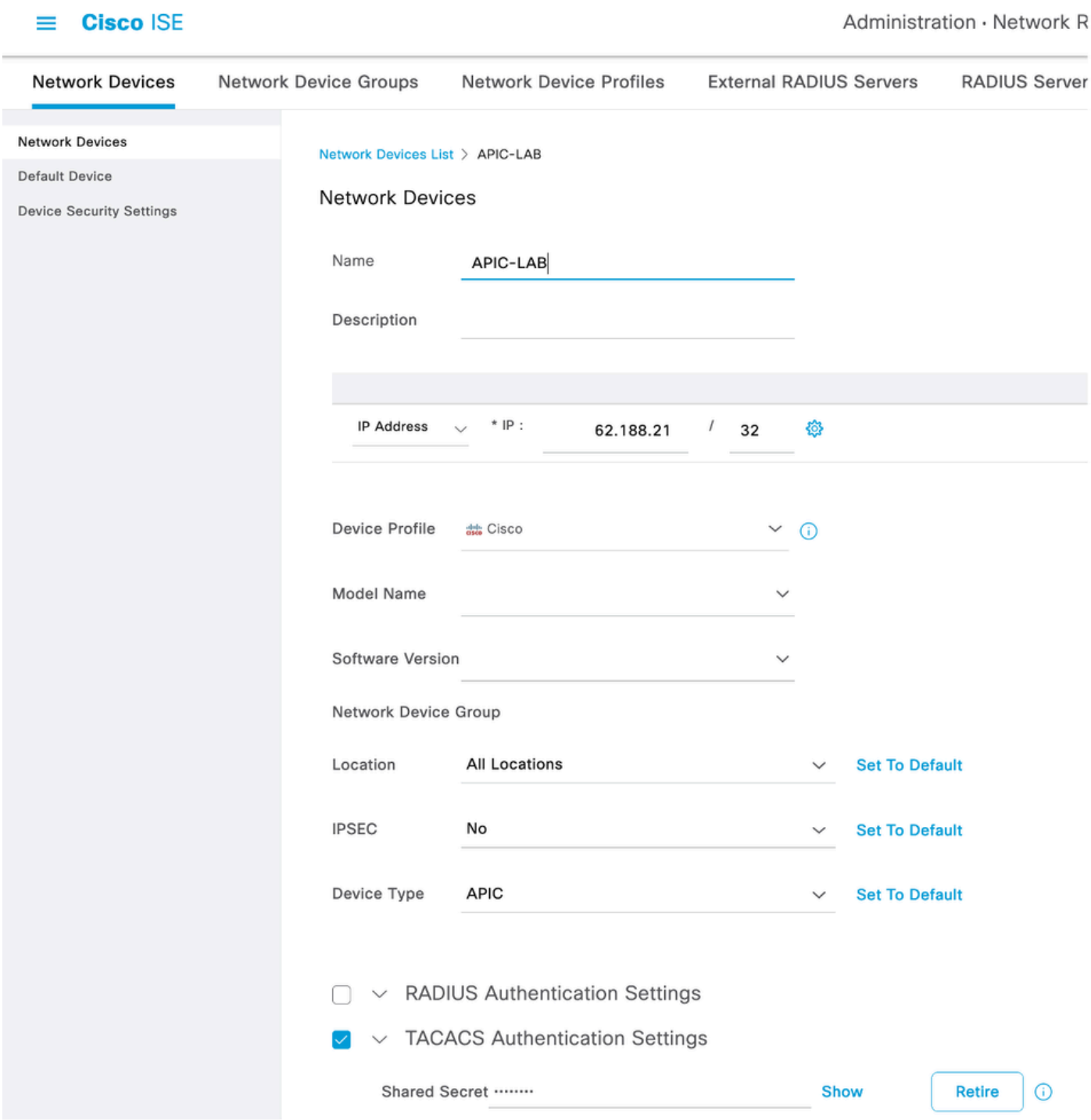
ISE 組態

步驟1.導覽至☰>>網路資源>網路裝置群組。在All Device Types下建立網路裝置組。



ISE網路裝置組

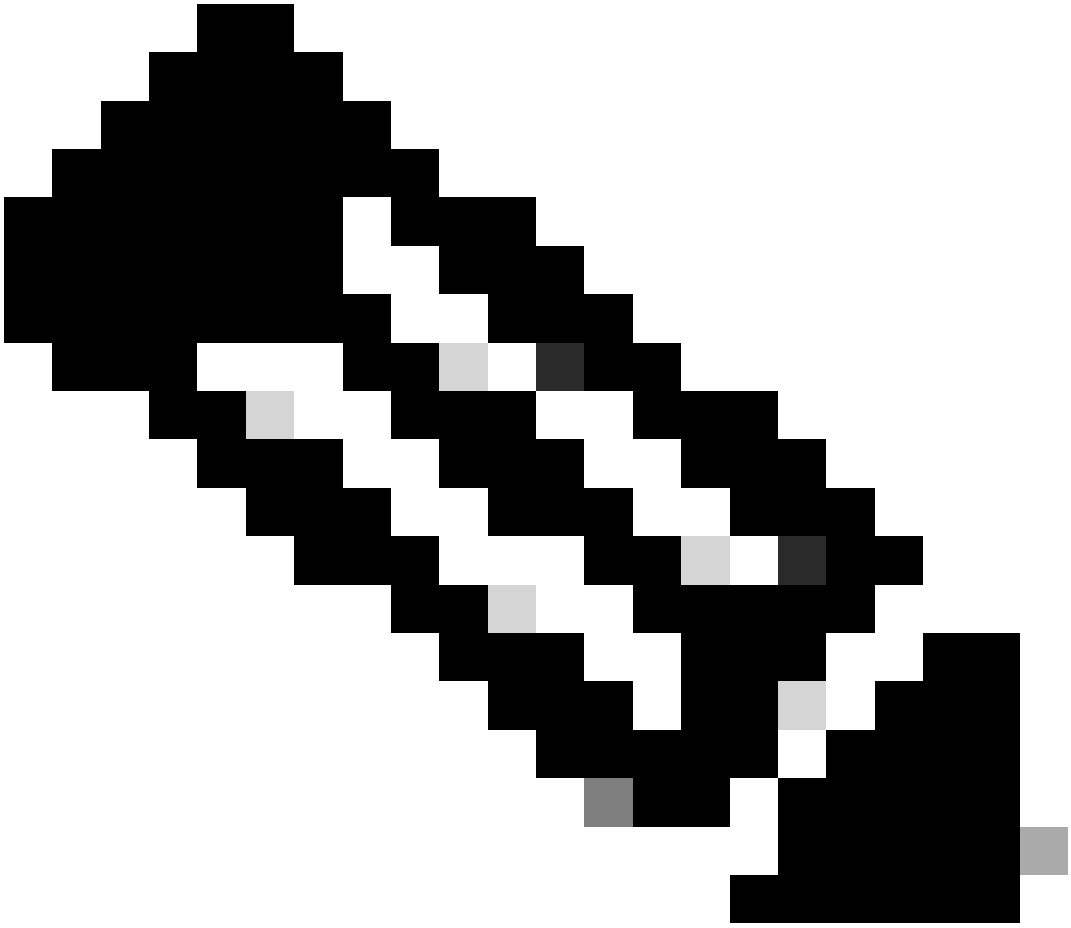
步驟2.導航至Administration > Network Resources > Network Devices。選擇Add「定義APIC名稱和IP地址」，在「裝置型別」和「TACACS+」覈取方塊下選擇「APIC」，並定義APIC TACACS+提供程式配置中使用的密碼。按一下Submit。



對枝葉交換機重複步驟1和步驟2。

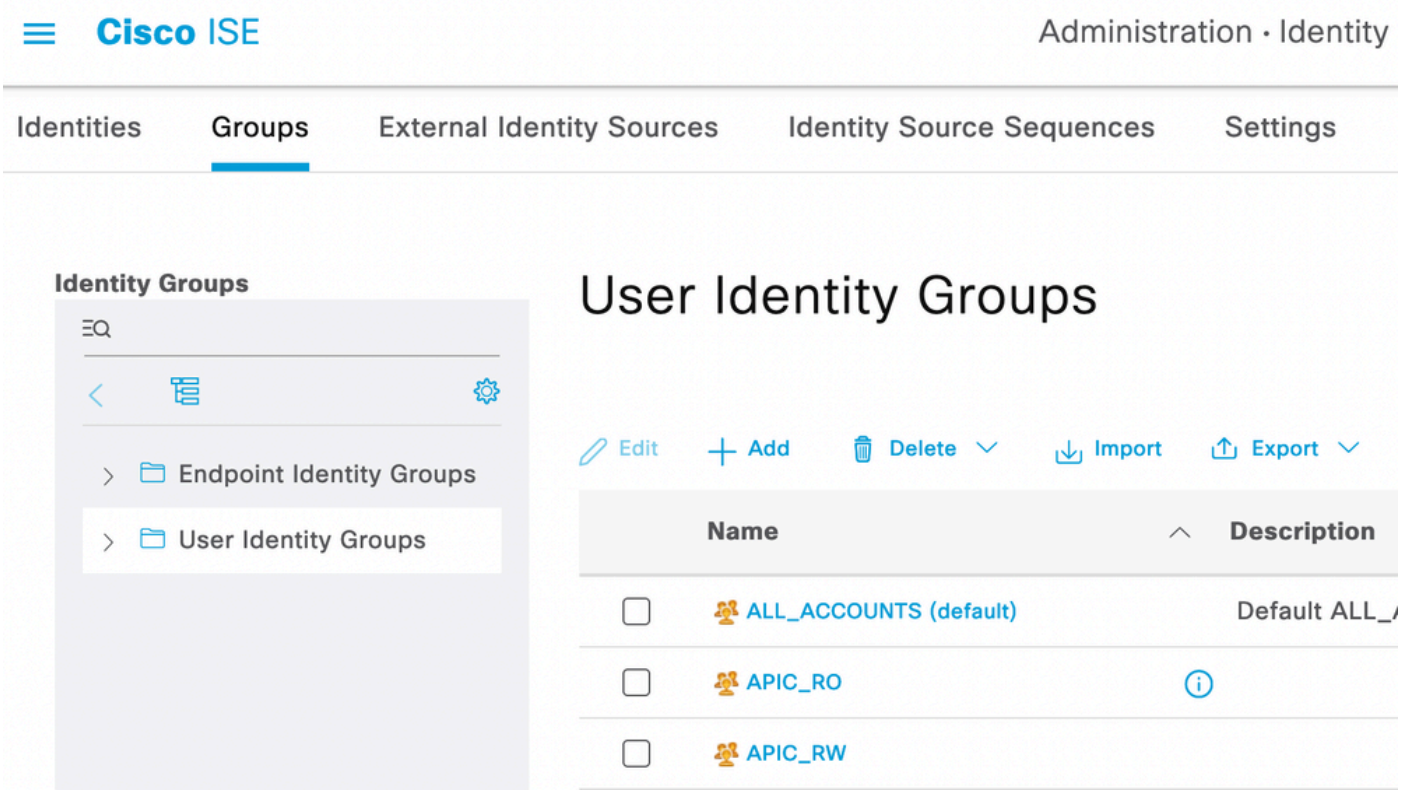
步驟3.使用此連結上的說明將ISE與Active Directory整合；

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html。



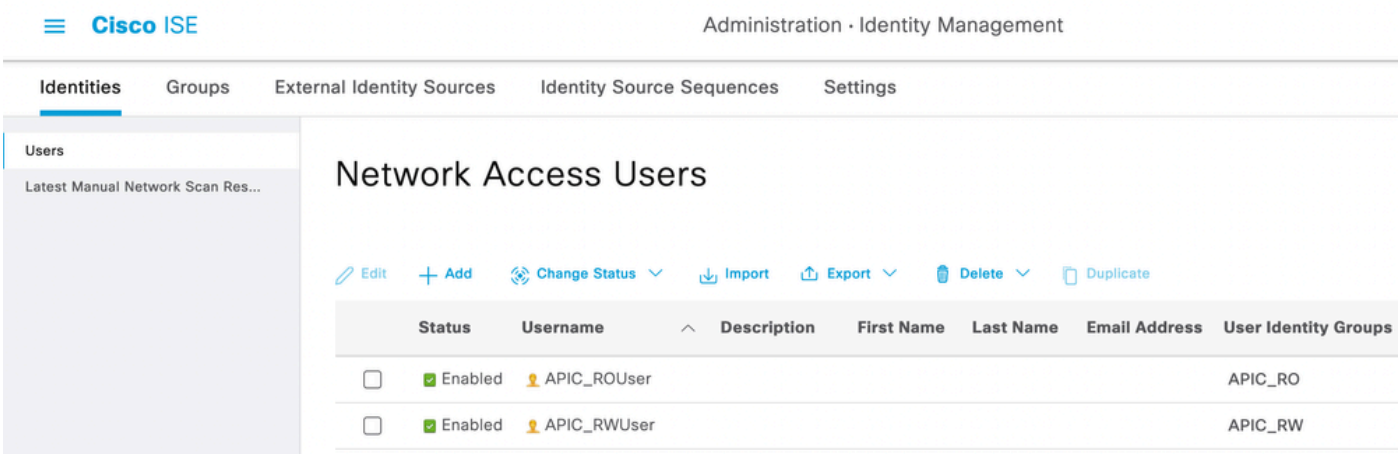
附註：本文檔將內部使用者和AD管理員組都作為身份源，但是，將使用內部使用者的身份源執行測試。AD組的結果相同。

步驟4.（可選）導覽至☰ >Administration > Identity Management > Groups。選擇User Identity Groups 並按一下 Add。為只讀管理員用戶和管理員用戶建立一個組組。

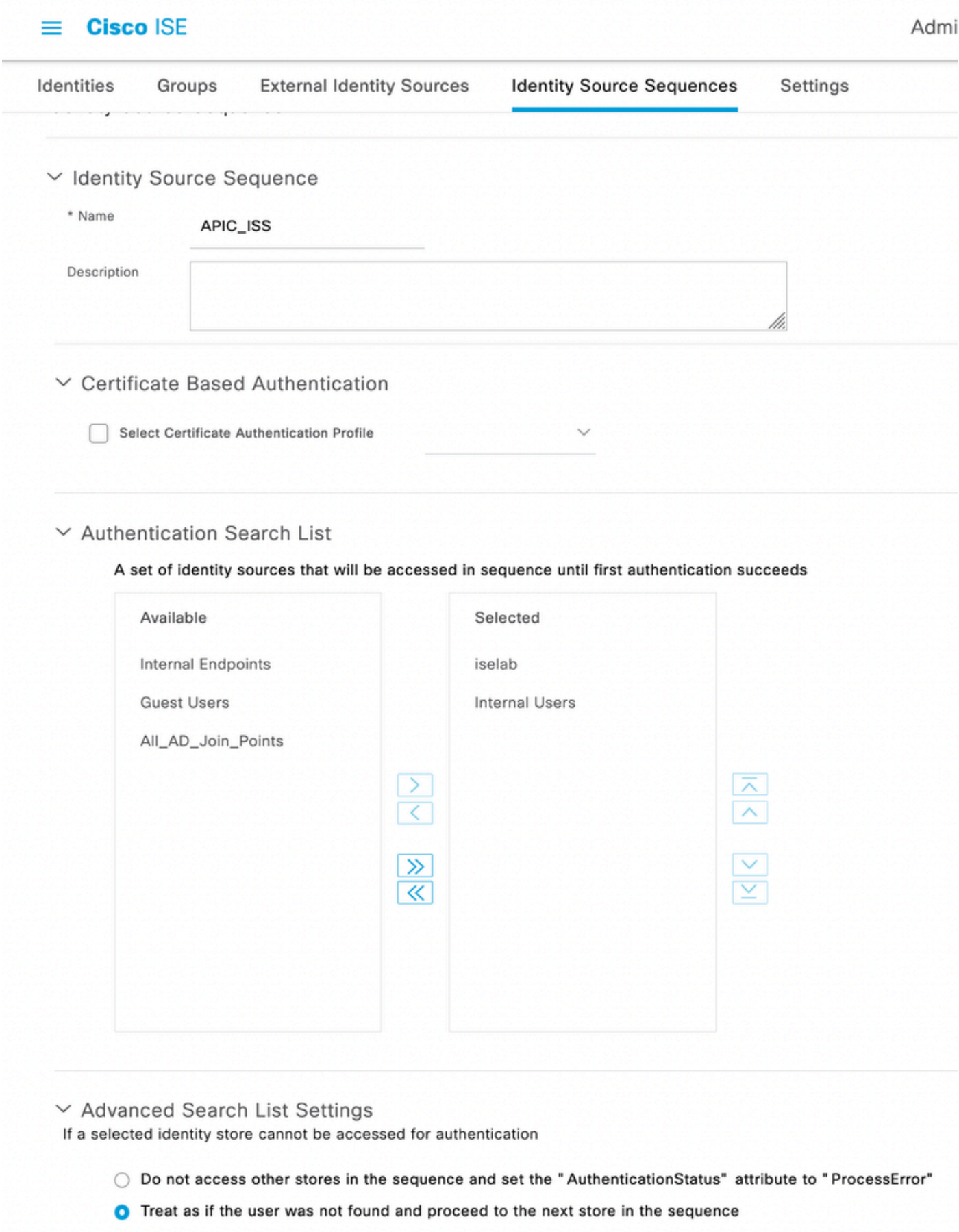


身份組

步驟5.（可選）導覽至☰ > Administration > Identity Management > Identity. Click Add並建立一個使Read Only Admin用者和Admin使用者。將每個使用者分配到步驟4中建立的每個組。



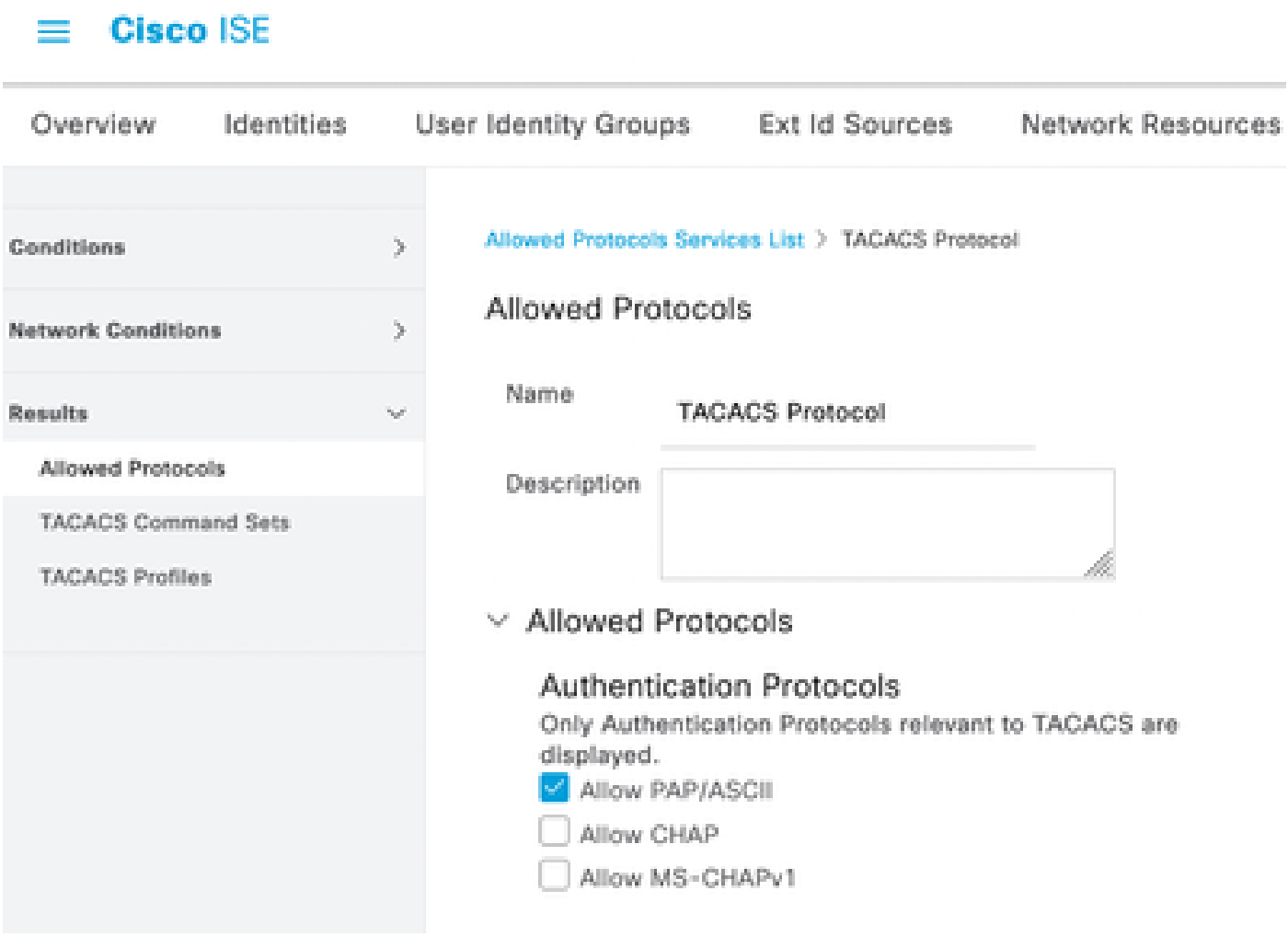
步驟6.導覽至☰ >Administration > Identity Management > Identity Source Sequence。從清單中選擇Add，定義名稱，AD Join Points然後選擇Internal Users和Identity Source。在Treat as if the user was not found and proceed to the next store in the sequence下選擇Advanced Search List Settings，然後按一下Save。



身份源序列

☰ 7.導航至>**Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols**.選擇Add，定義名稱

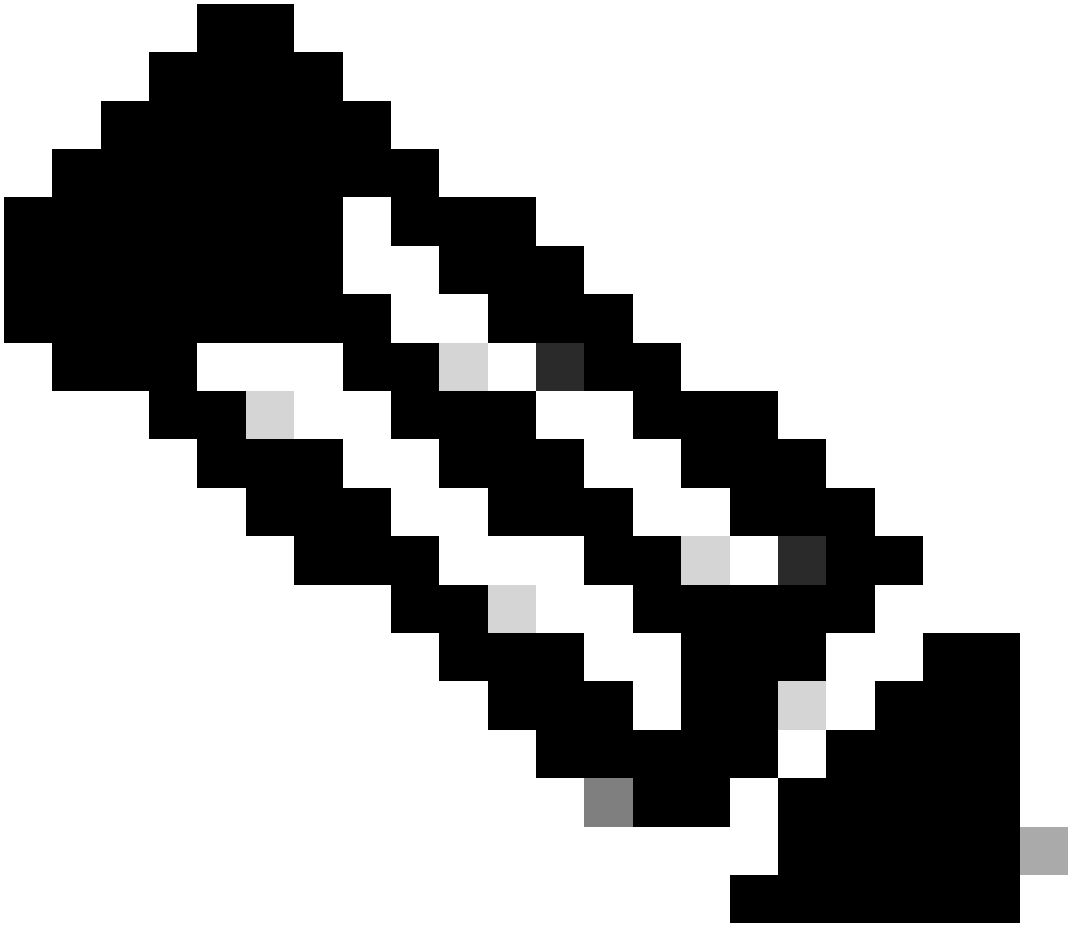
，並取消選中Allow CHAP和Allow MS-CHAPv1 from Authentication protocol清單。選擇Save。



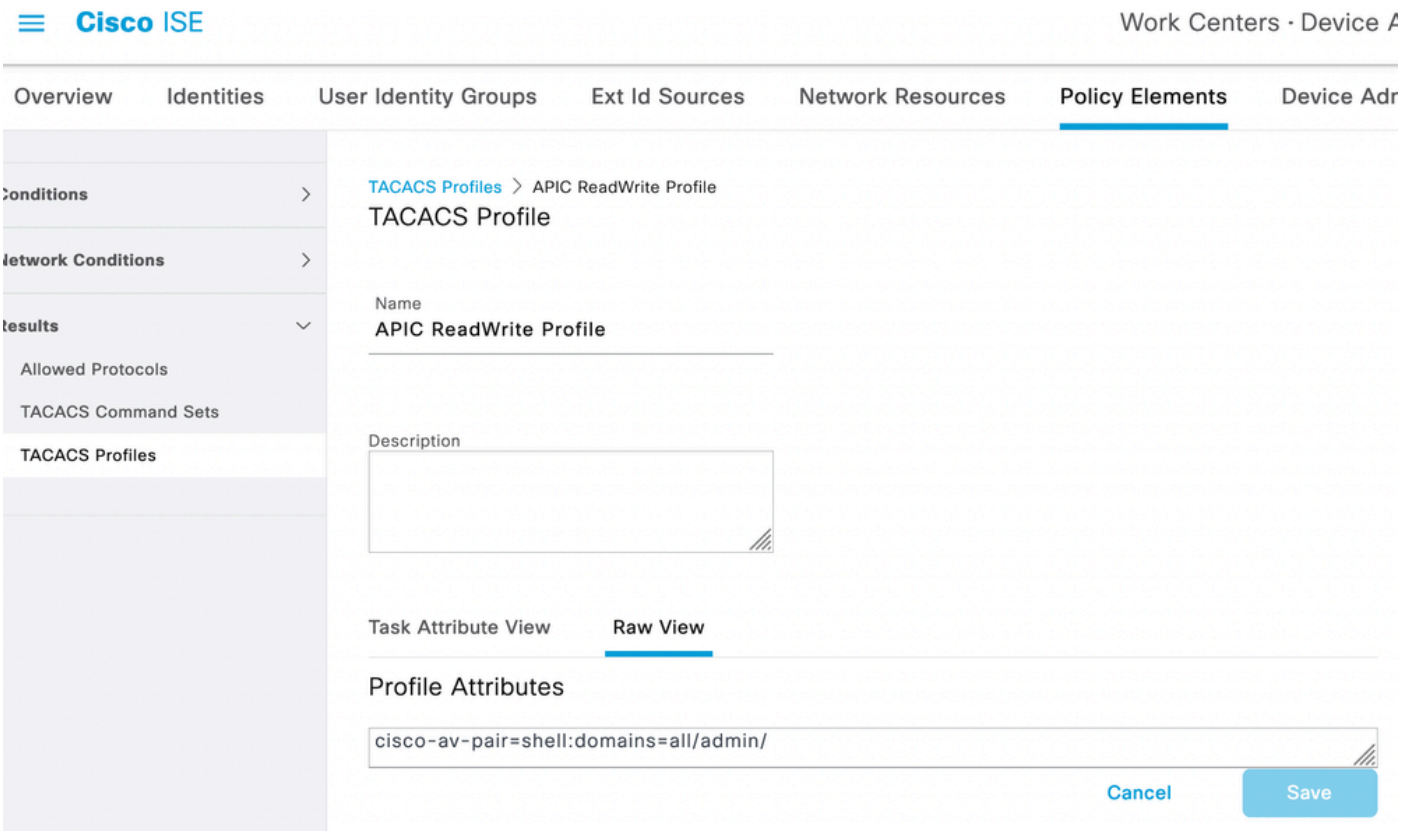
TACACS允許通訊協定

8.導覽至☰ >Work Centers > Device Administration > Policy Elements > Results > TACACS Profile。 按一下add並根據下方的清單上的屬性建立兩個配置檔案Raw View。 按一下Save。

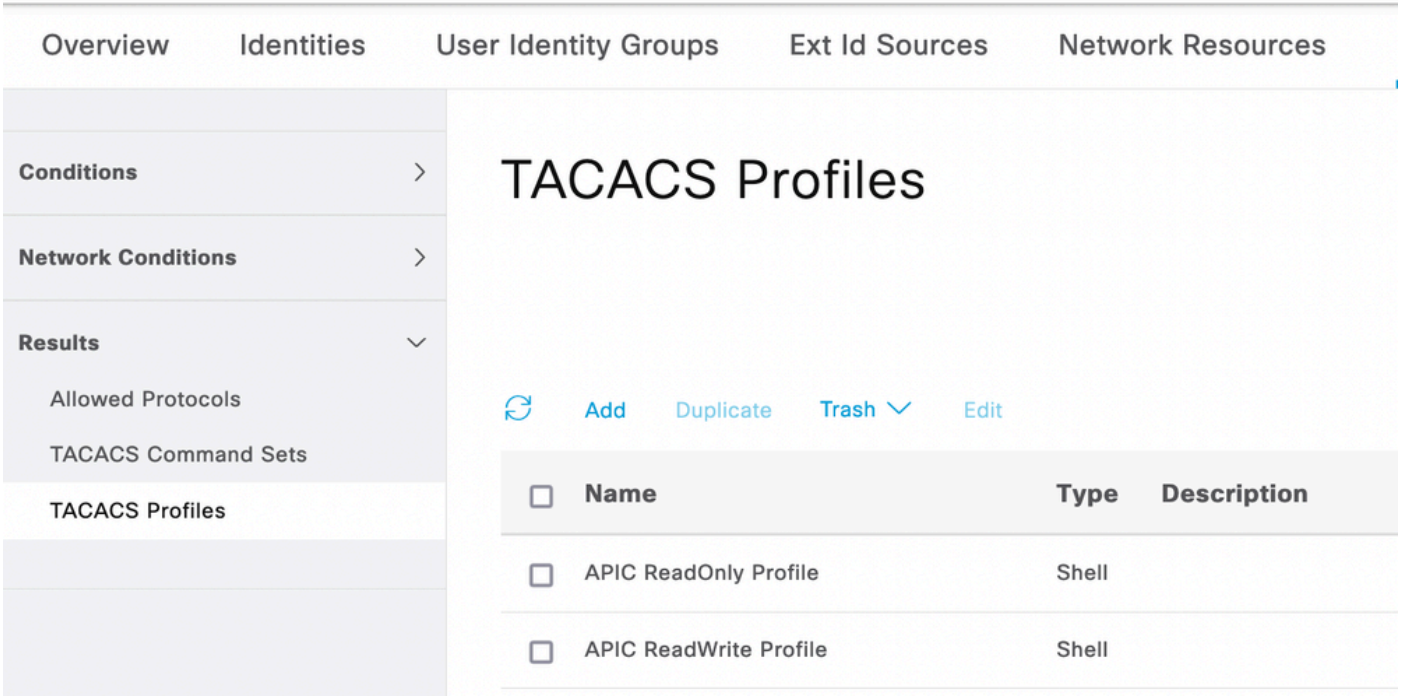
- 管理員使用者： cisco-av-pair=shell:domains=all/admin/
- 只讀管理員使用者： cisco-av-pair=shell:domains=all//read-all



附註：如果出現空格或其他字元，授權階段將失敗。

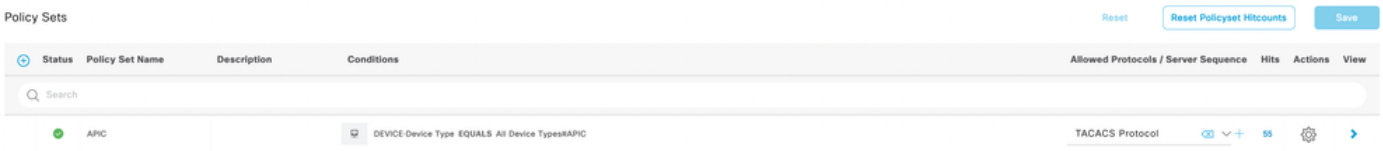


TACACS設定檔



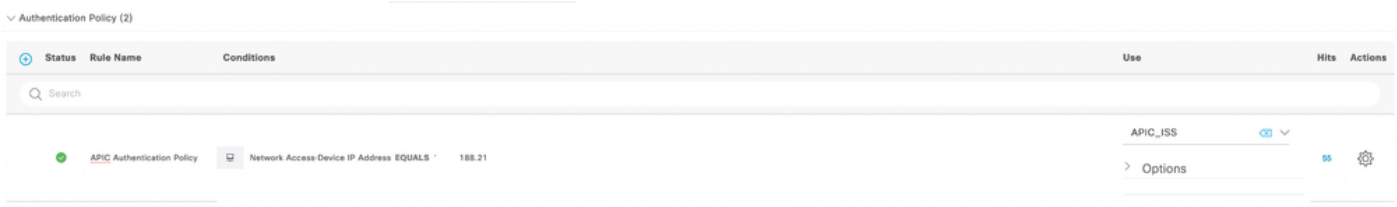
TACACS管理員和只讀管理員配置檔案

步驟9.導覽至☰ >Work Centers > Device Administration > Device Admin Policy Set 。建立新策略集，定義名稱，並選擇在步驟1中建立的裝置類APIC型。選擇在步驟7中建立TACACS Protocol的。作為允許的協定，然後單擊Save。

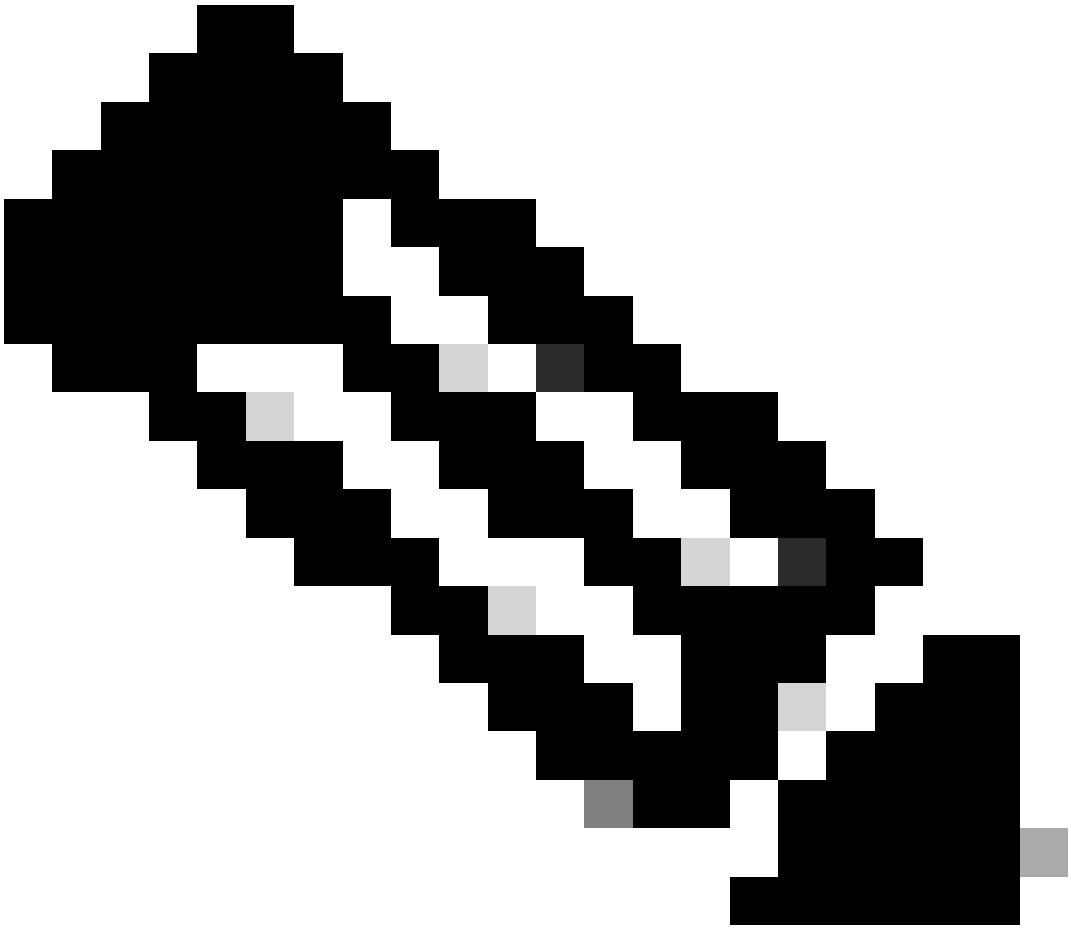


TACACS策略集

步驟10.在new下Policy Set，按一下右箭頭>，建立身份驗證策略。定義名稱並選擇裝置IP地址作為條件。然後選擇在步驟6中建立的身份源序列。

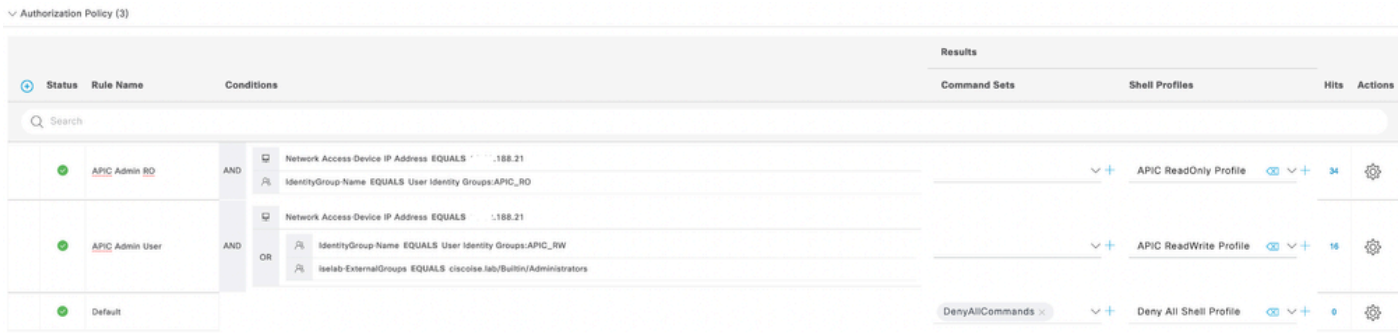


身份驗證策略



附註：位置或其他屬性可用作身份驗證條件。

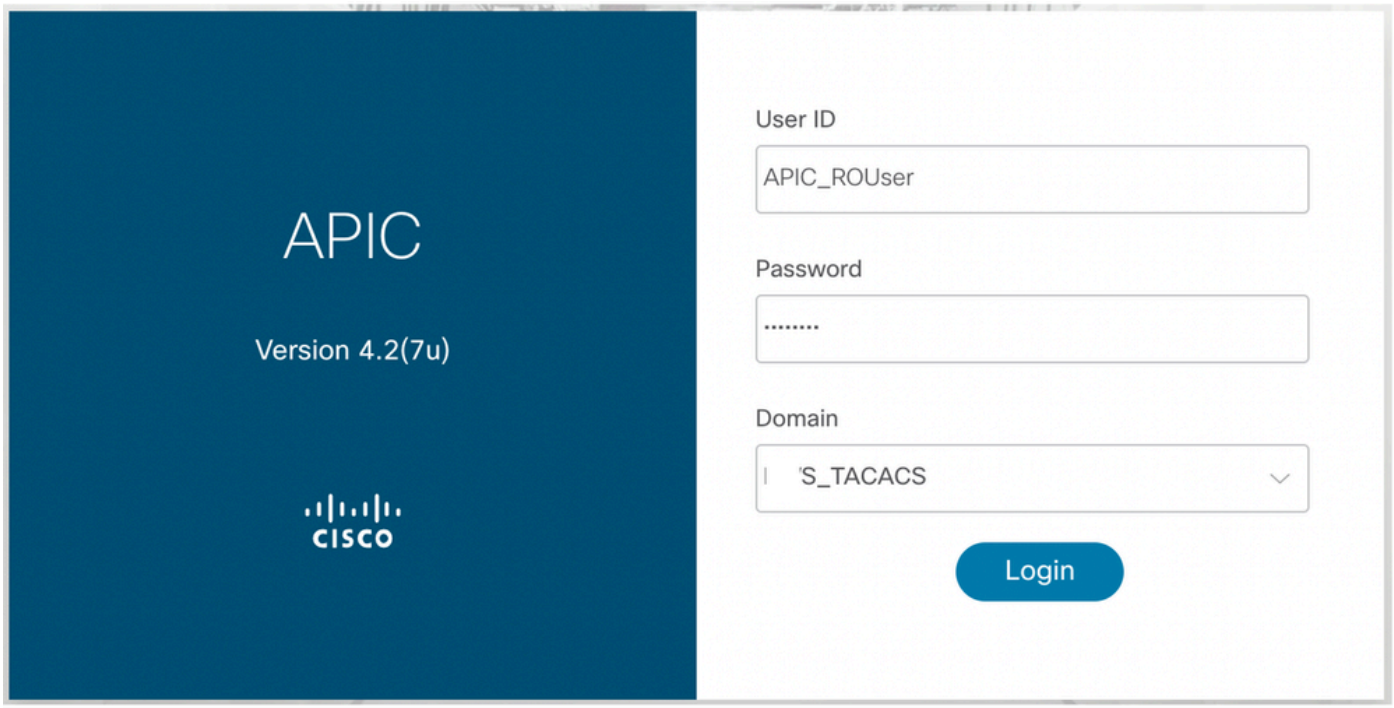
步驟11.為每個管理員使用者型別建立授權配置檔案，定義名稱，並選擇內部使用者和/或AD使用者組作為條件。可以使用其他條件，如APIC。在每個授權策略上選擇適當的外殼配置檔案，然後按一下Save。



TACACS授權配置檔案

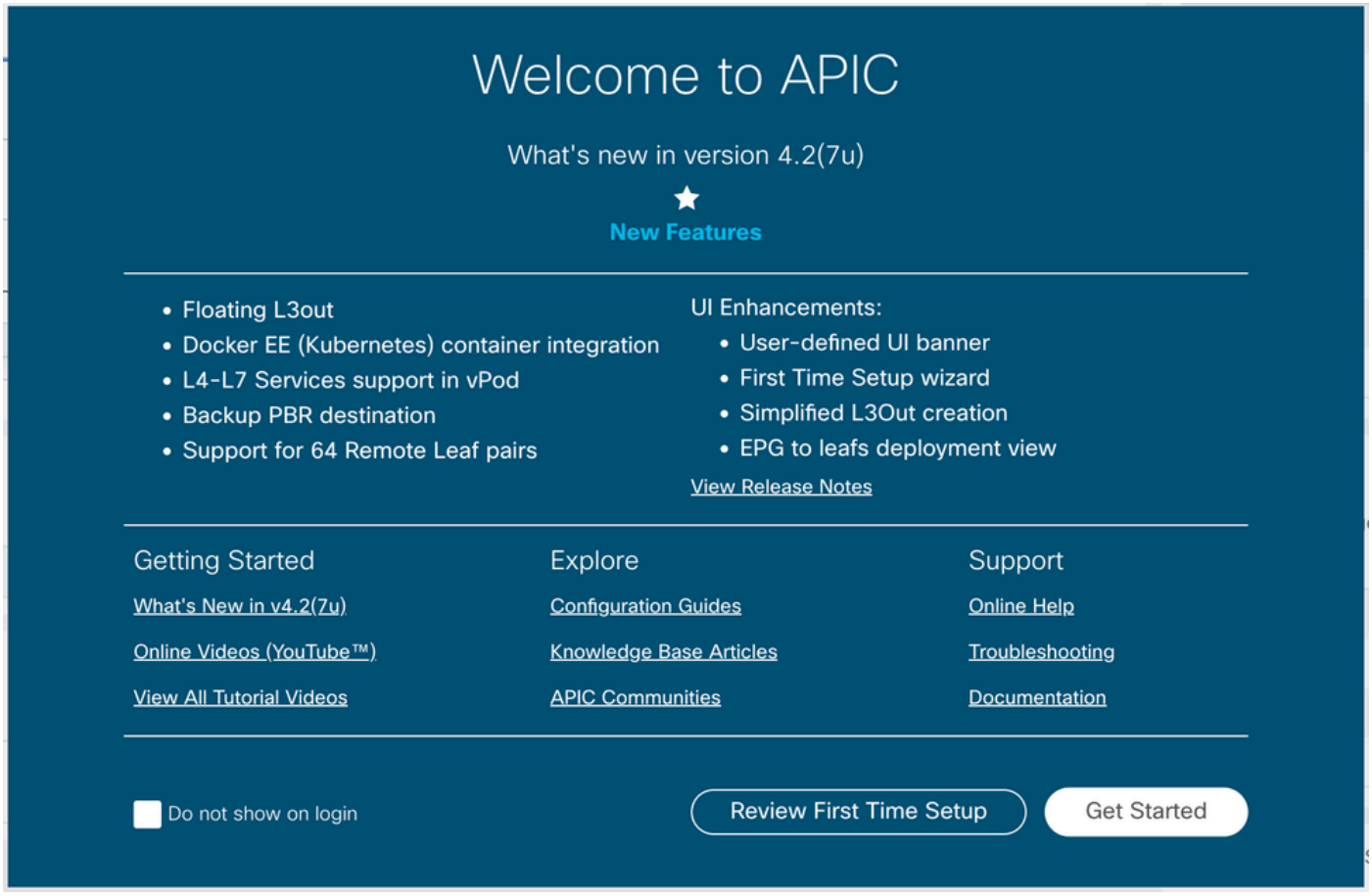
驗證

步驟1.使用使用者管理員憑據登入APIC UI。從清單中選擇TACACS選項。



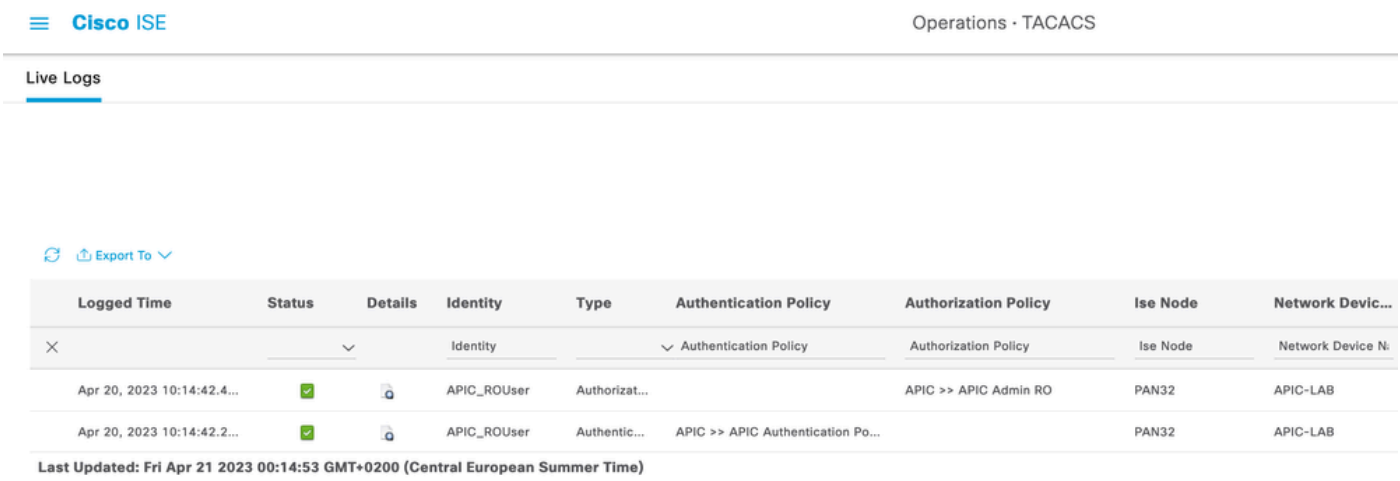
APIC登入

步驟2.檢驗APIC UI上的訪問情況，並驗證TACACS Live日誌上應用了正確的策略。



APIC歡迎資訊

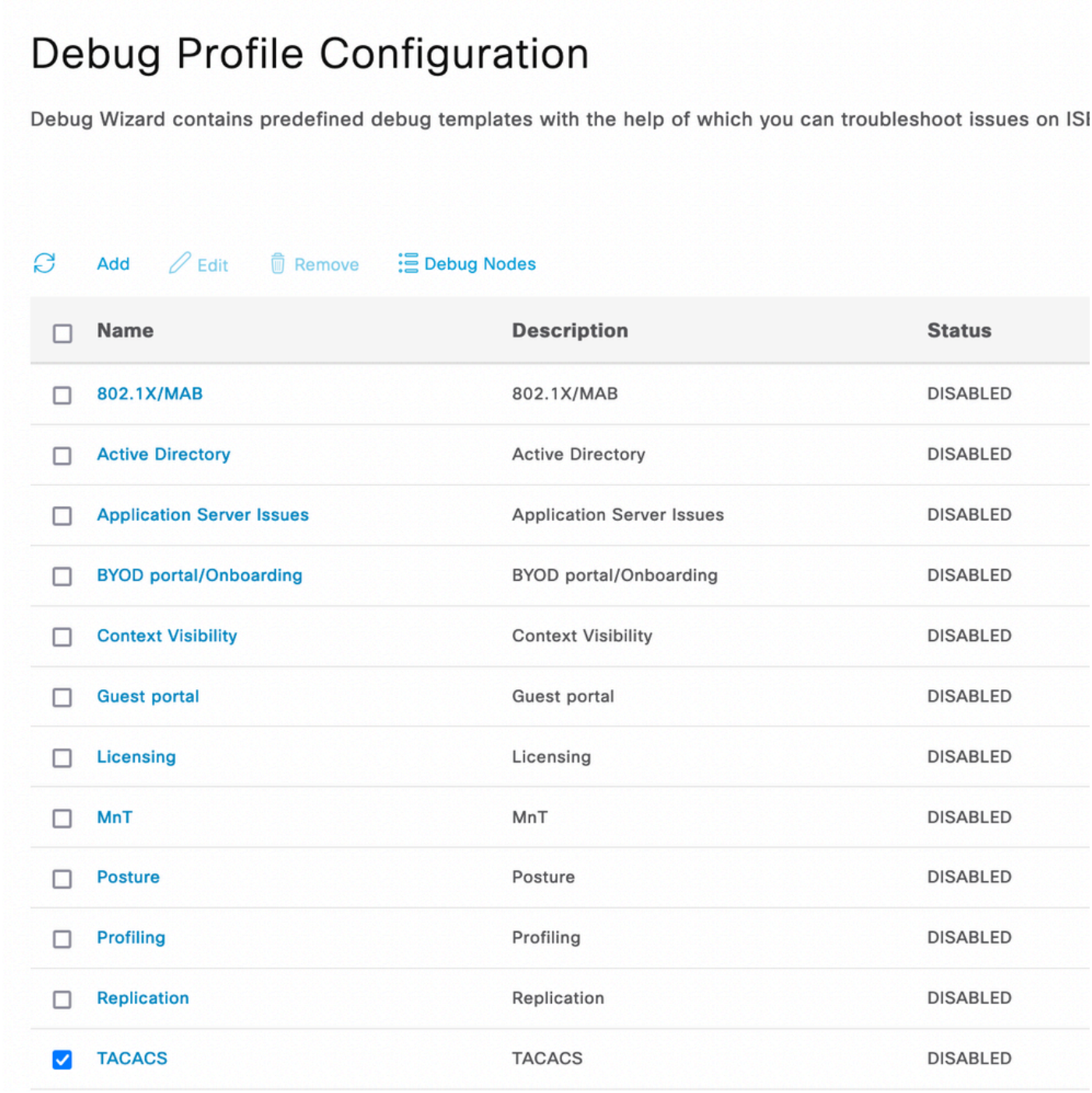
對只讀管理員使用者重複步驟1和2。



TACACS+即時日誌

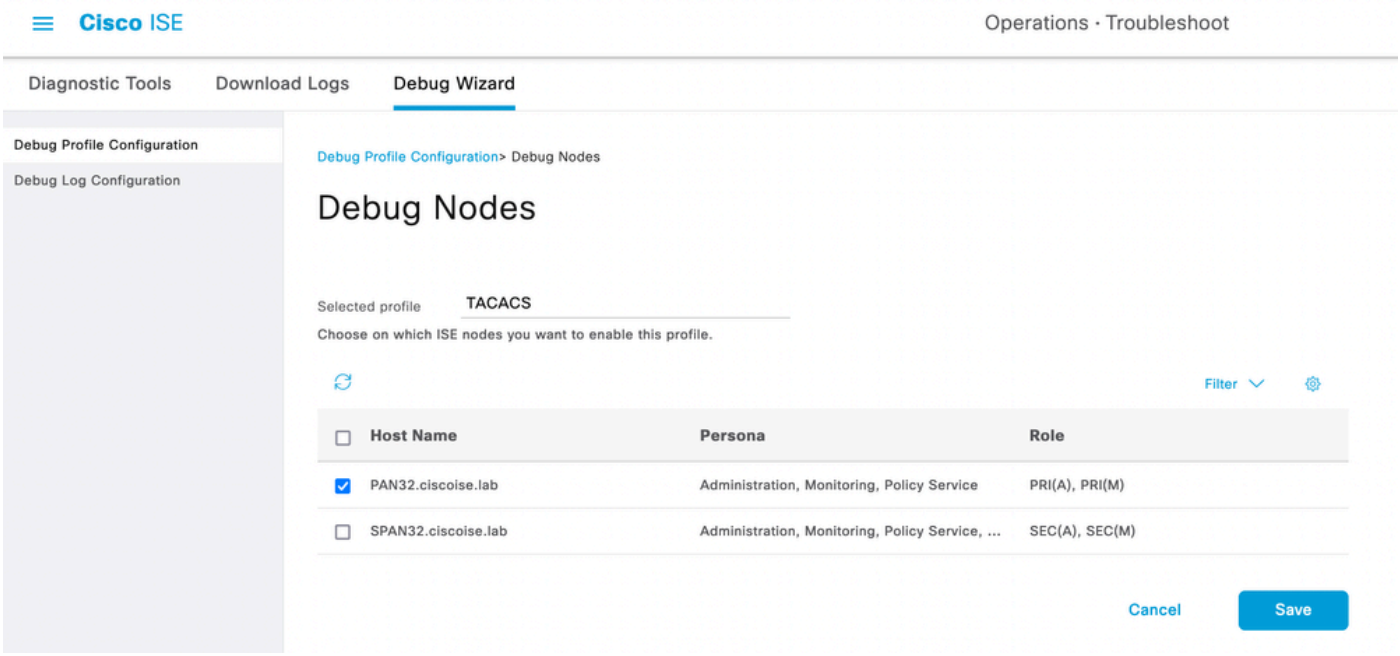
疑難排解

步驟1。導覽至☰ >Operations > Troubleshoot > Debug Wizard。選擇TACACS並按一下 Debug Nodes。



調試配置檔案配置

步驟2.選擇接收流量的節點，然後按一下Save。



調試節點選擇

步驟3.執行新測試並下載下的日誌，Operations > Troubleshoot > Download logs 如下所示：

```
AcsLogs,2023-04-20 22:17:16,866,DEBUG,0x7f93cabc7700,cntx=0004699242,sesn=PAN32/469596415/70,CPMSession
```

如果調試不顯示身份驗證和授權資訊，請驗證以下情況：

1. 在ISE節點上啟用裝置管理服務。
2. 已將正確的ISE IP地址新增到APIC配置。
3. 如果中間有防火牆，請驗證是否允許埠49(TACACS)。

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）。