在FTD上設定使用本機驗證的SSL安全使用者端

目錄

簡介

本檔案介紹如何在思科FMC管理的Cisco FTD上使用本機驗證來設定思科安全使用者端（包括Anyconnect）。

必要條件

需求

思科建議您瞭解以下主題：

- 通過Firepower管理中心(FMC)進行SSL安全客戶端配置
- 通過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)版本7.0.0（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

在此範例中，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。可以將其定義為主要身份驗證方法，或者在主要方法失敗時將其定義為回退。在本示例中，本地身份驗證配置為主身份驗證。

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Cisco Firepower裝置管理器(FDM)上可用。

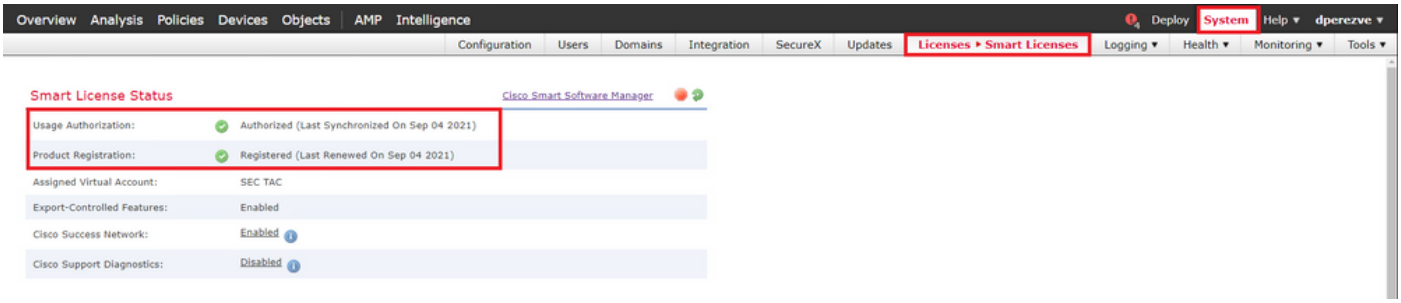
設定

組態

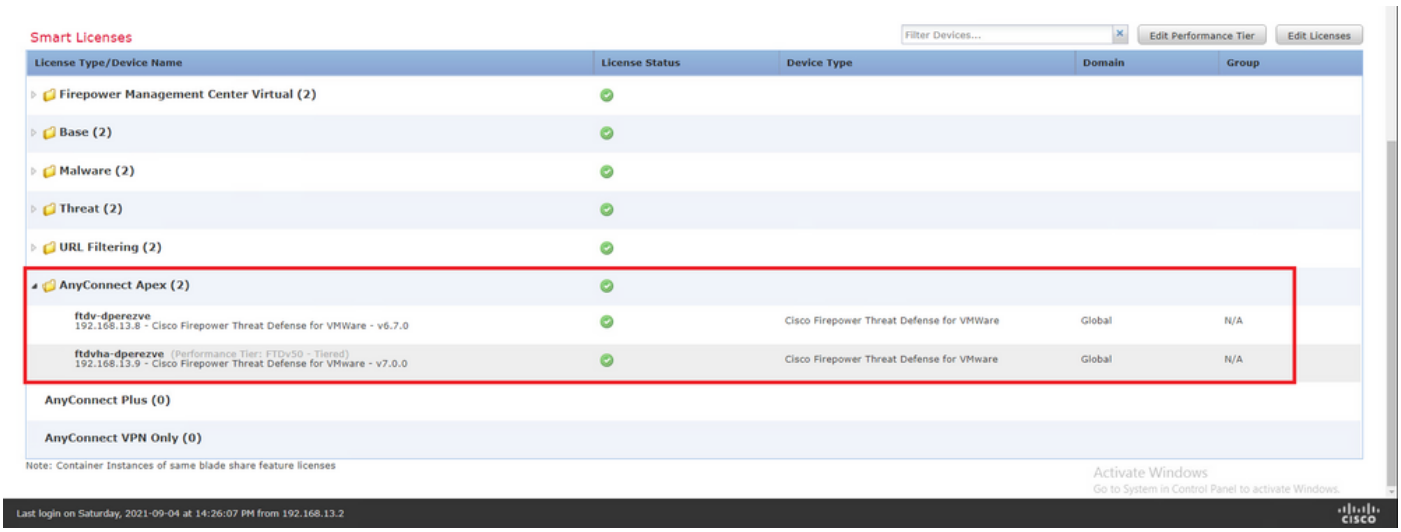
步驟 1.驗證許可

在配置Cisco Secure Client之前，必須註冊FMC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Cisco Secure Client。

導覽至System > Licenses > Smart Licenses，以驗證FMC是否已註冊且符合智慧許可門戶的規定。



在同一頁上向下滾動，在Smart Licenses圖表底部，您可以看到不同型別的可用思科安全客戶端(AnyConnect)許可證以及每個許可證所訂用的裝置。驗證手頭的FTD是否已按以下任一類別註冊。

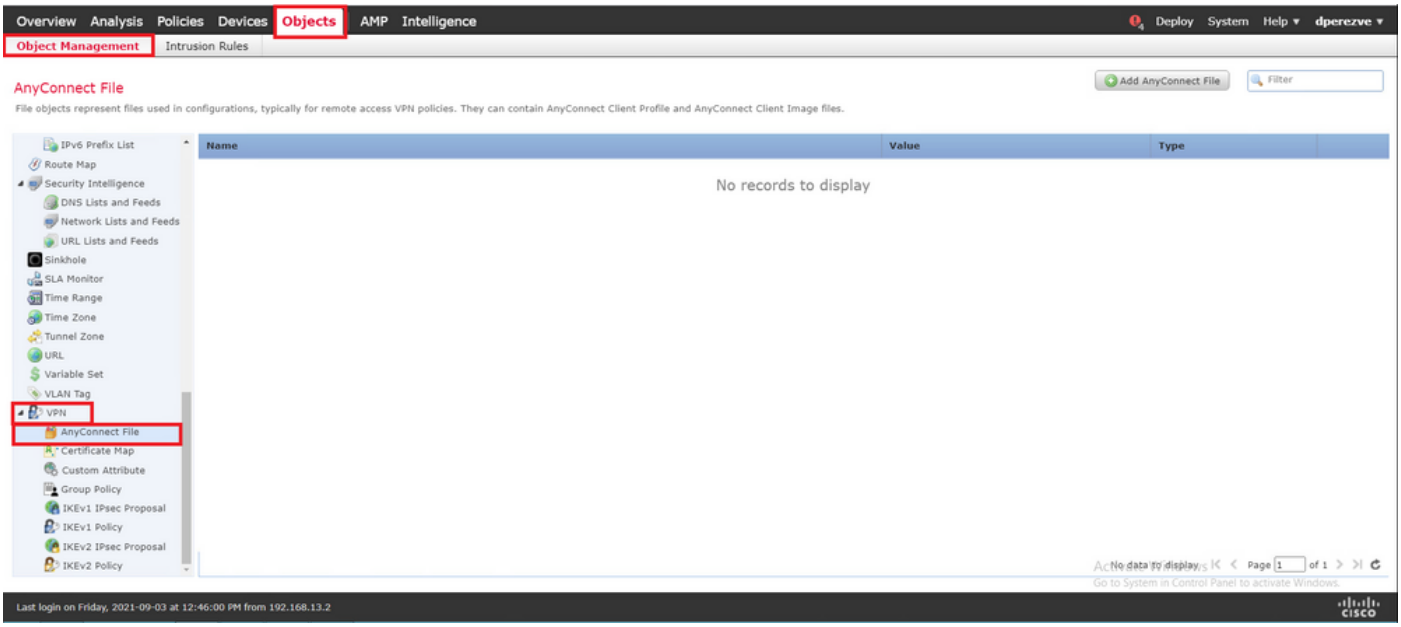


步驟 2.將思科安全客戶端軟體包上傳到FMC

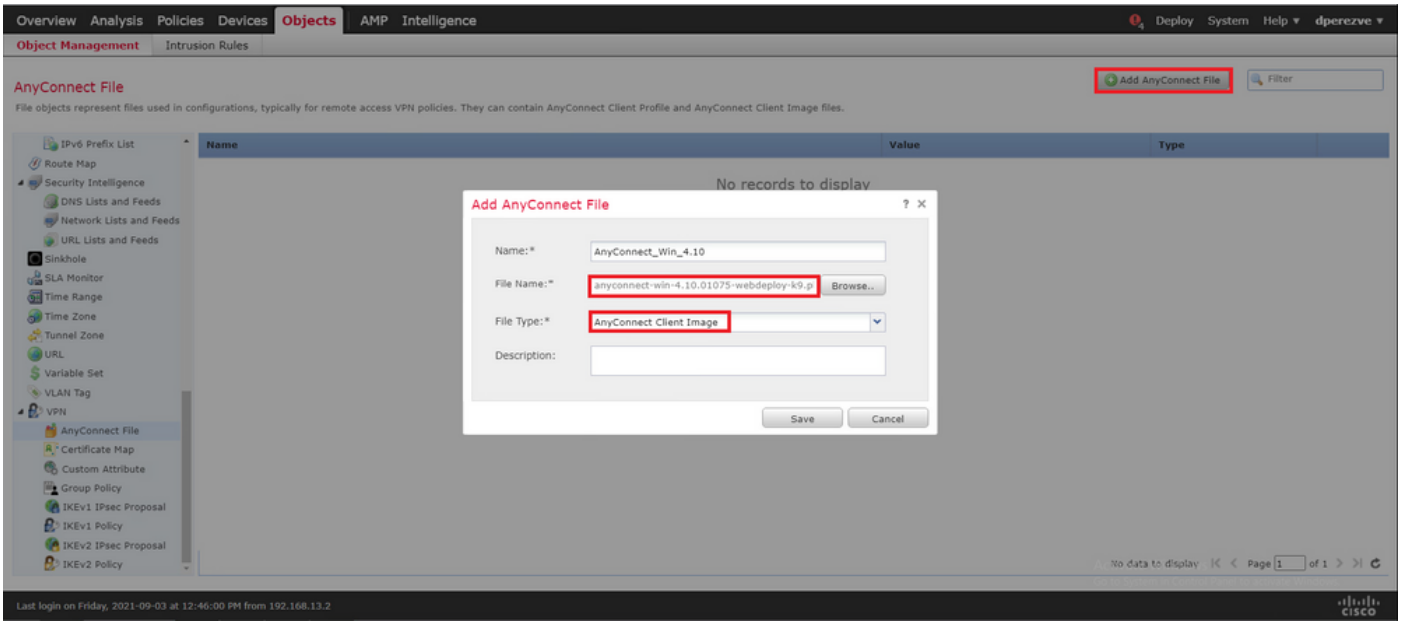
從cisco.com下載適用於Windows的Cisco Secure Client(AnyConnect)頭端部署包。

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

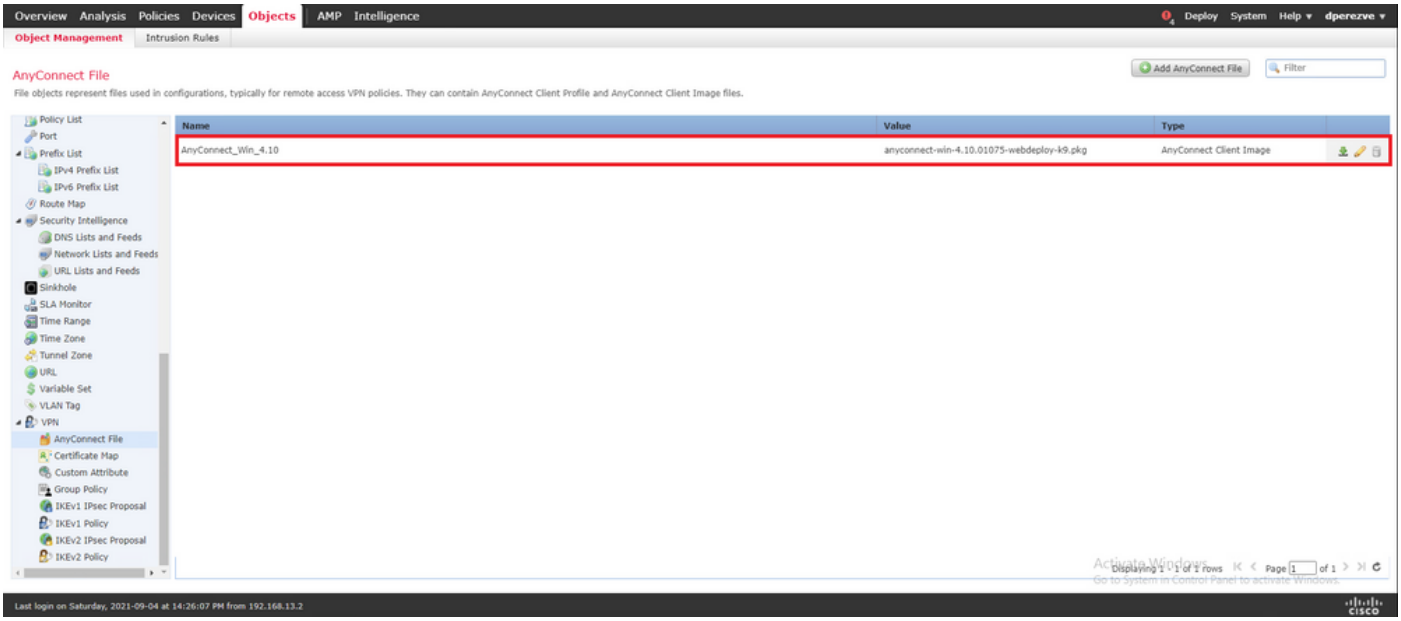
若要上傳Cisco Secure Client映像，請導航到Objects > Object Management，然後在目錄的VPN類別下選擇Cisco Secure Client File。



選擇Add AnyConnect File按鈕。在「Add AnyConnect Secure Client File」視窗中，為對象指定名稱，然後選擇Browse..，以選擇Cisco Secure Client軟體包，最後在下拉選單中選擇AnyConnect Client Image作為檔案型別。



選擇Save按鈕。必須將對象新增到對象清單中。



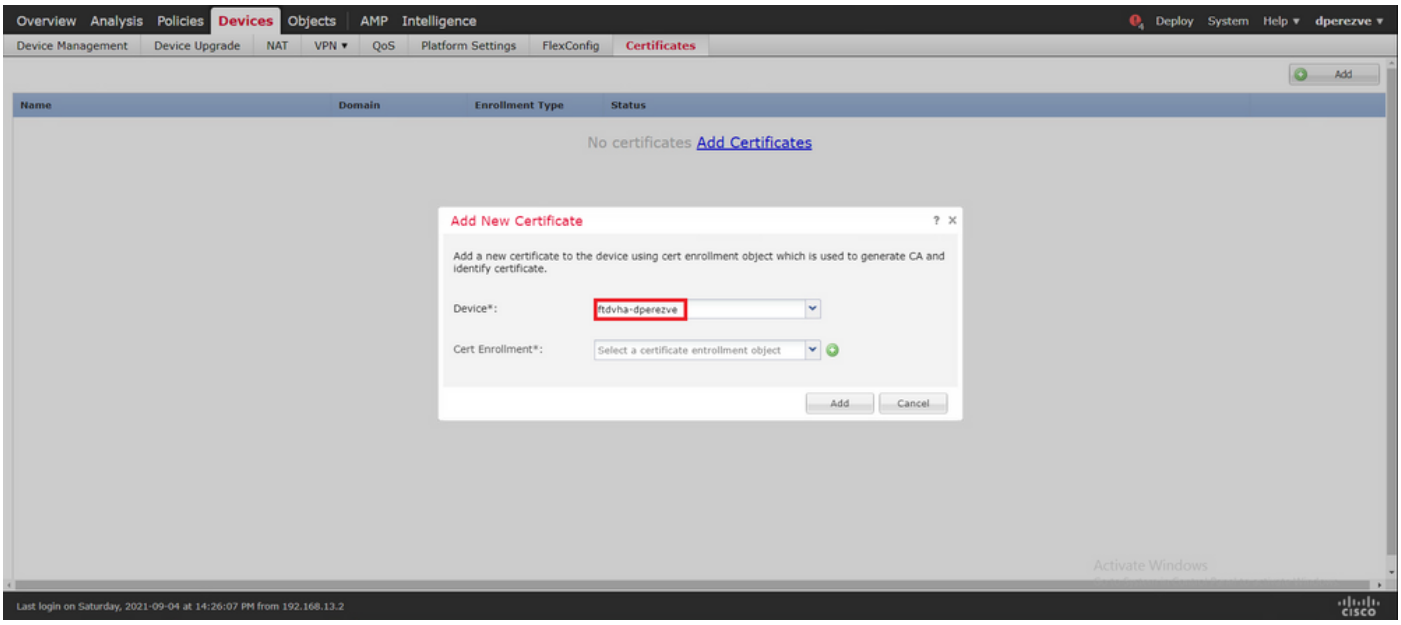
步驟 3.生成自簽名證書

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。

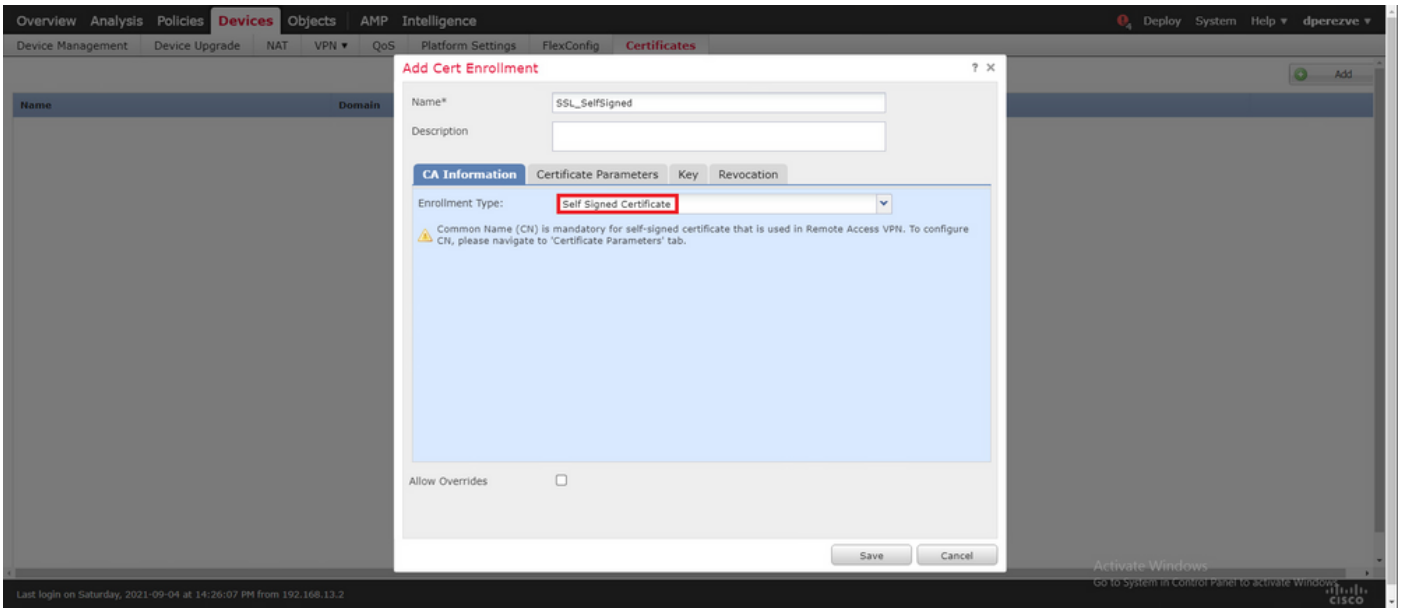
註：在此示例中，將為此生成自簽名證書。但是，除了自簽名的憑證外，還可以上傳由內部憑證授權單位(CA)或公認的CA簽名的憑證。

若要建立自簽名的憑證，請導覽至Devices > Certificates。

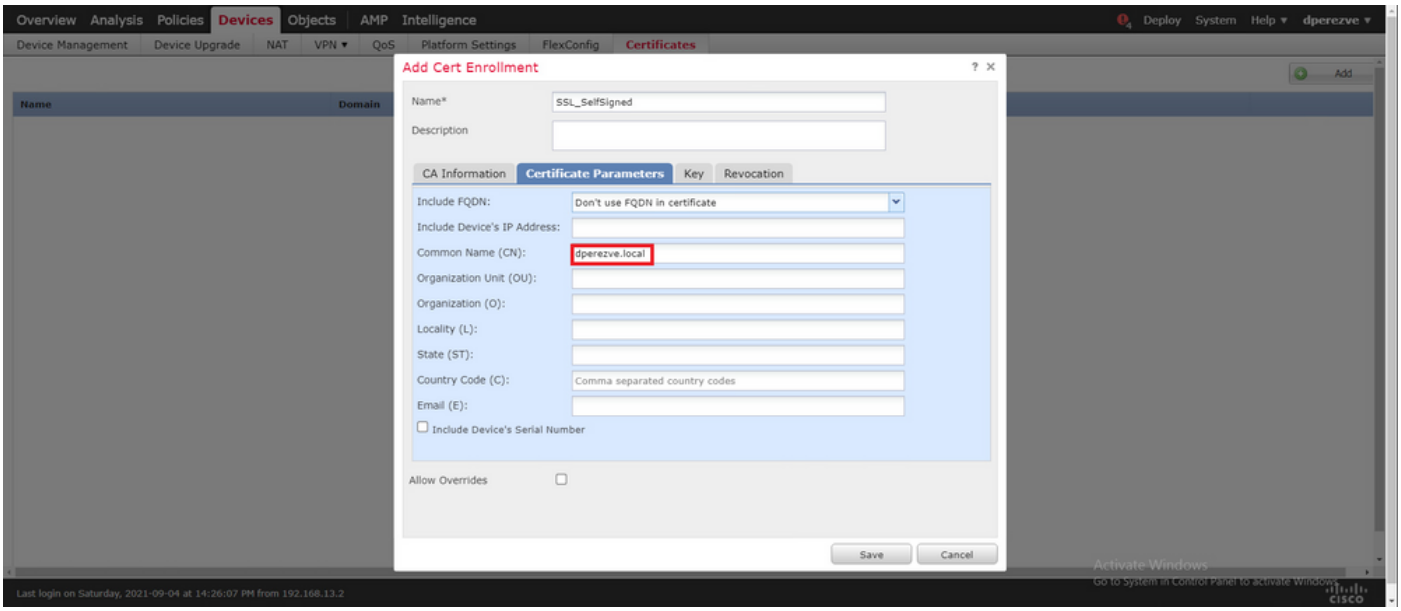
選擇Add按鈕。接著在Add New Certificate視窗的Device下拉式功能表中選擇手頭的FTD。



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」視窗中，為對象分配名稱，然後在「Enrollment Type」下拉選單中選擇「Self Signed Certificate」。



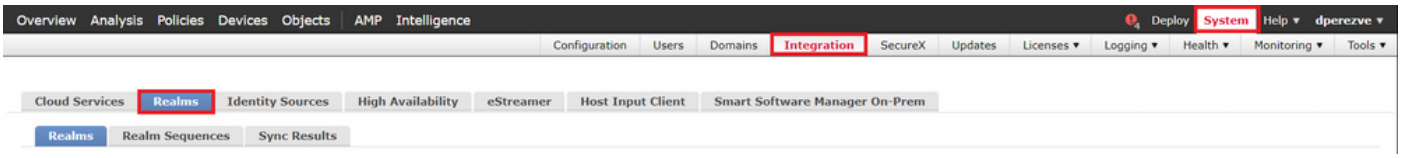
最後，對於自簽名證書，必須有一個公用名(CN)。導覽至Certificate Parameters索引標籤以定義CN。



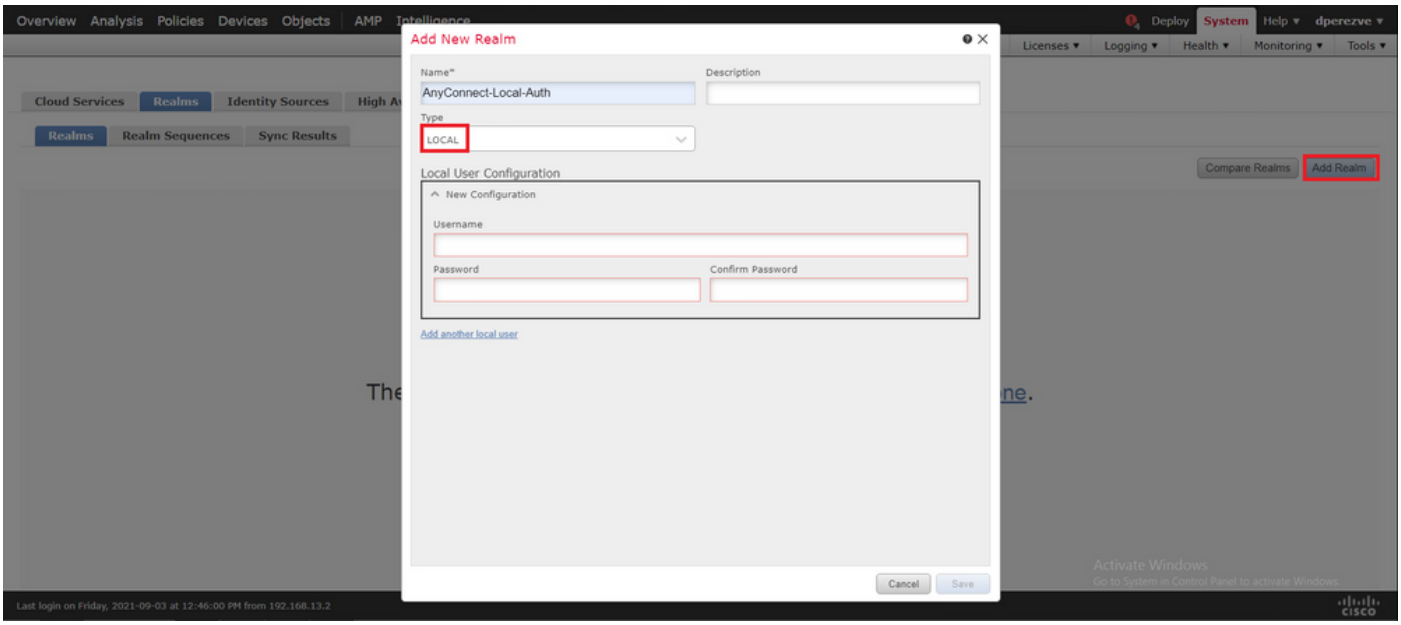
選擇Save和Add按鈕。幾秒鐘後，必須將新憑證新增到憑證清單中。

步驟 4.在FMC上建立本地領域

本地使用者資料庫和各自的口令儲存在本地領域中。要建立本地領域，請導航到System > Integration > Realms。

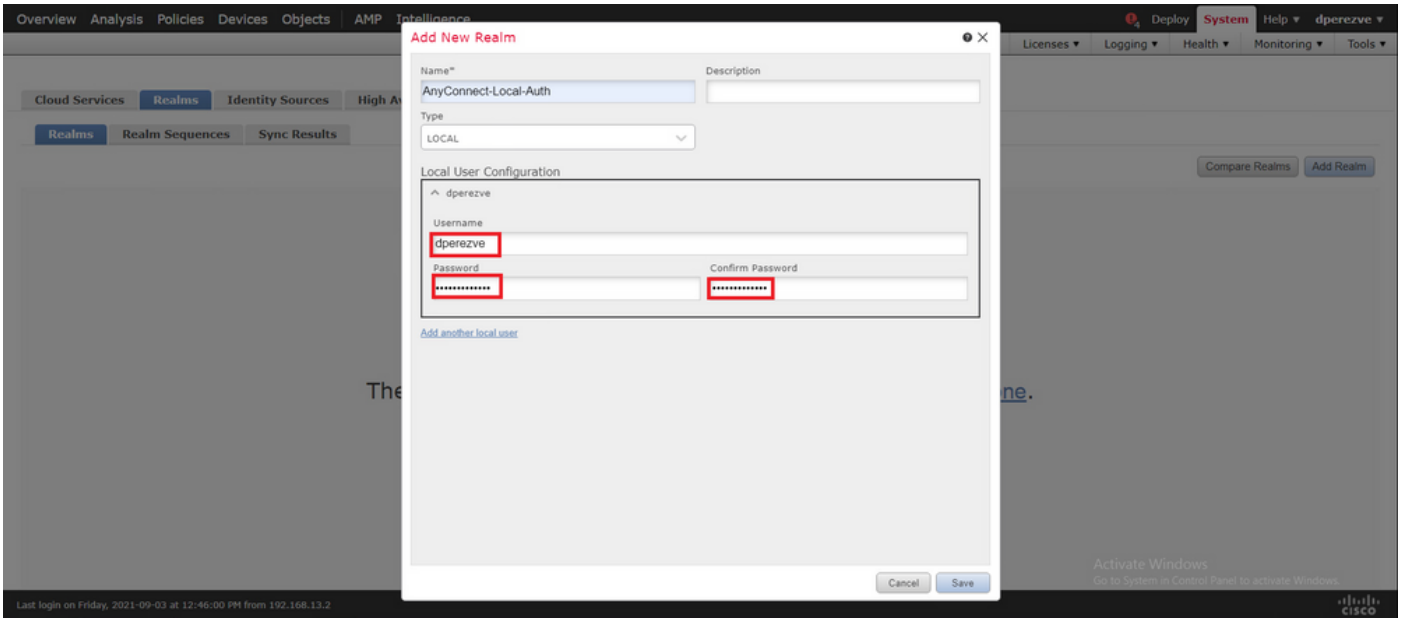


選擇Add Realm按鈕。在新增新領域視窗中，分配名稱並在型別下拉選單中選擇LOCAL選項。

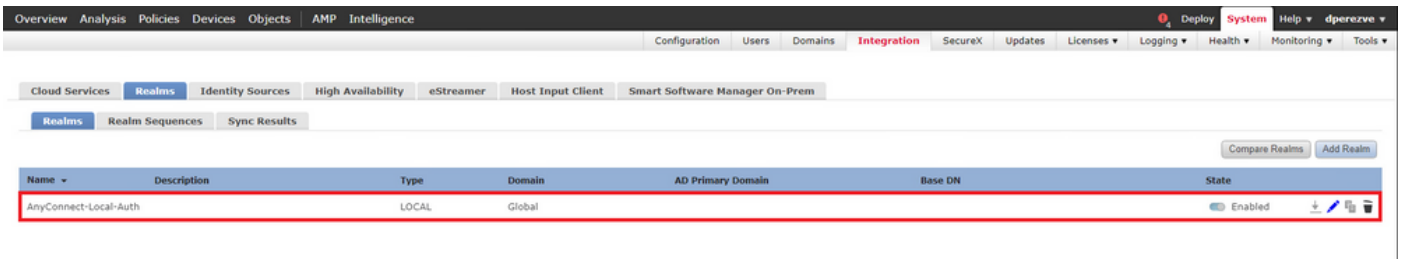


使用者帳戶和密碼在Local User Configuration部分建立。

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。

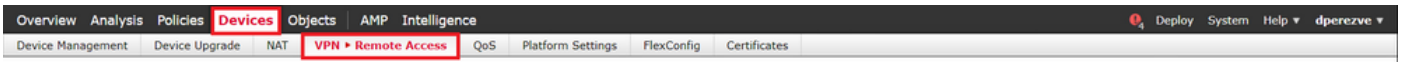


必須將儲存更改和新領域新增到現有領域清單中。

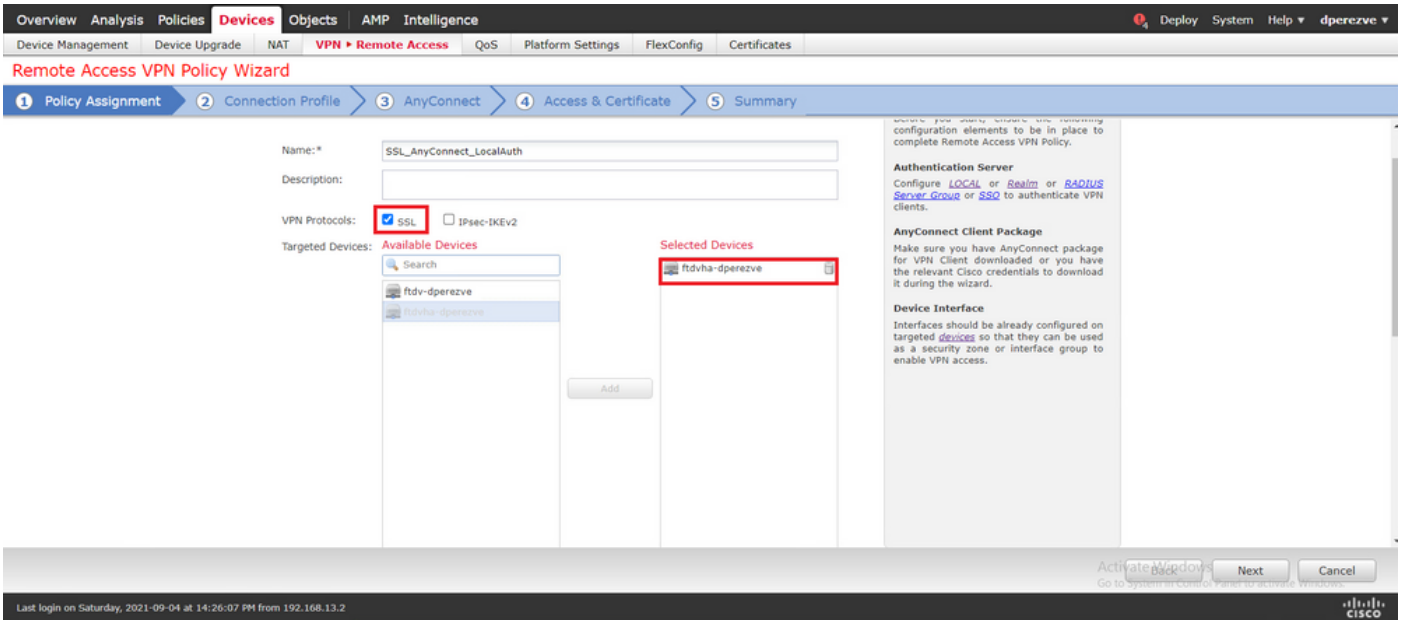


步驟 5.配置SSL思科安全客戶端

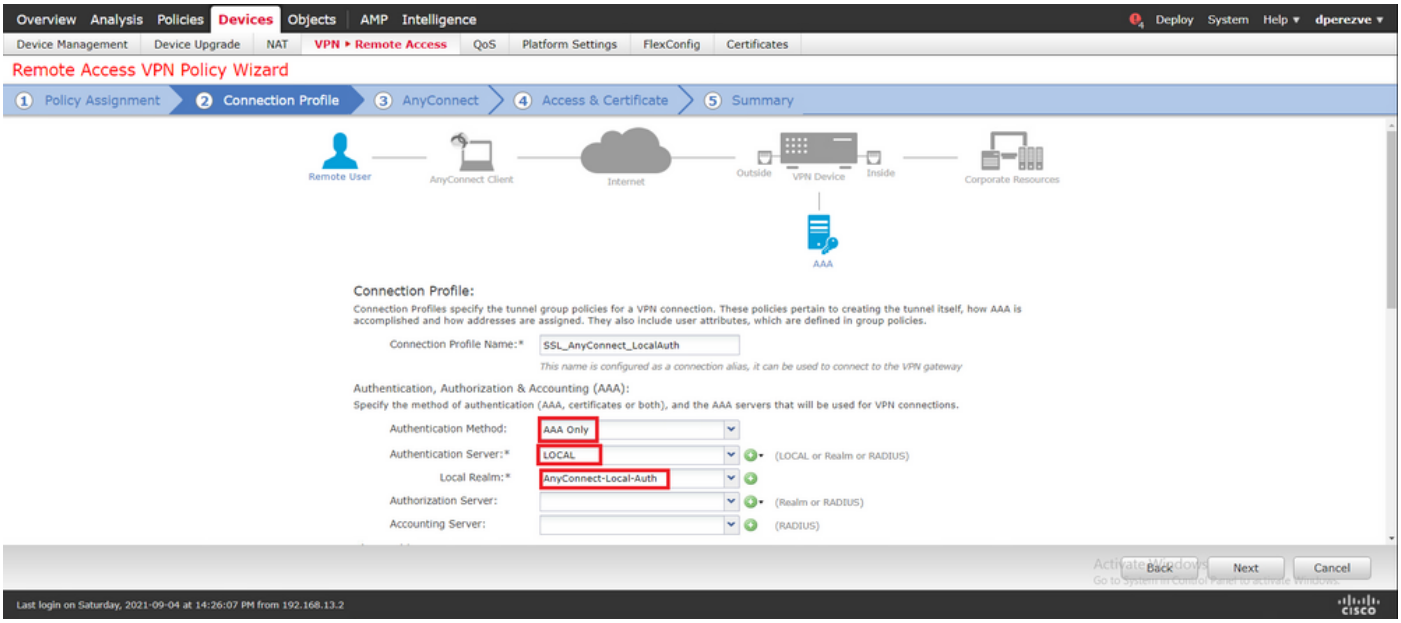
要配置SSL思科安全客戶端，請導航到Devices > VPN > Remote Access。



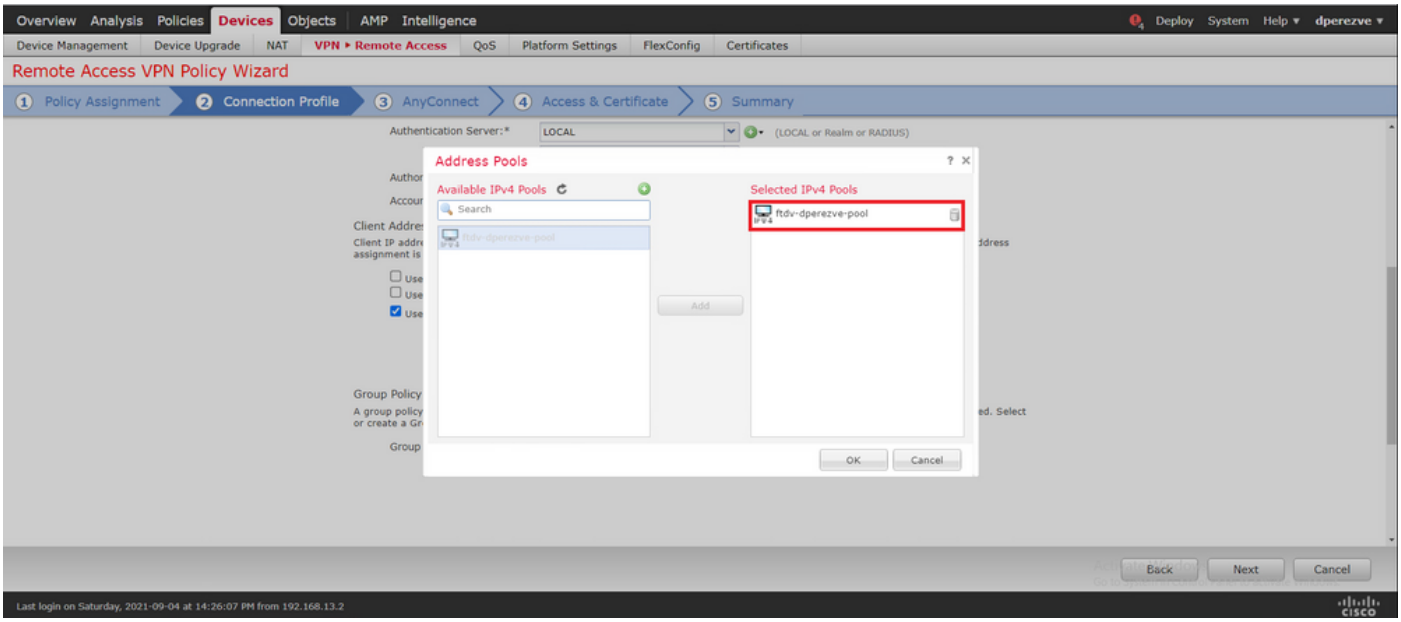
選擇Add按鈕以建立新的VPN策略。定義連線配置檔案的名稱，選中SSL覈取方塊，然後選擇手邊的FTD作為目標裝置。必須在遠端訪問VPN策略嚮導的策略分配部分中配置所有內容。



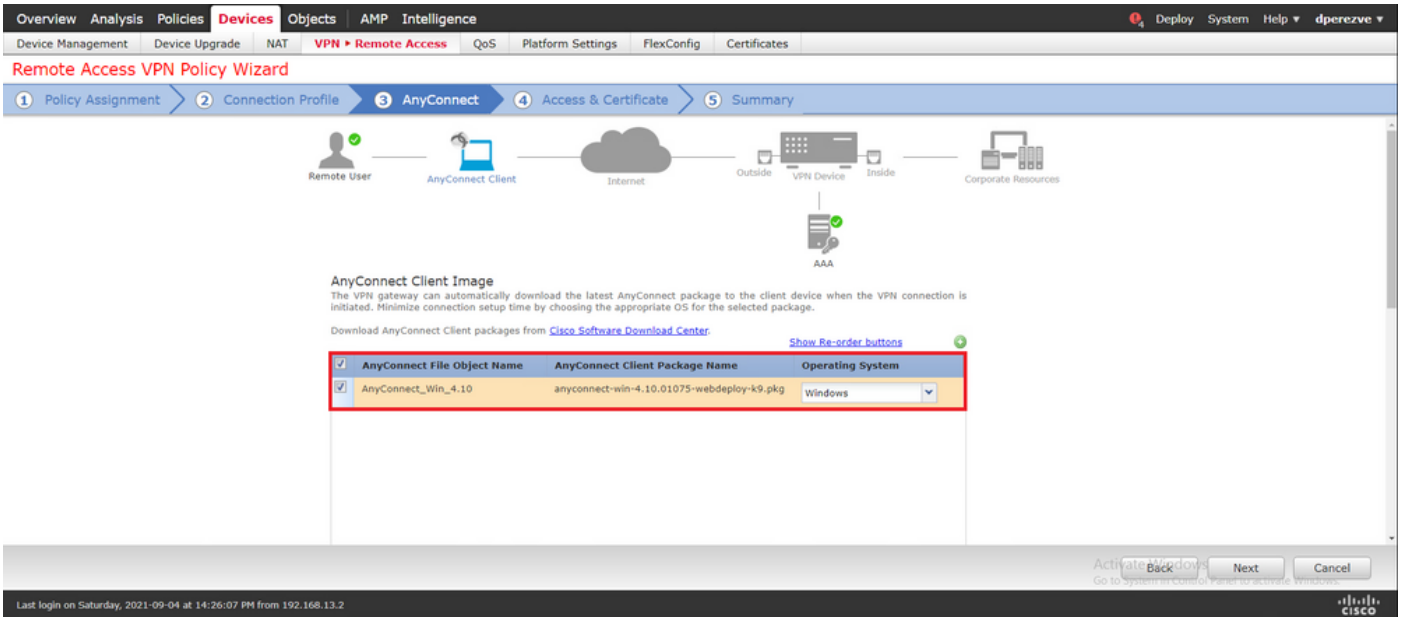
選擇Next以轉到連線配置檔案配置。定義連線配置檔案的名稱，然後選擇AAA Only作為身份驗證方法。然後，在Authentication Server下拉選單中，選擇LOCAL，最後在Local Realm下拉選單中選擇步驟4中建立的本地領域。



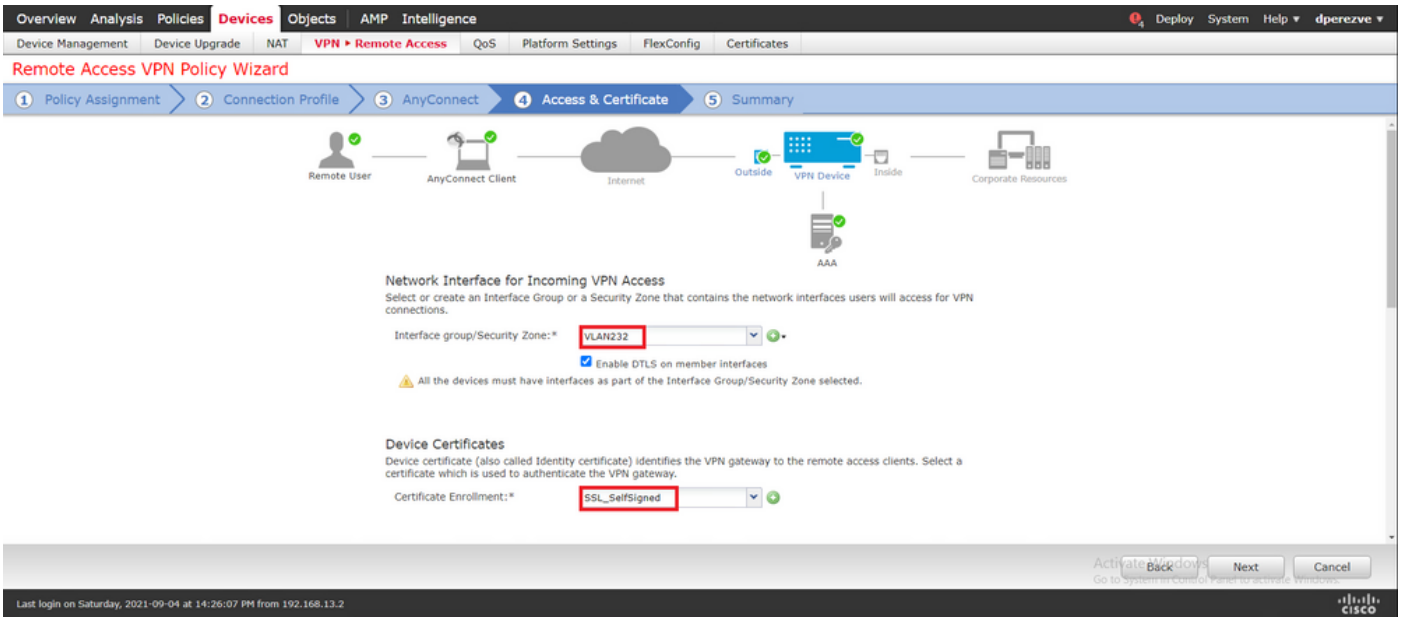
在同一頁上向下滾動，然後在IPv4地址池部分中選擇鉛筆圖示，以定義Cisco安全客戶端使用的IP池。



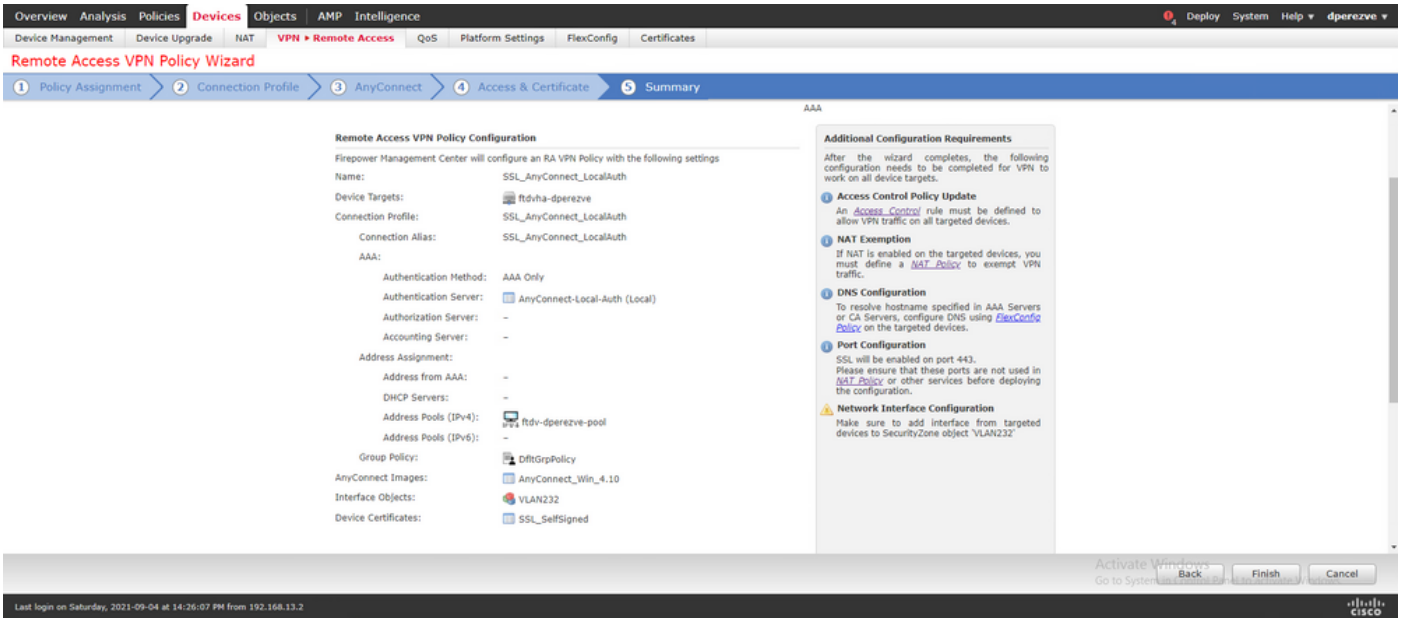
選擇Next以轉到AnyConnect部分。現在，選擇步驟2中上傳的思科安全客戶端映像。



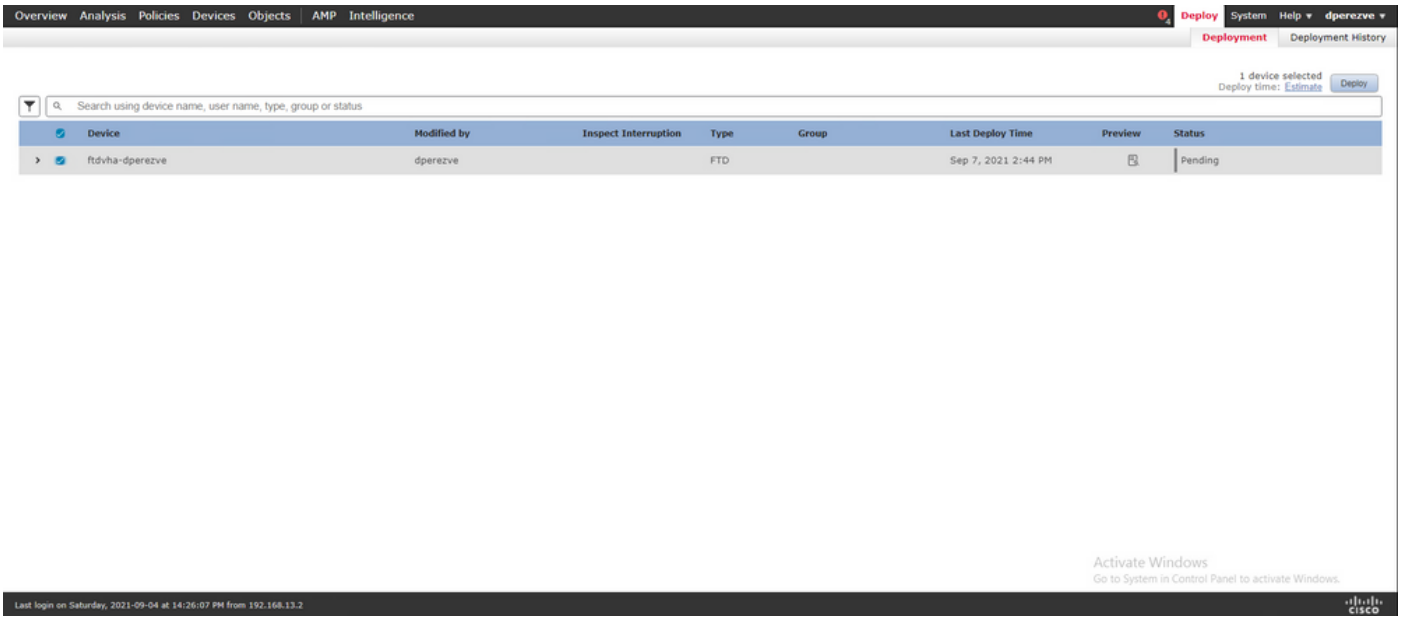
選擇Next以轉到Access & Certificate部分。在「Interface group/Security Zone」下拉選單中，選擇需要啟用Cisco Secure Client(AnyConnect)的介面。然後，在「Certificate Enrollment」下拉選單中，選擇在步驟3中建立的憑證。



最後，選擇下一步以檢視Cisco安全客戶端配置的摘要。

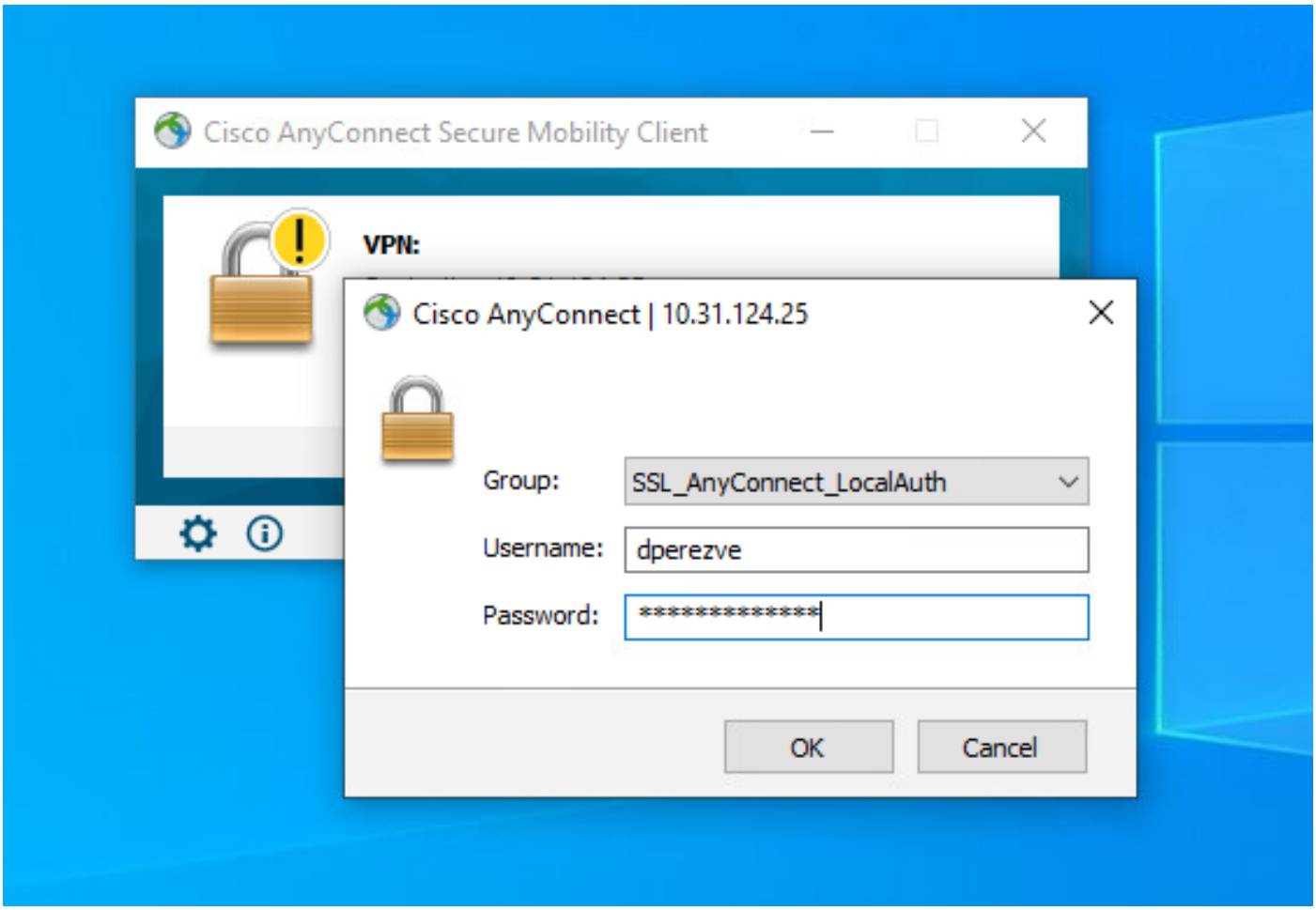


如果所有設定都正確，請選擇完成並將更改部署到FTD。

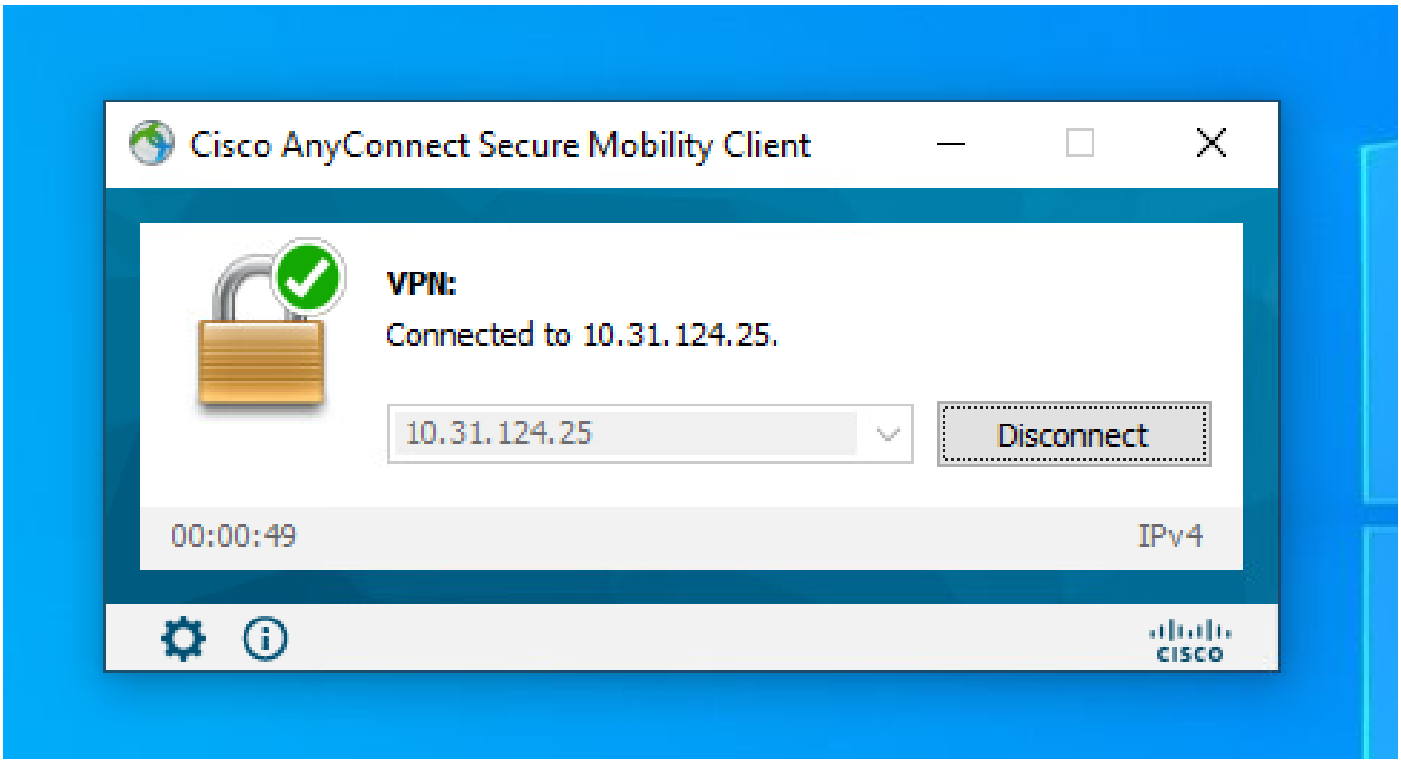


驗證

部署成功後，啟動Cisco AnyConnect安全移動客戶端從Windows客戶端到FTD的連線。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。



憑證經FTD批准後，Cisco AnyConnect安全行動化使用者端應用必須顯示已連線狀態。



您可以在FTD中執行show vpn-sessiondb anyconnect 命令，以顯示防火牆上目前作用中的思科安全使用者端作業階段。

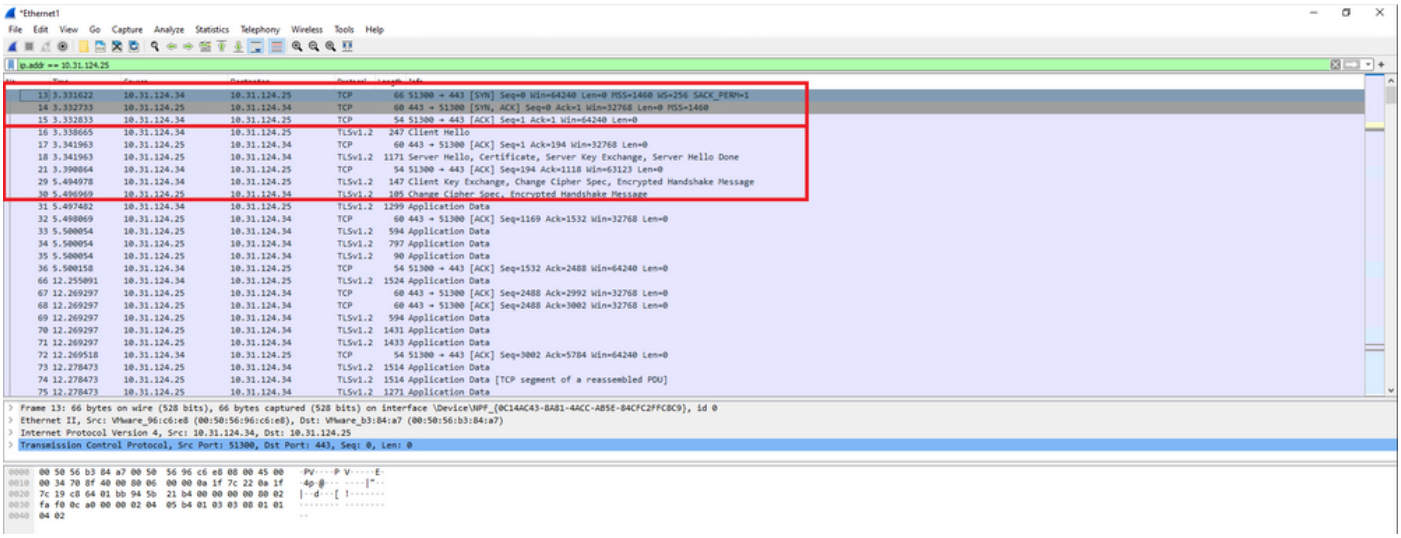
```
firepower# show vpn-sessiondb anyconnect

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 : 00000000000080006137dcc9
Security Grp : none                   Tunnel Zone  : 0
```

疑難排解

在FTD上執行debug webvpn anyconnect 255命令，以檢視FTD上的SSL連線流程。

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

除Cisco安全客戶端調試外，還可以通過TCP資料包捕獲觀察連線流。以下是成功連線的範例，Windows使用者端和FTD之間會完成三次定期交涉，然後執行一次用於同意密碼的SSL交涉。



協定握手後，FTD必須使用儲存在本地領域中的資訊驗證憑據。

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）。