

設定SSL安全使用者端在FTD上使用本機驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[組態](#)

[步驟 1. 驗證授權](#)

[步驟 2. 將思科安全客戶端軟體套件上傳到FMC](#)

[步驟 3. 生成自簽名證書](#)

[步驟 4. 在FMC上建立本機範圍](#)

[步驟 5. 配置SSL Cisco Secure Client](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹如何在思科FMC管理的思科FTD上使用本地身份驗證配置思科安全客戶端 (包括 Anyconnect) 。

必要條件

需求

思科建議您瞭解以下主題：

- [透過Firepower管理中心\(FMC\)配置SSL安全客戶端](#)
- [透過FMC配置Firepower對象](#)
- [Firepower上的SSL證書](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Firepower威脅防禦(FTD) 7.0.0版 (內部版本94)
- Cisco FMC 7.0.0版 (內部版本94)
- 思科安全行動化使用者端4.10.01075

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。

背景資訊

在本範例中，安全通訊端層(SSL)用於在FTD和Windows 10使用者端之間建立虛擬私人網路(VPN)。

自7.0.0版起，由FMC管理的FTD支援思科安全使用者端的本機驗證。這可以定義為主要驗證方法，或者在主要方法失敗時作為回退。在本示例中，本地身份驗證被配置為主身份驗證。

在此軟體版本之前，FTD上的思科安全客戶端本地身份驗證僅在思科Firepower裝置管理器(FDM)中可用。

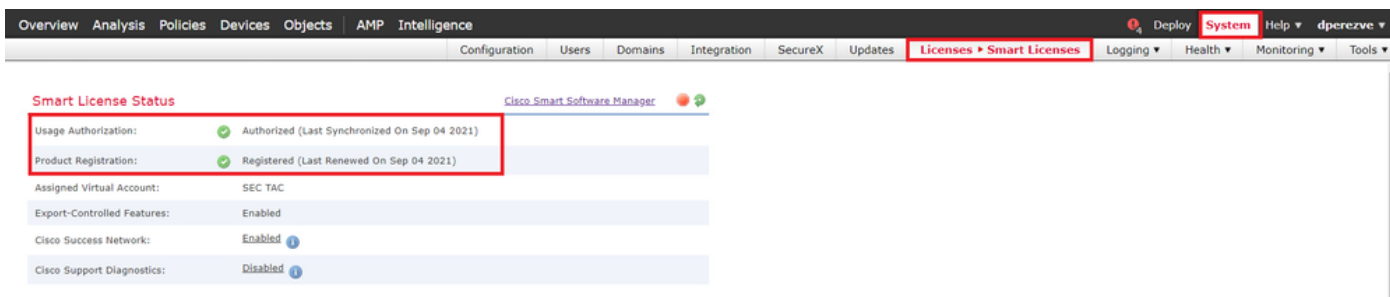
設定

組態

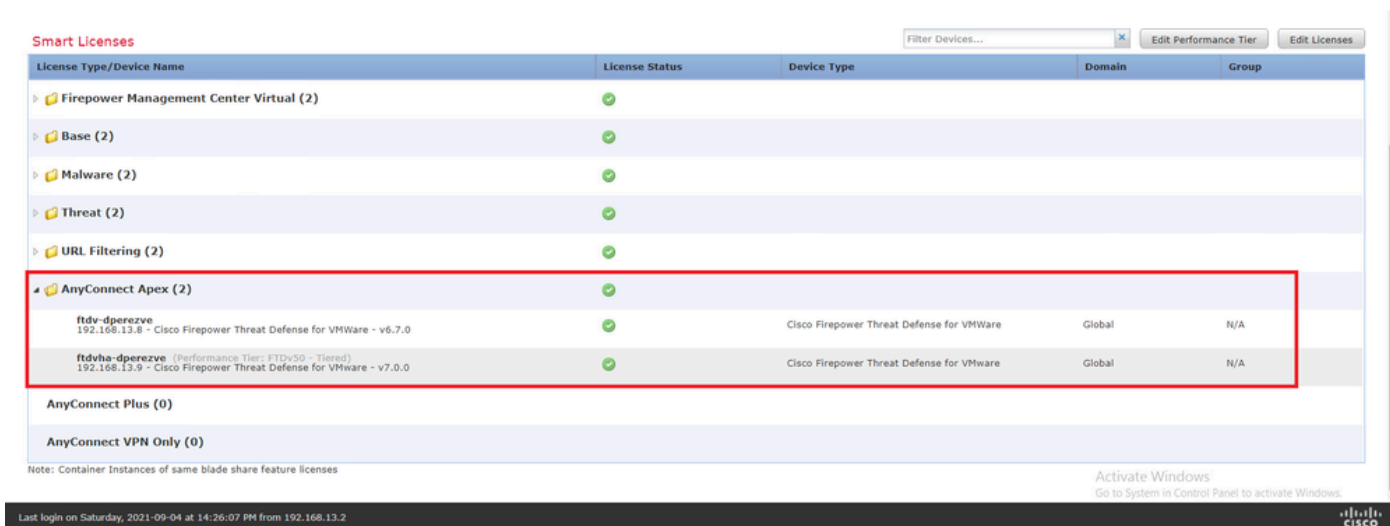
步驟 1. 驗證授權

在配置思科安全客戶端之前，FMC必須已註冊並符合智慧許可門戶的要求。如果FTD沒有有效的Plus、Apex或僅VPN許可證，則無法部署思科安全客戶端。

導航到系統>許可證>智慧許可證，確保FMC已註冊並符合智慧許可門戶要求：



























在同一頁上向下滾動。在智慧許可證圖表底部，您可以看到不同型別的可用思科安全客戶端(AnyConnect)許可證和每個許可證訂購的裝置。確保手頭的FTD已註冊為以下任一類別：

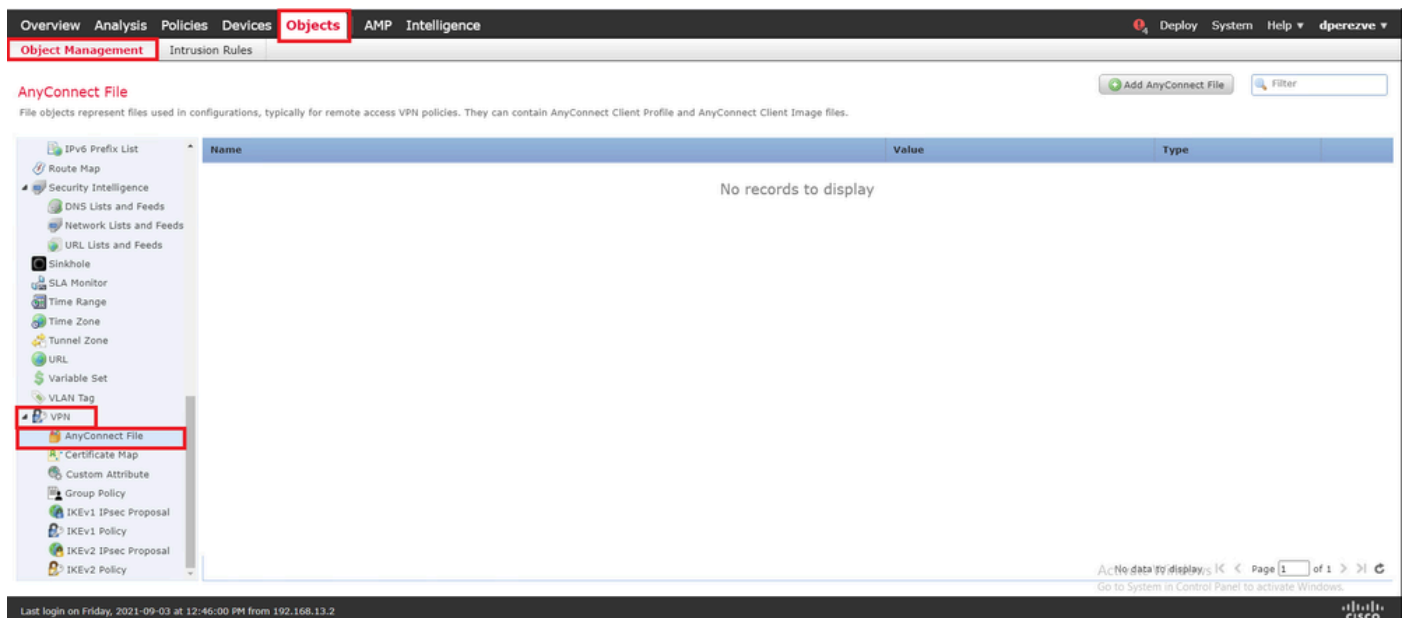


步驟 2.將Cisco安全客戶端軟體套件上傳到FMC

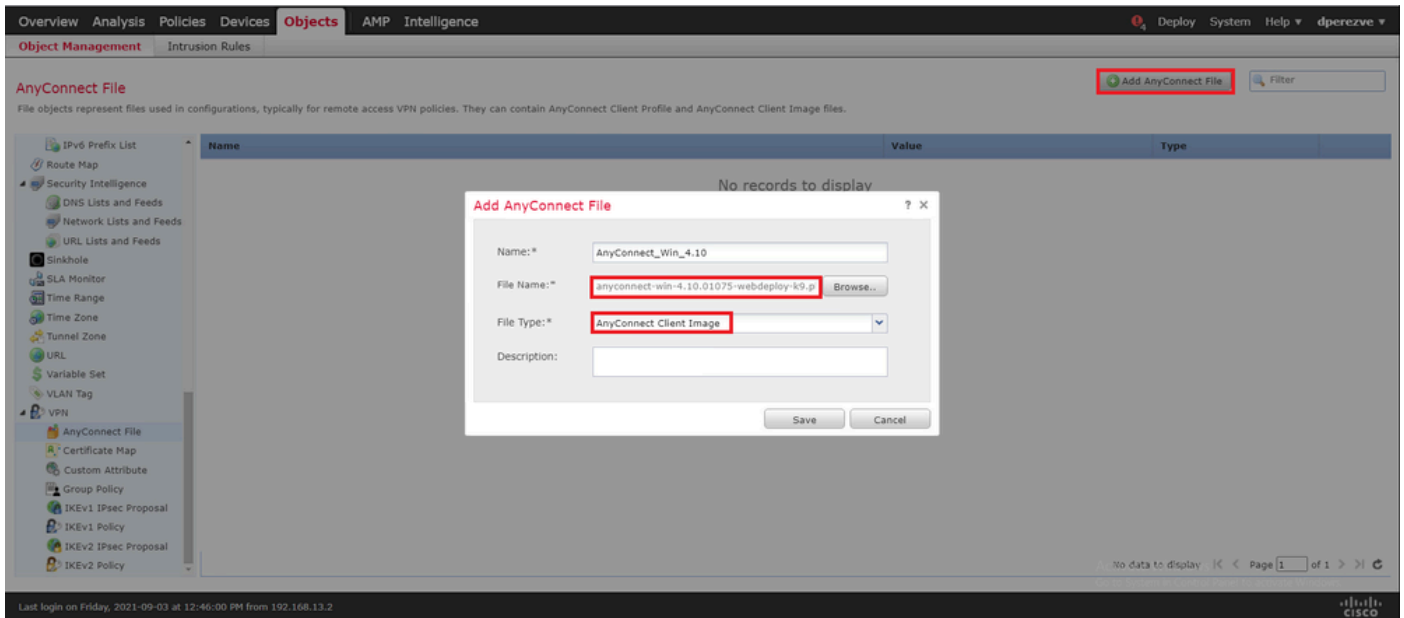
從cisco.com下載適用於Windows的Cisco安全客戶端(AnyConnect)頭端部署軟體套件：

Application Programming Interface [API] (Windows)  anyconnect-win-4.10.01075-vpnapi.zip Advisories 	21-May-2021	141.72 MB	 
AnyConnect Headend Deployment Package (Windows)  anyconnect-win-4.10.01075-webdeploy-k9.pkg Advisories 	21-May-2021	77.81 MB	 
AnyConnect Pre-Deployment Package (Windows 10 ARM64) - includes individual MSI files  anyconnect-win-arm64-4.10.01075-predeploy-k9.zip Advisories 	21-May-2021	34.78 MB	 
AnyConnect Headend Deployment Package (Windows 10 ARM64)  anyconnect-win-arm64-4.10.01075-webdeploy-k9.pkg Advisories 	21-May-2021	44.76 MB	 
Profile Editor (Windows)  tools-anyconnect-win-4.10.01075-profileeditor-k9.msi Advisories 	21-May-2021	10.90 MB	 
AnyConnect Installer Transforms (Windows)  tools-anyconnect-win-4.10.01075-transforms.zip Advisories 	21-May-2021	0.05 MB	 

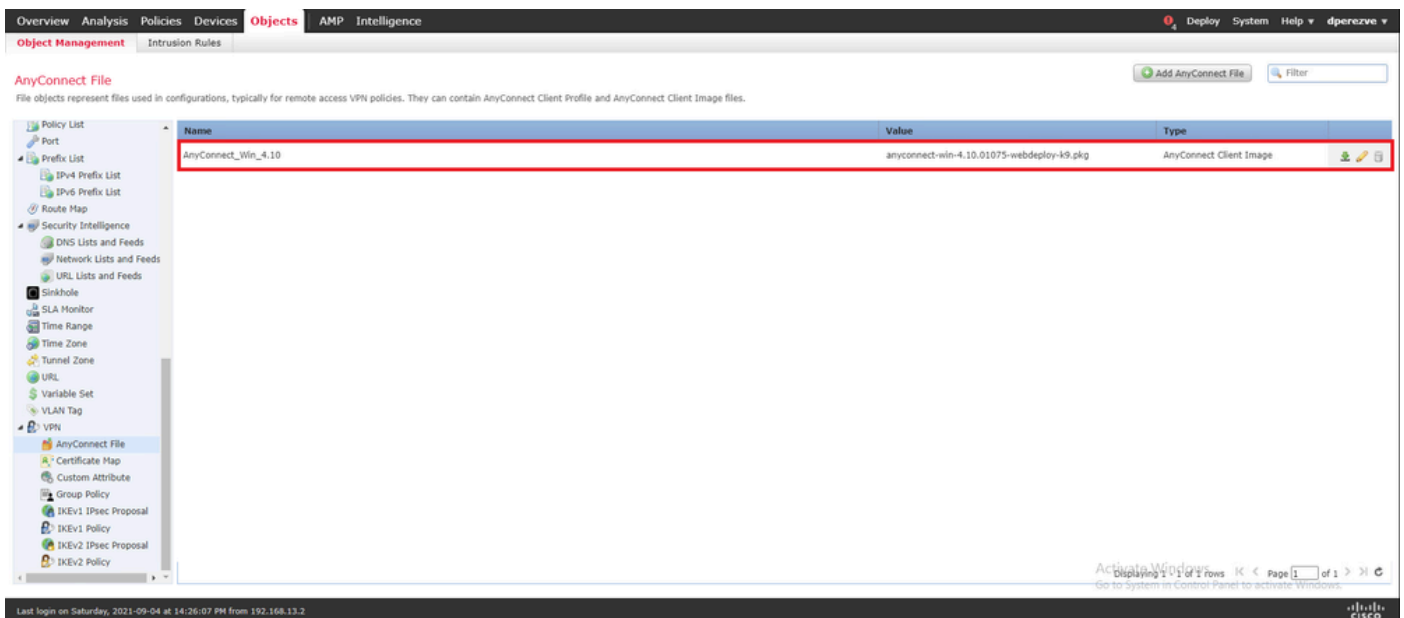
要上傳Cisco Secure Client映像，請導航到對象>對象管理，並在目錄中的VPN類別下選擇Cisco Secure Client File：



選擇Add AnyConnect File按鈕。在增加AnyConnect安全客戶端檔案窗口中，為對象指定名稱，然後選擇瀏覽.....以選擇Cisco安全客戶端軟體套件。最後，在下拉選單中選擇AnyConnect Client Image作為檔案型別：



選擇Save按鈕。必須將物件加入物件清單：



步驟 3.生成自簽名證書

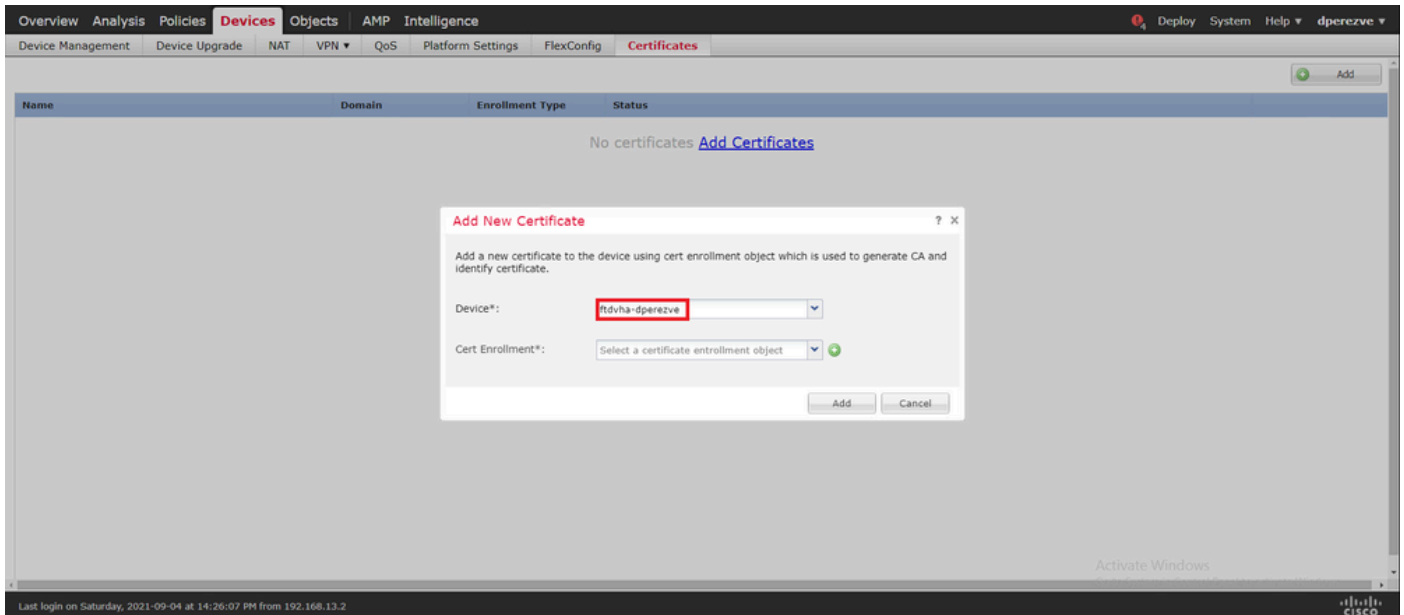
SSL思科安全客戶端(AnyConnect)要求在VPN頭端和客戶端之間的SSL握手中使用一個有效證書。

附註：在此範例中，會為此用途產生自簽章憑證。此外，除了自簽憑證之外，還以上傳由內部憑證授權單位(CA)或公認的CA簽署的憑證。

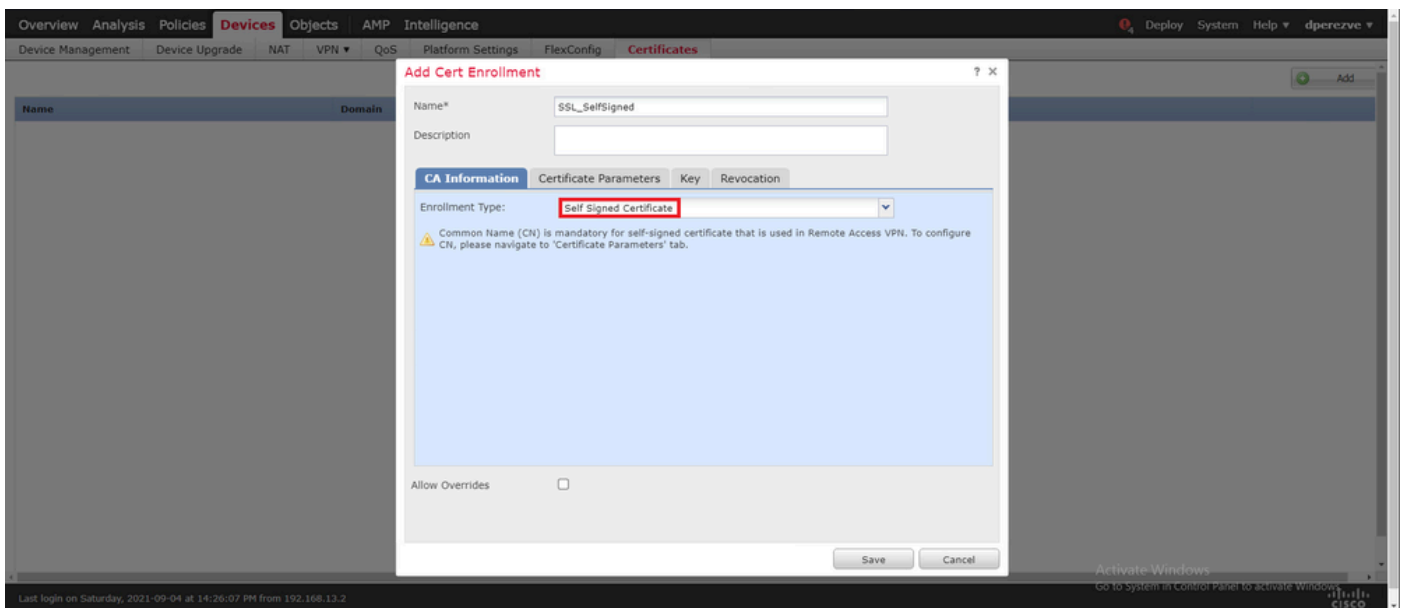
要建立自簽名證書，請導航到裝置>證書。



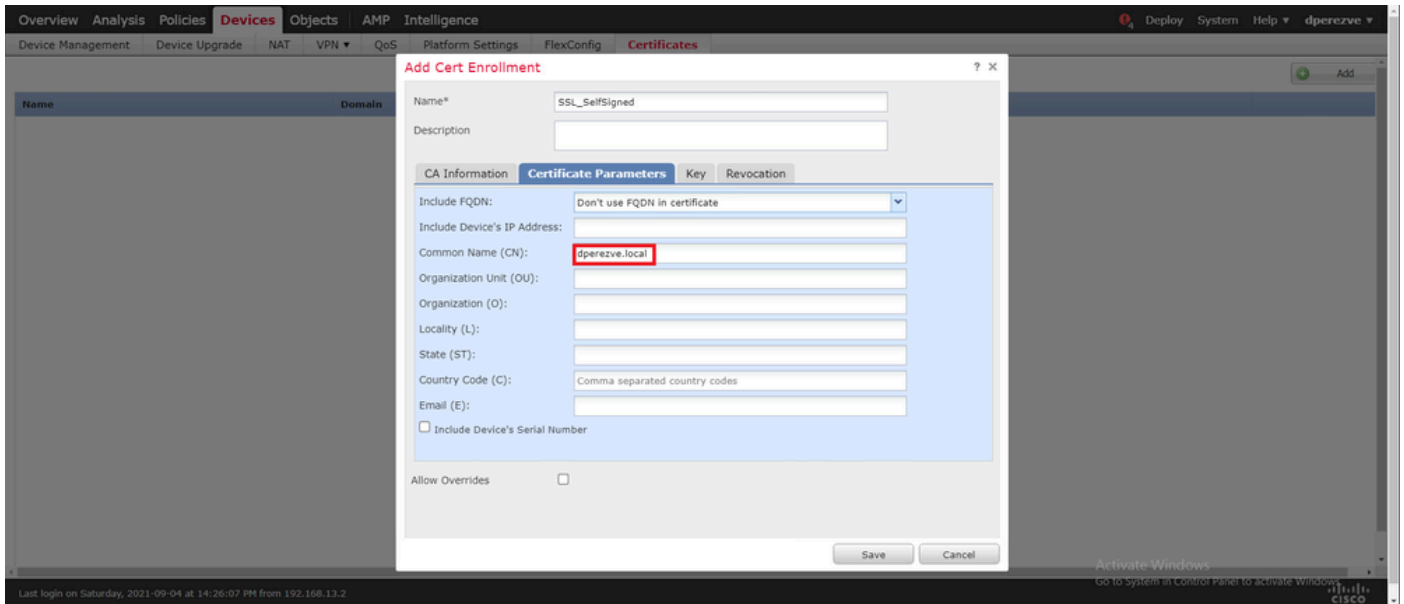
選擇Add按鈕。然後選擇Add New Certificate窗口的Device下拉選單中列出的FTD。



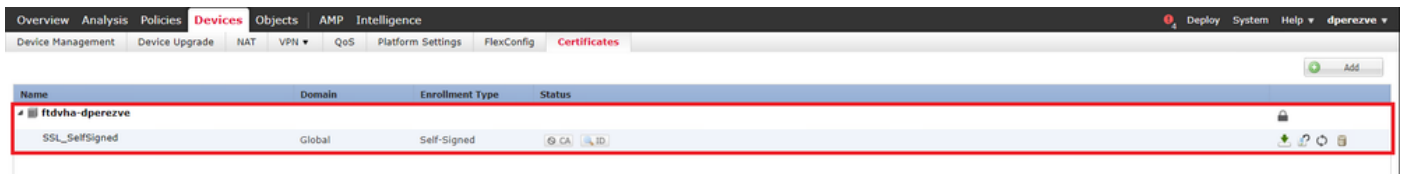
選擇Add Cert Enrollment按鈕（綠色+符號）以建立新的註冊對象。現在，在Add Cert Enrollment窗口中，為對象分配一個名稱，並在Enrollment Type下拉選單中選擇Self Signed Certificate。



最後，對於自簽名證書，必須使用公用名(CN)。導航到證書引數頁籤以定義CN：

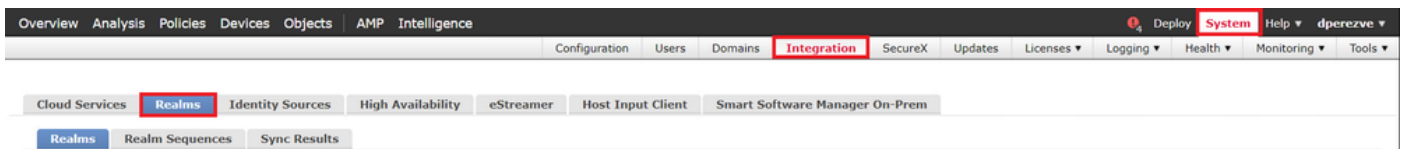


按一下Save和Add按鈕。幾秒鐘後，新證書必須增加到證書清單中：

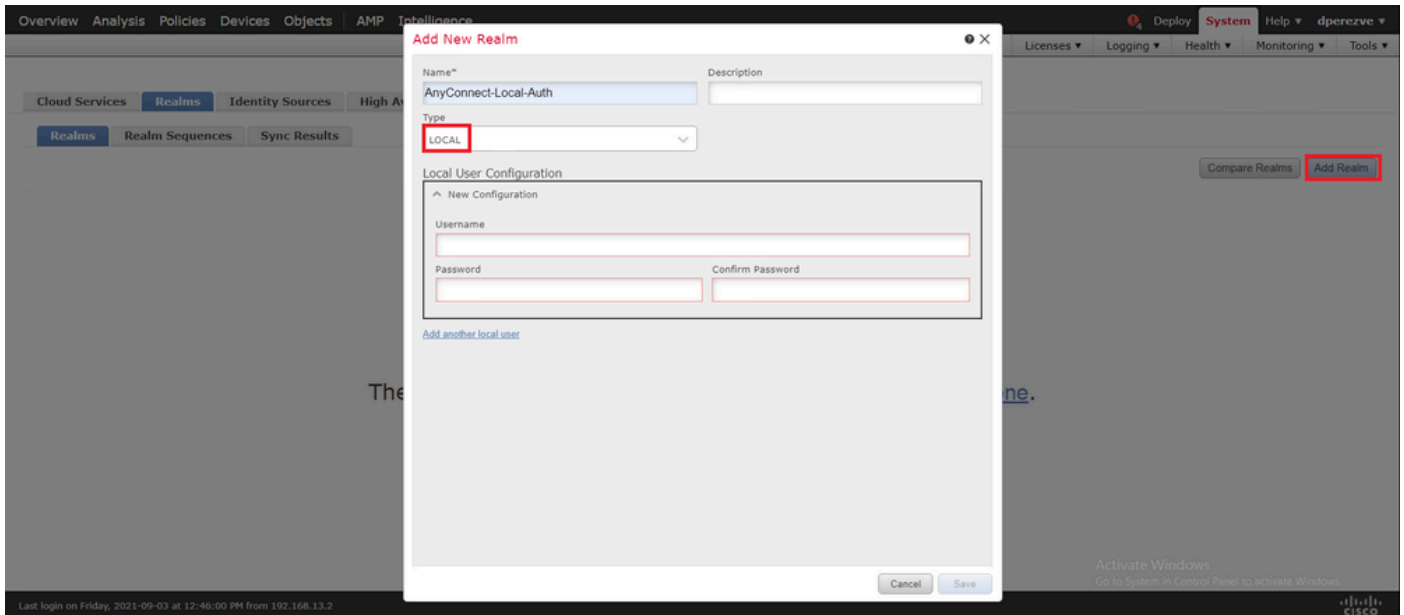


步驟 4. 在FMC上建立本機範圍


本機使用者資料庫和各自的密碼儲存在本機範圍中。若要建立本機範圍，請導覽至系統>整合>範圍：

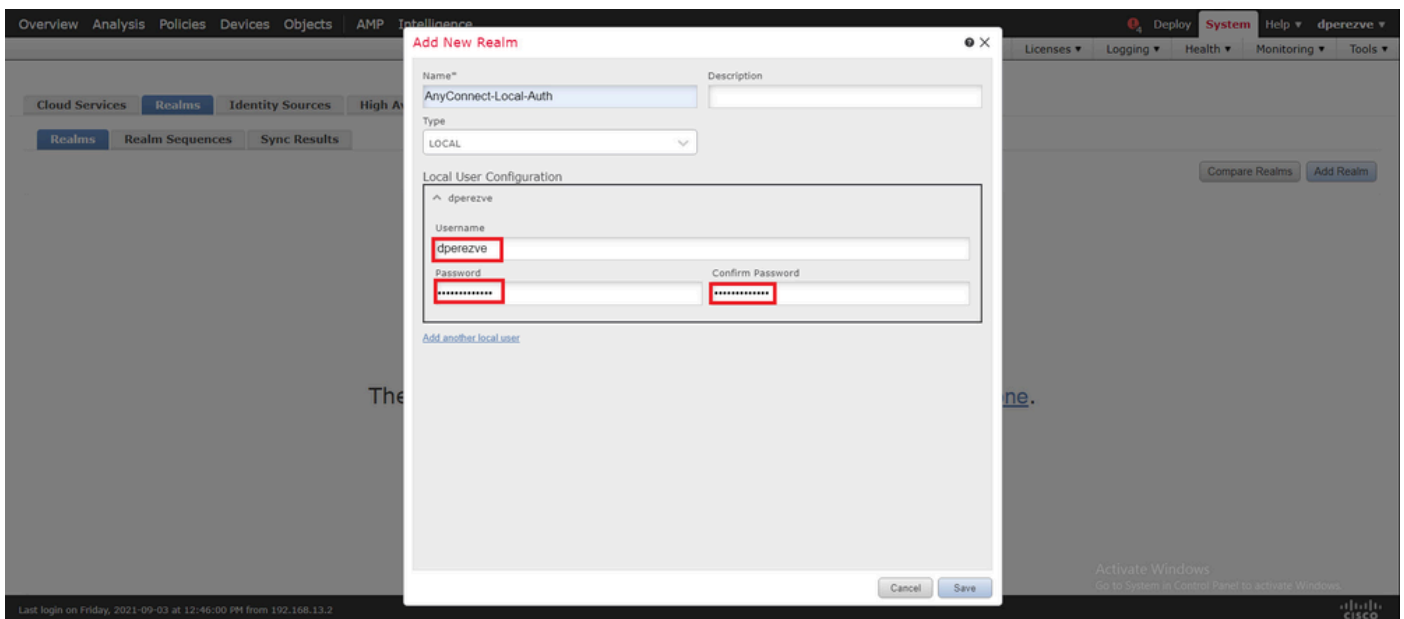


選擇增加領域按鈕。在增加新領域窗口中，分配名稱並在型別下拉選單中選擇本地選項：

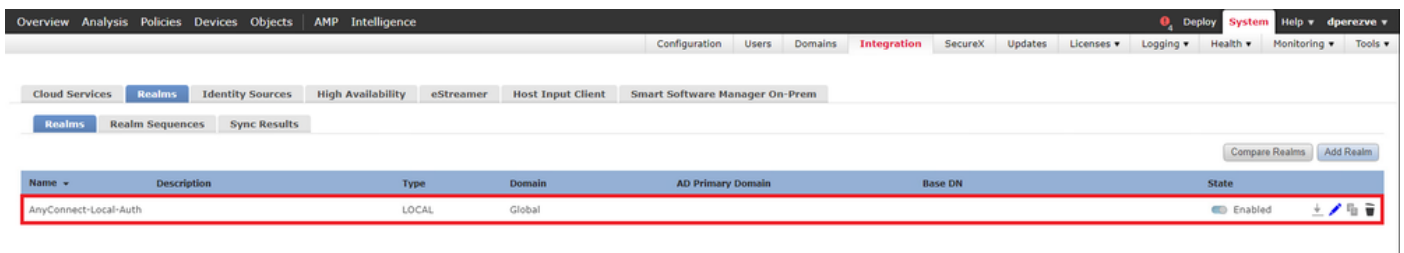


使用者帳戶和密碼在Local User Configuration部分中建立。

 注意：密碼必須至少包含一個大寫字母、一個小寫字母、一個數字和一個特殊字元。

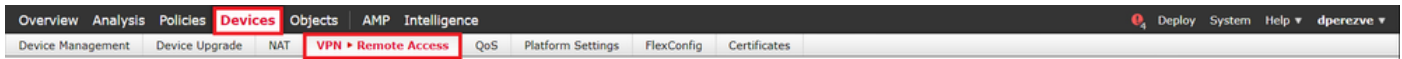


儲存變更，然後按一下新增範圍，將新的範圍新增至現有範圍清單。

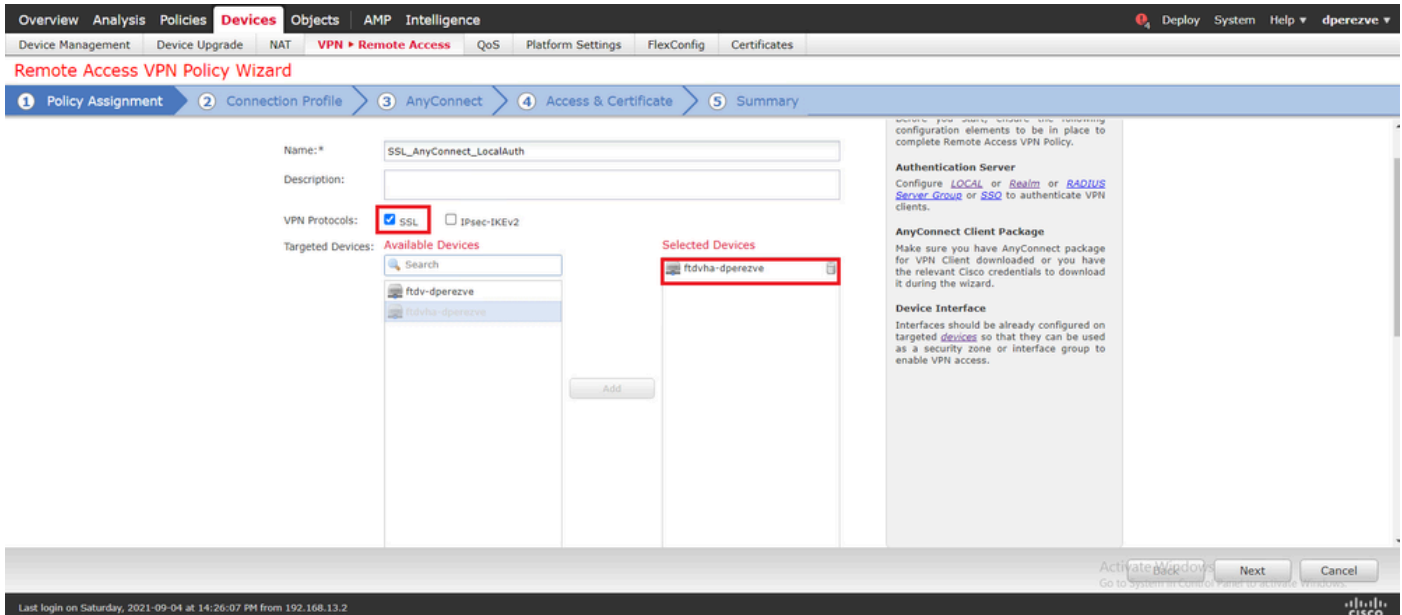


步驟 5. 配置SSL Cisco Secure Client

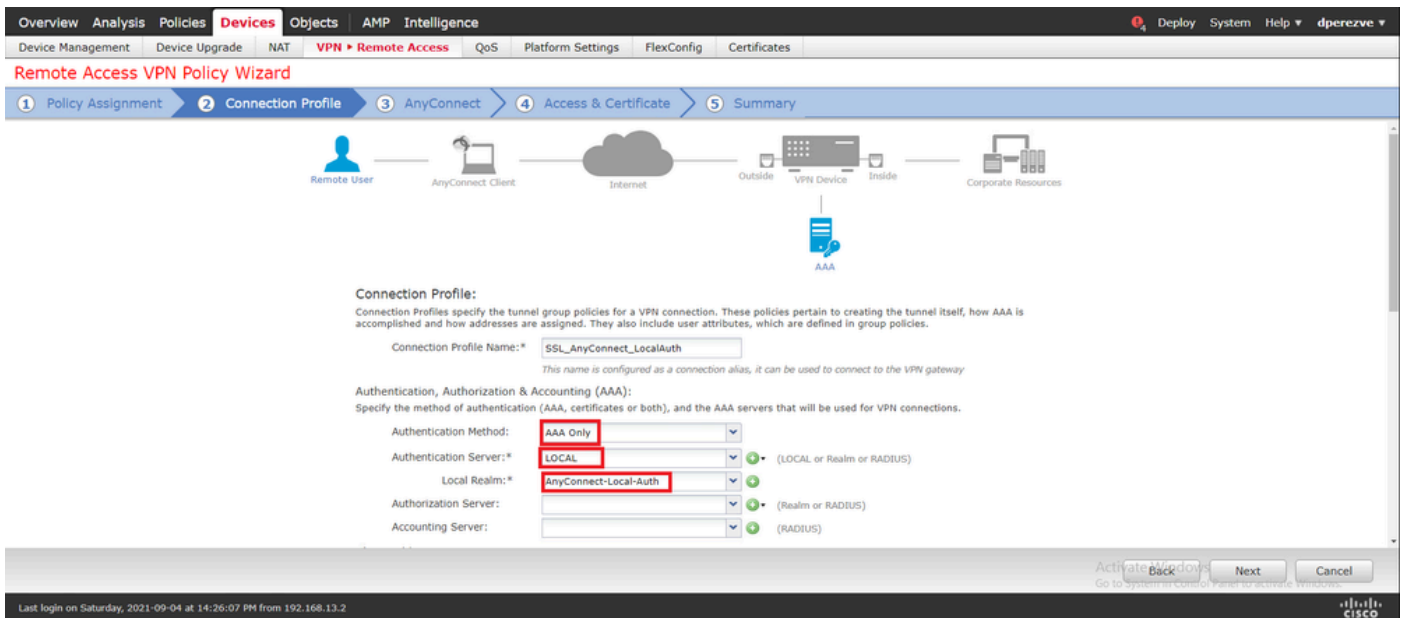
要配置SSL Cisco安全客戶端，請導航到Devices > VPN > Remote Access：



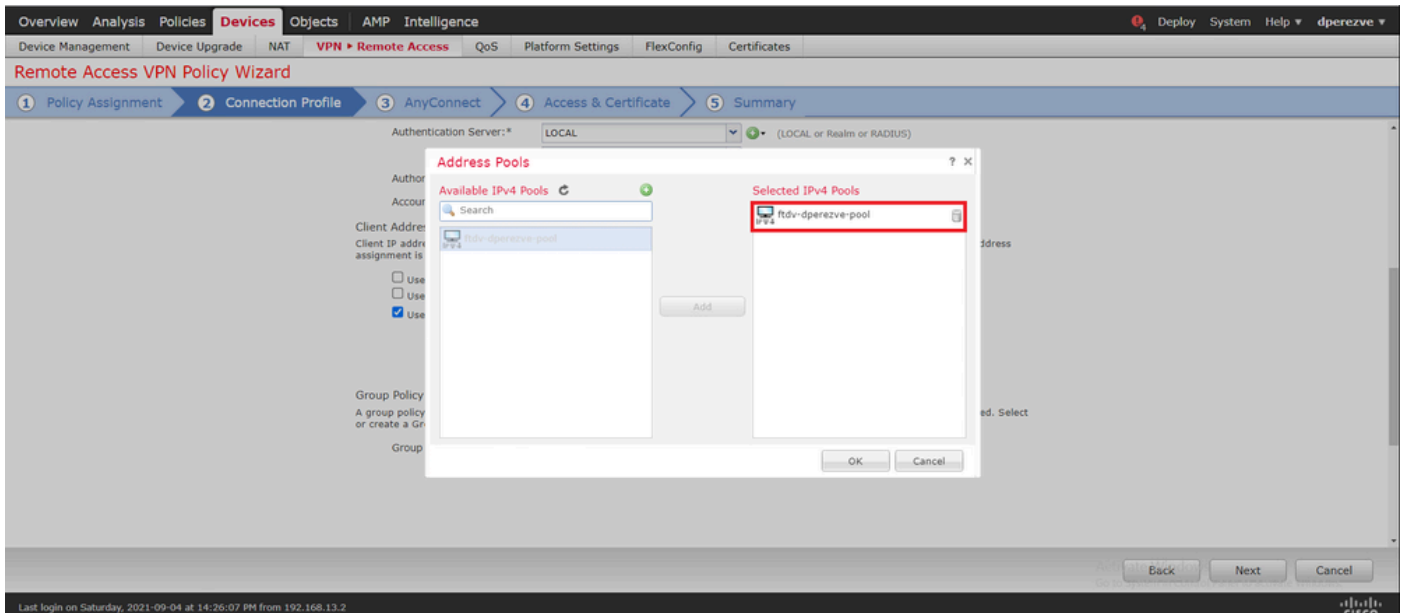
按一下Add按鈕以建立新的VPN策略。定義連線設定檔的名稱，勾選「SSL」核取方塊，然後選擇列為目標裝置的FTD。必須在遠端訪問VPN策略嚮導的策略分配部分中配置所有內容：



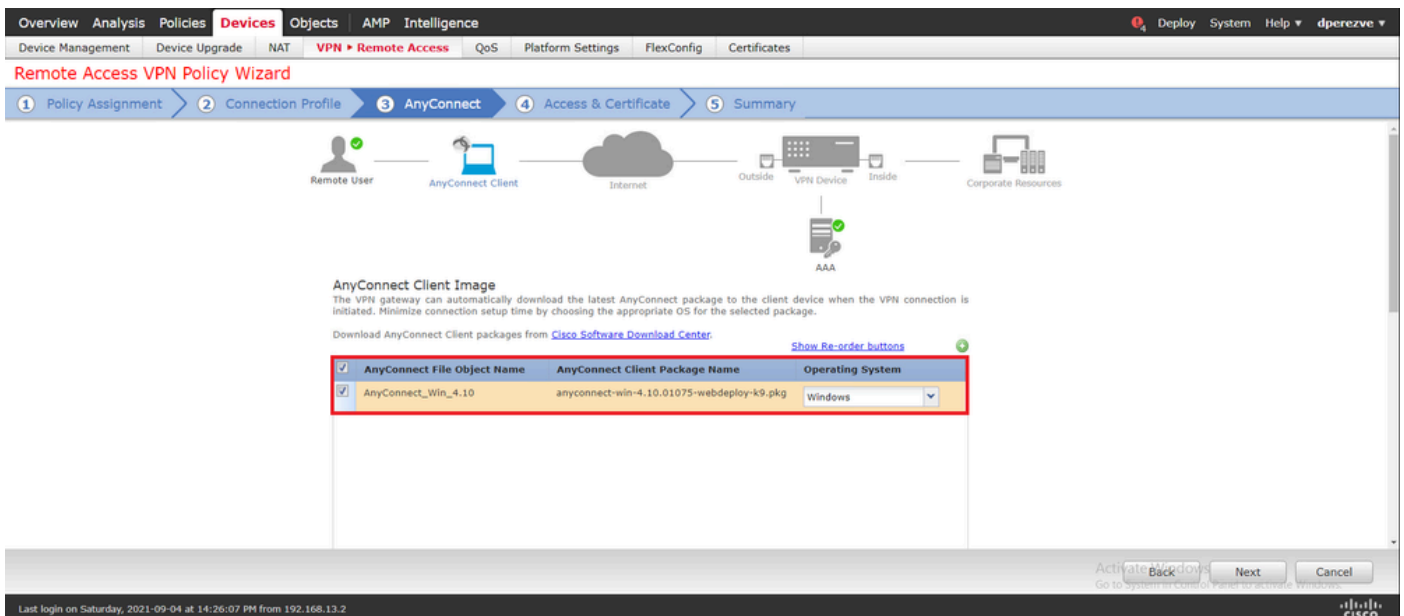
選擇下一步轉到連線配置檔案配置。定義連線配置檔案的名稱，然後選擇AAA Only作為身份驗證方法。然後，在Authentication Server下拉選單中，選擇LOCAL，最後，在Local Realm下拉選單中選擇步驟4中建立的本地領域：



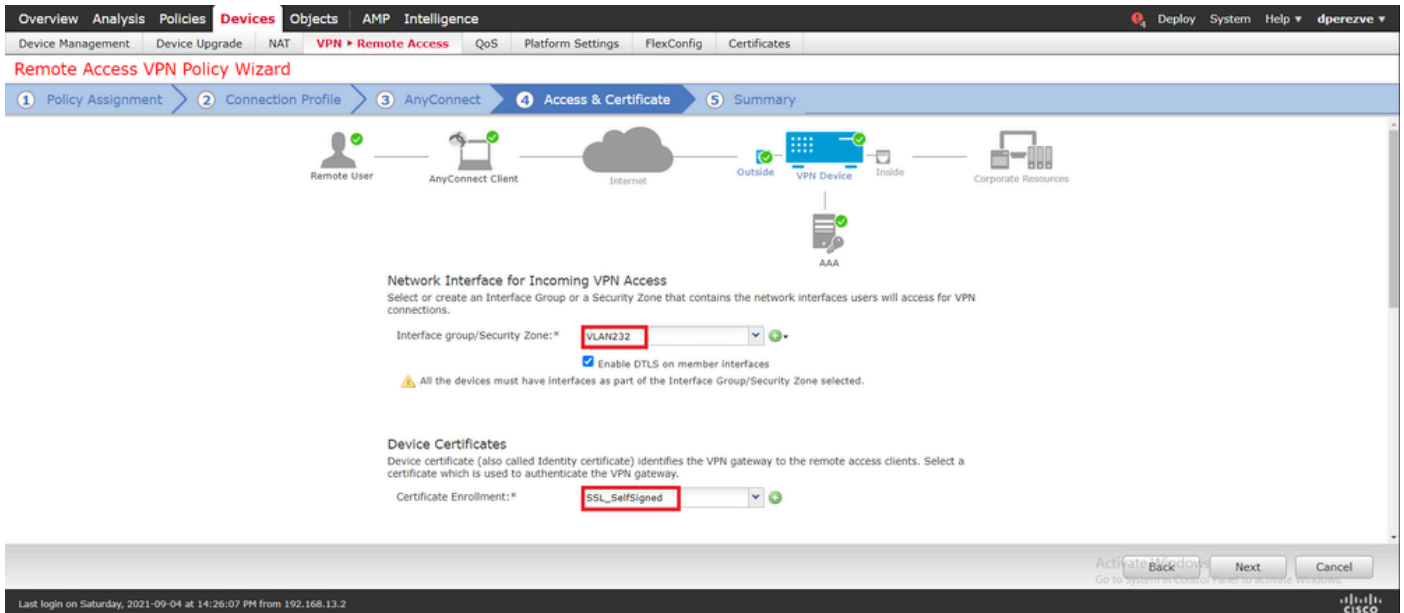
在同一頁上向下滾動，然後按一下IPv4地址池部分中的鉛筆圖示以定義Cisco Secure Client使用的IP池：



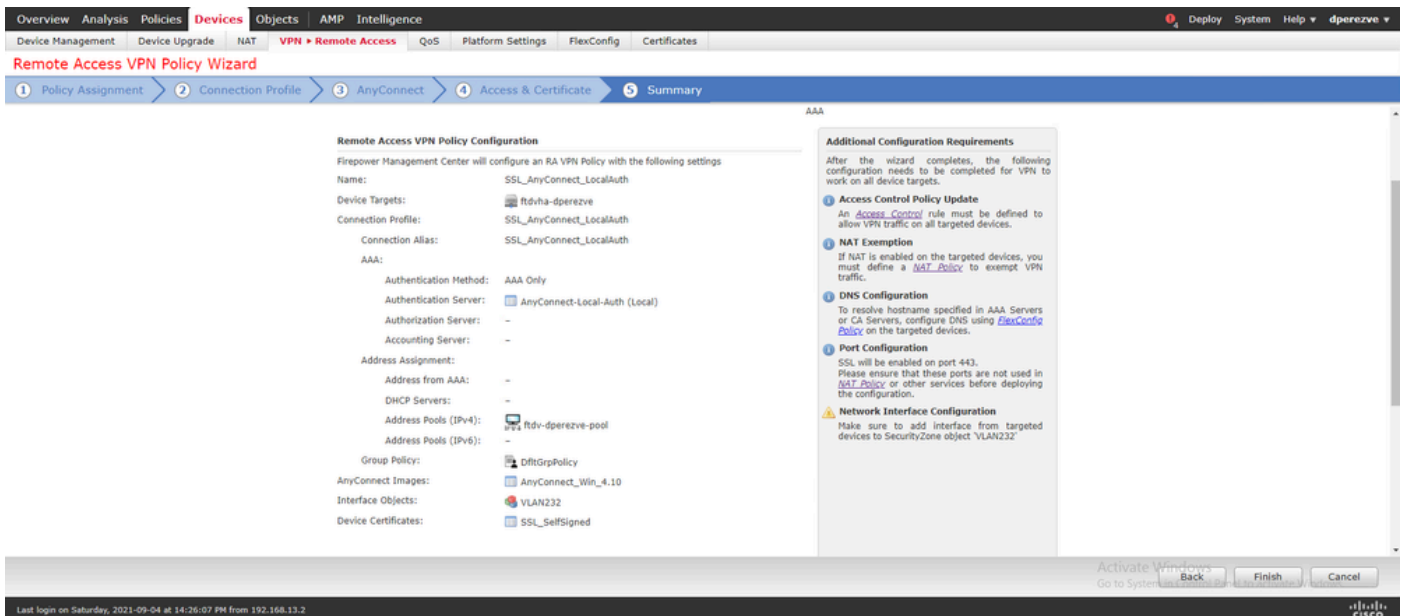
點選下一步轉到AnyConnect部分。現在，請選擇步驟2中上傳的Cisco Secure Client映像：



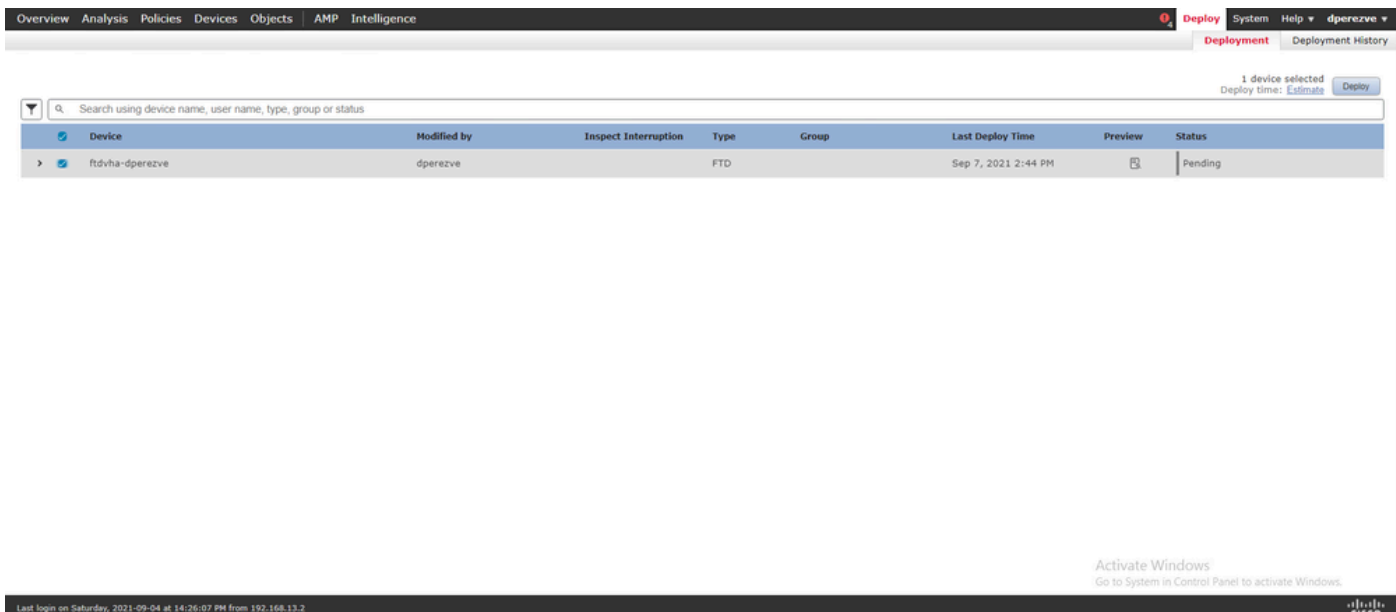
按一下下一步，轉到訪問和證書部分。在Interface group/Security Zone下拉選單中，選擇需要啟用Cisco安全客戶端(AnyConnect)的介面。然後，在Certificate Enrollment下拉選單中，選擇在第3步中建立的證書：



最後，按一下下一步檢視Cisco安全客戶端配置的摘要：

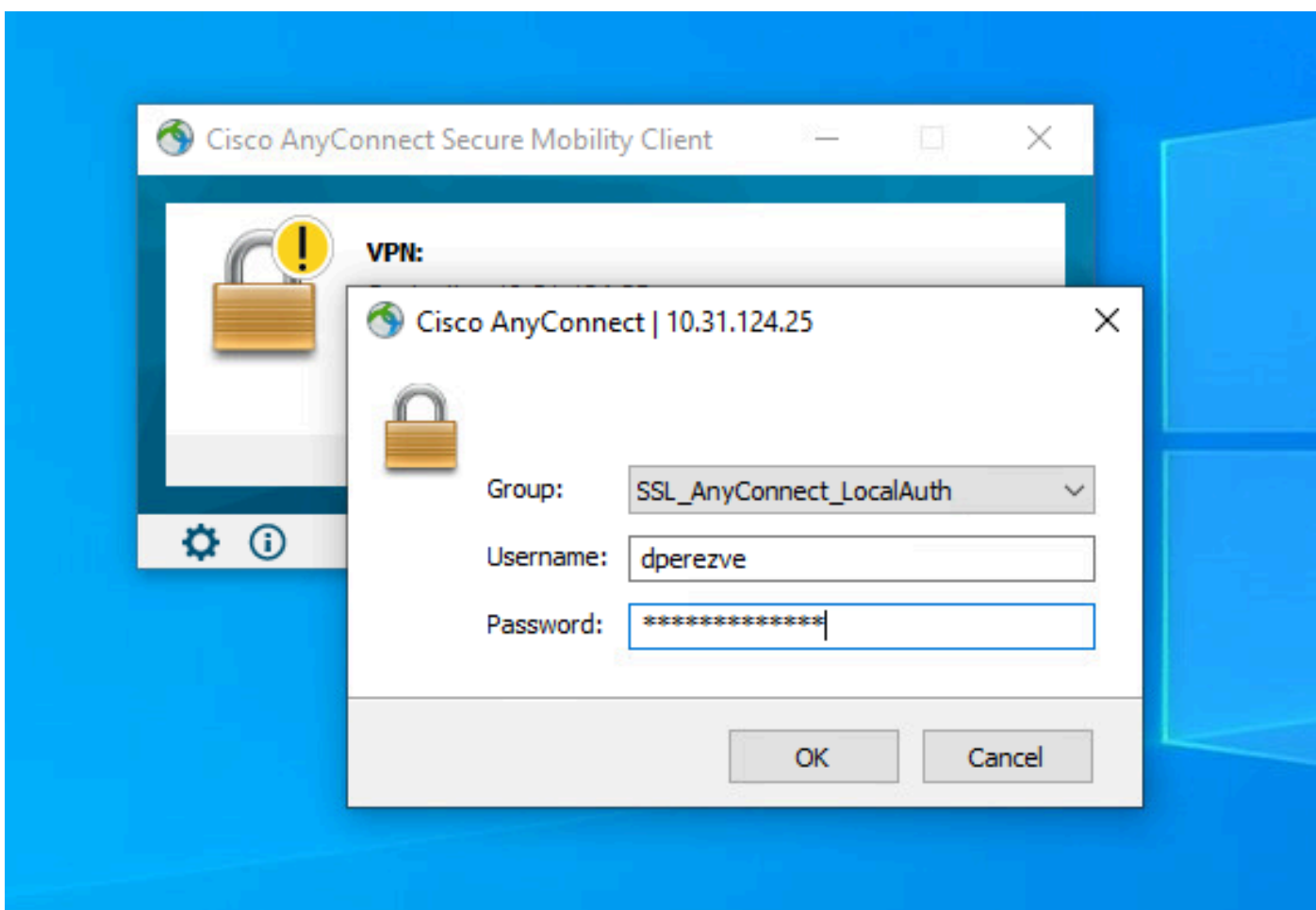


如果所有設定均正確，請按一下Finish並將更改部署到FTD。

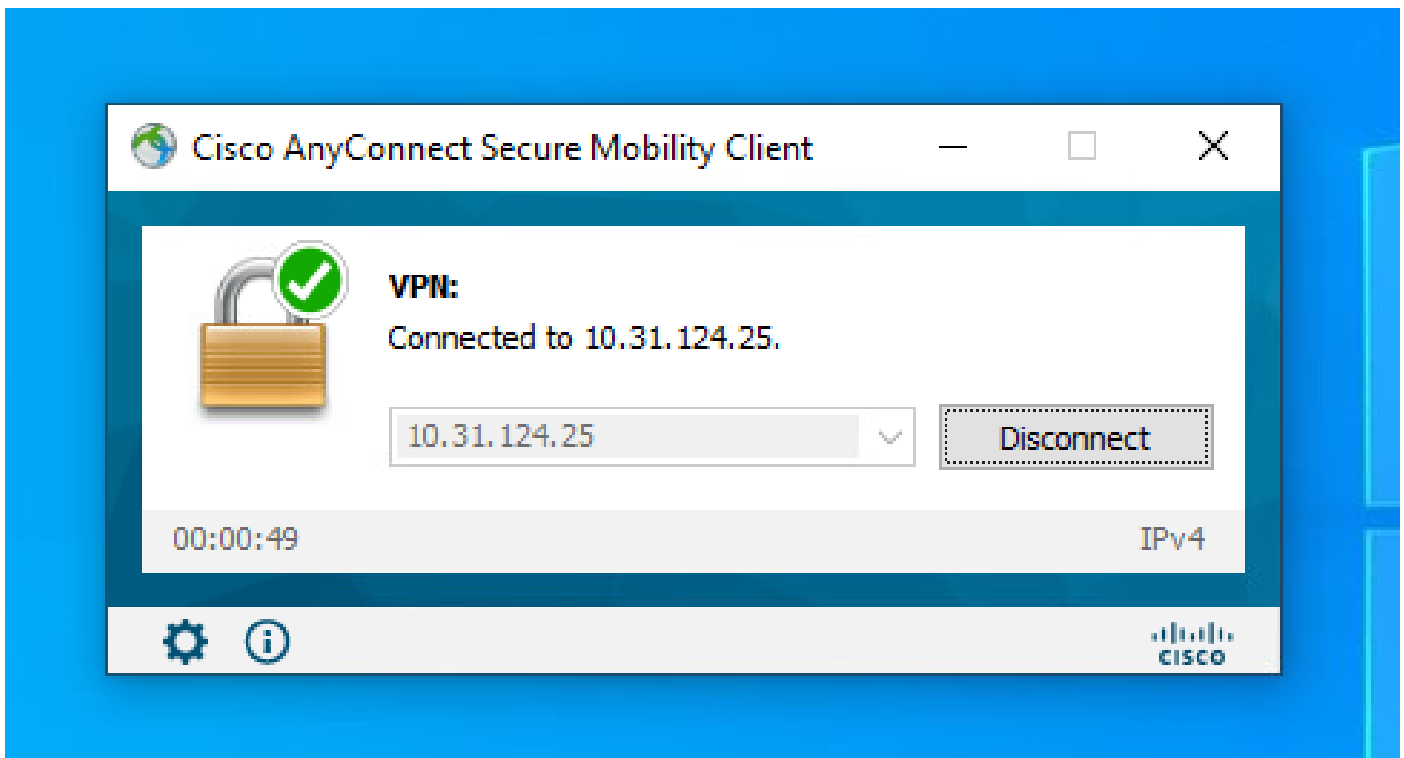


驗證

部署成功後，啟動從Windows客戶端到FTD的Cisco AnyConnect安全移動客戶端連線。在身份驗證提示中使用的使用者名稱和密碼必須與步驟4中建立的使用者名稱和密碼相同：



憑據經FTD批准後，Cisco AnyConnect安全移動客戶端應用必須顯示連線狀態：



從FTD中，您可以運行show vpn-sessiondb anyconnect 命令以顯示防火牆上當前處於活動狀態的Cisco安全客戶端會話：

```
firepower# show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

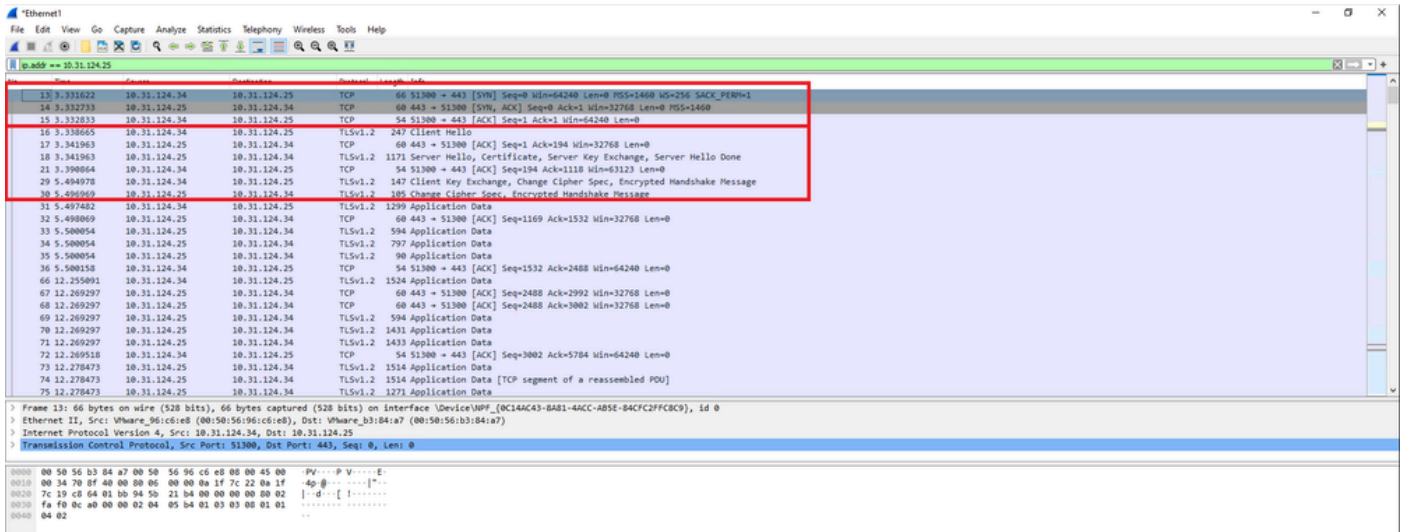
```
Username       : dperezve           Index       : 8
Assigned IP    : 172.16.13.1         Public IP   : 10.31.124.34
Protocol       : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License        : AnyConnect Premium
Encryption     : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing        : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx       : 15756              Bytes Rx    : 14606
Group Policy   : DfltGrpPolicy
Tunnel Group   : SSL_AnyConnect_LocalAuth
Login Time     : 21:42:33 UTC Tue Sep 7 2021
Duration       : 0h:00m:30s
Inactivity     : 0h:00m:00s
VLAN Mapping   : N/A                VLAN        : none
Audt Sess ID   : 0000000000080006137dcc9
Security Grp   : none                Tunnel Zone : 0
```

疑難排解

對FTD執行debug webvpn anyconnect 255命令，以檢視FTD上的SSL連線流：

```
firepower# debug webvpn anyconnect 255
```

除了Cisco Secure Client調試之外，還可以使用TCP資料包捕獲來觀察連線流。以下範例顯示連線成功，Windows使用者端和FTD之間完成一般三次握手，然後進行用於同意密碼的SSL握手。



在通訊協定交涉之後，FTD必須使用儲存在本機範圍中的資訊來驗證證明資料。

收集DART捆綁包，並聯絡思科TAC進行進一步研究。

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）。