

# 為安全防火牆機箱管理器(FCM)配置ISE RADIUS身份驗證

## 目錄

---

---

## 簡介

本文檔介紹如何為使用ISE的安全防火牆機箱管理器配置RADIUS授權/身份驗證訪問的過程。

## 必要條件

### 需求

思科建議瞭解以下主題：

- 安全防火牆機箱管理員(FCM)
- 思科身份辨識服務引擎(ISE)
- RADIUS 驗證

### 採用元件

- Cisco Firepower 4110安全裝置FXOS v2.12
- 思科身份服務引擎(ISE) v3.2修補4

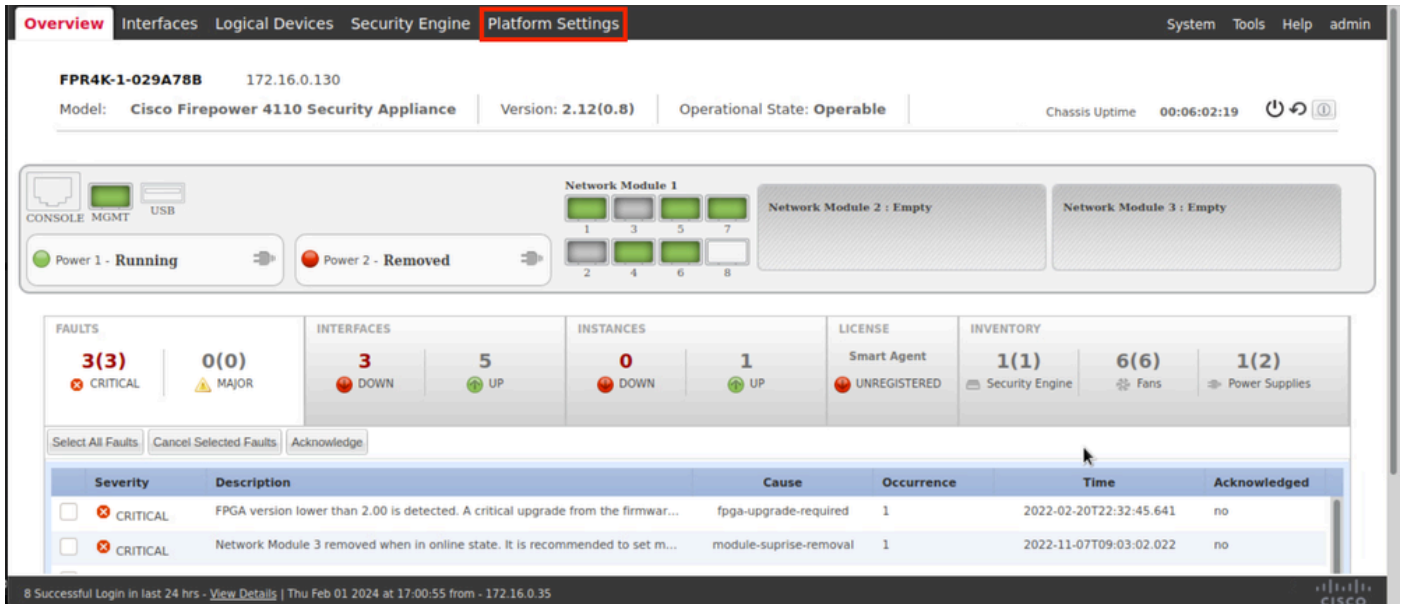
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 設定

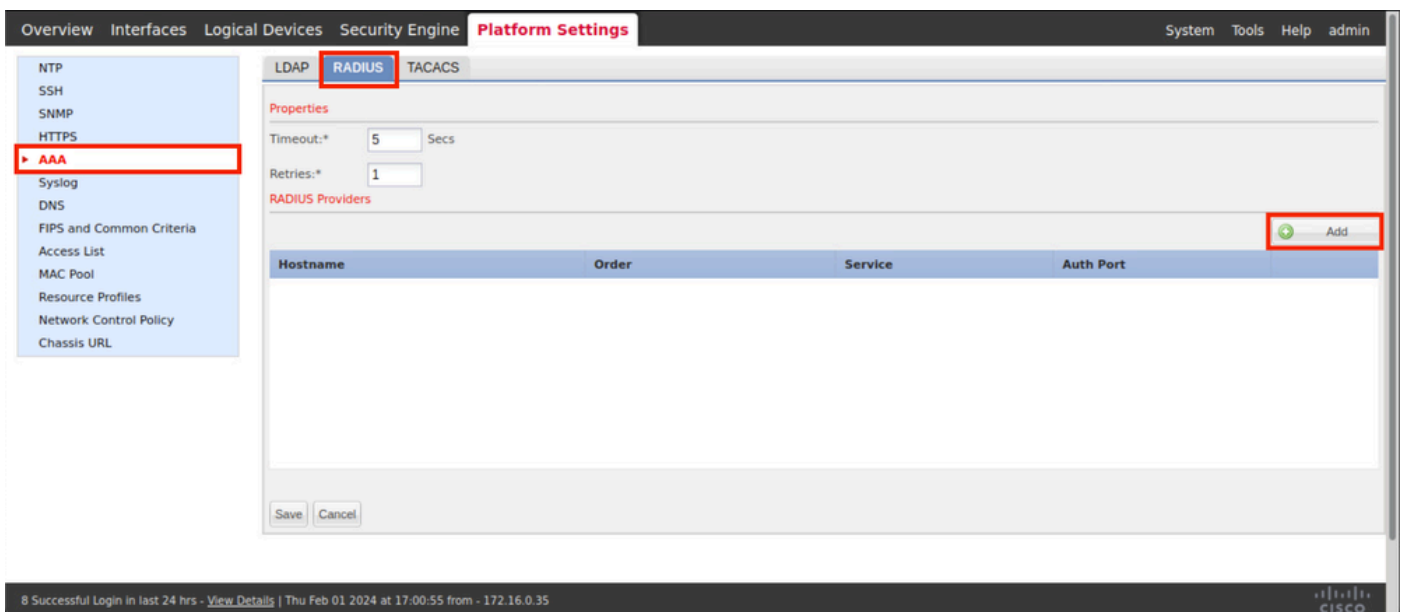
### 組態

#### 安全防火牆機箱管理員

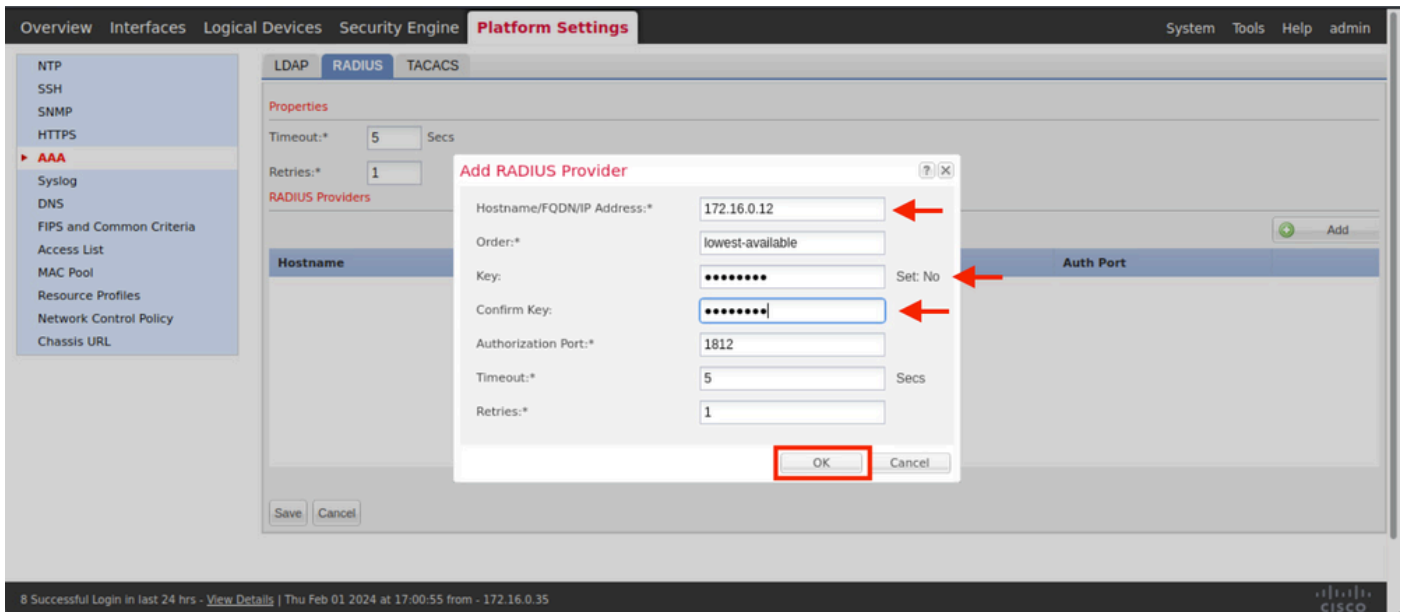
- 步驟 1.登入到Firepower機箱管理器GUI。
- 步驟 2.導航至平台設定



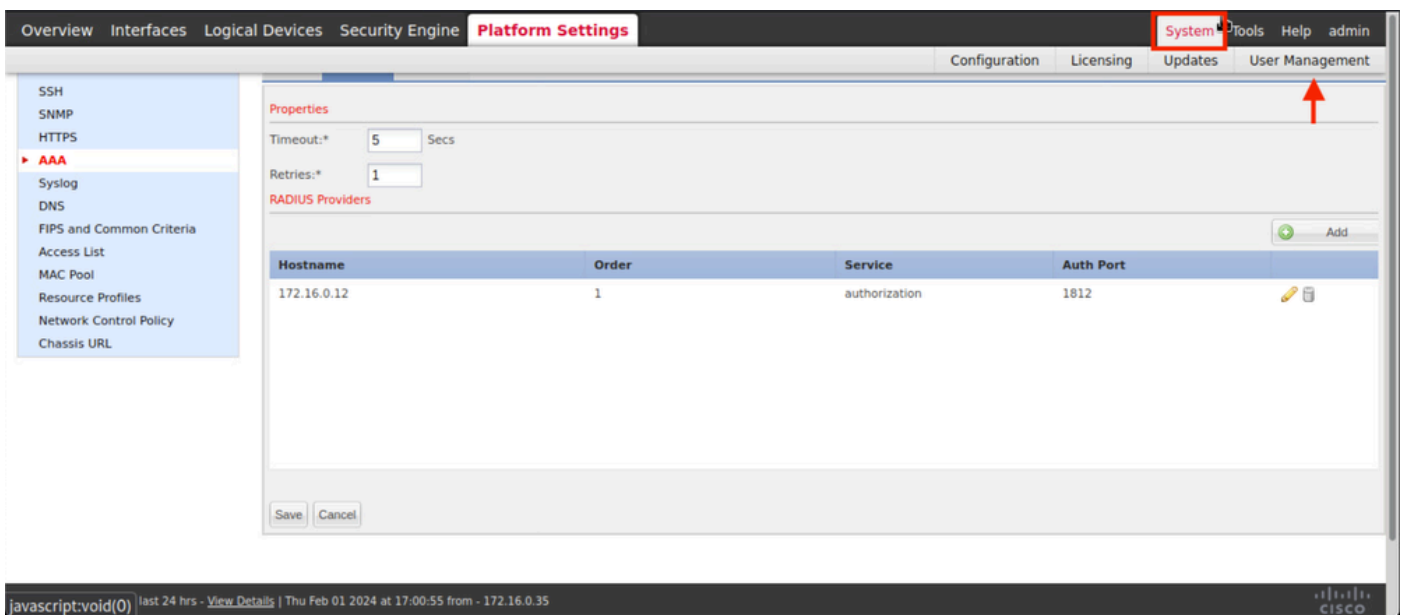
步驟 3. 從左側選單中按一下over AAA。 選擇Radius並增加新的RADIUS提供程式。



步驟 4. 使用Radius提供者要求的資訊填入提示選單。按一下「OK」(確定)。



步驟 5. 導航到系統>使用者管理



步驟 6. 點選Settings頁籤並將下拉選單中的Default Authentication設定為Radius，然後向下滾動並儲存配置。


Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help admin

Configuration Licensing Updates **User Management**

Local Users **Settings**

**Default Authentication**

Local  \*Local is fallback authentication method

Local  
RADIUS   
LDAP  
TACACS  
None

Console Authentication

**Remote User Settings**

Remote User Role Policy

**Local User Settings**

Password Strength Check  Enable

History Count  (0-disabled,1-15)

Change Interval   (1-730 hours)

Change Count  (1-10)

No Change Interval   (1-730 hours)

Days until Password Expiration  (0-never,1-9999 days)

Password Expiration Warning Period  (0-9999 days)

Expiration Grace Period  (0-9999 days)

Password Reuse Interval  (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet)  (0-never,3600 seconds)

8 Successful Login in last 24 hrs - [View Details](#) | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

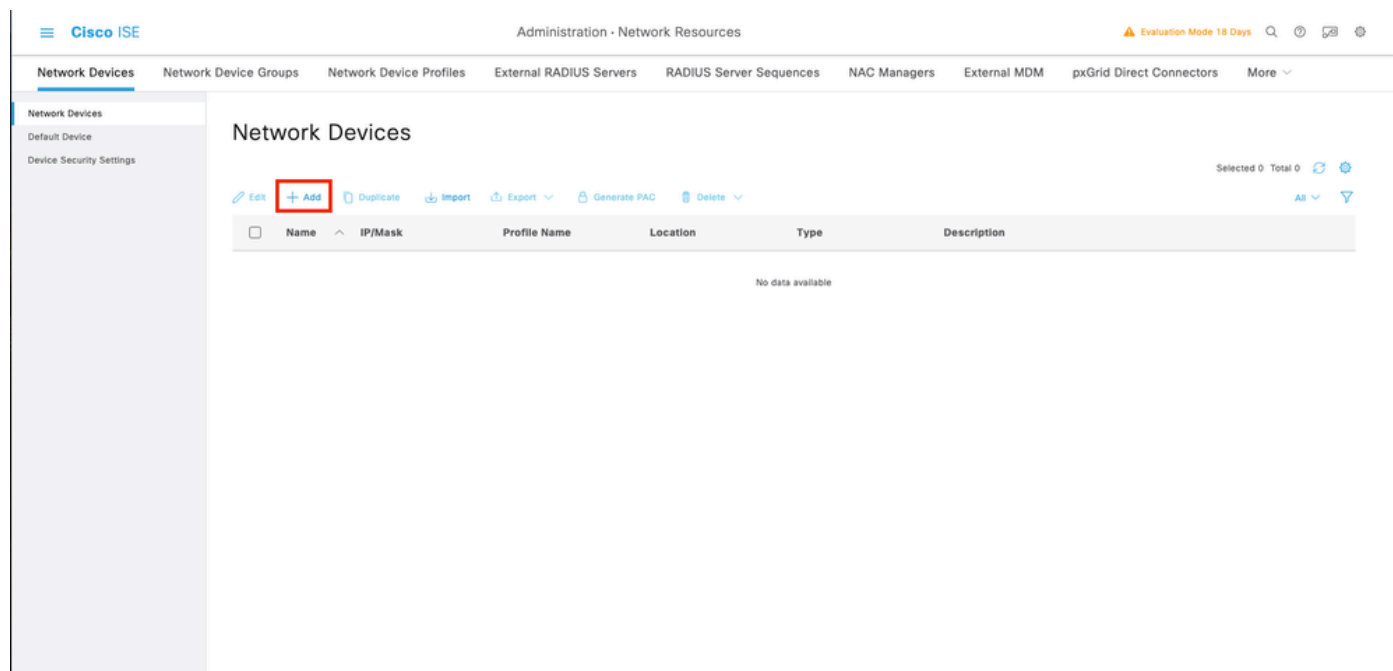
CISCO

注意：此時已完成FCM組態。

## 身分辨識服務引擎

步驟 1. 新增網路裝置。

導航到位於左上角的漢堡圖示 ≡ > Administration > Network Resources > Network Devices > +Add。

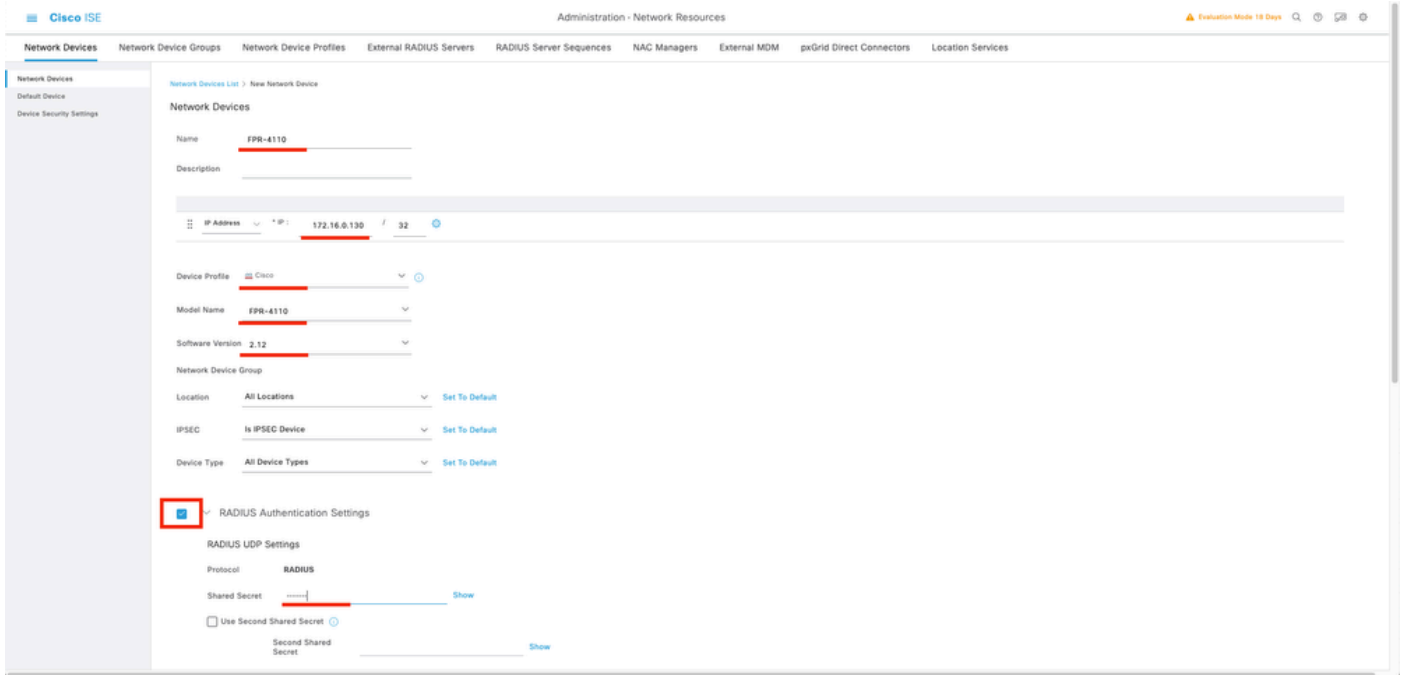


步驟 2. 填寫有關新網路裝置資訊請求的引數。

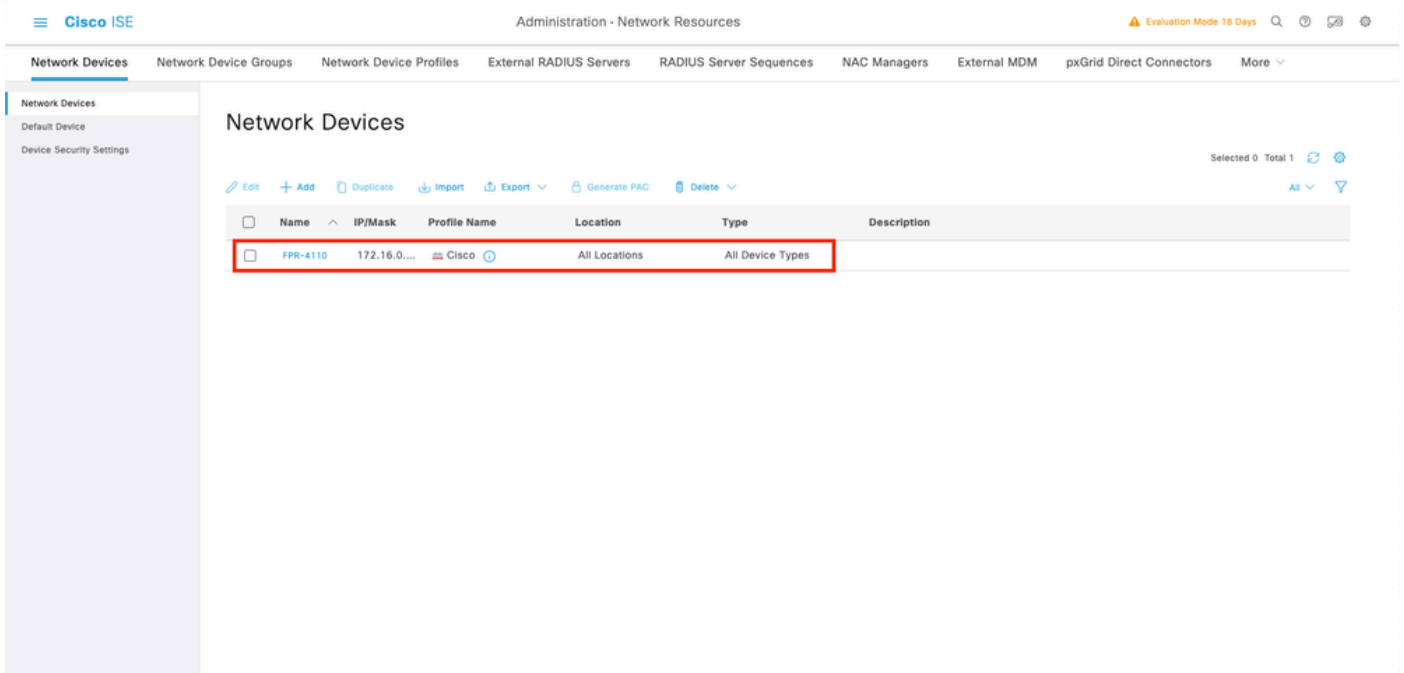
2.1 選中 RADIUS 覈取方塊

2.2 配置與 FCM Radius 配置相同的共用金鑰。

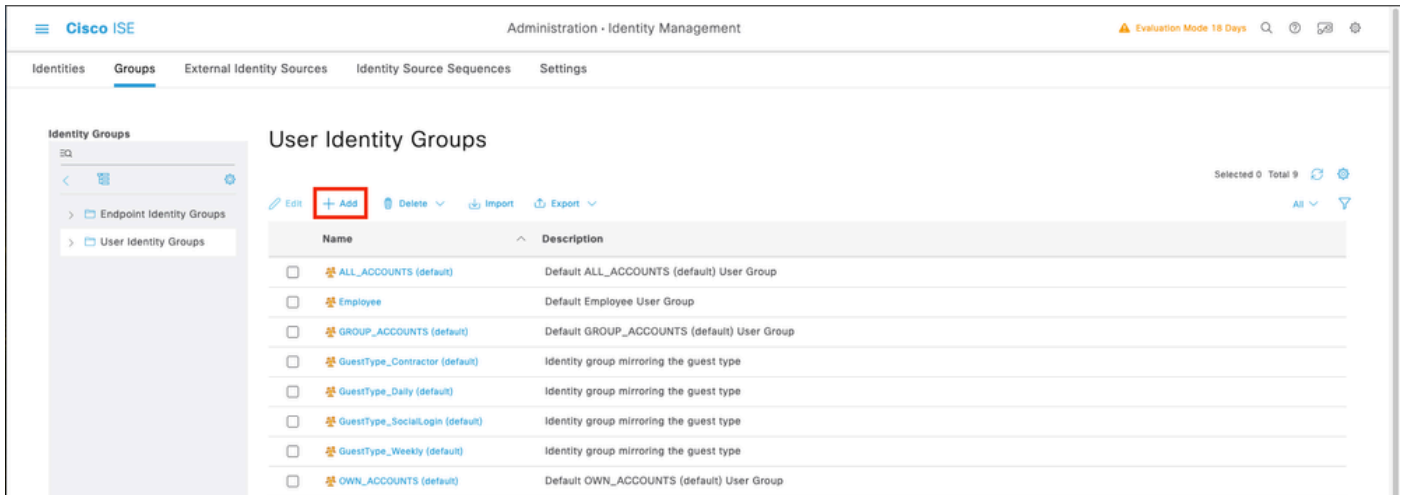
2.1 向下滾動並按一下「Submit (提交)」。



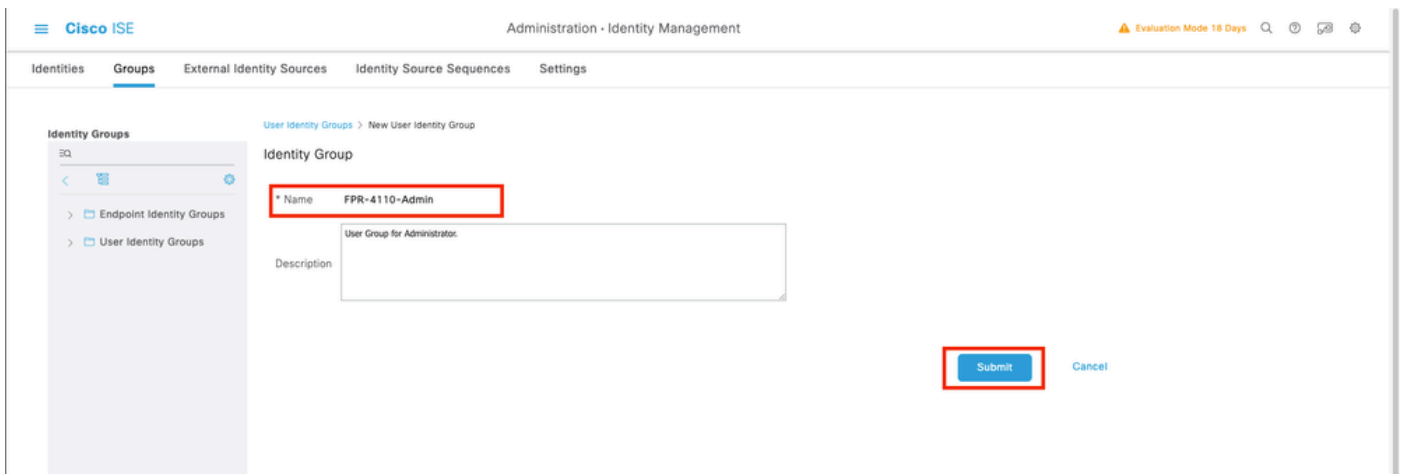
步驟 3. 驗證新裝置是否顯示在「網路裝置」下。



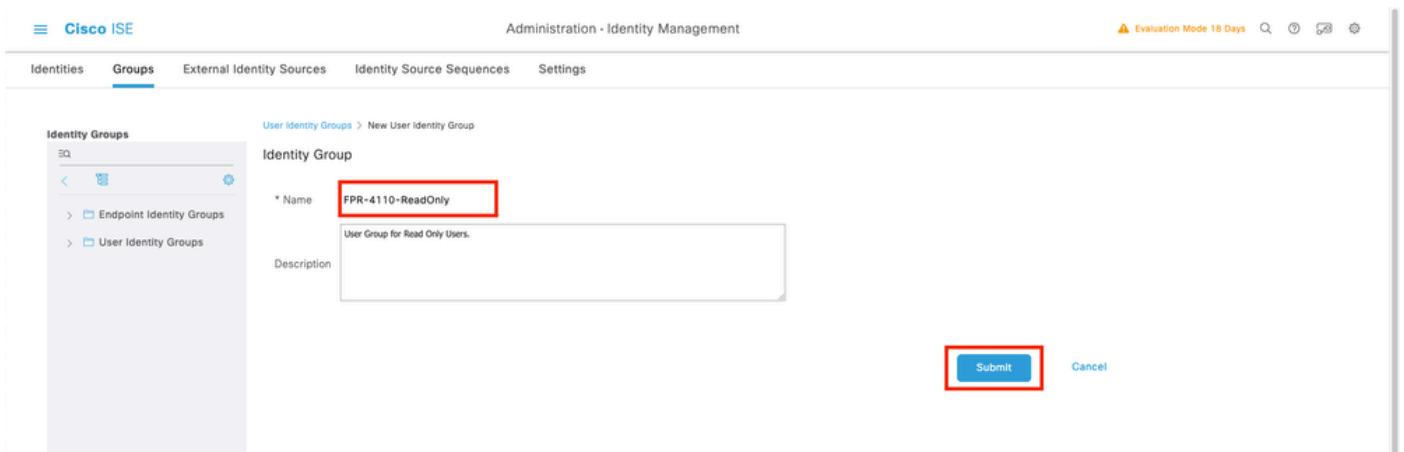
步驟 4. 建立所需的使用者身份組。導航到位於左上角的漢堡圖示 ≡ > Administration > Identity Management > Groups > User Identity Groups > + 增加



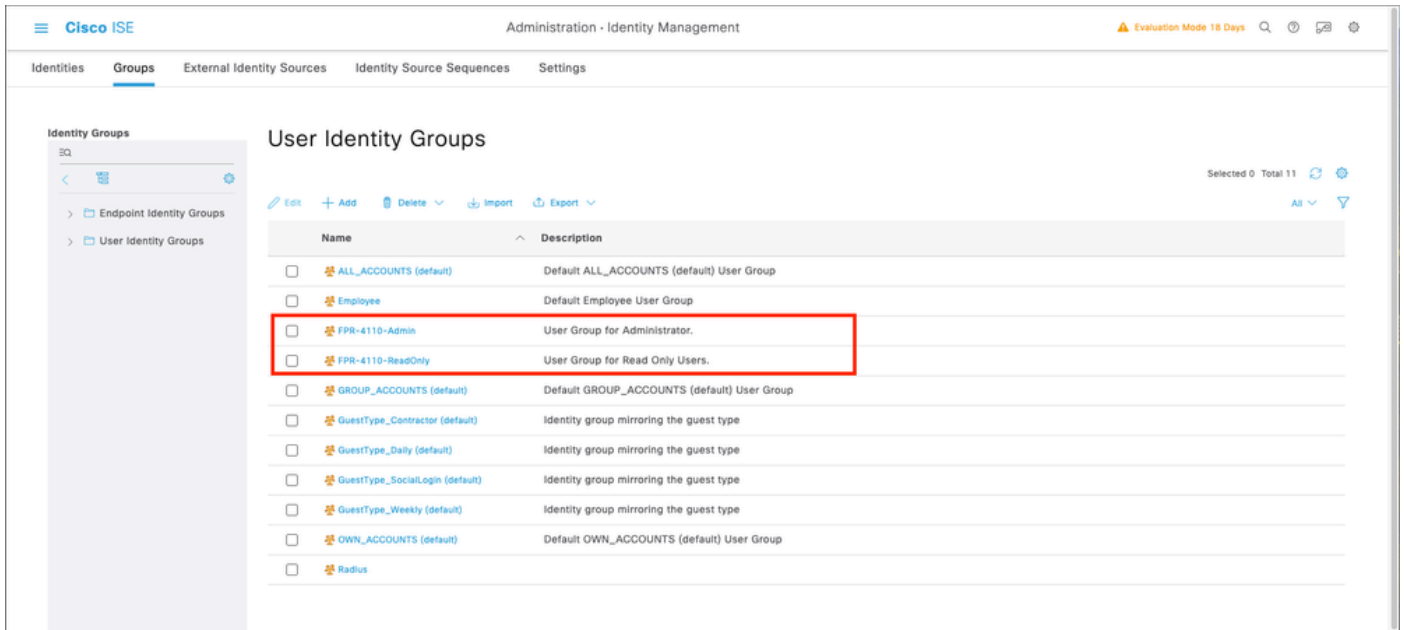
步驟 5. 設定管理員使用者身份組的名稱，然後點選提交以儲存配置。



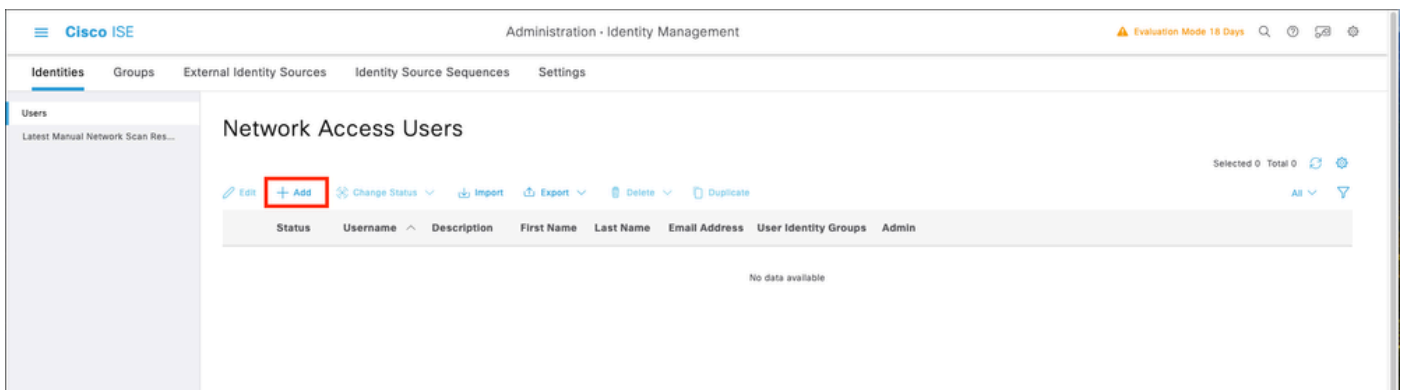
5.1 對唯讀使用者重複相同的程式。



步驟 6. 驗證使用者身份組下顯示的新使用者組。

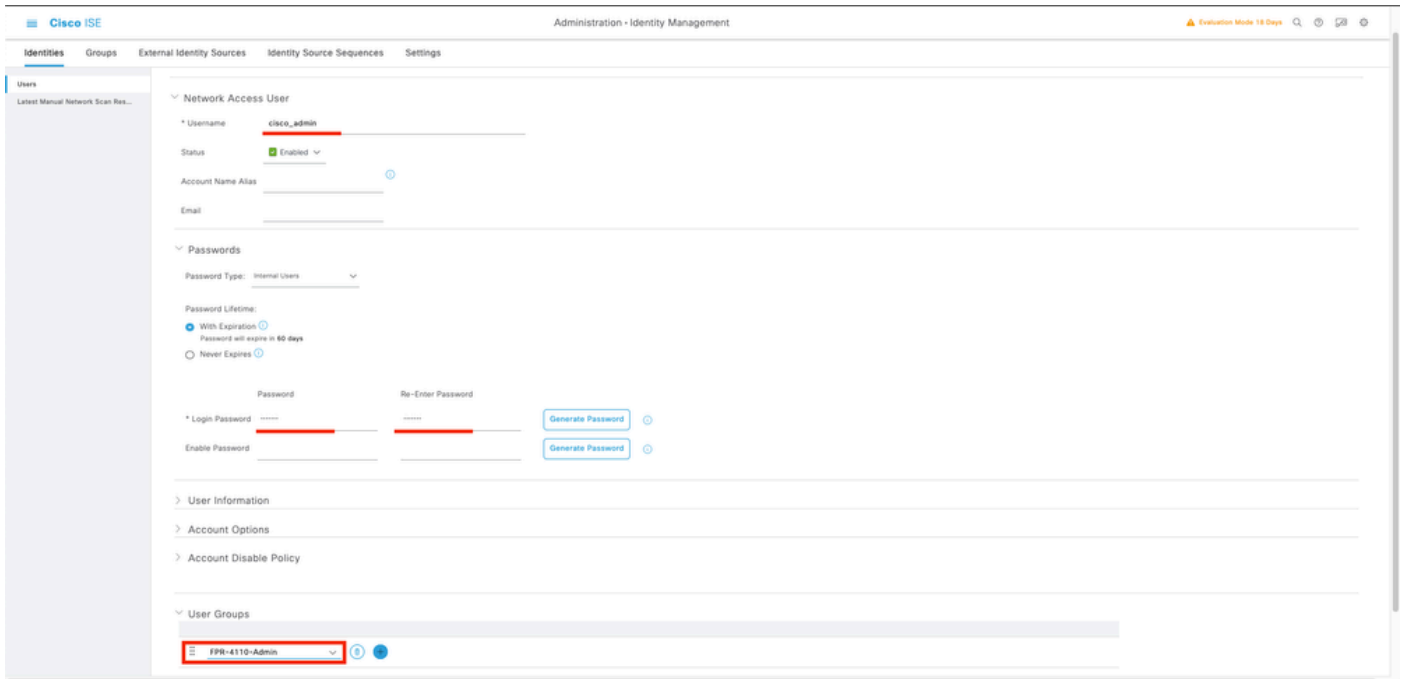


步驟 7. 建立本地使用者並將他們增加到其對應組。 導航到漢堡圖示=>管理>身份管理>身份> +增加。

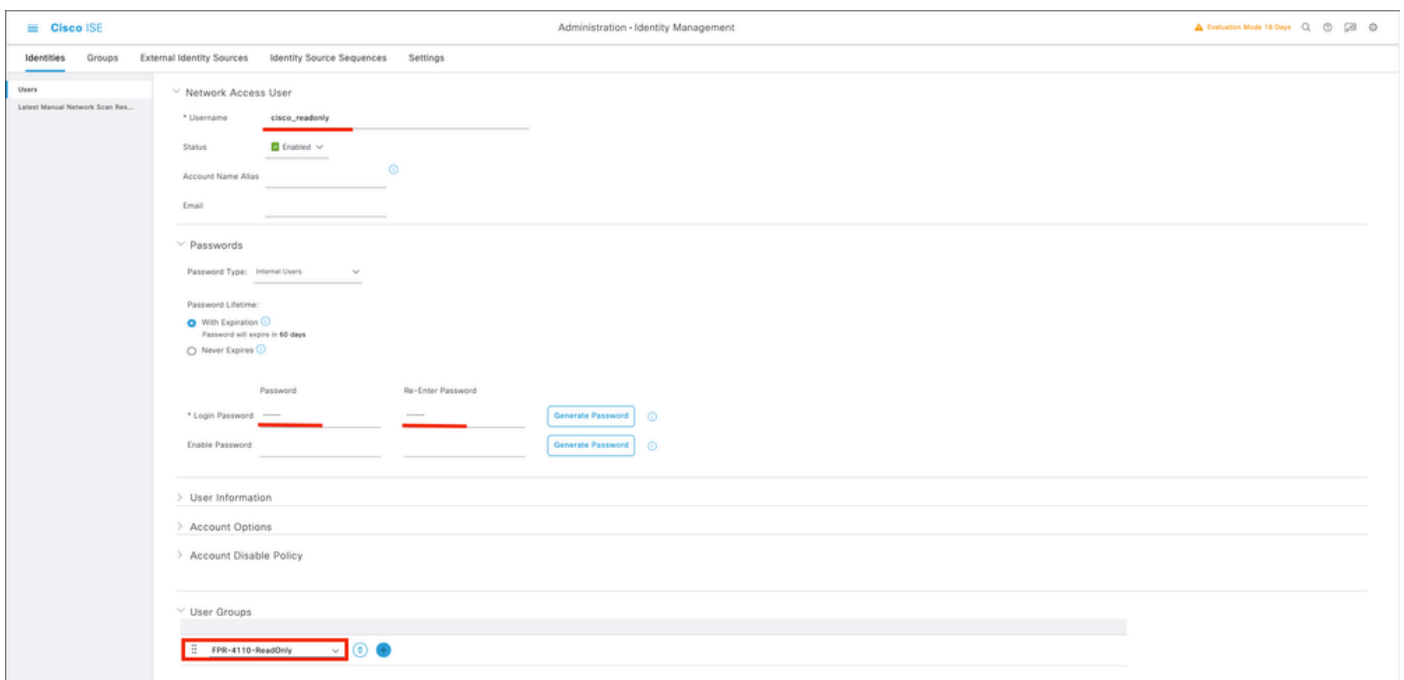


7.1增加具有管理員許可權的使用者。設定名稱和口令，分配給FPR-4110-Admin，然後向下滾動並按一下Submit以儲存更改。

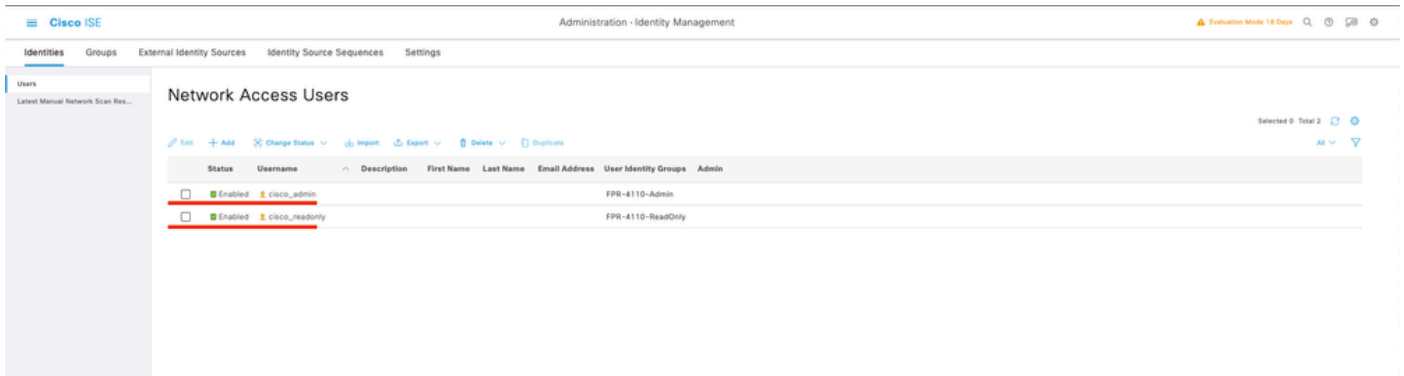




7.2 增加具有只讀許可權的使用者。設定名稱和口令，並將其分配給FPR-4110-ReadOnly，然後向下滾動並按一下Submit以儲存更改。



7.3 驗證使用者是否在網路訪問使用者下。



第8步：為管理員使用者建立授權配置檔案。

FXOS機箱包括以下使用者角色：

- 管理員-對整個系統的完整讀寫存取權。預設管理員帳戶預設分配此角色，且無法更改。
- 唯讀-對沒有修改系統狀態之許可權的系統組態唯讀存取權。
- 操作-對NTP配置、智慧許可的Smart Call Home配置和系統日誌（包括系統日誌伺服器 and 故障）的讀寫訪問許可權。對系統的其餘部分具有讀取許可權。
- AAA -對使用者、角色和AAA配置的讀寫訪問許可權。對系統其餘部分的讀取許可權

每個角色的屬性：

cisco-av-pair=shell : roles="admin"

cisco-av-pair=shell : roles="aaa"

cisco-av-pair=shell : roles="operations"

cisco-av-pair=shell : roles="read-only"

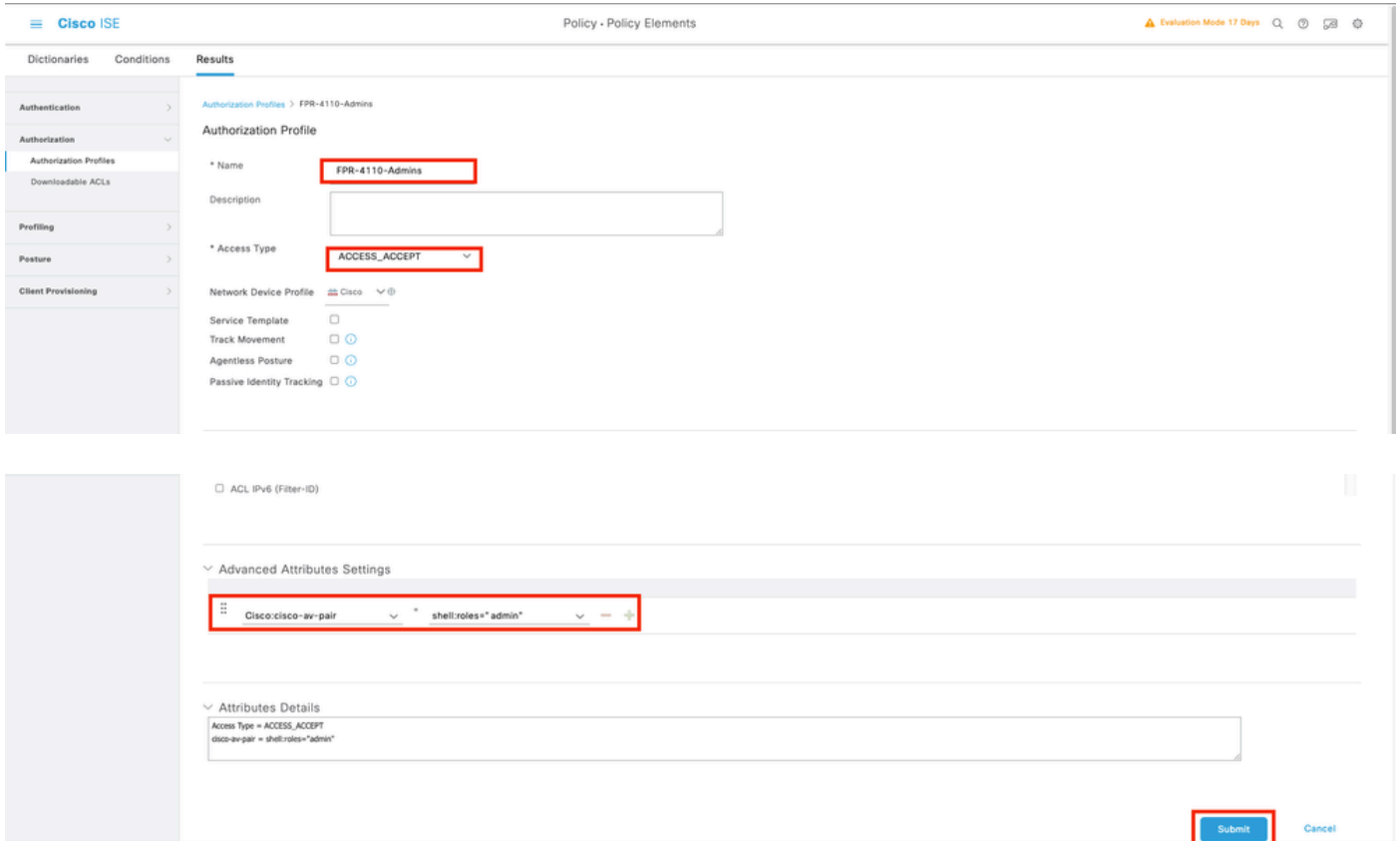


附註：本檔案僅定義管理屬性和唯讀屬性。

---

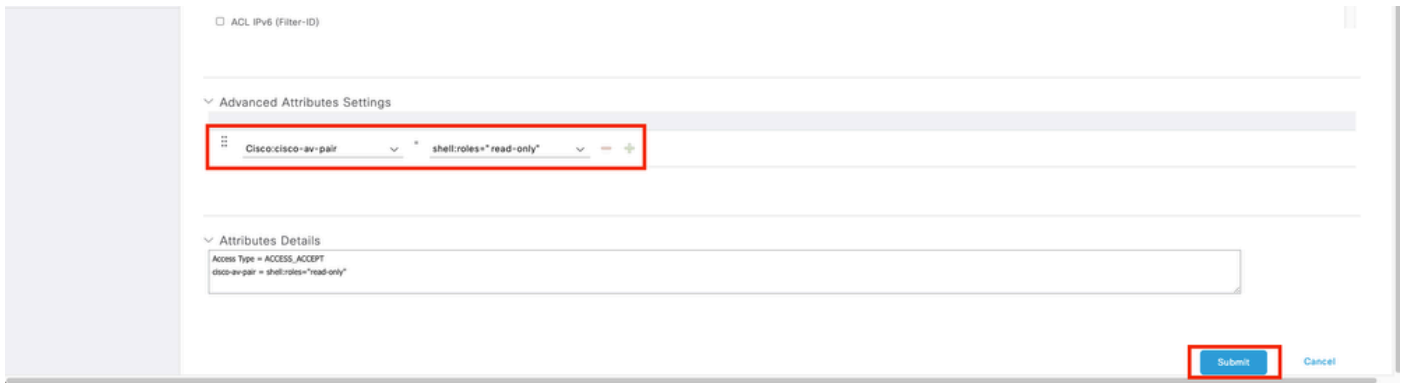
導航到Burger圖示 ≡ > Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add。

定義授權配置檔案的名稱，將訪問型別保留為ACCESS\_ACCEPT，並在Advanced Attributes Settings下增加cisco-av-pair=shell : roles="admin" with，然後按一下Submit。

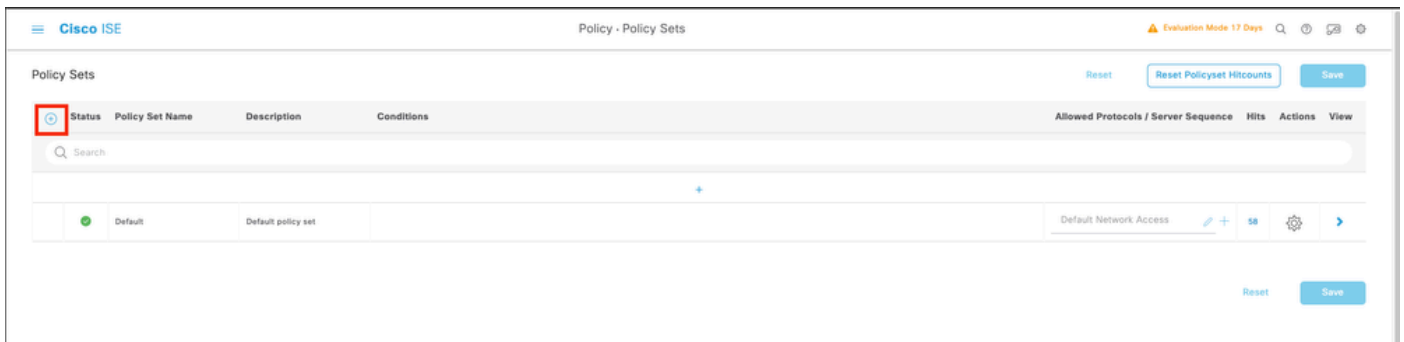


8.1 重複以上步驟，為只讀使用者建立授權配置檔案。這次使用值read-only Administrator建立RADIUS類。

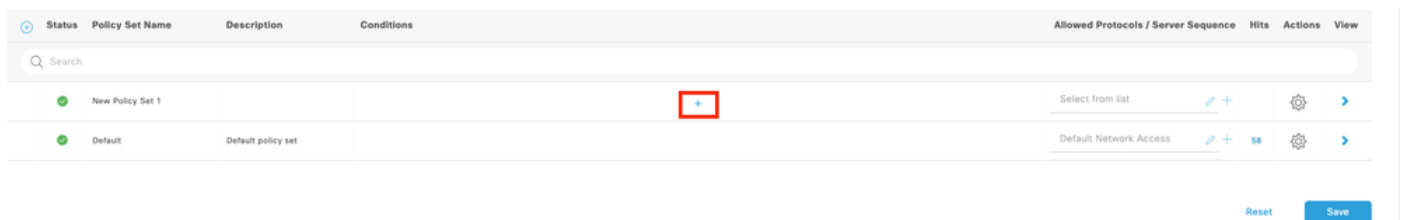




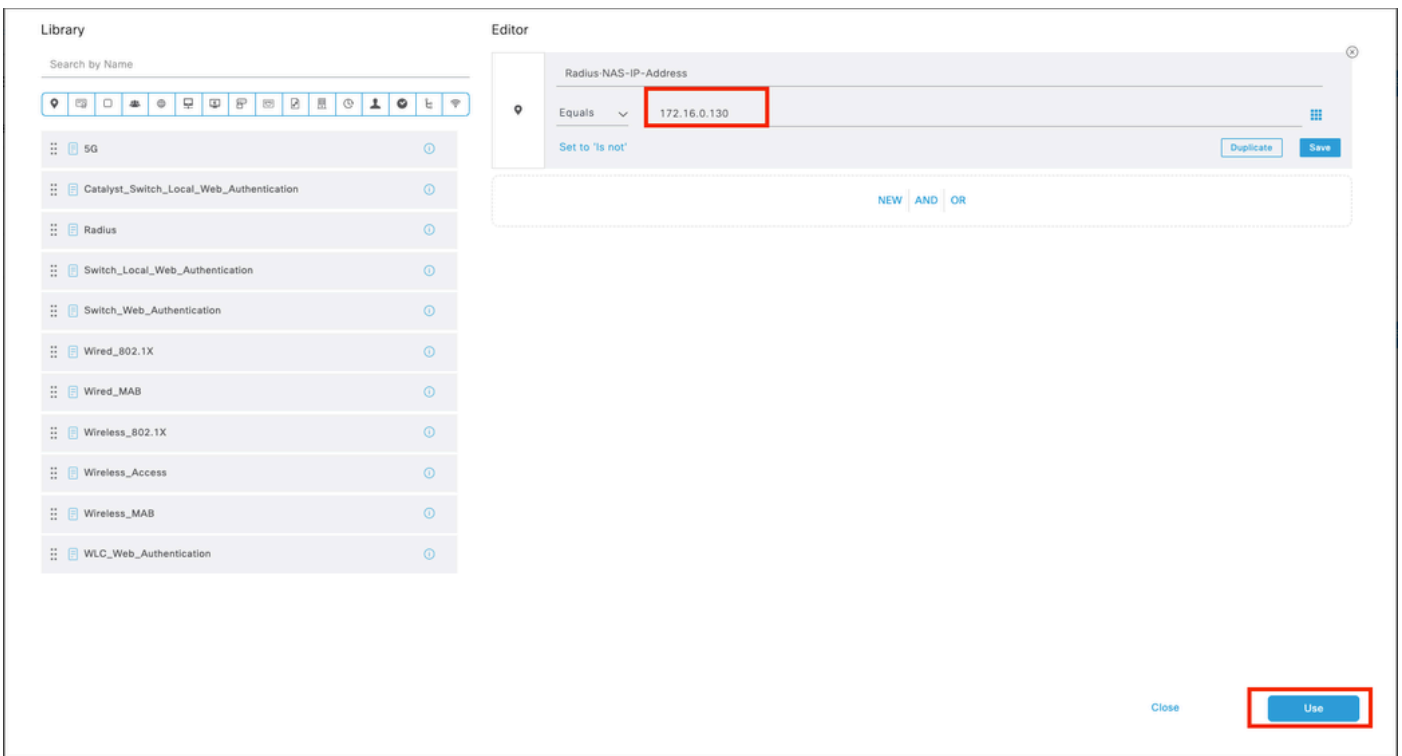
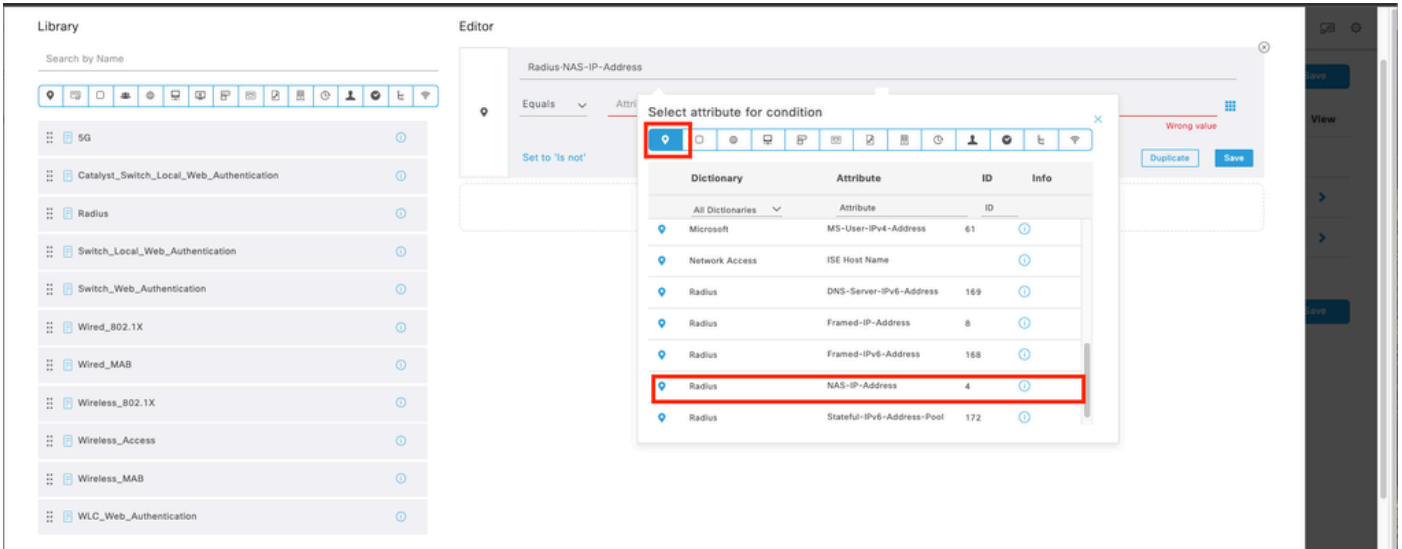
第9步：建立與FMC IP地址匹配的策略集。這是為了防止其他裝置向使用者授予訪問許可權。  
導航到 ≡ > Policy > Policy Sets > Add icon sign (位於左上角)。



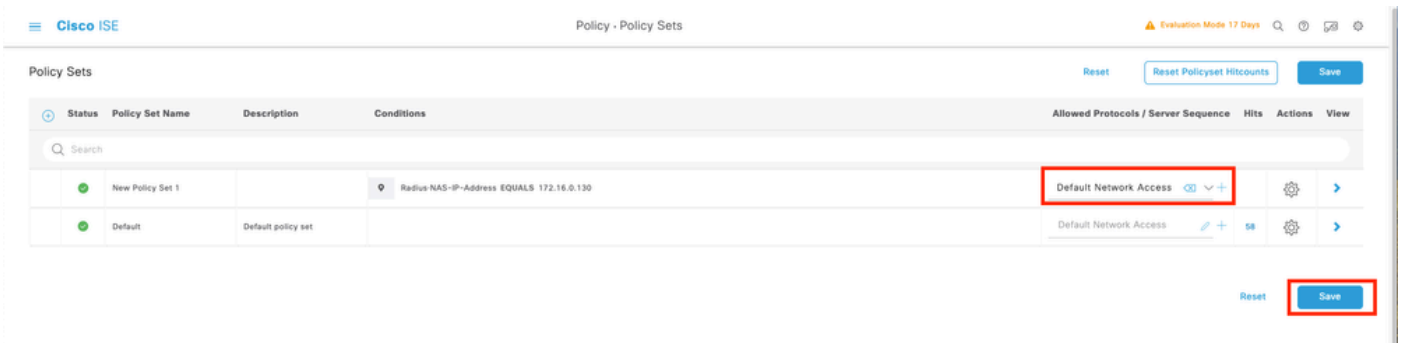
9.1 新行位於策略集的頂部。按一下Add圖示配置新條件。

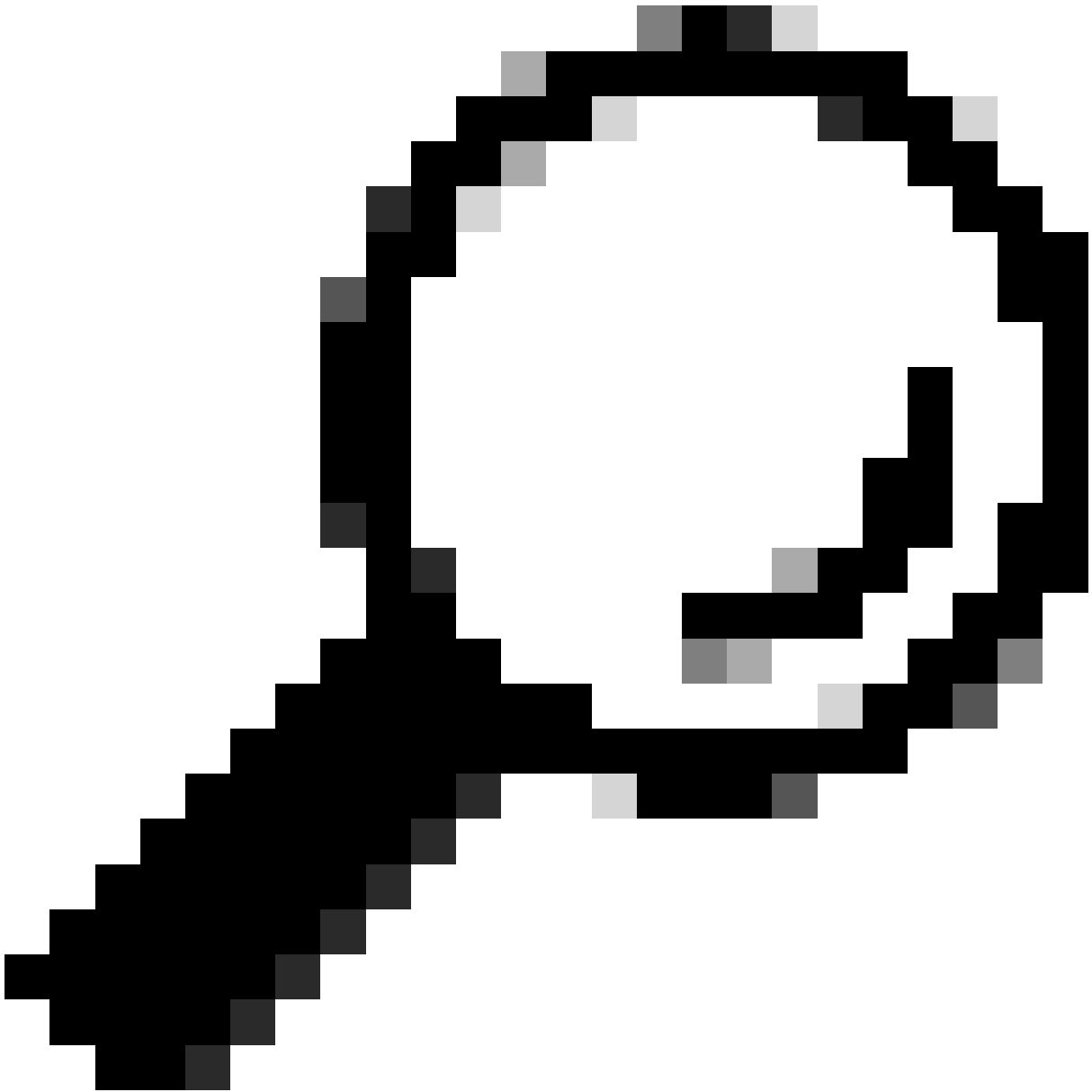


9.2 為RADIUS NAS-IP-Addressattribute增加匹配FCM IP地址的頂部條件，然後按一下使用。



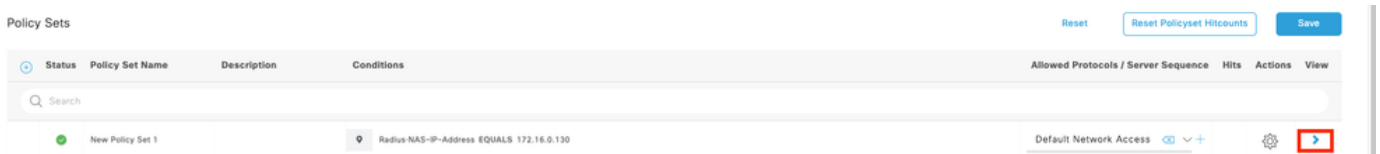
9.3完成後，按一下Save。



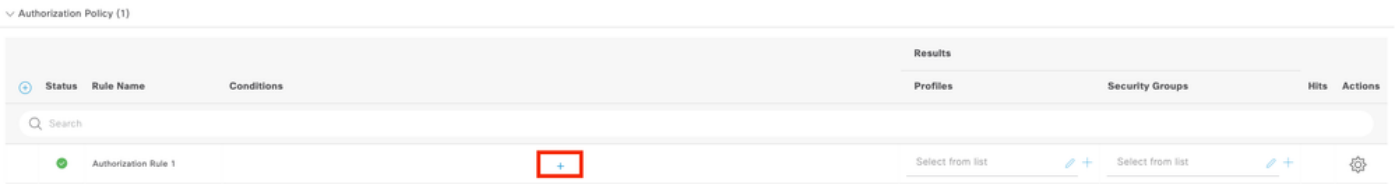


提示：在本練習中，我們允許使用預設網路訪問協定清單。您可以建立一個新清單，並根據需要縮小其範圍。

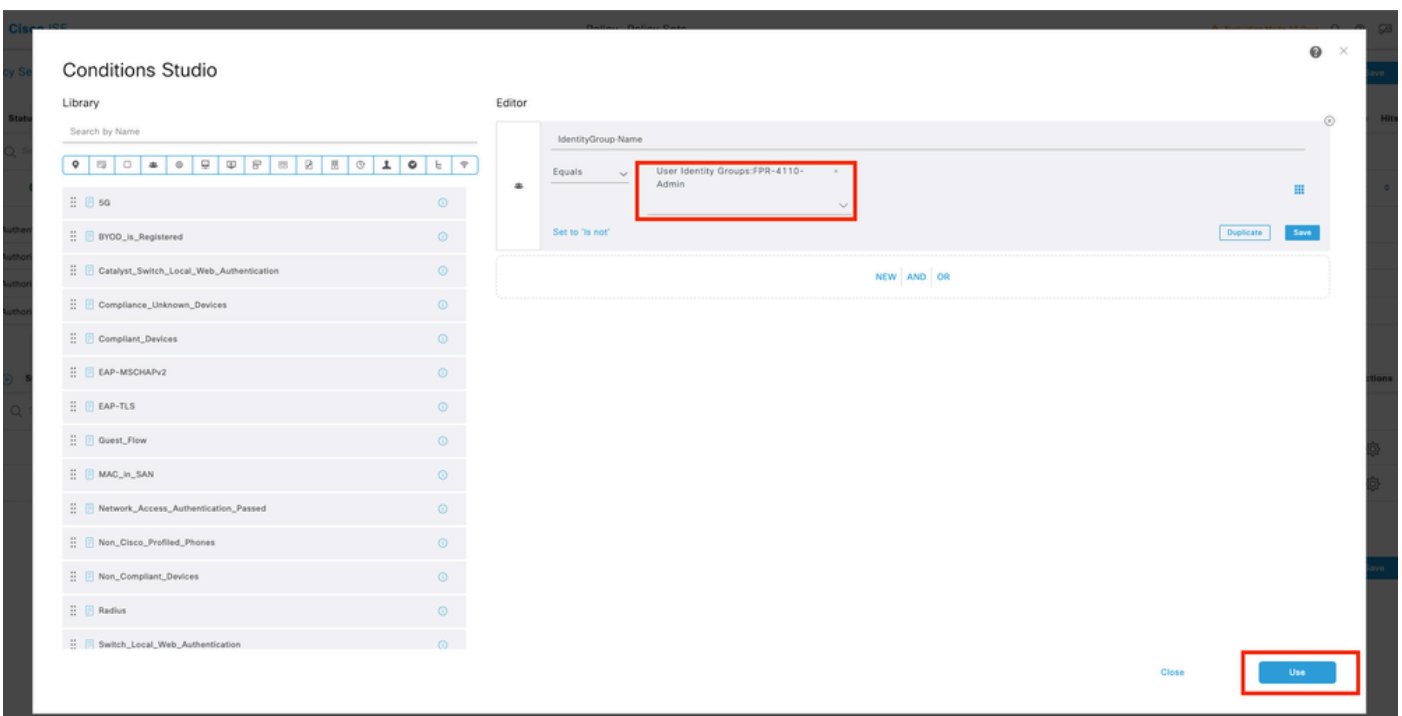
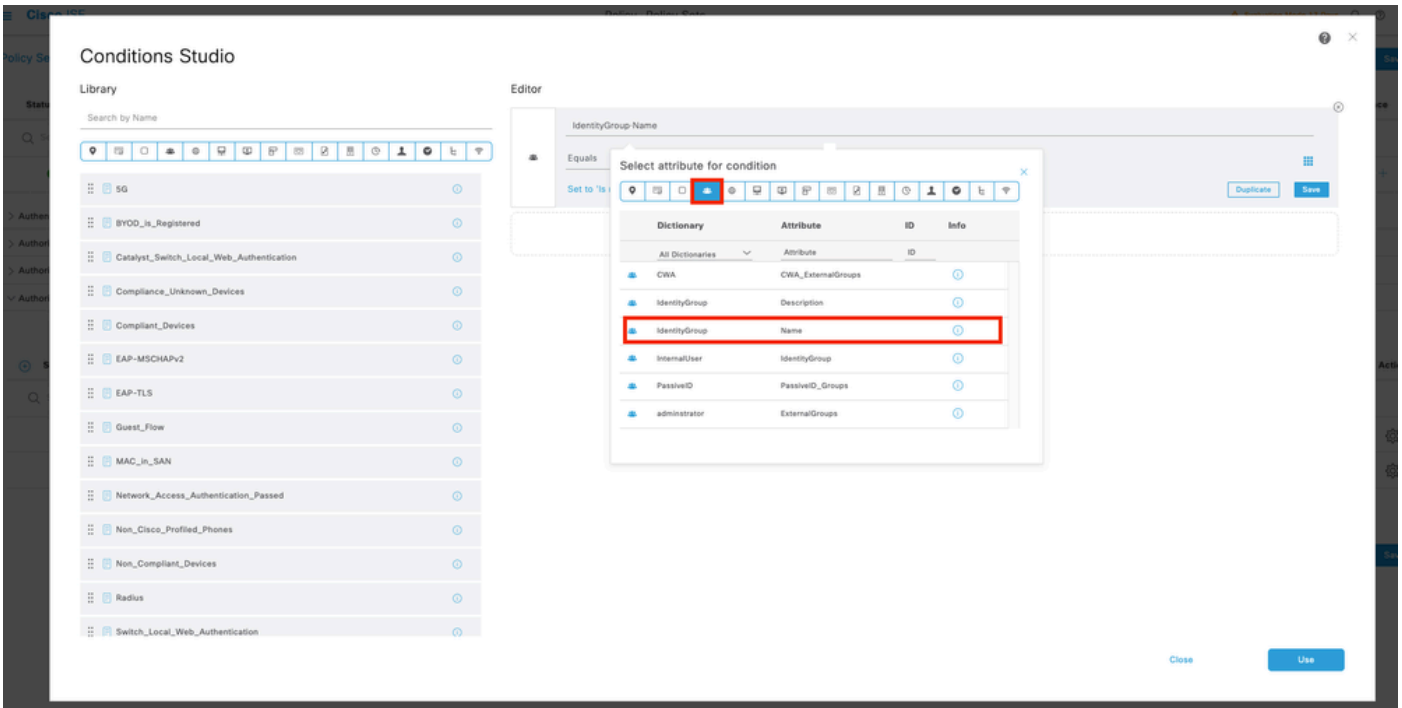
步驟 10. 透過按一下行末尾的>圖示檢視新的策略集。



10.1 展開Authorization Policy 選單，然後按一下in (+)增加新條件。

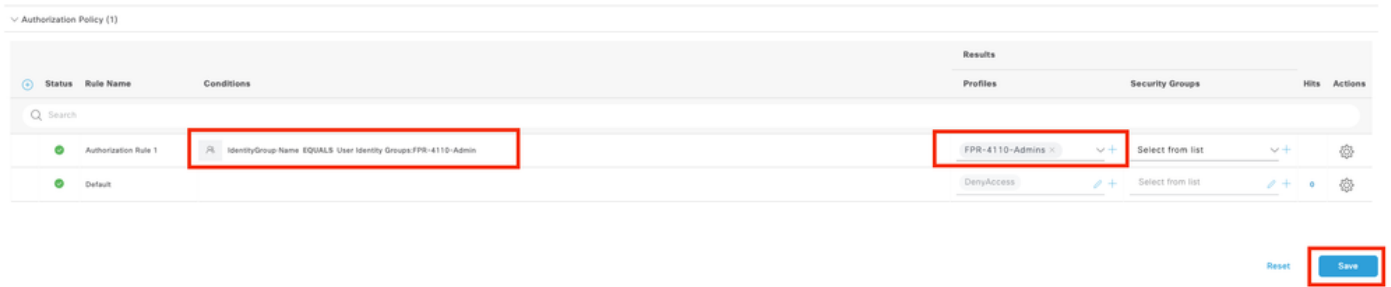


10.2 設定條件以匹配 Dictionary Identity Group with Attribute Name Equals User Identity Groups : FPR-4110-Admins (在步驟7中建立的組名) 並按一下 Use。





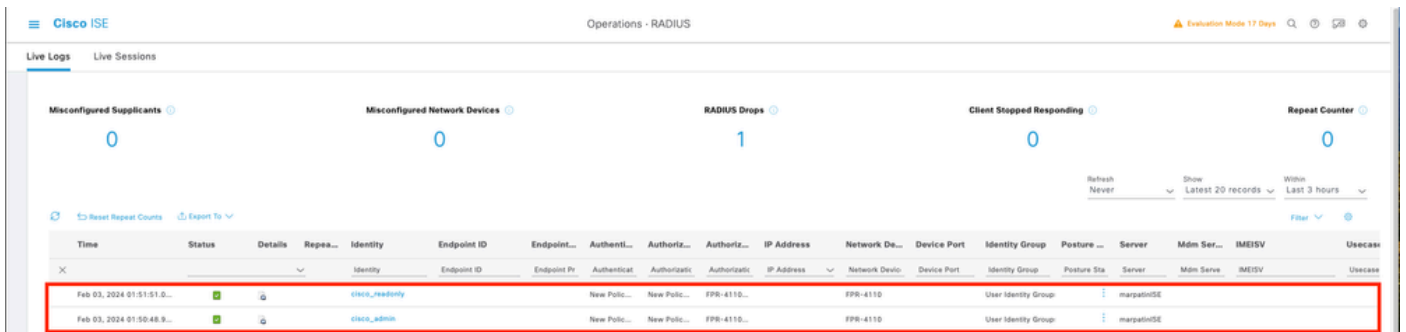
第10.3步驗證新條件是否在授權策略中配置，然後在配置檔案下增加使用者配置檔案。



步驟 11.在步驟9中，針對唯讀使用者重複相同的程式，然後按一下「儲存」。

### 驗證

1. 嘗試使用新的RADIUS憑證登入FCM GUI
2. 切換作業選項至Burger 圖示 => Operations > Radius > Live logs。
3. 顯示的資訊會顯示使用者是否成功登入。



4. 從Secure Firewall機箱CLI驗證已記錄使用者角色。

```
FPR4K-1-029A78B# scope se
security          server          service-profile

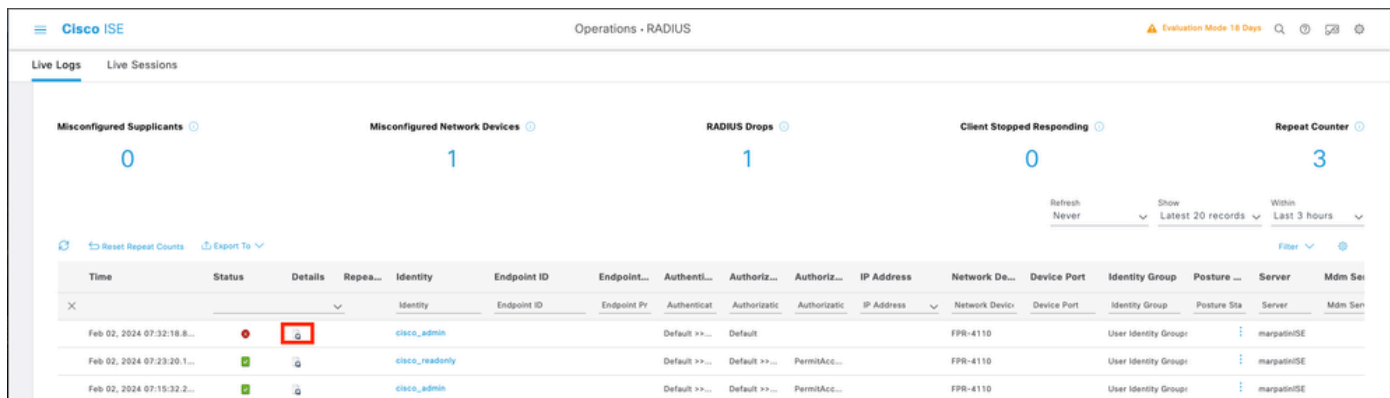
FPR4K-1-029A78B# scope security
FPR4K-1-029A78B /security # show remote-user detail
Remote User cisco_admin:
  Description:
  User Roles:
    Name: admin
    Name: read-only
FPR4K-1-029A78B /security #
```

# 疑難排解

1. 透過ISE GUI，導航到漢堡圖示=>操作> Radius >即時日誌。

1.1驗證日誌會話請求是否到達ISE節點。

1.2若為失敗狀態，請檢閱階段作業的詳細資訊。



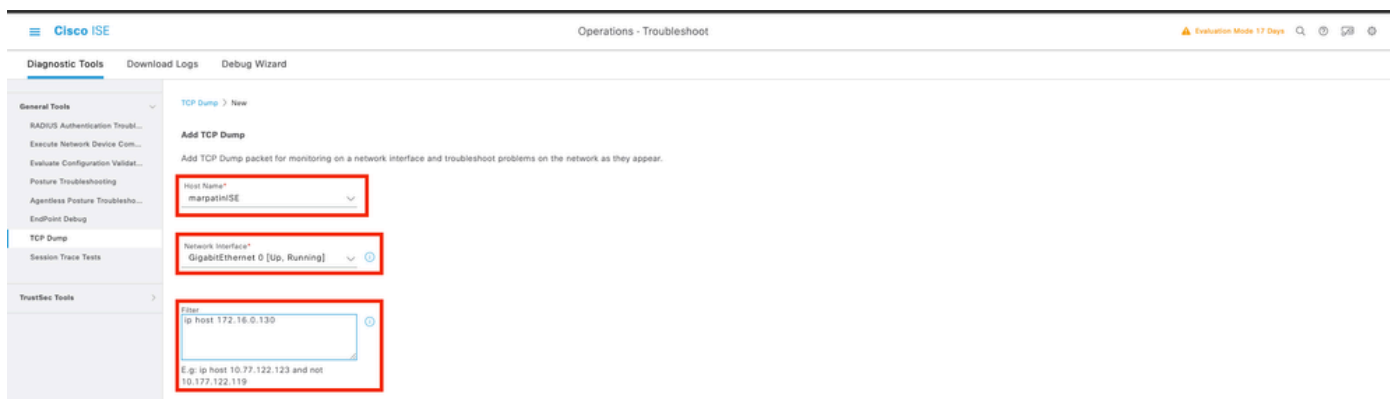
The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are summary statistics: Misconfigured Supplicants (0), Misconfigured Network Devices (1), RADIUS Drops (1), Client Stopped Responding (0), and Repeat Counter (3). Below these are options to Refresh, Show (Latest 20 records), and Within (Last 3 hours). A table below displays log entries with columns for Time, Status, Details, Identity, Endpoint ID, Endpoint Pr, Authent..., Authoriz..., Authoriz..., IP Address, Network De..., Device Port, Identity Group, Posture Sta, Server, and Mdm Sen. The first entry shows a failed status for 'cisco\_admin' on Feb 02, 2024 at 07:32:18.8.

| Time                       | Status  | Details | Repea... | Identity       | Endpoint ID | Endpoint Pr | Authent...   | Authoriz...  | Authoriz...  | IP Address | Network De... | Device Port | Identity Group       | Posture Sta | Server      | Mdm Sen |
|----------------------------|---------|---------|----------|----------------|-------------|-------------|--------------|--------------|--------------|------------|---------------|-------------|----------------------|-------------|-------------|---------|
| Feb 02, 2024 07:32:18.8... | Failed  | ⓘ       |          | cisco_admin    |             |             | Default >... | Default      |              |            | FPR-4110      |             | User Identity Group: |             | marpatinISE |         |
| Feb 02, 2024 07:23:20.1... | Success | ⓘ       |          | cisco_readonly |             |             | Default >... | Default >... | PermitAcc... |            | FPR-4110      |             | User Identity Group: |             | marpatinISE |         |
| Feb 02, 2024 07:15:32.2... | Success | ⓘ       |          | cisco_admin    |             |             | Default >... | Default >... | PermitAcc... |            | FPR-4110      |             | User Identity Group: |             | marpatinISE |         |

2. 對於未顯示在RADIUS即時日誌中的請求，檢視UDP請求是否透過資料包捕獲到達ISE節點。

導航到Burger圖示=> Operations > Troubleshoot > Diagnostic Tools > TCP dump。增加新的捕獲並將檔案下載到本地電腦，以檢視UDP資料包是否到達ISE節點。

2.1填寫所需資訊，向下滾動並按一下Save。



The screenshot shows the Cisco ISE Operations - Troubleshoot Diagnostic Tools page. The 'TCP Dump' section is active, showing a 'New' configuration. The 'Host Name' is set to 'marpatinISE', the 'Network Interface' is 'GigabitEthernet 0 [Up, Running]', and the 'Filter' is 'ip host 172.16.0.130'. There are red boxes around the Host Name, Network Interface, and Filter fields.

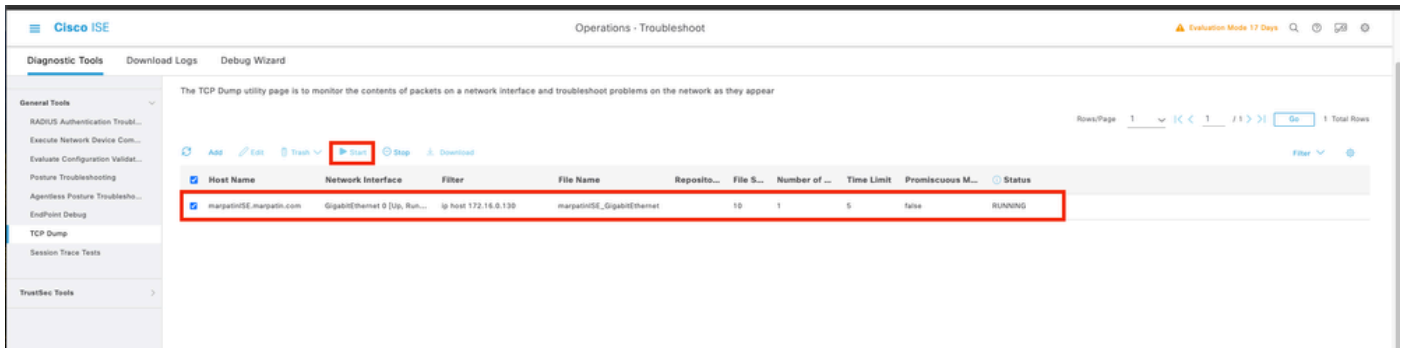
Host Name: marpatinISE

Network Interface: GigabitEthernet 0 [Up, Running]

Filter: ip host 172.16.0.130

E.g: ip host 10.77.122.123 and not 10.77.122.119

2.2選取並啟動擷取。



2.3當ISE捕獲運行時，嘗試登入到安全防火牆機箱

2.4停止ISE中的TCP轉儲並將檔案下載到本地電腦。

2.5檢視流量輸出。

預期輸出：

資料包No1。透過埠1812 (RADIUS)從安全防火牆向ISE伺服器發出請求  
資料包No2。ISE伺服器答覆接受初始請求。

| No. | Time                       | Source       | Destination  | Length | Protocol | Message Transaction ID | Info                 |
|-----|----------------------------|--------------|--------------|--------|----------|------------------------|----------------------|
| 1   | 2024-02-02 20:21:52.999276 | 172.16.0.130 | 172.16.0.12  | 128    | RADIUS   |                        | Access-Request id=22 |
| 2   | 2024-02-02 20:21:53.090894 | 172.16.0.12  | 172.16.0.130 | 186    | RADIUS   |                        | Access-Accept id=22  |

## 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）。