

# 在FMC管理的FTD上安裝並續訂憑證

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景](#)

### [設定](#)

#### [證書安裝](#)

##### [自簽名註冊](#)

##### [手動註冊](#)

##### [PKCS12註冊](#)

#### [證書續訂](#)

##### [自簽名證書續訂](#)

##### [手動證書續訂](#)

##### [PKCS12續訂](#)

#### [使用OpenSSL建立PKCS12](#)

### [驗證](#)

#### [檢視FMC中安裝的證書](#)

#### [在CLI中檢視已安裝的證書](#)

### [疑難排解](#)

#### [Debug指令](#)

#### [常見問題](#)

---

## 簡介

本檔案介紹如何在FMC管理的FTD上安裝、信任和續訂憑證。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 手動證書註冊需要訪問受信任的第三方CA。
- 第三方CA供應商的示例包括 ( 但不限於 ) Entrust、Geotrust、GoDaddy、Thawte和VeriSign。
- 驗證FTD的時鐘時間、日期和時區是否正確。透過憑證驗證，建議使用網路時間通訊協定(NTP)伺服器同步FTD上的時間。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行6.5的FMCv
- 執行6.5的FTDv
- 建立PKCS12時使用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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景

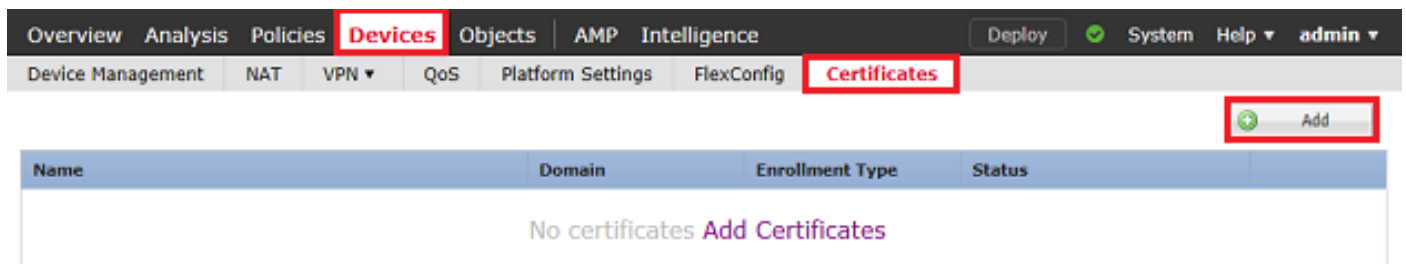
本文說明如何在Firepower管理中心(FMC)管理的Firepower威脅防禦(FTD)上安裝、信任和續訂由第三方證書頒發機構(CA)或內部CA簽名的自簽名證書和證書。

## 設定

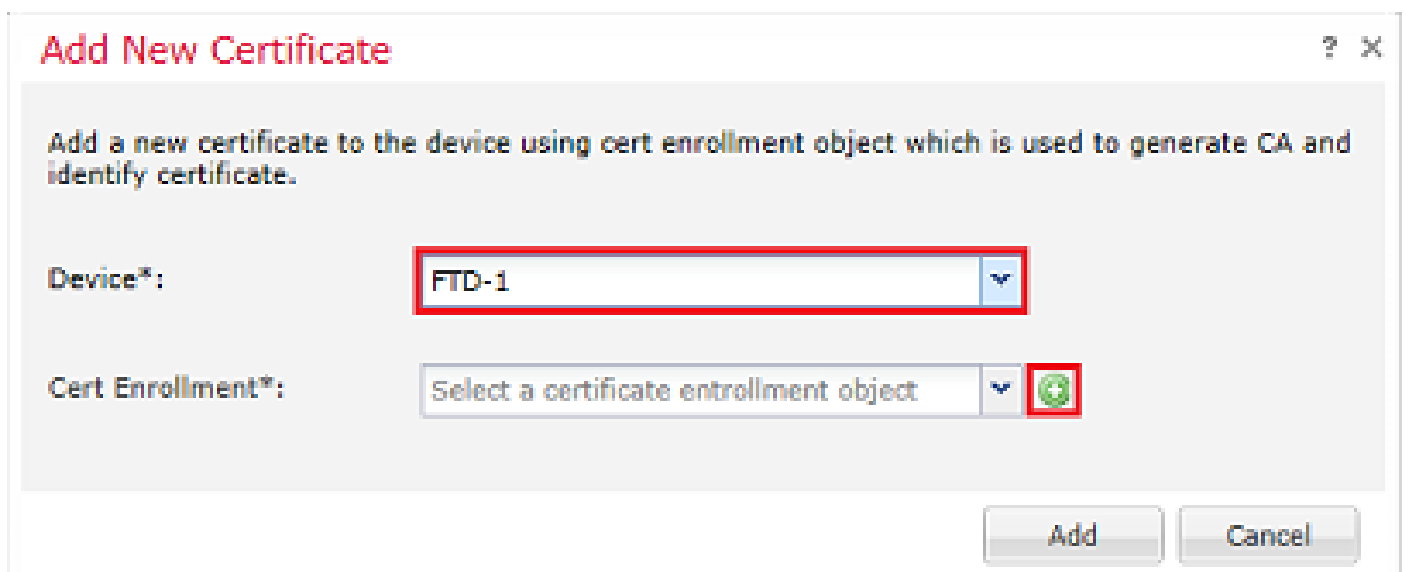
### 證書安裝

#### 自簽名註冊

1.導覽至Devices > Certificates，然後按一下Add，如下圖所示。



2.選擇裝置，並將證書新增到Device\*下拉列表中。然後按一下綠色+符號，如圖所示。



3.指定信任點的名稱，然後在「CA資訊」頁籤下，選擇「註冊型別：自簽名證書」，如下圖所示。

## Add Cert Enrollment



Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.

Allow Overrides

4.在「Certificate Parameters」頁籤下，輸入證書的公用名。此專案必須與使用憑證的服務的fqdn或IP位址相符，如下圖所示。

## Add Cert Enrollment



Name\*

Description

CA Information Certificate Parameters Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

5. (可選) 在Key索引標籤下，可以指定用於憑證的私鑰的型別、名稱和大小。預設情況下，金鑰使用名為<Default-RSA-Key>、大小為2048的RSA金鑰；但是，建議對每個證書使用唯一的名稱，以便它們不使用與圖中所示相同的專用/公共金鑰對。

## Add Cert Enrollment



Name\*

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:  RSA  ECDSA

Key Name:\*

Key Size:

**Advanced Settings**

Ignore IPsec Key Usage  
*Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.*

Allow Overrides

Save Cancel

6.完成後，按一下「Save」，然後按一下「Add」，如下圖所示。

### Add New Certificate ? ✕

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:  ▼

Cert Enrollment\*:  ▼ +

**Cert Enrollment Details:**

Name: FTD-1-Self-Signed

Enrollment Type: Self-Signed

SCEP URL: NA

Add Cancel

7.完成後，自簽名證書如下圖所示。

Overview Analysis Policies <b>Devices</b> Objects AMP Intelligence <span style="float: right;">Deploy System Help admin</span>			
Device Management NAT VPN QoS Platform Settings FlexConfig <b>Certificates</b>			
Add			
Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA ID

### 手動註冊

1.導覽至Devices > Certificates，然後按一下Add，如下圖所示。


Overview Analysis Policies <b>Devices</b> Objects AMP Intelligence <span style="float: right;">Deploy System Help admin</span>			
Device Management NAT VPN QoS Platform Settings FlexConfig <b>Certificates</b>			
Add			
Name	Domain	Enrollment Type	Status
No certificates <a href="#">Add Certificates</a>			

2.在Device\*下拉選單中，選擇證書新增到的裝置，然後按一下綠色+符號，如下圖所示。

### Add New Certificate ? X

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:  

3. 指定信任點的名稱，然後在「CA資訊」頁籤下選擇「註冊型別：手動」。輸入用於對身份證書進行簽名的CA的pem格式證書。如果此證書目前不可用或未知，請新增任何CA證書作為佔位符，在頒發身份證書後，重複此步驟以新增實際頒發的CA，如下圖所示。

### Add Cert Enrollment ? X

Name\*

Description

**CA Information** | Certificate Parameters | Key | Revocation

Enrollment Type:

CA Certificate:\* 

```
-----BEGIN CERTIFICATE-----
MIIESzCCAjOgAwIBAgIIItsWwBSsr5QwDQYJKoZIhvcNAQELBQAw
MjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUxhZDAsBgNVBAMTC1ZQTiBSb29
0IENBMB4XDTEw
MDQwNTIzMDQwNTIzMDQwNTIzMDQwNTIzMDQwNTIzMDQwNTIzMDQw
ChMRQ2lzY28gU3lzdGVtcyBUQUxhZDAsBgNVBAMTE1ZQTiBjb290IENB
wggEIMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCII/m7uyjRUoyjyob7sWS
AUVmnUMtovHen
9VbgjowZs0hVcigl/Lp2YyuawWRJhW99nagUBYtMyvY744sRw7AK
AwlyROO1J6IT
ls5suK60Yryz7JG3eNDqAroqJg/VeDeAjprpCW0YhHHYXAI0s7GXjHI
S6nGIy/qP
SRcPLdqx4/aFXw+DONJYTHLoESFlsfknrOeketnbABjkAkmOauNpS
zN4FAISIKd4
DU3yx7d31GD4BBhxI7IPsDH933AUM6zxntC9AxK6qHAY8/BpUPV
```

Allow Overrides

4.在「Certificate Parameters」頁籤下，輸入證書的公用名。此專案必須與使用憑證的服務的fqdn或IP位址相符，如下圖所示。

The screenshot shows a web-based configuration window titled "Add Cert Enrollment". At the top, there are fields for "Name\*" (containing "FTD-1-Manual") and "Description". Below these are four tabs: "CA Information", "Certificate Parameters", "Key", and "Revocation". The "Certificate Parameters" tab is active and contains several fields: "Include FQDN:" (a dropdown menu set to "Use Device Hostname as FQDN"), "Include Device's IP Address:" (empty), "Common Name (CN):" (containing "ftd1.example.com" and highlighted with a red border), "Organization Unit (OU):" (containing "Cisco Systems"), "Organization (O):" (containing "TAC"), "Locality (L):" (empty), "State (ST):" (empty), "Country Code (C):" (containing "Comma separated country codes"), and "Email (E):" (empty). There is also a checkbox for "Include Device's Serial Number" which is unchecked. At the bottom left, there is a checkbox for "Allow Overrides" which is also unchecked. At the bottom right, there are "Save" and "Cancel" buttons.

5. (可選) 在Key標籤下，可以選擇指定用於證書的私鑰的型別、名稱和大小。預設情況下，金鑰使用名為<Default-RSA-Key>、大小為2048的RSA金鑰；但是，建議對每個證書使用唯一的名稱，以便它們不使用如圖所示的相同私有/公共金鑰對。



## Add Cert Enrollment

? X

The screenshot shows the 'Add Cert Enrollment' dialog box with the 'Key' tab selected. The 'Name' field contains 'FTD-1-Manual'. The 'Description' field is empty. The 'Key Type' is set to 'RSA'. The 'Key Name' is '<Default-RSA-Key>'. The 'Key Size' is '2048'. The 'Advanced Settings' section is expanded, showing the 'Ignore IPsec Key Usage' checkbox, which is unchecked. The 'Allow Overrides' checkbox is also unchecked. The 'Save' and 'Cancel' buttons are visible at the bottom right.

Name\*

Description

CA Information Certificate Parameters **Key** Revocation

Key Type:  RSA  ECDSA

Key Name:\*

Key Size:

**Advanced Settings**

Ignore IPsec Key Usage  
*Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.*

Allow Overrides

Save Cancel

6. (可選) 在Revocation頁籤下，會檢查並且可以配置Certificate Revocation List(CRL)或Online Certificate Status Protocol(OCSP)Revocation。預設情況下，兩者均未勾選，如下圖所示。

## Add Cert Enrollment



Name\*

Description

CA Information Certificate Parameters Key **Revocation**

Enable Certificate Revocation Lists (CRL)

- Use CRL distribution point from the certificate
- User static URL configured

CRL Server URLs:\*

Enable Online Certificate Status Protocol (OCSP)

OCSP Server URL:

Consider the certificate valid if revocation information can not be reached

Allow Overrides

Save Cancel

7.完成後，按一下「Save」，然後按一下「Add」，如下圖所示。

### Add New Certificate ? X

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:  +

**Cert Enrollment Details:**

Name: FTD-1-Manual

Enrollment Type: Manual

SCEP URL: NA

8.處理請求後，FMC提供新增身份證書的選項。按一下「ID」按鈕，如下圖所示。

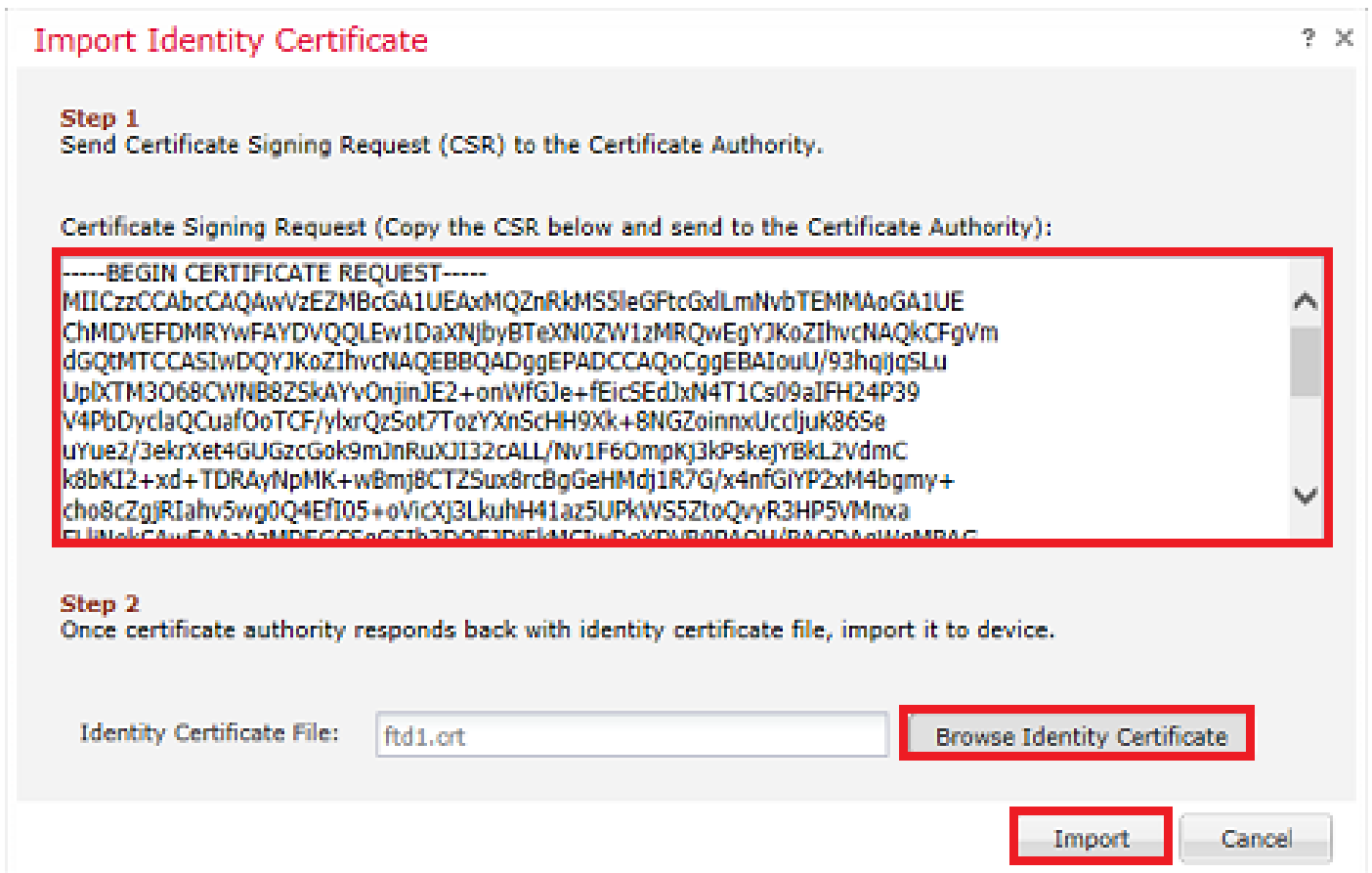
Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Manual	Global	Manual	<input type="button" value="CA"/> <input type="button" value="ID"/> <input type="button" value="Identity certificate import required"/>

9.彈出一個視窗，通知已生成CSR。按一下「Yes」，如下圖所示。

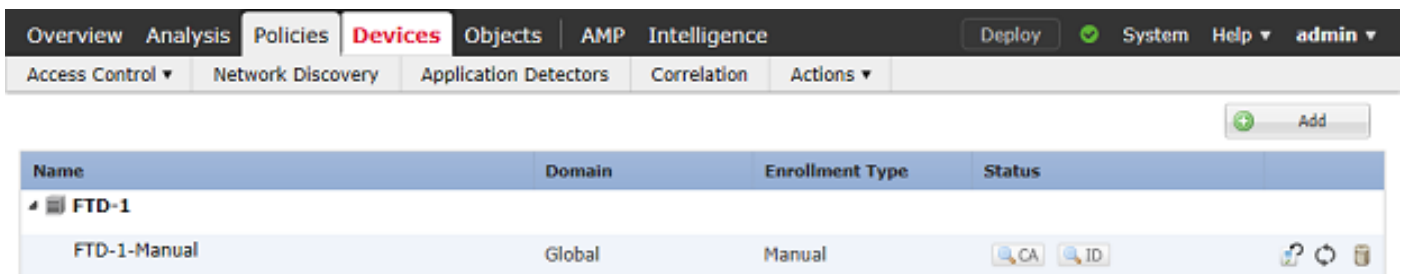
## Warning

This operation will generate Certificate Signing Request do you want to continue?

10.接下來，會產生CSR，您可以將其複製並傳送到CA。簽署CSR後，會提供身份證書。瀏覽到提供的身份證書並將其選中，然後按一下Import，如下圖所示。

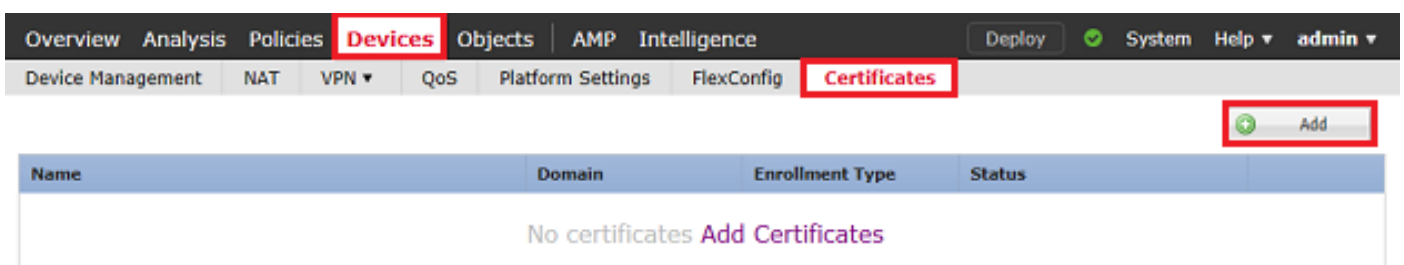


11. 手動證書一旦完成，如下圖所示。



## PKCS12註冊

1. 若要安裝已接收或已建立的PKCS12檔案，請導覽至Devices > Certificates，然後按一下Add，如下圖所示。




2. 在Device\*下拉選單中，選擇證書新增到的裝置，然後按一下綠色+符號，如下圖所示。

### Add New Certificate ? X

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:  

3. 指定信任點的名稱，然後在CA資訊頁籤下，選擇Enrollment Type: PKCS12 File。瀏覽到建立的PKCS12檔案並選擇它。輸入建立PKCS12時使用的密碼，如下圖所示。

### Add Cert Enrollment ? X

Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

PKCS12 File\*:

Passphrase:

Allow Overrides

4. (可選) Certificate Parameters和Key頁籤呈灰色顯示，因為它們是使用PKCS12建立的，但是

，可以修改啟用CRL和/或OCSP撤銷檢查的Revocation頁籤。預設情況下，兩者均未勾選，如下圖所示。

The screenshot shows a dialog box titled "Add Cert Enrollment" with a close button (X) in the top right corner. The dialog has four tabs: "CA Information", "Certificate Parameters", "Key", and "Revocation". The "Revocation" tab is selected and highlighted in blue. Below the tabs, there are several settings:

- Name\***: A text field containing "FTD-1-PKCS12".
- Description**: An empty text field with a refresh icon on the right.
- Enable Certificate Revocation Lists (CRL)**: An unchecked checkbox.
- Use CRL distribution point from the certificate**: A checked checkbox.
- User static URL configured**: An unchecked checkbox.
- CRL Server URLs:\***: A large empty text area with a green plus icon on the right.
- Enable Online Certificate Status Protocol (OCSP)**: An unchecked checkbox.
- OCSP Server URL:**: A text field containing "Gets OCSP URL from certificate if not provided".
- Consider the certificate valid if revocation information can not be reached**: A checked checkbox.
- Allow Overrides**: An unchecked checkbox.

At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

5.完成後，按一下Save，然後按一下Add，即可進入此視窗，如下圖所示。

### Add New Certificate ? X

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:  +

**Cert Enrollment Details:**

Name: FTD-1-PKCS12

Enrollment Type: PKCS12 file

SCEP URL: NA

6.完成後，PKCS12證書如下圖所示。

Overview Analysis Policies <b>Devices</b> Objects AMP Intelligence <span style="float: right;">Deploy System Help admin</span>			
Device Management NAT VPN QoS Platform Settings FlexConfig <b>Certificates</b>			
Add			
Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID

## 證書續訂

### 自簽名證書續訂

1.按「Re-enroll certificate」按鈕，如下圖所示。

Overview Analysis Policies <b>Devices</b> Objects AMP Intelligence <span style="float: right;">Deploy System Help admin</span>			
Device Management NAT VPN QoS Platform Settings FlexConfig <b>Certificates</b>			
Add			
Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA ID <span style="border: 1px solid red; padding: 2px;">Re-enroll</span>

2.出現一個視窗，提示已移除並替換自簽名證書。按一下「Yes」，如下圖所示。

## Warning



Re-enrolling the certificate will clear the existing certificate from the device and install the certificate again.

Are you sure, you want to re-enroll the certificate?

Yes

No

3.重新簽署後，系統會將使用者推送至未來發展中心。按一下ID按鈕並選中「Valid time (有效時間)」可以驗證這一點。

### 手動證書續訂

1.按「Re-enroll certificate」按鈕，如下圖所示。

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Manual	Global	Manual	CA ID

2.出現一個視窗，提示生成證書簽名請求。按一下「Yes」，如下圖所示。

## Warning



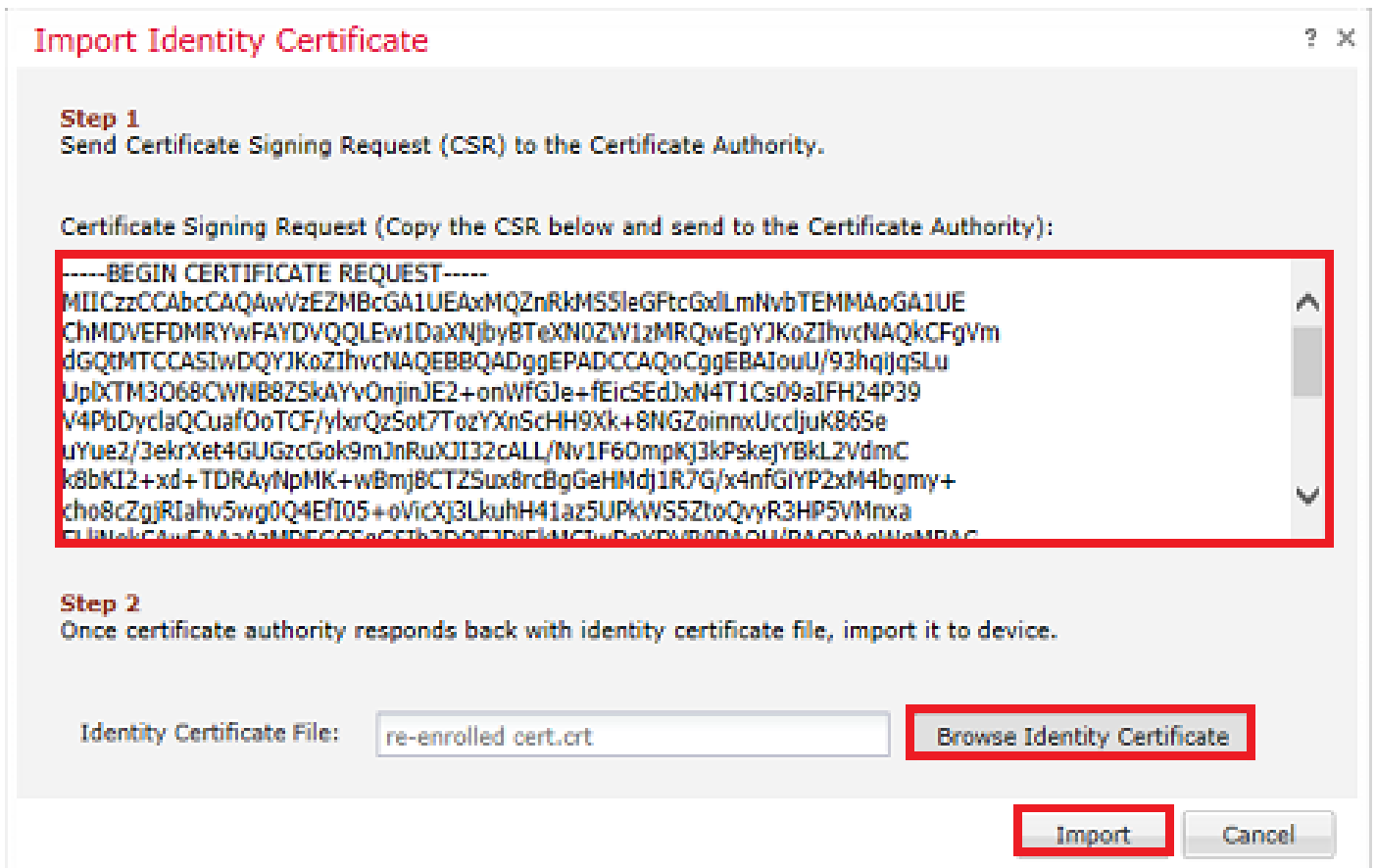
This operation will generate Certificate Signing Request do you want to continue?

Yes

No

3.在此視窗中，生成一個CSR，它可以複製並傳送到之前簽署身份證書的同一CA。簽署CSR後，會提供續訂的身分識別憑證。瀏覽到提供的身份證書並將其選中，然後按一下Import，如下圖所示。





4.續訂的手動憑證會被推送到FTD。按一下ID按鈕並選中「Valid time (有效時間)」可以驗證這一點。

## PKCS12續訂

如果按一下「重新註冊證書」按鈕，則不會續訂證書。為了更新PKCS12，需要使用前面提到的方法建立和上傳新的PKCS12檔案。

## 使用OpenSSL建立PKCS12

1.使用OpenSSL或類似應用程式，產生私鑰和憑證簽署請求(CSR)。此範例顯示名為private.key的2048位RSA金鑰和在OpenSSL中建立的名為ftd1.csr的CSR:

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd1.csr
Generating a 2048 bit RSA private key
.....+++
.....+++
written to a new private key to 'private.key'
-----
You are about to be asked to enter information that is incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', the field is left blank.
-----
Country Name (2 letter code) [AU]:.
```

State or Province Name (full name) [Some-State]:.  
Locality Name (eg, city) []:.  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems  
Organizational Unit Name (eg, section) []:TAC  
Common Name (e.g. server FQDN or YOUR name) []:ftd1.example.com  
Email Address []:.

Please enter these 'extra' attributes  
to be sent with your certificate request  
A challenge password []:  
An optional company name []:

2.複製產生的CSR，並將其傳送到CA。簽署CSR後，會提供身份證書。通常也會提供CA憑證。要建立PKCS12，請在OpenSSL中運行以下命令之一：

若要僅包括在PKCS12中頒發的CA證書，請使用以下命令：

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -certfile ca.crt  
Enter Export Password: *****  
Verifying - Enter Export Password: *****
```

- ftd.pfx是由openssl匯出的pkcs12檔案的名稱（格式為der）。
- ftd.crt是CA以pem格式簽發的已簽名身份證書的名稱。
- private.key是在步驟1中建立的金鑰對。
- ca.crt是證書頒發機構的證書，採用pem格式。

如果證書是包含根CA和1個或多個中間CA的鏈的一部分，則可以使用以下命令在PKCS12中新增完整的鏈：

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -chain -CAfile cachain.pem  
Enter Export Password: *****  
Verifying - Enter Export Password: *****
```

- ftd.pfx是由OpenSSL匯出的pkcs12檔案的名稱（格式為der）。
- ftd.crt是CA以pem格式簽發的已簽名身份證書的名稱。
- private.key是在步驟1中建立的金鑰對。
- cachain.pem是一個檔案，其中包含鏈中的CA證書，該檔案以頒發中間CA開頭，以pem格式以根CA結尾。

如果返回PKCS7檔案(.p7b，.p7c)，則這些命令還可用於建立PKCS12。如果p7b採用der格式，請確保將-inform der新增到引數中，否則不要包括：

```
openssl pkcs7 -in ftd.p7b -inform der -print_certs -out ftdpem.crt
```

```
openssl pkcs12 -export -in ftdpem.crt -inkey private.key -out ftd.pfx
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

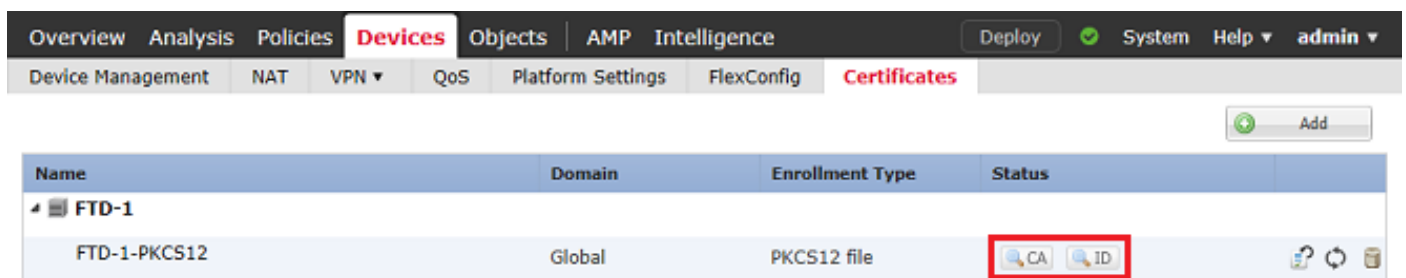
- ftd.p7b是CA傳回的PKCS7，其中包含簽名的身分憑證和CA鏈結。
- ftdpem.crt是已轉換的p7b檔案。
- ftd.pfx是由OpenSSL匯出的pkcs12檔案的名稱 ( 格式為der ) 。
- private.key是在步驟1中建立的金鑰對。

## 驗證

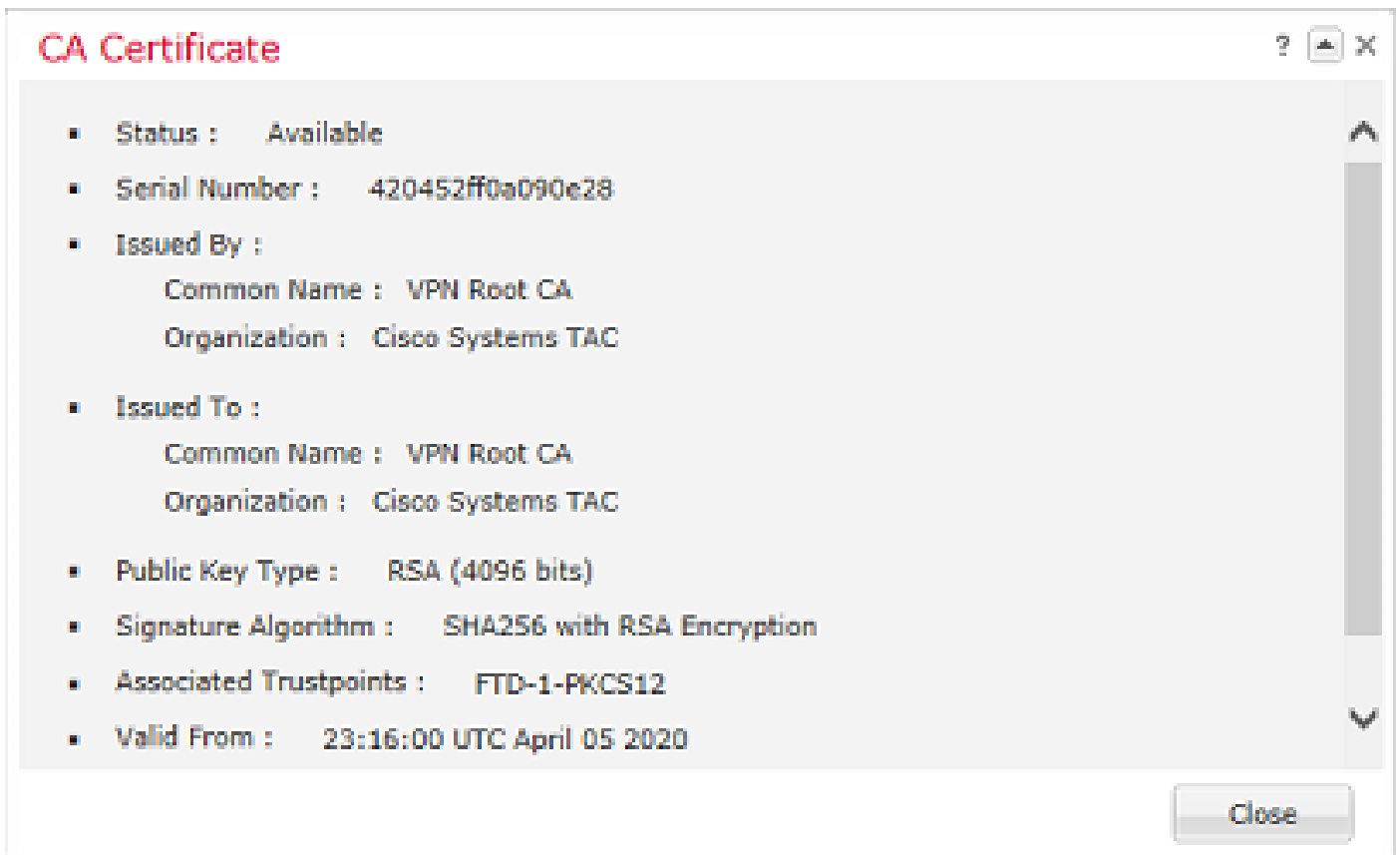
使用本節內容，確認您的組態是否正常運作。

### 檢視FMC中安裝的證書

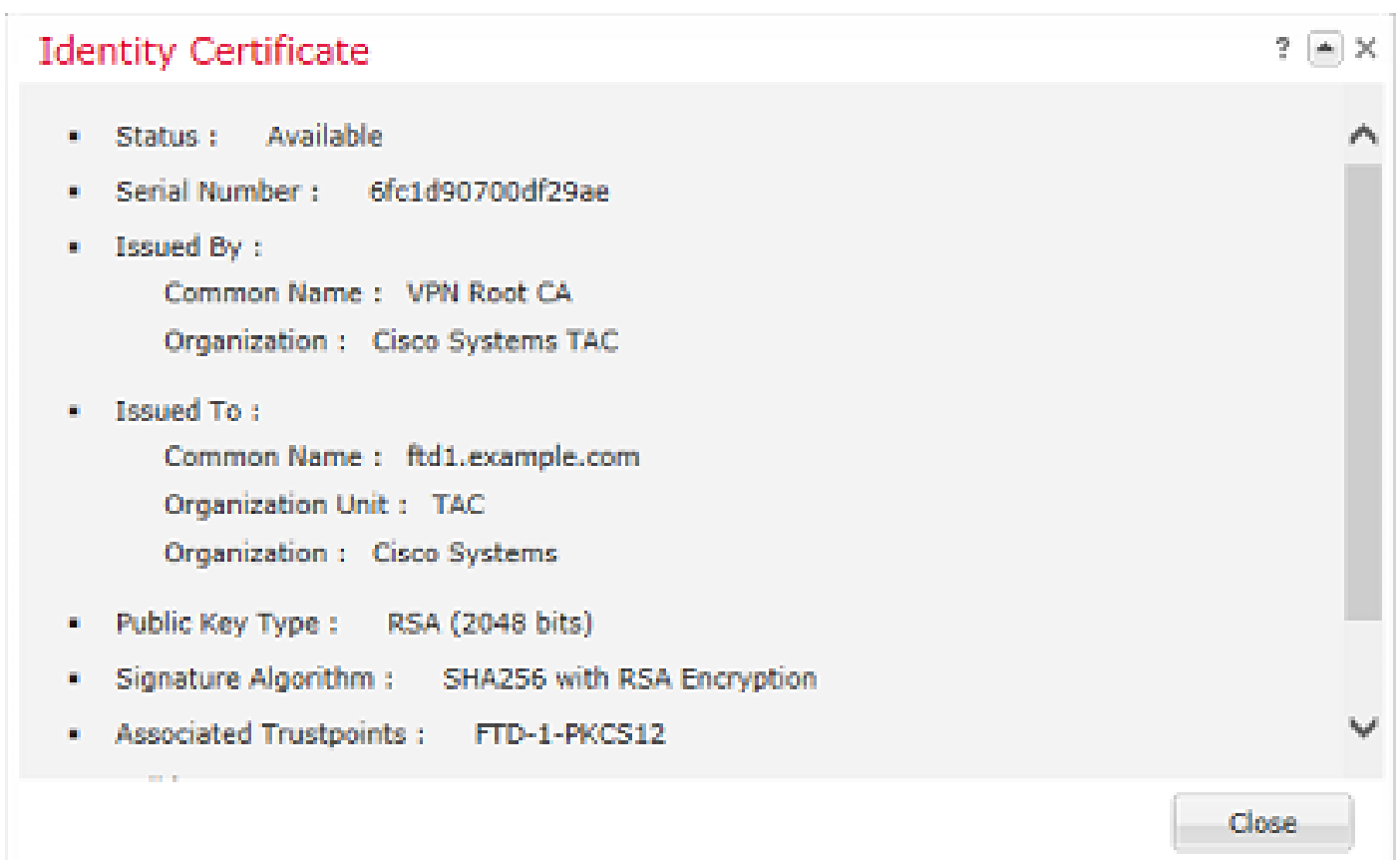
在FMC中，導覽至Devices > Certificates。有關相關信任點，請點選CA或ID以檢視證書的更多詳細資訊，如下圖所示。



如圖所示驗證CA憑證。



如圖所示驗證身份證書。



在CLI中檢視已安裝的證書

使用SSH連線到FTD，然後輸入命令show crypto ca certificate。

```
> show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 6fc1d90700df29ae
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Subject Name:
    cn=ftd1.example.com
    ou=TAC
    o=Cisco Systems
  Validity Date:
    start date: 15:47:00 UTC Apr 8 2020
    end date: 15:47:00 UTC Apr 8 2021
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12
```

```
CA Certificate
  Status: Available
  Certificate Serial Number: 420452ff0a090e28
  Certificate Usage: General Purpose
  Public Key Type: RSA (4096 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Subject Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Validity Date:
    start date: 23:16:00 UTC Apr 5 2020
    end date: 23:16:00 UTC Apr 5 2030
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12
```

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

### Debug指令

如果SSL證書安裝失敗，則FTD透過SSH連線後，可以從診斷CLI運行調試：

```
debug crypto ca 14
```

在舊版FTD中，以下偵錯功能可用且建議用於疑難排解：

```
debug crypto ca 255
```

debug crypto ca message 255

debug crypto ca transaction 255

## 常見問題

匯入已頒發的身份證書後，仍會看到消息「需要匯入身份證書」。

出現這種情況可能是由於兩個不同的問題：

### 1. 手動註冊時未新增頒發的CA證書

匯入身份證書後，系統將根據手動註冊時在「CA資訊」頁籤下新增的CA證書檢查該證書。有時，網路管理員沒有用於簽署其身份證書的CA的CA證書。在這種情況下，當您進行手動註冊時，必須新增佔位符CA證書。一旦簽發了身份證書並且提供了CA證書，就可以使用正確的CA證書進行新的手動註冊。再次完成手動註冊嚮導時，請確保為金鑰對指定與原始手動註冊中相同的名稱和大小。完成後，不再將CSR重新轉送到CA，而是可以將先前頒發的身分憑證匯入到新建立的信任點，且此信任點具有正確的CA憑證。

要檢查在手動註冊時是否應用了相同的CA證書，請按一下「驗證」部分中指定的CA按鈕，或檢查show crypto ca certificates的輸出。「Issued to」和「Serial Number」等欄位可與證書頒發機構提供的CA證書中的欄位進行比較。

### 2. 所建立信任點中的金鑰對不同於為已頒發證書建立CSR時使用的金鑰對。

透過手動註冊，在產生金鑰配對和CSR時，公鑰會新增到CSR，以便可以包含到核發的身分憑證中。如果由於某些原因修改了FTD上的金鑰對，或頒發的身分憑證包含不同的公鑰，則FTD不會安裝頒發的身分憑證。若要檢查是否發生這種情況，有兩種不同的測試：

在OpenSSL中，可以核發以下命令，以將CSR中的公鑰與核發憑證中的公鑰進行比較：

```
openssl req -noout -modulus -in ftd.csr
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B
B966DA10BF24771CFE55327C5A14B96235E9
```

```
openssl x509 -noout -modulus -in id.crt
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B
B966DA10BF24771CFE55327C5A14B96235E9
```

- ftd.csr是手動註冊時從FMC複製的CSR。
- id.crt是CA簽名的身份證書。

或者，FTD上的公鑰值也可以與核發的身分憑證中的公鑰進行比較。請注意，由於進行填充，憑證

中的第一個字元與FTD輸出中的字元不匹配：

已在Windows PC上開啟頒發的身份證書：

Certificate

General Details Certification Path

Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	VPN Intermediate CA, Cisco S...
Valid from	Wednesday, April 8, 2020 1:0...
Valid to	Monday, April 5, 2021 7:29:00...
Subject	ftd-1, Cisco Systems, TAC, ftd...
Public key	RSA (2048 Bits)
Public key parameters	05 00

```
ec 91 e8 d8 06 42 f6 55 d9 82 93 c6 ca 23
6f b1 77 e4 c3 44 0c 8d a4 c2 be c0 19 a3
f0 24 d9 4a ec 7c ad c0 60 19 e1 cc 76 3d
51 ec 6f f1 e2 77 c6 89 83 f6 c4 ce 1b 82
6c be 72 1a 3c 71 98 23 44 86 a1 bf 9c 20
d1 0e 04 7c 8d 39 fa 85 62 71 78 f7 2e 4b
a1 1f 8d 5a cf 95 0f 91 64 b9 66 da 10 bf
24 77 1c fe 55 32 7c 5a 14 b9 62 35 e9 02
03 01 00 01
```

Edit Properties... Copy to File...

OK

從身份證書提取的公鑰輸出：

```
3082010a02820101008a2e53ff7786a8a3a922ee5299574ccdceebc096341f194a4018bce9e38a7244dbea2759f1897be7c489c
f6e0fdfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b8af3a49
1b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8da4c2bec
e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f8d5acf9
55327c5a14b96235e90203010001
```

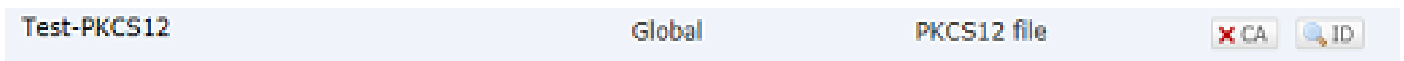
Show crypto key mypubkey rsa output from the FTD。完成手動註冊後，<Default-RSA-Key>用於建立CSR。加粗部分與從身份證書提取的公鑰輸出相匹配。

```
> show crypto key mypubkey rsa
Key pair was generated at: 16:58:44 UTC Jan 25 2019
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 2048
Storage: config
Key Data:
```

```
30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
008a2e53 ff7786a8 a3a922ee 5299574c cdceebc0 96341f19 4a4018bc e9e38a72
44dbea27 59f1897b e7c489c4 84749c4d e13d42b3 4f5a2051 f6e0fdfd 5783db0f
27256900 ae69f3a8 4c217fca 5c6b4334 a8b7b4e8 cd85e749 c1c7f579 3ef0d199
a229e7c5 471c963b 8af3a49e b98b9edb fdde92b5 deb78194 1b3706a2 4f662674
6e5c9237 d9c00b2f f36fd45e 8e9a92a3 de43ec91 e8d80642 f655d982 93c6ca23
6fb177e4 c3440c8d a4c2bec0 19a3f024 d94aec7c adc06019 e1cc763d 51ec6ff1
e277c689 83f6c4ce 1b826cbe 721a3c71 98234486 a1bf9c20 d10e047c 8d39fa85
627178f7 2e4ba11f 8d5acf95 0f9164b9 66da10bf 24771cfe 55327c5a 14b96235
e9020301 0001
```

FMC中CA旁邊的紅色X

PKCS12註冊時可能會發生這種情況，因為CA證書沒有包含在PKCS12軟體包中。



要解決此問題，PKCS12需要新增CA證書。

核發以下命令，以便提取身份證書和私鑰。需要建立PKCS12時使用的密碼和安全私鑰：

```
openssl pkcs12 -info -in test.p12
Enter Import Password: [pkcs12 pass phrase here]
MAC Iteration 1
MAC verified OK
PKCS7 Encrypted data: pbewithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    friendlyName: Test
```



```
localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
subject=/CN=ftd1.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Intermediate CA
-----BEGIN CERTIFICATE-----
MIIC+TCCAeGgAwIBAgIIAUIM3+3IMhIwDQYJKoZIhvcNAQELBQAwOjEaMBGGA1UE
ChMRQ2l2Y28gU3lzdGVtcyBUQUUMxHDAaBgNVBAMTE1ZQTiBJbnR1cm1lZG1hdGUG
Q0EwHhcNMjAwNDA0MTY1ODAwWhcNMjEwNDA1MjMyOTAwWjAbMRkwFwYDVQQDExBm
dGQxLmV4Yw1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
043eLVP18K0jnYfHCBZuFUyRXTTB28Z1ouIJ5yyrDzCN781GFrHb/wCczRx/jW4n
pF9q2z7FHr5bQCI4oSUSX40UQfr0/uOK5riI1uZuMPuX1Vp1zVkyuqDd/i1r0+0j
PyS7BmyGfV7aebYWZnr8R9ebDsnC2U3nKjP5RaE/wNdVGTs/180H1rIjMpcFMXps
LwxixiEz0hCmDm9RC+7uWZQd1wZ9oNANCBQC0px/Zikj9Dz70RhhbzBTuNKD3p
sN3VqdDPvGZHFGLPcnhKYyZ79+6p+CHC8X8BFjuTJYoo116uGgiB4Jz2Y9ZeFSQz
Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBg1ghkgBhvCAQ0EERYPeGnhIGN1
cnRpZm1jYXR1MA0GCsQGSiB3DQEBcUAA4IBAQCv/MgshWxXtwpwmMF/6KqEj8nB
S1jbfz1zNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRY54taRI27W+gLneCbQAux
9amxXuhpxP5E0hnc+tsY9eriAKpHuS1Y/2uwn92FHIb3HEXPO1HBJueI8PH3ZK
41rPKA9oIQPUW/uueHEF+xCbG4xCLi5H0GeHX+FTigGNqazaX5GM4RBUa4bk8jks
Ig53twvop71wE53COTH0EkSRCsVcW5mdJsd9BUZHjguhpw8Giv7Z36qWv18I/Owf
RhLhtsgenc25udglv9S5yXK53a5Ieg8biRpWL9tIjgUgjxYZwtyVeHi32S7
-----END CERTIFICATE-----
```

PKCS7 Data

Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048

Bag Attributes

friendlyName: Test

localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2

Key Attributes: <No Attributes>

Enter PEM pass phrase: [private-key pass phrase here]

Verifying - Enter PEM pass phrase: [private-key pass phrase here]

-----BEGIN ENCRYPTED PRIVATE KEY-----

```
MIIFDjBAbGkqhkiG9w0BBQ0wMzAbGkqhkiG9w0BBQwwDgQI1KyWxk8cgTMCaggA
MBQGcCqGSiB3DQMhBAgCm0qRKh/dcwSCBmiF7BpgJNIPhdU5Zorn1jm3pmsI/XkJ
MRHc1Ree10ziSLCZOSTr84JFQxNpbThXLhsHC9WhpPy5sNXIvXS7Gu+U10/V1NSA
rW1X6SPftAYiFq5QxyEutSHdZZwgQIqpj97seu3Px0agvI0bw1Lo8or51SydnMjp
Ptv50Ko95BSHwWycqkTAia4ZKxytyIc/mIu5m72LucOFmoRB05JZu1avWXjbCAA+
k2ebkb1FT0YRQT1Z4tZHSqX1LFPZe170NZEUG7rIcWak1Yw7XNUPhOn6FHL/ieIZ
IhvIfj+IgQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E
Gnh8r31903A1kPMBkMdx0q1pzo2naIy2KGrUnOSHajVwclR9dTPWIDyjd95YoeS
IUE7Ma00pjJc02FNbWyxNrxRyt+4hp3aJt0ZW83FHiS1B5UIzGrBMAgKJc2Hb2RTV
9gxZGve1cRco1LeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShn0wHzridF8Zn
F06XvBDSyXVSpkxwAd1Twxq62tUnLIkyRXo2CSz8z8W29UxmF04o3G67n28//LJ
Ku8wj1jeq1vFgXSQiWLADNH772RNwzCMeobfxG1BprF9DPT8yvyBdQviUIuFpJ
nNs5FYbLTv9ygZ1S9xwQpTcqEu+y4F5BJuYLMHqcZ+VpFA4nM0YHhZ5M3sccRSR4
1L+a3BPJJsh1TIJQg0TixDaveCfpDcpS+ydUgS6WY8xw17v0+1f7y5z1t4TkZrt
ItBHHA6yDzR0Cn0/ZH3y88a/asDcuKw6bsRaY5i78nAWGTQVed3xXj+EgeRs25HB
dIBBX5gTvqN7qDanhkaPucEawj1/38M0pAYULEi3e1fKKrhwAySBFaV/BeUMWuNW
BmKprkKKQv/JdWnoJ149KcS4bfa3GHG9Xxnyvbg8HxopcYFMTEjao+wLZH9agqKe
Y0jyoHFN6ccBBC7vn7u12tmXOM5RcnPLmaDaBFDSBBFS8Y8VkeHn3P0q7+sEQ26d
vL807WdgLH/wKqovoJRyxwzz+TryRq9cd5BNyyLaABESa1sWRhk81C2P+B+Jdg9w
d6RsvJ2dt3pd1/+pUR3CdC0b8qRZOoL03+onUIUoEsCCNDp0x8Yj/mvc6ReXtOKB
2qVmhVMYseiU1rOaQGT7XMe1UuiJ+dRnqcfAfbDGeOp+6epm1TK1BJL2mA1QWx51
73Qo4M7rR71aeq/dqob3o1PhcoMLa5z/Lo5vDe7S+LZMuAwjRksfsoKQOY3kAP1
eZ2Eh2go4eJ7hHf5VFqBLL8Ci3rd3EOijRkNm3fAQmFJ1aFmooBM3Y2Ba+U8cMTH
1gjSFk11FAWpfx9aSEECNCvEMm1Ghm6/tJDLV1jyTqWajHnWIZCc+P2AXgn1LzG
HVvfxs0c8FGUJJPQHatXYd7worWCxszaufJ99E4PaoZnAOYUFW2jaZEwo0NBpbD1
AjQ8aciuosv0FKpp/jXDI78/aYAEk662tPsfGmxvAWB+UMFarA9ZTiihK3x/tDPy
GZ6ByGWJYp/0tNNmJRCFhcAYY83EtzHK9h+8LatFA6WrJ4j3dhceUPzrPXjMffNN
0Yg=
```

-----END ENCRYPTED PRIVATE KEY-----

完成之後，可以使用使用OpenSSL建立PKCS12的步驟2.中提到的步驟，將身份證書和私鑰放入單獨的文件，並且CA證書可以匯入到新的PKCS12檔案中。

## 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）。