在FMC管理的FTD上設定安全使用者端憑證驗證

目錄

簡介

本檔案介紹在由Firepower管理中心(FMC)透過憑證驗證管理的Firepower威脅防禦(FTD)上設定遠端存取VPN的程式。

作者：Dolly Jain和Rishabh Aggarwal，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

· 手動註冊憑證及SSL的基本概念
· FMC
· 遠端訪問VPN的基本身份驗證知識
· 第三方證書頒發機構(CA)，如Entrust、Geotrust、GoDaddy、Thawte和VeriSign

採用元件

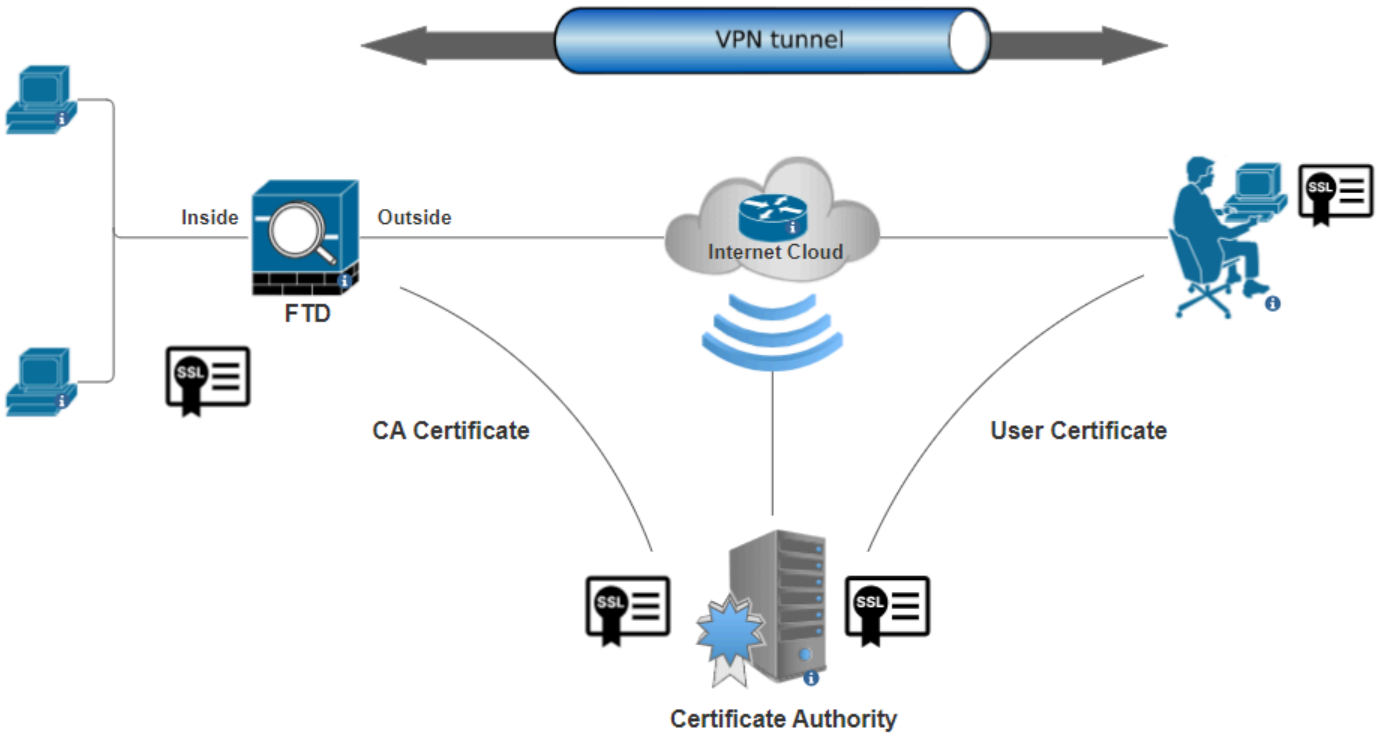
本檔案中的資訊是根據以下軟體版本：

· 安全Firepower威脅防禦7.4.1版
· Firepower管理中心(FMC)版本7.4.1
· 安全使用者端5.0.05040版
· Microsoft Windows Server 2019作為CA伺服器

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

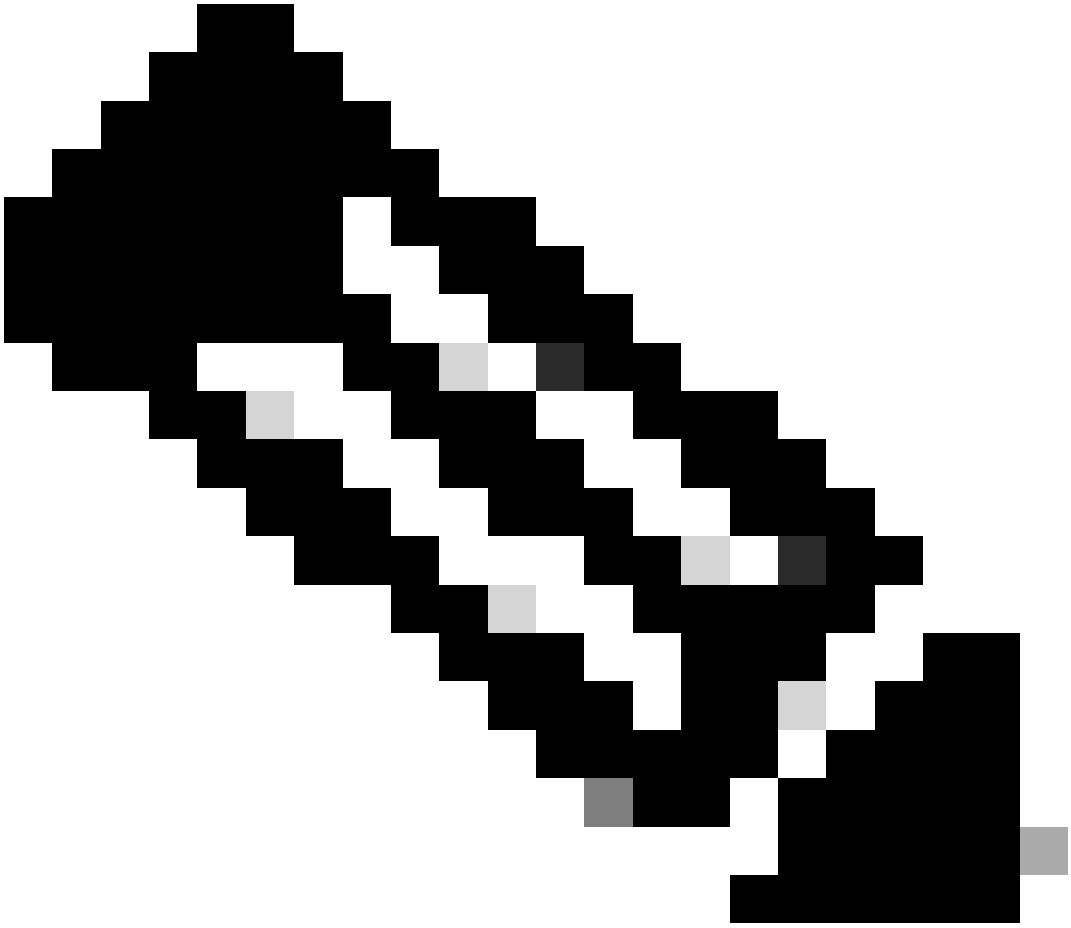
網路圖表



網路圖表

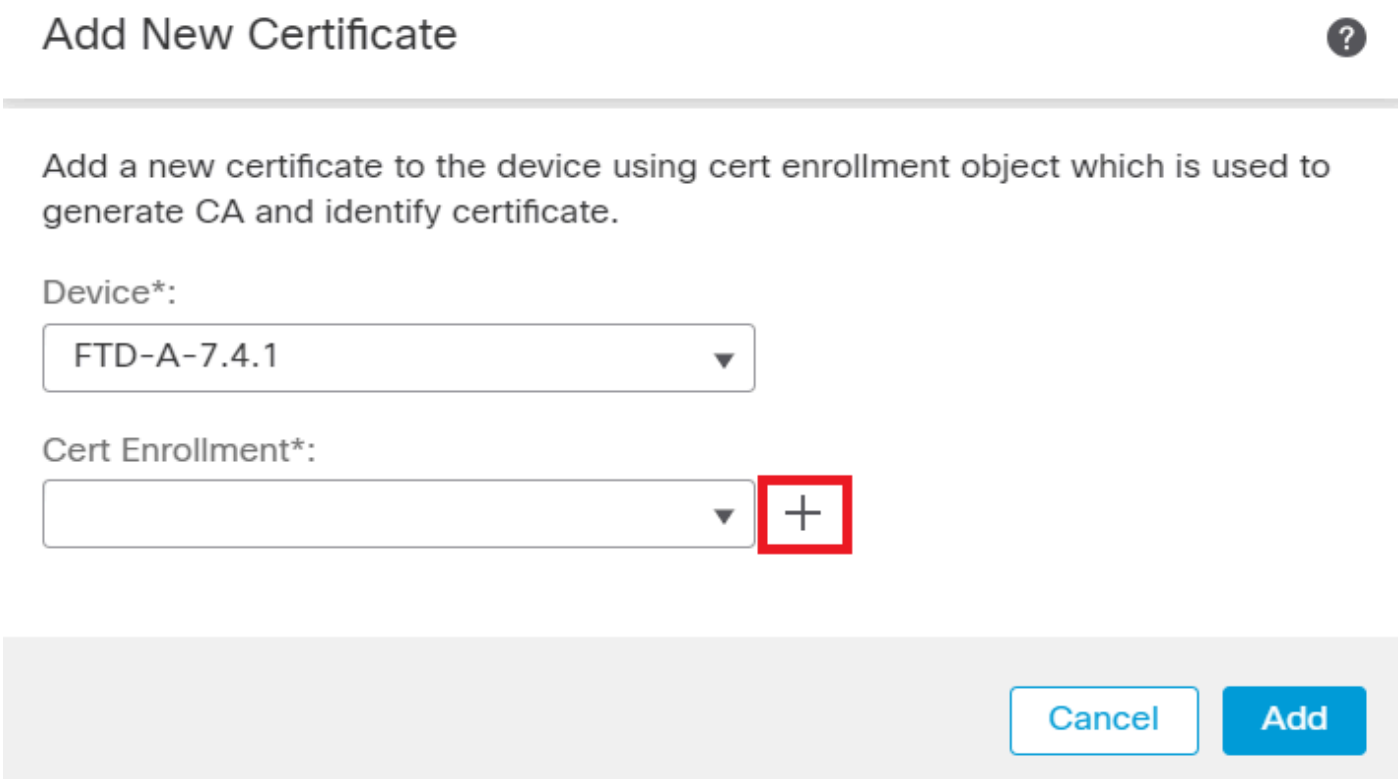
組態

a.建立/匯入用於伺服器驗證的憑證



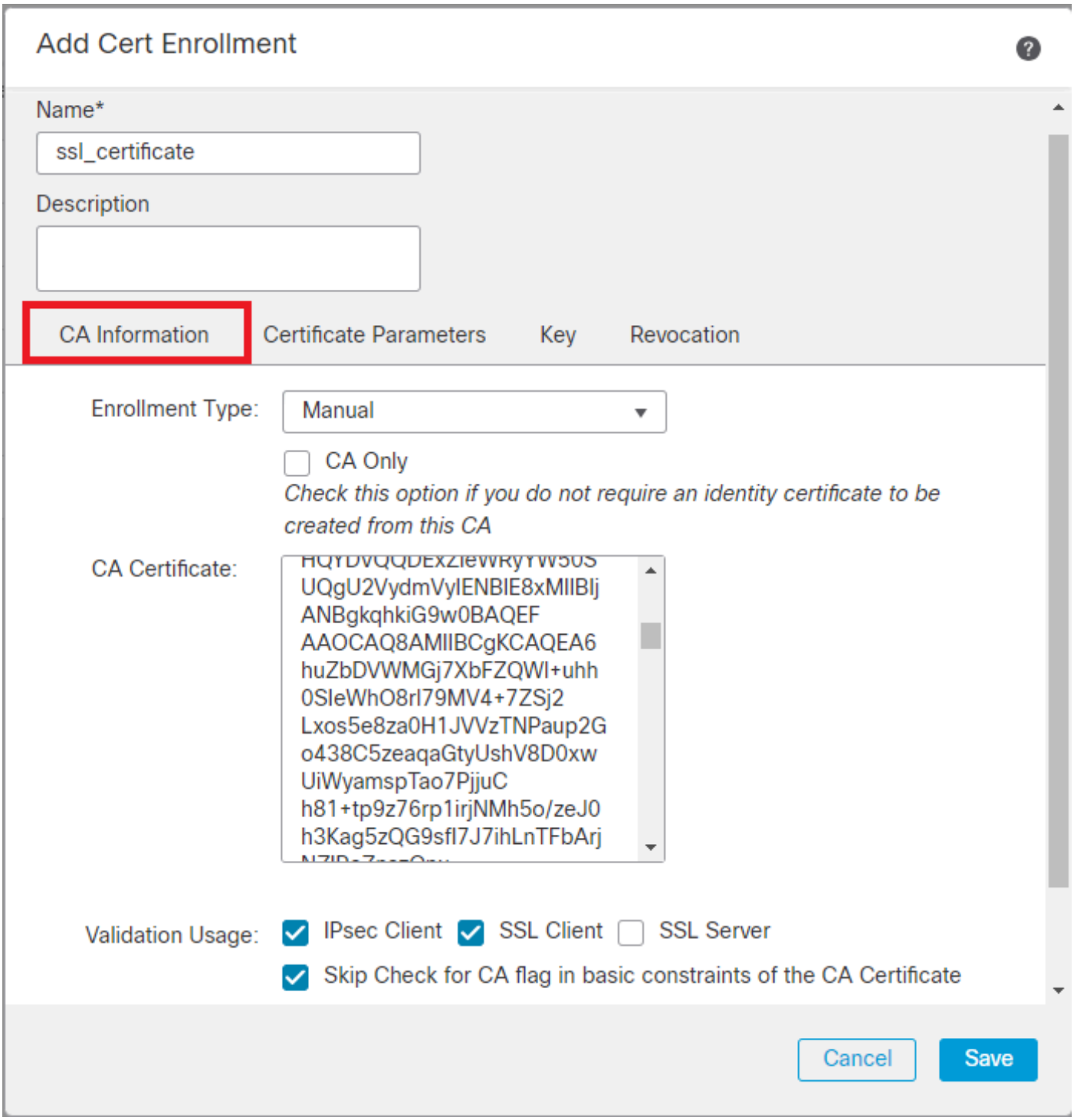
附註：在FMC上，產生CSR之前需有CA憑證。如果從外部源（OpenSSL或第三方）生成CSR，則手動方法失敗，必須使用PKCS12證書格式。

步驟 1.導航到 Devices > Certificates，然後按一下Add。選擇Device（裝置），然後點選Cert Enrollment（證書註冊）下的加號(+)。



增加證書註冊

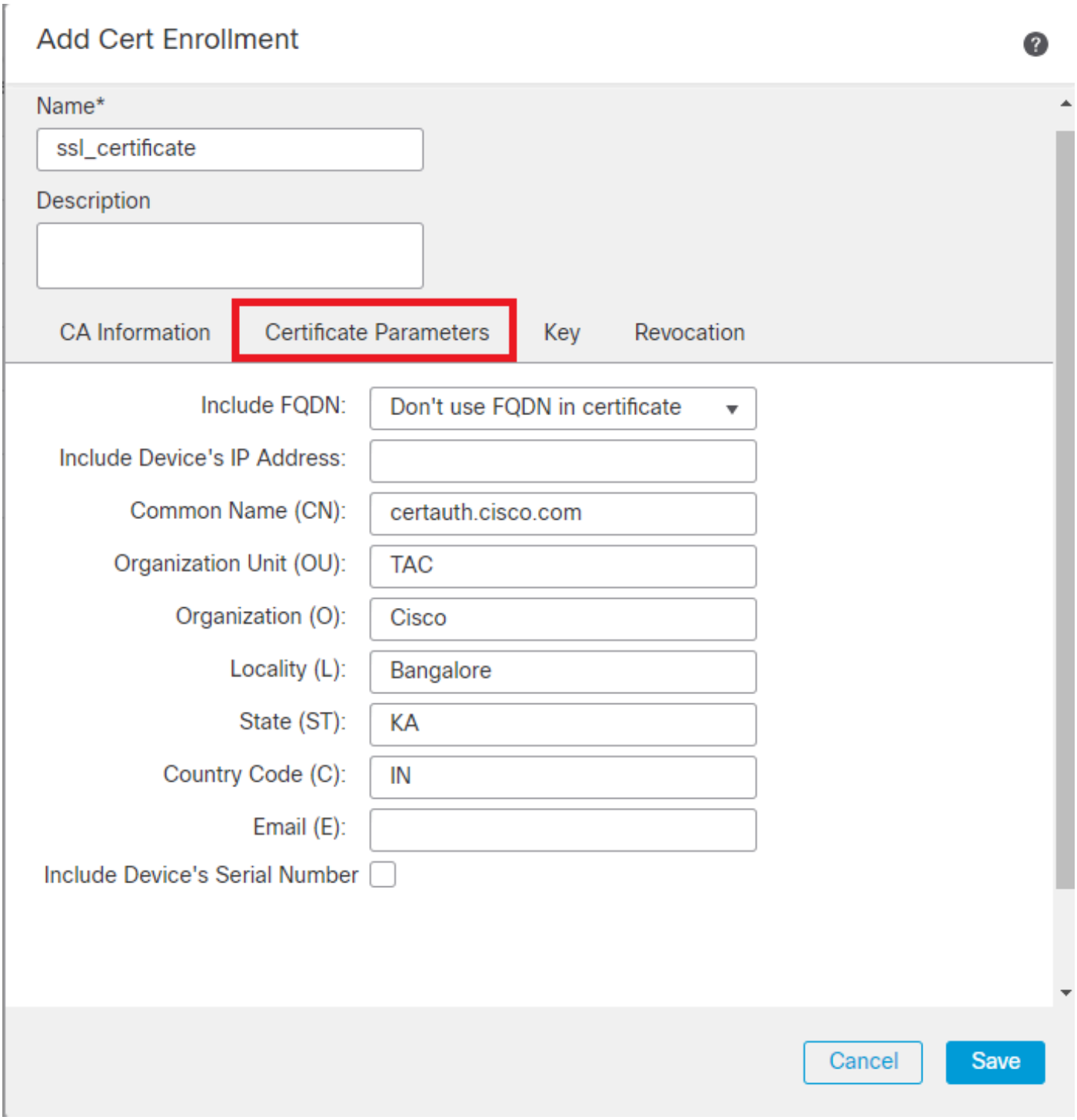
步驟 2. 在CA Information下，選擇「Enrollment Type」作為Manual，並貼上用於簽署CSR的證書頒發機構(CA)證書。



增加*CA*資訊

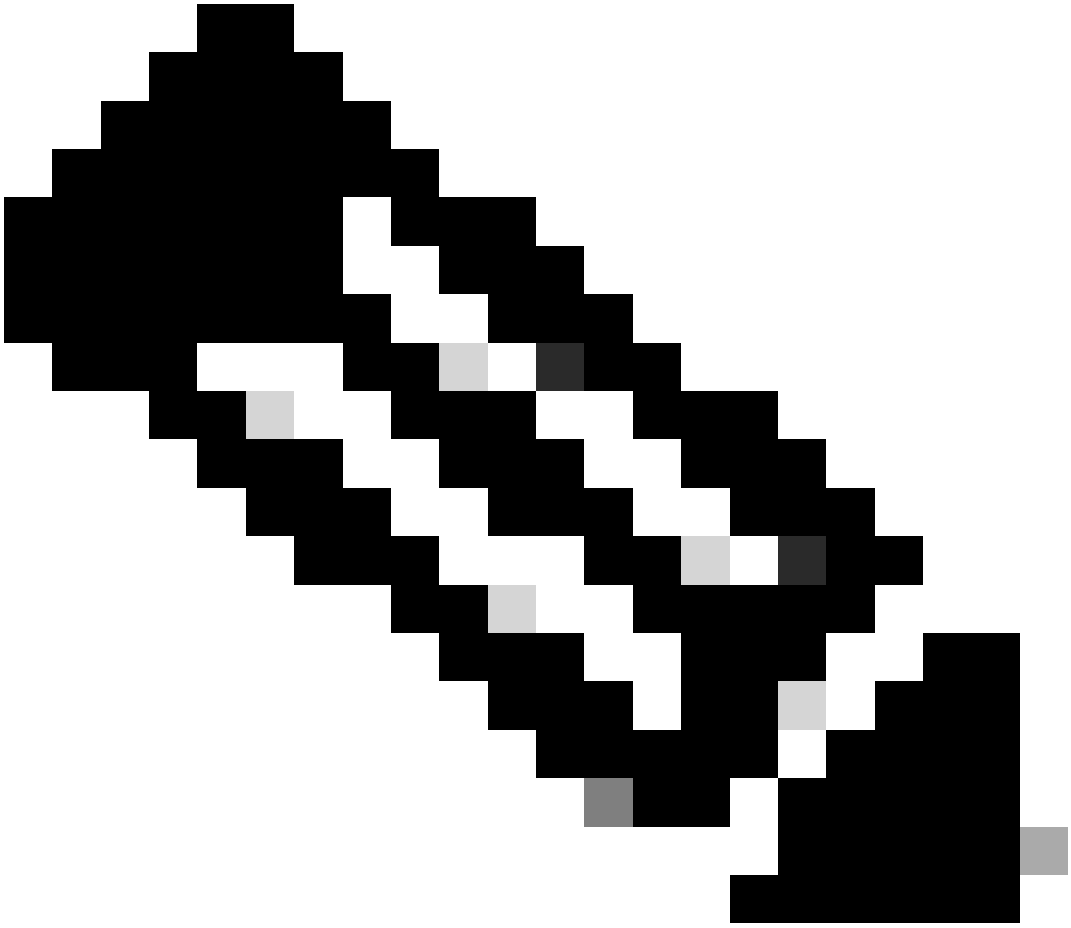
步驟 3.對於驗證用法，選擇IPsec Client, SSL Client和Skip Check for CA flag in basic constraints of the CA Certificate。

步驟 4.在Certificate Parameters下，填寫主題名稱詳細資訊。

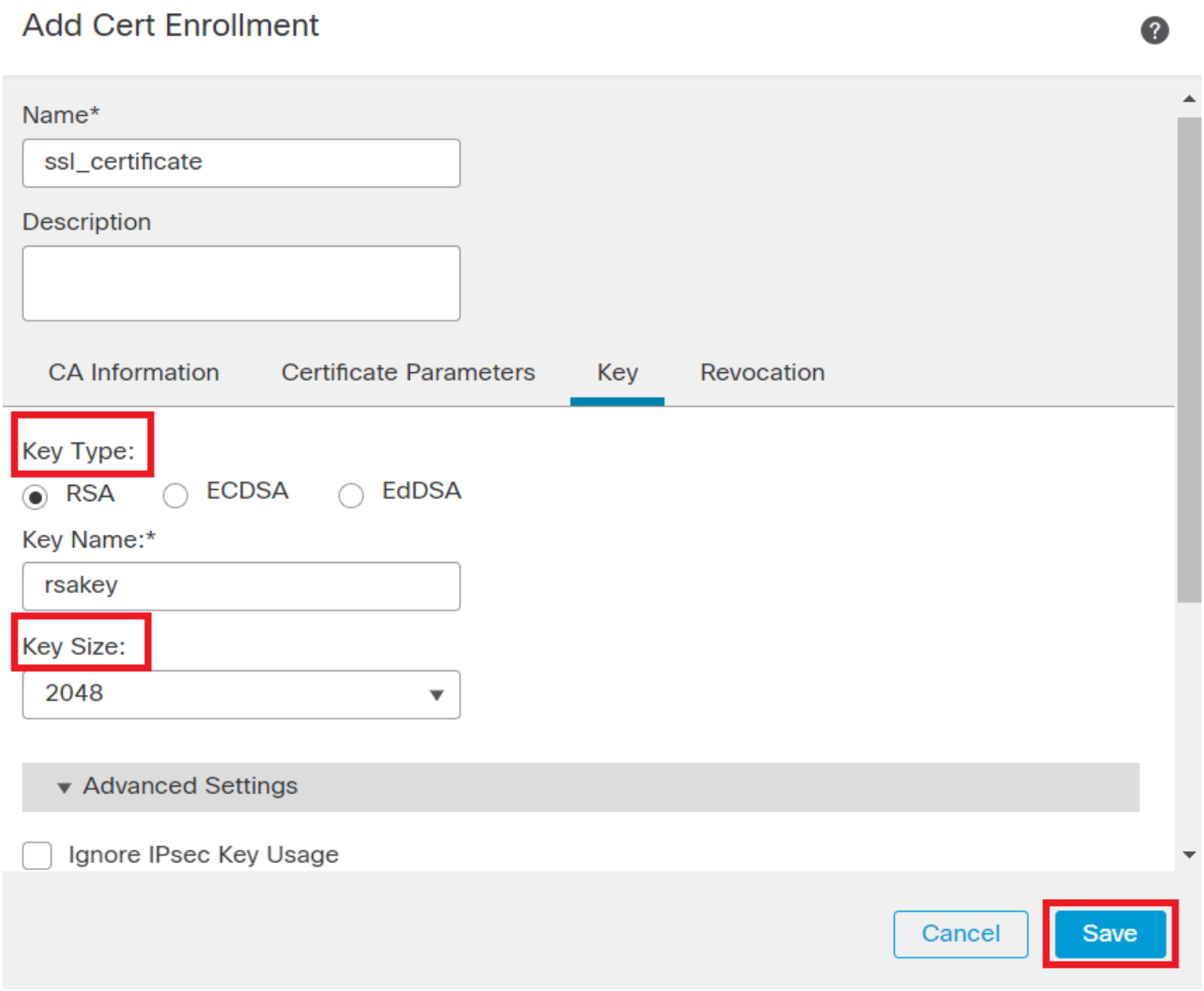


增加證書引數

步驟 5.在Key下選擇金鑰型別為RSA且具有金鑰名稱和大小。 按一下Save。

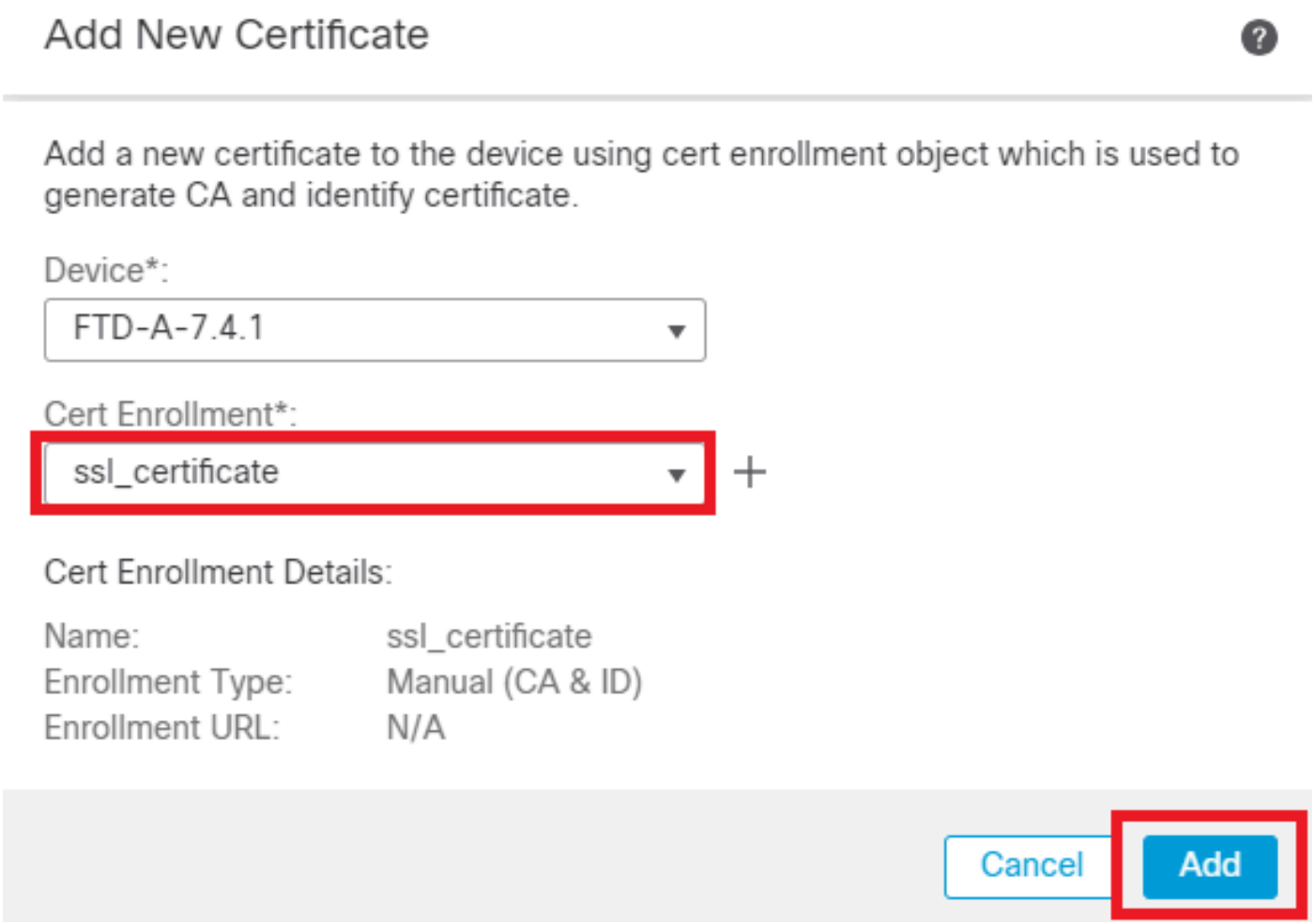


注意：對於RSA金鑰型別，最小金鑰大小為2048位。



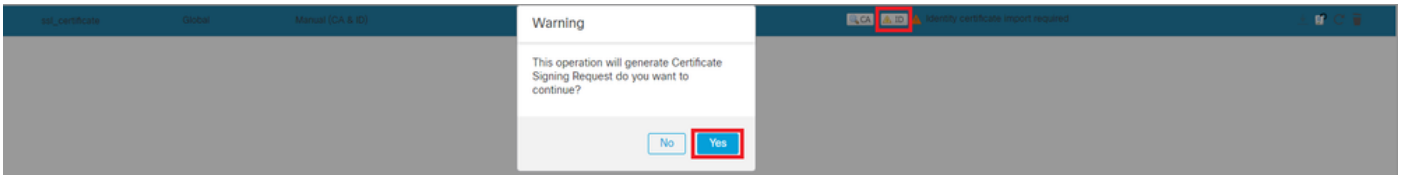
增加*RSA*金鑰

步驟 6.在Cert Enrollment下，從剛建立的下拉選單中選擇信任點，然後按一下Add。



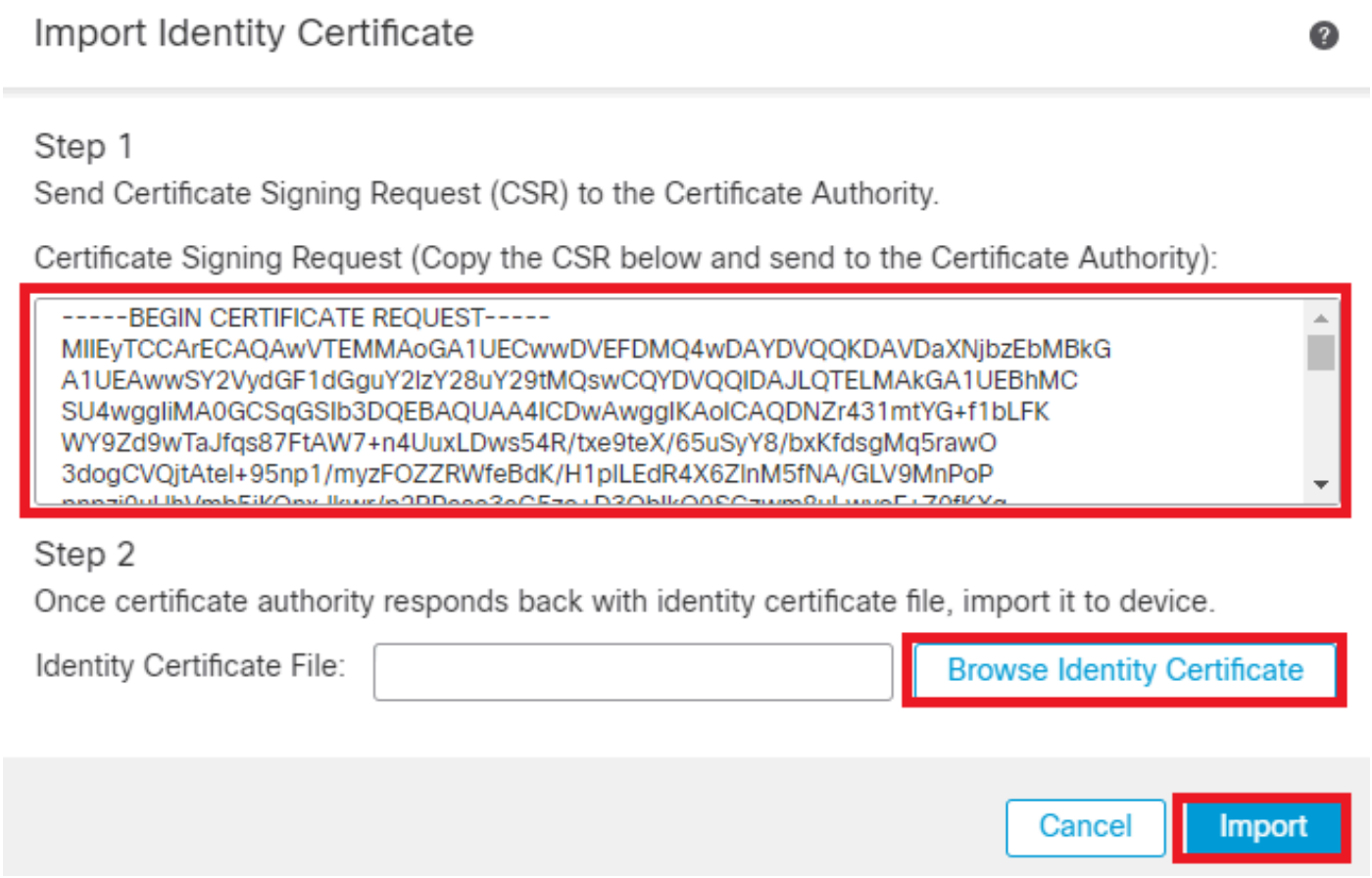
增加新證書

步驟 7.點選ID，然後點選Yes，顯示進一步的提示，生成CSR。

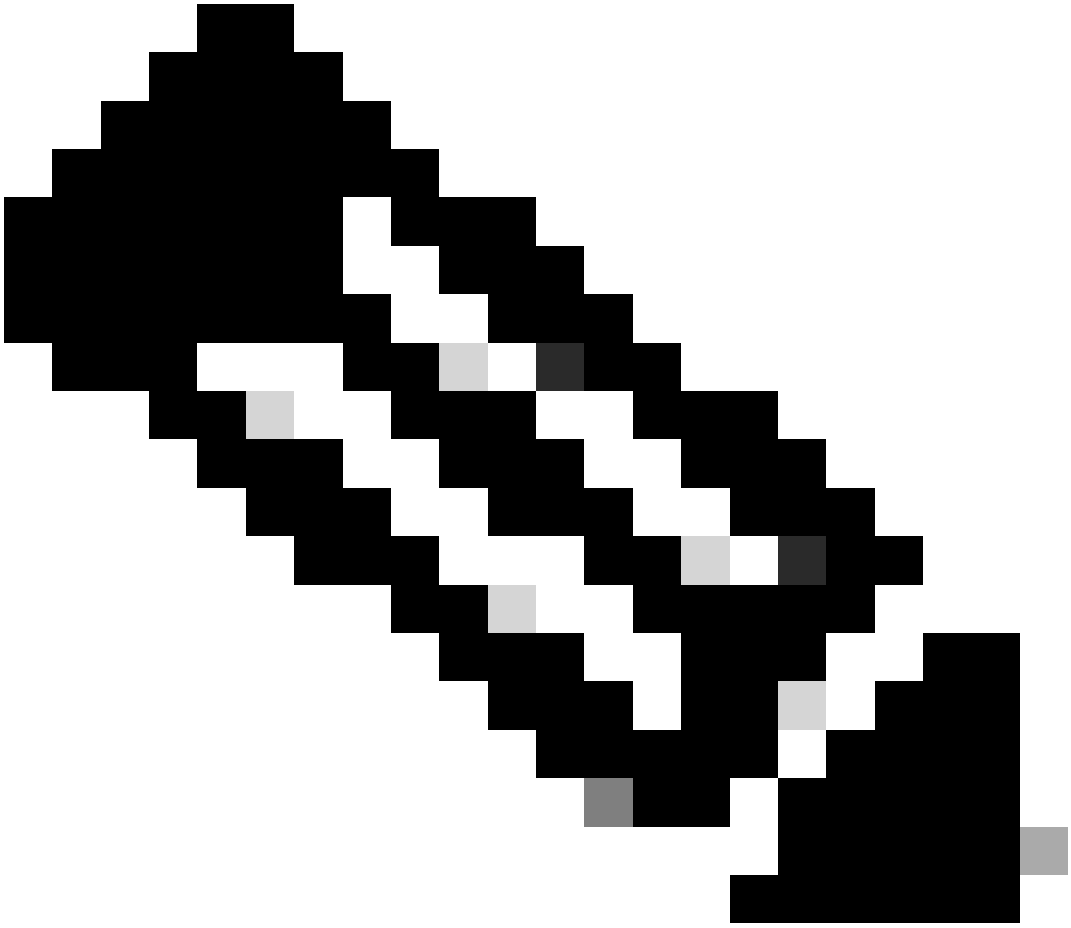


產生*CSR*

步驟 8.複製CSR並由憑證授權單位簽署。身份證書由CA發佈之後，透過按一下Browse Identity Certificate和Import進行導入。


Import Identity Certificate
Step 1
Send Certificate Signing Request (CSR) to the Certificate Authority.
Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):
-----BEGIN CERTIFICATE REQUEST-----
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMAkGA1UEBhMC
SU4wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1plLEdR4X6ZlnM5fNA/GLV9MnPoP
Step 2
Once certificate authority responds back with identity certificate file, import it to device.
Identity Certificate File:
Browse Identity Certificate
Cancel
Import

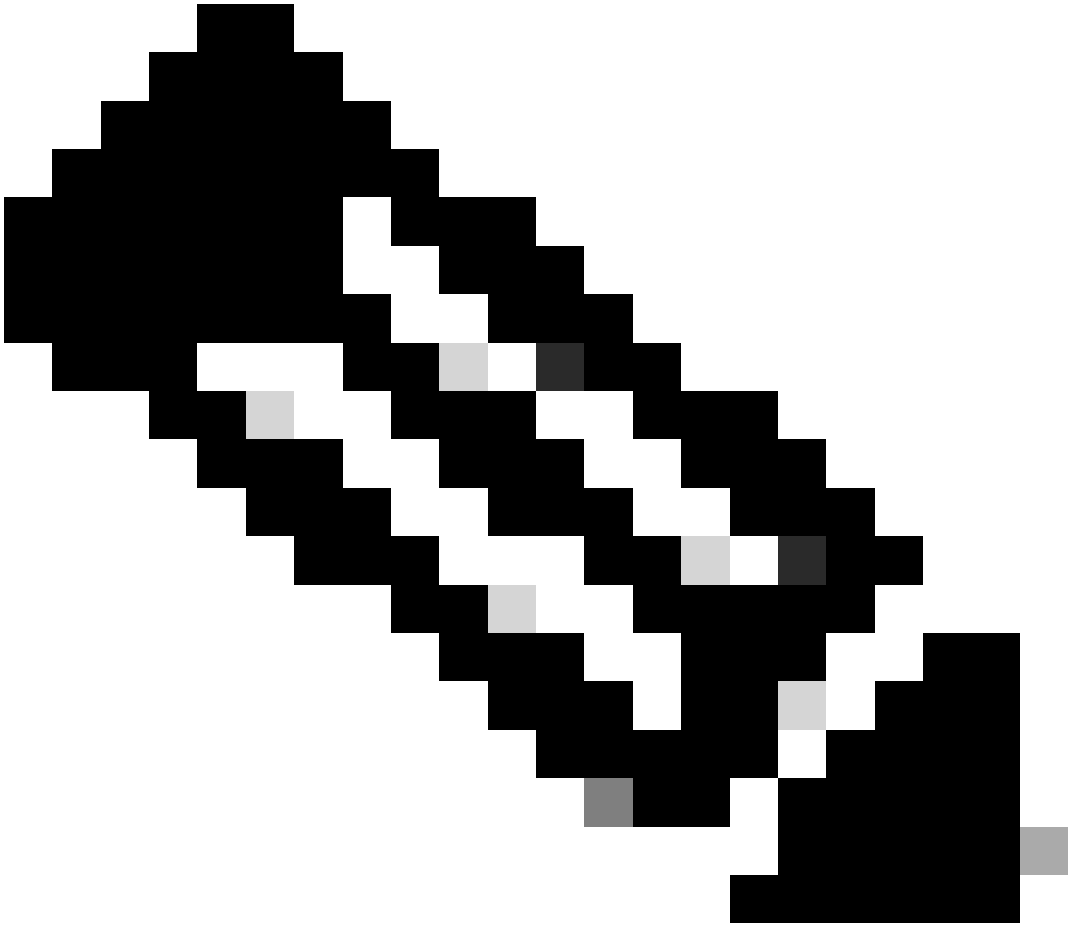
匯入*ID*憑證



注意：如果頒發ID證書需要時間，則可在以後重複步驟7。這將生成相同的CSR，我們可以導入ID證書。

---

b.增加受信任/內部CA證書

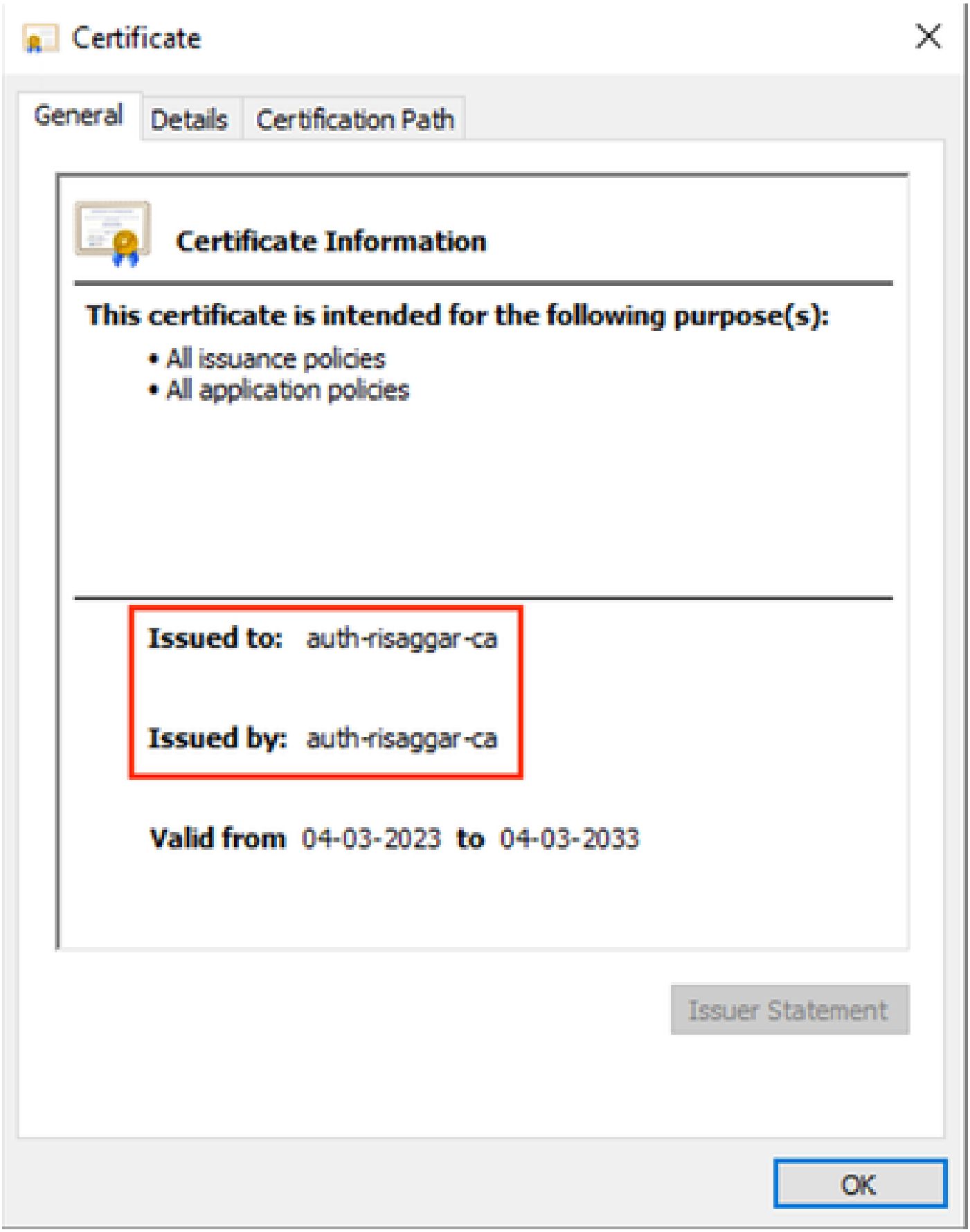


注意：如果步驟(a)「**建立/匯入用於伺服器驗證的憑證**」中使用的**憑證授權(**CA)**也會**發出使用者憑證，您可以跳過**步驟(b)**，「**新增受信任/內部CA憑證**」。 不需要再次增加相同的CA證書，也必須避免這種情況。如果再次增加相同的CA證書，則信任點配置為「validation-usage none」，這可能會影響RAVPN的證書身份驗證。

步驟 1.導航到Devices > Certificates，然後按一下Add。

選擇Device（裝置），然後點選Cert Enrollment（證書註冊）下的加號(+)。

此處，「auth-risaggar-ca」用於頒發身份/使用者證書。

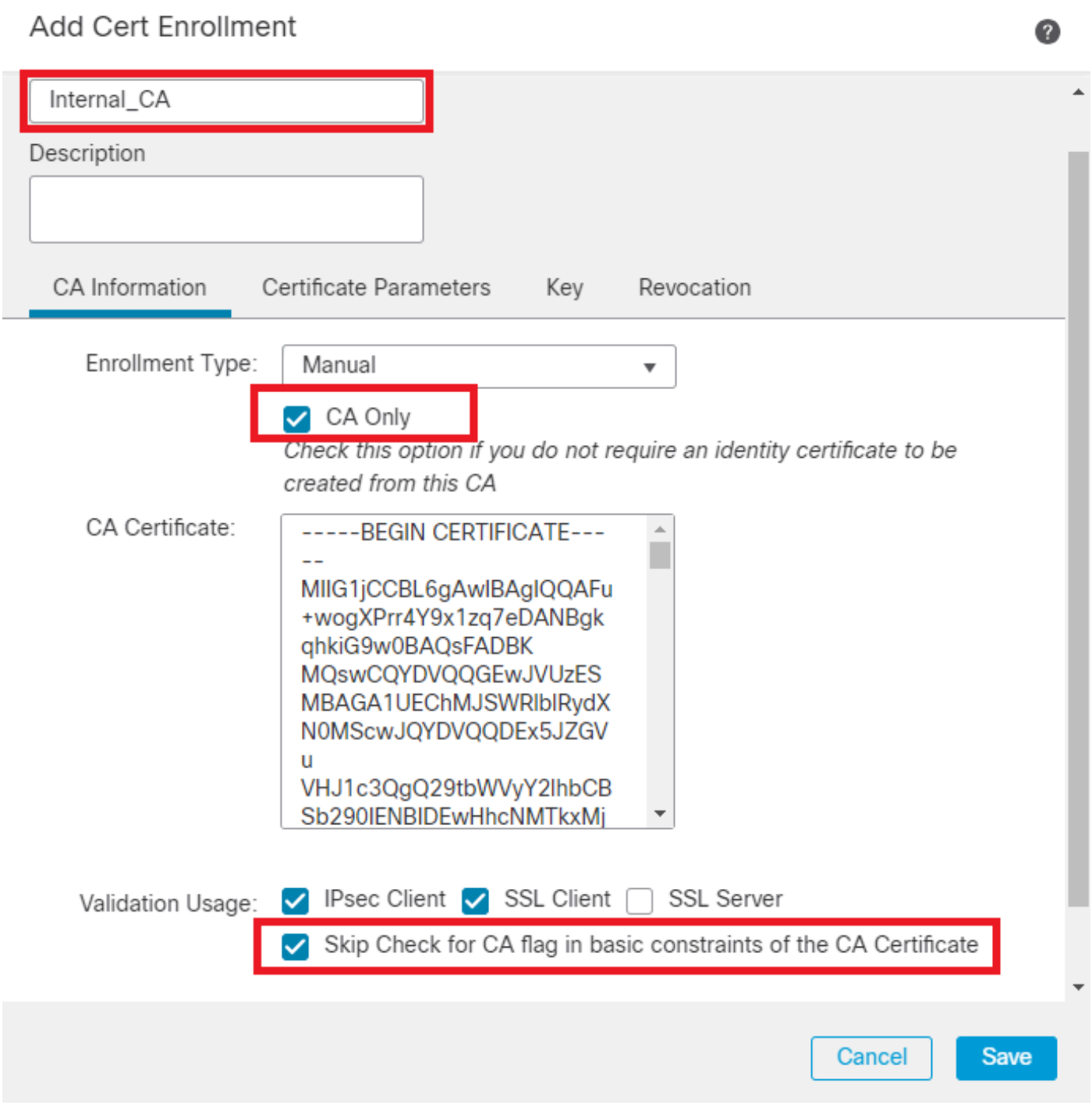


auth-risaggar-ca

步驟 2.輸入信任點名稱，然後在CA information下選擇Manual作為註冊型別。

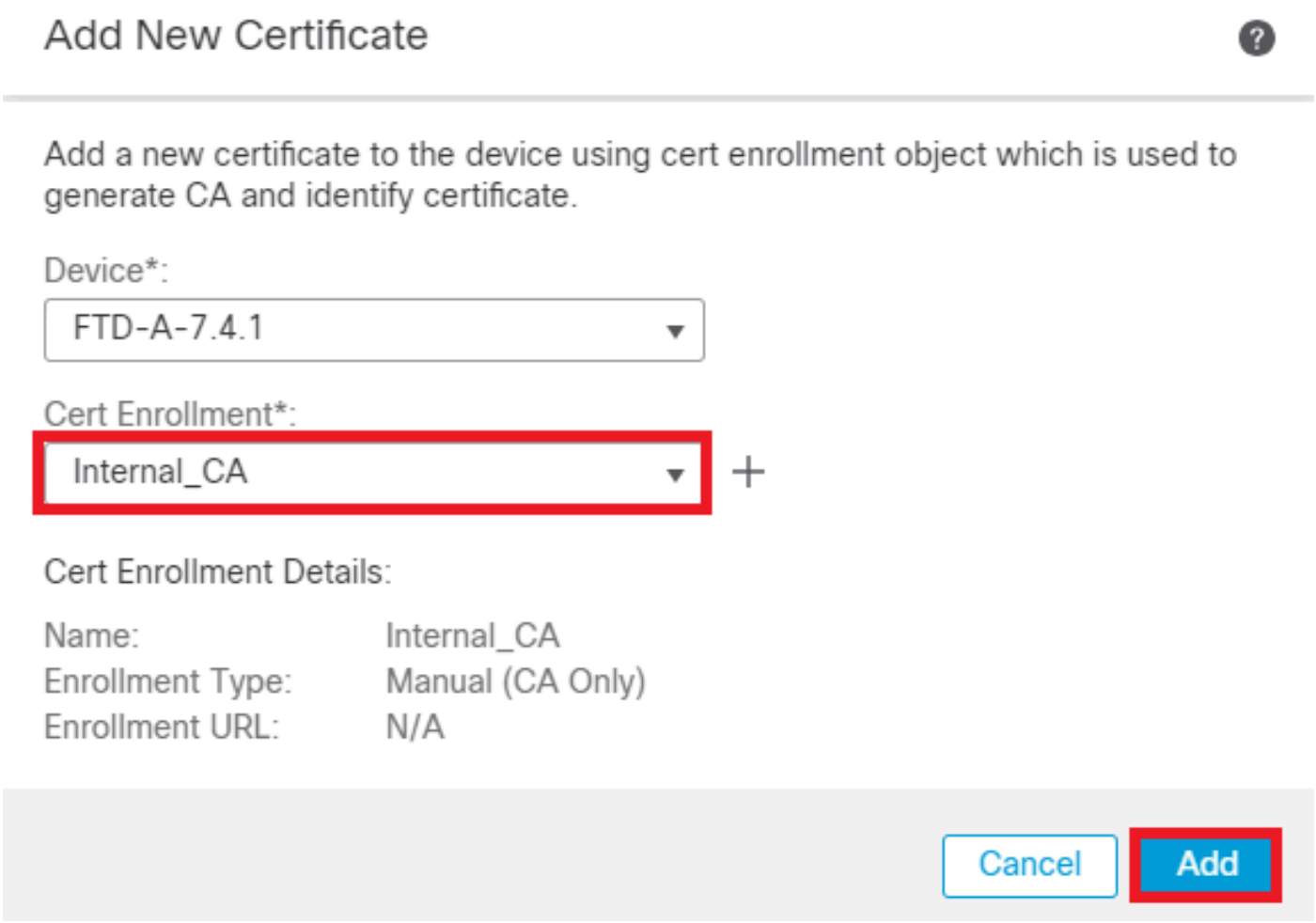
步驟 3.選中CA Only並貼上採用pem格式的受信任/內部CA證書。

步驟 4.選中**Skip Check for CA flag in basic constraints of the CA Certificate**並按一下Save。



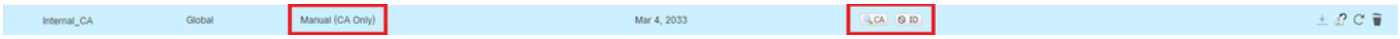
增加信任點

步驟 5. 在Cert Enrollment下，從剛建立的下拉選單中選擇信任點，然後按一下Add。



增加內部*CA*

步驟 6.之前增加的證書顯示為：

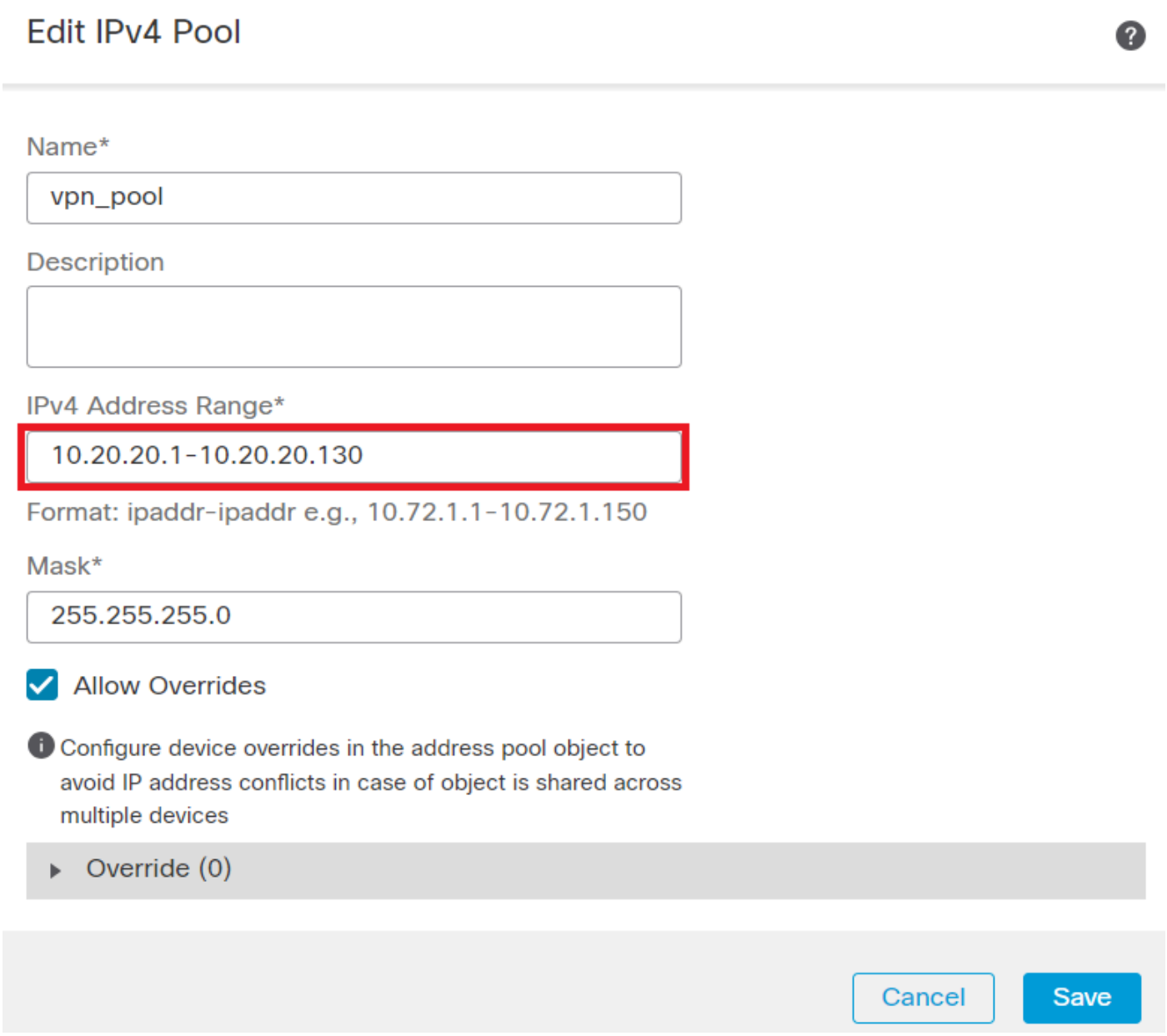


已增加證書

c.配置VPN使用者的地址池

步驟 1.導航到Objects > Object Management > Address Pools > IPv4 Pools。

步驟 2.輸入名稱及帶掩碼的IPv4地址範圍。



增加*IPv4*池

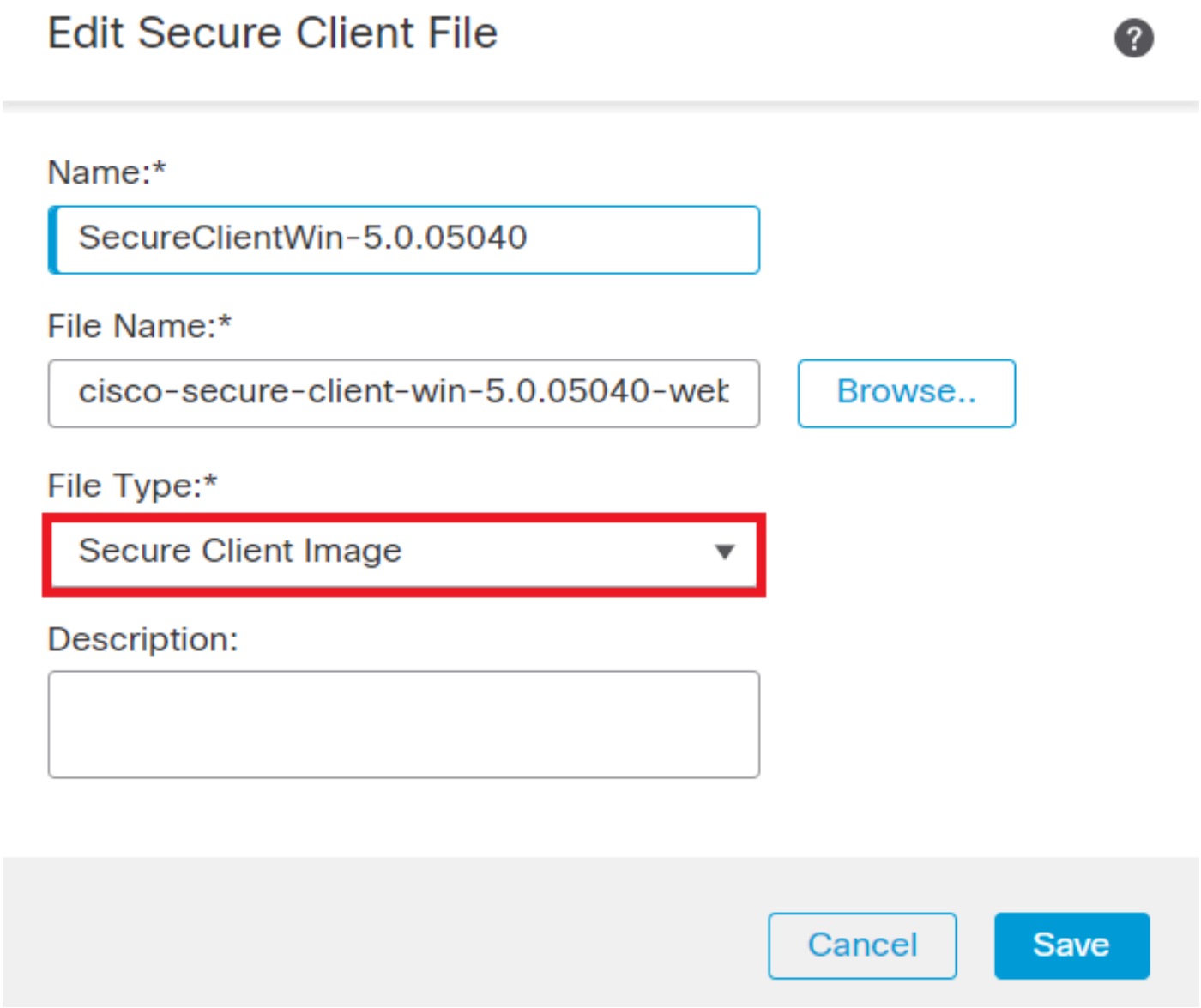
d.上傳安全客戶端映像

步驟 1.根據OS從思科軟體站點下載webdeploy安全客戶端映像。

步驟 2.導航到Objects > Object Management > VPN > Secure Client File > Add Secure Client File。

步驟 3.輸入名稱，然後從磁碟中選擇Secure Client檔案。

步驟 4.選取檔案型別作為Secure Client Image，然後按一下Save。



增加安全客戶端映像

e.建立和上傳XML配置檔案

步驟 1.從Cisco軟體站點下載並安裝Secure ClientProfile Editor。

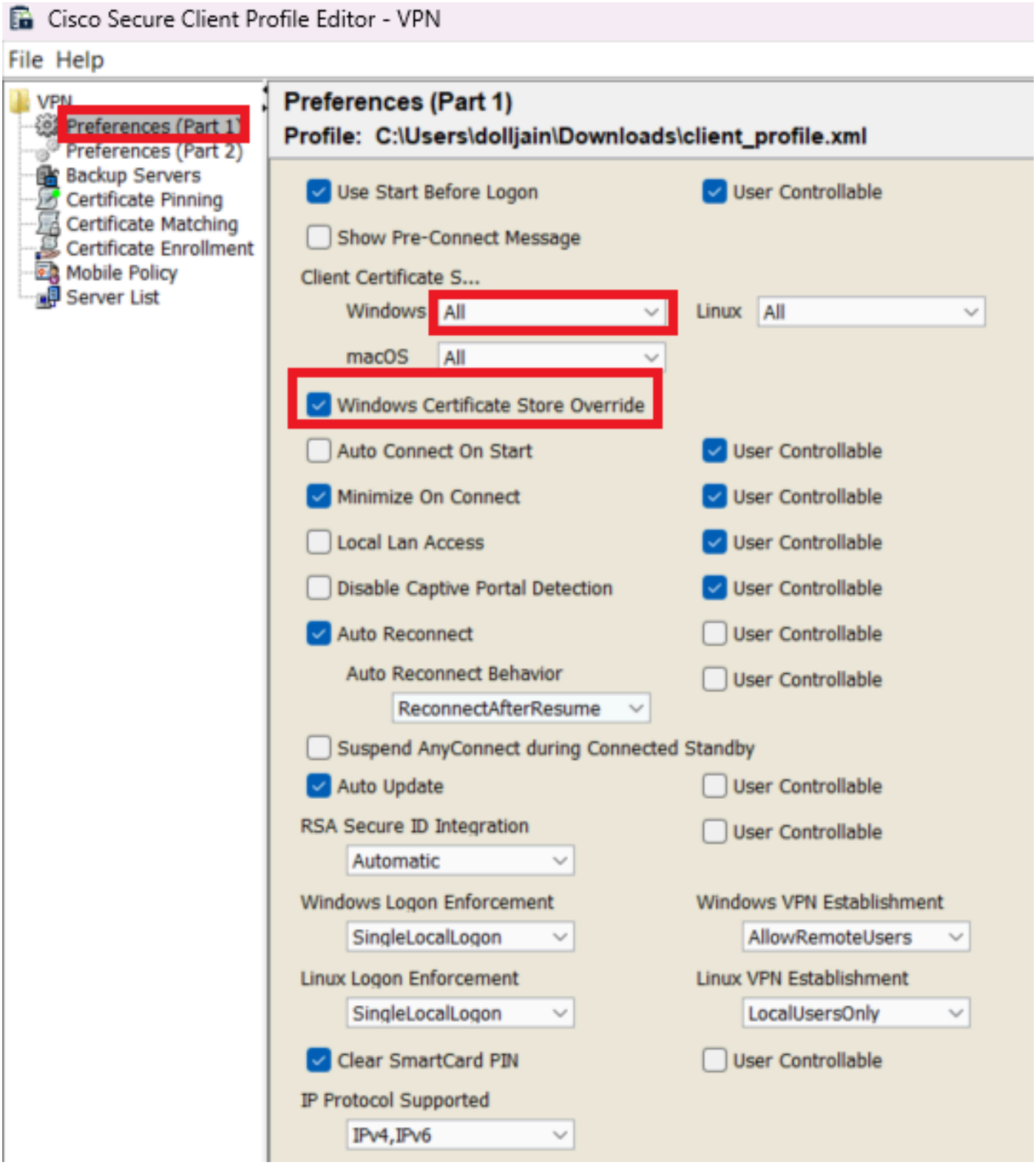
步驟 2.建立新配置檔案並從Client Certificate Selection下拉選單中選擇All。它主要控制Secure Client可以使用哪些證書儲存區來儲存和讀取證書。

其他兩個可用選項為：

- **電腦** -安全客戶端被限制為在Windows本地電腦證書儲存上查詢證書。
- **User** - Secure Client受限於在本地Windows使用者證書儲存上查詢證書。

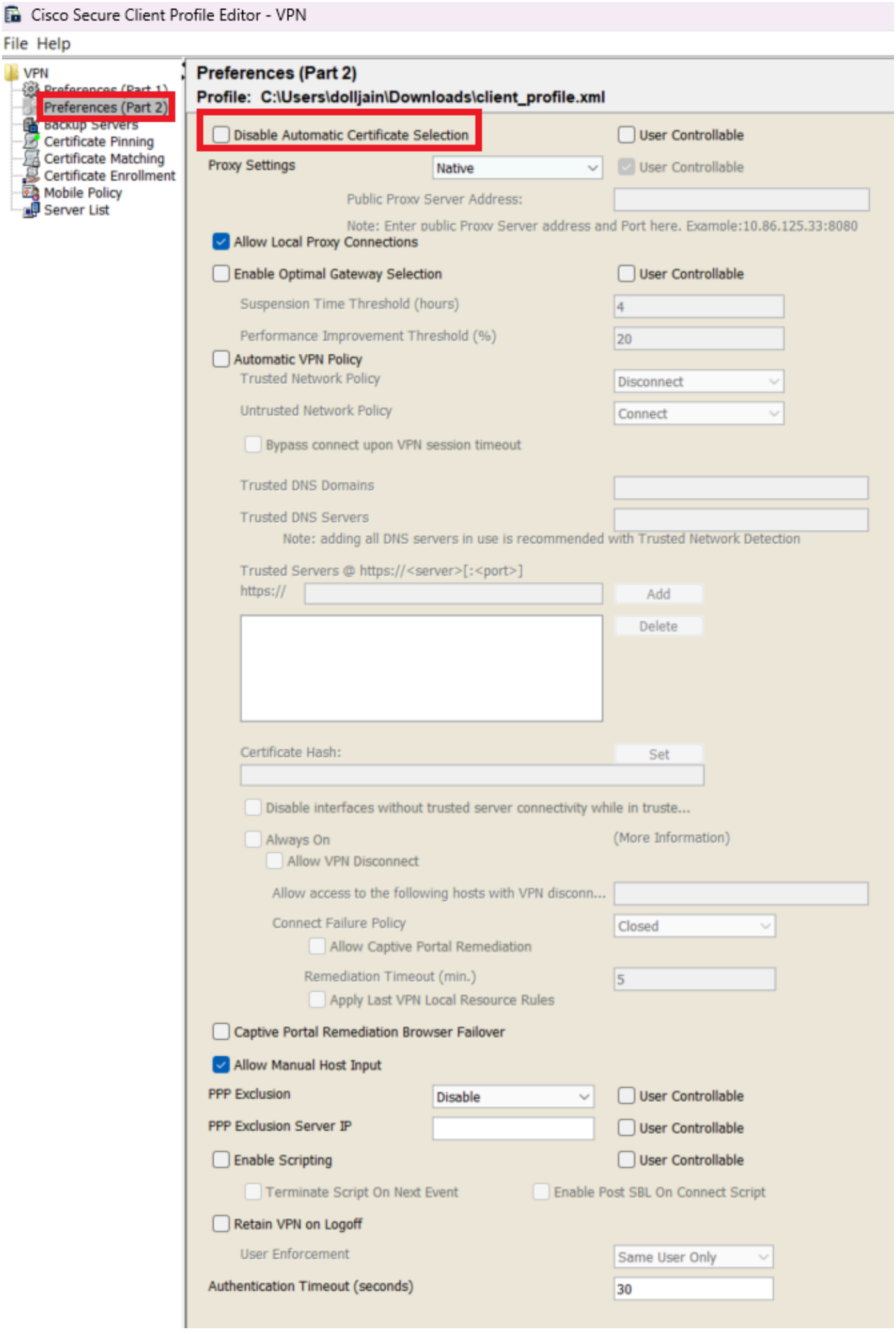
將證書儲存覆蓋設定為True 。

這允許管理員指示Secure Client利用Windows電腦（本地系統）證書儲存中的證書進行客戶端證書身份驗證。憑證存放區覆寫僅適用於SSL，依預設，UI處理作業會在此起始連線。使用IPSec/IKEv2時，安全客戶端配置檔案中的此功能不適用。



加入偏好設定（第1部分）

步驟3.（可選）取消選中Disable Automatic Certificate Selection，因為它避免了提示使用者選擇身份驗證證書。

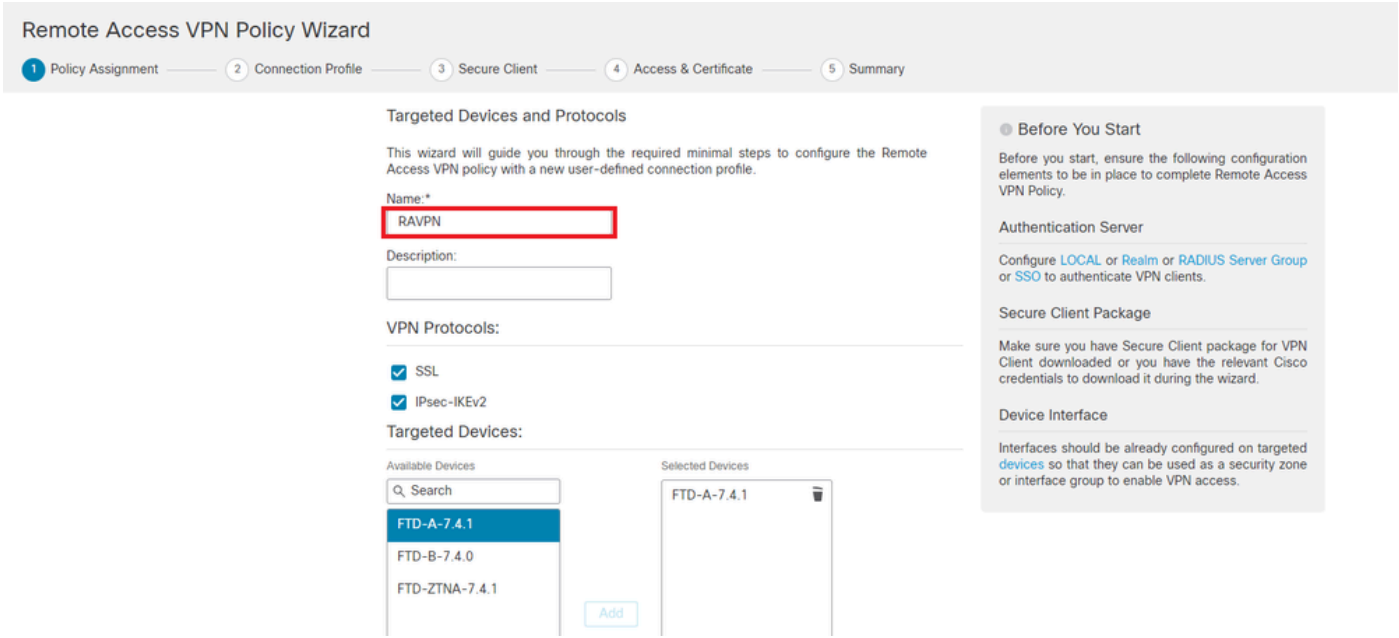


加入偏好設定(Part2)

注意：安全客戶端使用此ACL向內部資源增加安全路由。

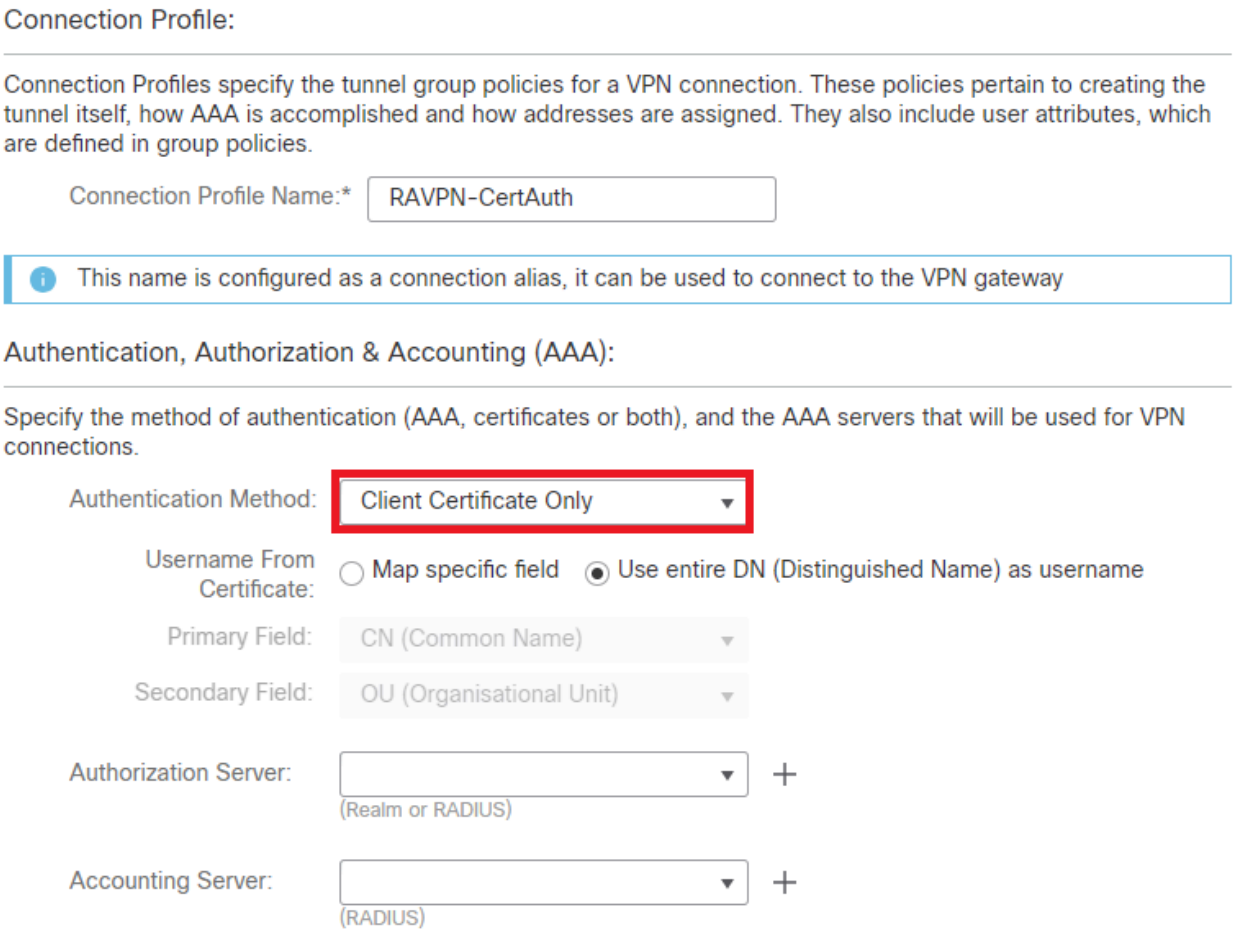
步驟 2.導航到Devices > VPN > Remote Access，然後按一下Add。

步驟 3.輸入設定檔的名稱，然後選取FTD裝置，再按下一步。



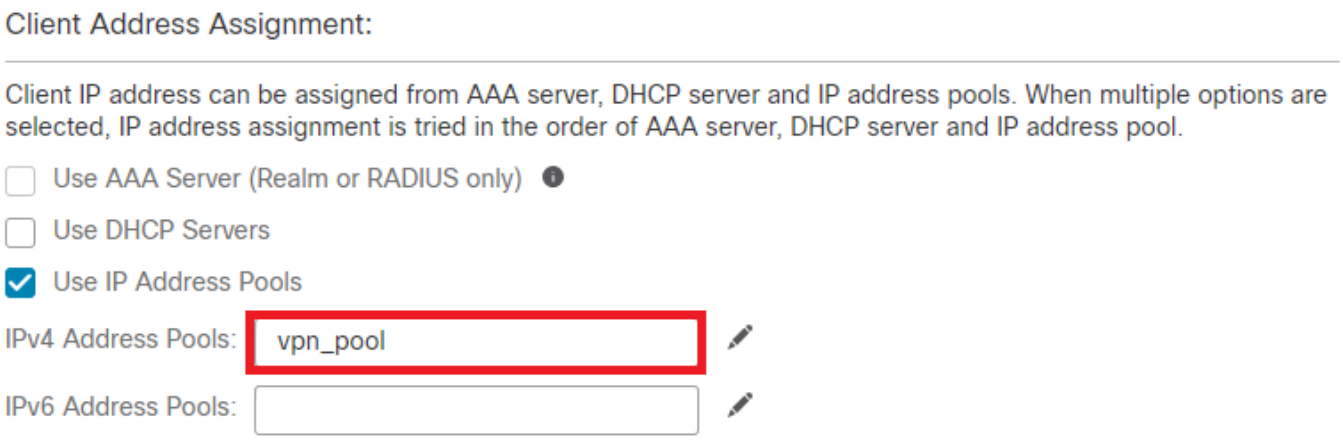
新增設定檔名稱

步驟 4.在「Authentication， Authorization and Accounting (AAA)」下，輸入Connection Profile Name並選擇Client Certificate Only「Authentication Method」。



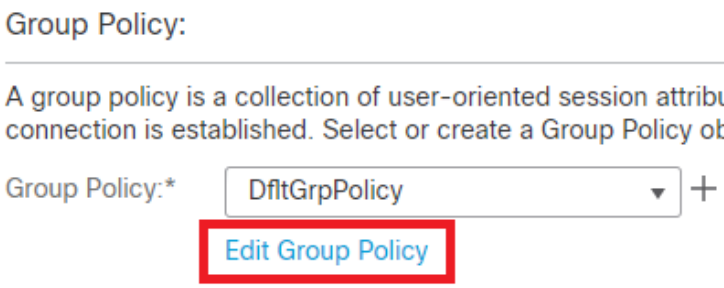
選取驗證方法

步驟 5.按一下Client Address Assignment下的Use IP Address Pools 並選擇之前建立的IPv4地址池。



選擇客戶端地址分配

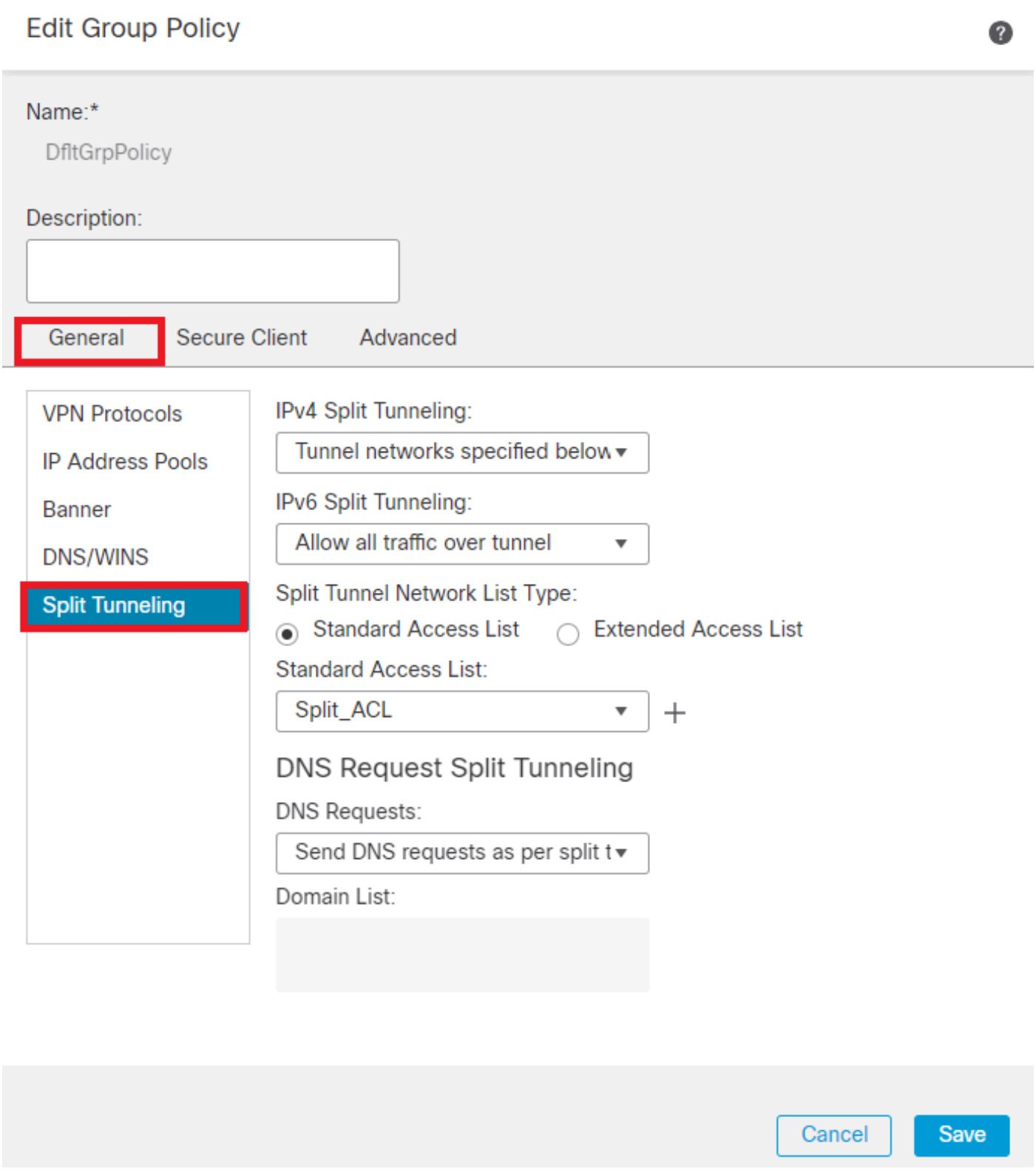
步驟 6.編輯組策略。



編輯組策略

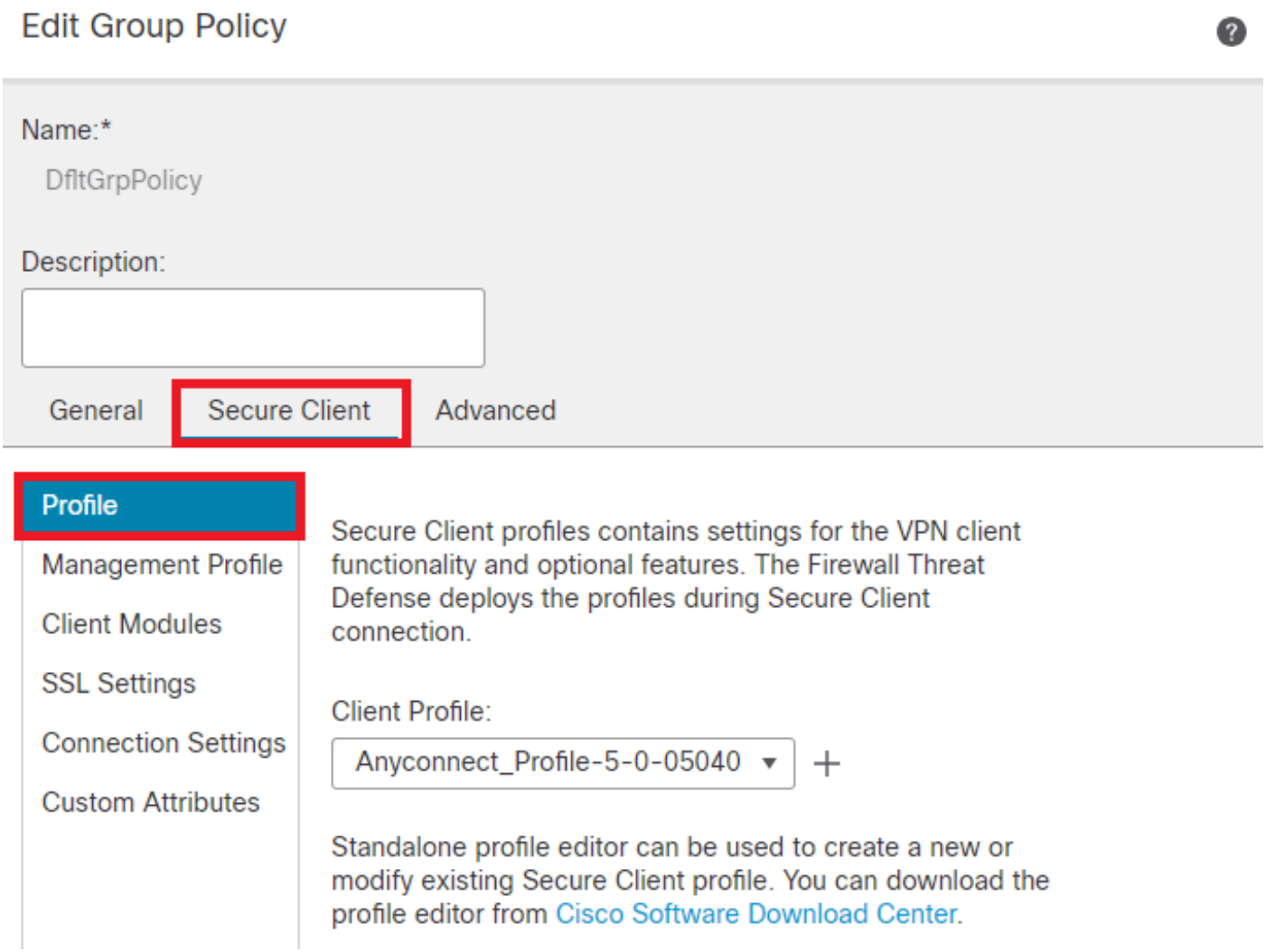
步驟 7.導航到General > Split Tunneling，選擇Tunnel networks specified below，然後在Split Tunnel Network List Type下選擇Standard Access List。

選擇之前建立的ACL。



增加分割隧道

步驟 8.導航到Secure Client > Profile，選擇Client Profile ，然後按一下Save。

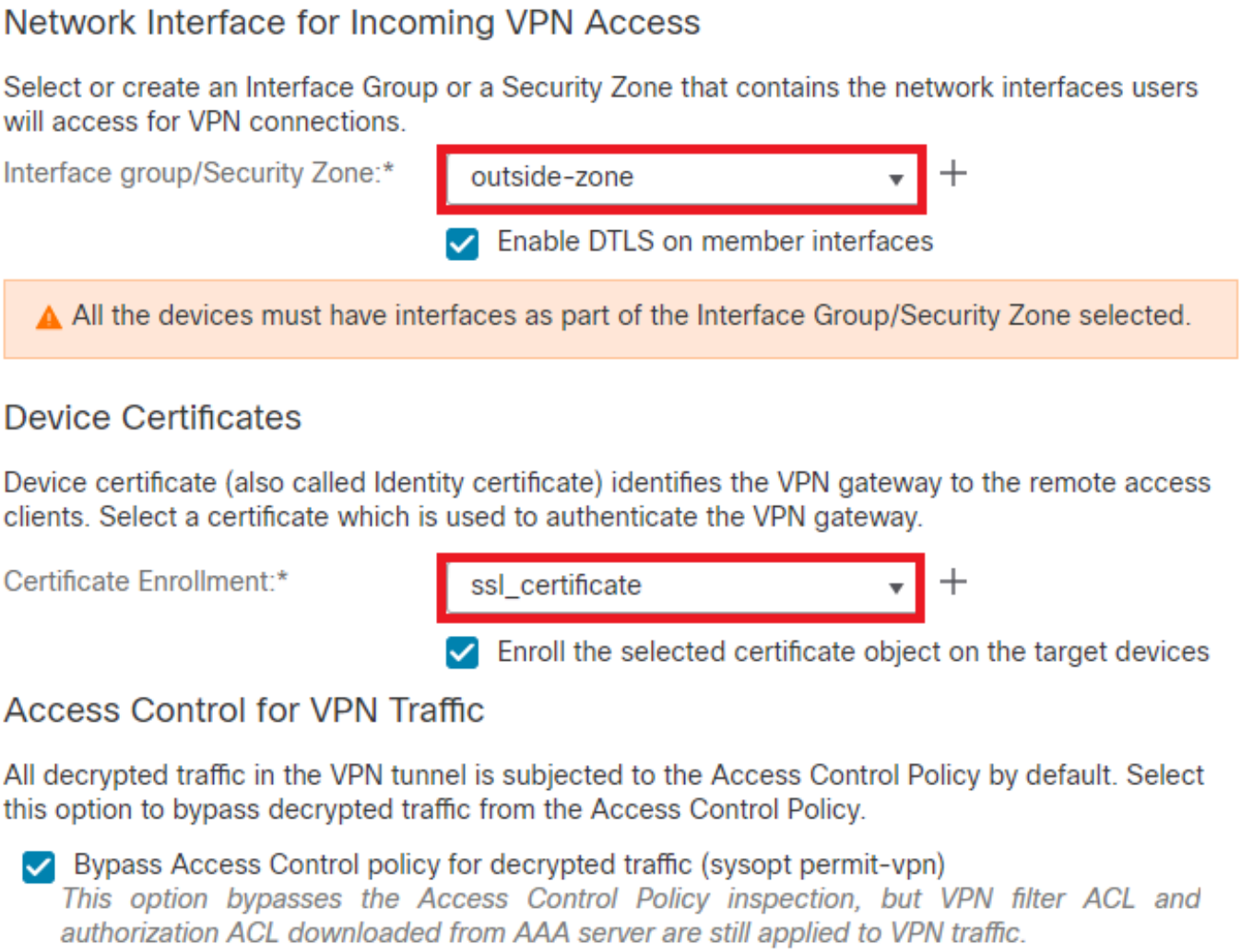


增加安全客戶端配置檔案

步驟 9.點選Next，然後選擇Secure Client Image，然後點選Next。

增加安全客戶端映像

步驟 10.選擇VPN訪問的網路介面，選擇Device Certificates並選中sysopt permit-vpn，然後按一下Next。



為*VPN*流量增加訪問控制

步驟 11.最後，檢視所有配置並按一下Finish。

Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	FTD-B-7.4.0
Connection Profile:	RAVPN-CertAuth
Connection Alias:	RAVPN-CertAuth
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
Secure Client Images:	AnyconnectWin-5.0.05040
Interface Objects:	outside-zone
Device Certificates:	ssl_certificate

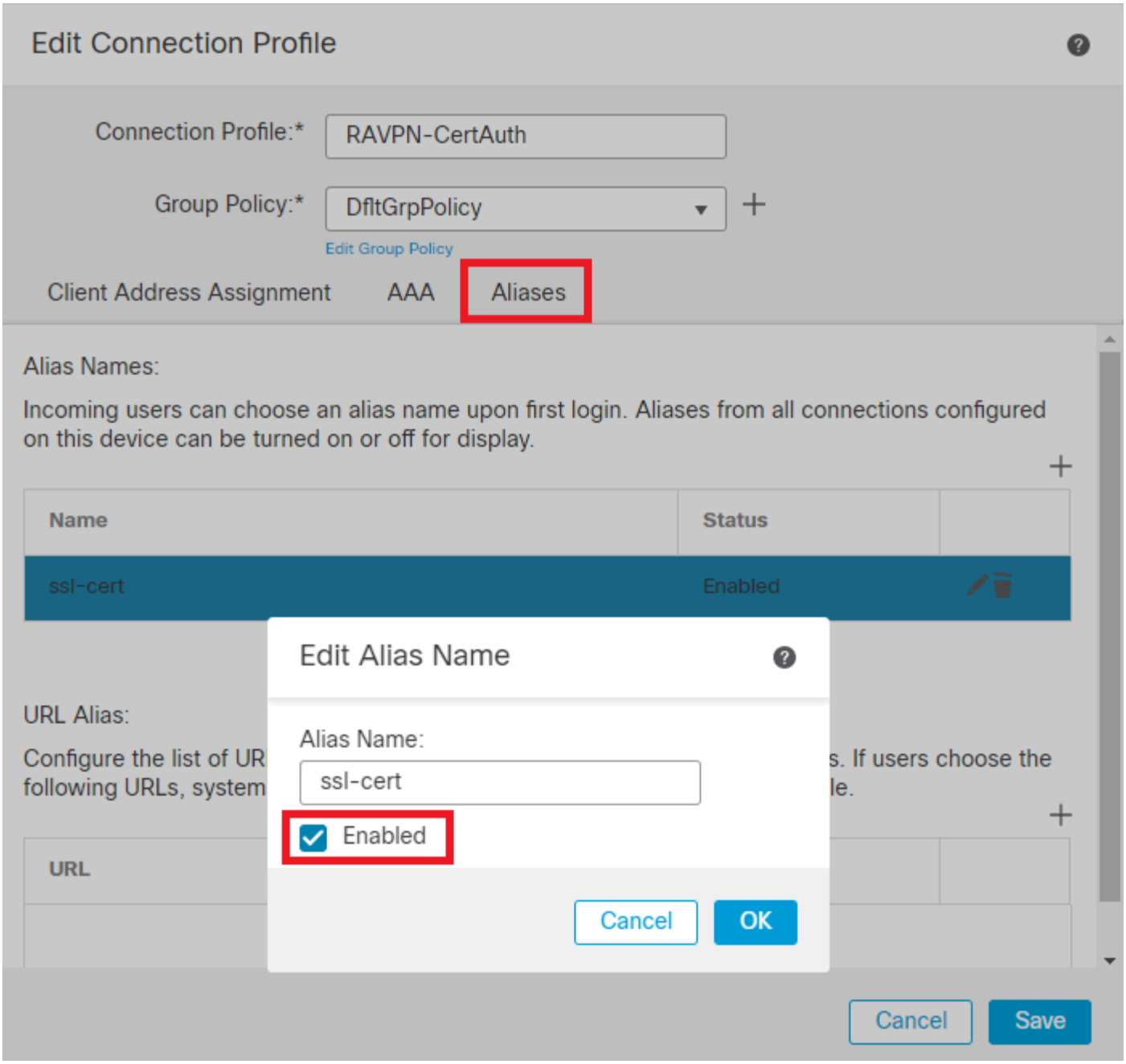
Device Identity Certificate Enrollment

Certificate enrollment object 'ssl_certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the *Certificates* page to check the status of the installation.

遠端訪問*VPN*策略配置

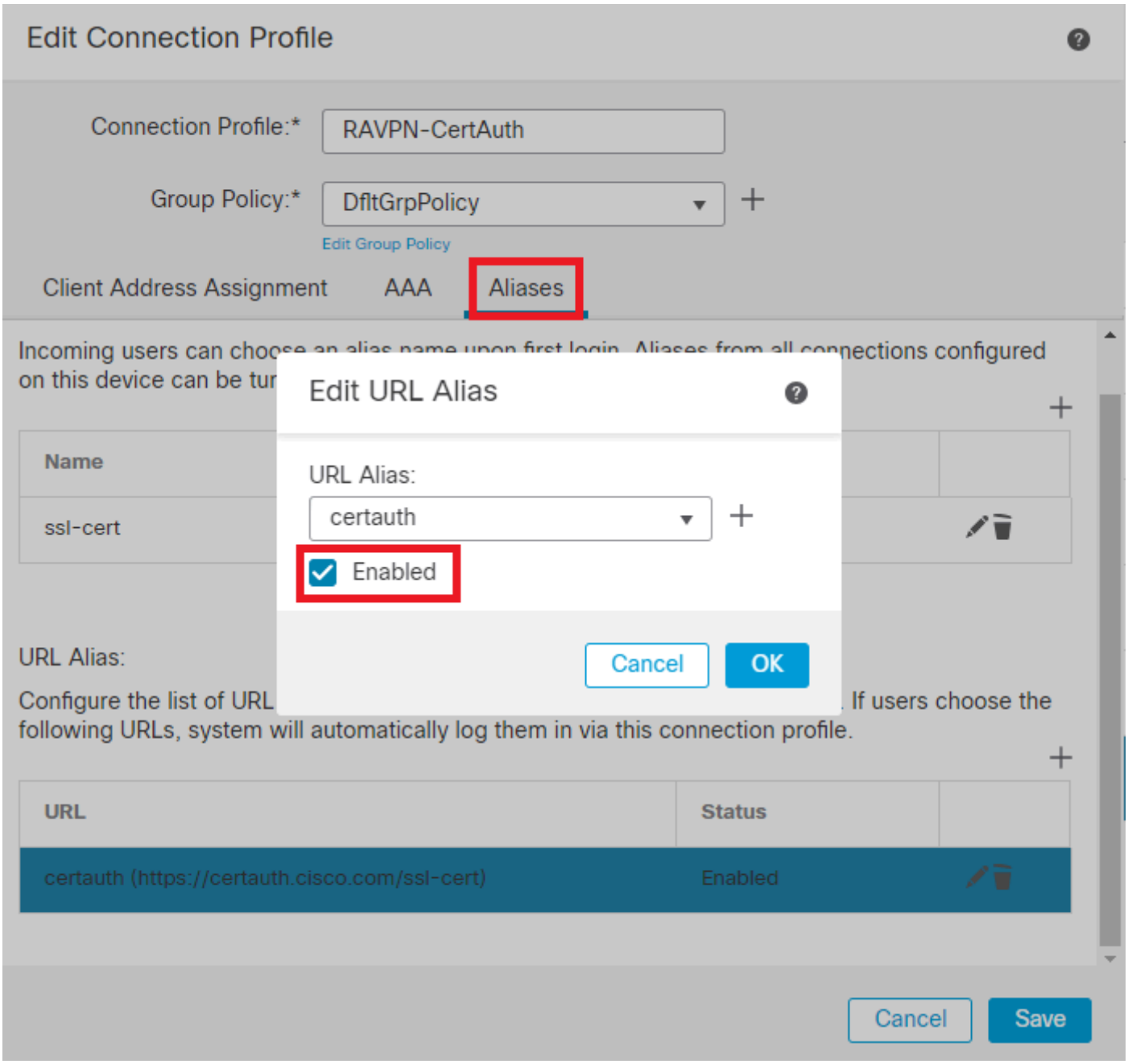
步驟 12.完成遠端訪問VPN的初始設定後，編輯建立的連線配置檔案，並轉到Aliases。

步驟 13.透過點選加號圖示(+)配置group-alias。



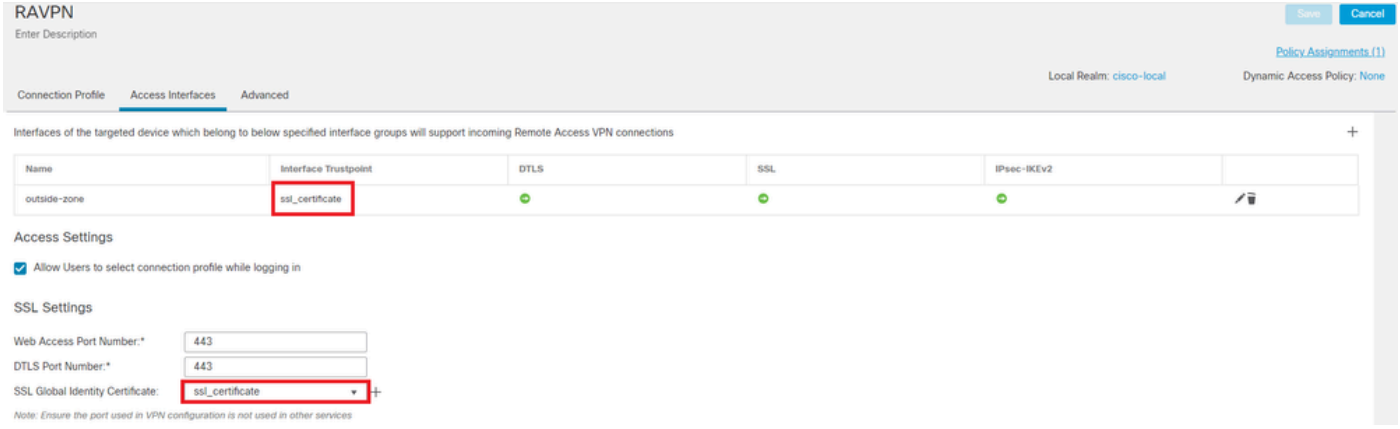
編輯群組別名

步驟 14.透過點選加號圖示(+)配置group-url。使用使用者端設定檔中之前設定的相同群組URL。



編輯群組*URL*

步驟 15.導航至Access Interfaces。在SSL settings下選擇Interface Truspoint和SSL Global Identity Certificate。



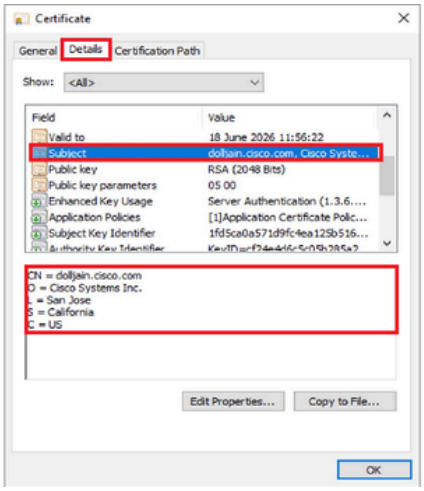
編輯訪問介面

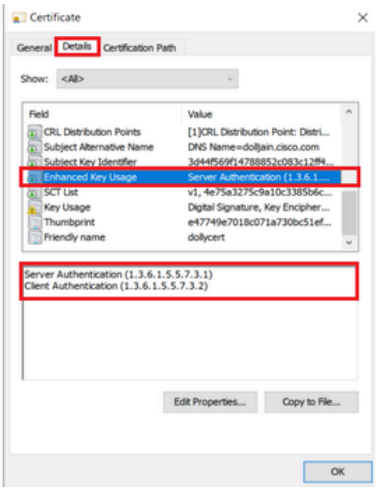
步驟 16.點選Save，部署這些更改。

驗證

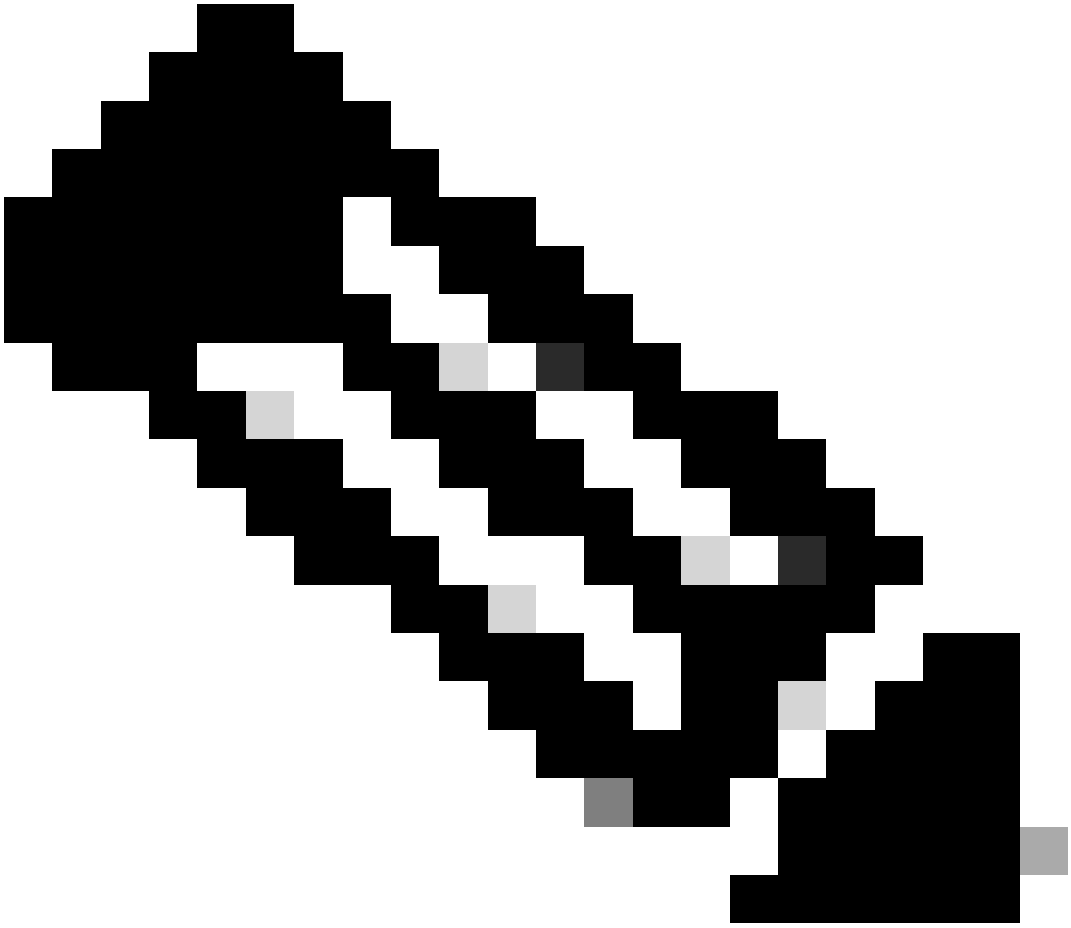
使用本節內容，確認您的組態是否正常運作。

1. 安全客戶端PC必須在使用者PC上安裝具有有效日期、主題和EKU的證書。此憑證必須是由其憑證安裝在FTD上的CA核發，如先前所示。此處，身份或使用者證書由「auth-risaggar-ca」頒發。



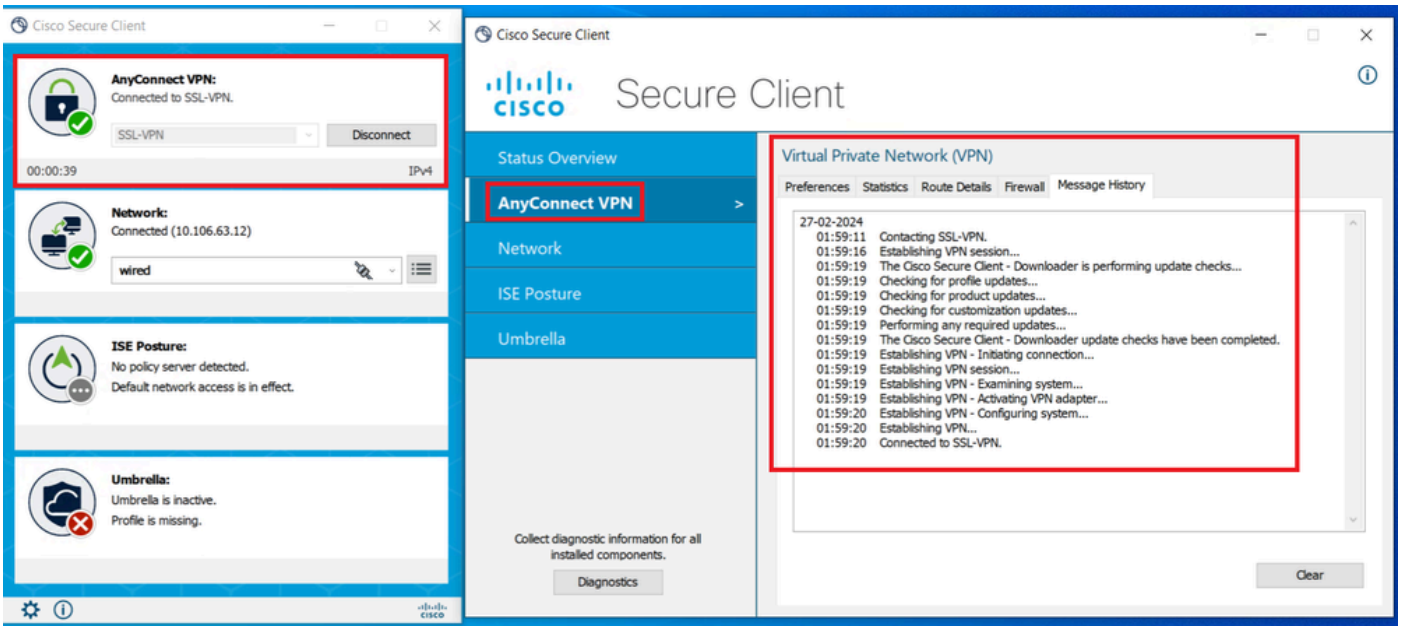


憑證亮點



注意：客戶端證書必須具有「客戶端身份驗證」增強型金鑰使用(EKU)。

2. 安全客戶端必須建立連線。



成功的安全客戶端連線

3. 運行show vpn-sessiondb anyconnect以確認使用隧道組下活動使用者的連線詳細資訊。

```
firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dolljain.cisco.com Index :
```

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FTD的診斷CLI執行偵錯：

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

2. 有關常見問題，請參閱本指南。

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）。