配置證書身份驗證&DUO SAML身份驗證

目錄

簡介

本檔案將介紹實施憑證型驗證和雙重SAML驗證的範例。

必要條件

本指南中使用的工具和裝置包括：

- Cisco Firepower威脅防禦(FTD)
- Firepower Management Center (FMC)
- 內部憑證授權單位(CA)
- Cisco DUO Premier帳戶
- Cisco DUO驗證代理
- 思科安全使用者端(CSC)

需求

思科建議您瞭解以下主題：

- 基本VPN，
- SSL/TLS
- 公開金鑰基礎架構

- 使用FMC的經驗
- 思科安全使用者端
- FTD代碼7.2.0或更高版本
- Cisco DUO驗證代理

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科FTD(7.3.1)
- 思科FMC(7.3.1)
- 思科安全使用者端(5.0.02075)
- Cisco DUO驗證代理(6.0.1)
- Mac OS(13.4.1)
- Active Directory

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。

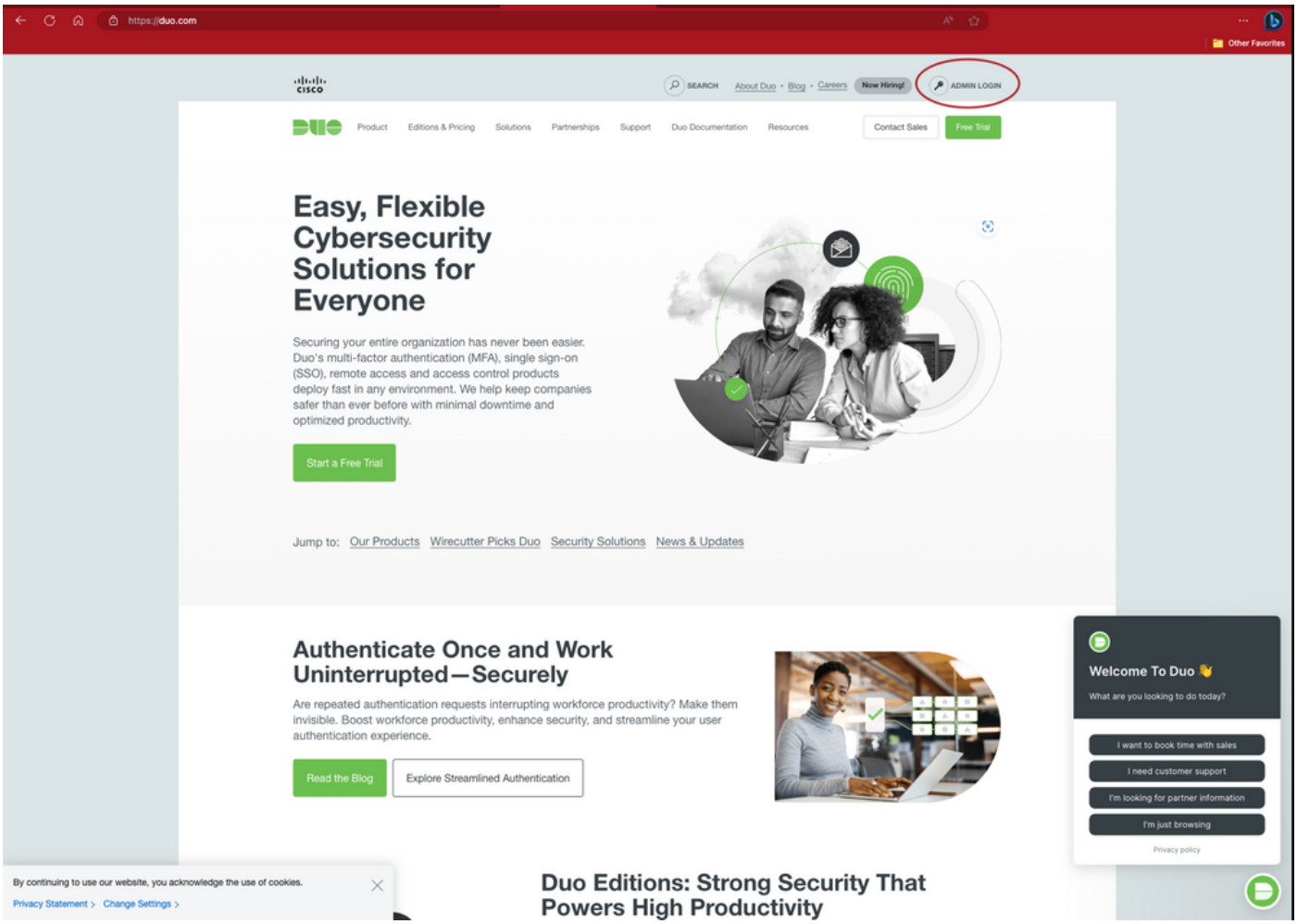
配置DUO上的步驟

本節介紹配置Cisco DUO單一登入(SSO)的步驟。開始之前，請確保已實施身份驗證代理。

警告：如果尚未實施身份驗證代理，此連結包含此任務的指南。DUO Authentication Proxy指南

建立應用程式保護策略

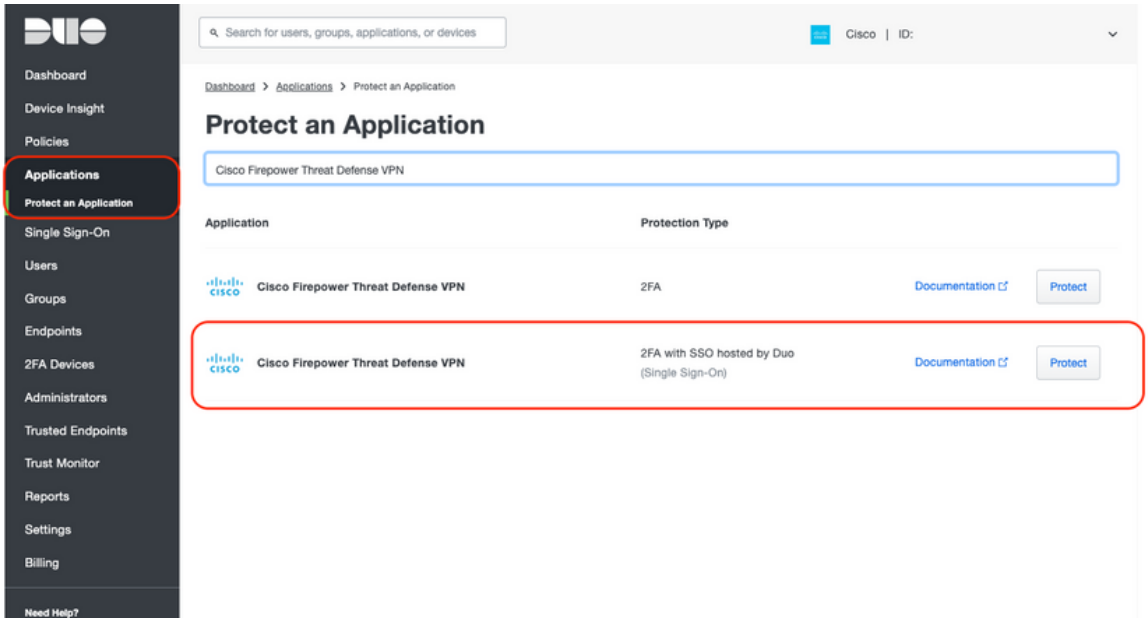
步驟1.通過此連結Cisco Duo登入到管理面板



Cisco DUO首頁

步驟2.導航到控制面板>應用程式>保護應用程式。

在搜尋欄中，輸入「Cisco Firepower Threat Defense VPN」，然後選擇「Protect」。



保護應用程式螢幕截圖

選擇僅具有保護型別「2FA with SSO hosted by Duo」的選項。

步驟 3:在後設資料下複製此URL資訊。

- 標識提供程式實體ID
- SSO URL
- 註銷URL

要複製的資訊示例

附註：螢幕截圖中已省略了連結。

步驟4.選擇「Download certificate」下載「Downloads」下的Identity Provider Certificate。

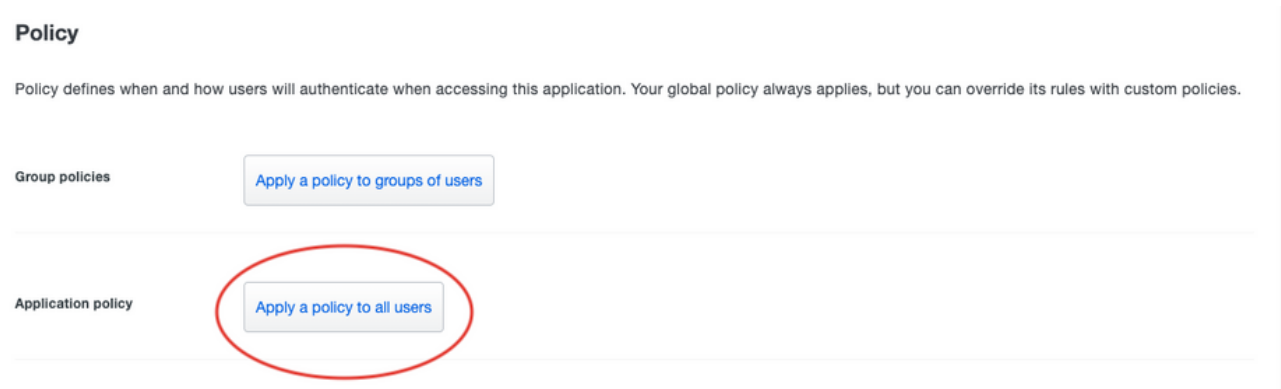
步驟5.填寫服務提供商資訊

Cisco Firepower基礎URL — 用於訪問FTD的FQDN

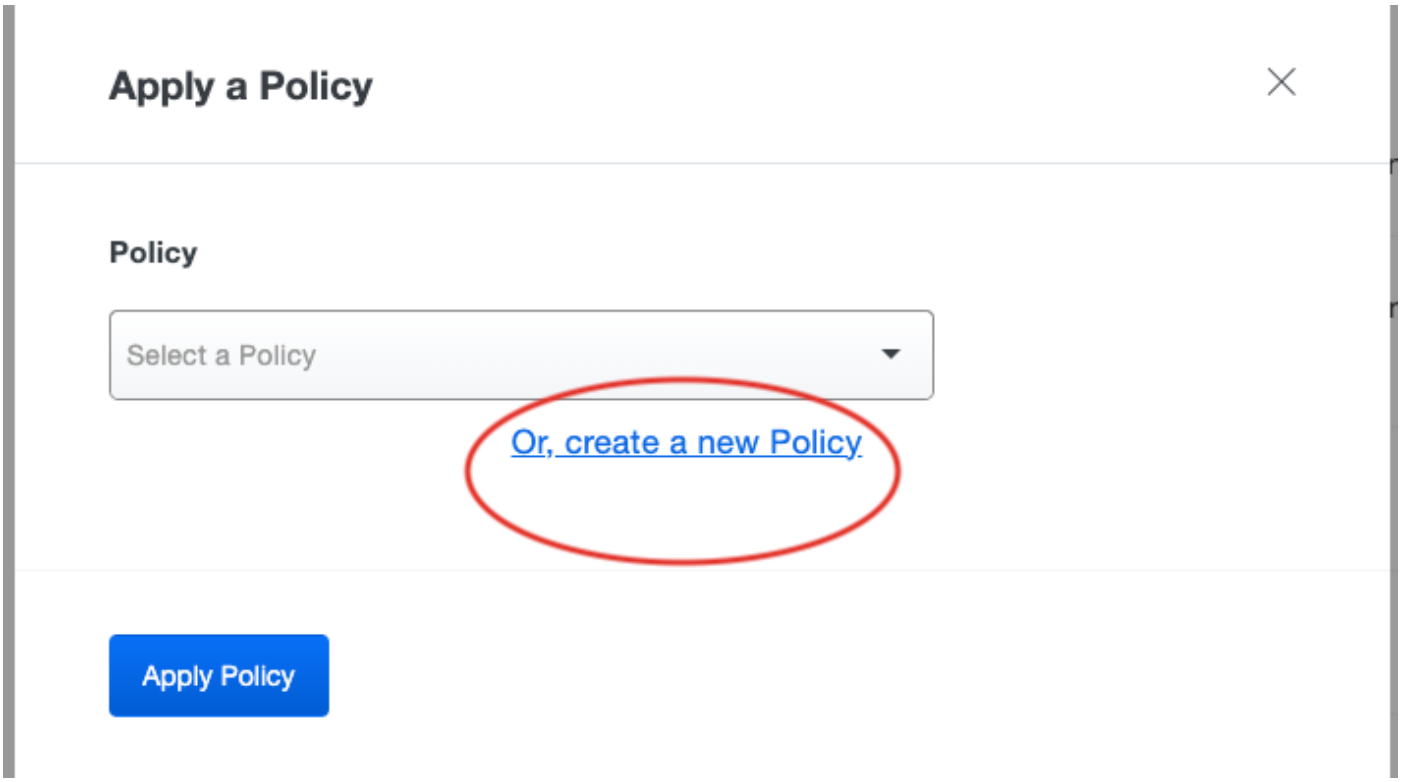
連線配置檔案名稱 — 隧道組名稱

建立應用程式策略

步驟 1:要在Policy 下建立Application Policy選擇「Apply a policy to all users」，然後選擇「Or，create a new Policy」，如下圖所示。

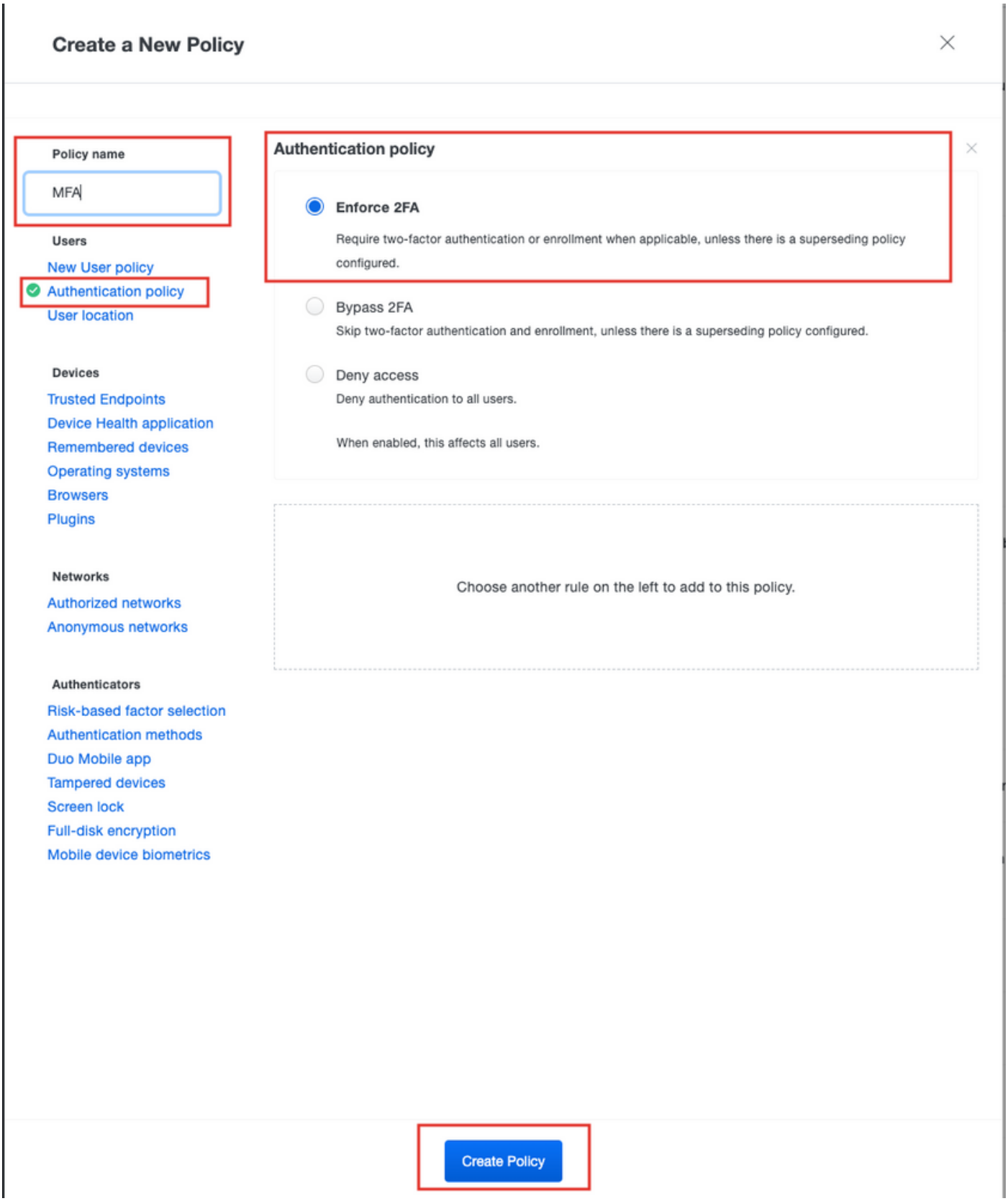


建立應用程式策略的示例



建立應用程式策略的示例

步驟2.在Policy name下，輸入所需的名稱，在Users下選擇「Authentication policy」，然後選擇「」實施2FA。」 然後使用「建立策略」進行儲存。



建立應用程式策略的示例

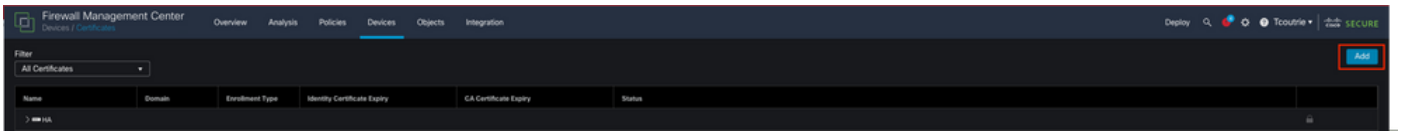
步驟3.在下一個視窗中使用「Apply Policy」應用策略。然後滾動到頁面底部並選擇「Save」以完成DUO配置

FMC的配置步驟

將身分憑證部署到FTD

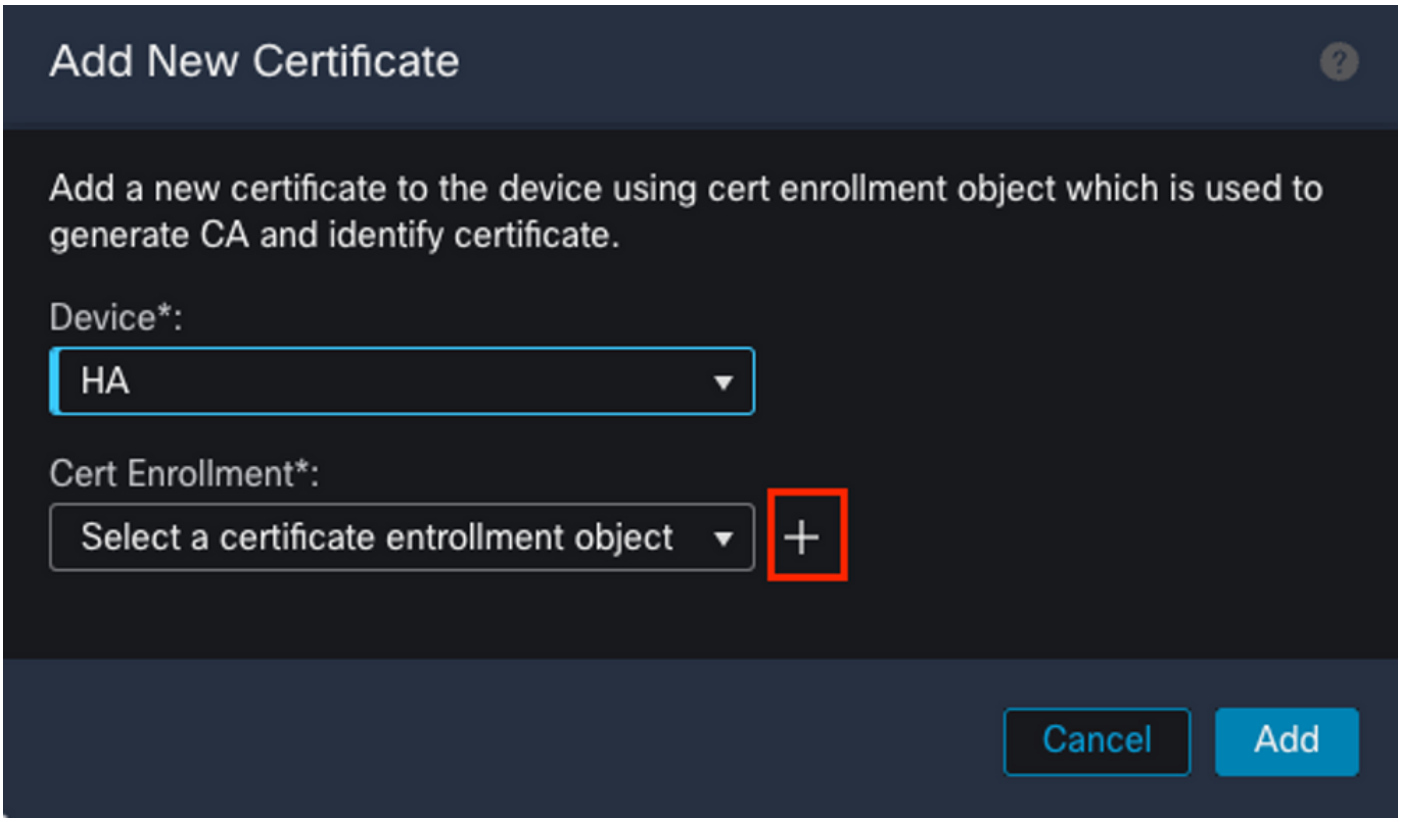
本節介紹如何配置身份證書並將其部署到FTD（證書身份驗證所需的）。開始之前，請確保部署所有配置。

步驟1。導覽至Devices > Certificates，然後選擇Add，如下圖所示。



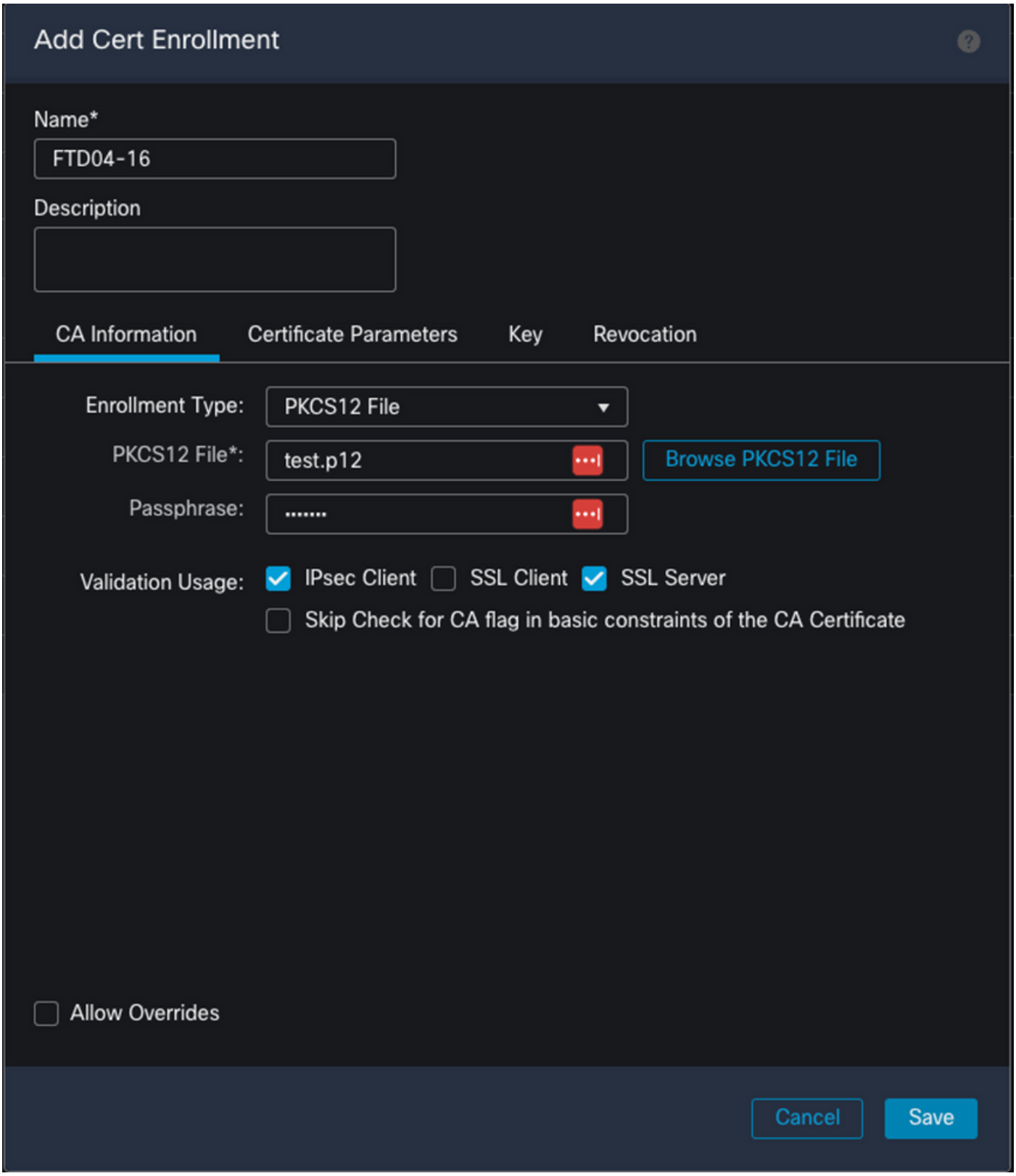
裝置/證書的截圖

步驟 2:從devices下拉選單中選擇FTD裝置。按一下+圖示可新增新的證書註冊方法。



新增新證書的螢幕快照

步驟3:選擇通過「Enrollment Type」在環境中獲取證書的首選方法的選項，如下圖所示。



新證書註冊頁面的螢幕截圖

提示：可用選項包括：Self Signed Certificate — 在本地生成新證書， SCEP — 使用簡單證書註冊協定從CA獲取證書， Manual — 手動安裝根和身份證書， PKCS12 — 上傳包含根、標識和私鑰的加密證書捆綁包。

將IDP憑證部署到FTD

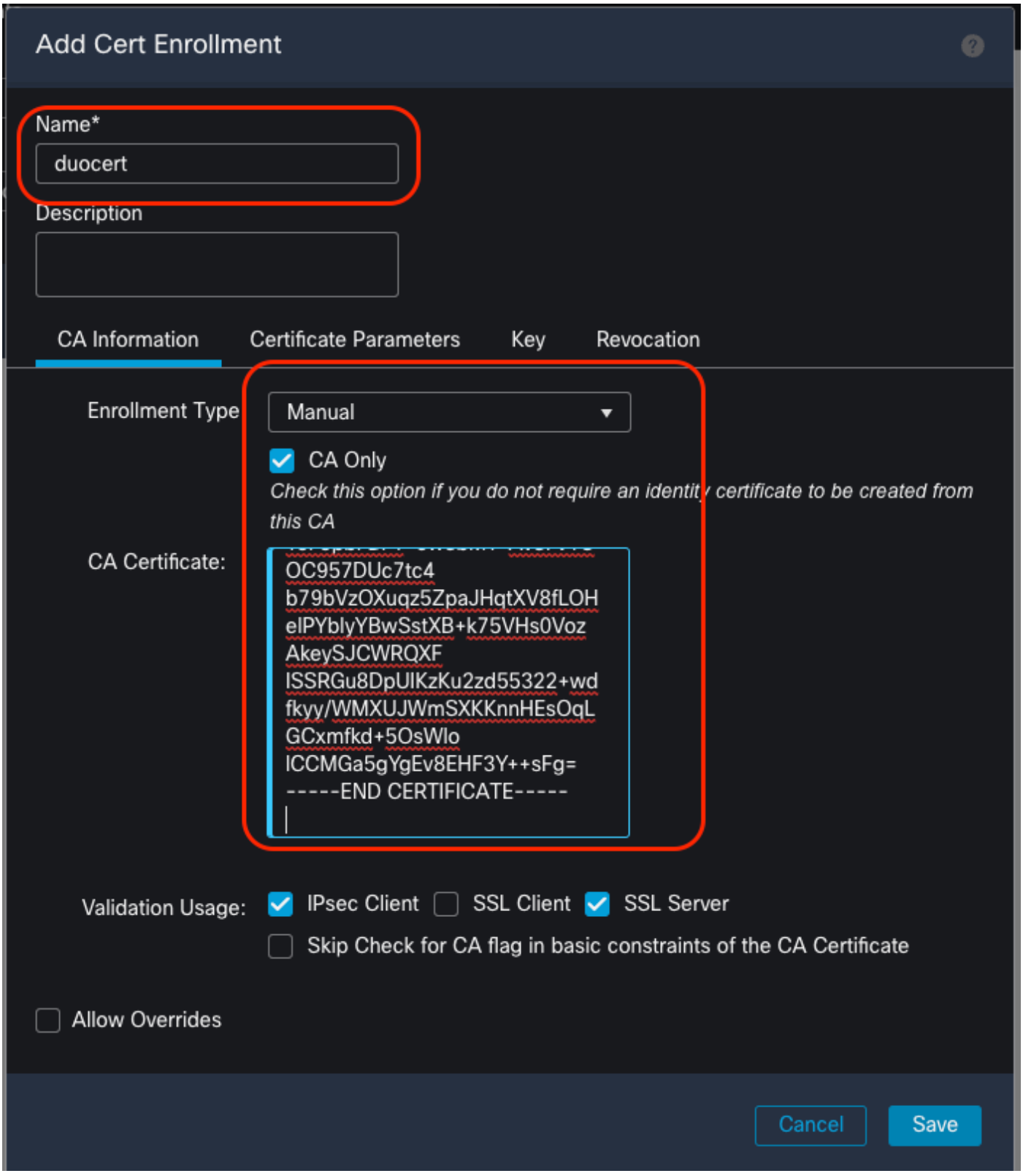
本節介紹如何配置並將IDP證書部署到FTD。開始之前，請務必部署所有配置。

步驟 1:導覽至Devices > Certificate，然後選擇Add。」

步驟 2:從devices下拉選單中選擇FTD裝置。按一下+圖示可新增新的證書註冊方法。

第3步：在「新增證書註冊」視窗中，輸入所需的資訊（如圖所示），然後「保存」（如圖所示）。

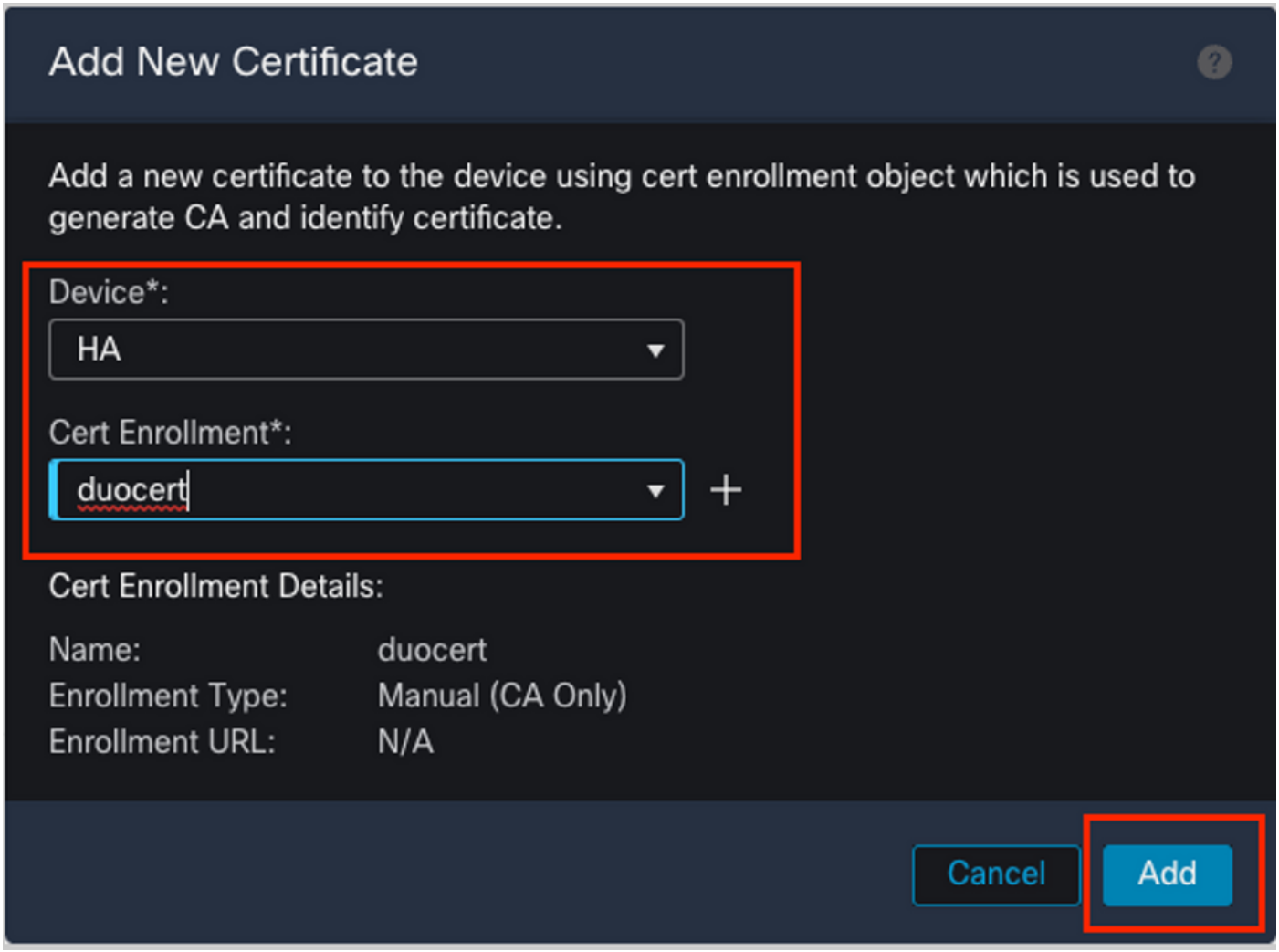
- 名稱:對象的名稱
- 註冊型別:手動
- 竅取方塊已啟用:僅限CA
- CA證書:憑證的PEM格式



建立證書註冊對象的示例

⚠ 注意：如果需要，可以使用「CA憑證基本約束中的CA標誌跳過」。請謹慎使用該選項。

步驟 4:在「Cert Enrollment*：」下選擇新建立的證書註冊對象，然後選擇「Add」，如下圖所示。



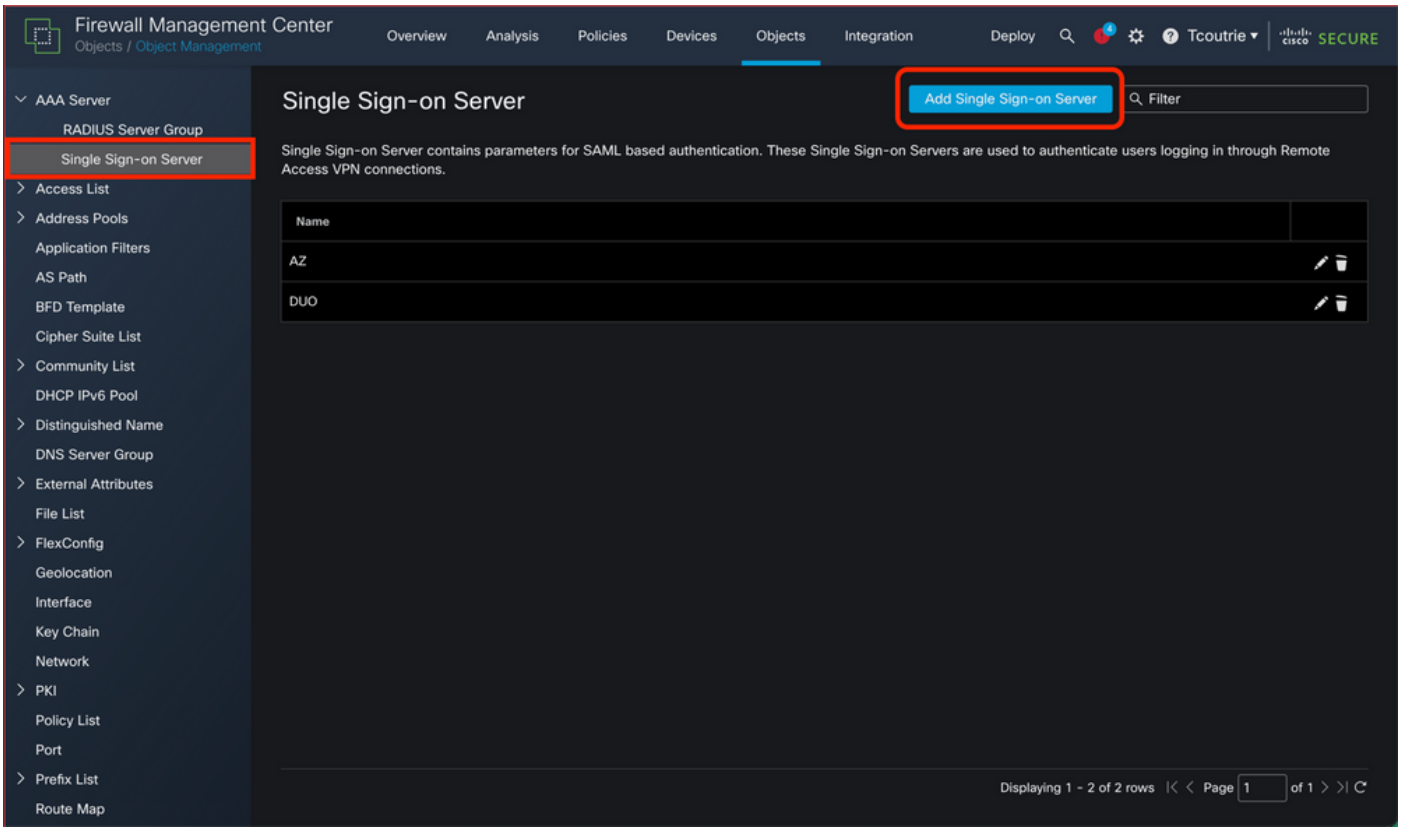
新增的證書註冊對象和裝置的螢幕截圖

附註：新增證書後，立即部署。

建立SAML SSO對象

本節介紹通過FMC配置SAML SSO的步驟。開始之前，請確保部署所有配置。

步驟1.導航到Objects > AAA Server > Single Sign-on Server，然後選擇「Add Single Sign-on Server」。

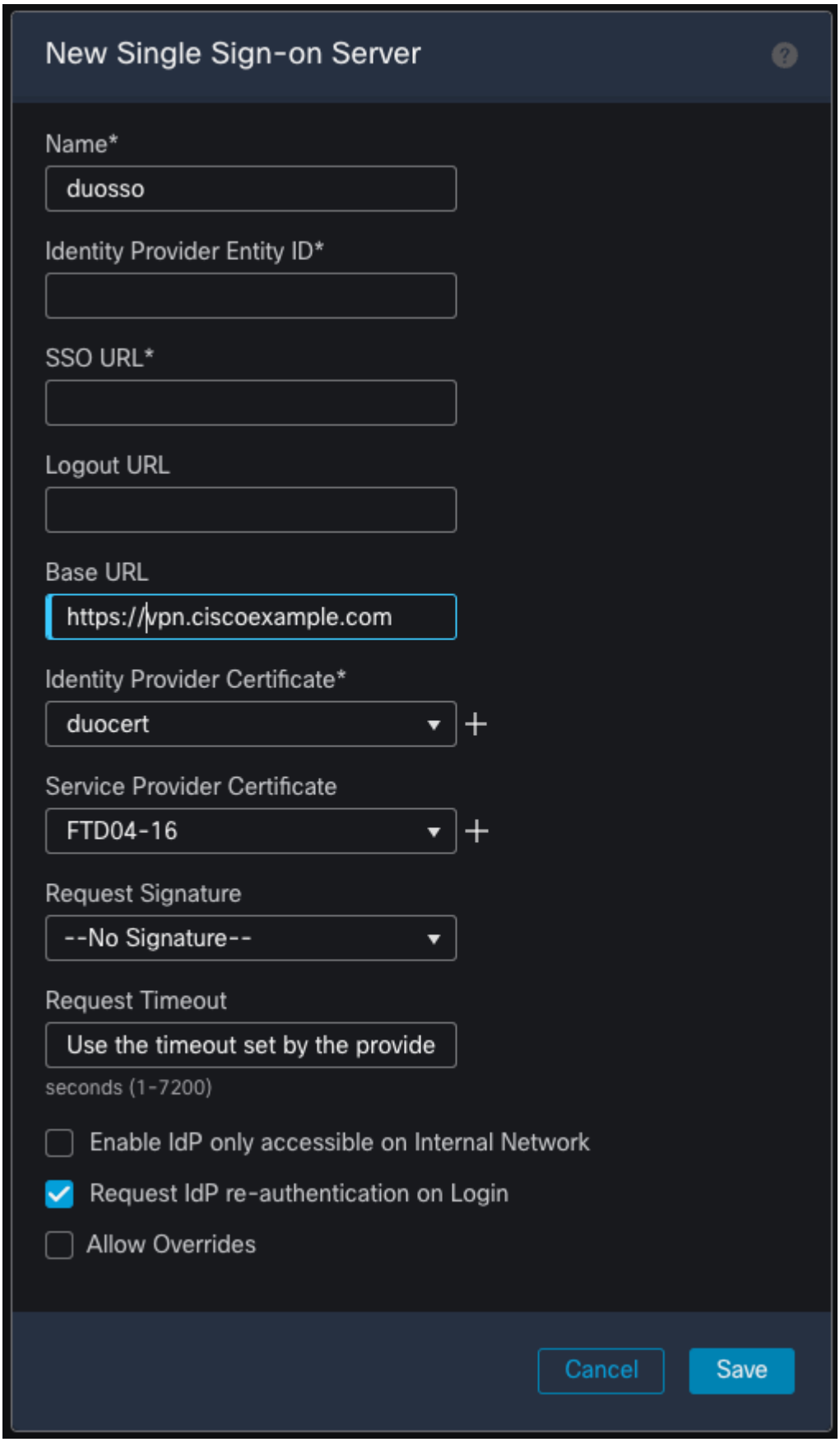


建立新SSO對象的示例

步驟2.從「建立應用程式保護策略」輸入所需的信息

"。 要在完成之後繼續，請選擇「儲存」。

- 名稱*:對象的名稱
- 身份提供程式實體ID*:第3步中的實體ID
- SSO URL*:從步驟3複製的登入URL
- 註銷URL:從步驟3複製的註銷URL
- 基本URL:使用與步驟5中的「Cisco Firepower Base URL」相同的FQDN
- 身份提供程式證書*:已部署的IDP證書
- 服務提供商證書:FTD外部介面上的憑證



新SSO對象的示例。

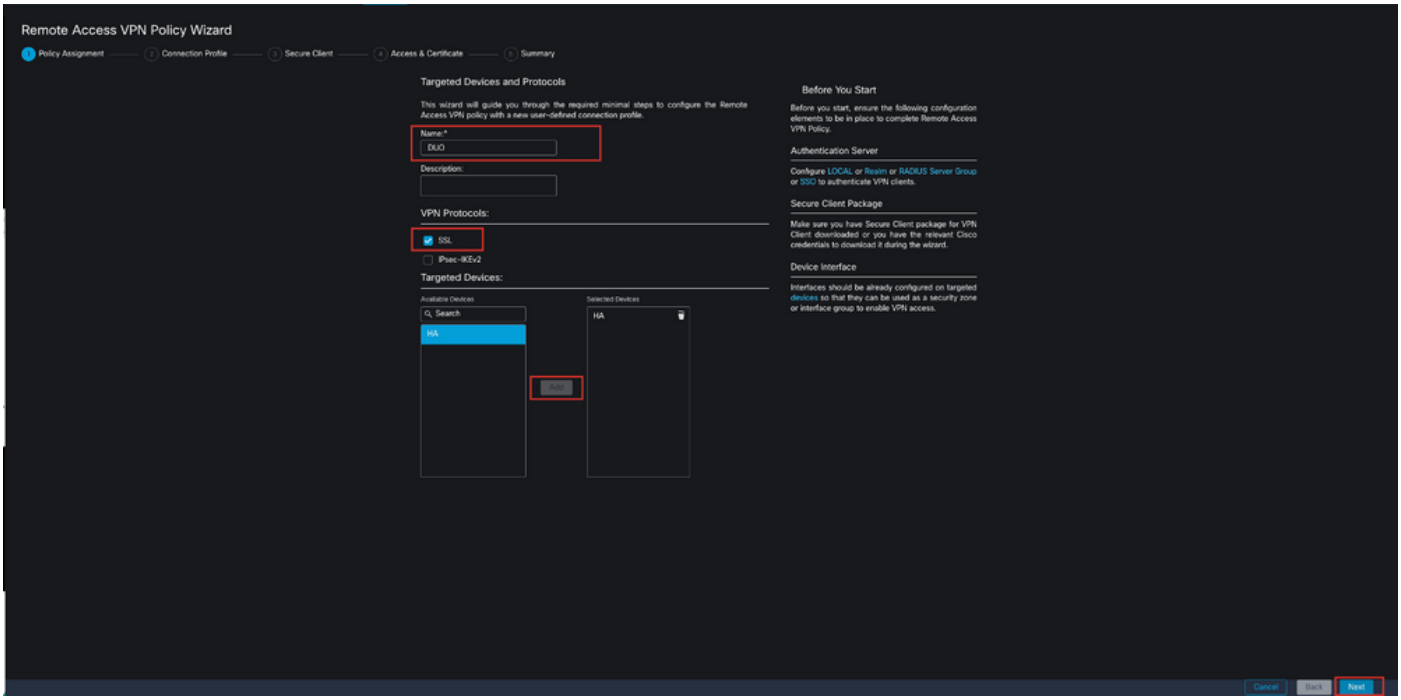
附註：螢幕截圖中省略了實體ID、SSO URL和註銷URL連結

建立遠端訪問虛擬專用網路(RAVPN)配置

本節介紹使用嚮導配置RAVPN的步驟。

步驟1.導覽至Devices > Remote Access Select "Add."

步驟2.在該嚮導中，輸入新的RAVPN策略嚮導的名稱，在VPN協定：新增目標裝置下選擇SSL，如下圖所示。完成後，選擇「下一步」。



RAVPN嚮導的第1步

步驟2.對於連線配置檔案，請設定選項（如下所示）：完成後選擇「下一步」。

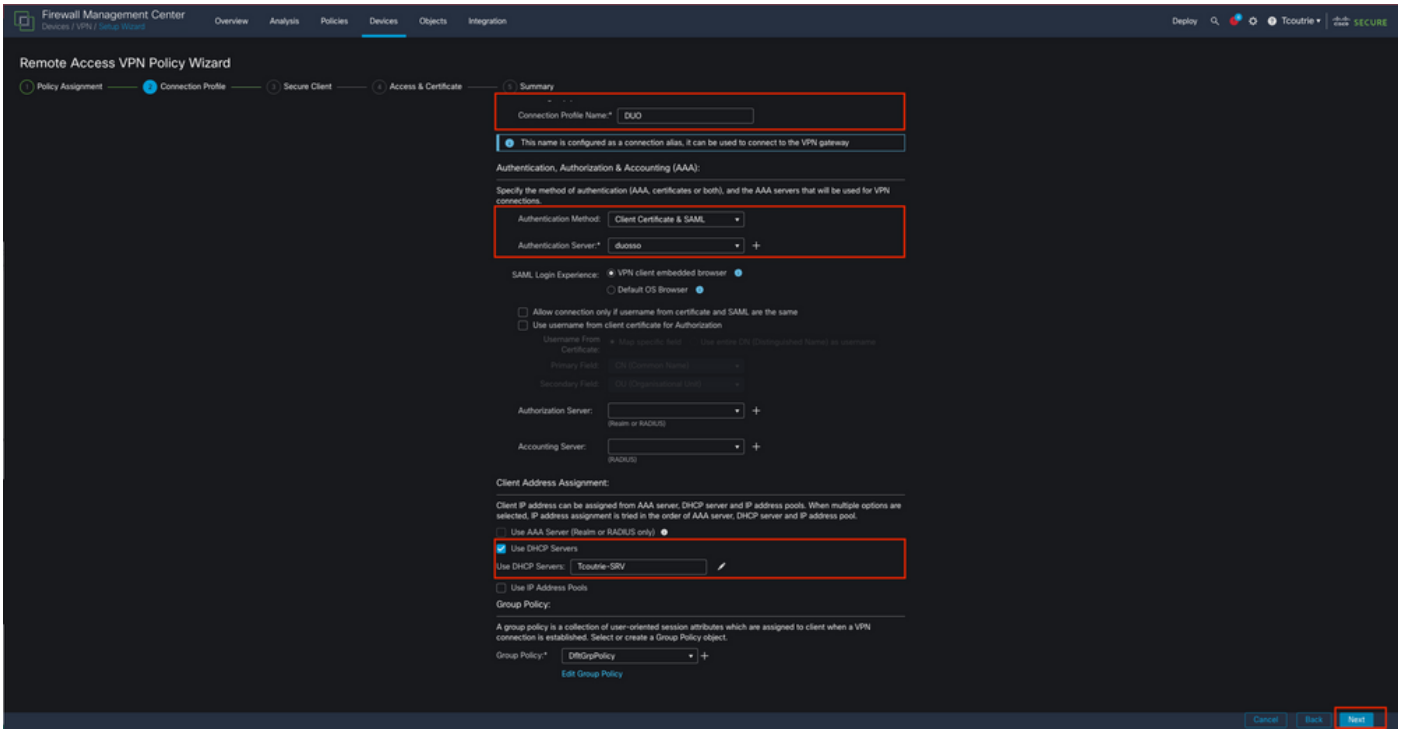
- 連線配置檔名稱： 在建立應用保護策略的步驟5中使用隧道組名稱。

驗證、授權及記帳(AAA):

- 身份驗證方法： 客戶端證書和SAML
- 身份驗證伺服器:*選擇在「建立SAML SSO對象」期間建立的SSO對象。

客戶端地址分配：

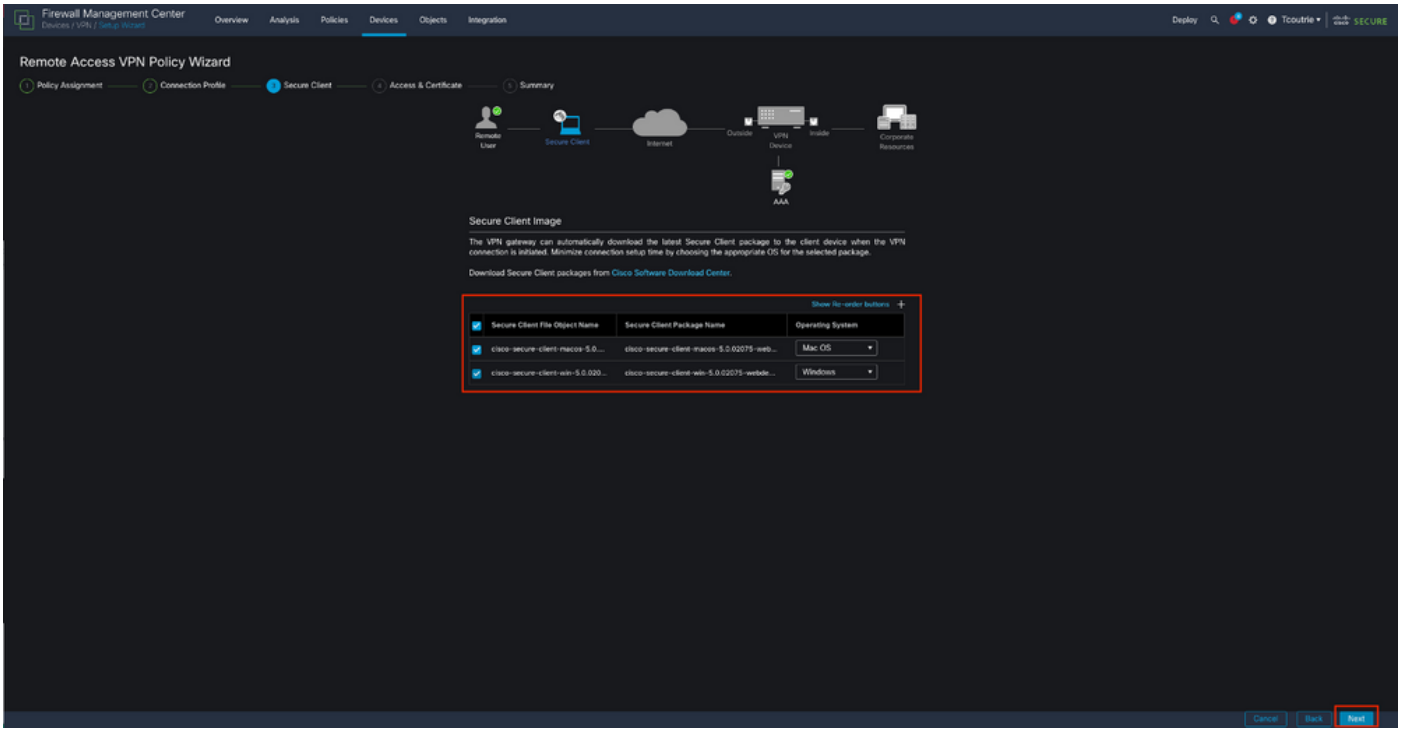
- 使用AAA伺服器(僅限領域或RADIUS)- Radius或LDAP
- 使用DHCP服務器 — DHCP伺服器
- 使用IP位址池- FTD上的本機池



RAVPN嚮導的第2步

提示：本實驗使用DHCP伺服器。

步驟3.選擇「+」以上傳要部署的Cisco安全客戶端的Web部署映像。然後，選中要部署的CSC映像的覈取方塊。如下圖所示。完成後選擇「Next」。

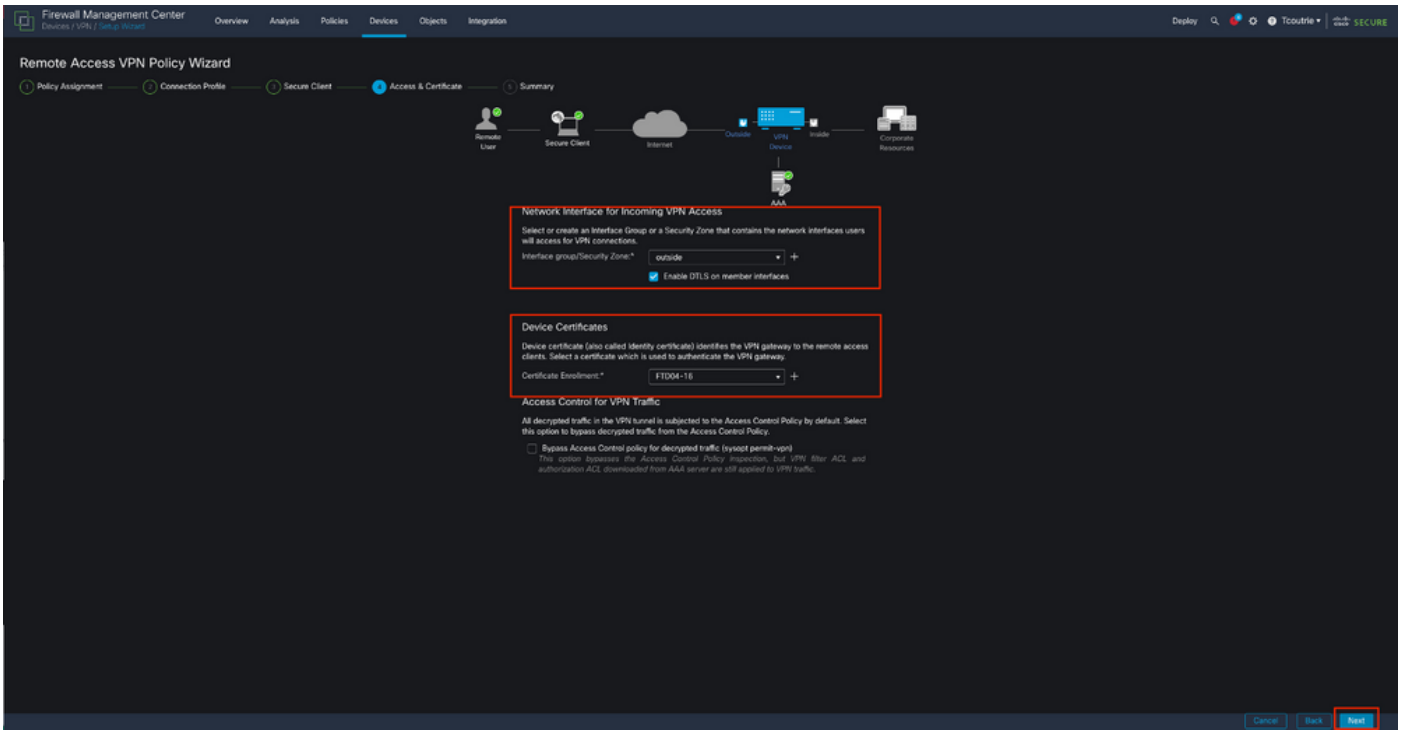


步驟3:RAVPN嚮導

步驟4.設定這些對象（如圖所示）：完成之後選擇「下一步」。

介面組/安全區域：*:外部介面

"Certificate Enrollment:*":在本指南的「將身份證書部署到FTD」部分期間建立的身份證書

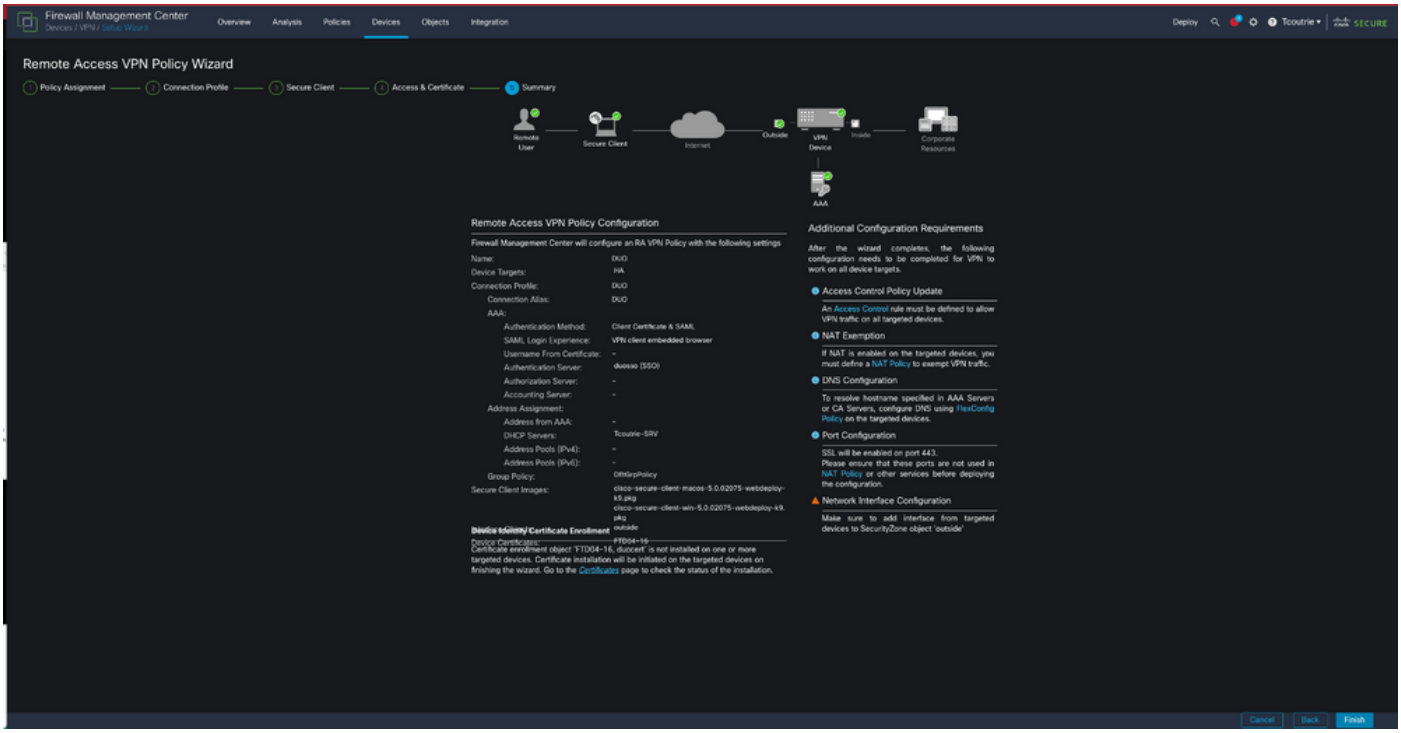


RAVPN嚮導的第4步

提示：如果尚未建立此對象，則通過選擇「+」新增新的證書註冊對象。

步驟6.摘要

驗證所有資訊。如果一切正常，則繼續執行「完成」。



摘要頁面

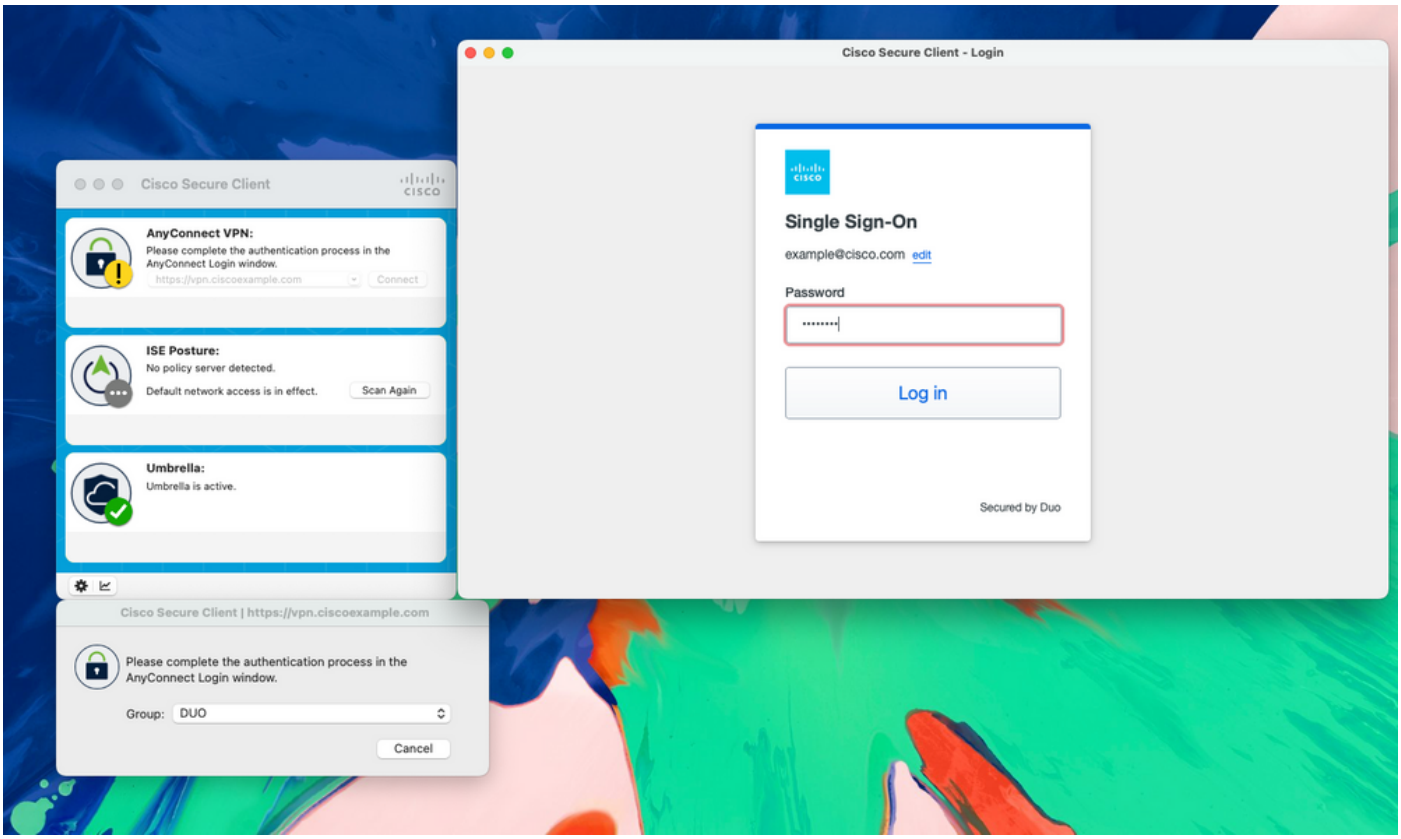
步驟7.部署新增的配置。

驗證

本節介紹如何驗證連線嘗試是否成功。

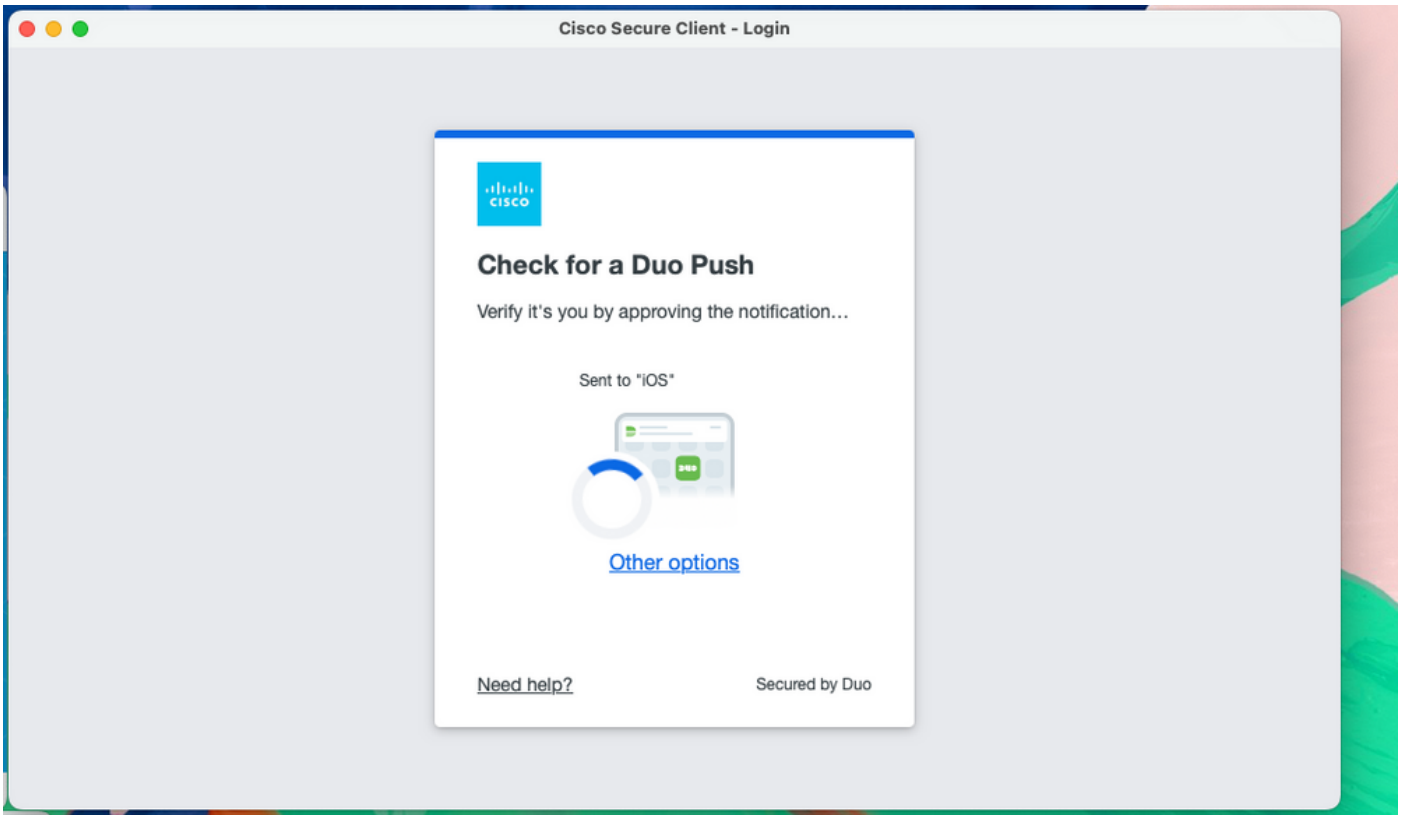
開啟Cisco Secure Client並輸入FTD的FQDN並進行連線。

在SSO頁上輸入憑據。



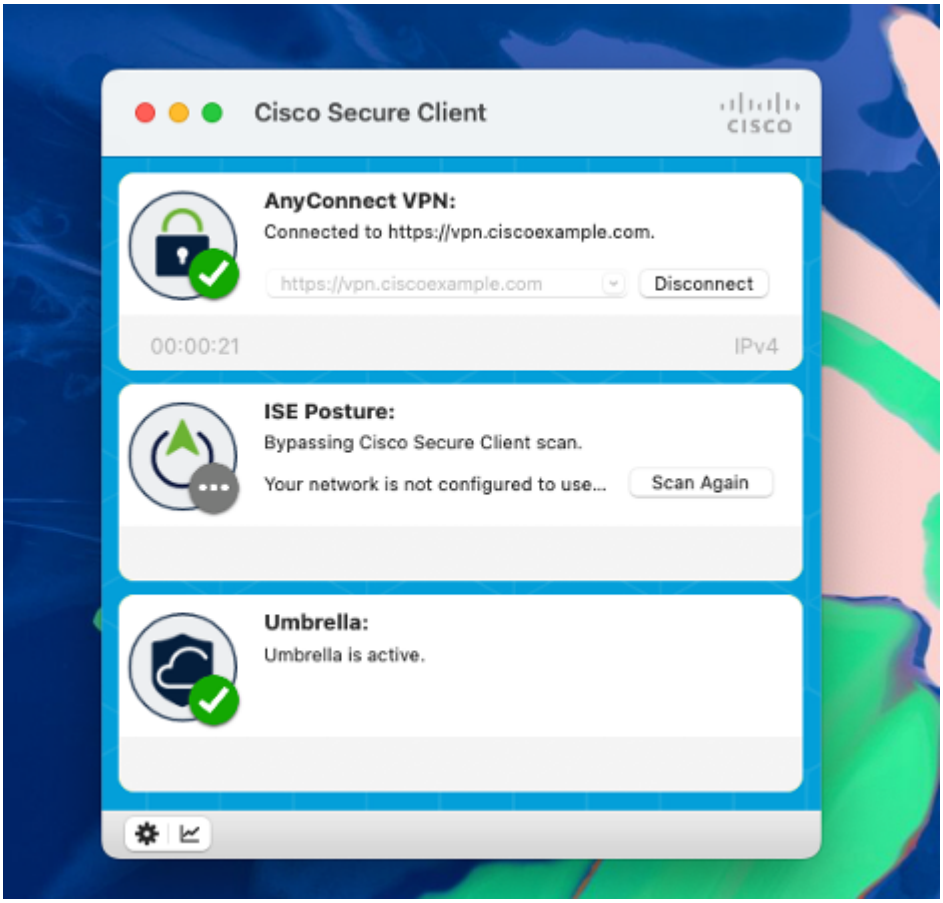
通過Cisco Secure Client的SSO頁面

接受DUO推入註冊裝置。



DUO推送

連線成功。



已連線到FTD

使用以下命令驗證FTD上的連線：show vpn-sessiondb detail anyconnect

```
tcoutrie-ftd2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     :                        Index        : 1916
Assigned IP  :                        Public IP    :
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel:
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SH
Bytes Tx     : 390964                 Bytes Rx     : 124114
Pkts Tx      : 1216                   Pkts Rx      : 1223
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy :                        Tunnel Group :
Login Time   : 23:54:41 UTC Tue Jul 18 2023
Duration     : 0h:11m:28s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a7aa95d0077c00064b72641
Security Grp : none                   Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 1916.1
  Public IP    :
  Encryption   : none                   Hashing      : none
  TCP Src Port : 53859                  TCP Dst Port : 443
  Auth Mode    : Certificate and SAML
  Idle Time Out: 30 Minutes             Idle TO Left : 18 Minutes
  Client OS    : mac-intel
```

輸出示例中省略了某些資訊

疑難排解

這些是在實施後可能出現的問題。

問題1:證書身份驗證失敗。

確保在FTD上安裝根憑證；

使用以下調試：

debug crypto ca 14

debug aaa shim 128

debug aaa common 128

問題2:SAML故障

可以啟用這些調試進行故障排除：

debug aaa shim 128

debug aaa common 128

debug webvpn anyconnect 128

debug webvpn saml 255

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）。