

# 排解憑證疑難錯誤"；無法在FMC上設定CA憑證"

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

### [問題](#)

### [解決方案](#)

#### [步驟 1.找到.pfx證書](#)

#### [步驟 2.從.pfx檔案中提取證書和金鑰](#)

#### [步驟 3.在文字編輯器中驗證憑證](#)

#### [步驟 4.驗證記事本中的私鑰](#)

#### [步驟 5.拆分CA證書](#)

#### [步驟 6.合併PKCS12檔案中的證書](#)

#### [步驟 7.在FMC中匯入PKCS12檔案](#)

### [驗證](#)

---

## 簡介

本文描述如何對由FMC管理的Firepower威脅防禦裝置上的證書頒發機構(CA)匯入錯誤進行故障排除和修復。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- [公開金鑰基礎架構 \(PKI\)](#)
- [Firepower Management Center \(FMC\)](#)
- [Firepower Threat Defense \(FTD\)](#)
- [OpenSSL](#)


### 採用元件

本檔案中的資訊是根據以下軟體版本：

- MacOS x 10.14.6
- FMC 6.4
- OpenSSL

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

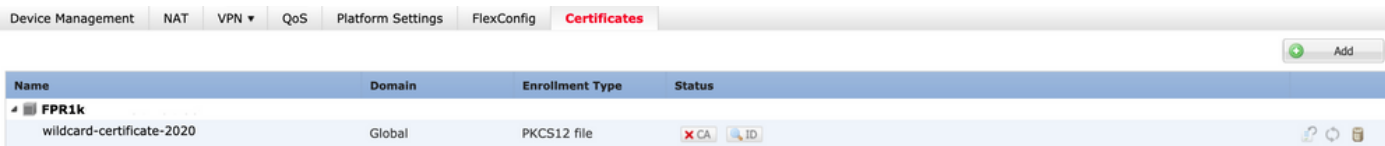
## 背景資訊

 註：在FTD裝置上，需要先使用CA憑證，才能產生憑證簽署請求(CSR)。

- 如果在外部伺服器（例如Windows Server或OpenSSL）中產生CSR，則手動註冊方法會失敗，因為FTD不支援手動金鑰註冊。必須使用其他方法，例如PKCS12。


## 問題

在此特定案例中，FMC在CA憑證狀態中會顯示一個紅十字（如圖所示），表示憑證註冊無法安裝CA憑證。當證書沒有正確打包或PKCS12檔案不包含正確的頒發者證書時，通常會出現此錯誤，如圖所示。



The screenshot shows the 'Certificates' tab in the FMC GUI. A table lists certificates with columns for Name, Domain, Enrollment Type, and Status. One certificate, 'wildcard-certificate-2020', has a status of 'CA' with a red 'X' icon, indicating an error.

Name	Domain	Enrollment Type	Status
wildcard-certificate-2020	Global	PKCS12 file	CA

 注意：在較新的FMC版本中，已解決此問題以匹配ASA行為，該行為會建立根CA包含在.pfx證書的信任鏈中的其他信任點。

## 解決方案

### 步驟 1. 找到.pfx證書

獲取在FMC GUI中註冊的pfx證書儲存，然後在Mac終端(CLI)中查詢該檔案。

```
docs# ls -l
total 16
-rw-r--r--  1 holguins  staff  4701 May 23 15:11 cert.pfx
```

ls

### 步驟 2. 從.pfx檔案中提取證書和金鑰

從pfx檔案中提取客戶端證書（非CA證書）（需要用於生成.pfx檔案的密碼）。

```
openssl pkcs12 -in cert.pfx -clcerts -nokeys -out id.pem
```

```
docs# openssl pkcs12 -in cert.pfx -clcerts -nokeys -out id.pem
Enter Import Password:
MAC verified OK
```

身份匯出

擷取CA憑證 ( 不是使用者端憑證 ) 。

```
openssl pkcs12 -in cert.pfx -cacerts -nokeys -out certs.pem
```

```
docs# openssl pkcs12 -in cert.pfx -cacerts -nokeys -out certs.pem
Enter Import Password:
MAC verified OK
```

cacerts export

從pfx檔案中提取私鑰 ( 需要步驟2中的相同密碼 ) 。

```
openssl pkcs12 -in cert.pfx -nocerts -out key.pem
```

```
docs# openssl pkcs12 -in cert.pfx -nocerts -out key.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

金鑰匯出

現在存在四個檔案 : cert.pfx ( 原始pfx捆綁包 ) 、 certs.pem ( CA證書 ) 、 id.pem ( 客戶端證書 ) 和 key.pem ( 私鑰 ) 。

```
docs# ls -l
total 40
-rw-r--r--  1 holguins  staff  4701 May 23 15:11 cert.pfx
-rw-r--r--  1 holguins  staff  2301 Jun 10 01:34 certs.pem
-rw-r--r--  1 holguins  staff  2410 Jun 10 01:34 id.pem
-rw-r--r--  1 holguins  staff  1958 Jun 10 01:34 key.pem
docs#
```

匯出後的ls

### 步驟 3.在文字編輯器中驗證憑證

使用文字編輯器驗證憑證 ( 例如nano certs.pem ) 。

對於此特定案例 , certs.pem僅包含子CA ( 核發CA ) 。

從步驟5開始，本文介紹檔案certs.pem包含2個證書（一個根CA和一個子CA）的情境中的程式。

```
Bag Attributes: <No Attributes>
subject=/C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Intermediate CA
issuer=/C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Root CA
-----BEGIN CERTIFICATE-----
MIIF0zCCA7ugAwIBAgICEAUwDQYJKoZIhvcNAQELBQAwdjELMAkGA1UEBhMCTVgx
DTALBgNVBAGMBENETVgxEjAQBgNVBAoMVCVUz3UgQ29ycDEoMCMYGA1UECwwfVW5n
dSBDb3JwIENlcnRpZmljYXRlIEF1dGhvcml0eTEaMBGGA1UEAwwRVW5ndSBDb3Jw
IFJvb3QgQ0EwHhcNMjIwMjYyMTQ0NDQ4WhcNMjIwMjYyMTQ0NDQ4WjB+MQswCQYD
VQQGEwJNWDEnMAcGA1UECAwEQ0RNWDESMBAGA1UECgwJVW5ndSBDb3JwMSgwJgYD
VQQGLDB9Vbmd1IENvcnAgQ2VydG1maWNhdGUgQXV0aG9yaXR5MSIwIAYDVQQDDb1V
bmd1IENvcnAgS5W0ZXJtZWVpYXRlIENBMTIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAt9zB5lbrhMTEEyGmRVRnuQ+mt86axF3QZEeSYCfV5gZs9R25cw+N
L7U9agbL/bNfvR00N8I8ywVahITWJP9kuzGksEDaUzyHXybDslyPhUNT0fYn5zFi
GGa8lr90KmxSpsXeQB+GB0D8wezA1bAAGSKDiQymtBdQQMpnKTCmCRCjcPD1rBq1
EwiO/7ePWhHK4KhtBBfSmjQxZYb1QIG5DBWCKA4q2DlME9/o+pL944Utw+HMLrAH
4bT86kT7cYQVbeVSmocastuN+1jux2aJ+4jT0GJM44yn0KzVANOlgEjw/DPhW460
u9I1oJGMCh4j7Efl8bYvHTd+8yEejmHR+ASycsy+8qoymWq3wIPiWJA0r160Hn2c
JOZpu2oQQs+90+wBrzn/yV7aZmVDdbEJSXKHJKIGA7k5VWe/CvXbfExHSCfdZ5EV
uIx4AixdgwEdd0rgrpHvY0GS1IHBmXNKoPp6s41oLmSmSr8lgZqm5mgdDlUKNA8tG
0jVrURiHLalHhyyoYHHVihEjhPrjNL9T26Dq9iAhX6yMclIXB1QG/QUxef7AL07
nzIBASrYnAEv+TvgYkRE4Z9gVKxYhNLpxnVg0ycHiZbco2IcQzqIwdQAqQS2LRWP
8eNuPd9l+5BgsSYgK3NxQPzMXZwmMXgnGye3lueBUL9DSkuknx0aFVMCAwEAAAnj
MGEwHQYDVR00BBYEFEDAVTSyUoHTThBtxlvip1L0TEQoMB8GA1UdIwQYMBaAFJMO
DF6TWO6EkboLkLC0t59z01QwMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgGGA0GCSqGSIb3DQEBCwUAA4ICAQBUNUuk9jMTGmcP6j/tqBFM3Inhj/84ABMY
T4RBdtxi1v5HPjtknyEIp1B31QxrWi4pLiyh0ILb181mNxnawZDOMvzv7Bsxepvx
xHrGhGac2y4yT72vGcIp/++8H2LatFaGAGePissCjzTcLG9brubP/MXYJ3MrlGXl
FbqvTdDJS5qB0+jRnMbACbV/nTUVXl6f6vb3AW2Zy0/u0+S6VoIB5Uk4xLZuhrwl
IXxSTghQWLqK4FBLj+XxyK2u+10iR3+6JGkkaIbb62zJsklnSJ+gVHgsMhEjATto
H0Zw5+uoJQyl/pa4uk0UaRpkSicH82p+4gPeCg5cEQAcI4niqJgIH0oPYJQszRwD
IB2w3nTAaNMtDyH6Ih/N/MvPibhaYI3jynGEMjansw8zCBPoeak4bTsEx3hu7a/
kWddLmv2TscsfkGCL0XL0fclLcW4R6QvsZaj3Ia0AsX/Lm0eYb7RnXfjPHenp3rA
a9I0LNe9/AyQrAqp3hQ4XSNs3zgScCja40ZcXiSgJcf1XI58Ml2phT4bob89vY+u
xIawv6bXiTQE7P2RBUeJWPMFclJ75JMplRYsj2xogkneMiPpc9w5moZLxZpvznqgy
aCi37m1d+CT6hYTWxe3HztS03VJ+24IqEr+wmi+FB04VHZtqc/Bpajb0TpGBUGex
wxMFkoFWSA==
-----END CERTIFICATE-----
```

證書檢視

## 步驟 4. 驗證記事本中的私鑰

使用文本編輯器（例如 nano certs.pem）驗證 key.pem 檔案的內容。



```
Bag Attributes
  localKeyID: 4B ED BA 56 76 3A C9 22 C3 75 54 A7 0A 1A F1 7D 3B 5E B0 D8
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI9vQUkrEl0MMCAggA
MBQGCCqGSIB3DQMHBajnRV9YTIYsSwSCBMjqf1Lhs3v0RL0DHkvi7yvWSd3xWLMn
jt1hgOLsU1TDmBAWp/LXpqSP27c4XCQiZc0eiFDqm8aKw9xTDjgkEUBVactZs+Sz
yCE1gcG6NRH9lZFiwOYy+MCR4EPYh06DJPQ+MxLvtjjHrErruyXlAlYwfAtrAcQk
E5tJniCaNTppwfvOfLpd/oHa2tF0kBMVVjS3HyxAXEfNThmzMwKRYgsLPUKShTfb
iv0bu8zI6fVfB4db3J/FjqikoiCHKXbWetm/GewZ071H3DW0HamtPw3InUuvYuzv
SM08x+Nji6uo7gtrQ6Rld2z5fN6vTtAw3x10AHjxm+vf0xt95zXhABYkMg2zHaQg
0djTHYFwdHwPdmSSNWM8hWnY8AvFxdjXURp/5MNP+v6ty5W/ETVe6o+Dh1sa9i7v
PzUwIDWs6kt0rxp0v8200lmqSKD6C4UnD1Vf2hH7AyMuwRpYamOEIuPtg8GgeiHJ
6vxpIJ3dY9/s0eyElkvKimZgiXpexBV/nDnksCLJTgyR08AE56iq2+XiBkwIoUai
QTZNi3S+PmPf8glHFtVKR8V6Zk4u8xov3reNTTmKXXcH3mHPaMU/Nhdldn8fpx+
phTzULmdtIpD3r1Hknh0uMvjrw0RYTLp1WGiEo5DU1SyI5jrMCYa0mhufOI7vtPp
rQqXNo6JleXuBteWSIHdqFynrtIdLyUVhK5QwF40m9+OvGkXNuqMDv4fH4+7nv9l
KqK2NS4yUXW1KjbaFe+Cxz9E7stt4Nyvwx56l/FpYLHymYDjQA3kFrC3tPHeULjT
fp95fJ+6g2R0nr4yKerHbV5BAaiOV3rRVpBWhgzBK5o3w4+C+QIH6tgD1f2Jp9YA
TZLj/BDxIc40Q6AORATjWcbE1fvuNmNvMEQpDFM0gP8mlqnnBGzc5mwxC1xTNcQD
nmaFYykWvXyCzsvQAgwkvzyzzZw2mPNQpj3lVIOVRdZy8NWVvKcBLpq2XTSA6AQIK
mnJLY+rSAEi6miVnHeUW683un8KND9+HQ1YZbpKDK+JGcwKp/KhEHKmipEoHS8b5
MLby4tL7qrA3sfddMooJJYsCC372WYrd8xPrDZ9kYJ0N64ks9sYhvRUxRMJaxqaY
Int7b6p90i1r0LpielhUUrEvbu0CudM4sLDyXq8Fqf9G5u8dMuchCjXrEPGhmf4Y
ZhTfQF3xxQYtLBbLfwEQUft6GBsJMLGZFTFPM06/e3vToRu/Opw4Z9hrA6zBfQWa
bcT868DNME+UQxoT825SLwsFFPcj0pixn21FSm6baiq6QWvTV9+5797+AEPnG23i
1x/KKsvTEuwyHGgAX6p9Z0bfP0VcikMzk09MvMDU5MOUm01bnb0zINrrblG0qmRX
SYNNOL7lJ3joAKzv056KURWAMk9tQE8hAefWAZHS1PacwgUIWxOSAszRMkneptiR
VCm5UvzbYiMIA0rJjx6PTakuPIhdfokLyWfMI74ETao0Hl7KdDD1i/w11fAWFqtN
2gzfPw7Q02F7iZiYtxV9ryVBnH4wqut9pFjPYGu2oXC5q4Y7lJ1DrMzc879vAchM
C1dBcaJLWdpdTmrg2WNiao/rv3A20JjP0zAOeUwRo9r50S0oF9ez1ghBpAAtehyi
FGY=
-----END ENCRYPTED PRIVATE KEY-----
```

## 步驟 5. 拆分CA證書

如果certs.pem檔案有2個憑證（1個根CA和1個子CA），則需要從信任鏈中移除根CA，才能在FMC中匯入pfx格式的憑證，只需在鏈中保留子CA即可進行驗證。

將certs.pem拆分為多個檔案，下一個命令將證書重新命名為cacert-XX。

```
split -p "-----BEGIN CERTIFICATE-----" certs.pem cacert-
```

```
docs# split -p "-----BEGIN CERTIFICATE-----" certs.pem cacert-
docs#
```

拆分

```
docs# ls -l
total 56
-rw-r--r--  1 holguins  staff    219 Jun 10 01:46 cacert-aa
-rw-r--r--  1 holguins  staff   2082 Jun 10 01:46 cacert-ab
-rw-r--r--  1 holguins  staff   4701 May 23 15:11 cert.pfx
-rw-r--r--  1 holguins  staff   2301 Jun 10 01:34 certs.pem
-rw-r--r--  1 holguins  staff   2410 Jun 10 01:34 id.pem
-rw-r--r--  1 holguins  staff   1958 Jun 10 01:34 key.pem
docs#
```

拆分後的ls

使用以下命令將.pem副檔名新增到這些新檔案。

```
for i in cacert-*;do mv "$i" "$i.pem";done
```

```
docs# for i in cacert-*;do mv "$i" "$i.pem";done
docs#
```

重新命名指令碼

檢查兩個新檔案，並使用所述的命令確定哪個檔案包含根CA，哪個檔案包含子CA。

首先，找到id.pem檔案（即身份證書）的頒發者。

```
openssl x509 -in id.pem -issuer -noout
```

```
docs# openssl x509 -in id.pem -issuer -noout
issuer= /C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Intermediate CA
```

頒發者檢視

現在，找到兩個cacert-files（CA證書）的主題。

```
openssl x509 -in cacert-aa.pem -subject -noout
openssl x509 -in cacert-ab.pem -subject -noout
```

```
docs# openssl x509 -in cacert-ab.pem -subject -noout
subject= /C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Intermediate CA
```

主題檢查

將Subject與id.pem檔案的Issuer匹配的cacert檔案（如前面的影象所示）是以後用於建立PFX證書

的子CA。

刪除沒有匹配主題的cacert檔案。在本例中，該證書是cacert-aa.pem。

```
rm -f cacert-aa.pem
```

## 步驟 6. 合併PKCS12檔案中的證書

在新的pfx檔案中合併子CA證書（在本例中，名稱為cacert-ab.pem）以及ID證書(id.pem)和私鑰(key.pem)。您必須使用密碼保護此檔案。如果需要，請更改cacert-ab.pem檔名以匹配您的檔案。

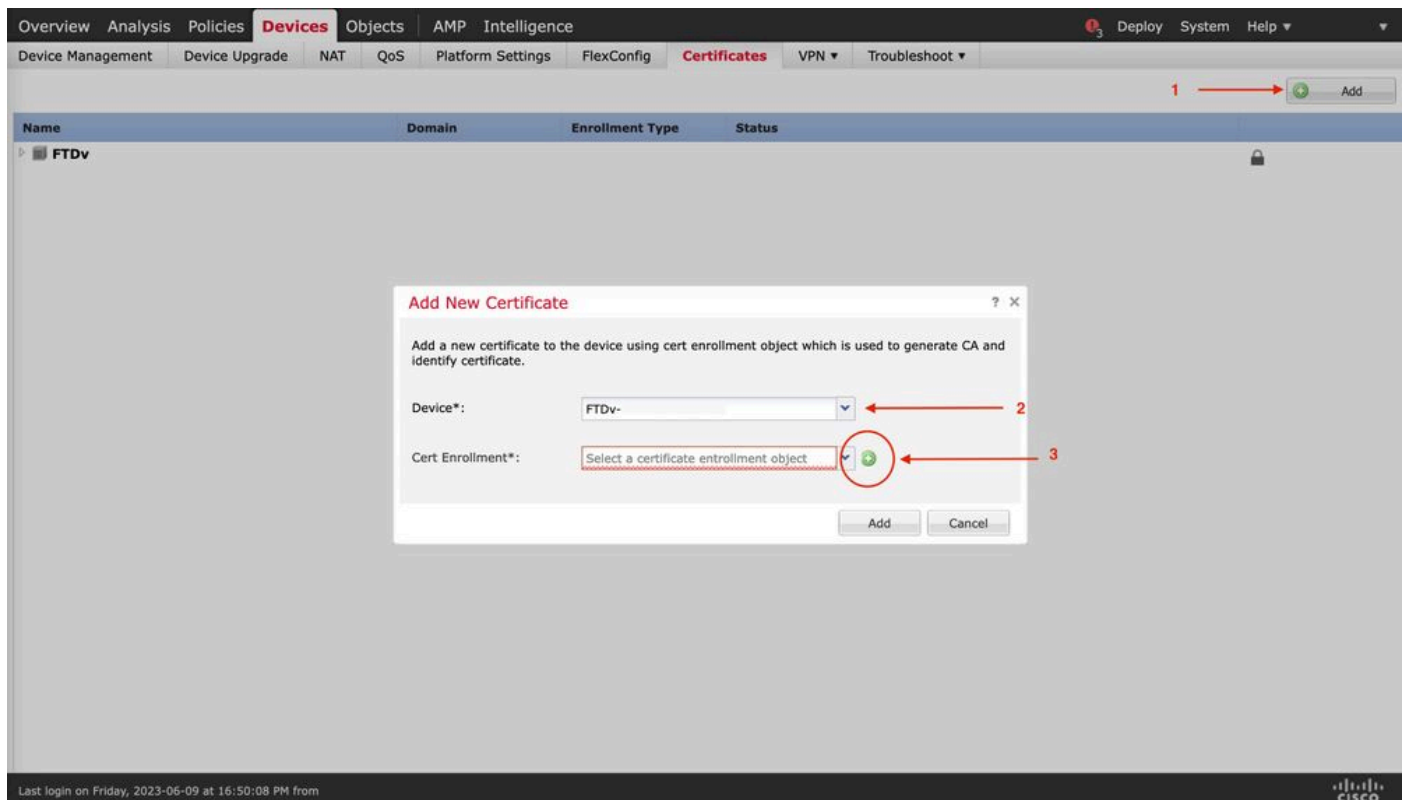
```
openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
```

```
docs# openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
Enter Export Password:
Verifying - Enter Export Password:
```

pfx建立

## 步驟 7. 在FMC中匯入PKCS12檔案

在FMC中，導覽至Device > Certificates，並將憑證匯入所需的防火牆，如下圖所示。



證書註冊

插入新證書的名稱。

## Add Cert Enrollment

? X

Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

PKCS12 File\*:

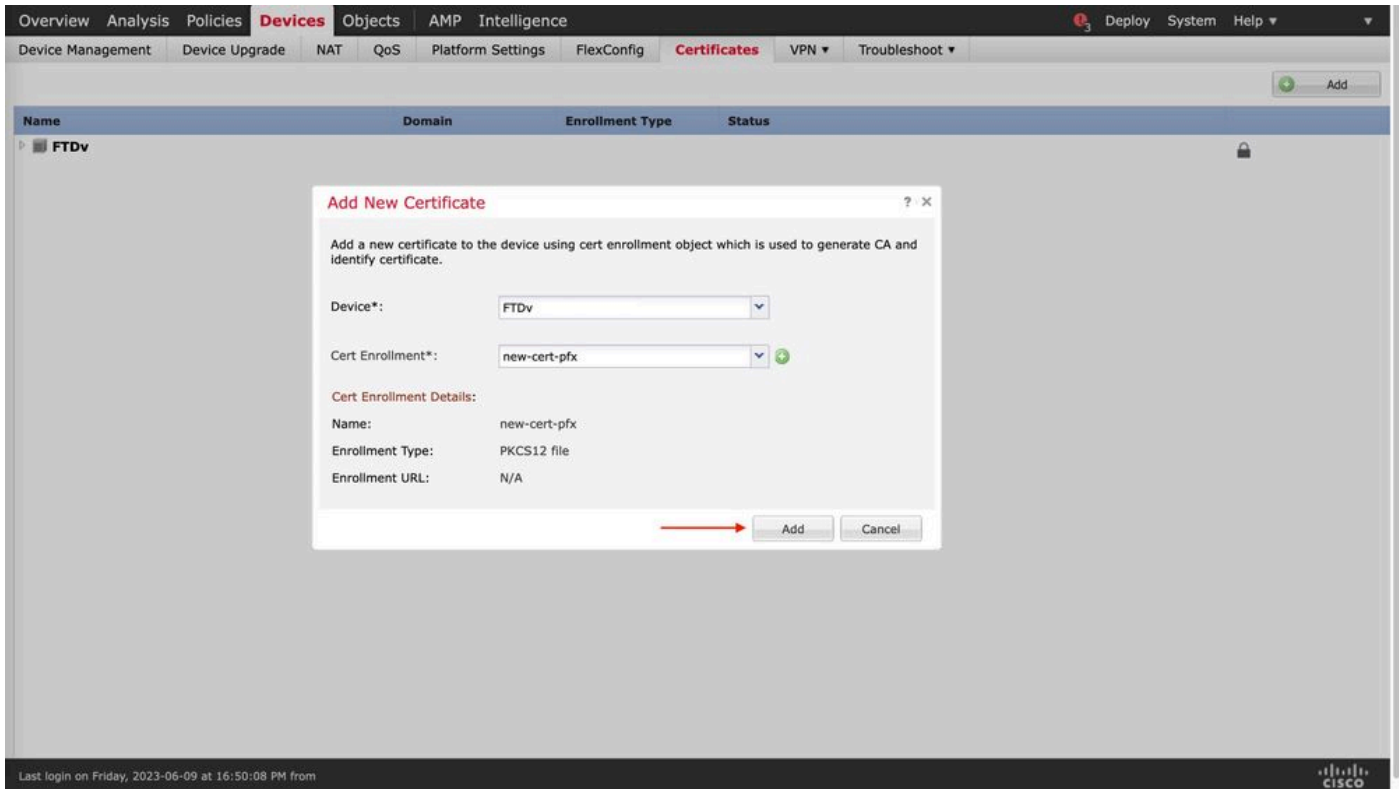
Passphrase:

Allow Overrides

註冊

新增憑證，然後等待註冊程式將新憑證部署到FTD。





new-cert

新證書必須可見，CA欄位中不能有紅十字標籤。

## 驗證

使用本節內容，確認您的組態是否正常運作。

在Windows中，您可能會遇到這樣的問題：即使.pfx檔案只包含ID證書，但作業系統仍顯示證書的整個鏈（如果它的儲存中有subCA，CA鏈）。

若要檢查.pfx檔案中的憑證清單，可以使用certutil或openssl等工具。

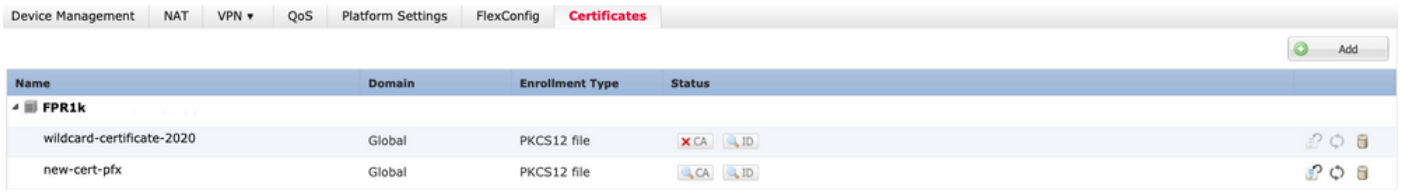
```
certutil -dump cert.pfx
```

certutil是一個命令列實用程式，它提供.pfx檔案中的證書清單。您必須看到包含ID、SubCA、CA（如果有）的整個憑證鏈。





或者，您也可以使用openssl命令，如下面的命令所示。

```
openssl pkcs12 -info -in cert.pfx
```

若要驗證憑證狀態以及CA和ID資訊，您可以選擇圖示並確認其已成功匯入：



The screenshot shows a web interface for managing certificates. At the top, there are navigation tabs: Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig, and Certificates (highlighted in red). An 'Add' button is located in the top right corner. Below the navigation is a table with the following columns: Name, Domain, Enrollment Type, and Status. The table contains two entries:

Name	Domain	Enrollment Type	Status
wildcard-certificate-2020	Global	PKCS12 file	 CA 
new-cert-pfx	Global	PKCS12 file	 CA 

## 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）。