在FDM管理的FTD上安裝及更新憑證

目錄

簡介

本檔案介紹如何在FTD上安裝、信任及更新由第三方CA或內部CA簽署的自我簽署憑證和憑證。

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證書頒發機構(CA)。第三方CA供應商的示例包括但不限於Entrust、Geotrust、GoDaddy、Thawte和VeriSign。
- 確認Firepower威脅防禦(FTD)具有正確的時鐘時間、日期和時區。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：

- 執行6.5的FTDv。

- 建立金鑰配對和憑證簽署請求(CSR)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。

設定

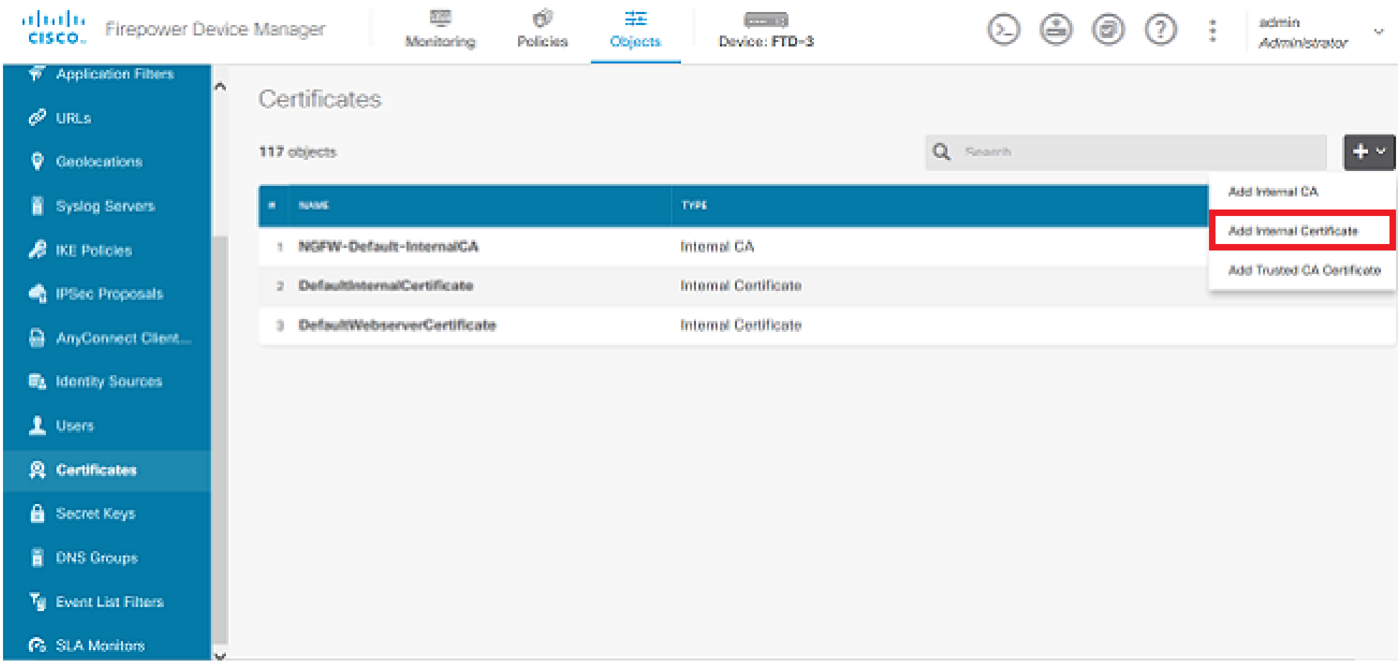
憑證安裝

自簽名註冊

自簽名證書是一種將適當欄位增加到FTD裝置的簡單證書獲取方法。雖然在大多數地方無法信任它們，但它們仍可提供與第三方簽名證書類似的加密優勢。建議使用受信任CA簽署的憑證，以便使用者和其他裝置能夠信任FTD提供的憑證。

註：Firepower裝置管理(FDM)具有名為DefaultInternalCertificate的預設自簽名證書，可用於類似用途。

1. 導航到對象>證書。點選+符號，然後選擇Add Internal Certificate，如下圖所示。

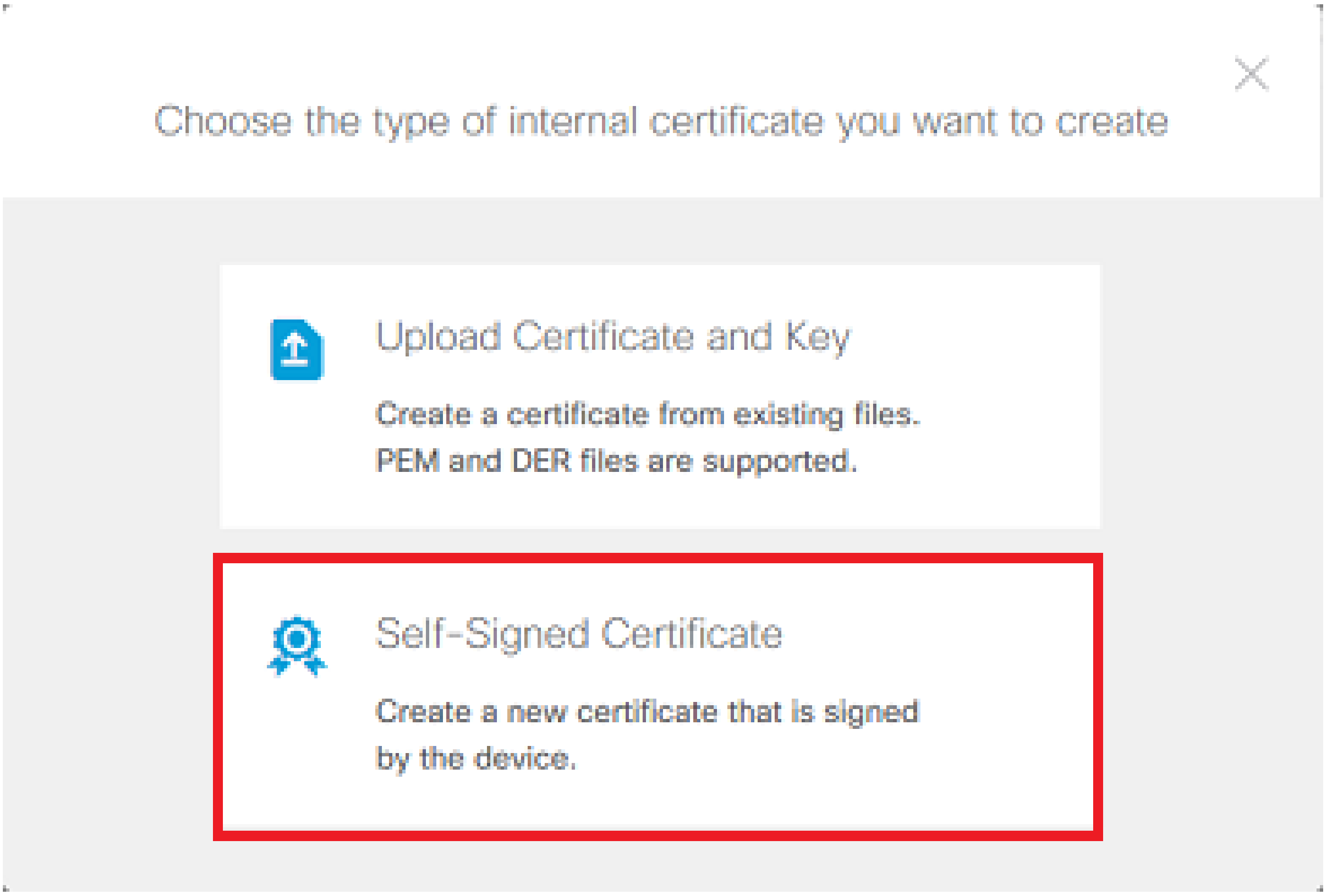


Certificates

117 objects

#	NAME	TYPE
1	NGFW-Default-InternalCA	Internal CA
2	DefaultInternalCertificate	Internal Certificate
3	DefaultWebserverCertificate	Internal Certificate

2. 在彈出窗口中選擇自簽名證書，如圖所示。



Choose the type of internal certificate you want to create

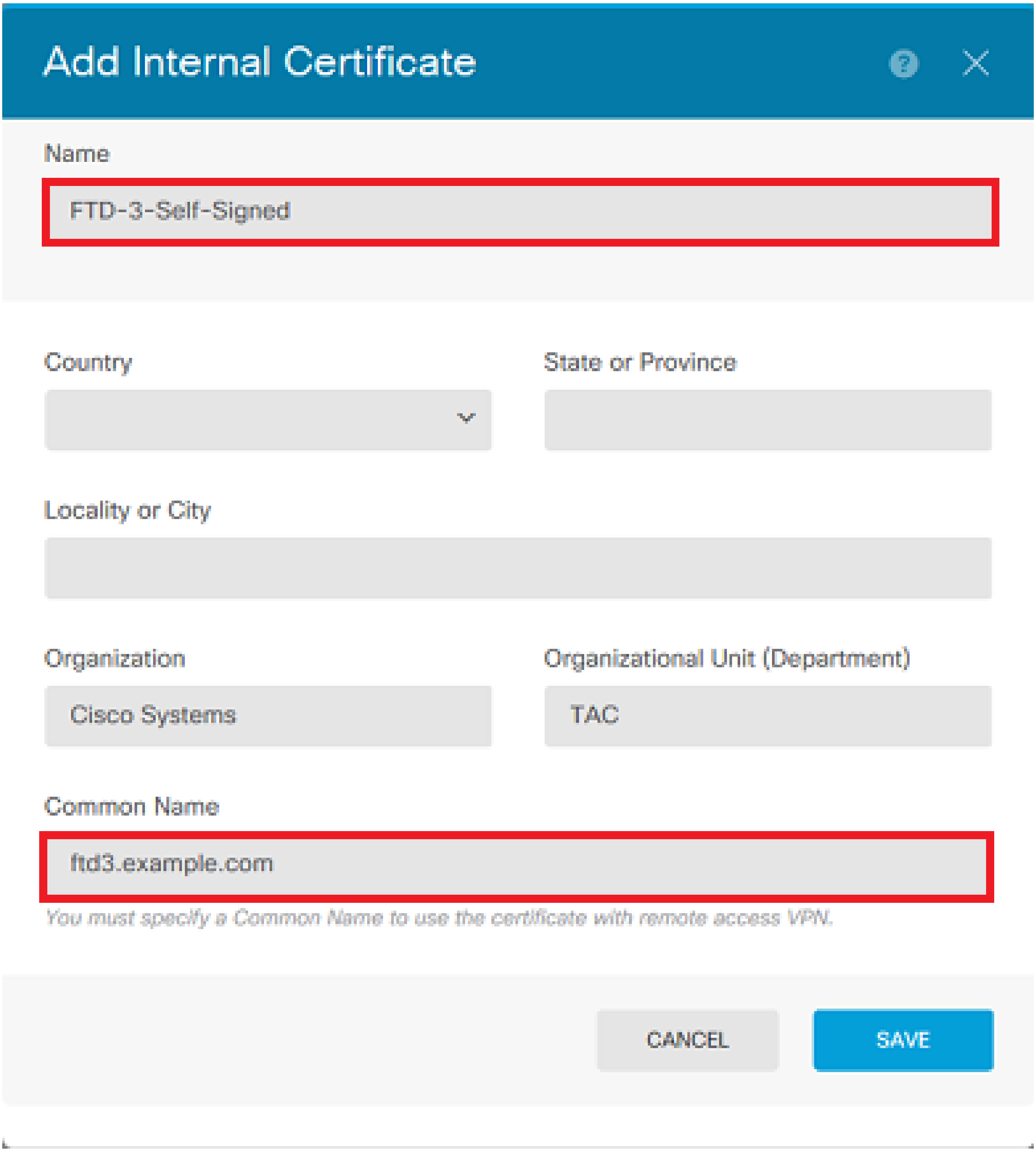
Upload Certificate and Key

Create a certificate from existing files. PEM and DER files are supported.

Self-Signed Certificate

Create a new certificate that is signed by the device.

3. 為信任點指定Name，然後填寫主題可分辨名稱欄位。至少可以增加公用名欄位。這可以與使用憑證的服務的完整網域名稱(FQDN)或IP位址相符。 完成後，請按一下Save（如圖所示）。



Add Internal Certificate

Name

FTD-3-Self-Signed

Country

State or Province

Locality or City

Organization

Cisco Systems

Organizational Unit (Department)

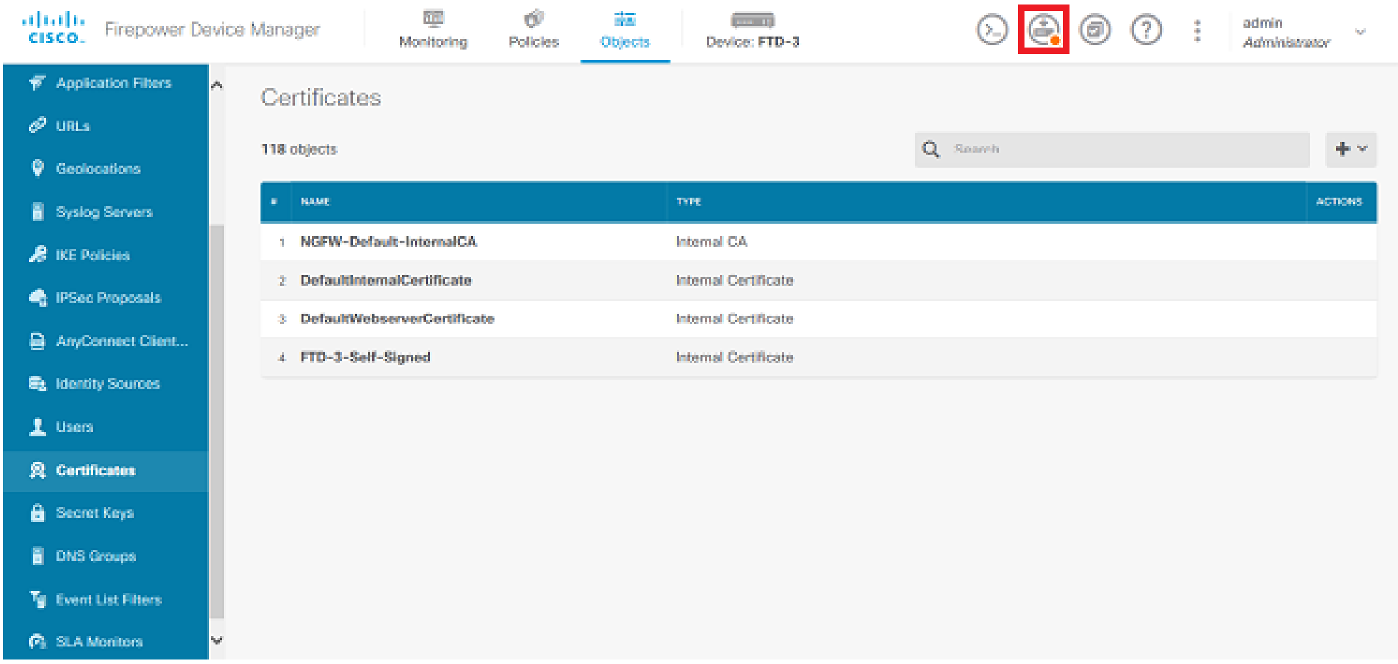
TAC

Common Name

ftd3.example.com

You must specify a Common Name to use the certificate with remote access VPN.

4. 按一下螢幕右上方的待定更改按鈕，如圖所示。

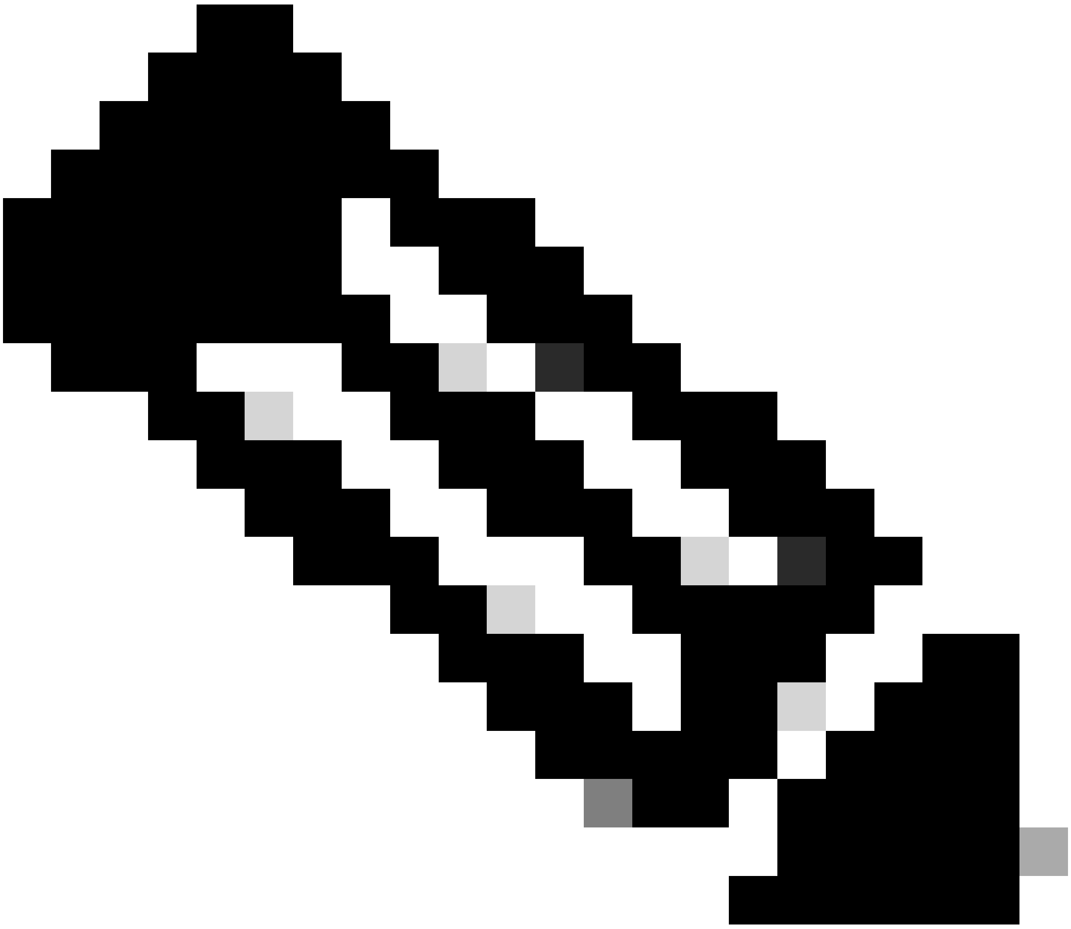


Certificates

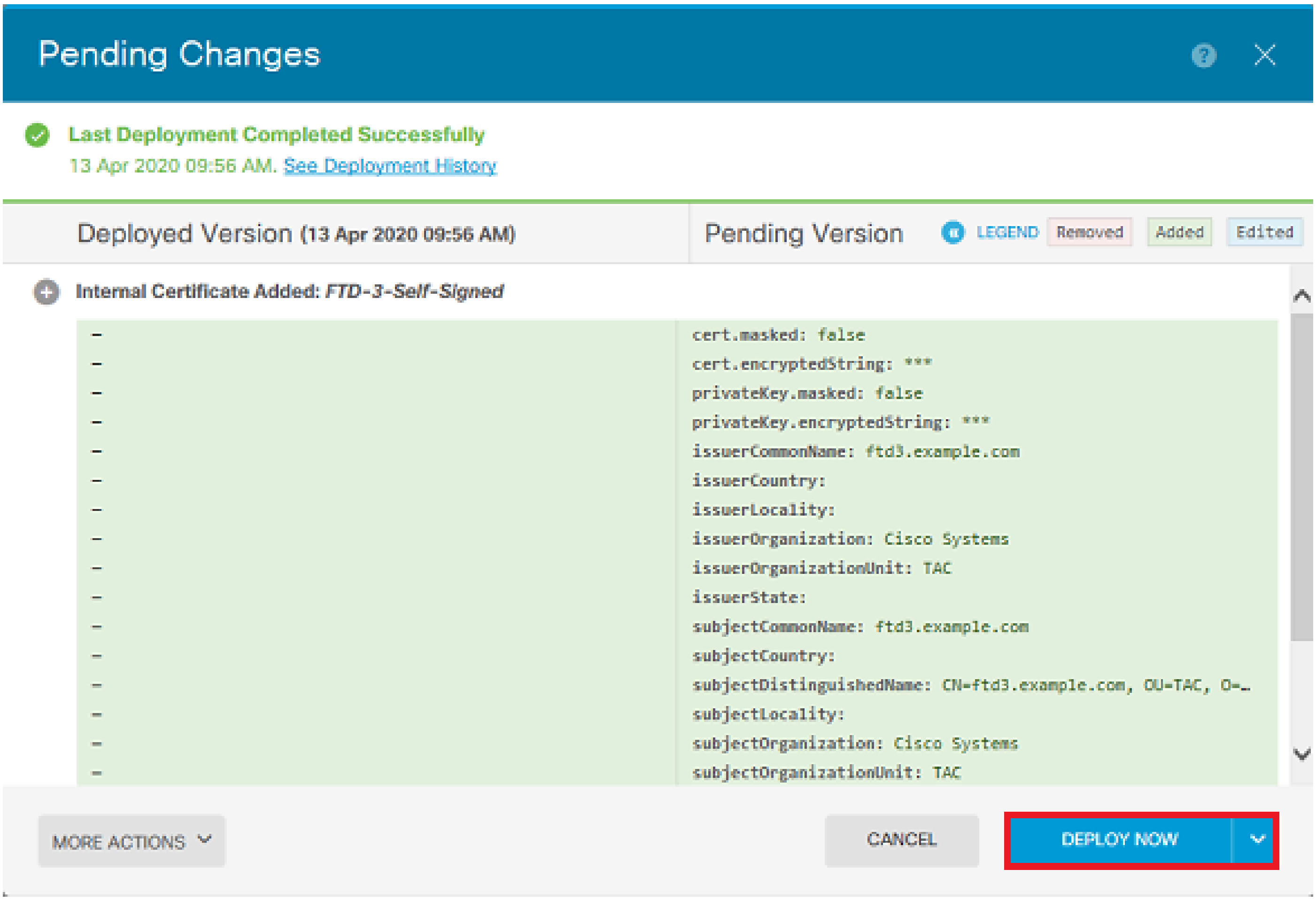
118 objects

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Self-Signed	Internal Certificate	

5. 按一下Deploy Now按鈕。



注意：完成部署後，在存在使用證書的服務（如AnyConnect）之前，無法在CLI中看到證書，如圖所示。


Pending Changes
Last Deployment Completed Successfully
13 Apr 2020 09:56 AM. See Deployment History
Deployed Version (13 Apr 2020 09:56 AM)
Pending Version
LEGEND
Removed
Added
Edited
MORE ACTIONS
CANCEL
DEPLOY NOW

Internal Certificate Added: *FTD-3-Self-Signed*

```
cert.masked: false
cert.encryptedString: ***
privateKey.masked: false
privateKey.encryptedString: ***
issuerCommonName: ftd3.example.com
issuerCountry:
issuerLocality:
issuerOrganization: Cisco Systems
issuerOrganizationUnit: TAC
issuerState:
subjectCommonName: ftd3.example.com
subjectCountry:
subjectDistinguishedName: CN=ftd3.example.com, OU=TAC, O=…
subjectLocality:
subjectOrganization: Cisco Systems
subjectOrganizationUnit: TAC
```

手動註冊

手動註冊可用於安裝受信任CA頒發的證書。OpenSSL或類似工具可用於生成接收CA簽名證書所需的私鑰和CSR。以下步驟包含產生私密金鑰和CSR的常用OpenSSL指令，以及在取得憑證和私密金鑰後安裝憑證的步驟。

1. 使用OpenSSL或類似應用程式，產生私密金鑰和憑證簽署請求(CSR)。此範例顯示名為private.key的2048位元RSA金鑰和在OpenSSL中建立的名為ftd3.csr的CSR。

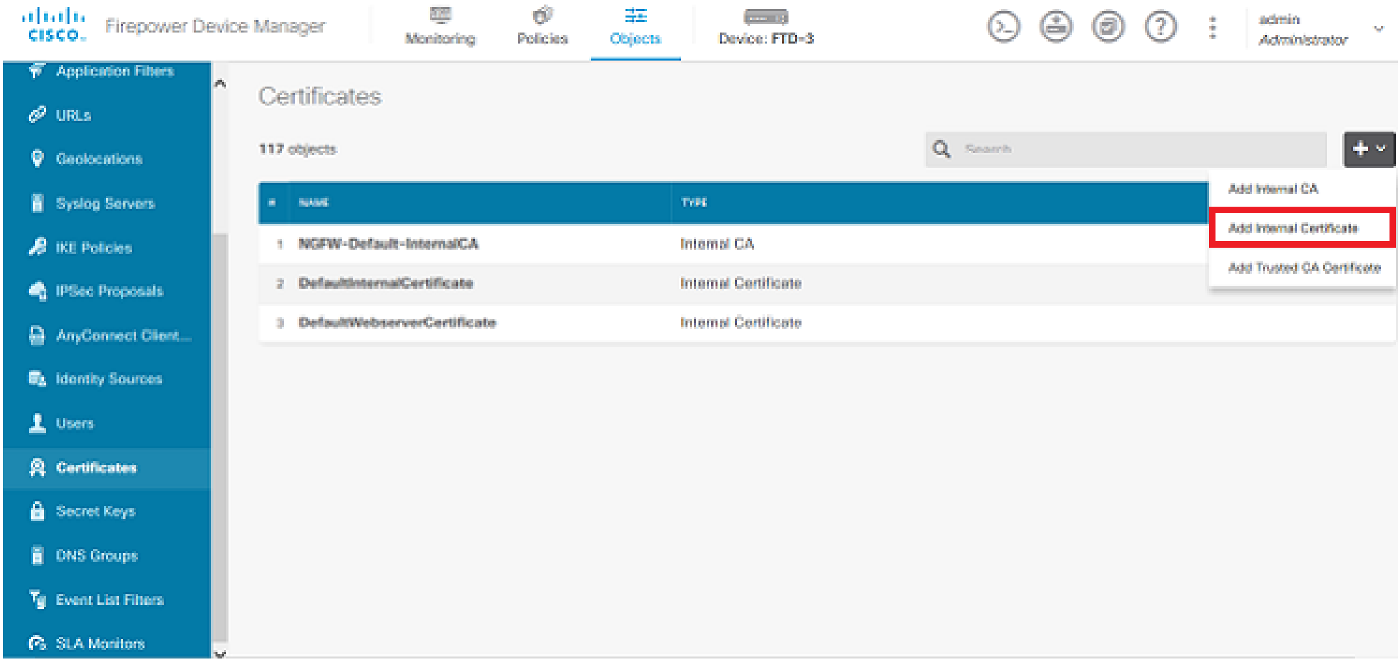
```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
..........................................+++
..................................................................................+++
writing new private key to 'private.key'
-----
You are 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) []:ftd3.example.com
Email Address []:.

Please enter the following '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。一旦簽署CSR，就會提供身份憑證。

3. 導航到對象>證書。 點選+符號，然後選擇Add Internal Certificate，如下圖所示。

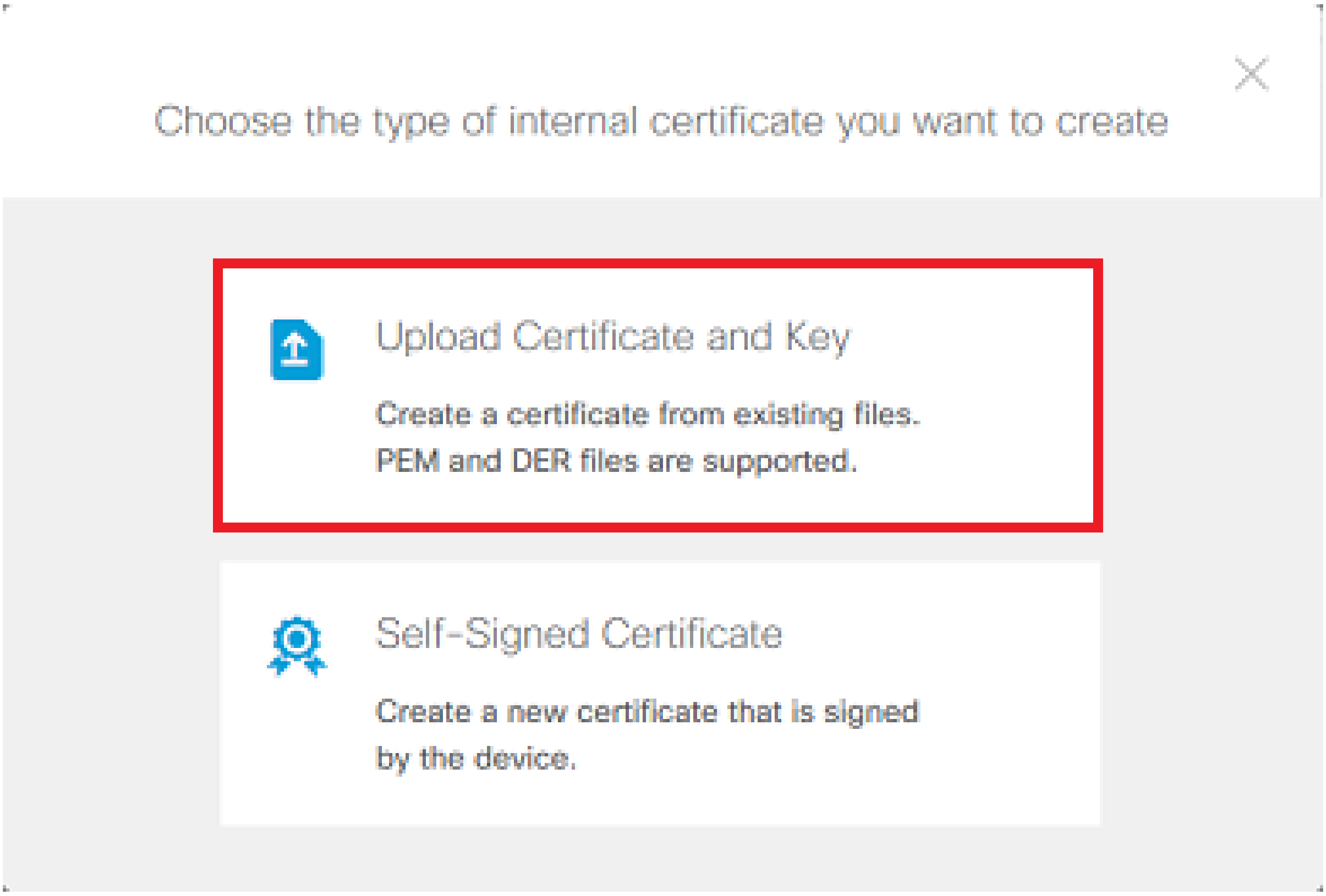


Certificates

117 objects

#	NAME	TYPE
1	NGFW-Default-InternalCA	Internal CA
2	DefaultInternalCertificate	Internal Certificate
3	DefaultWebserverCertificate	Internal Certificate

4. 在彈出窗口中選擇上傳證書和金鑰，如圖所示。



Choose the type of internal certificate you want to create

Upload Certificate and Key

Create a certificate from existing files.
PEM and DER files are supported.

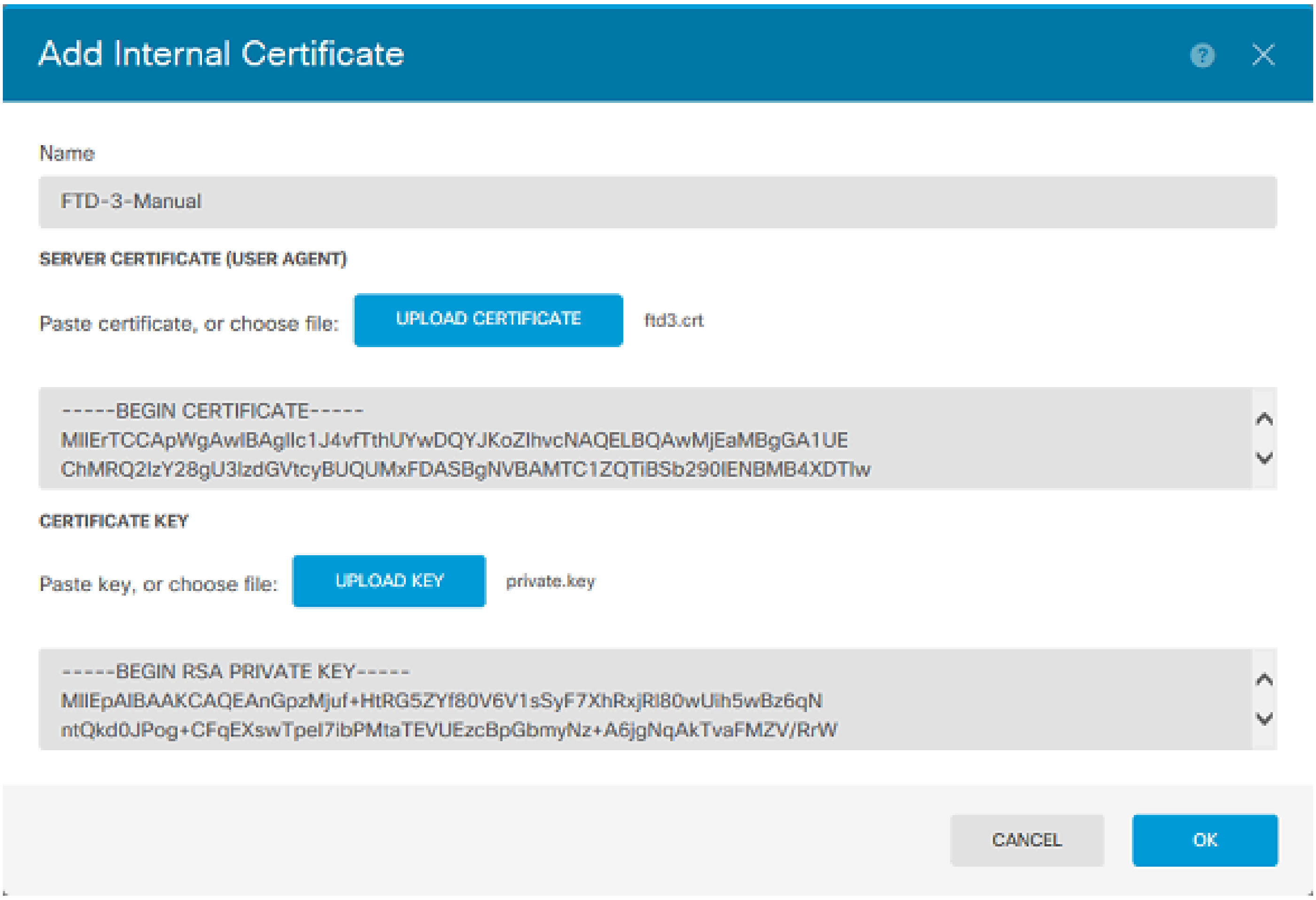
Self-Signed Certificate

Create a new certificate that is signed
by the device.

5. 為信任點指定名稱，然後上傳或複製並貼上身份證書和私鑰(採用Privacy Enhanced Mail (PEM)格式)。如果CA在單個PKCS12中同時提供證書和金鑰，請閱讀本文檔後面部分中標題為從PKCS12檔案中提取身份證書和私鑰，以便將其分開。

注意：檔案名稱不能有任何空格，或FDM不接受它們。此外，私密金鑰不可加密。

完成後按一下OK（如圖所示）。



Add Internal Certificate

Name

FTD-3-Manual

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file: ftd3.crt

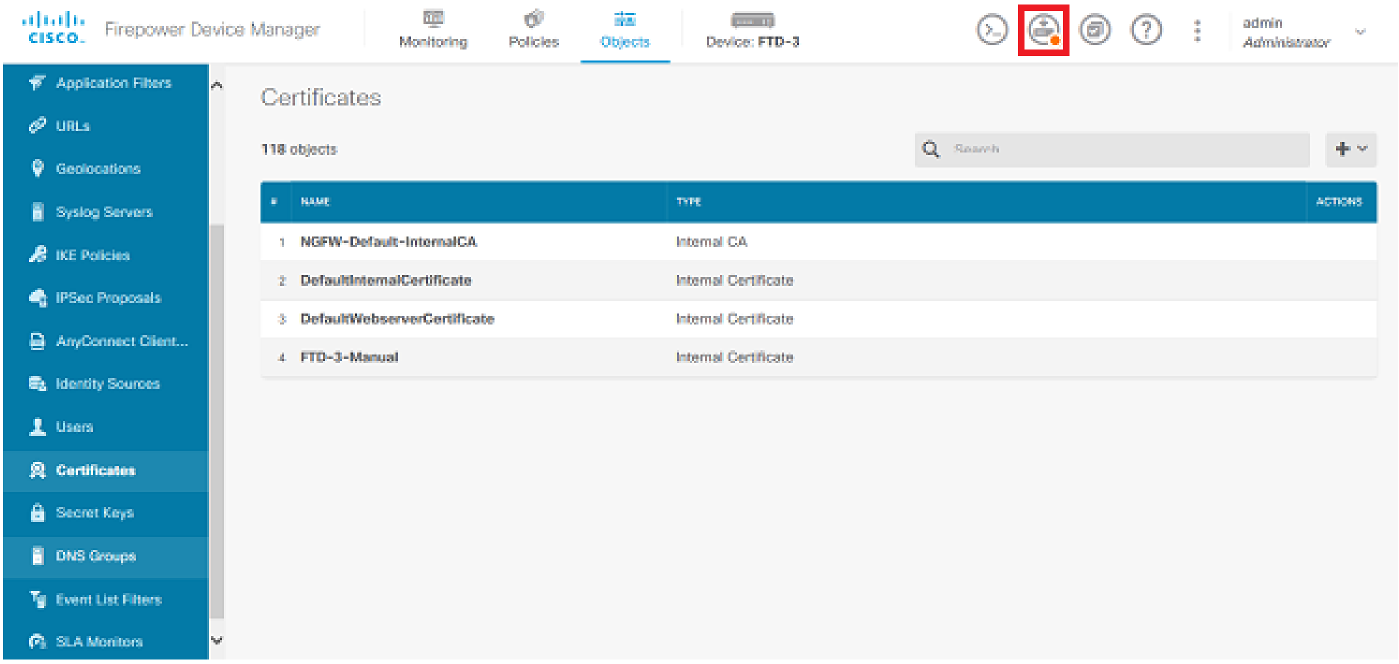
```
-----BEGIN CERTIFICATE-----
MIIErTCCApWgAwIBAgIlc1J4vfTthUYwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2IzY28gU3IzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
```

CERTIFICATE KEY

Paste key, or choose file: private.key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnGpzMjuf+HtRG5ZYf80V6V1sSyF7XhRxjRI80wUih5wBz6qN
ntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGbmyNz+A6jgNqAkTvaFMZV/RrW
```

6. 按一下螢幕右上方的待定更改按鈕，如圖所示。



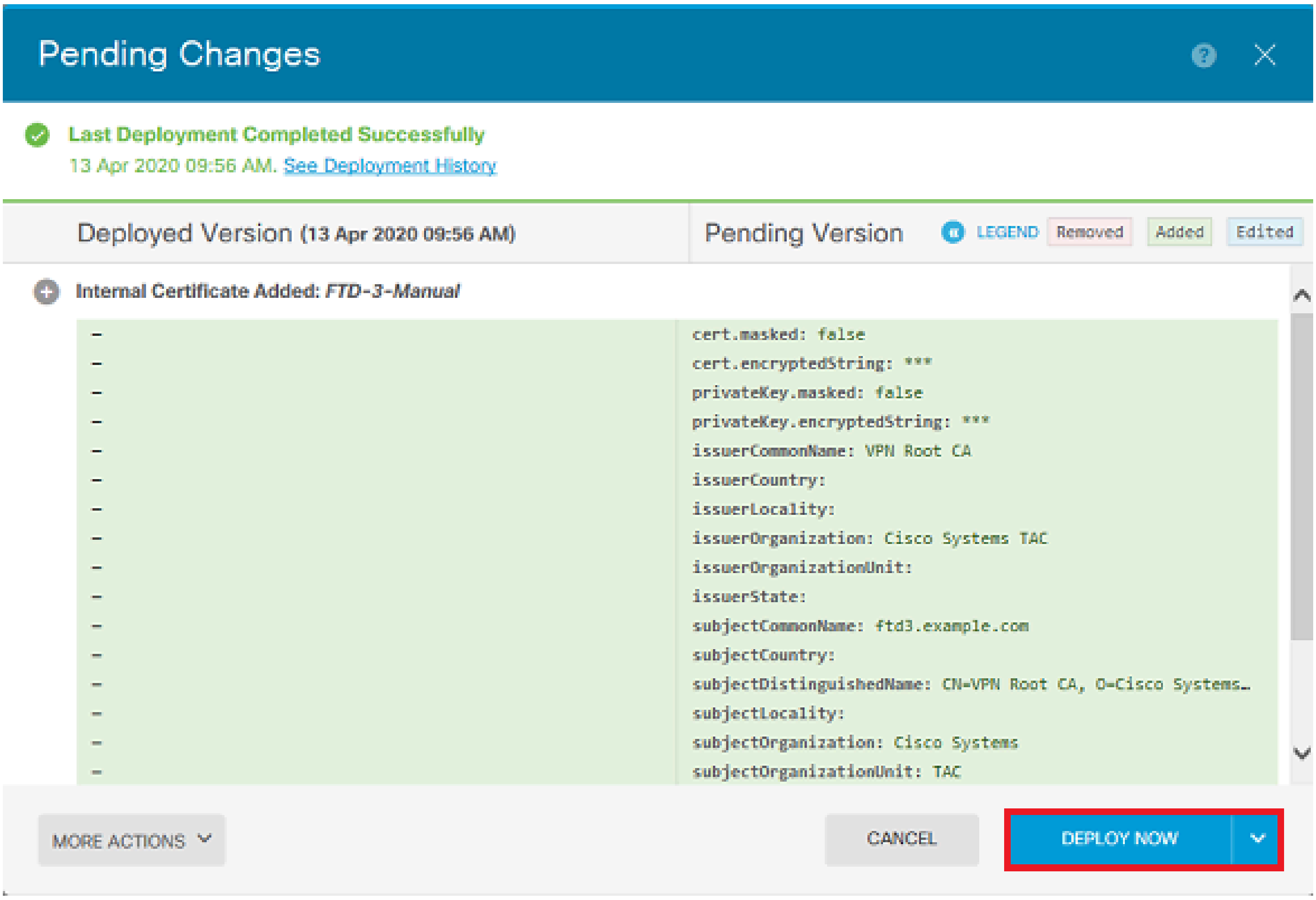
Certificates

118 objects

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Manual	Internal Certificate	

7. 按一下Deploy Now按鈕。

注意：完成部署後，在存在使用證書的服務（如AnyConnect）之前，無法在CLI中看到證書，如圖所示。


Pending Changes
Last Deployment Completed Successfully
13 Apr 2020 09:56 AM. See Deployment History
Deployed Version (13 Apr 2020 09:56 AM)
Pending Version
LEGEND
Removed
Added
Edited
MORE ACTIONS
CANCEL
DEPLOY NOW

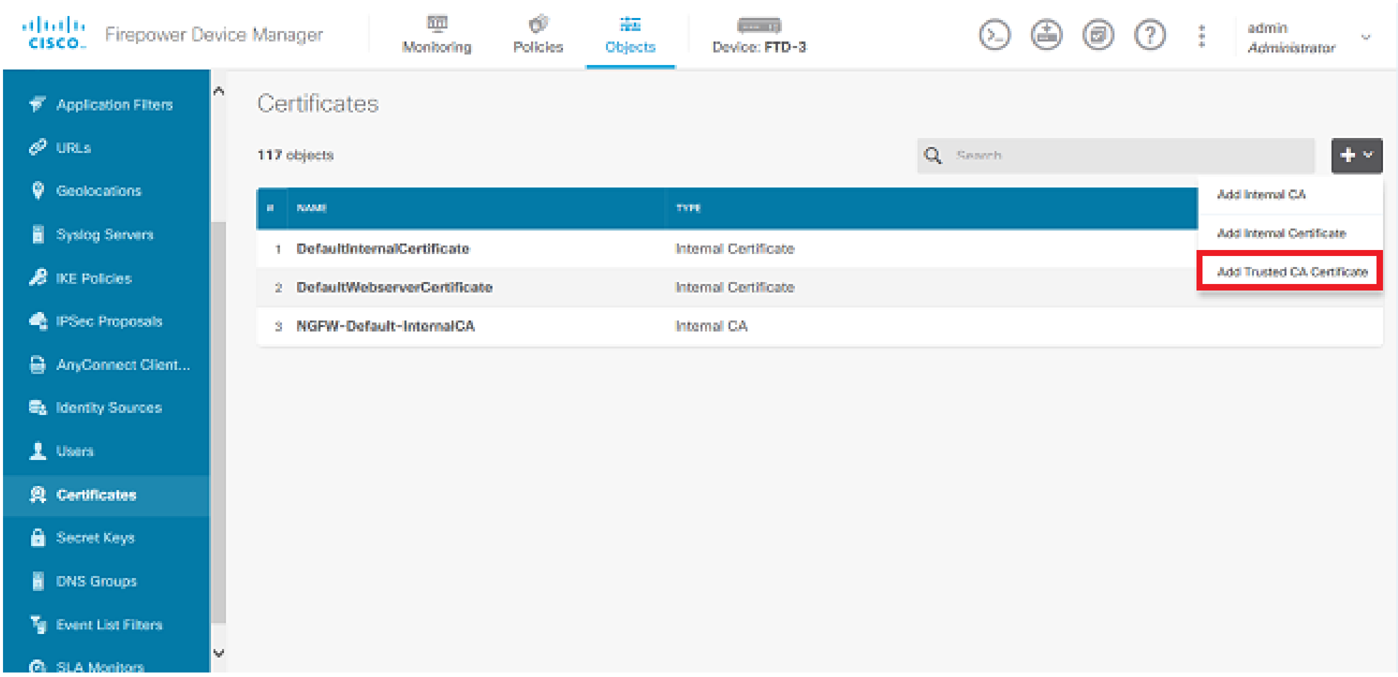
Internal Certificate Added: *FTD-3-Manual*

```
-        cert.masked: false
-        cert.encryptedString: ***
-        privateKey.masked: false
-        privateKey.encryptedString: ***
-        issuerCommonName: VPN Root CA
-        issuerCountry:
-        issuerLocality:
-        issuerOrganization: Cisco Systems TAC
-        issuerOrganizationUnit:
-        issuerState:
-        subjectCommonName: ftd3.example.com
-        subjectCountry:
-        subjectDistinguishedName: CN=VPN Root CA, O=Cisco Systems…
-        subjectLocality:
-        subjectOrganization: Cisco Systems
-        subjectOrganizationUnit: TAC
```

受信任的CA憑證安裝

安裝信任的CA憑證時，必須具備以下條件，才能成功驗證向FTD提供辨識憑證的使用者或裝置。常見示例包括AnyConnect證書身份驗證和S2S VPN證書身份驗證。以下步驟說明如何信任CA憑證，以便讓該CA核發的憑證也能受到信任。

1. 導航到對象>證書。 點選+符號，然後選擇增加受信任CA證書，如圖所示。

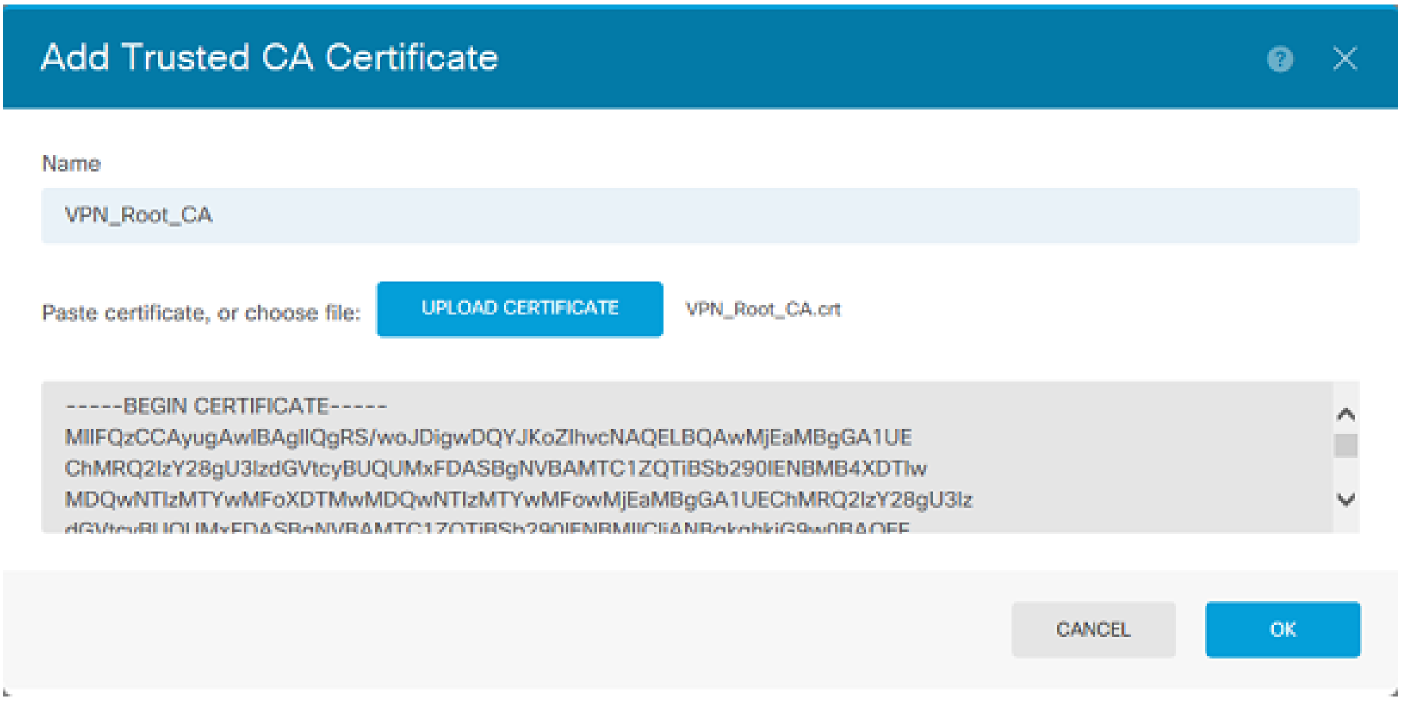


Certificates

117 objects

#	NAME	TYPE
1	DefaultInternalCertificate	Internal Certificate
2	DefaultWebserverCertificate	Internal Certificate
3	NGFW-Default-InternalCA	Internal CA

2. 指定信任點的名稱。然後上傳，或複製並貼上PEM格式的CA憑證。完成後按一下OK（如圖所示）。



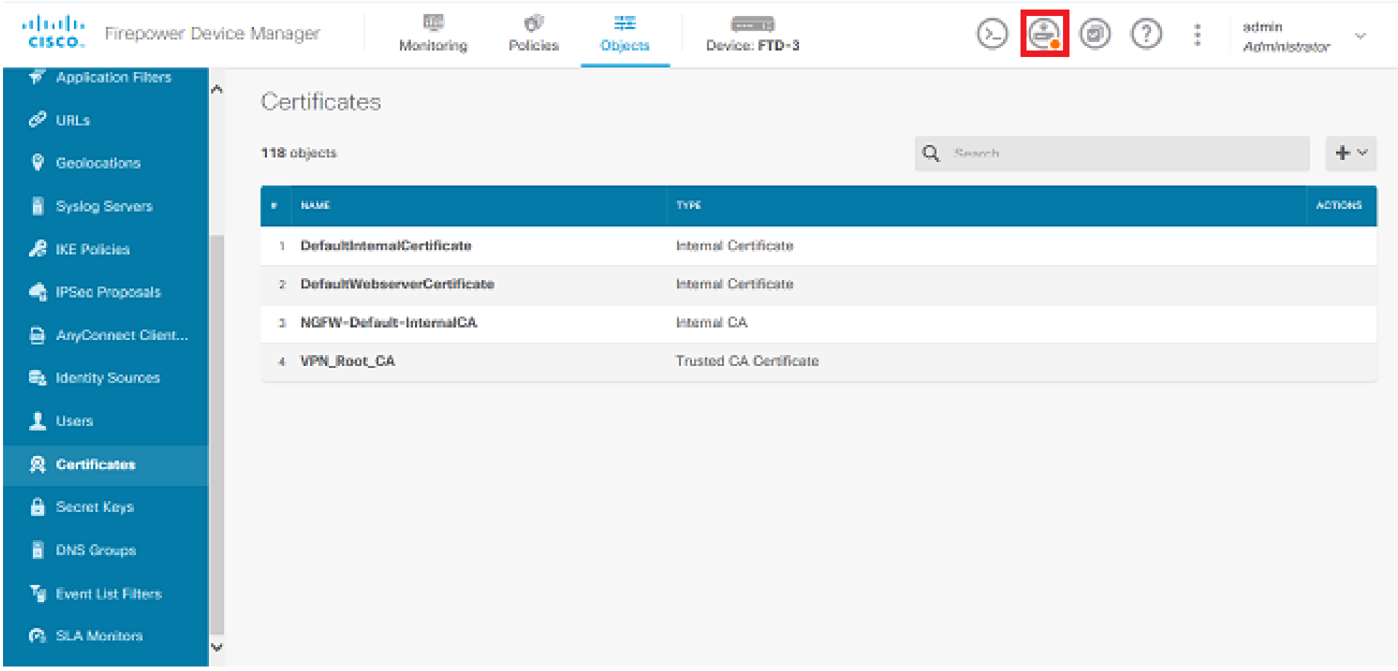
Add Trusted CA Certificate

Name: VPN_Root_CA

Paste certificate, or choose file: VPN_Root_CA.crt

```
-----BEGIN CERTIFICATE-----
MIIFQzCCAyugAwIBAgIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQwNTIzMTYwMFoXDTMwMDQwNTIzMTYwMFowMjEaMBgGA1UEChMRQ2lzY28gU3lz
dGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMIICIjANBgkqhkiG9w0BAQEF
```

3. 按一下螢幕右上方的待定更改按鈕，如圖所示。

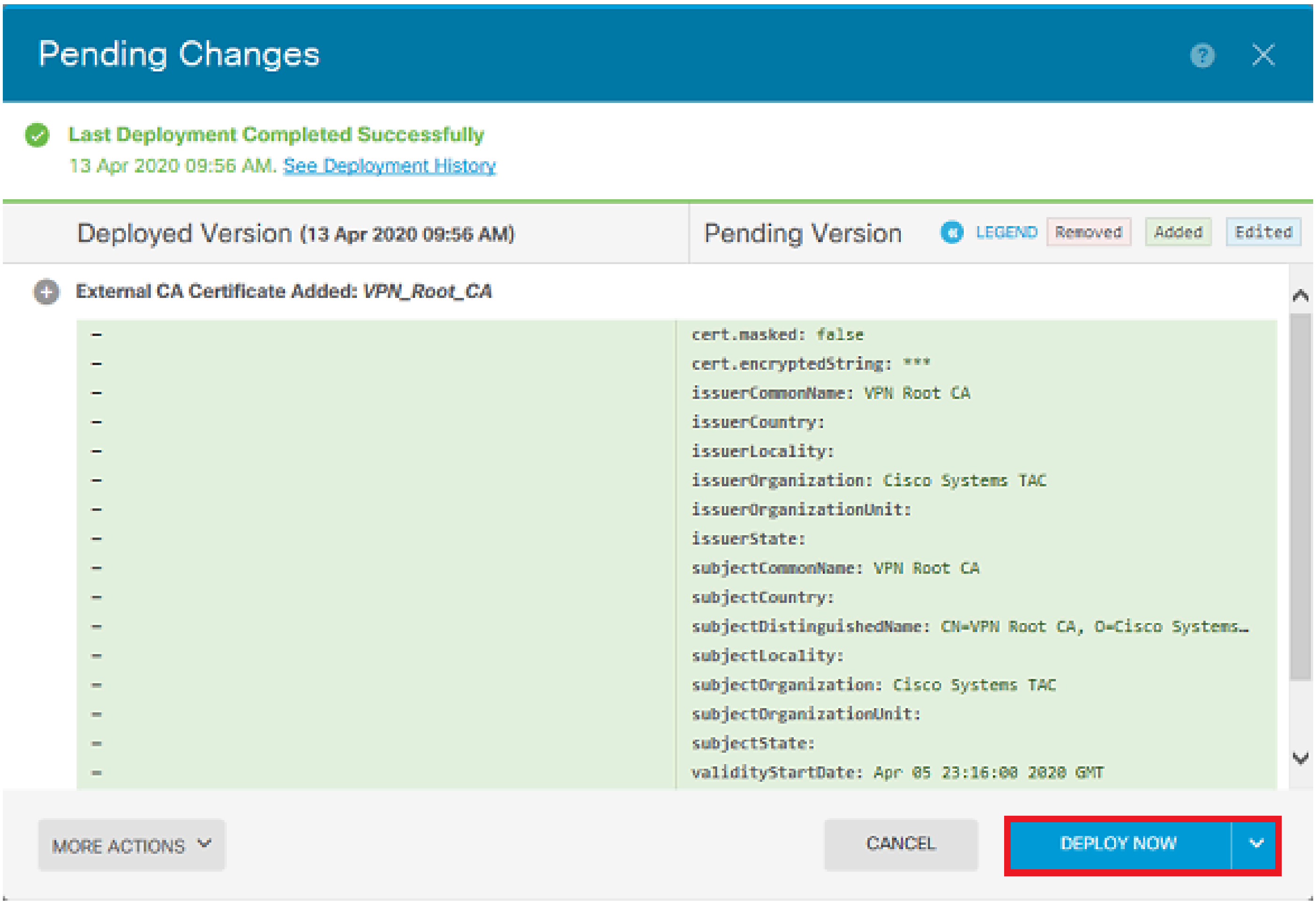


Certificates

118 objects

#	NAME	TYPE	ACTIONS
1	DefaultInternalCertificate	Internal Certificate	
2	DefaultWebserverCertificate	Internal Certificate	
3	NGFW-Default-InternalCA	Internal CA	
4	VPN_Root_CA	Trusted CA Certificate	

4. 按一下Deploy Now按鈕，如圖所示。



Last Deployment Completed Successfully
13 Apr 2020 09:56 AM. See Deployment History

Deployed Version (13 Apr 2020 09:56 AM) | Pending Version

External CA Certificate Added: *VPN_Root_CA*

```
-    cert.masked: false
-    cert.encryptedString: ***
-    issuerCommonName: VPN Root CA
-    issuerCountry:
-    issuerLocality:
-    issuerOrganization: Cisco Systems TAC
-    issuerOrganizationUnit:
-    issuerState:
-    subjectCommonName: VPN Root CA
-    subjectCountry:
-    subjectDistinguishedName: CN=VPN Root CA, O=Cisco Systems…
-    subjectLocality:
-    subjectOrganization: Cisco Systems TAC
-    subjectOrganizationUnit:
-    subjectState:
-    validityStartDate: Apr 05 23:16:00 2020 GMT
```

證書續訂

在FDM管理的FTD上更新憑證涉及取代先前的憑證，並可能取代私密金鑰。如果沒有使用原始CSR和私密金鑰來建立原始憑證，則需要建立新的CSR和私密金鑰。

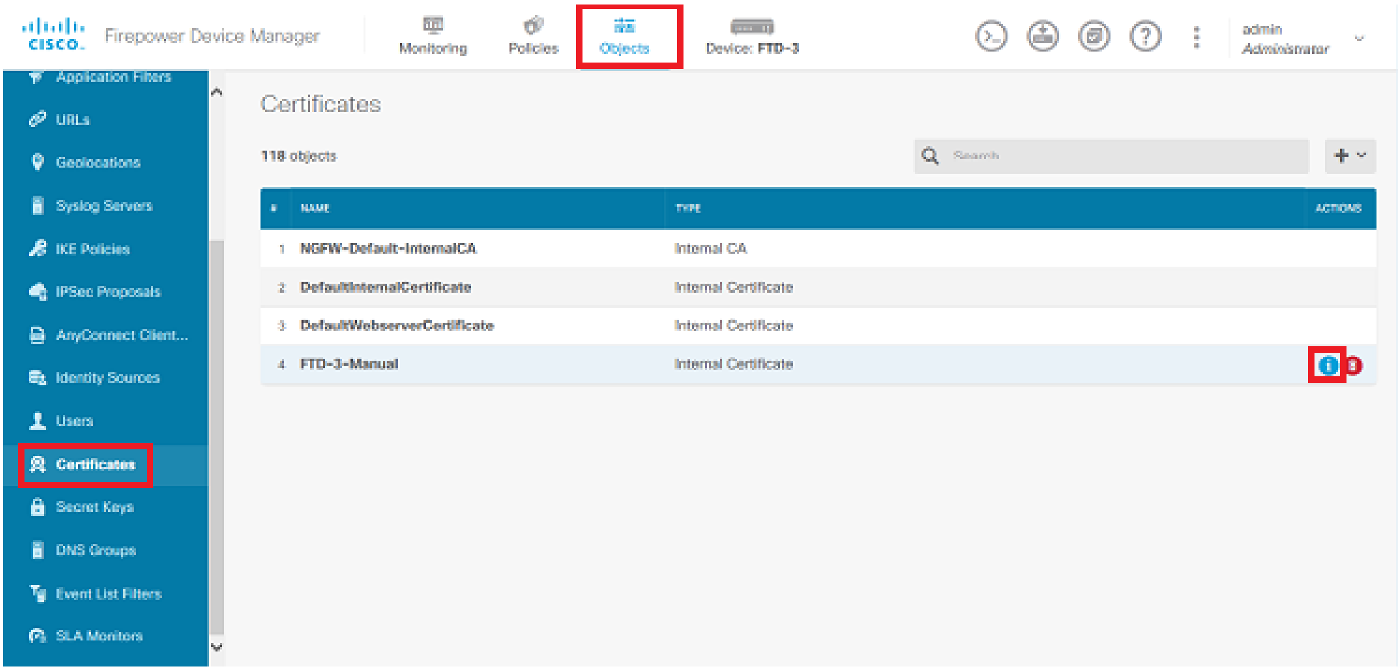
1. 如果您有原始的CSR和私密金鑰，則可以忽略此步驟。否則，需要建立新的私鑰和CSR。使用OpenSSL或類似的應用程式來產生私密金鑰和CSR。此範例顯示名為private.key的2048位元RSA金鑰和在OpenSSL中建立的名為ftd3.csr的CSR。

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
..........................................+++
....................................................................................+++
writing 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 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) []:ftd3.example.com
Email Address []:.

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

2. 將產生的CSR或原始CSR傳送給憑證授權單位。一旦簽署CSR，就會提供更新的身份憑證。

3. 導航到對象>證書。 將滑鼠懸停在您要續訂的證書上，然後按一下View按鈕，如圖所示。

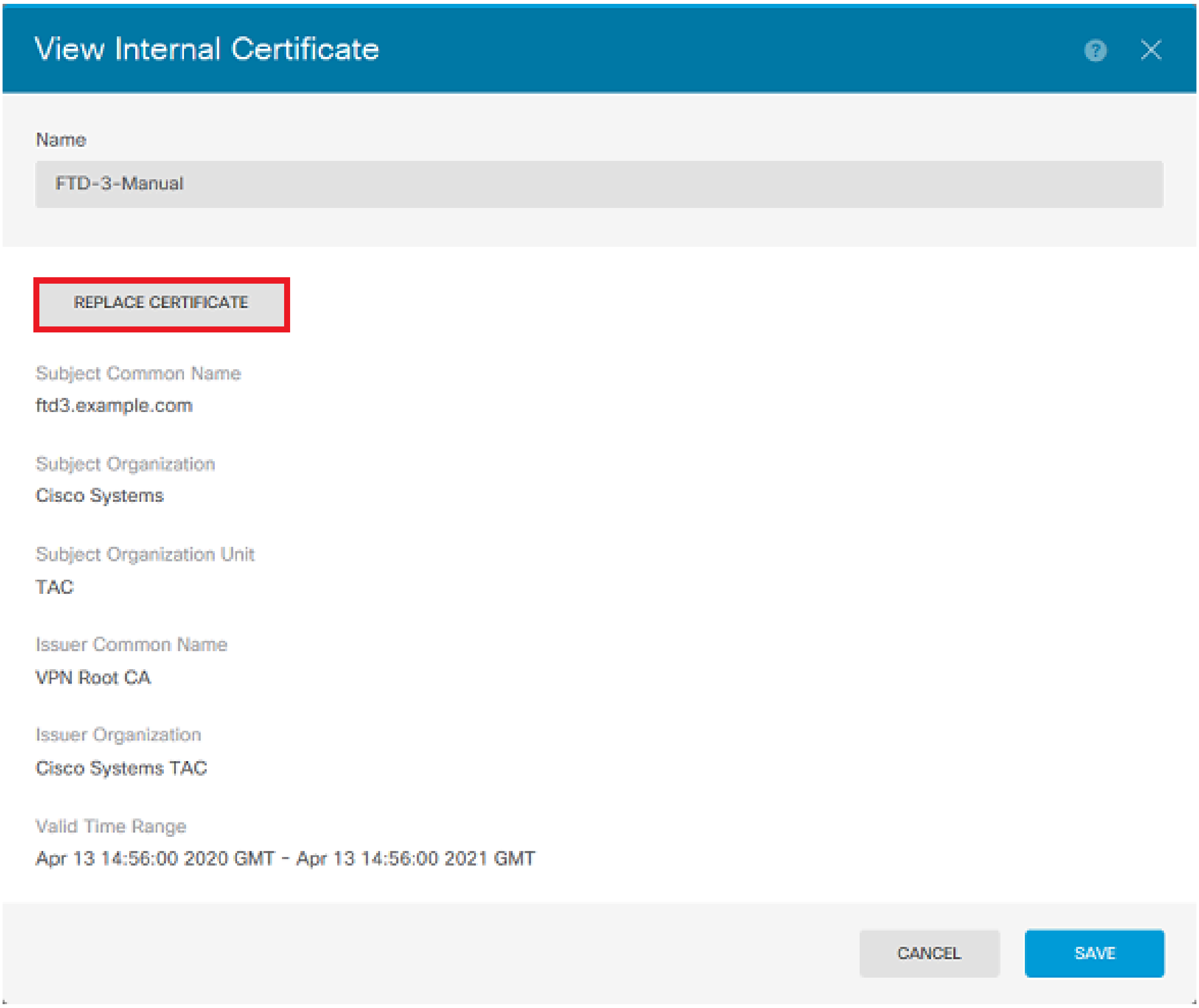


Certificates

118 objects

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Manual	Internal Certificate	

4. 在彈出窗口中，按一下Replace Certificate，如圖所示。



View Internal Certificate

Name

FTD-3-Manual

REPLACE CERTIFICATE

Subject Common Name

ftd3.example.com

Subject Organization

Cisco Systems

Subject Organization Unit

TAC

Issuer Common Name

VPN Root CA

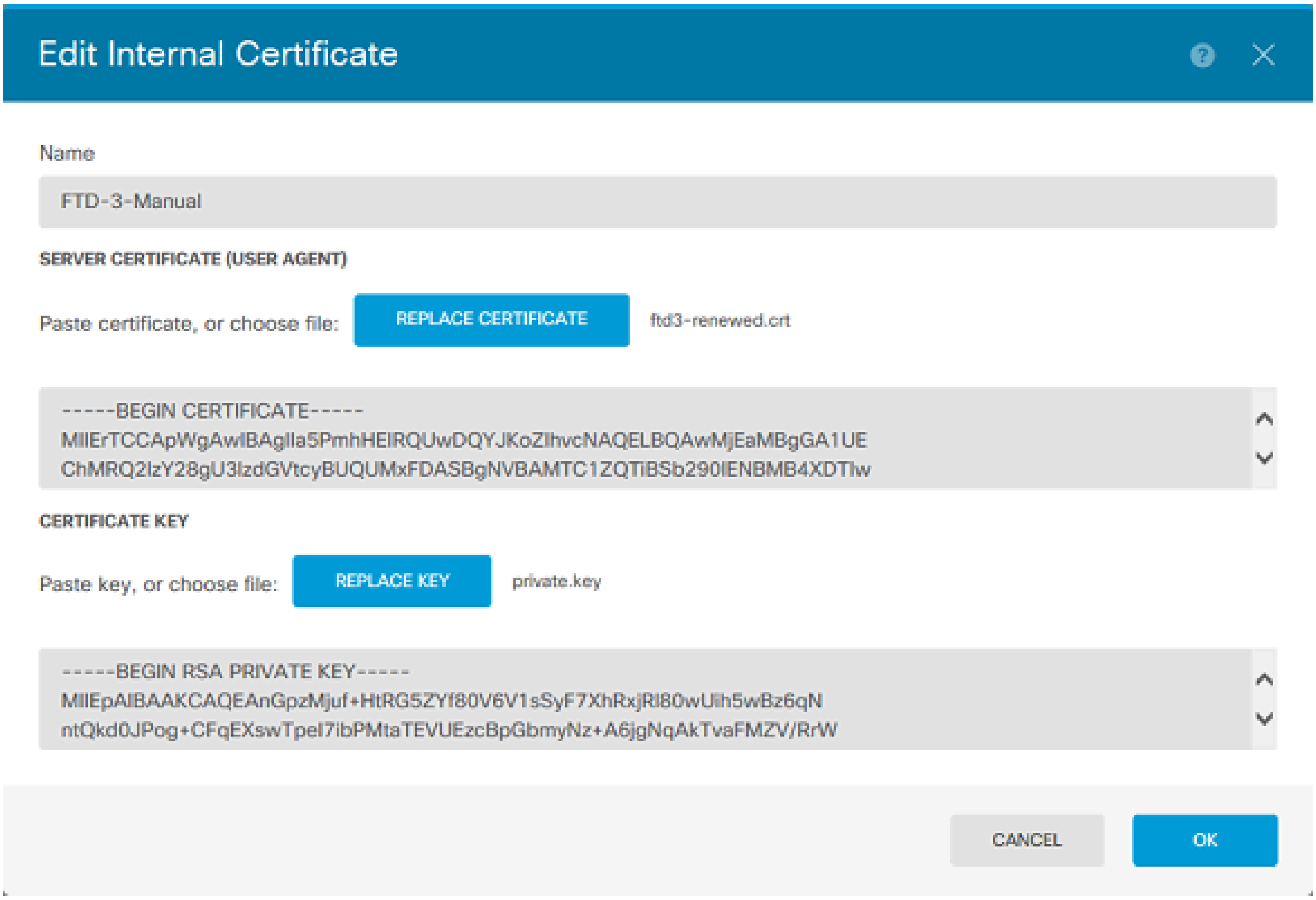
Issuer Organization

Cisco Systems TAC

Valid Time Range

Apr 13 14:56:00 2020 GMT - Apr 13 14:56:00 2021 GMT

5. 上傳或複製並貼上PEM格式的身份證明和私密金鑰。完成後按一下OK（如圖所示）。



Name

FTD-3-Manual

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file: ftd3-renewed.crt

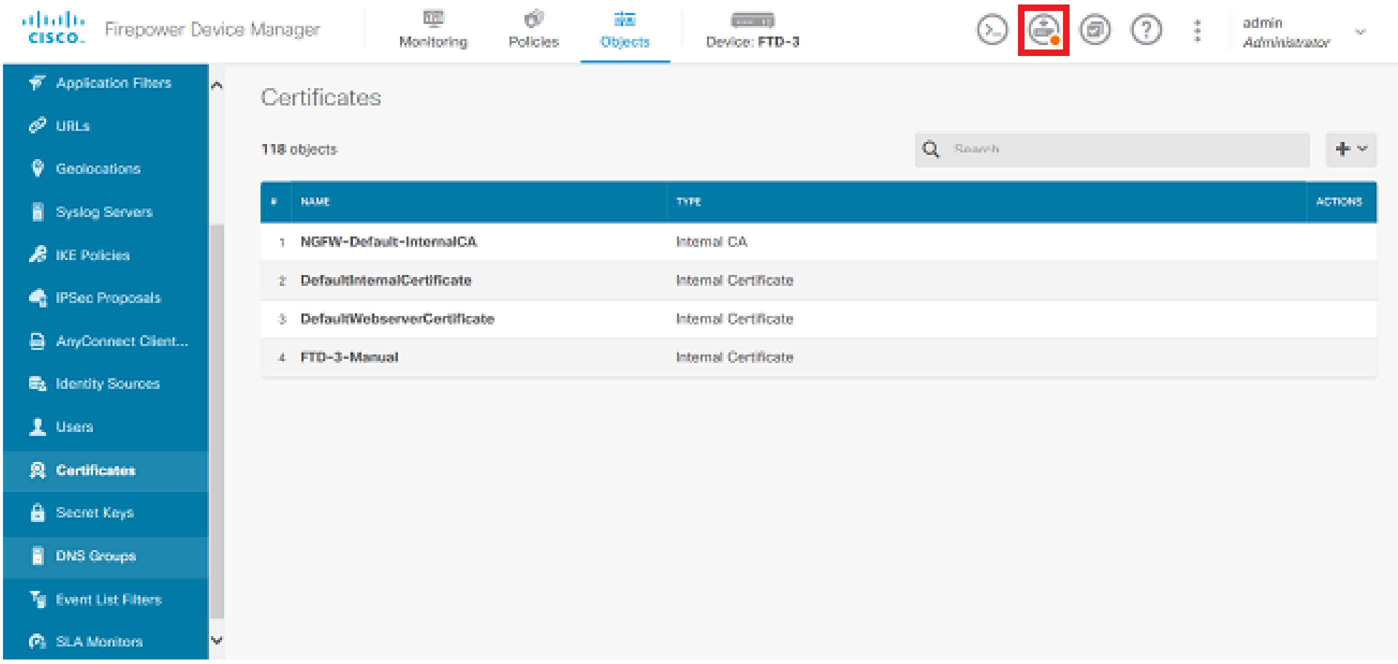
```
-----BEGIN CERTIFICATE-----
MIIErTCCApWgAwIBAgIla5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2IzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
```

CERTIFICATE KEY

Paste key, or choose file: private.key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnGpzMjuf+HtRG5ZYf80V6V1sSyF7XhRxjRl80wUih5wBz6qN
ntQkd0JPog+CFqEXswTpel7ibPMtaTEVUEzcBpGbmyNz+A6jgNqAkTvaFMZV/RrW
```

6. 按一下螢幕右上方的待定更改按鈕，如圖所示。

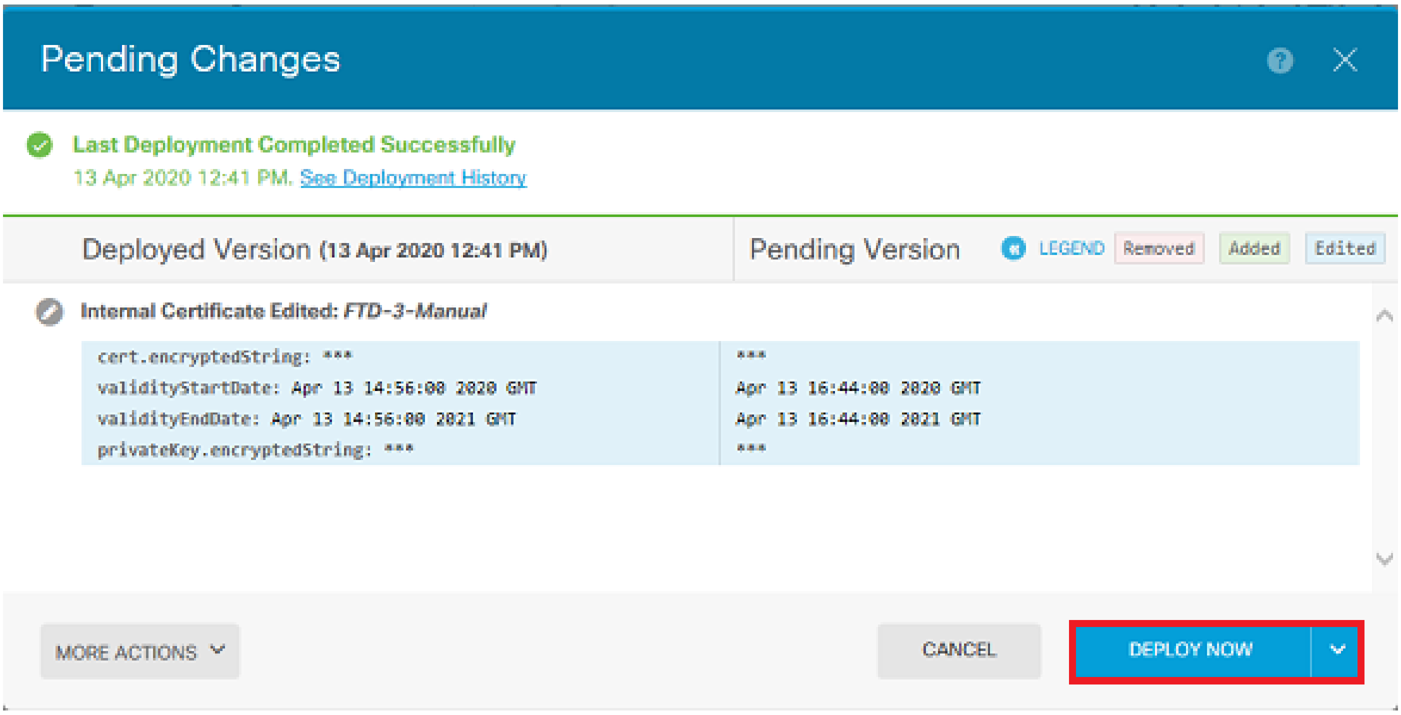


Certificates

118 objects

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Manual	Internal Certificate	

7. 按一下Deploy Now按鈕，如圖所示。



Pending Changes

Last Deployment Completed Successfully
13 Apr 2020 12:41 PM. See Deployment History

Deployed Version (13 Apr 2020 12:41 PM)

Pending Version

Internal Certificate Edited: *FTD-3-Manual*

```
cert.encryptedString: ***                        ***
validityStartDate: Apr 13 14:56:00 2020 GMT      Apr 13 16:44:00 2020 GMT
validityEndDate: Apr 13 14:56:00 2021 GMT        Apr 13 16:44:00 2021 GMT
privateKey.encryptedString: ***                  ***
```

常用OpenSSL作業

從PKCS12檔案擷取辨識憑證和私密金鑰

管理員可以接收需要匯入到FTD的PKCS12檔案。FDM目前不支援匯入PKCS12檔案。為了導入PKCS12檔案內包含的證書和私鑰，必須使用如OpenSSL之類的工具從PKCS12中提取各個檔案。您需要用來加密PKCS12的密碼。

```
openssl pkcs12 -info -in pkcs12file.pfx
Enter Import Password: [PKCS12-passcode]
MAC Iteration 1
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    localKeyID: 28 20 C1 B4 08 1E 65 2E 4D 1D F9 F3 25 07 62 F7 D9 96 A7 F4
    friendlyName: ftd3.example.com
subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIErTCCApWgAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQxMzE2NDQwMFoXDTIxMDQxMzE2NDQwMFowQTEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEMMAoGA1UECxMDVEFDMRkwFwYDVQQDExBmdGQzLmV4YW1wbGUuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnGpzMjuf+HtRG5ZYf80V6V1s
SyF7XhRxjRl80wUih5wBz6qNntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZOIcpzVqL6hOziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50
QpQDTgvIiD1bYpPiWKpS0g1PZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZa
HrP9Y0x09+MpVMH33R9vRl3SOEF6kpZ6VEdGI4s6/IRvaM1zlBcK10N/N2+mjwID
AQABo4G3MIG0MAkGA1UdEwQCMAAwHQYDVR0OBBYEFMcvjL0XiSTzNADJ/ptNb/cd
zB8wMB8GA1UdIwQYMBaAFHekzDnhi40727mjLXuwCRVFgyguMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwGwYDVR0RBBQwEoIQZnRk
My5leGFtcGxlLmNvbTAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMA0G
```

```
CSqGSIb3DQEBCwUAA4ICAQCjjrMjruGH5fpcFND8qfuVU0hkszCwq201oMqMrvXn
gENKcXxxT27z6AHnQXeX3vhDcY3zs+FzFSoP5tRRPmy/413HAN+QEP2L9MQVD9PH
f5OrQ/Ke5c16hMOJO8daR7wNzvFkcbicKCLRH0EvEoI0SPKsLyGSSxGmh6QXfZcM
GX3jG9Krglugp2UEqOug9HPTpgsbuNcHw8xXgFp6IAlOLrytwrLeMIh5V+Vh5pll
yTl9wo5VADoYKgN4O8D21TeJIj6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwfMXM4Tl
Rk3EOdSTENqzq2ZwnqJ4HCoqar7ASlQ5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBUlbadlnEfi5Jl8G+/vZl6ykcmXe9hokKYxY8cg/U717On/FbAmdYwRYgMAE4
RWfBp0voNzn97cG+qzogo7j/0kTfYu3O9DzdU3uy+R8JJkBrerktrZR7w7OfP61O
IAs86N5Zb18U14Gfc9m0eXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2Px0yam/bROnOFoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJFOiV0GV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfpMwTiT47I
ng==
-----END CERTIFICATE-----
Certificate bag
Bag Attributes: <No Attributes>
subject=/O=Cisco Systems TAC/CN=VPN Root CA
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQwNTIzMTYwMFoXDTMwMDQwNTIzMTYwMFowMjEaMBgGA1UEChMRQ2lzY28gU3lz
dGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAxhTBKiB1xzLg2Jr48h/2u84RcWahOTmPYCNGYZg0PvSf
JOpKvAu5tz4z625Yx1nBtjSsEgzF+qETpSplEhjW2NxIclxuNirfrmSJQfIw51yT
PaFv7u+VhgyYbYsSxGAB/m6RWWpiNbg8SDoUACU7R/bvp1Rb8W6tXk/rsTljc7L2
c/G5MeDLNmc/i/M1zuMjhj0tCphsJPhvNII7lcNj6K0pvg2yB/Md7PXOZnLaz9pf
GgpjpH0zzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXmlHQcgp
g5BgZMGqro0l5rcq0PjtK9Tqg7q013Vf0kMlsofMp+Bu1CiFDpawF/j8uSPuswEs
rzvJ+8GbOY1WEHtohgNGjPOOq8wnKQu0C47Ft1UMpdSwUsMMze0X43dyp/WoZtLW
4v/Pn/NibE3aoPOaMhIo4CdwSBHZOgVag4INqVsuFX1uPKD25Whrl09LQ93P/sN3
FhoAh98HKOcuQ64Ua3AaShdzornD+G2J2pd1Nf1DahlzlskIMtlURSWdLjsHLKft
JqSOoLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/lyNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cxl1jIN0LdB+/jQqkfzmx9ziB1PXnIshNRbflLLrNfdDO9agqQsvsC
AwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDKC4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDKC4wCwYDVR0PBAQD
AgEGMA0GCSqGSIb3DQEBCwUAA4ICAQC6B+Y3obatEZqv0RQz1MS6oOumCgNWGi8d
kcRDxkY2F+zw3pBFa54Sin1OfRPJvZvLNJV5OdXmvH5luh6KJDMVrLMWNiSgI7Tn
0ipqKraokS2Oo0STwQ7Q9Wk1xCrwxMfTuDJFMe80qabFAU557O5PDXPtFEutn0xz
Ou8VMLBRy+gDc+0WARsjFj+0gU0c2Wj3gQ81GlyoPYgufWRnztN5rQxWzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AydsGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p7O2FZly5lxuzuA/wPnR89HiIkSF13OMTpnOIl3d6d07s3bwyNja8JikYTCflle5
2CSsz4Cn/BlwfWyAcLN3HxUjG4Ev2818fWWpkYmuxujpKDFFzF0skpKAK53tNKPf
pn4+w5FyLo18oOAydtPoKjYkDqbvG/SRPbt92mdTIF7E6J+o8J6OV3YL+IyrZ+u0
MYqPd45Oi4cgHdMFICAndN3PYScrrGYHawfVxp+R+G4dTJWdMvthh3ftSOmkiKJ8
m1NH7WYST1kYcTbcokZiOIcZa+VVv5UOLIt/hDOVG7xqZOlpMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpxTIsmDv9rQzxBjuCyKn+23FkkUhFJtOD989UUyp08H9vDoJr
yzm9JOpMrg==
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    localKeyID: 28 20 C1 B4 08 1E 65 2E 4D 1D F9 F3 25 07 62 F7 D9 96 A7 F4
    friendlyName: ftd3.example.com
Key Attributes: <No Attributes>
Enter PEM pass phrase: [private-key-passcode]
Verifying - Enter PEM pass phrase: [private-key-passcode]
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIScA8TOogup4CAggA
MBQGCCqGSIb3DQMHBAgKqoTuZzoXsASCBMgOTEb24ENJl4/qh3GpsE2C2OCnJeid
ptDDIFdyOV4A+su3OJWzlnHrCuIhjR8+/p/N0WlA73x47R4T6+u4w4/ctHkvEbQj
gZJZzFWTed9HqidhcKxxOoM/w6/uDv/opc6/rlIZiaKp6FO9hOibqlGI9kjxkWQC
EQR8cM1U2yiOvagL8pOYdeujCrzBtorRp9BMJelCP1Mw9t0EbAC4mmuedzs+86r1
```

```
xadK7qHBuWUJcO3SLXLCmX5yLSGteWcoaPZnIKO9UhLxpUSJTkWLHr2VtE1ACMRc
RlPBXMLb70nMtPTqctl58+Q/axtQCWUs8caHs3LvVf0nRG+War49/F8Ii8mqnNnb
M6ZTwTOZ1sn0f4ohVePrW/kkdlQavJbPa+0dzjZvs88ClEXAJ/XIegfSWifJAXqP
3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jjlKgfoxubtnuFq
un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZHOBuFls+wZEmzYqw+cuc+I8XEFVOMl8
P3ah28Nno0jXMk4MpfFJlYMCmMq66xj5gZtcVZxOGCOswOCKU0JiFFQTEmmVf9/C
65a96np7YCI8s6UnUWi5Zp/NrbN31HkP0wt7+1DFGFit1pTTGvOFchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG1l5NSslwKbTGiiwCYw0N8c09TXQb04rMomFDAv8
aef1aBsjMqEUkzOZK0U2ZgTxMline8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubp0
qtmFX/DtSu9J2yevfV+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc4O
w94fQH/DJ/lKsmSVwBLQLEKRl/nIDz36kmA27+1nVtX42PbEaIaFgucU4xHKx3zN
mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaq8
fNl7vEB+aret+PmqCiQYlHqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUROTuBHQhRK
3XpHfGXpe/OOGdW3LeifNLvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP
VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzdOcJ3aGCeAl84XuPRfQhHe/Aj7q6l6uqB
W3Kt+kMJ9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/
QCyhIRk3mx+8a1YLqK+hOMjWWBDEHX2mvbdKickK/jhwRdR/WmFOALq51phgtZlz
Zedl5UbPqWahJsjoO9N5pp7Uq5iV0/xq4Ml+/xQIYo2GIrqyat4AdB2B6K8K3xQd
Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTfzH5zgneUwLwnuBAbGT3oMSQ/
OKXnhcmUGu8XvLEfU/PITvGzKr06o12/hHJtzXQ8eNPDJbvcD/okRRKZpmjH+ijp
FPD/WgQ/vmO9HdCWW3flhqceqfHff8ClCJYFLxsgZp4M3G+WyQTky4J8+6uTn/mj
yyZ5JCZdlt42haSNqU/ynioCjh5XY4m8WMZsOJBNPjKZiUX/vqVcc+/nodl7VRZy
ELk=
-----END ENCRYPTED PRIVATE KEY-----
```

pkcs12file.pfx是需要解除封裝的PKCS12檔案。

在此範例中，會建立三個不同的檔案：

一個用於身份證書。由於subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com，您可以將此身份證書辨認出來。

```
subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIErTCCApWgAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQxMzE2NDQwMFoXDTIxMDQxMzE2NDQwMFowQTEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEMMAoGA1UECxMDVEFDMRkwFwYDVQQDExBmdGQzLmV4YW1wbGUuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnGpzMjuf+HtRG5ZYf80V6V1s
SyF7XhRxjRl80wUih5wBz6qNntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZOIcpzVqL6hOziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50
QpQDTgvIiD1bYpPiWKpS0g1PZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZa
HrP9Y0xO9+MpVMH33R9vRl3SOEF6kpZ6VEdGI4s6/IRvaM1zlBcK10N/N2+mjwID
AQABo4G3MIG0MAkGA1UdEwQCMAAwHQYDVR0OBBYEFMcvjL0XiSTzNADJ/ptNb/cd
zB8wMB8GA1UdIwQYMBaAFHekzDnhi4O727mjLXuwCRVFgyguMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwGwYDVR0RBBQwEoIQZnRk
My5leGFtcGxlLmNvbTAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMA0G
CSqGSIb3DQEBCwUAA4ICAQCjjrMjruGH5fpcFND8qfuVU0hkszCwq201oMqMrvXn
gENKcXxxT27z6AHnQXeX3vhDcY3zs+FzFSoP5tRRPmy/413HAN+QEP2L9MQVD9PH
f5OrQ/Ke5c16hMOJO8daR7wNzvFkcbicKCLRH0EvEoI0SPKsLyGSSxGmh6QXfZcM
GX3jG9Krglugp2UEqOug9HPTpgsbuNcHw8xXgFp6IAlOLrytwrLeMIh5V+Vh5pll
yTl9wo5VADoYKgN4O8D21TeJIj6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwfMXM4Tl
Rk3EOdSTENqzq2ZwnqJ4HCoqar7ASlQ5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBUlbadlnEfi5Jl8G+/vZl6ykcmXe9hokKYxY8cg/U717On/FbAmdYwRYgMAE4
RWfBp0voNzn97cG+qzogo7j/0kTfYu3O9DzdU3uy+R8JJkBrerktrZR7w7OfP61O
```

```
IAs86N5Zb18U14Gfc9m0eXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2Px0yam/bROn0FoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJFOiVOGV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfpMwTiT47I
ng==
-----END CERTIFICATE-----
```

一個用於頒發CA證書。由於subject=/O=Cisco Systems TAC/CN=VPN Root CA，您可以將此身份證書辨認出來。此值與之前看到的身份證書中的頒發者值相同：

```
subject=/O=Cisco Systems TAC/CN=VPN Root CA
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQwNTIzMTYwMFoXDTMwMDQwNTIzMTYwMFowMjEaMBgGA1UEChMRQ2lzY28gU3lz
dGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAxhTBKiB1xzLg2Jr48h/2u84RcWahOTmPYCNGYZg0PvSf
JOpKvAu5tz4z625Yx1nBtjSsEgzF+qETpSplEhjW2NxIclxuNirfrmSJQfIw51yT
PaFv7u+VhgyYbYsSxGAB/m6RWWpiNbg8SDoUACU7R/bvp1Rb8W6tXk/rsTljc7L2
c/G5MeDLNmc/i/M1zuMjhj0tCphsJPhvNII7lcNj6KOpvg2yB/Md7PXOZnLaz9pf
GgpjpHOzzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXmlHQcgp
g5BgZMGqroOl5rcq0PjtK9Tqg7q013Vf0kMlsofMp+Bu1CiFDpawF/j8uSPuswEs
rzvJ+8GbOY1WEHtohgNGjPOOq8wnKQu0C47Ft1UMpdSwUsMMze0X43dyp/WoZtLW
4v/Pn/NibE3aoPOaMhIo4CdwSBHZOgVag4INqVsuFX1uPKD25Whrl09LQ93P/sN3
FhoAh98HKOcuQ64Ua3AaShdzornD+G2J2pd1Nf1DahlzlskIMtlURSWdLjsHLKft
JqSOoLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/lyNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cxl1jIN0LdB+/jQqkfzmx9ziB1PXnIshNRbflLLrNfdDO9agqQsvsC
AwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDKC4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDKC4wCwYDVR0PBAQD
AgEGMA0GCSqGSIb3DQEBCwUAA4ICAQC6B+Y3obatEZqv0RQz1MS6oOumCgNWGi8d
kcRDxkY2F+zw3pBFa54Sin1OfRPJvZvLNJV5OdXmvH5luh6KJDMVrLMWNiSgI7Tn
OipqKraokS2Oo0STwQ7Q9Wk1xCrwxMfTuDJFMe80qabFAU557O5PDXPtFEutn0xz
Ou8VMLBRy+gDc+0WARsjFj+0gU0c2Wj3gQ81GlyoPYgufWRnztN5rQxWzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AydsGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p7O2FZly5lxuzuA/wPnR89HiIkSF13OMTpnOIl3d6d07s3bwyNja8JikYTCflle5
2CSsz4Cn/BlwfWyAcLN3HxUjG4Ev2818fWWpkYmuxujpKDFFzF0skpKAK53tNKPf
pn4+w5FyLo18o0AydtPoKjYkDqbvG/SRPbt92mdTIF7E6J+o8J6OV3YL+IyrZ+u0
MYqPd450i4cgHdMFICAndN3PYScrrGYHawfVxp+R+G4dTJWdMvthh3ftS0mkiKJ8
m1NH7WYST1kYcTbcokZiOIcZa+VVv5UOLIt/hD0VG7xqZOlpMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpxTIsmDv9rQzxBjuCyKn+23FkkUhFJt0D989UUyp08H9vDoJr
yzm9JOpMrg==
-----END CERTIFICATE-----
```

一個用於私鑰：

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIScA8TOogup4CAggA
MBQGCCqGSIb3DQMHBAgKqoTuZzoXsASCBMgOTEb24ENJl4/qh3GpsE2C2OCnJeid
ptDDIFdyOV4A+su3OJWzlnHrCuIhjR8+/p/N0WlA73x47R4T6+u4w4/ctHkvEbQj
gZJZzFWTed9HqidhcKxxOoM/w6/uDv/opc6/rlIZiaKp6FO9hOibqlGI9kjxkWQC
EQR8cM1U2yiOvagL8pOYdeujCrzBtorRp9BMJelCP1Mw9tOEbAC4mmuedzs+86r1
xadK7qHBuWUJcO3SLXLCmX5yLSGteWcoaPZnIKO9UhLxpUSJTkWLHr2VtE1ACMRc
RlPBXMLb7OnMtPTqctl58+Q/axtQCWUs8caHs3LvVf0nRG+War49/F8Ii8mqnNnb
```

```
M6ZTwTOZ1sn0f4ohVePrW/kkdlQavJbPa+0dzjZvs88ClEXAJ/XIegfSWifJAXqP
3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jjlKgfoxubtnuFq
un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZHOBuFls+wZEmzYqw+cuc+I8XEFVOMl8
P3ah28Nno0jXMk4MpfFJlYMCmMq66xj5gZtcVZxOGCOswOCKU0JiFFQTEmmVf9/C
65a96np7YCI8s6UnUWi5Zp/NrbN31HkP0wt7+1DFGFit1pTTGvOFchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG1l5NSslwKbTGiiwCYw0N8c09TXQb04rMomFDAv8
aef1aBsjMqEUkzOZK0U2ZgTxMline8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubp0
qtmFX/DtSu9J2yevfV+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc4O
w94fQH/DJ/lKsmSVwBLQLEKRl/nIDz36kmA27+1nVtX42PbEaIaFgucU4xHKx3zN
mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaq8
fNl7vEB+aret+PmqCiQYlHqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUROTuBHQhRK
3XpHfGXpe/OOGdW3LeifNLvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP
VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzdOcJ3aGCeAl84XuPRfQhHe/Aj7q6l6uqB
W3Kt+kMJ9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/
QCyhIRk3mx+8a1YLqK+hOMjWWBDEHX2mvbdKickK/jhwRdR/WmFOALq51phgtZlz
Zedl5UbPqWahJsjoO9N5pp7Uq5iV0/xq4Ml+/xQIYo2GIrqyat4AdB2B6K8K3xQd
Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTfzH5zgneUwLwnuBAbGT3oMSQ/
OKXnhcmUGu8XvLEfU/PITvGzKr06o12/hHJtzXQ8eNPDJbvcD/okRRKZpmjH+ijp
FPD/WgQ/vmO9HdCWW3flhqceqfHff8ClCJYFLxsgZp4M3G+WyQTky4J8+6uTn/mj
yyZ5JCZdlt42haSNqU/ynioCjh5XY4m8WMZsOJBNPjKZiUX/vqVcc+/nodl7VRZy
ELk=
-----END ENCRYPTED PRIVATE KEY-----
```

附註：私密金鑰已加密，而FDM不接受加密的私密金鑰。

若要將私密金鑰解除加密，請將加密的私密金鑰複製到檔案中，然後執行此openssl指令：

```
openssl rsa -in encrypted.key -out unencrypted.key
Enter pass phrase for encrypted.key: [private-key passphrase]
writing RSA key
```

- encrypted.key是儲存加密私鑰的檔案的名稱。
- unencrypted.key是包含未加密金鑰的檔案的名稱。

未加密的私鑰可以顯示-----BEGIN RSA PRIVATE KEY-----而不是-----BEGIN ENCRYPTED PRIVATE KEY-----，如以下示例所示：

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnGpzMjuf+HtRG5ZYf8OV6V1sSyF7XhRxjRl8OwUih5wBz6qN
ntQkdOJPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGbmyNz+A6jgNqAkTvaFMZV/RrW
qCNktO8ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqNBqotoz3/8CrZOIcpzVqL6hOz
iJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS5OQpQDTgvIiD1bYpPiWKpSOg1P
ZDnX8b74OsOpVKVXTsujQqSqH1va9BB6hK1JCoZaHrP9YOxO9+MpVMH33R9vRl3S
OEF6kpZ6VEdGI4s6/IRvaM1zlBcK1ON/N2+mjwIDAQABAoIBAEQzCd1KMBrosdmk
eRvoMPiaemBbze2cXlJWXZ2orICSXhvMOokBGJFDQXN47ZCuVqYAqOecjU9RzGgE
NbXYfUsD6+P91k+/Gj1RiCNLBHBwdgewzw1quTxP54zSpAVlIXyQ+FolTzjH1yfW
7iHhuSujYsAYLWPy4Yg3NpU2IdzeQoK5ViuSTTNx8LHYBKw1Qf7HVaQTfmsWOAyg
/vjZqjRkukqKM41srgkO/HjPnEBDuUWVTehzMCk1etijENc7ttISzYIEMNPthe6O
NpidXAHoJ1lJM6HB9ZraBH5fu7MZJZOOn6YVKQuCdWOWfnKiNQCDsXq7X5EWsaj3
cgyjWlkCgYEAy33k1wxp7WEqg1zEwqOVq7AtoL6i4V9QCenMThQAHwNAAUGGOSIF
JhpKyApm/BUogSIOMzIPse+NgAA66TRn4qfkbpvTI98CeCUxiUPcbRmqZnYxCOfp
Pzosv5OnBLltoIOprIO2S5a261w6JGNAfD95tCjCYYrB8Cw/HbZOLPUCgYEAxMbZ
KVyosBxaAIFQinHaff3fVSTsEOZFpLCBbLybgLcP8LsLdahBsj6HK/hAffKXOdvM
35CAM7ZL/WCI1Jb+dx4YcD9q8lbVMu4HTvSl2deTZoZrBG2iFX6OSsn2rLKAH+cH
uLSHCNAj9cj9syldZErGLZtBQpJPtpLRd6iyOvMCgYBP/zoLYJHOBBLWeY3QioLO
cABABTG7L+EjRIpQ14QErR5oX/4IT9t+Uy+63HwH9blqqpyye6e359jUzUJbk4KT
lDU1VoT2wSETYmvK7qalLUXT6fr12FtVw+T7m2w5azwxshDuBQmRRbq7ZBJnY61i
KwIJVUy1U/tSE9LsN1McUQKBgQClc4ykeoRbj3sdcZ2GyrQru4pMzP6wNu3Xy5EH
HI6jaOi74ImCJDcY5/o/vjx7qb39qBJa5+TjliPOp5xlI5BSF7vOpV4G5XvdlsYO
XSYWRGxriBnzXzspV3/M4oPGMVAJgve7Fg9OGY4i2xx1yBH+geCf+CqnDt53ZHs7
YVz6gQKBgQDG42tZZ1kNAnOx/k1lUlZrEeF8iqdsyVcRf4fAvqsPbY3+kdae+8Or
+cQpVoeWzOQLUkA6eMsiTLmcWYb62qMgdpluyKoOciPG9+2AGNTvQp/ig34pF2F/
9OGuVYlA1p7mkP8Vb1Mo1ugVOzUqAIjHKiGUzBWVsxOZsGa+SY47uw==
-----END RSA PRIVATE KEY-----
```

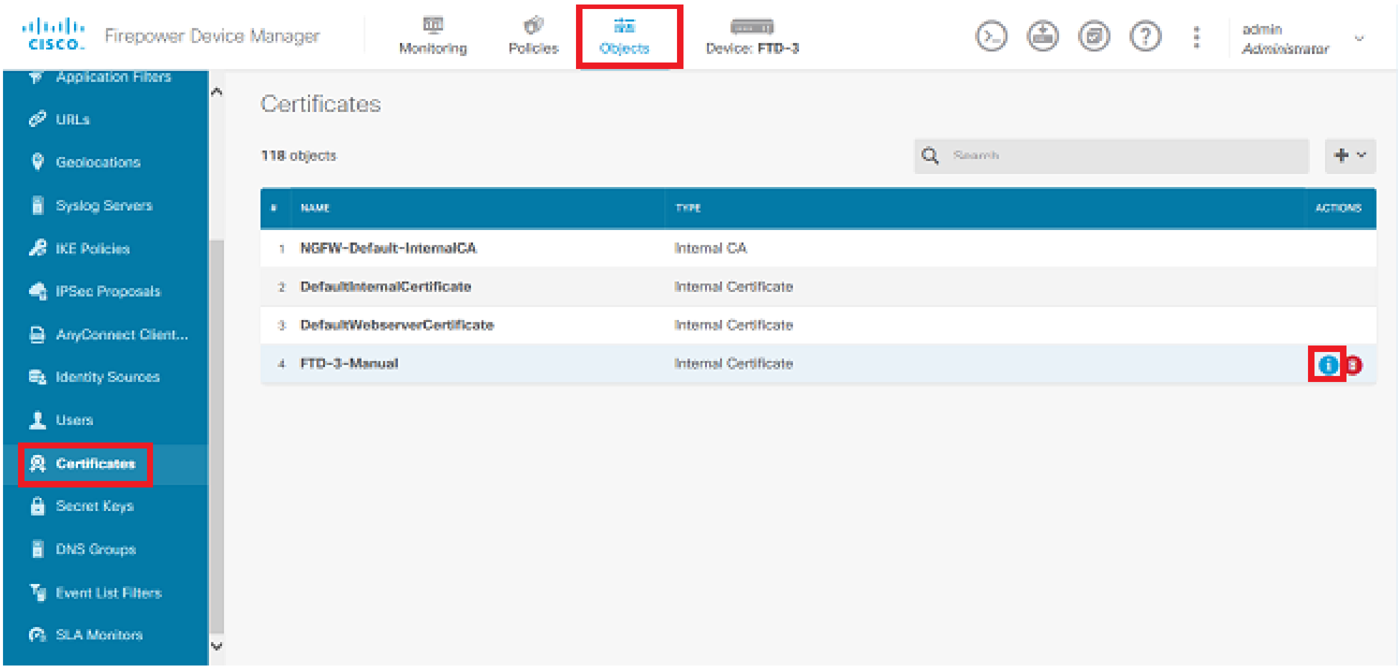
一旦私密金鑰未加密，您就可以上傳辨識與私密金鑰檔案，或複製並貼入FDM中（使用先前提及之「手動註冊」一節中的步驟3）。可以使用前面提到的受信任CA證書安裝步驟來安裝頒發CA。

驗證

使用本節內容，確認您的組態是否正常運作。

在FDM中檢視已安裝的憑證

1. 導航到對象>證書。將滑鼠懸停在要驗證的證書上，然後按一下view按鈕，如圖所示。

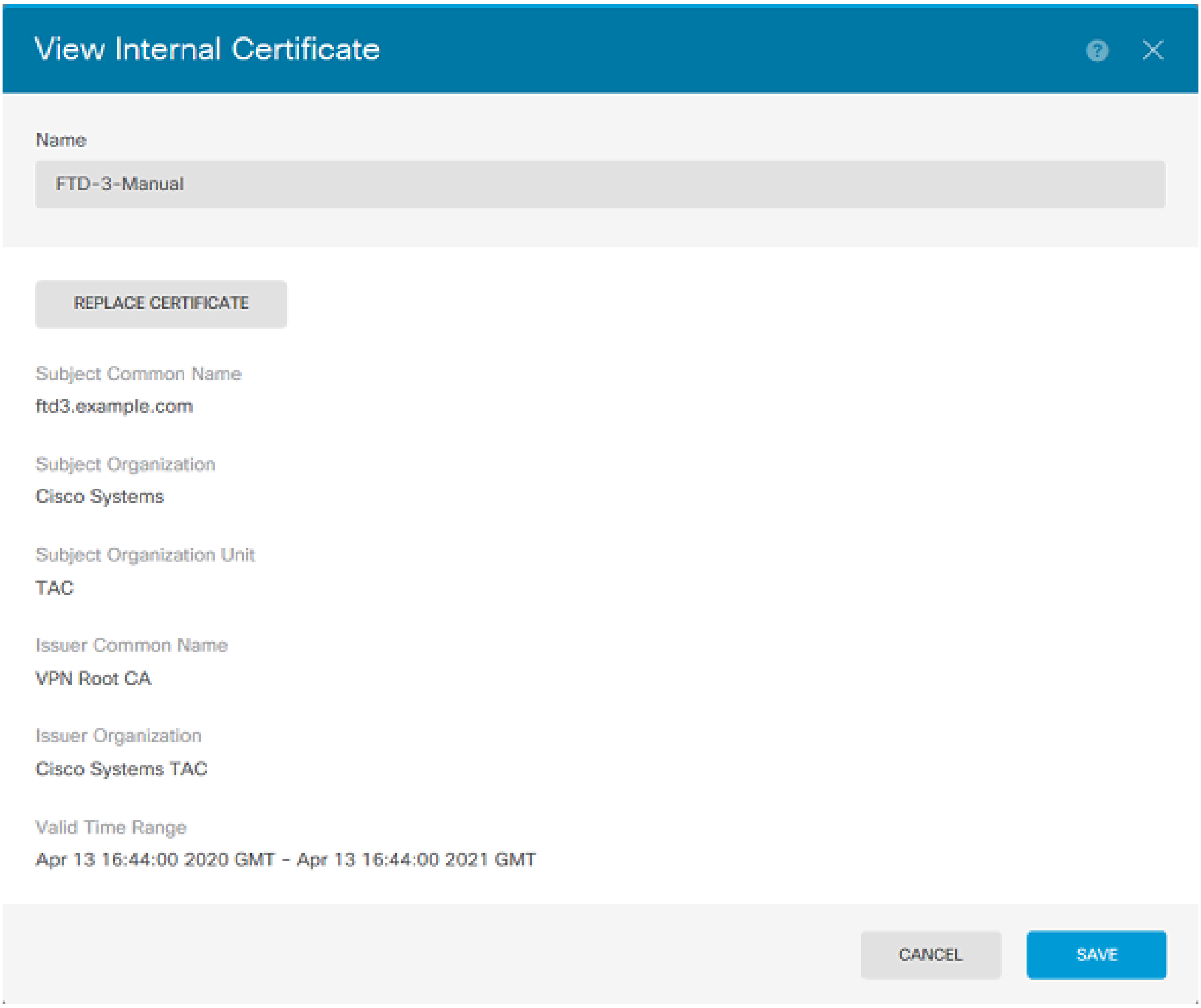


Certificates

118 objects

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Manual	Internal Certificate	

2. 快顯視窗提供憑證的其他詳細資訊，如下圖所示。



View Internal Certificate

Name

FTD-3-Manual

Subject Common Name
ftd3.example.com

Subject Organization
Cisco Systems

Subject Organization Unit
TAC

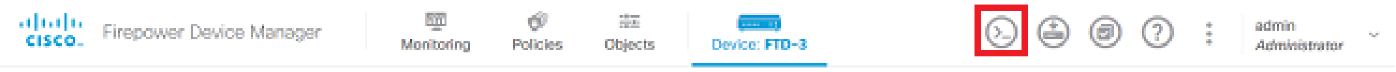
Issuer Common Name
VPN Root CA

Issuer Organization
Cisco Systems TAC

Valid Time Range
Apr 13 16:44:00 2020 GMT - Apr 13 16:44:00 2021 GMT

在CLI中檢視已安裝的證書

您可以使用FDM中的CLI控制檯或透過SSH登入到FTD，然後運行命令show crypto ca certificates以驗證證書是否已應用到裝置，如圖所示。



輸出範例：

```
> show crypto ca certificates

Certificate
  Status: Available
  Certificate Serial Number: 6b93e68471084505
  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=ftd3.example.com
    ou=TAC
    o=Cisco Systems
  Validity Date:
    start date: 16:44:00 UTC Apr 13 2020
    end   date: 16:44:00 UTC Apr 13 2021
  Storage: config
  Associated Trustpoints: FTD-3-Manual
```

注意：身份證書只有在CLI中與AnyConnect等服務一起使用時才會顯示。受信任的CA證書在部署後即會出現。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

調試命令

發生SSL憑證安裝失敗時，可以透過SSH連線FTD後，從診斷CLI執行偵錯：debug crypto ca 14

在FTD的舊版本中，以下調試是可用的，建議用於故障排除：

調試加密ca 255

debug crypto ca message 255

debug crypto ca transaction 255

常見問題

導入ASA導出的PKCS12

當您嘗試從OpenSSL中導出的ASA PKCS12中提取身份證書和私鑰時，您會收到類似如下所示的錯誤：

```
openssl pkcs12 -info -in asaexportedpkcs12.p12
6870300:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1220:
6870300:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:386:Type=PK
```

為了解決此問題，必須首先將pkcs12檔案轉換為DER格式：

```
openssl enc -base64 -d -in asaexportedpkcs12.p12 -out converted.pfx
```

完成此操作後，可按照本文檔前面部分的「從PKCS12檔案中提取身份證書和私鑰」部分中的步驟操作，以導入身份證書和私鑰。

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）。