在由FMC管理的安全防火牆威脅防禦上使用ACME協定配置證書註冊

簡介

本檔案介紹在安全防火牆Firepower威脅防禦(FTD)平台上透過自動憑證管理環境(ACME)通訊協定註冊傳輸層安全(TLS)憑證的程式。

必要條件

需求

思科建議您瞭解以下主題：

- 手動證書註冊過程和安全套接字層(SSL)的基礎。
- 適用於遠端存取VPN的基本驗證概念。
- 具有證書頒發機構(CA)的經驗。

採用元件

- Cisco FTDv版本10.0.0-35。
- Cisco FMC版本10.0.0-35。
- 支援ACME協定的證書頒發機構(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。

要求和限制

安全防火牆FTD上ACME註冊的當前先決條件和限制包括：

- FTD和FMC 10.0.0版及更新版本支援。
- ACME不允許發放萬用字元憑證；每個證書請求必須指定一個精確的域名。

- 通過ACME註冊的每個信任點都限制在單個介面上，因此通過ACME獲得的證書無法在多個介面上共用。
- 金鑰對是自動生成的，對通過ACME註冊的每個證書都是唯一的，可防止金鑰重複使用，並可增強安全性。

降級注意事項

當降級到不支援ACME註冊（版本7.7或更低版本）的安全防火牆FTD版本時：

- 10.0.0版或更高版本中引入的所有與ACME相關的信任點配置都將丟失。
- 仍然可以訪問通過ACME註冊的證書；但是，在第一次儲存並在降級後重新啟動後，它們的私鑰將解除關聯。

如果需要降級，請使用建議的解決方法：

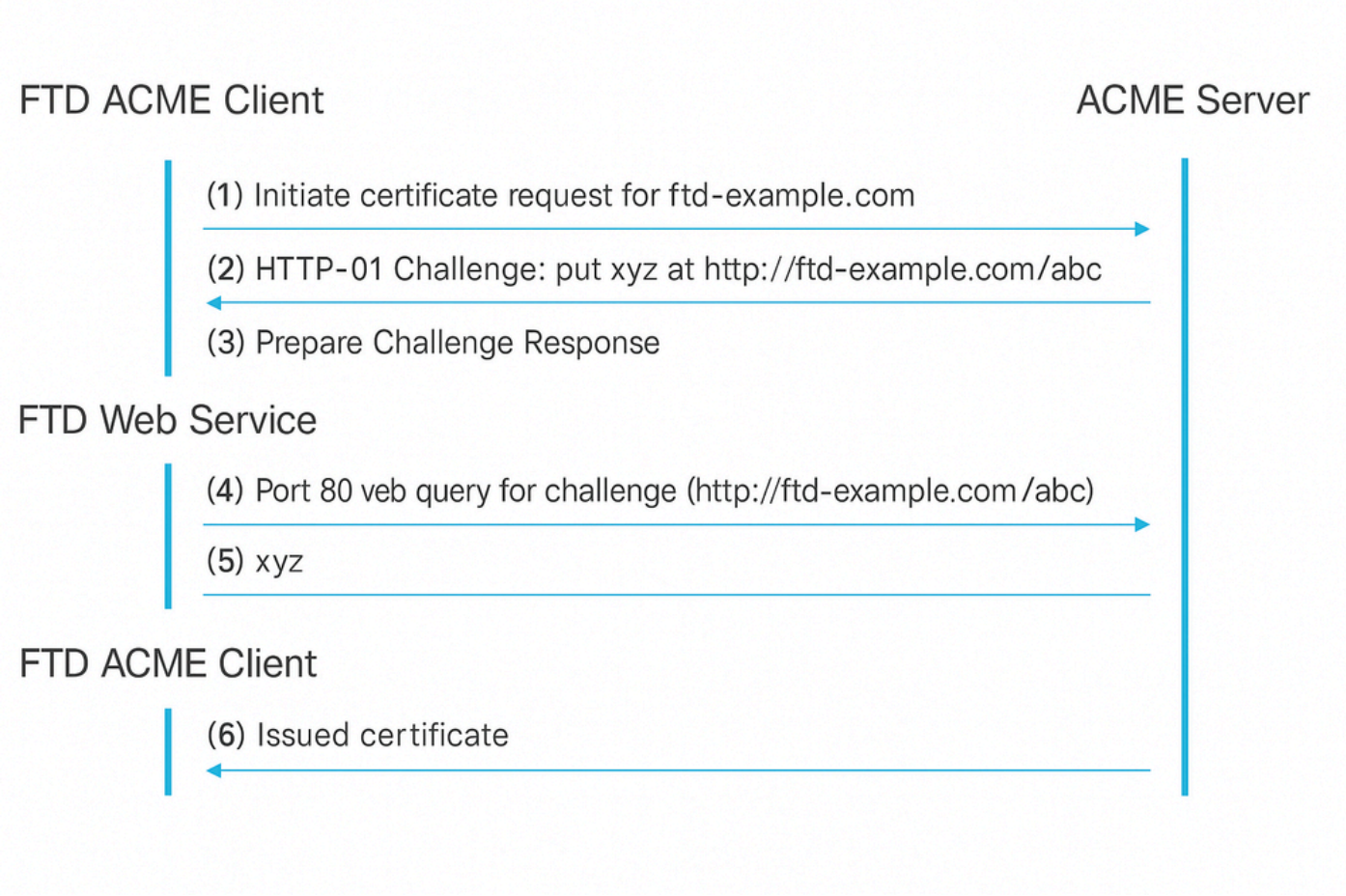
- 降級之前，以PKCS12格式匯出ACME證書。
- 降級之前，刪除ACME信任點配置。
- 降級後，匯入PKCS12證書。匯入的信任點將一直有效，直到ACME頒發的證書過期。

背景資訊

ACME協定旨在簡化網路管理員的TLS證書管理。通過ACME，管理員可以自動執行獲取和更新TLS證書所涉及的任務。在與證書頒發機構(CA)（如Let's Encrypt）一起使用時，此自動化特別有用，後者通過ACME協定提供免費的、自動的、可公開訪問的證書。ACME促進了域驗證(DV)證書的頒發。這些證書驗證證書請求者是否對指定的域擁有控制權。驗證通常通過基於HTTP的質詢過程進行，申請人將指定檔案放在其Web伺服器上。然後，證書頒發機構(CA)通過域的HTTP伺服器訪問此檔案，以確認域控制。成功通過此質詢使CA能夠頒發DV證書。

註冊過程包括以下步驟：

1. Initiate Certificate Request:客戶端向ACME伺服器提交證書請求，指定需要該證書的域。
2. 接收HTTP-01質詢：ACME伺服器使用HTTP-01質詢進行響應，該質詢包含客戶端必須用來證明域所有權的唯一令牌。
3. 準備質詢響應:
    1. 客戶端通過將來自ACME伺服器的令牌與其帳戶金鑰組合來生成金鑰授權。
    2. 客戶端將其Web伺服器配置為在特定URL路徑上提供此金鑰授權。
4. ACME伺服器檢索質詢：ACME伺服器對提供的URL執行HTTP GET請求以獲取金鑰授權。
5. ACME伺服器驗證所有權：伺服器將檢索到的金鑰授權與預期值進行比較，以驗證客戶端對域的控制。
6. 頒發證書：成功驗證後，ACME伺服器會向客戶端頒發SSL/TLS證書。



ACME註冊HTTP-01身份驗證流程。

使用ACME協定在安全防火牆FTD上註冊TLS證書的主要優勢包括：

- 憑證管理自動化:ACME簡化了獲取和維護安全防火牆FTD TLS介面的TLS域證書的過程，從而顯著減少了手動管理任務。
- 自動證書續訂:藉助支援ACME的信任點，證書在即將到期時自動更新，從而最大程度地減少持續管理干預的需要。
- 持續安全保證:此自動化可確保證書保持有效而不中斷，從而防止意外證書過期並保持安全通訊。

這些優勢共同提高了安全防火牆FTD部署的運行效率和安全性。

設定

必要條件配置

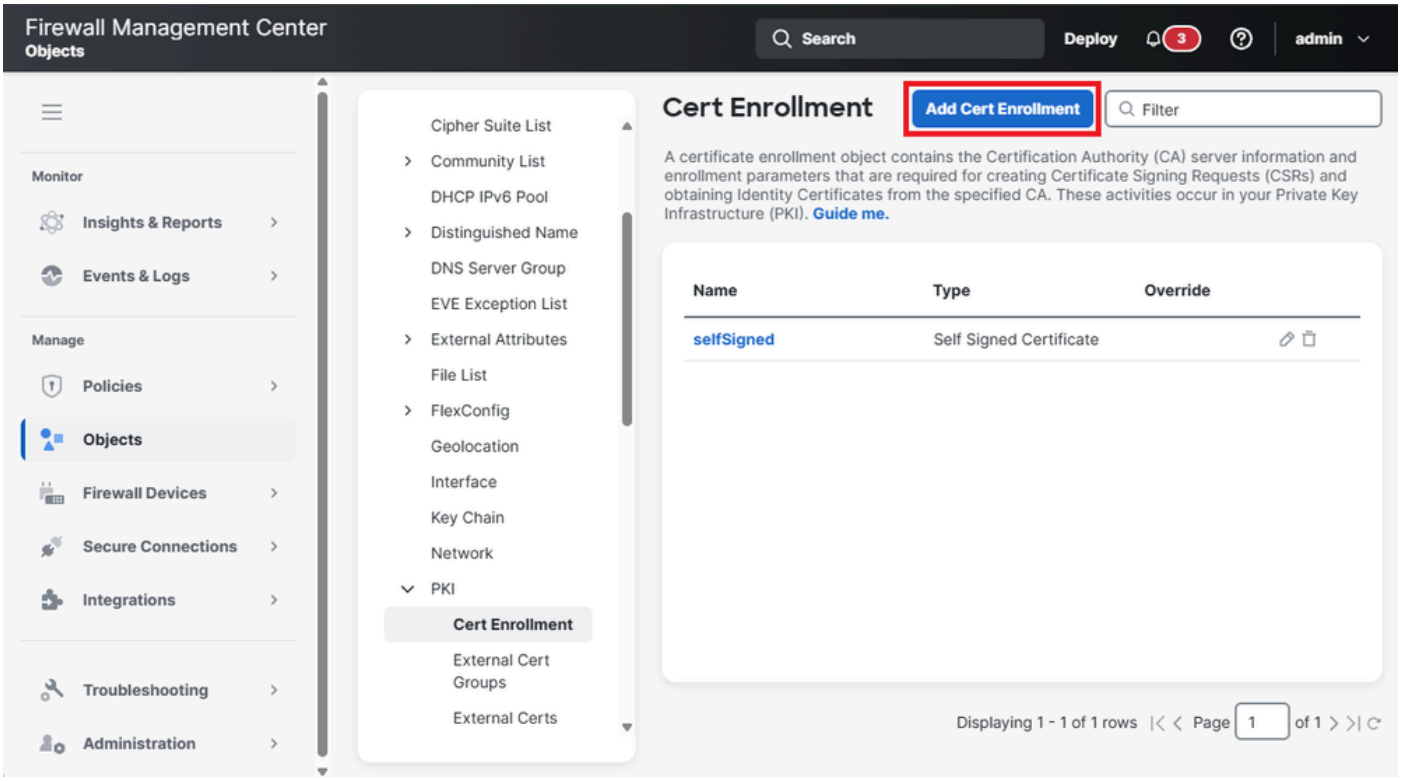
在啟動ACME註冊流程之前，請確保滿足以下條件：

1. 可解析域名:請求證書的域名必須由ACME伺服器進行解析。這可確保伺服器可以驗證域所有權。
2. 安全防火牆訪問ACME服務器：安全防火牆必須能夠通過其介面之一訪問ACME伺服器。此存取不需要透過要求其憑證的介面進行。
3. TCP埠80可用性：允許從ACME CA伺服器到與域名對應的介面的TCP埠80。在ACME交換過程中，需要此步驟才能完成HTTP-01質詢。

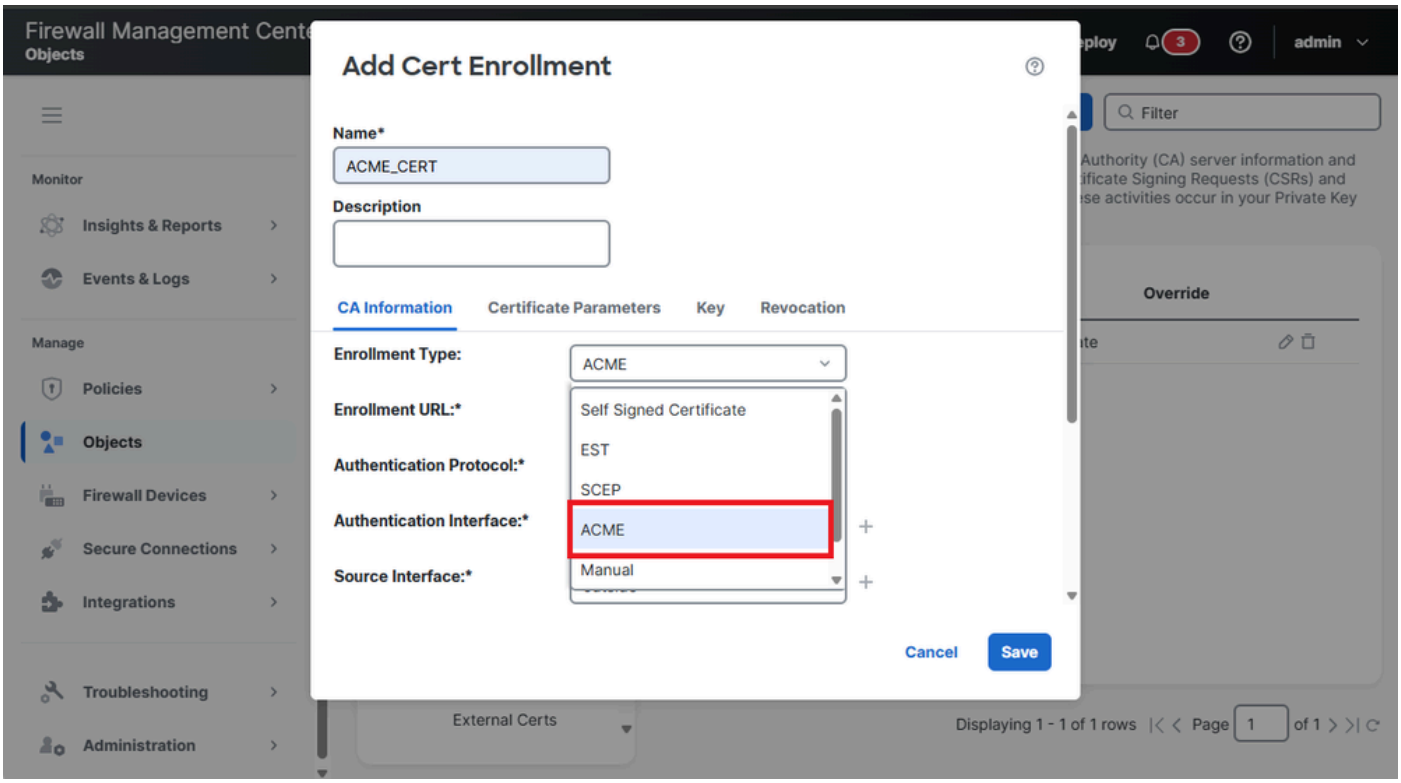
附註：在埠80開啟期間，只能訪問ACME質詢資料。

ACME證書註冊對象建立

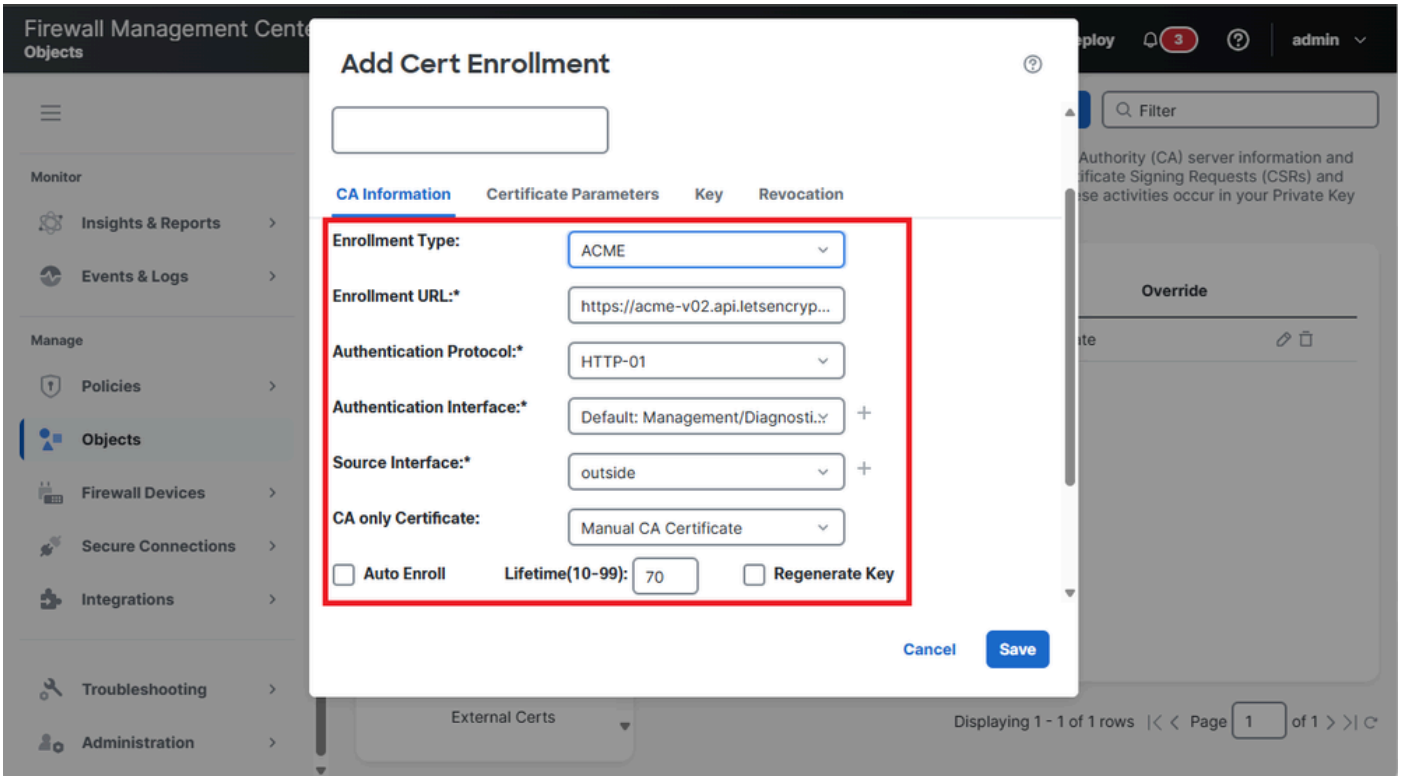
1.定位至對象> PKI >證書註冊，然後按一下新增證書註冊以開始配置過程。



2.下拉選單中列出ACME註冊選項以及其他註冊方法。從Enrollment Type下拉選單中選擇ACME以繼續。



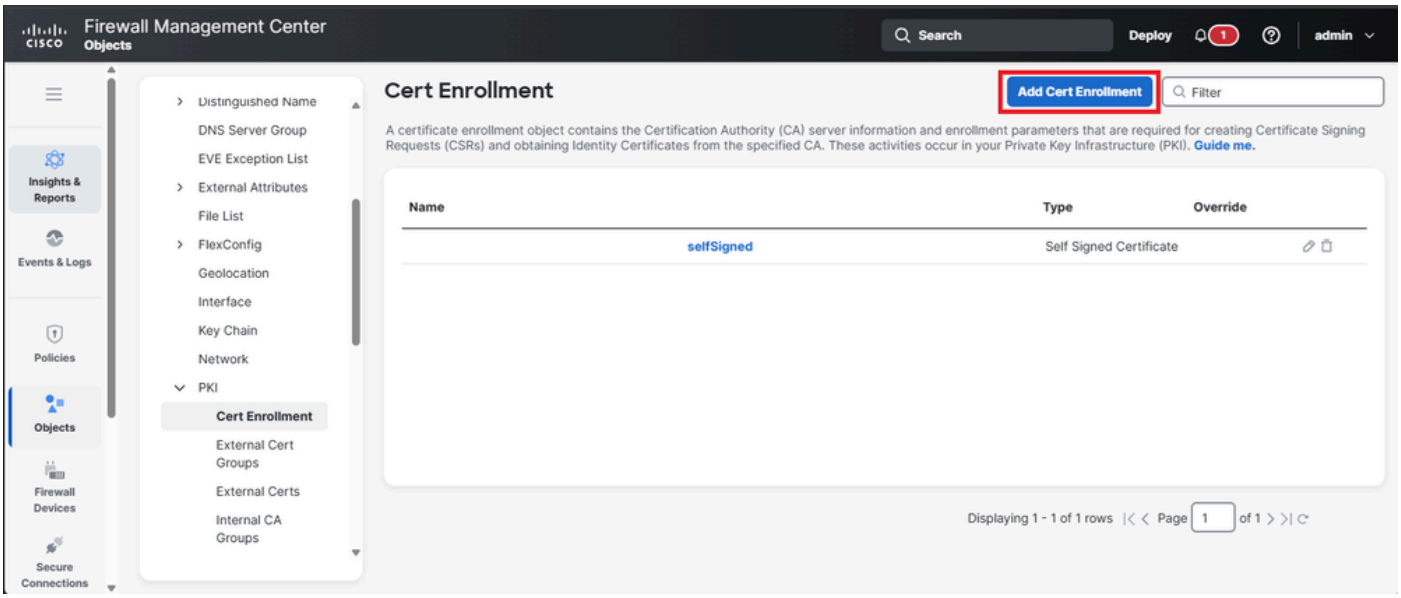
3.顯示配置證書引數的選項，使用相應資訊填寫欄位。



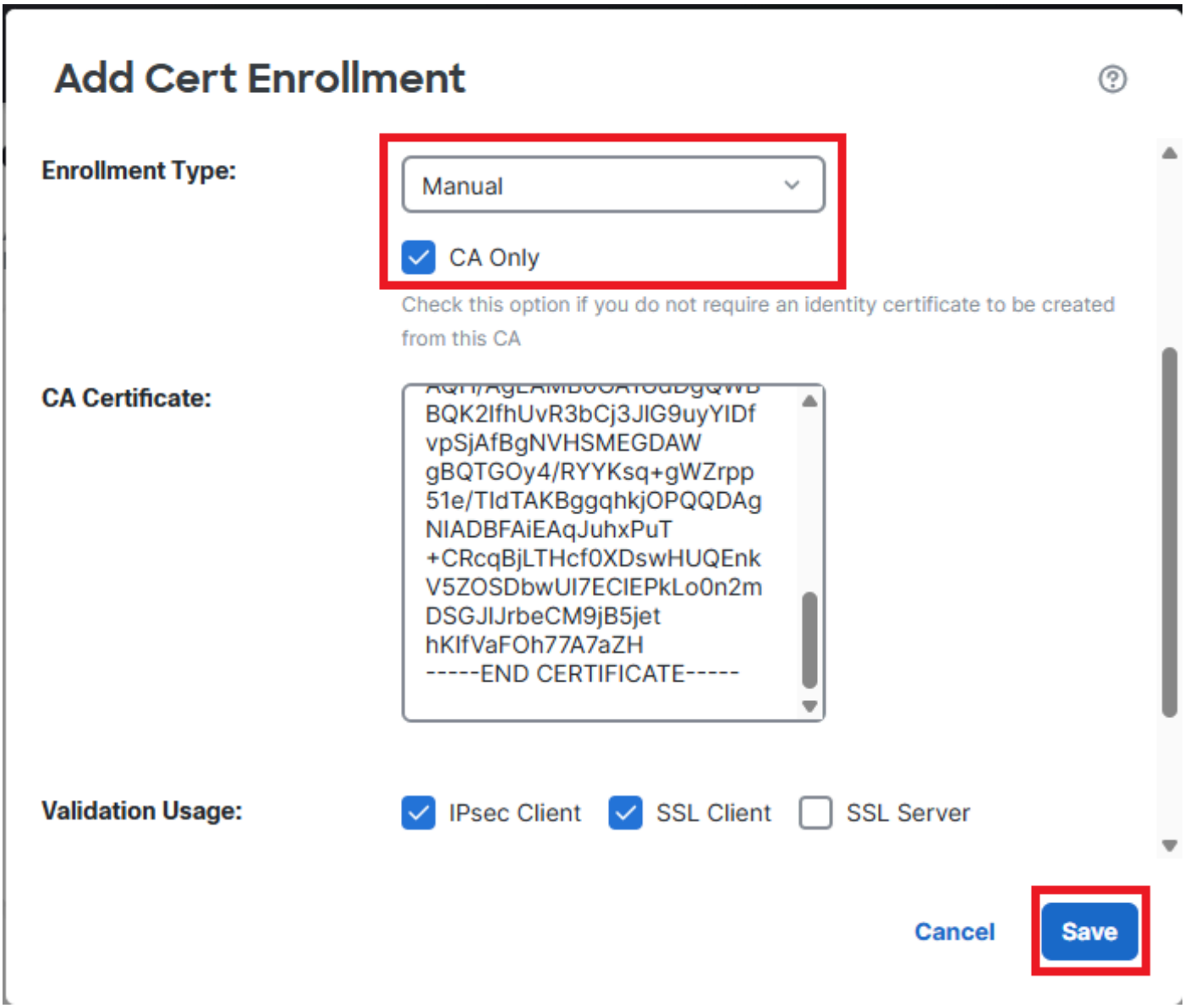
- 註冊URL:這是用於請求和檢索證書的ACME伺服器(如Let's Encrypt)的地址。
- 身份驗證協議：這指定用於驗證域所有權的方法。ACME挑戰支援的協定是HTTP-01。
- 驗證介面:從ACME伺服器接收HTTP-01質詢的FTD裝置上的網路介面。
- 僅CA證書:必須選擇來自證書頒發機構(CA)的證書以信任ACME伺服器。

附註：預設情況下，它指向公用Let's Encrypt服務URL:https://acme-v02.api.letsencrypt.org/directory。

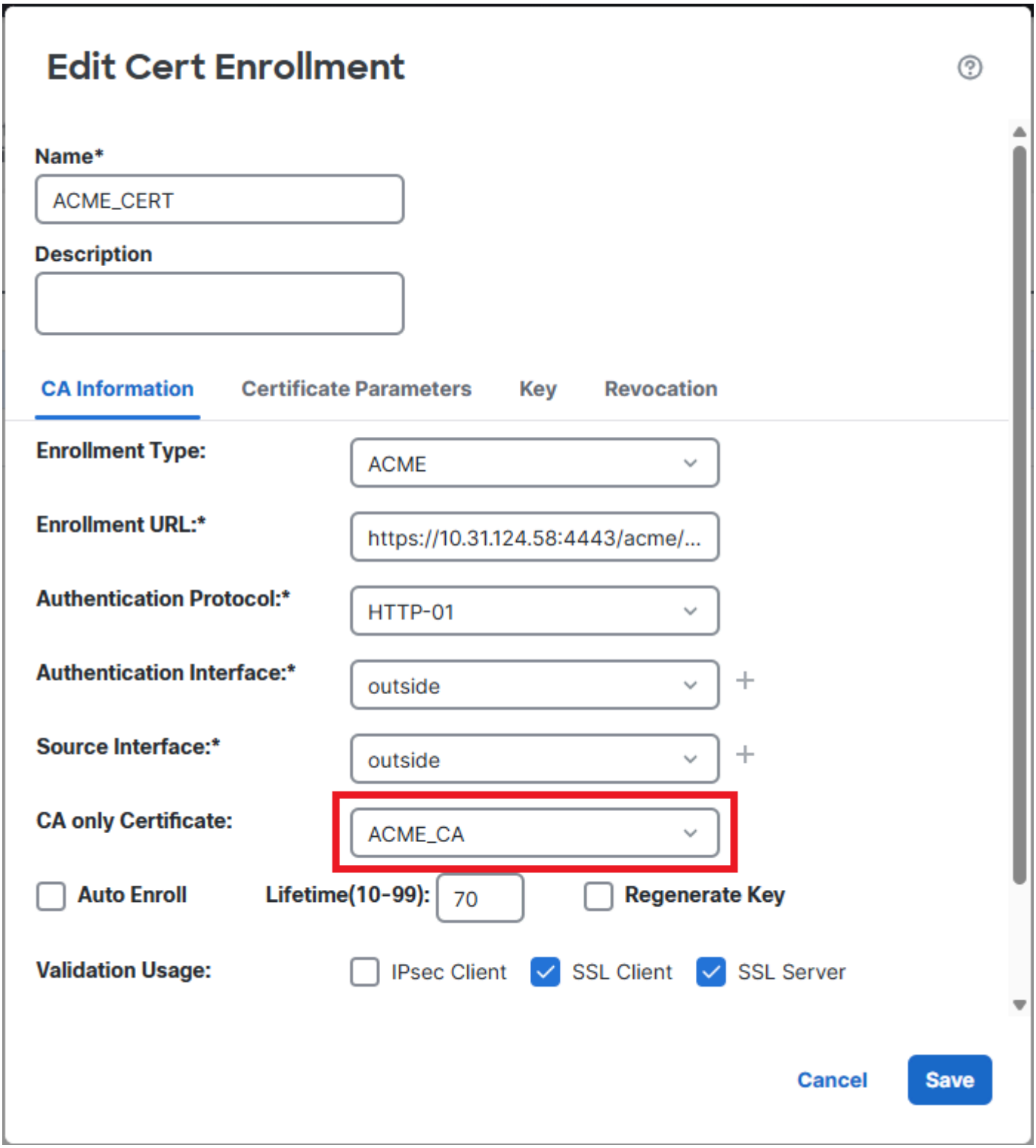
4.如果您使用的是不知名的ACME伺服器，則需要新增ACME伺服器的CA證書。導航到Objects > Cert Enrollment，然後按一下Add Cert Enrollment按鈕。



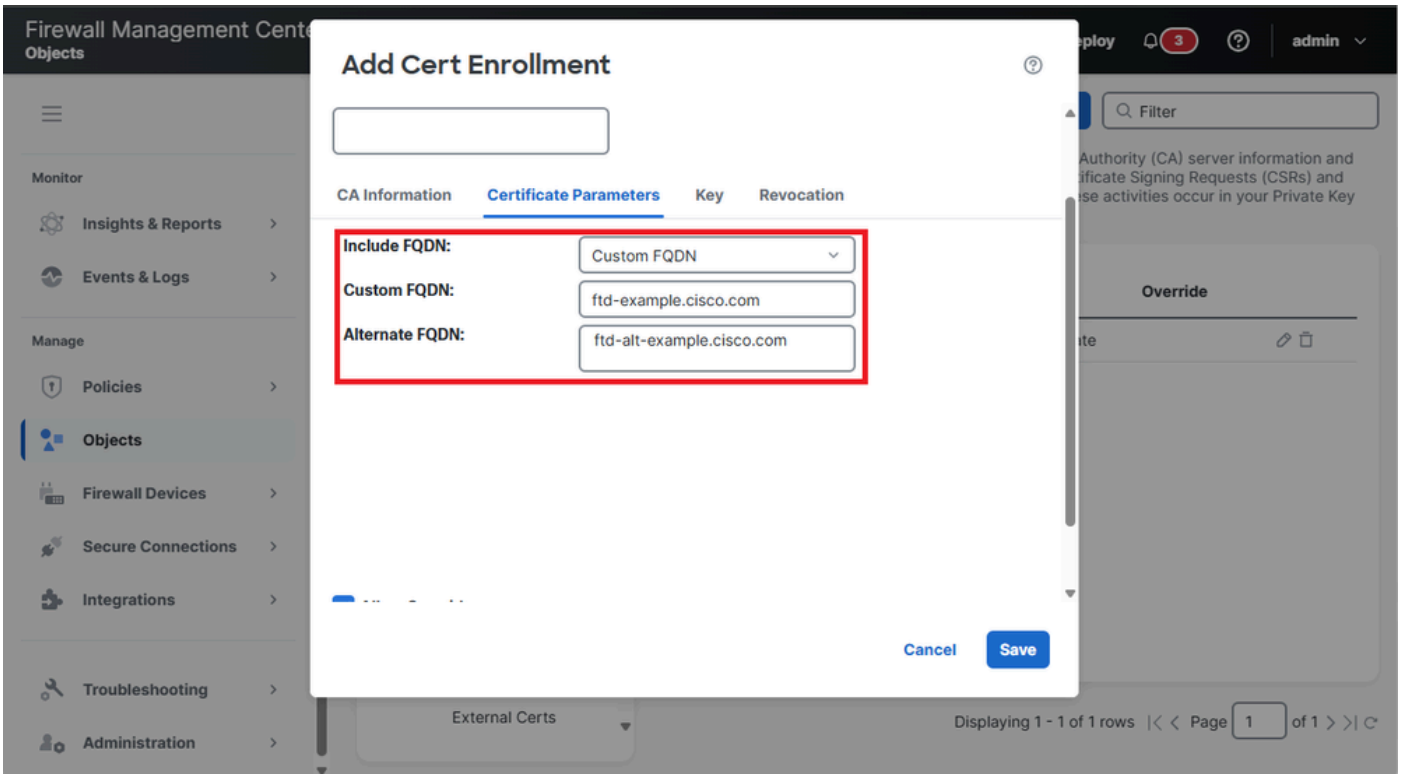
- 為信任點命名，然後選擇Enrollment Type作為Manual。然後，選中選項CA Only。最後，貼上ACME伺服器的CA證書，然後按一下Save。



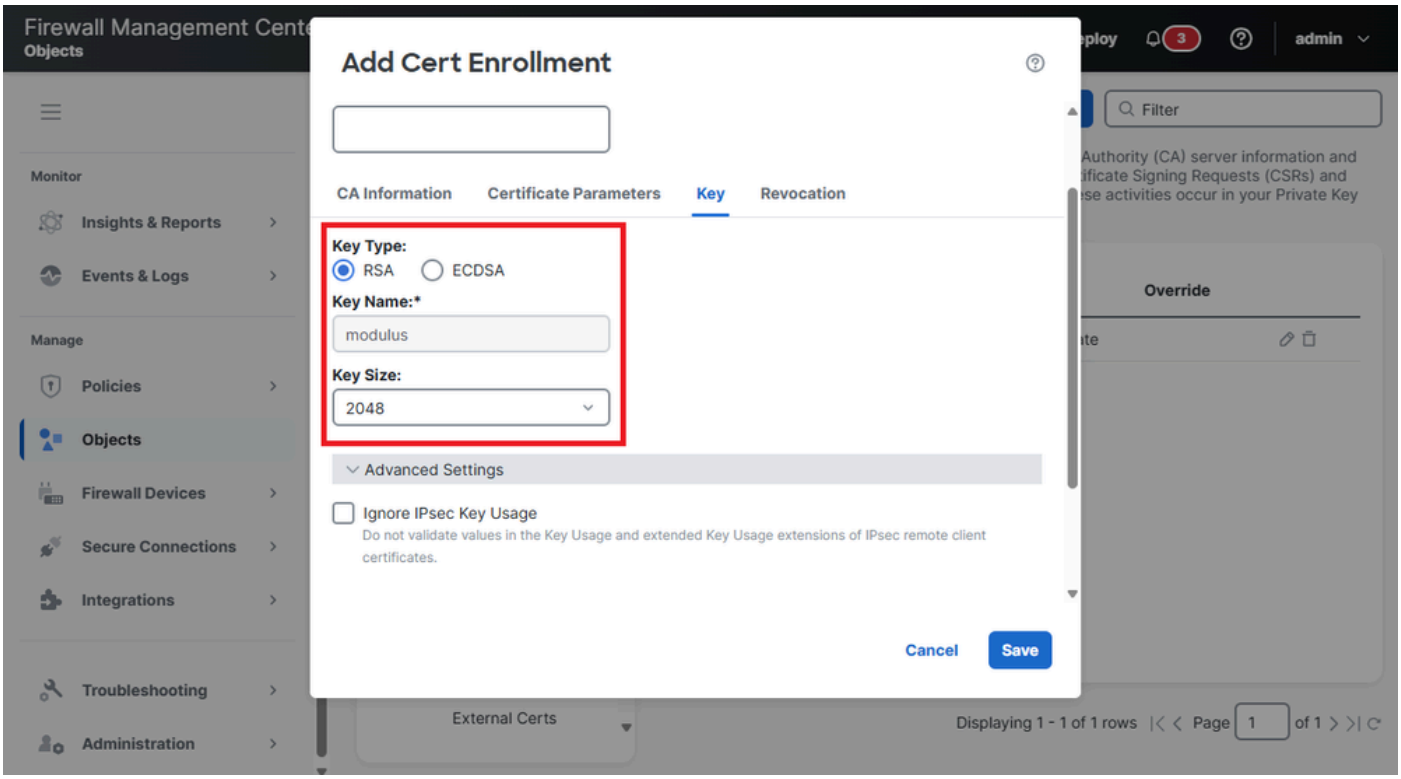
- 最後，在「僅CA證書」部分中選擇ACME CA伺服器的信任點。



5.導航到「證書引數」(Certificate Parameters)，在「包括FQDN」(Include FQDN)框中選擇「自定義FQDN」(Custom FQDN)選項，然後填寫「自定義FQDN」(Custom FQDN)和備用FQDN」(Alternate FQDN)欄位，以包括在證書中。



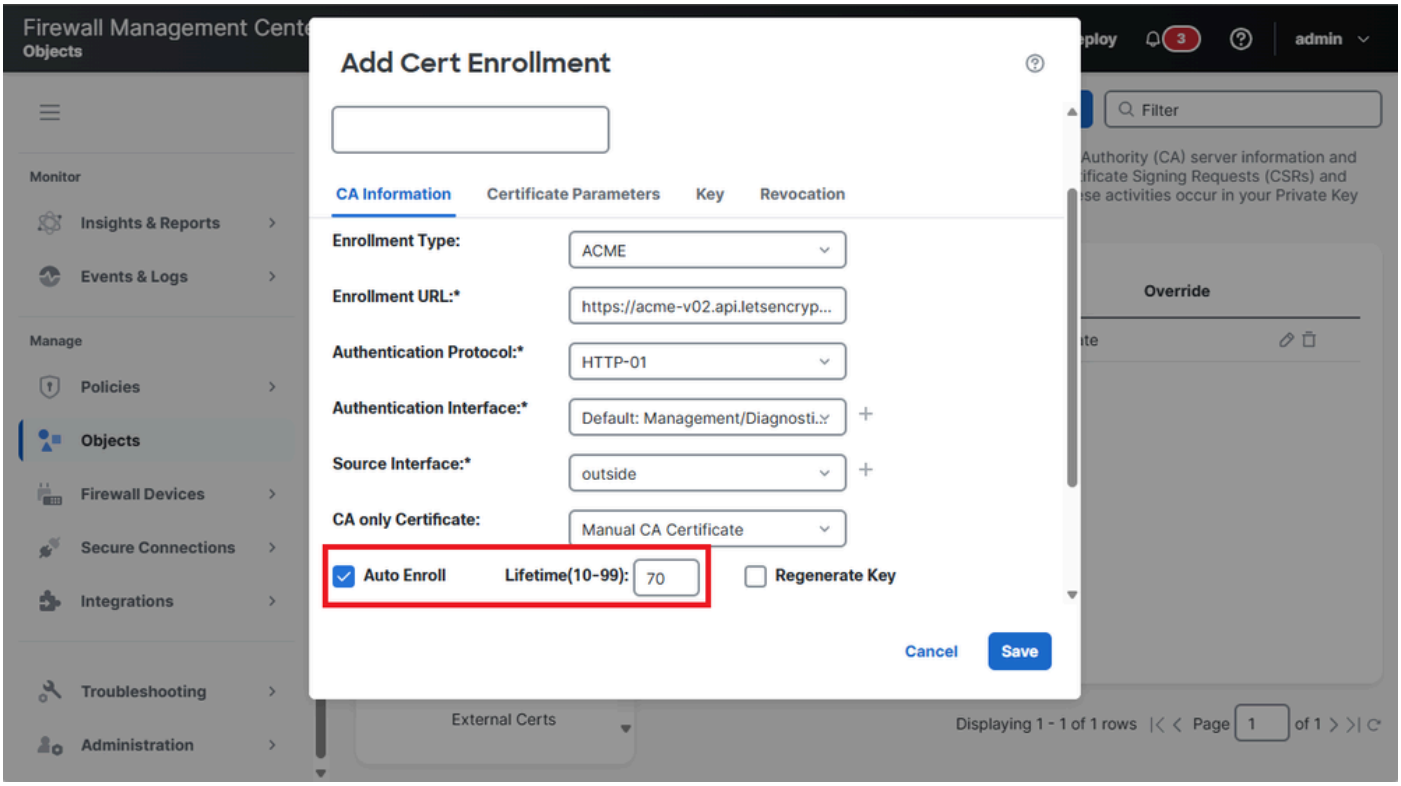
6.定位至鍵，以修改鍵型別和鍵大小設定。



7.（可選）為身份證書啟用Auto Enroll。

選中Auto Enrollback覈取方塊，並指定Auto Enroll Lifetime的百分比。

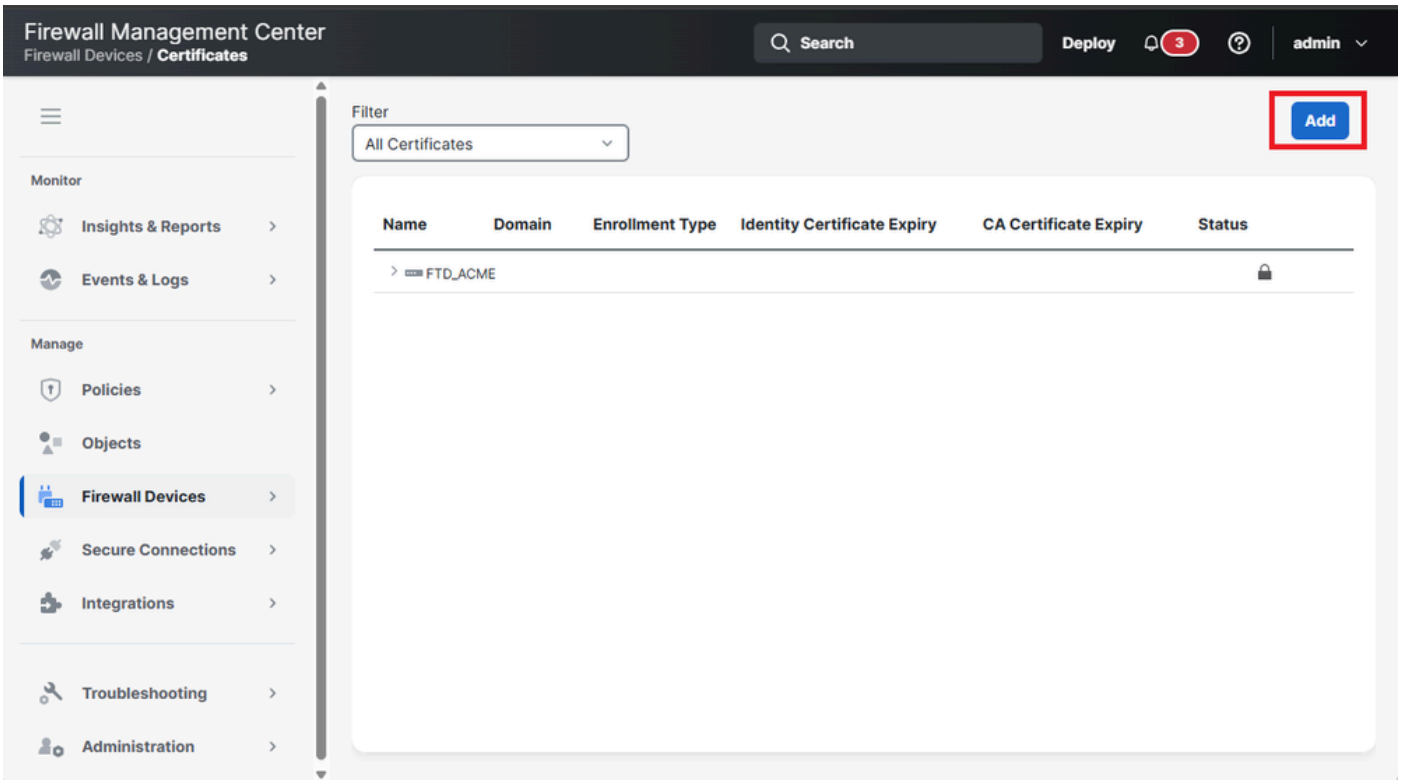
此功能可確保證書在到期之前自動續訂。該百分比確定證書的續訂過程在到期之前提前多長時間開始。例如，如果設定為80%，則當憑證達到其有效期的80%時，續約程式開始。



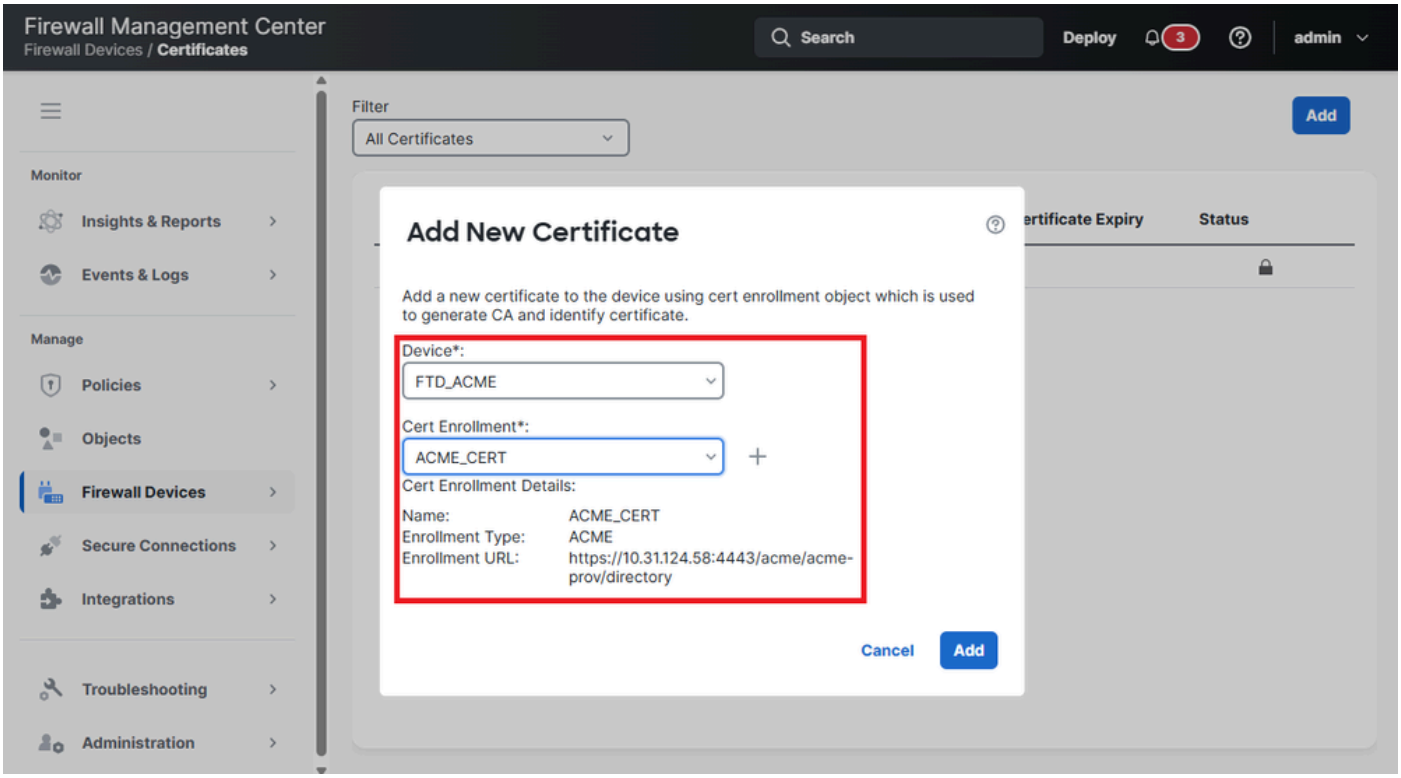
8.按一下儲存。

裝置上的ACME證書註冊

1.導航到Firewall Devices > Certificates，然後點選Add按鈕以註冊新證書。

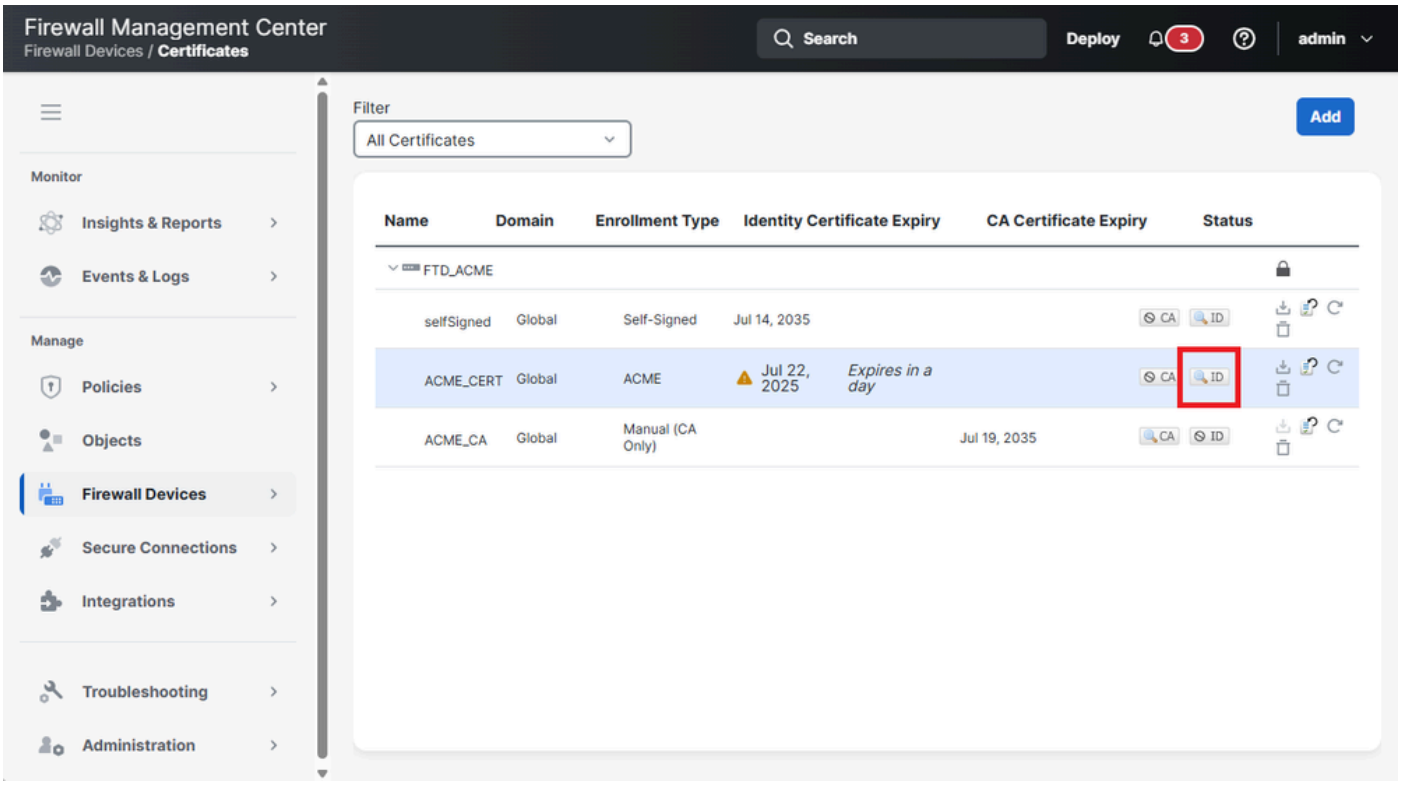


2.從Device下拉選單中選擇FTD裝置，以及以前在Cert Enrollment中建立的證書對象。

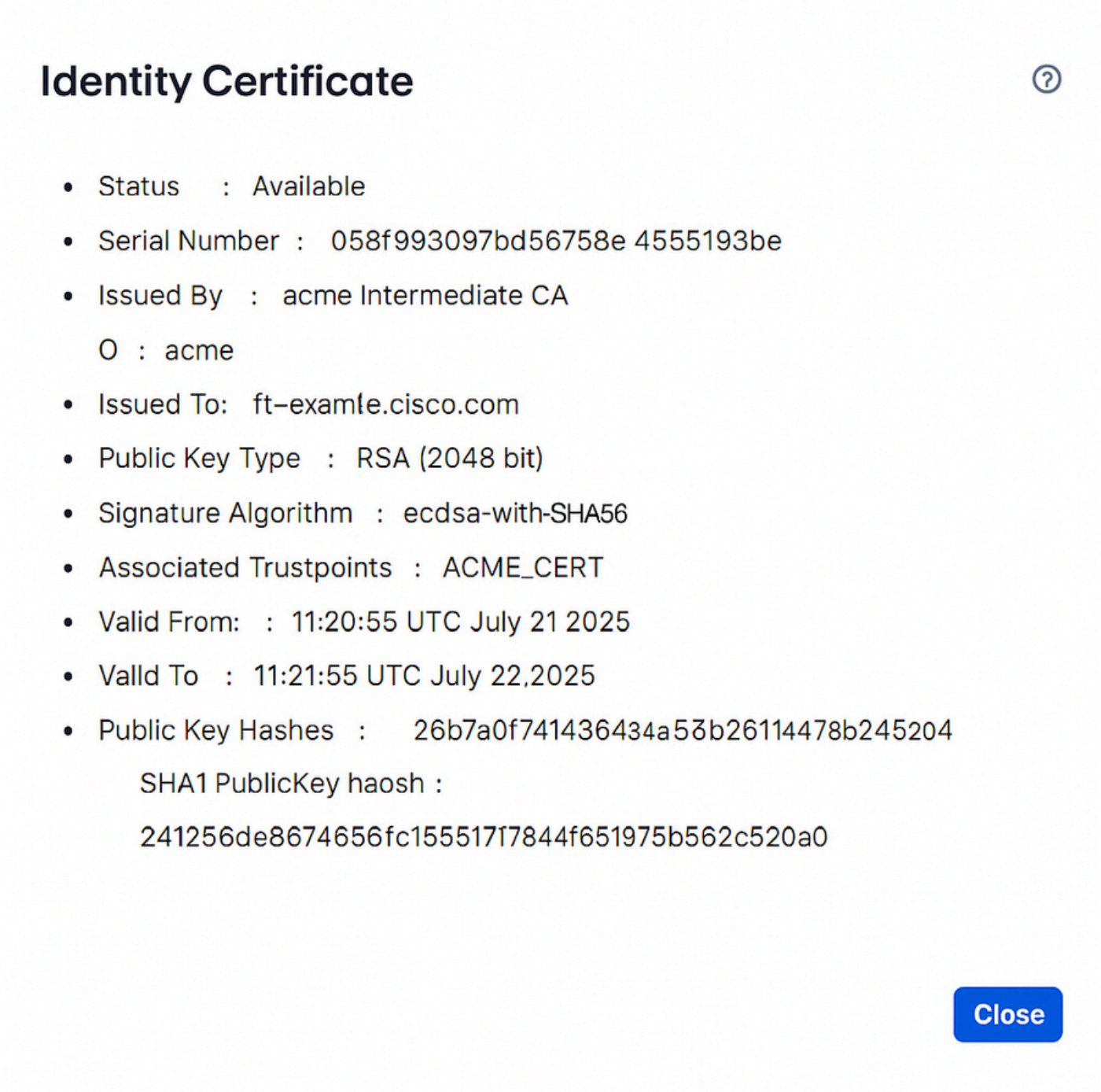


3.按一下Add。

4.部署完成後，狀態列將顯示ID certificate按鈕。



5.按一下ID按鈕驗證ID證書資訊。



驗證

檢視FTD中安裝的憑證

確認已使用命令註冊證書。show crypto ca certificates <Trust Point Name>。

<#root>

```
firepower#
```

show crypto ca certificates

ACME_CERT

```
Certificate
Status: Available
Certificate Serial Number: 058f993097bd56758e44554194a953be
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=acme Intermediate CA
O=acme
Subject Name:
CN=ftd-example.cisco.com
Validity Date:
start date: 11:20:55 UTC Jul 21 2025
end date: 11:21:55 UTC Jul 22 2025
Storage: immediate
Associated Trustpoints: ACME_CERT
Public Key Hashes:
SHA1 PublicKey hash: 26b7a0f7414364a45b246114478bb74f432520c4
SHA1 PublicKeyInfo hash: 24125d6e8674566c1551784f651975b562c520a
```

系統日誌事件

安全防火牆FTD中有新的系統來捕獲與使用ACME協定的證書註冊相關的事件：

- 717067:提供ACME證書註冊何時啟動的資訊。

```
%FTD-5-717067: Starting ACME certificate enrollment for the trustpoint <private_acme> with CA <ca-acme.
```

- 717068:提供ACME證書註冊成功的時間資訊。

```
%FTD-5-717068: ACME Certificate enrollment succeeded for trustpoint <private_acme> with CA <ca-acme.exa
```

- 717069:提供ACME註冊失敗時的資訊。

```
%FTD-3-717069: ACME Certificate enrollment failed for trustpoint <private_acme>
```

- 717070:提供與證書註冊或證書續訂的金鑰對相關的資訊。

```
%FTD-5-717070: Keypair <Auto.private_acme> in the trustpoint <private_acme> is regenerated for <manual>
```

疑難排解

如果ACME證書註冊失敗，請考慮以下步驟來識別和解決問題：

- 檢查與伺服器的連線：確認Secure Firewall與ACME伺服器具有網路連線。確認沒有網路問題或防火牆規則阻止通訊。
- 確保安全防火牆域名可解析：確保安全防火牆FTD上配置的域名可由ACME伺服器解析。此驗證對於伺服器驗證請求至關重要。
- 確認域所有權：驗證信任點中指定的所有域名是否歸安全防火牆FTD所有。這可確保ACME伺服器可以驗證域所有權。

疑難排解命令

如需其他資訊，請收集下一個debug命令的輸出：

- debug crypto ca acme <1-255>
- debug crypto ca <1-14>

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）。