在FMC上配置RAVPN證書身份驗證和ISE授權

目錄

簡介

本文檔介紹在FMC上由CSF管理的RAVPN連線中配置證書身份驗證的ISE伺服器授權策略。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆(CSF)
- 思科安全防火牆管理中心(FMC)
- 思科身分辨識服務引擎(ISE)
- 證書註冊和SSL基礎知識。
- 憑證授權單位(CA)

採用元件

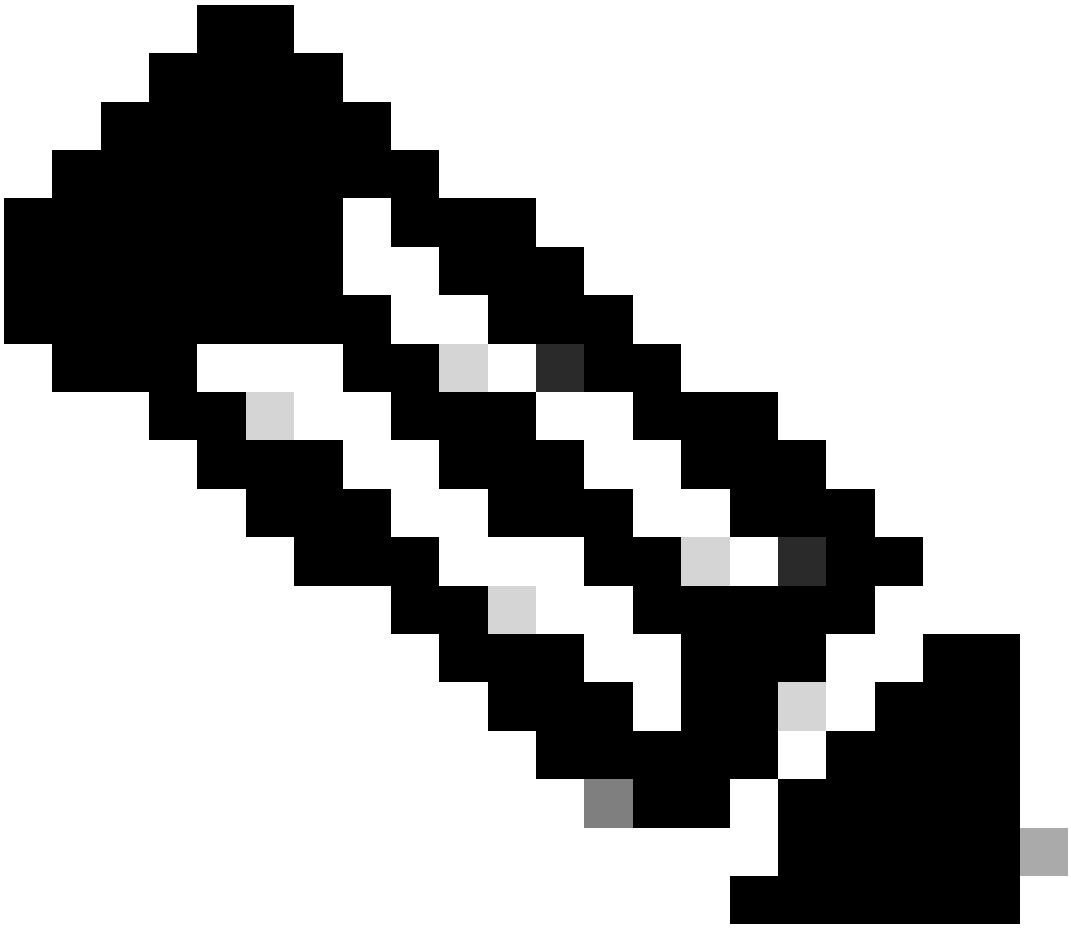
本檔案內容以這些軟體和硬體版本為基礎。

- 思科安全使用者端5.1.6版
- 思科安全防火牆版本7.2.8
- 思科安全防火牆管理中心版本7.2.8

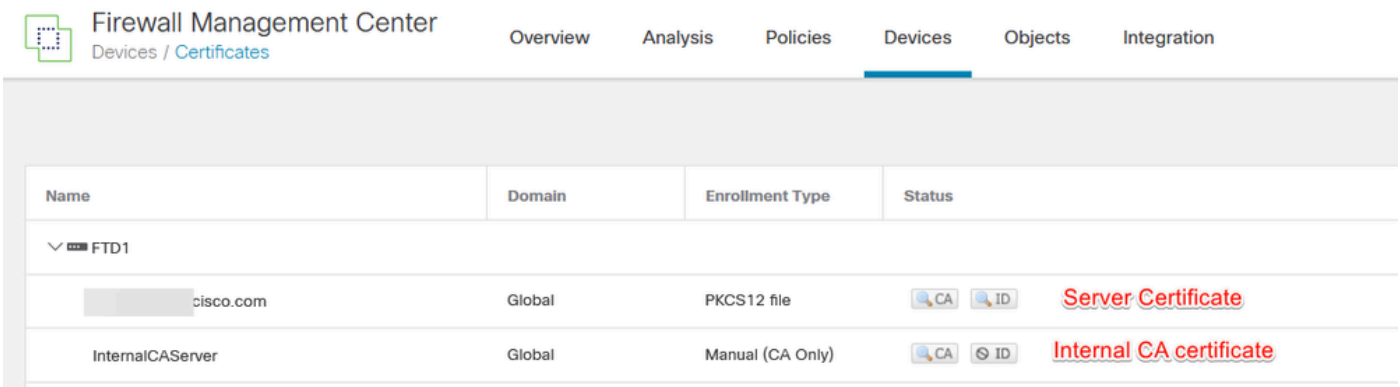
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

第1步：安裝受信任的CA證書



注意：如果CA證書與用於伺服器身份驗證的證書不同，則需要執行此步驟。如果同一CA伺服器向使用者頒發證書，則無需再次導入同一CA證書。

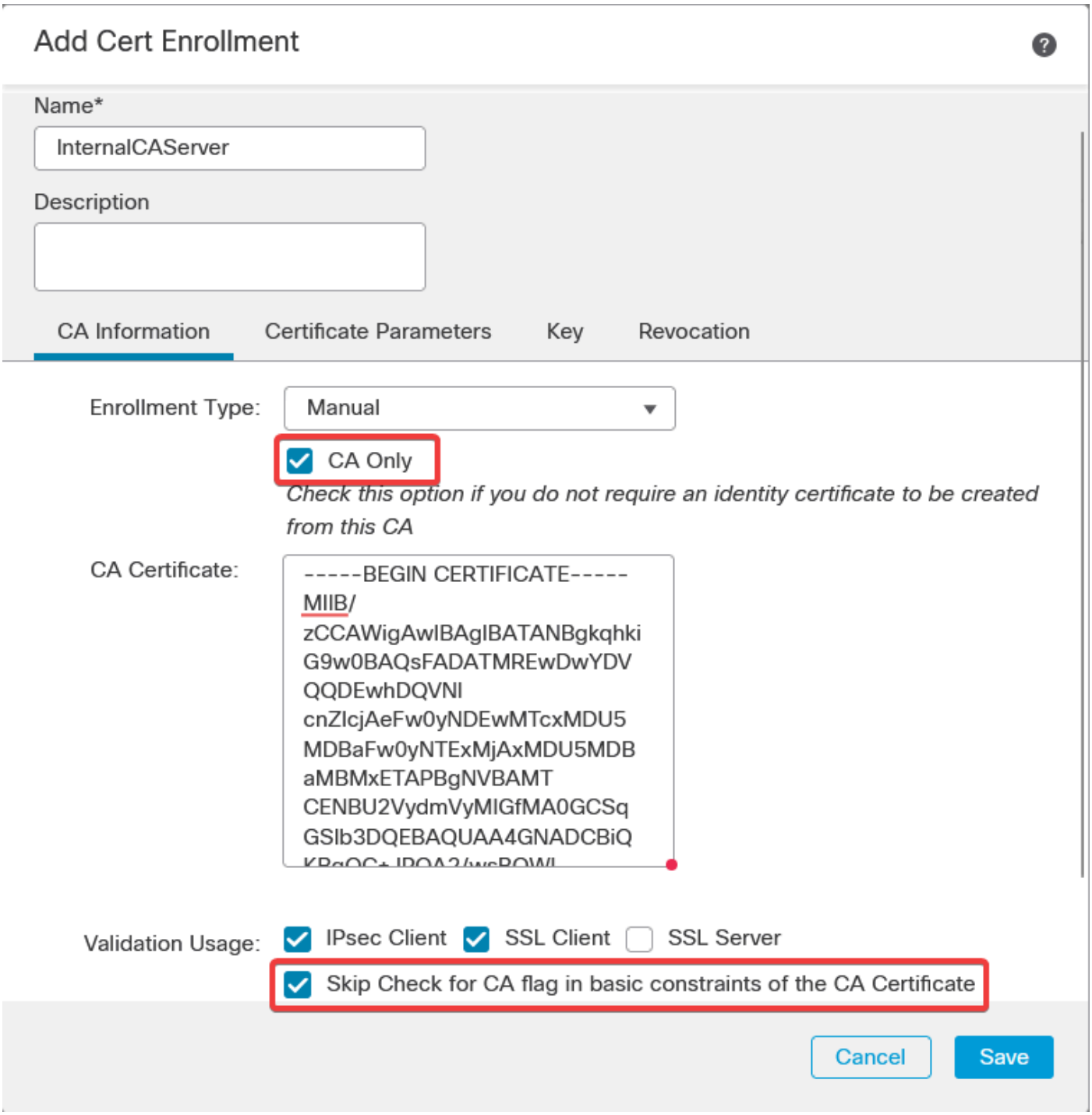


a.導航到Devices > Certificates並按一下**Add**。

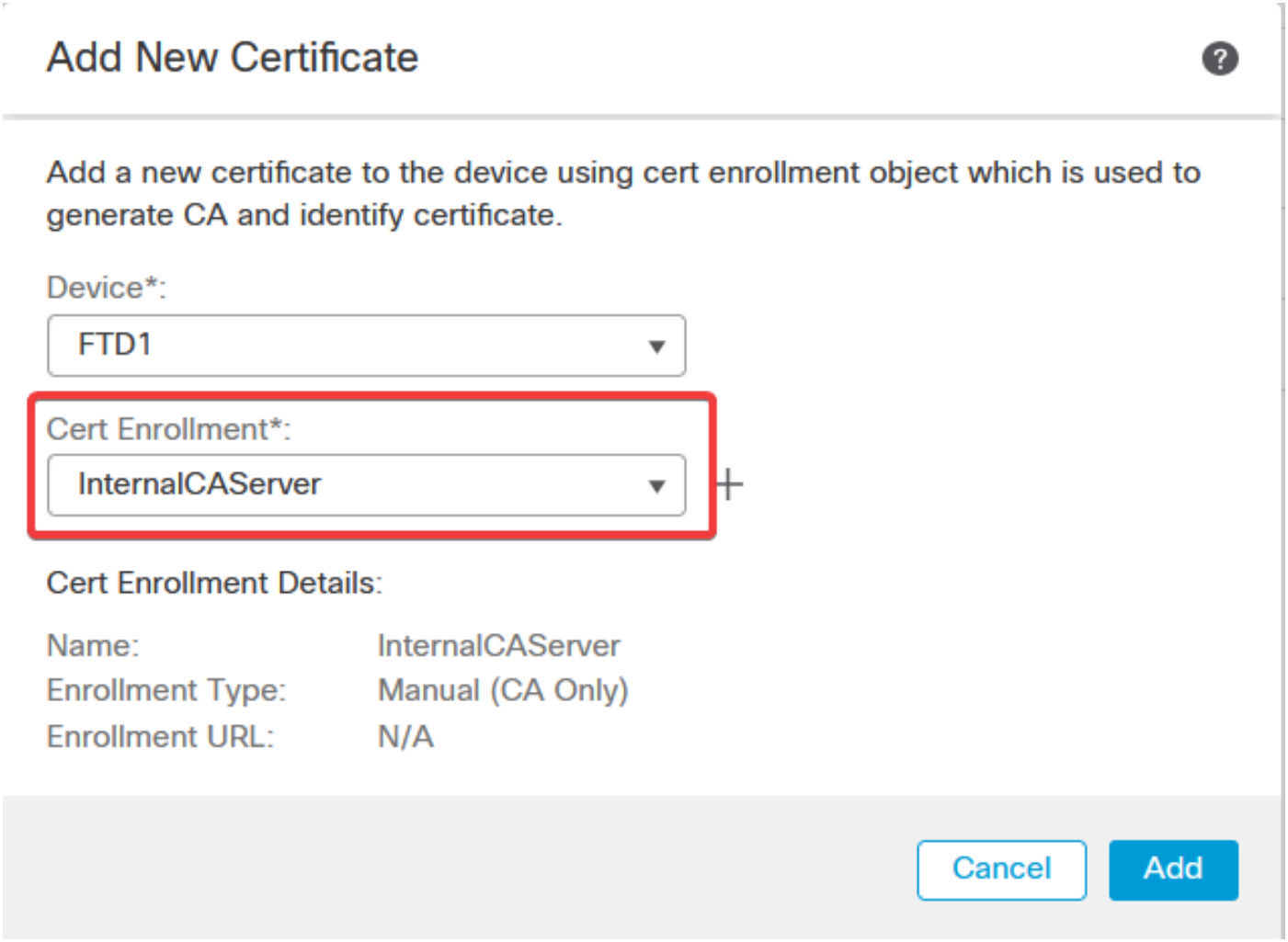
b.輸入**trustpoint name**並選擇Manual作為CA資訊下的登記型別。

c.檢查CA Only並貼上採用pem格式的受信任/內部CA證書。

d.選中**Skip Check for CA flag in basic constraints of the CA Certificate**並按一下**Save**。

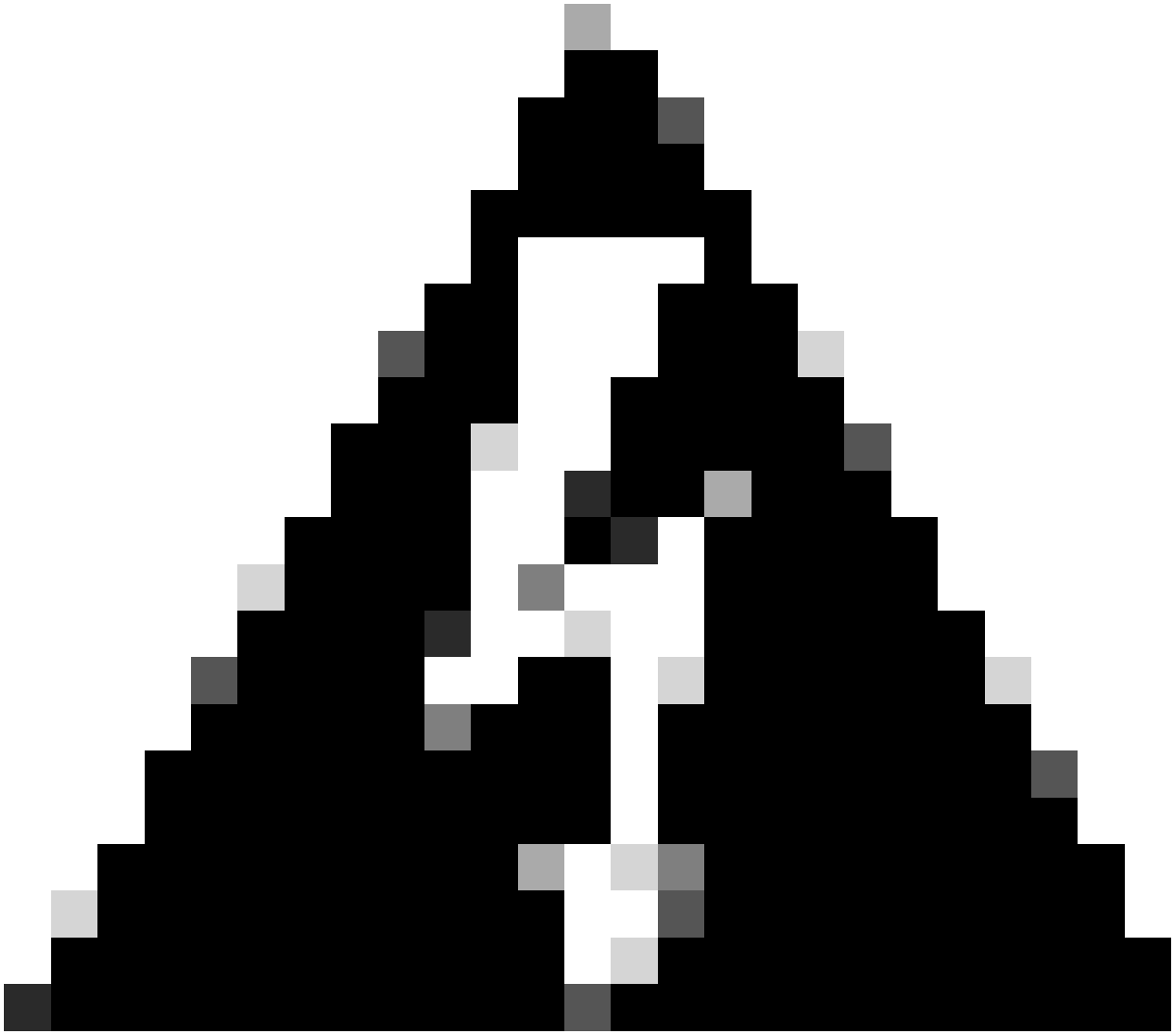


e.在**Cert Enrollment**下，從剛建立的下拉選單中選擇**trustpoint**，然後按一下**Add**。

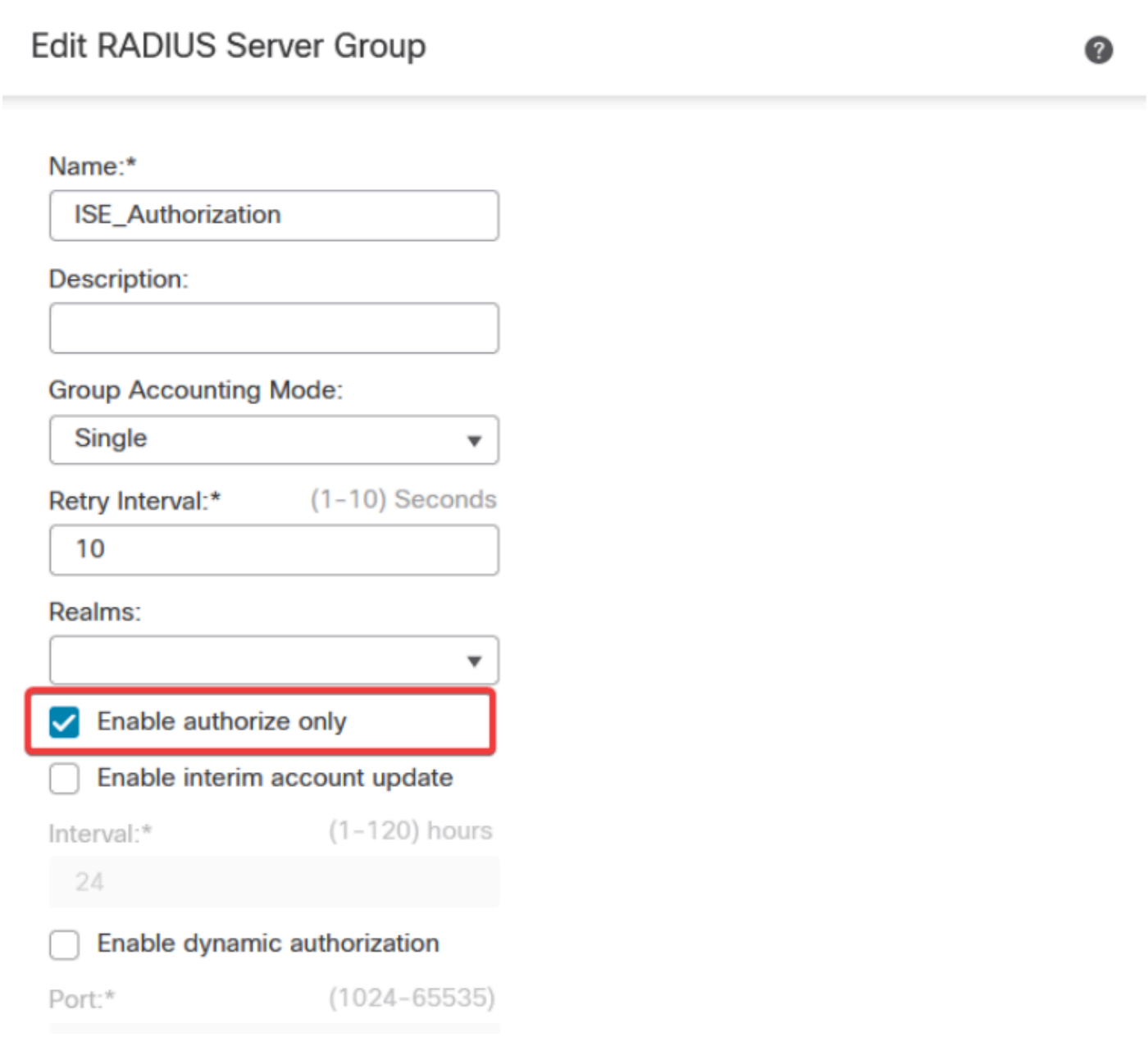


第2步：配置ISE/Radius伺服器組和連線配置檔案

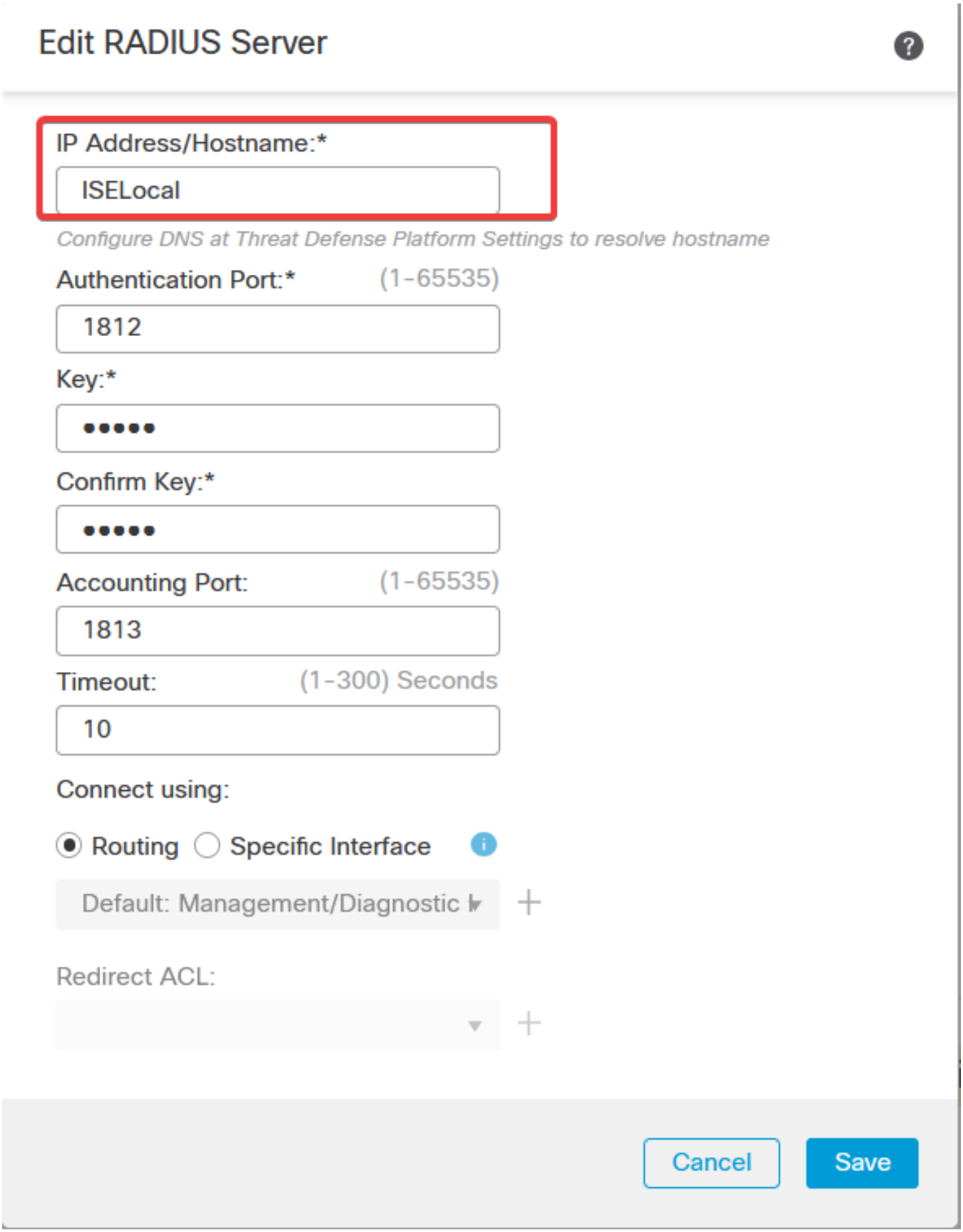
a.導航到**Objects > AAA Server > RADIUS Server Group**並按一下**Add RADIUS Server Group**。 選中**Enable authorize only**選項。



警告：如果未選中「僅啟用授權」選項，則防火牆將傳送身份驗證請求。但是，ISE期望接收該請求的使用者名稱和密碼，並且證書中未使用密碼。因此，ISE將請求標籤為身份驗證失敗。



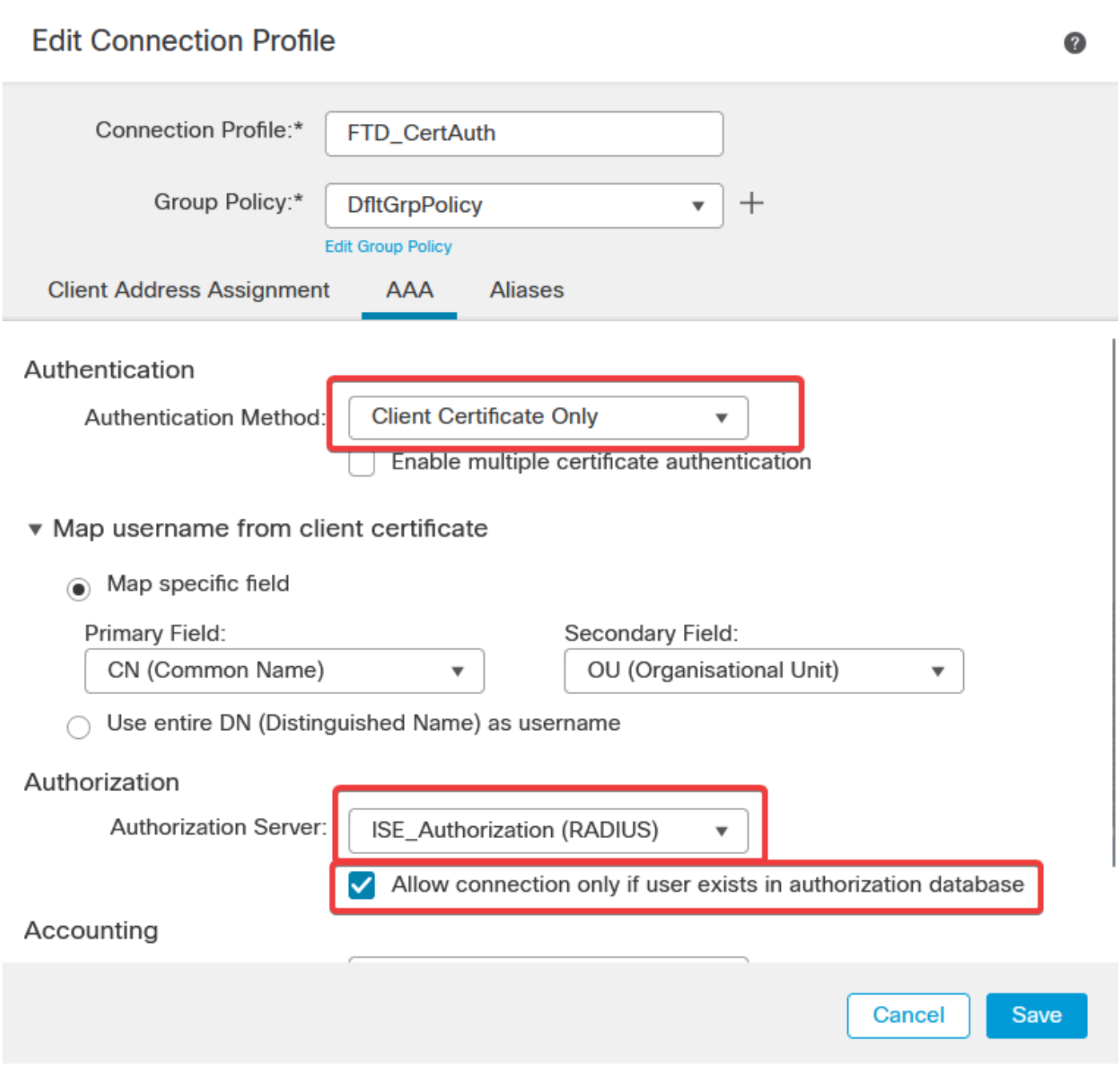
b.按一下**Add (+)**圖示，然後使用IP地址或主機名增加Radius server/ISE server。



c.導航到**Devices > Remote Access configuration**。 建立new connection profile並將驗證方法設定為Client Certificate Only。對於授權伺服器，請選擇在之前步驟中建立的授權伺服器。

確保您選中**Allow connection only if user exists in authorization database**選項。此設定可確保僅當授權允許時才完

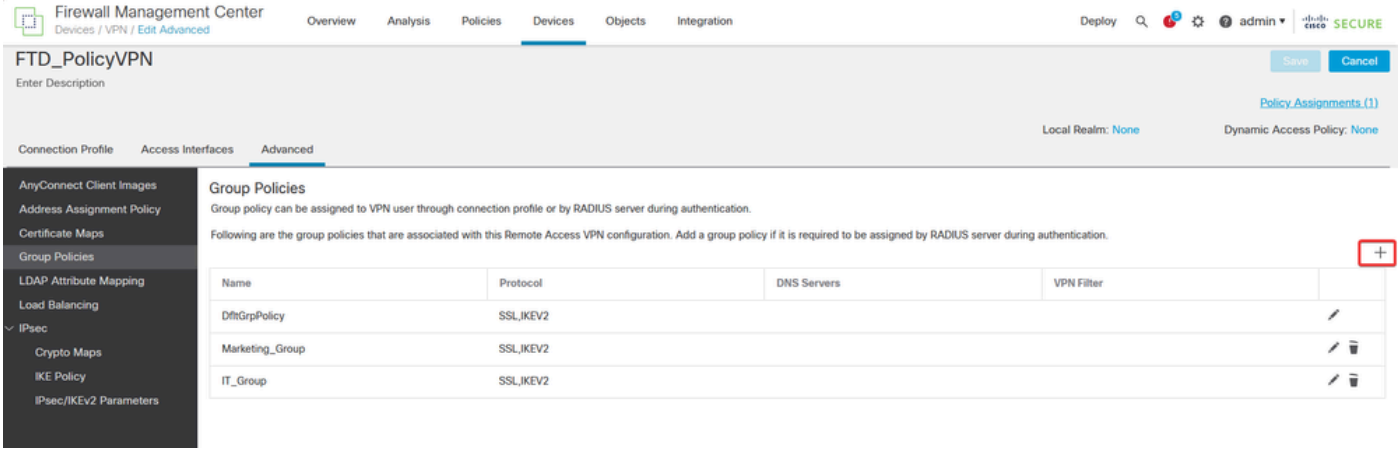
成與RAVPN的連線。



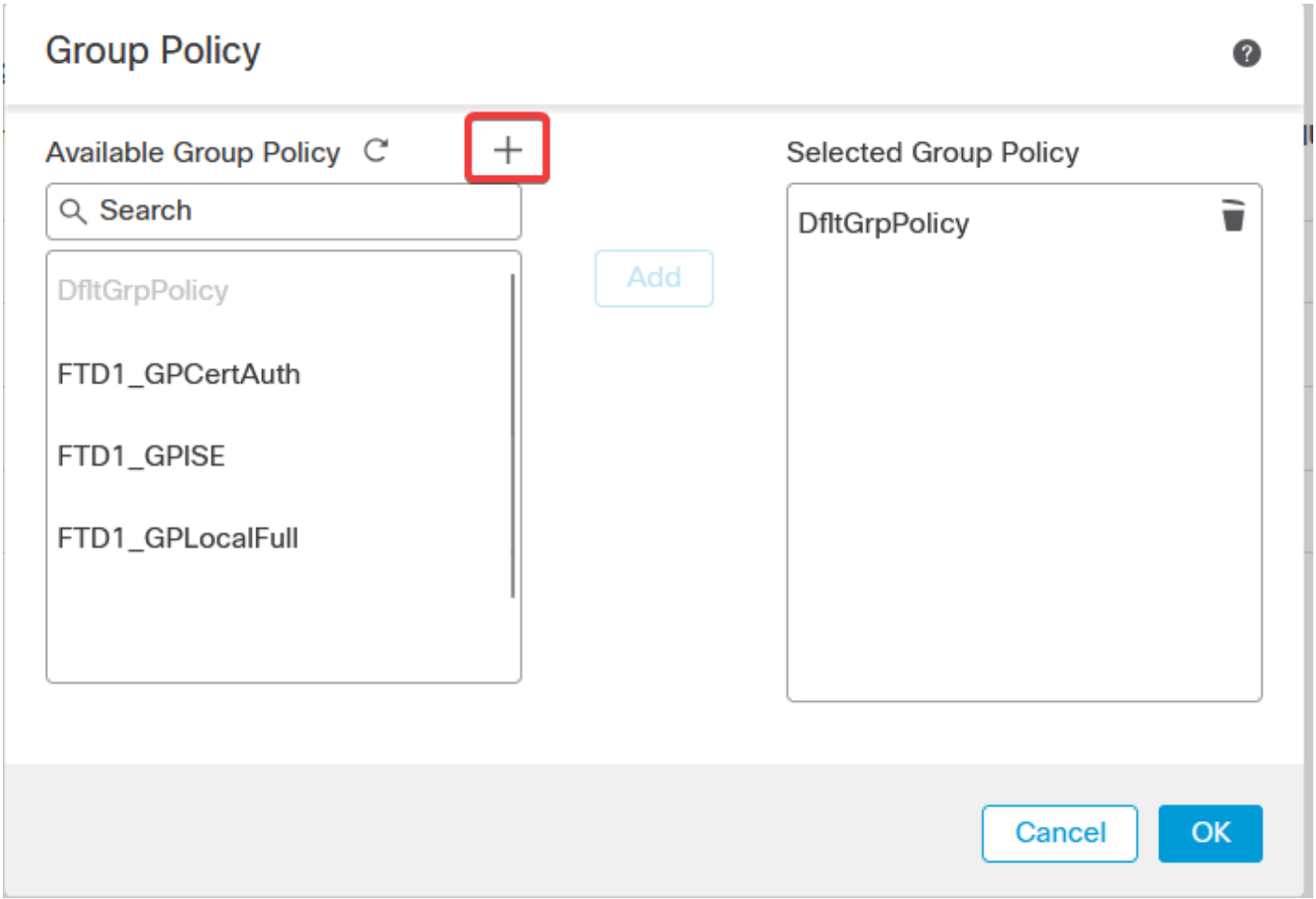
來自客戶端證書的Map Username是指從證書獲取的資訊以標識使用者。在本例中，您將保留預設配置，但可以根據用於標識使用者的資訊進行更改。

點選**Save**。

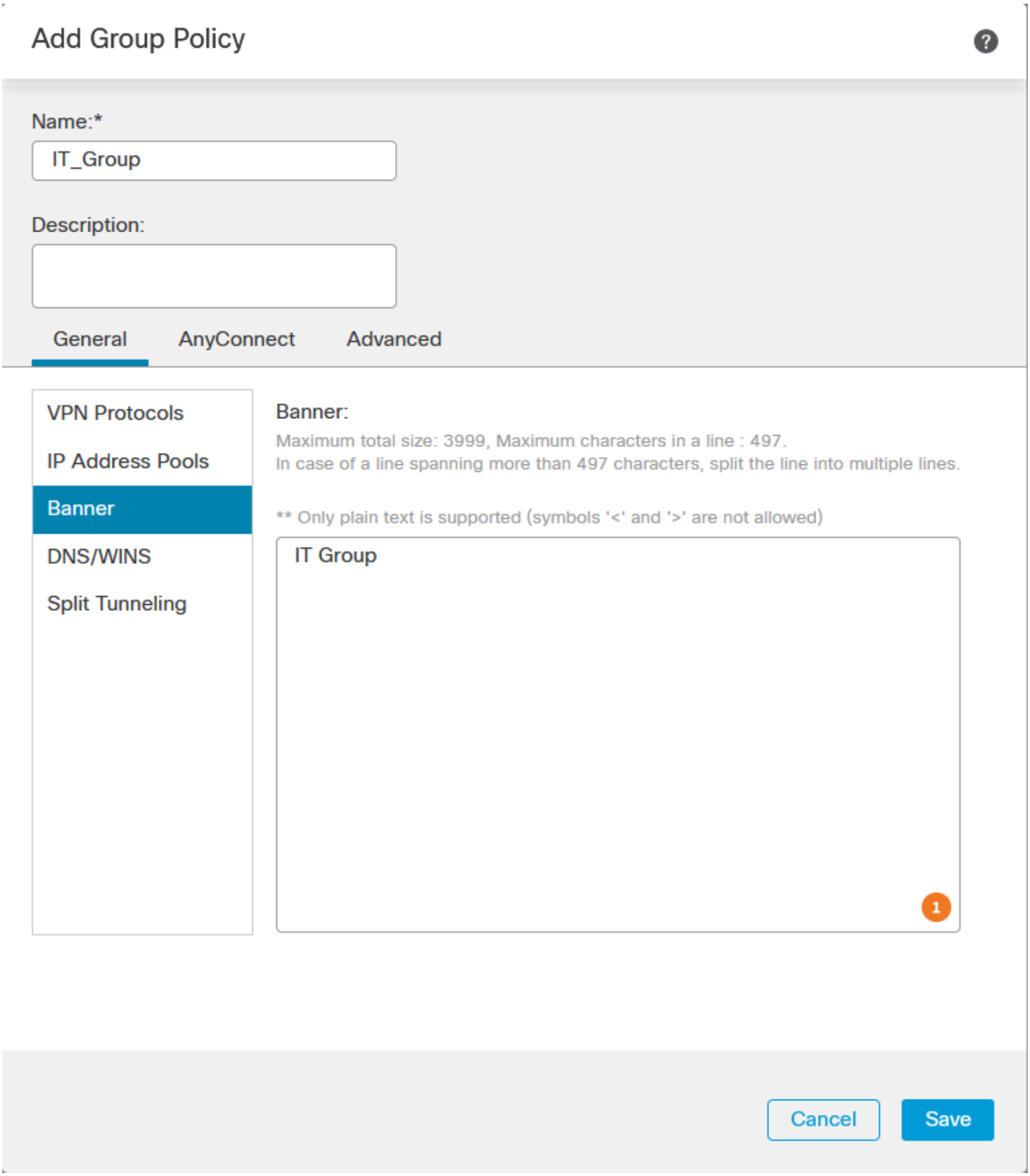
d.導航至**Advanced** > **Group Policies**。按一下右側的**Add (+)**圖示。



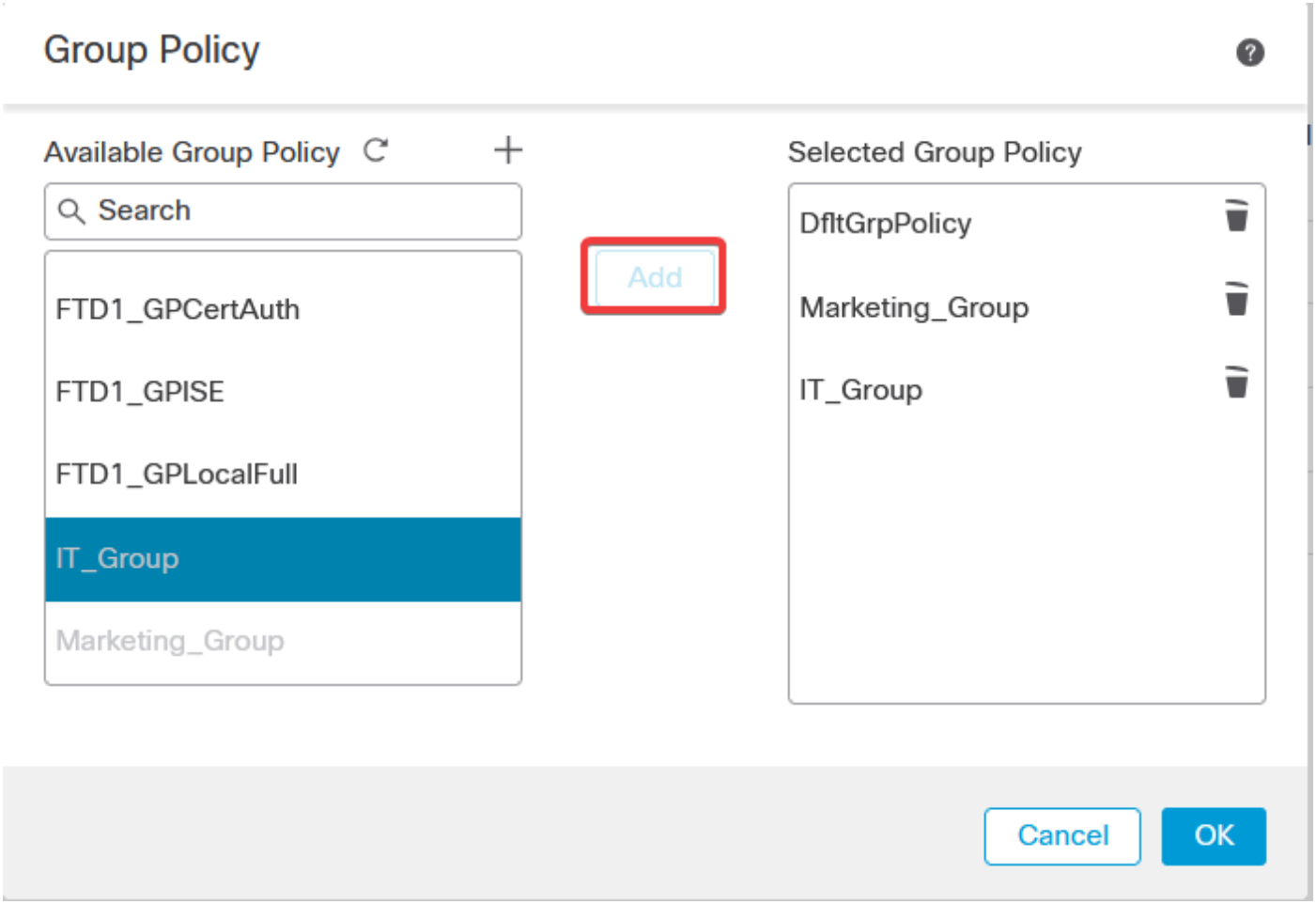
e.建立group policies。每個組策略都根據組織組和每個組可以訪問的網路進行配置。



f.在組策略上，執行每個組特定的配置。可以增加一條標語消息以在成功連線後顯示。



g.選擇左側的**group policies**，然後按一下Add將其移動到右側。這指定了配置中正在使用的組策略。

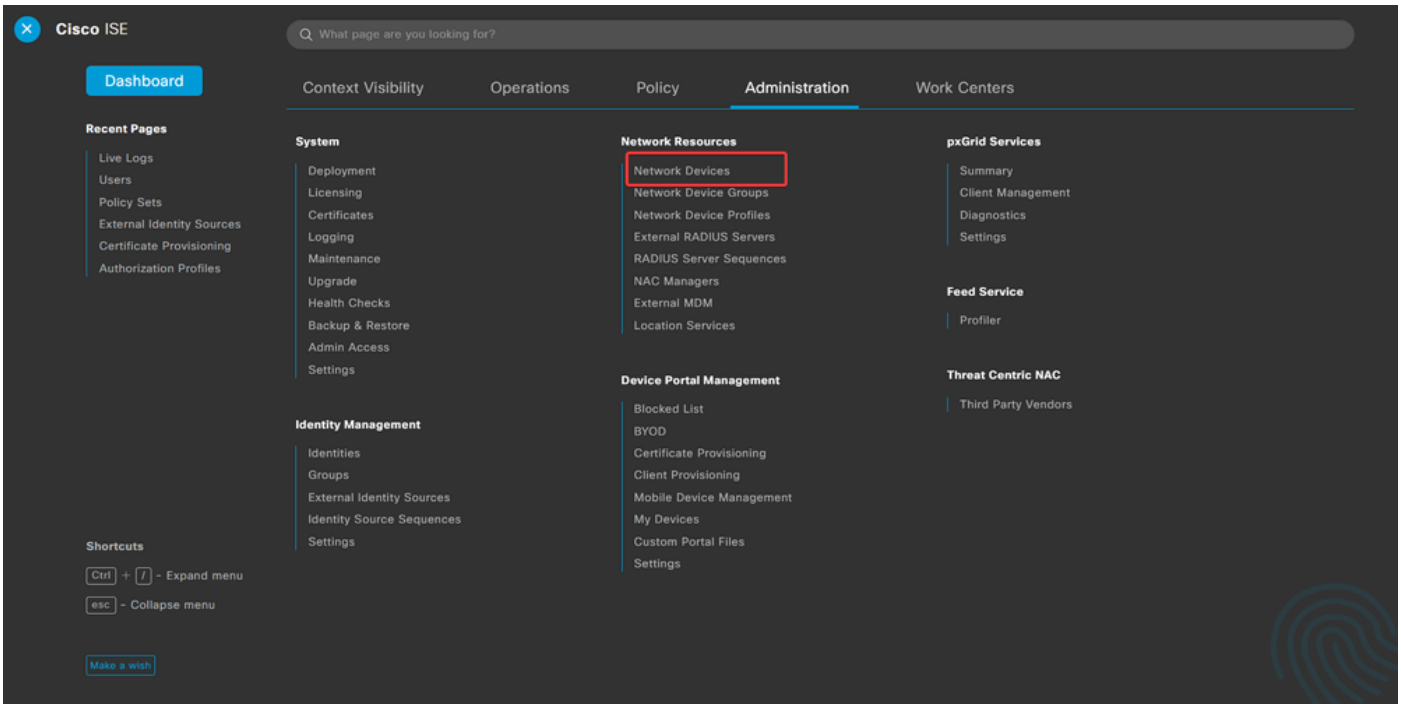


e.部署更改。

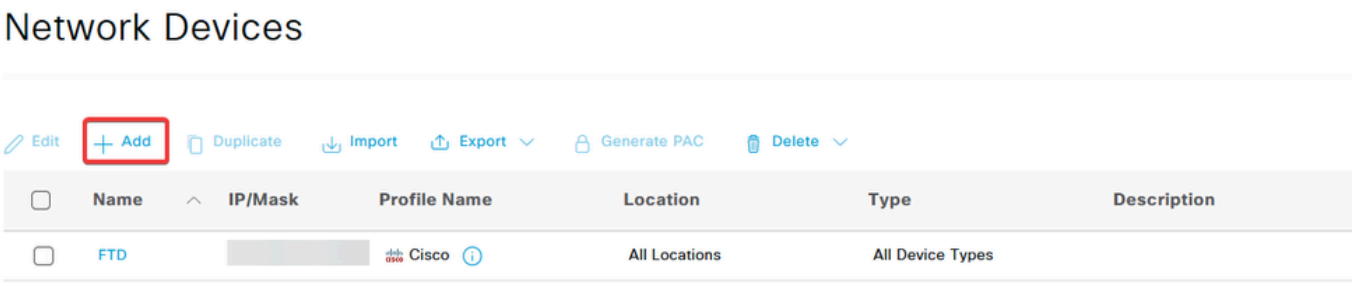
第3步：配置ISE

第3.1步：建立使用者、組和證書身份驗證配置檔案

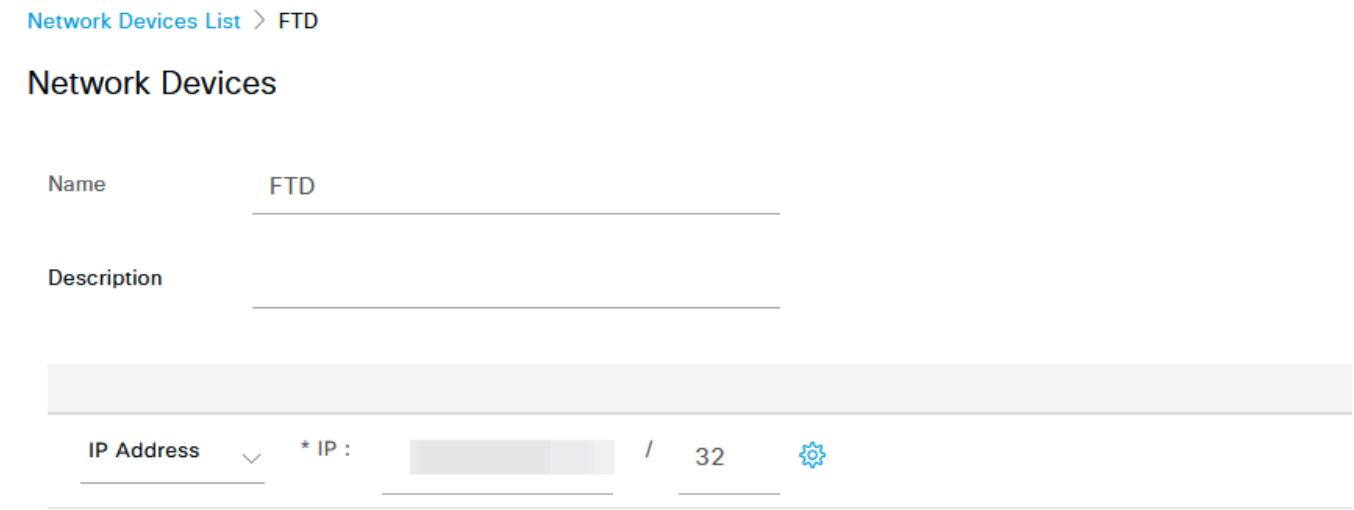
a.登入到ISE伺服器並導航至**Administration > Network Resources > Network Devices**。

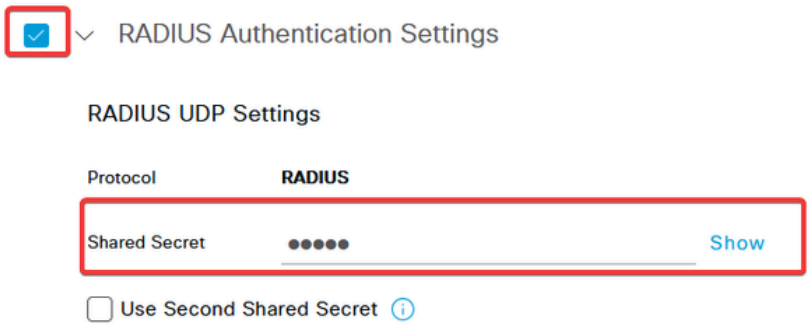


b.按一下Add將防火牆配置為AAA客戶端。

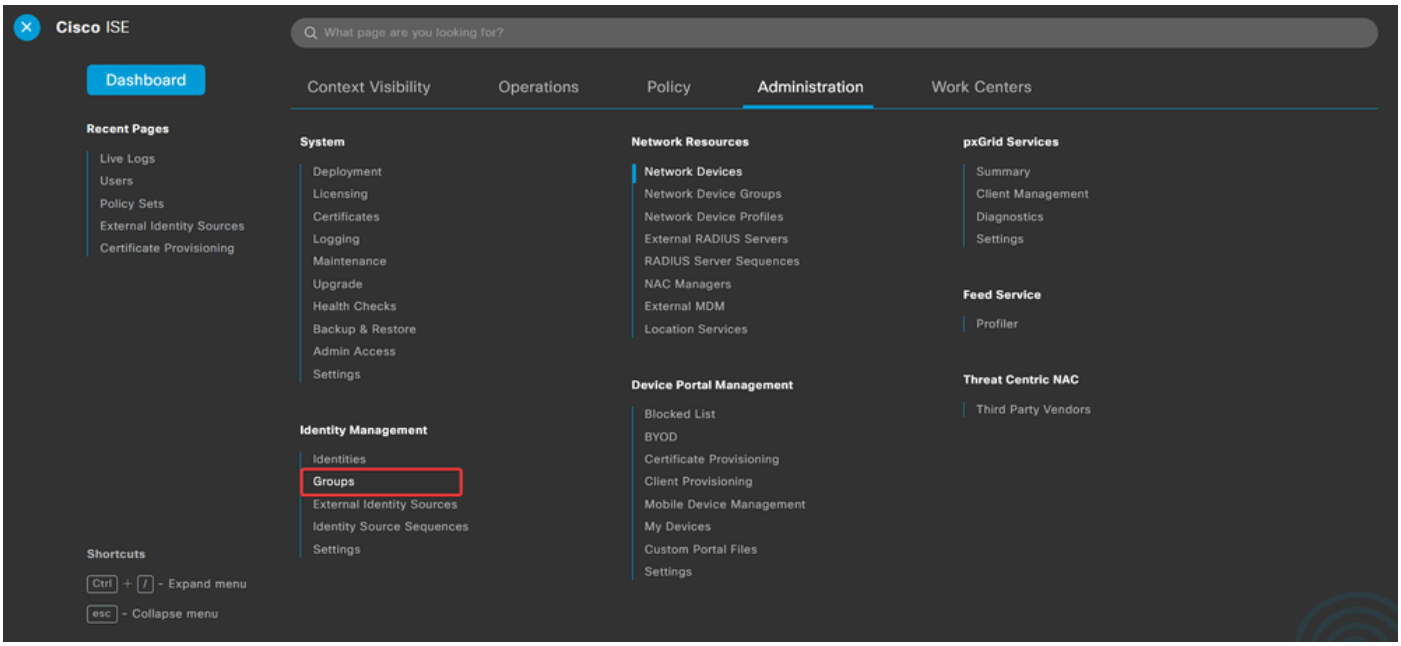


c.輸入網路裝置名稱和IP地址欄位，然後選中RADIUS Authentication Settings覈取方塊，並增加Shared Secret.「此值必須與在FMC上建立RADIUS伺服器對象時使用的值相同」。按一下Save。



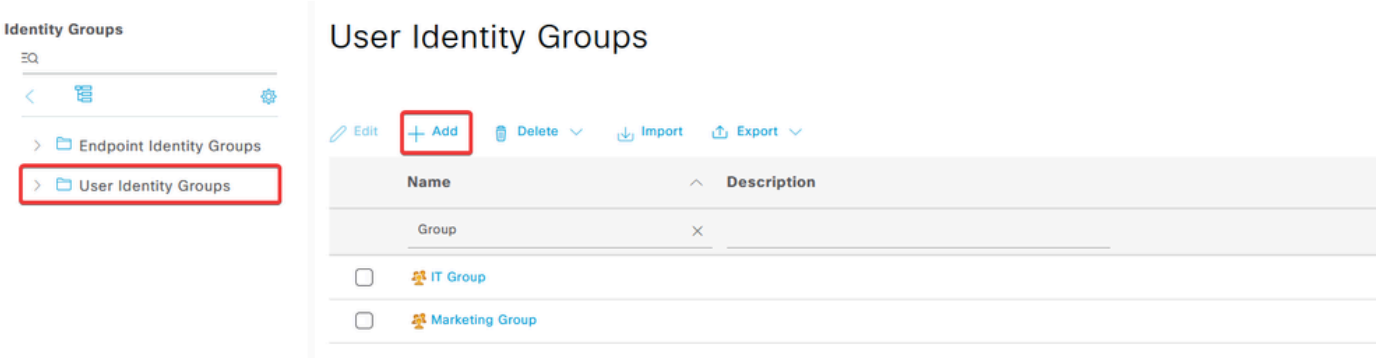


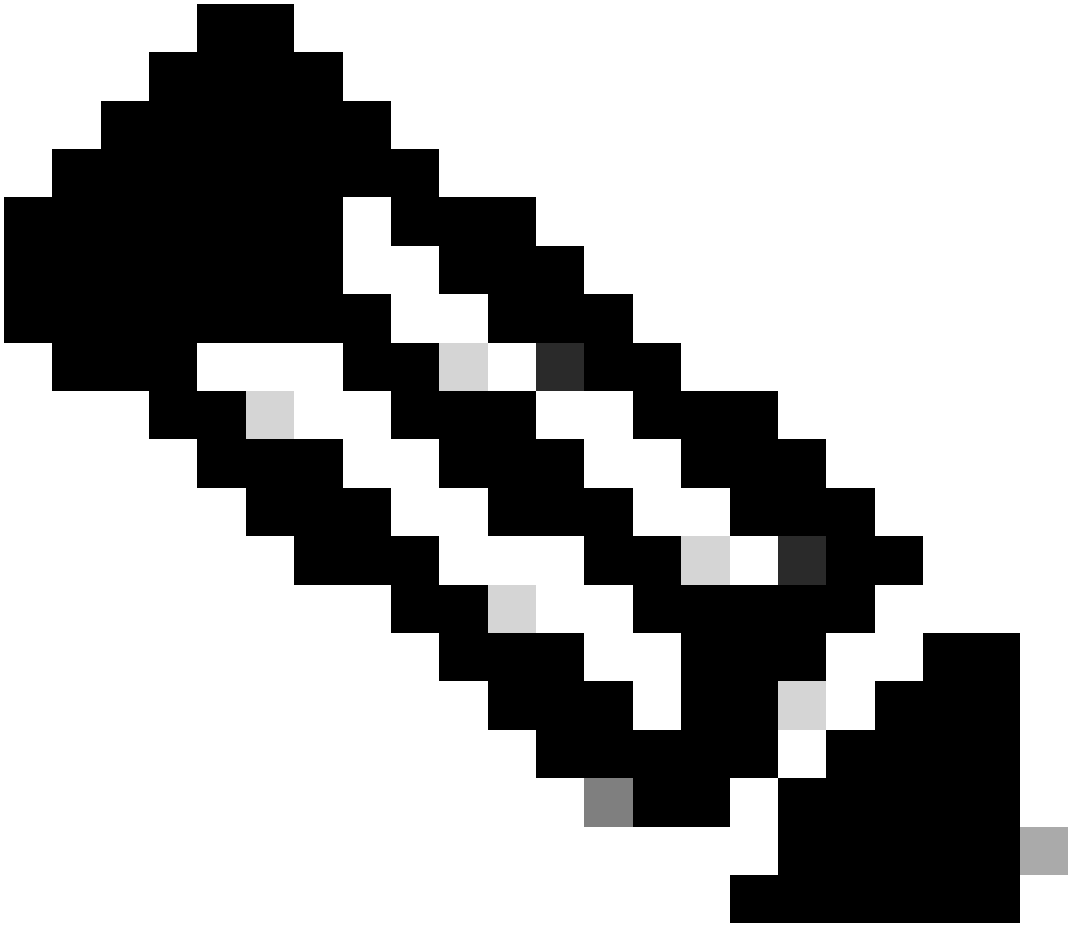
d.導航至Administration > Identity Management > Groups。



e.按一下User Identity Groups，然後按一下**Add**。

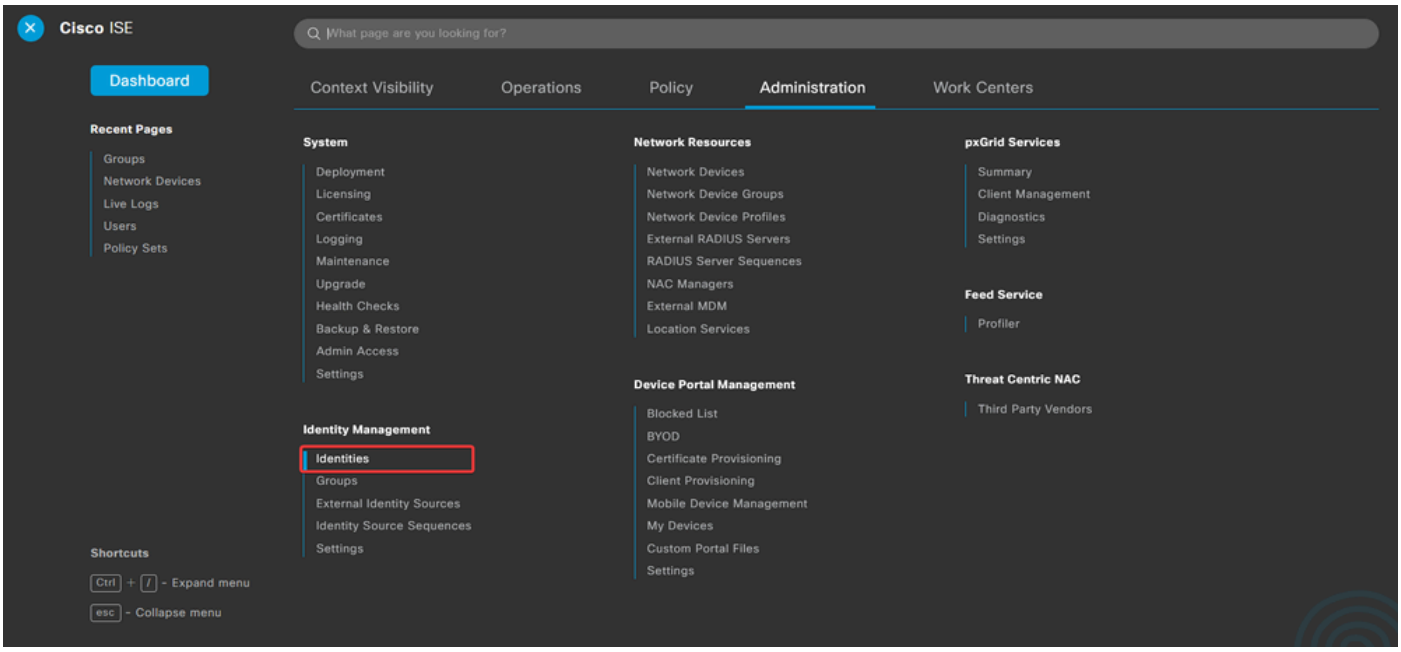
輸入group Name並按一下Submit。





注意：重複此步驟可根據需要建立任意多個組。

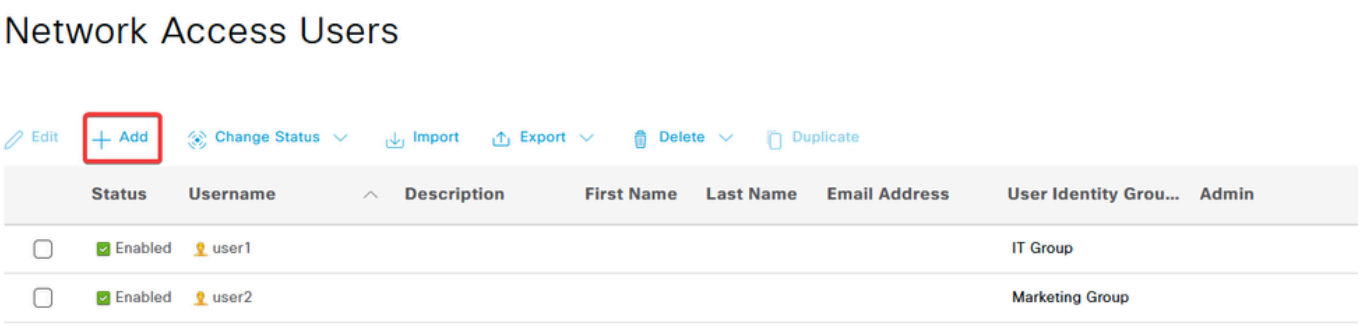
d.導航至**Administration > Identity Management > Identities**。

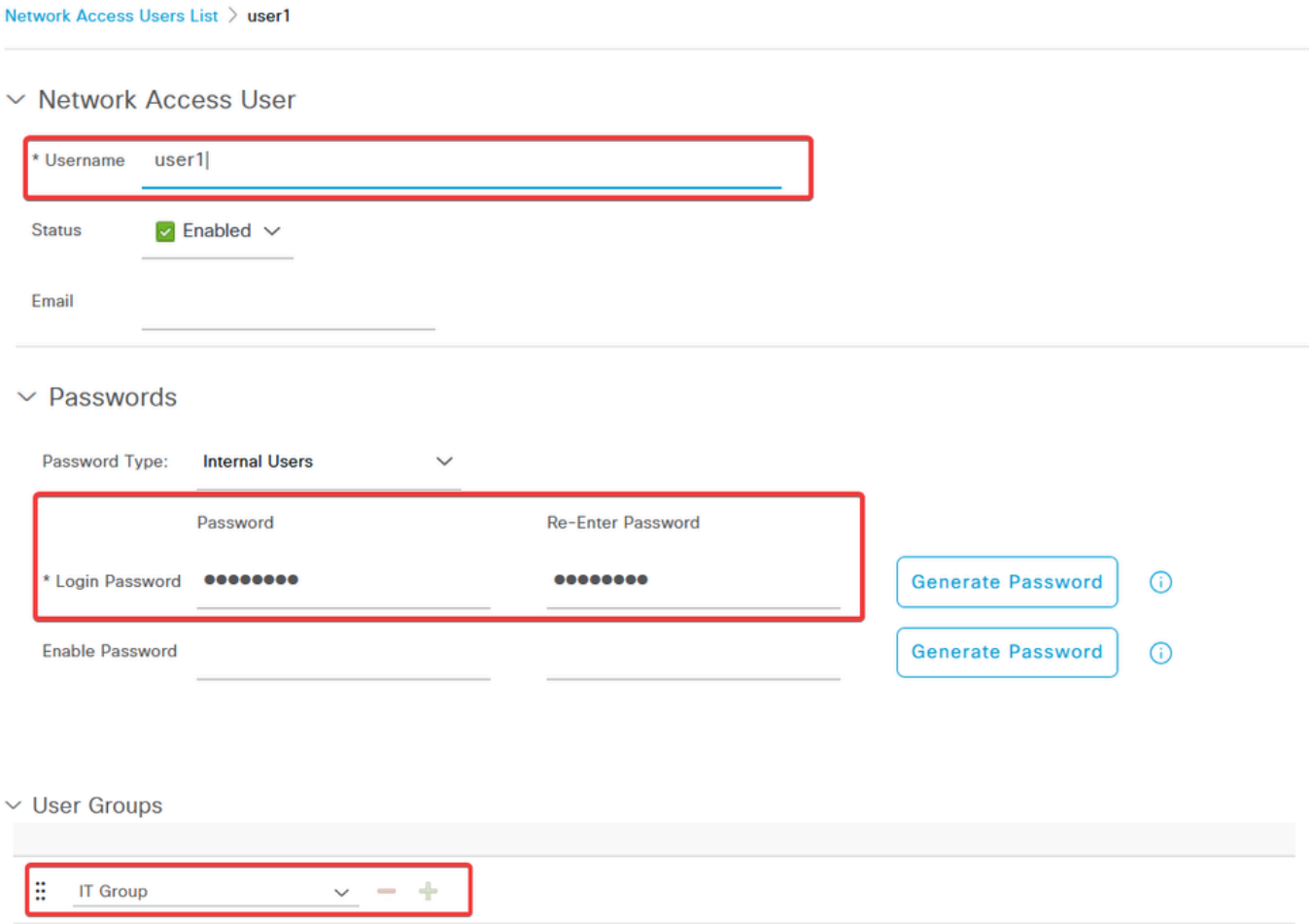


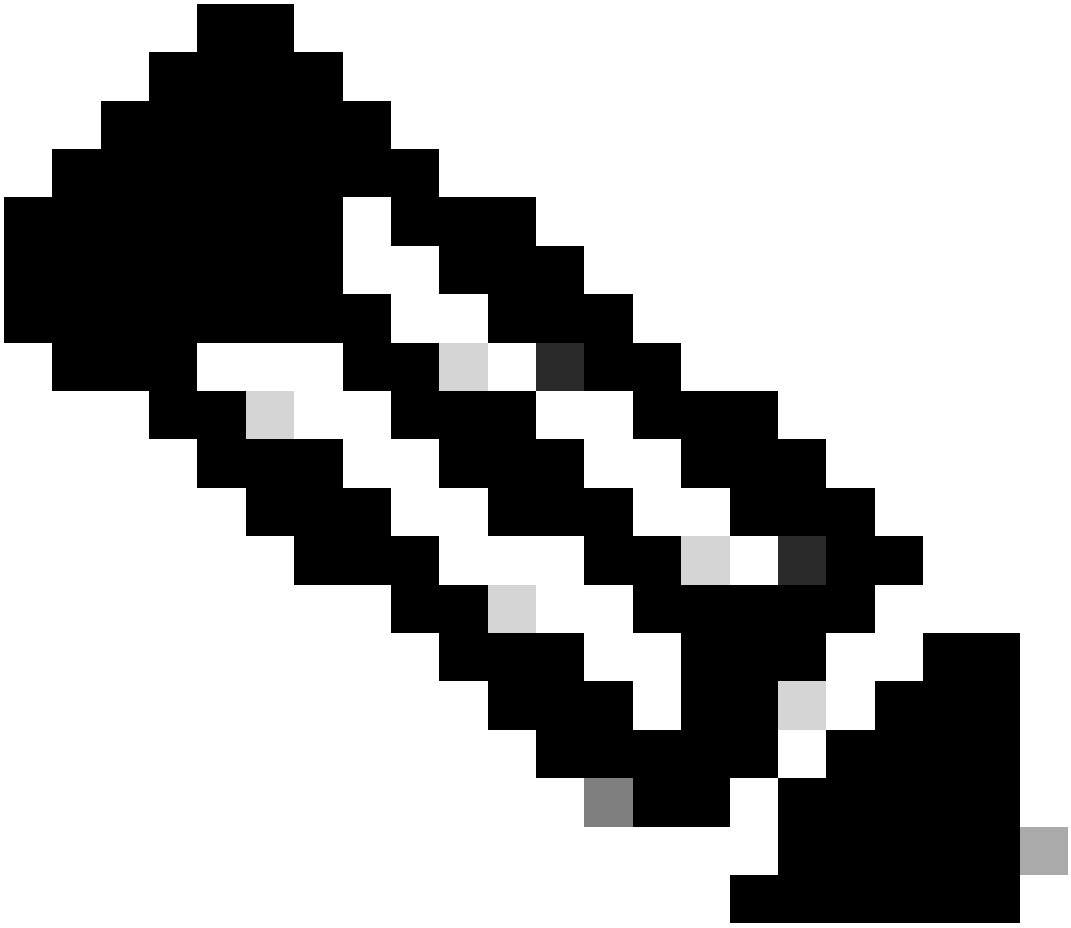
e.按一下Add，以便在伺服器本地資料庫中建立新使用者。

輸入Username和**Login Password**。然後，導航到此頁末尾，選擇User Group。

點選**Save**。

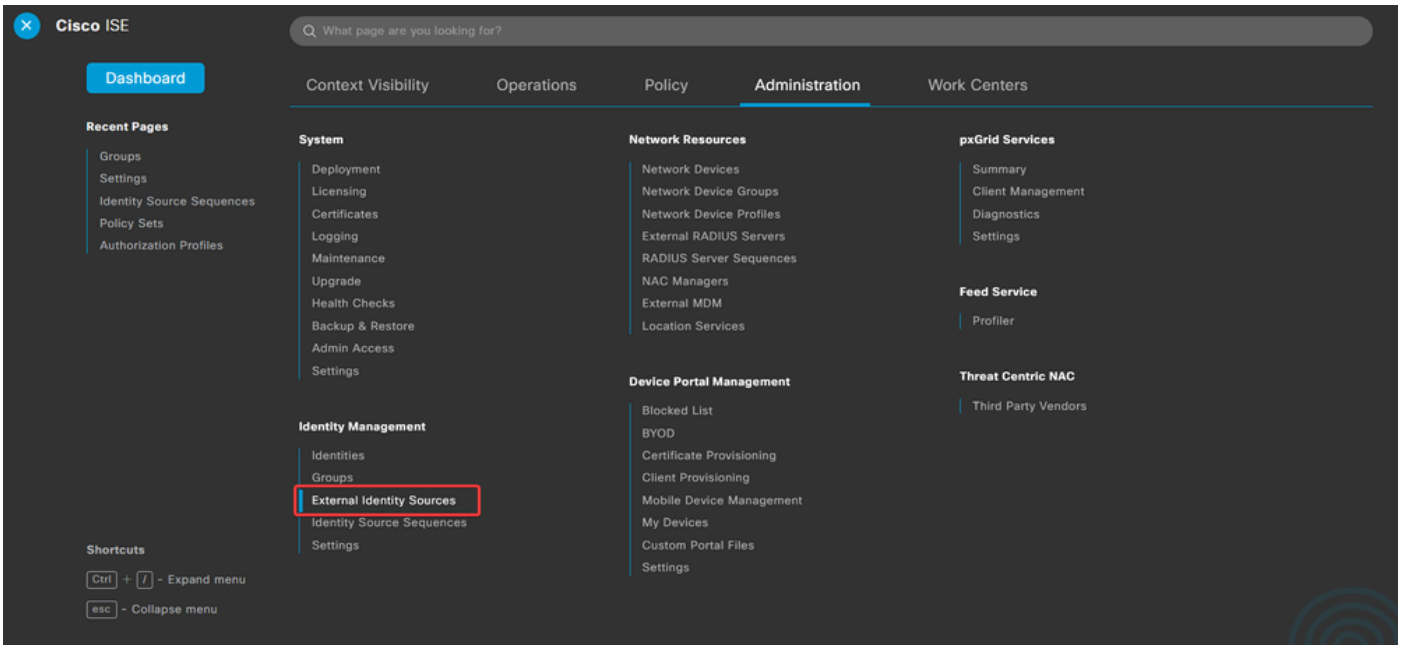



Network Access Users List
user1
Network Access User
* Username
user1
Status
Enabled
Email
Passwords
Password Type:
Internal Users
Password
Re-Enter Password
* Login Password
Generate Password
Enable Password
Generate Password
User Groups
IT Group



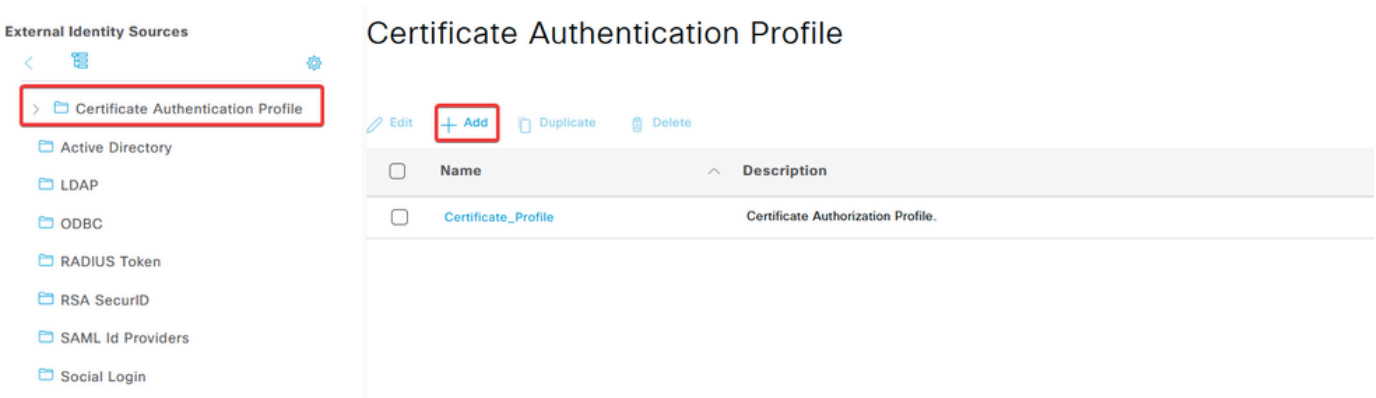
注意：必須配置使用者名稱和密碼才能建立內部使用者。即使在使用證書執行的RAVPN身份驗證中不需要此功能，這些使用者也可以用於其他需要密碼的內部服務。因此，請確保使用強密碼。

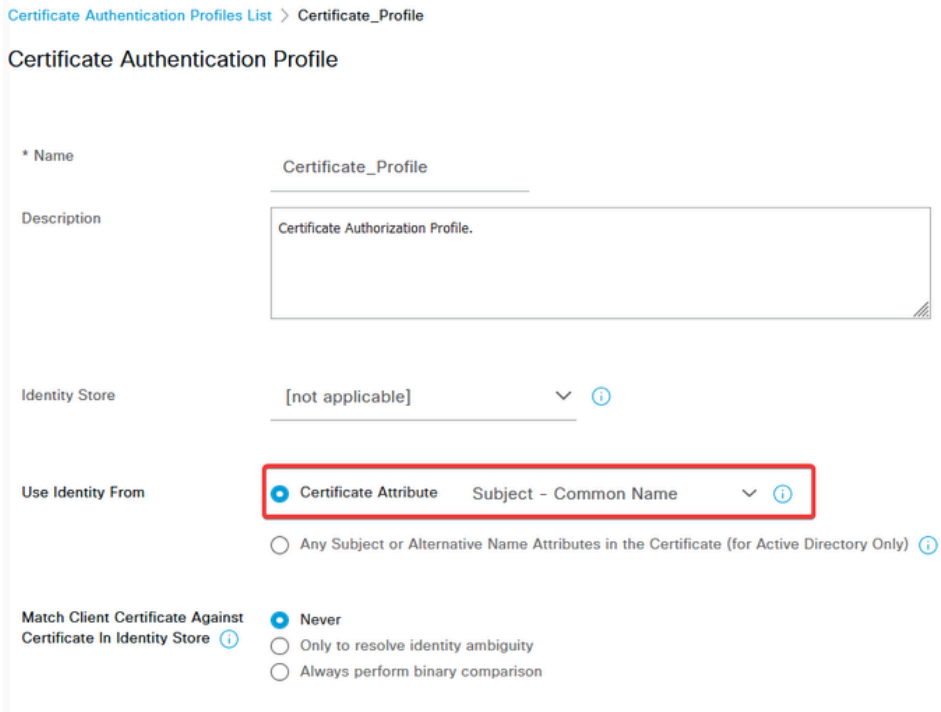
f.導航到**Administration > Identity Management > External Identify Sources**。



g.按一下Add建立**Certificate Authentication Profile**。

憑證驗證設定檔指定如何驗證使用者端憑證，包括可以檢查憑證中的哪些欄位（主體替代名稱、一般名稱等）。

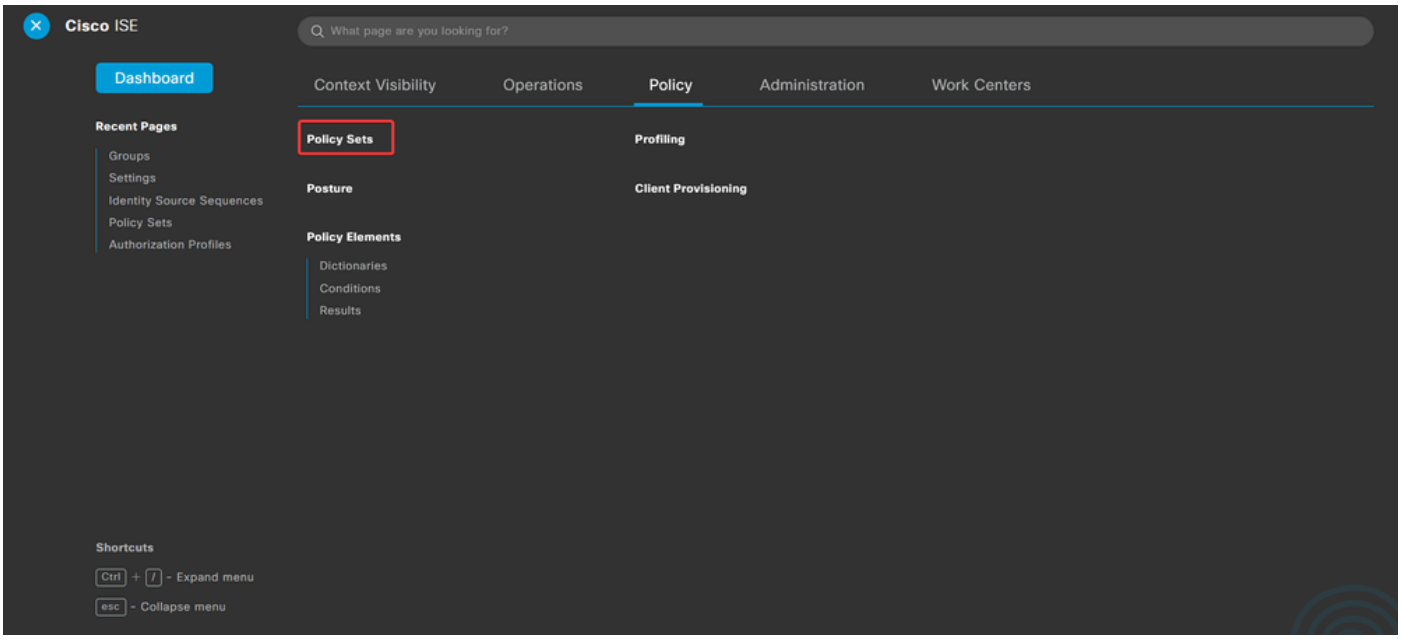




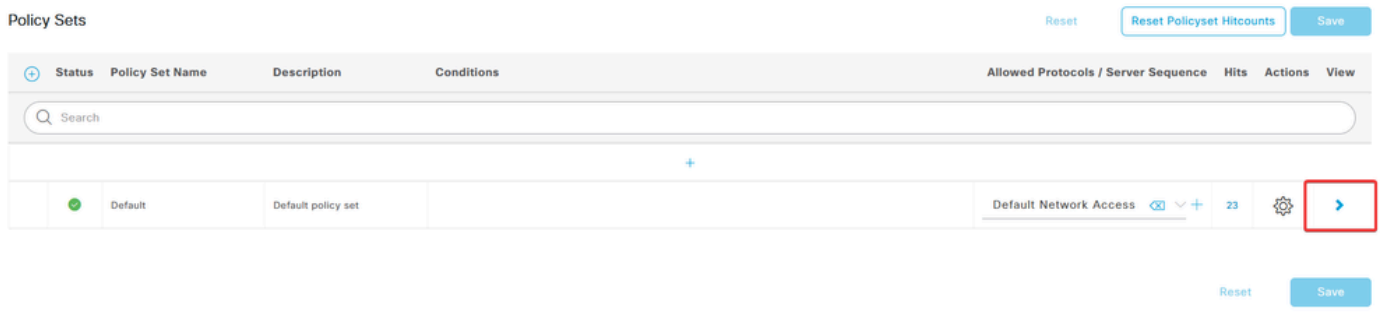
第3.2步：配置身份驗證策略

身份驗證策略用於驗證請求是否源自防火牆和特定連線配置檔案。

a.導航至**Policy > Policy Sets**。

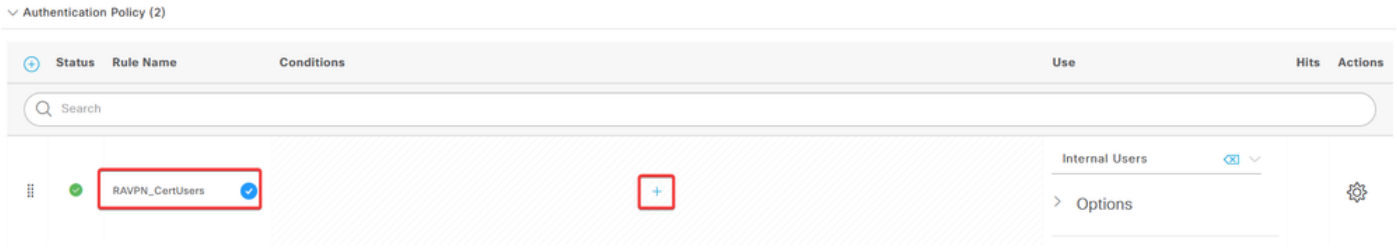


透過點選螢幕右側的箭頭選擇default authorization policy：

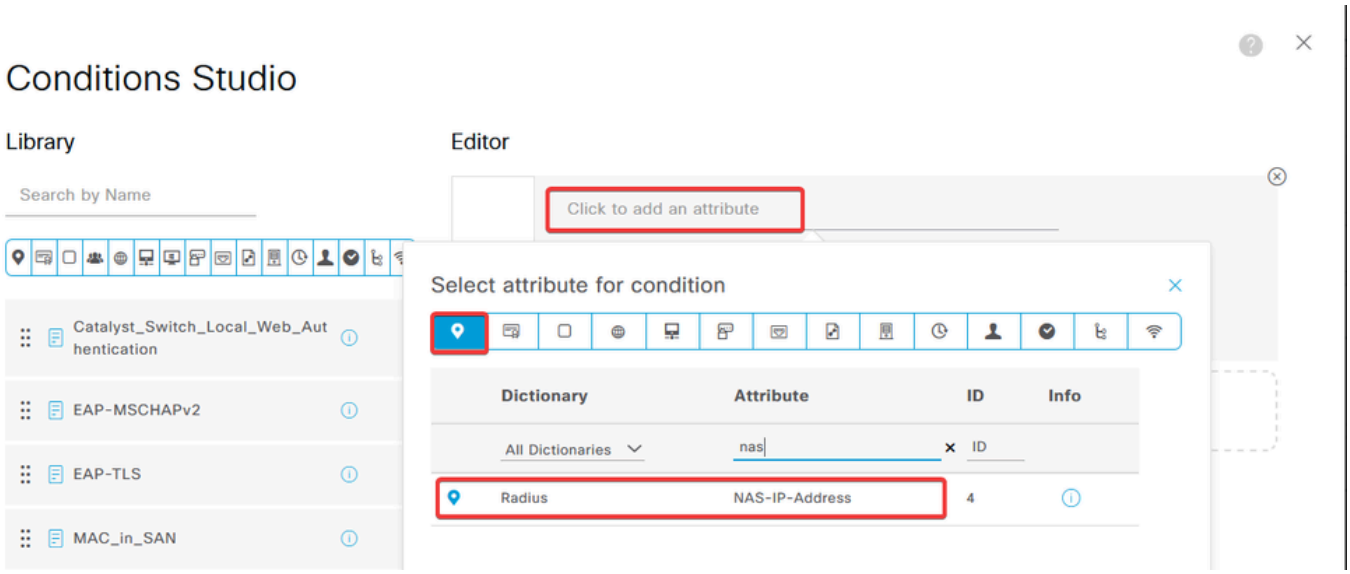


b.按一下Authentication Policy旁邊的下拉選單箭頭將其展開。然後，按一下**add (+)**圖示以增加新規則。

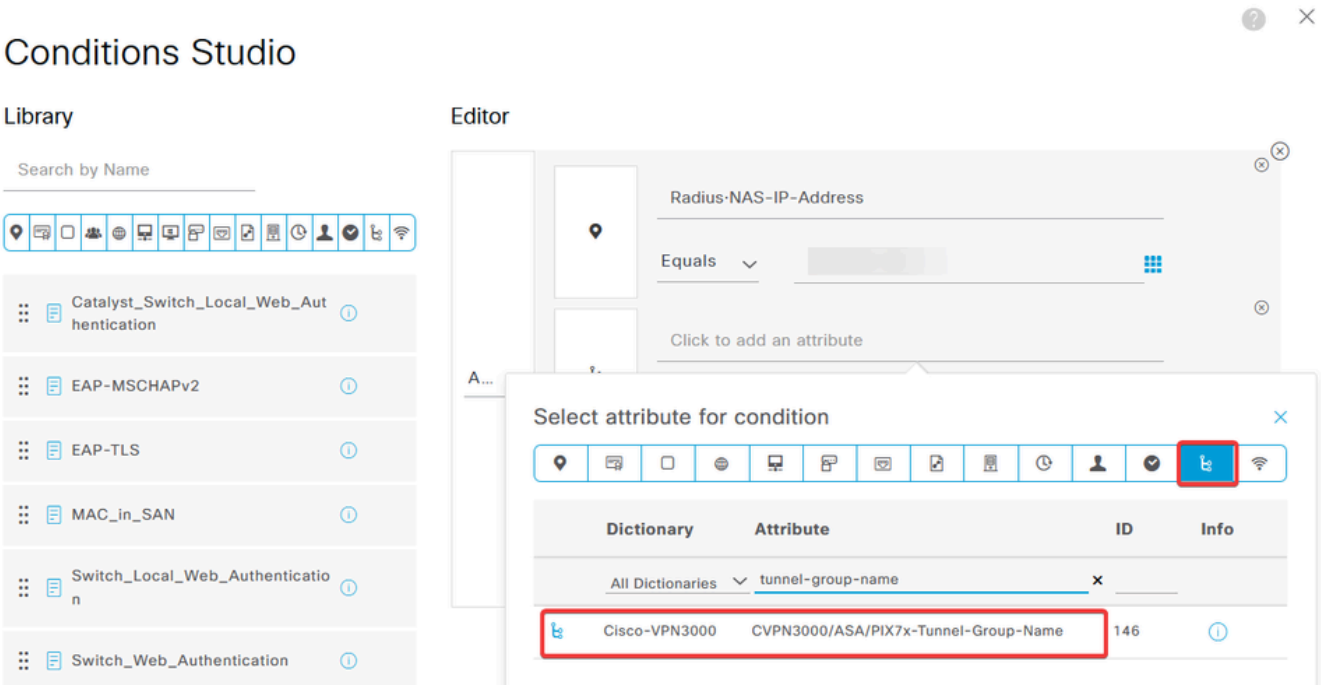
輸入規則的名稱，然後選擇條件列下的add (+)圖示。

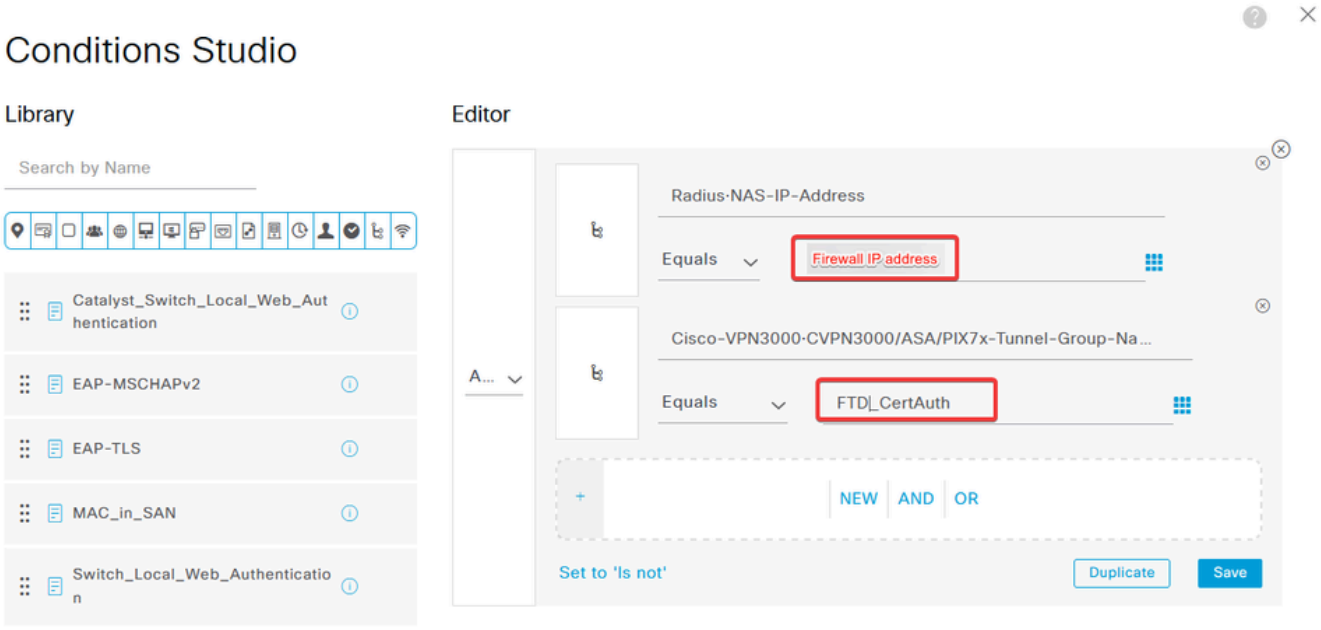


c.按一下屬性編輯器文本框並按一下NAS-IP-Address圖示。輸入防火牆的IP地址。

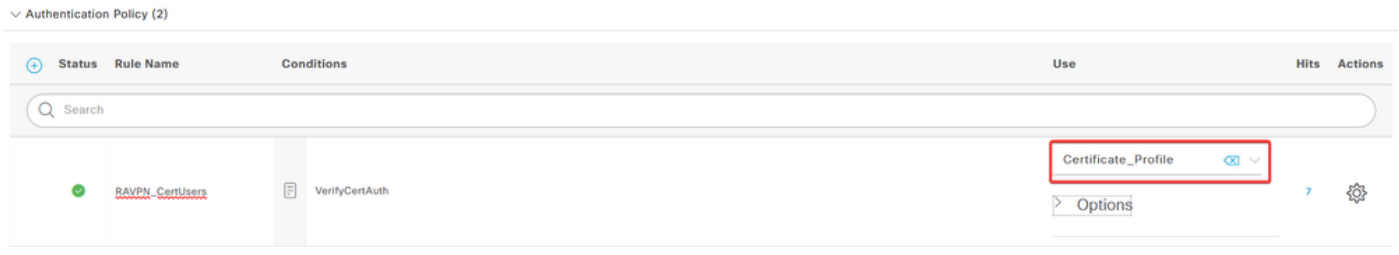


d.按一下**New**然後增加其他屬性Tunnel-Group-name。 Connection Profile 輸入在FMC上配置的名稱。





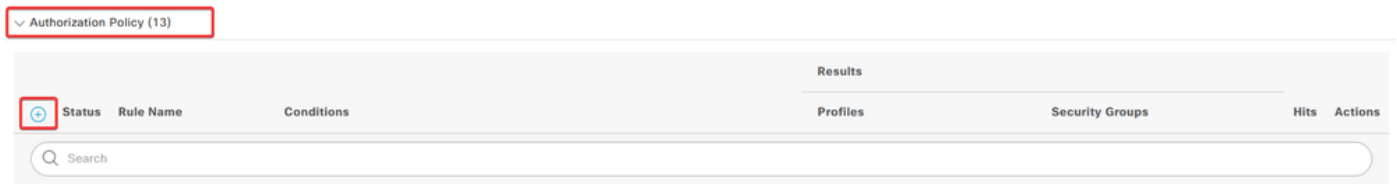
e.在「使用」列下，選擇已建立的**Certificate Authentication Profile**。藉由執行此動作，它會指定設定檔中定義用於辨識使用者的資訊。



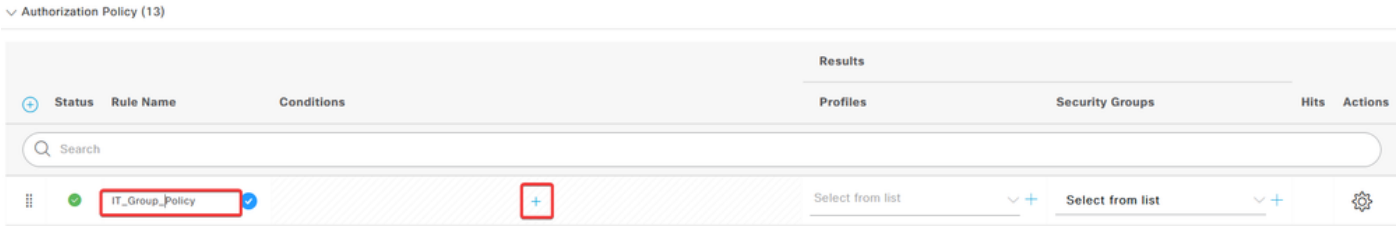
按一下Save。

第3.3步：配置授權策略

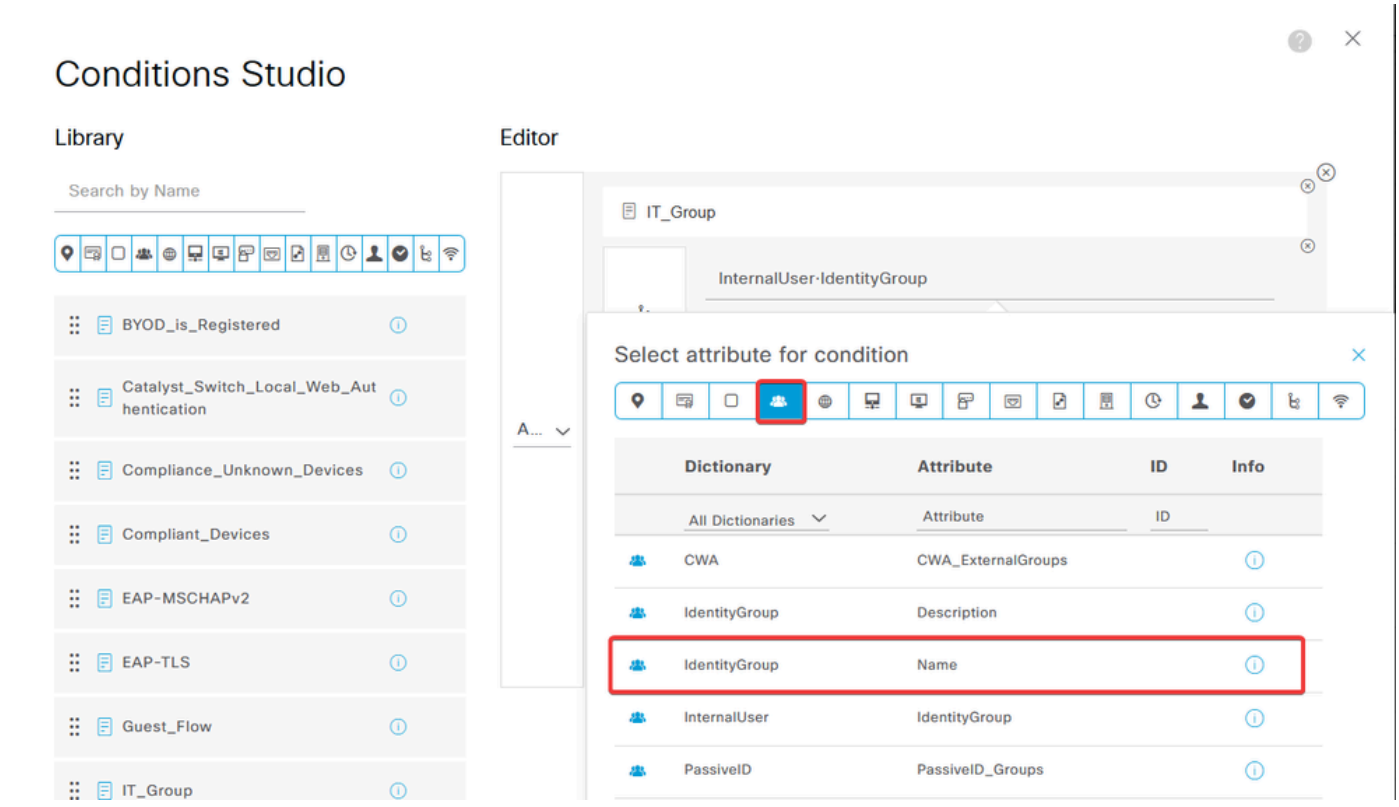
a.按一下Authorization Policy旁邊的下拉選單箭頭將其展開。然後，按一下**add (+)**圖示以增加新規則。



輸入規則的名稱，然後選擇條件列下的圖示**add (+)**。

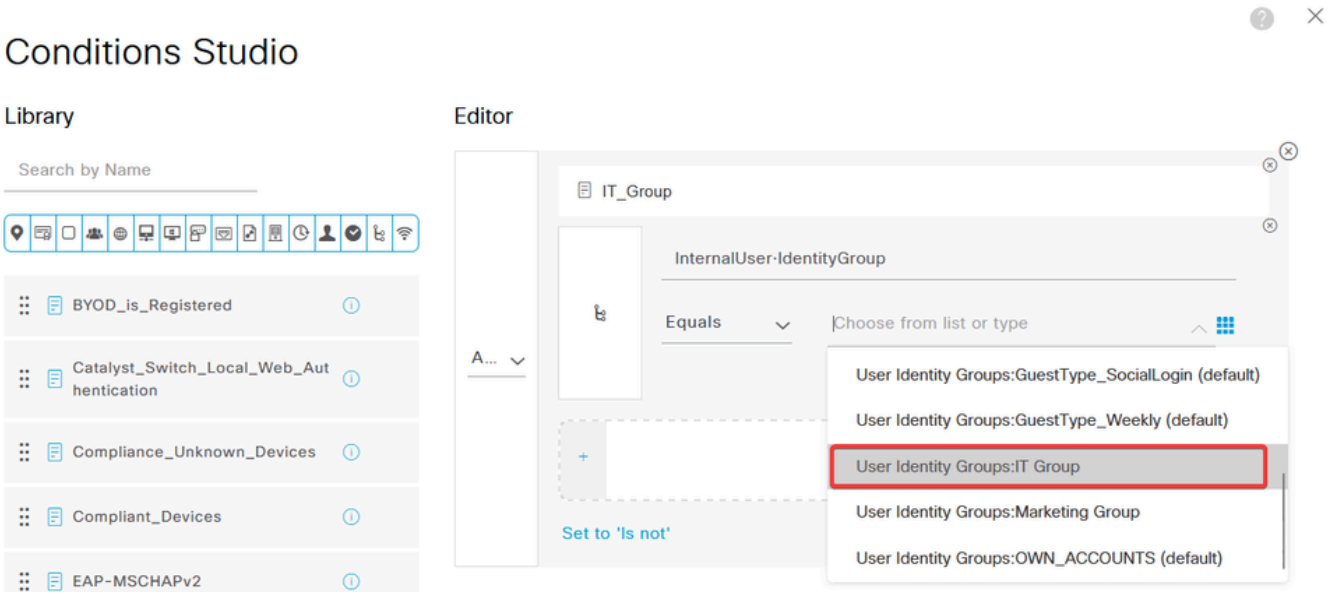


b.按一下屬性編輯器文本框並按一下Identity group圖示。選擇**Identity group - Name**屬性。

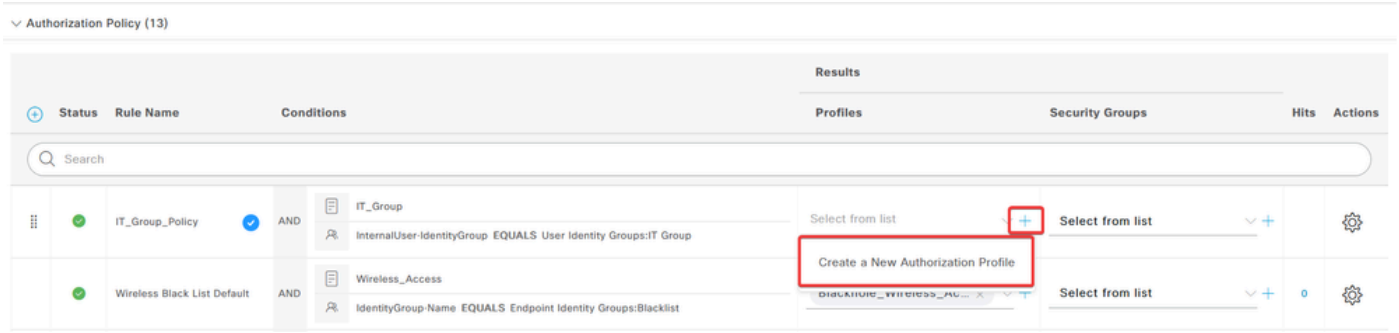


選擇Equals作為運算子，然後按一下下拉選單箭頭顯示可用選項並選擇**User Identity Groups:**

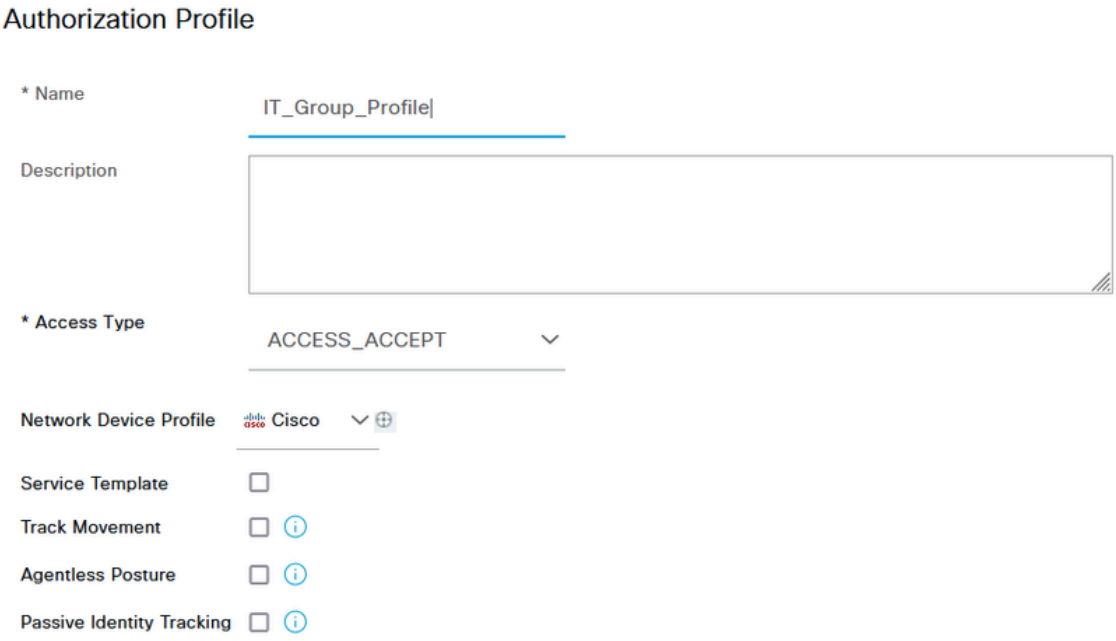
。



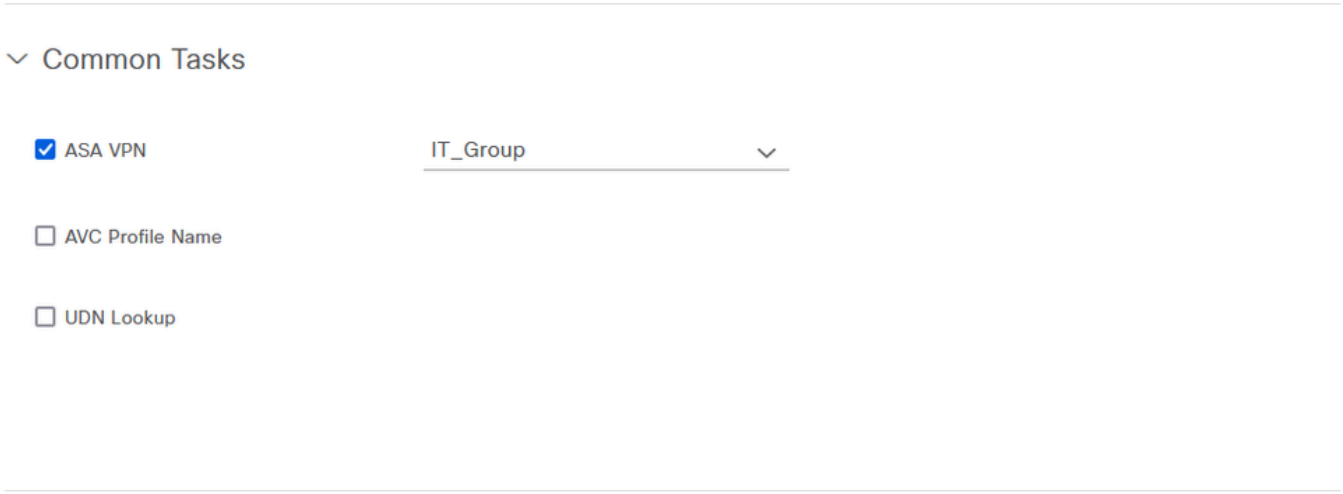
c.在配置檔案列中，按一下add (+)圖示並選擇**Create a New Authorization Profile**。



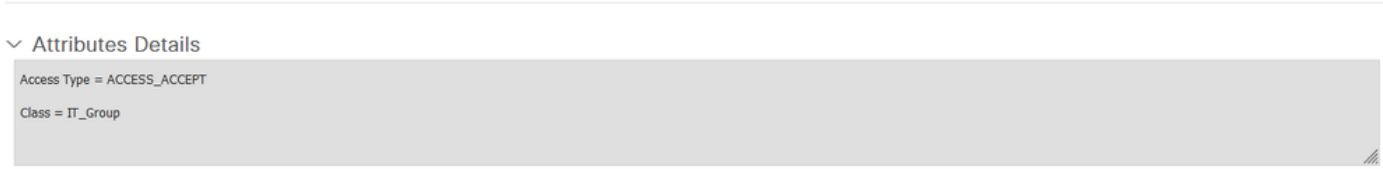
輸入profile **Name**。



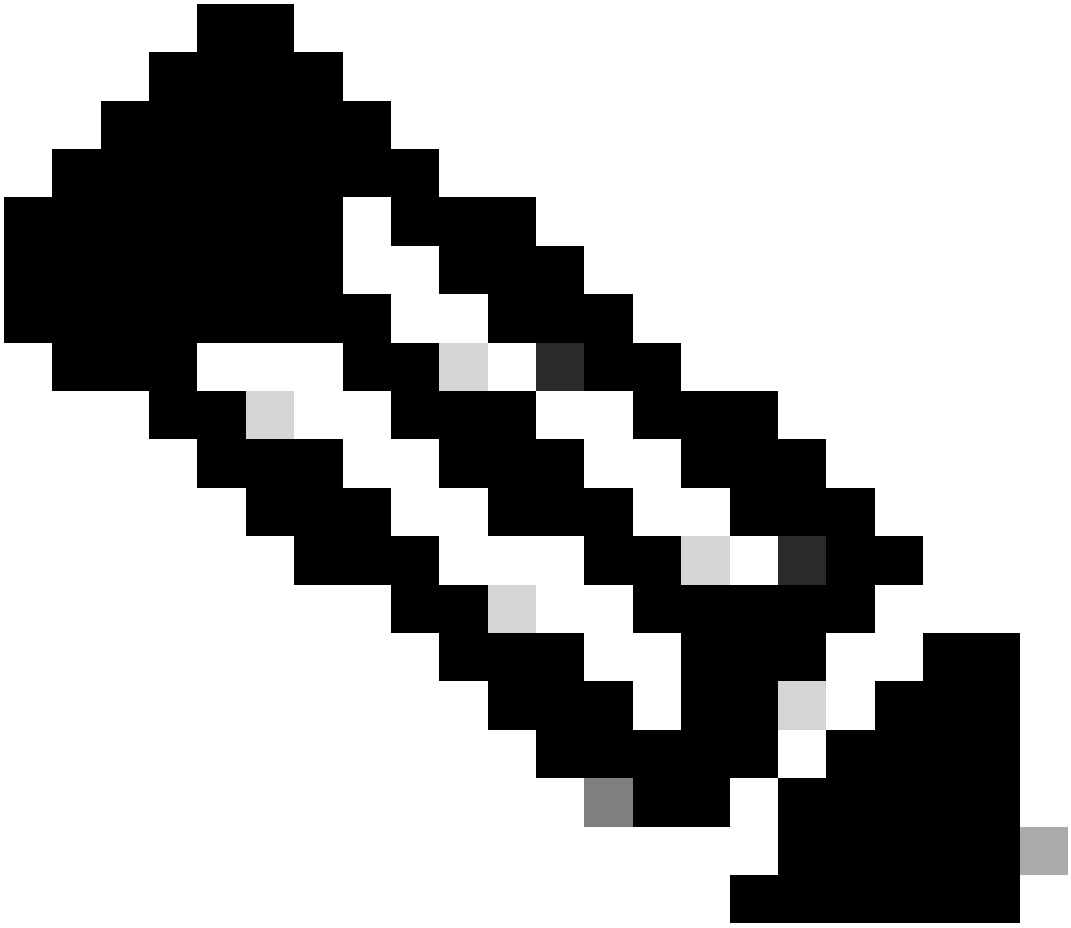
導航到**Common Tasks**並選中**ASA VPN**。然後，鍵入**group policy name**，該命令需要與FMC上建立的命令相同。



下一個屬性已指定給每個群組：



按一下Save。



注意：重複步驟3.3：為建立的每個組配置授權策略。

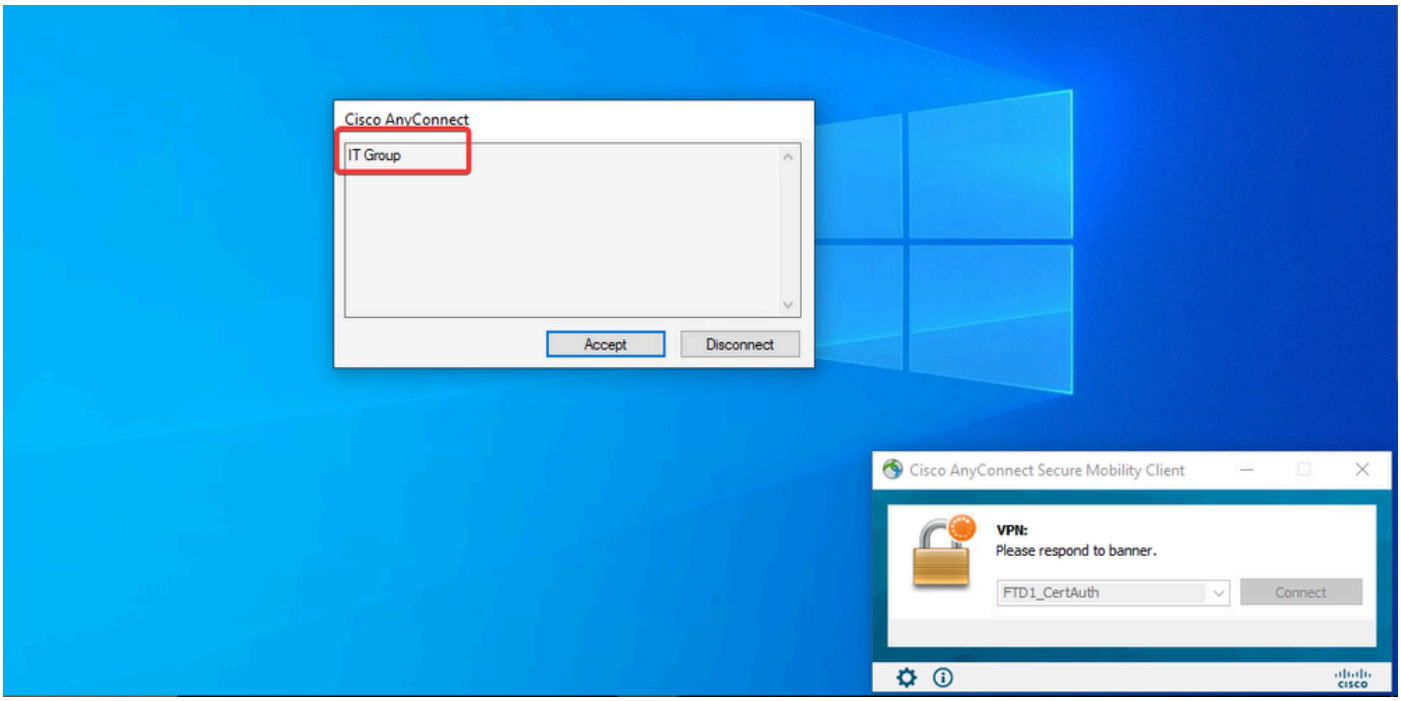
驗證

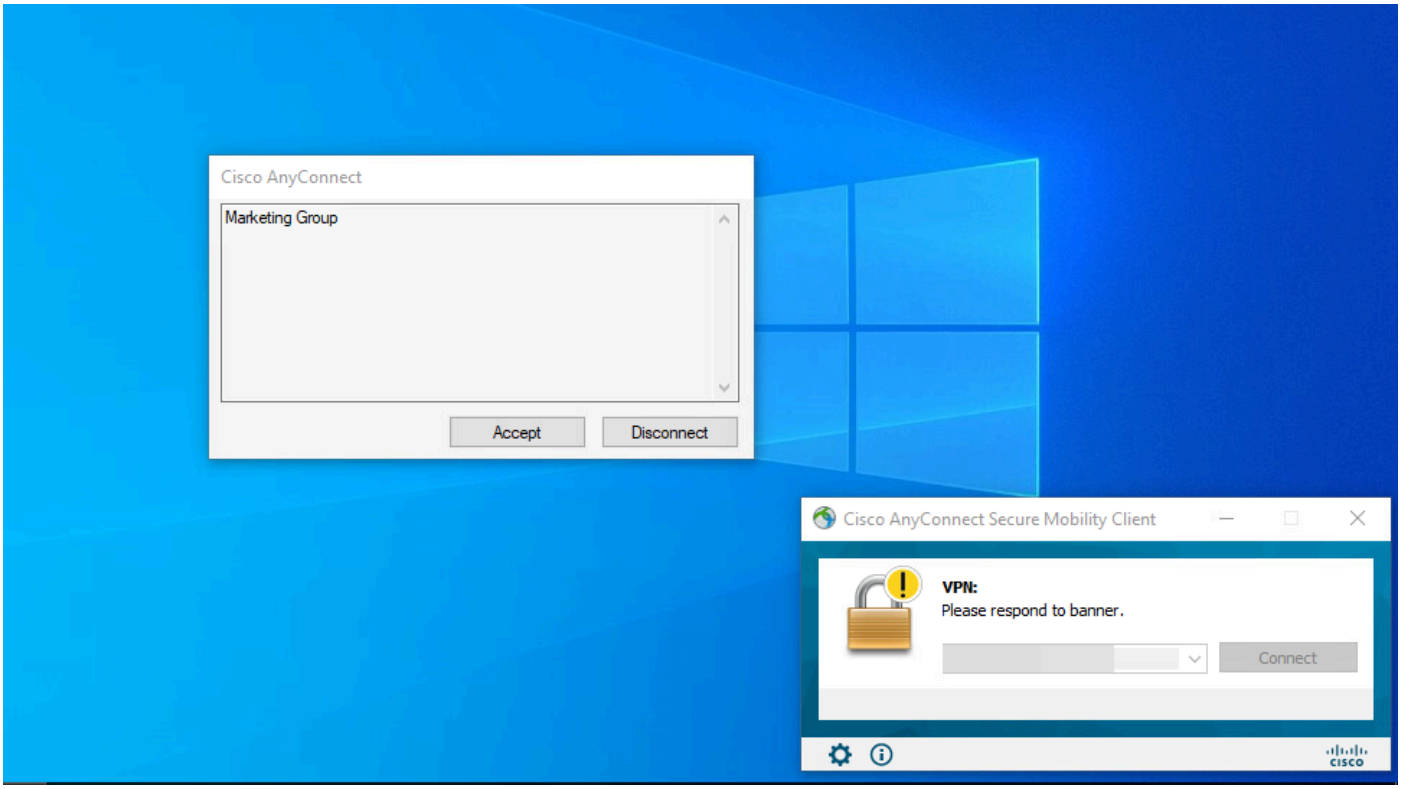
1. 運行命令show vpn-sessiondb anyconnect，並驗證使用者是否使用了正確的組策略。

```
<#root>

firepower#

show vpn-sessiondb anyconnect


Session Type : AnyConnect

Username     : user1

               Index        : 64
Assigned IP  : 192.168.55.2          Public IP    :
```

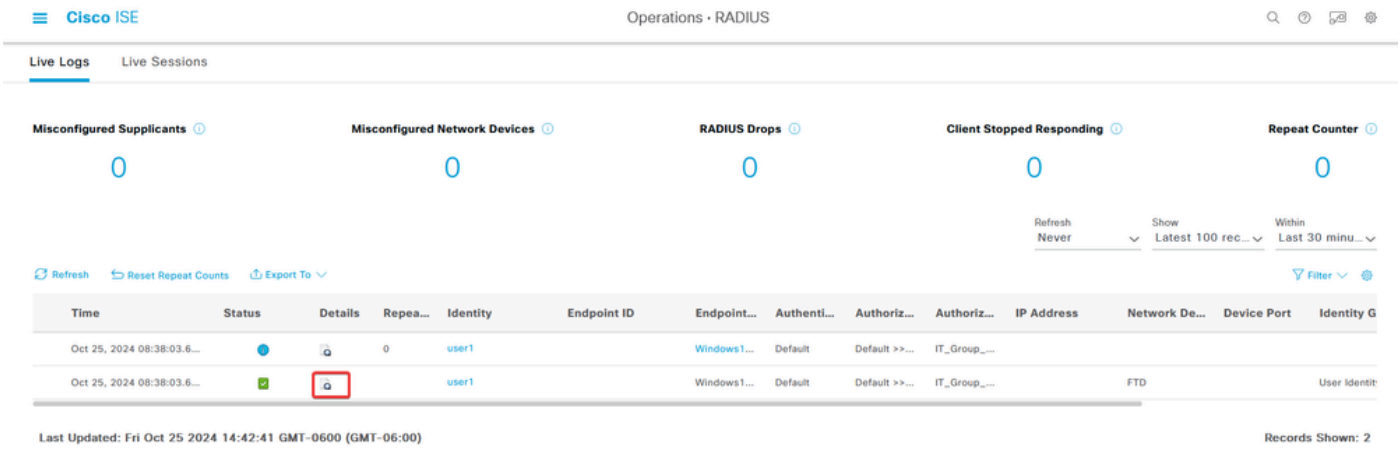
```
Protocol      : AnyConnect-Parent
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none
Hashing       : AnyConnect-Parent: (1)none
Bytes Tx      : 15084                 Bytes Rx     : 99611

Group Policy  : IT_Group              Tunnel Group : FTD_CertAuth


Login Time    : 22:21:43 UTC Tue Oct 22 2024
Duration      : 3h:03m:50s
Inactivity    : 0h:41m:44s
VLAN Mapping  : N/A                   VLAN         : none
Audt Sess ID  : 96130a0f0004000067182577
Security Grp  : none                  Tunnel Zone  : 0


Username      : User2

                  Index        : 70
Assigned IP   : 192.168.55.3          Public IP    :
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx      : 15112                 Bytes Rx     : 19738

Group Policy  : Marketing_Group       Tunnel Group : FTD_CertAuth


Login Time    : 01:23:08 UTC Wed Oct 23 2024
Duration      : 0h:02m:25s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                   VLAN         : none
Audt Sess ID  : 96130a0f0004600067184ffc
Security Grp  : none                  Tunnel Zone  : 0

firepower#
```

2. 在組策略中，可以配置當使用者成功連線時顯示的標語消息。每個標語都可用於標識具有授權的組。





3. 在即時日誌中，驗證連線是否使用適當的授權策略。按一下Details並顯示Authentication Report。



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. 可以從CSF的診斷CLI運行調試以進行證書身份驗證。

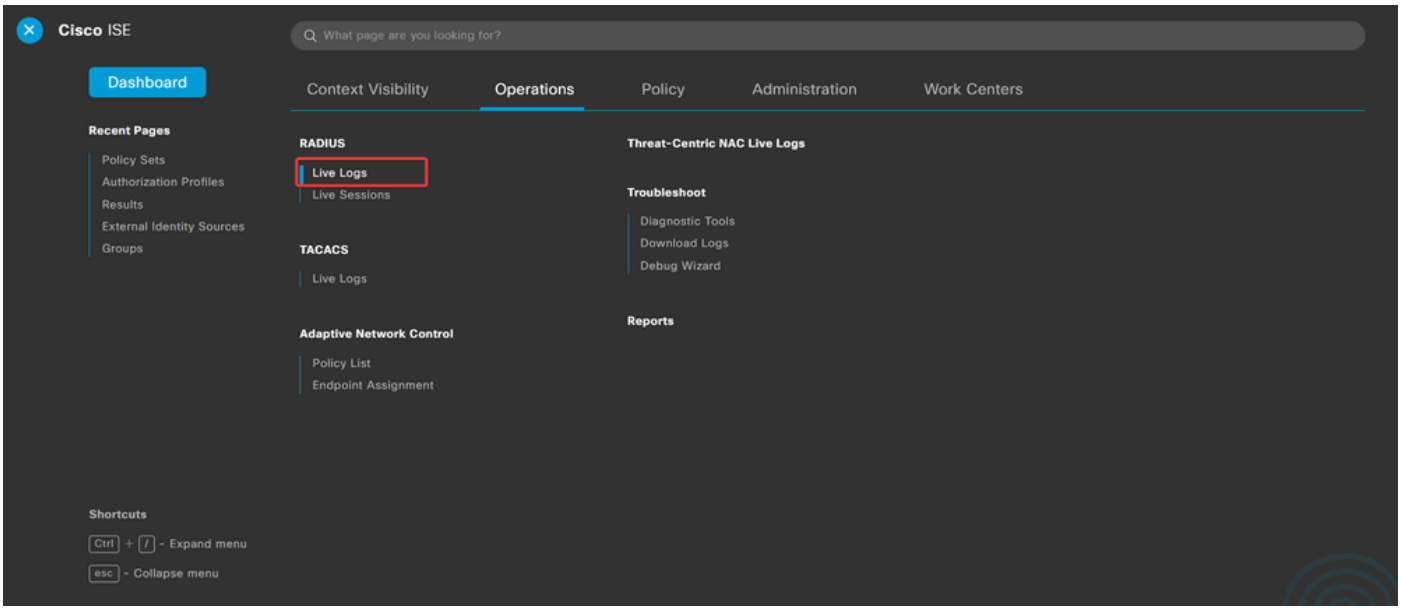
```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

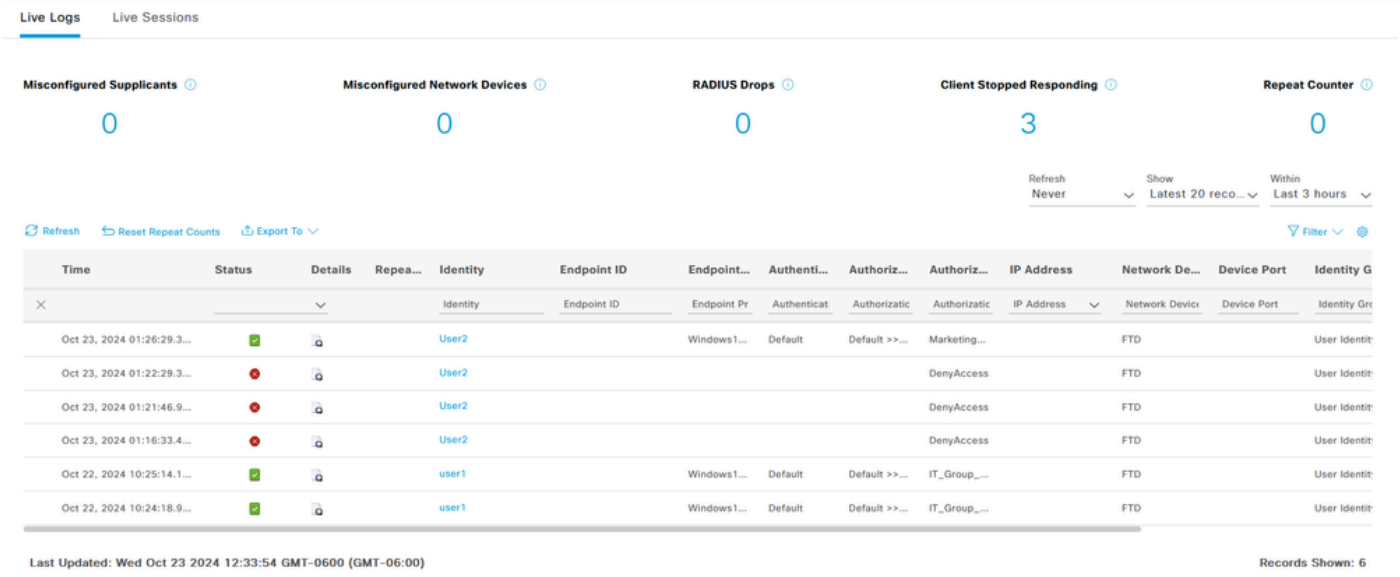
2. 使用AAA調試驗證本地和/或遠端屬性的分配。

```
debug aaa common 255
debug aaa shim 255
debug aaa authentication
debug aaa authorization
debug radius all
```

在ISE上：

1. 定位至Operations > RADIUS > Live Logs。


Cisco ISE
What page are you looking for?
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Recent Pages
Policy Sets
Authorization Profiles
Results
External Identity Sources
Groups
RADIUS
Live Logs
Live Sessions
TACACS
Live Logs
Adaptive Network Control
Policy List
Endpoint Assignment
Threat-Centric NAC Live Logs
Troubleshoot
Diagnostic Tools
Download Logs
Debug Wizard
Reports
Shortcuts
Ctrl + / - Expand menu
esc - Collapse menu


Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
3
Repeat Counter
0
Refresh
Never
Show
Latest 20 reco...
Within
Last 3 hours
Refresh
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repea...
Identity
Endpoint ID
Endpoint...
Authenti...
Authoriz...
Authoriz...
IP Address
Network De...
Device Port
Identity G
Oct 23, 2024 01:26:29.3... User2 Windows1... Default Default >>... Marketing... FTD User Identit
Oct 23, 2024 01:22:29.3... User2 DenyAccess FTD User Identit
Oct 23, 2024 01:21:46.9... User2 DenyAccess FTD User Identit
Oct 23, 2024 01:16:33.4... User2 DenyAccess FTD User Identit
Oct 22, 2024 10:25:14.1... user1 Windows1... Default Default >>... IT_Group_... FTD User Identit
Oct 22, 2024 10:24:18.9... user1 Windows1... Default Default >>... IT_Group_... FTD User Identit
Last Updated: Wed Oct 23 2024 12:33:54 GMT-0600 (GMT-06:00)
Records Shown: 6

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）。