

「Install and Renew Certificates on FTD Managed by FMC」

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[バックグラウンド](#)

[設定](#)

[証明書のインストール](#)

[自己署名証明書の登録](#)

[手動登録](#)

[PKCS12登録](#)

[証明書の更新](#)

[自己署名証明書の更新](#)

[証明書の手動更新](#)

[PKCS12更新](#)

[OpenSSLでのPKCS12の作成](#)

[確認](#)

[FMCでインストールされた証明書を表示する](#)

[CLIでのインストール済み証明書の表示](#)

[トラブルシューティング](#)

[デバッグコマンド](#)

[一般的な問題](#)

はじめに

このドキュメントでは、FMCによって管理されるFTDの証明書をインストール、信頼、および更新する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 証明書を手動で登録するには、信頼できるサードパーティCAにアクセスする必要があります。
- サードパーティCAベンダーの例としては、Entrust、Geotrust、GoDaddy、Thawte、VeriSignなどがあります。

- FTDのクロック時刻、日付、およびタイムゾーンが正しいことを確認します。証明書認証では、ネットワークタイムプロトコル(NTP)サーバを使用してFTDの時刻を同期することをお勧めします。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 6.5を実行するFMCv
- 6.5を実行するFTDv
- PKCS12の作成には、OpenSSLが使用されます

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド

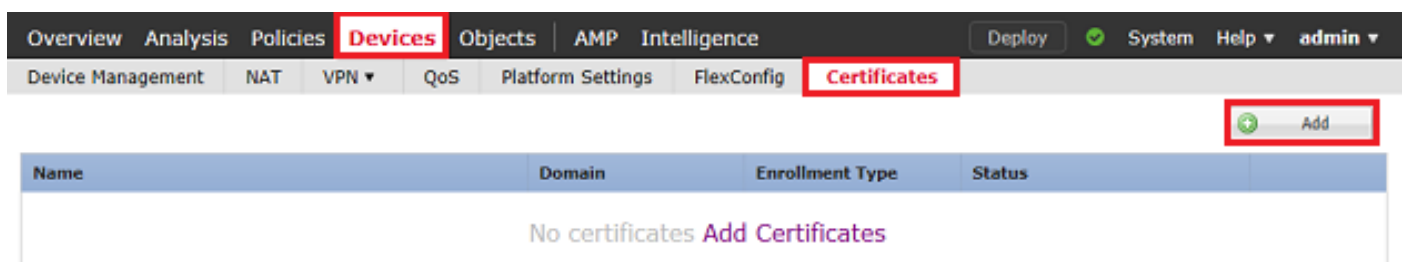
このドキュメントでは、Firepower Management Center(FMC)によって管理されるFirepower Threat Defense(FTD)上で、サードパーティの認証局(CA)または内部CAによって署名された自己署名証明書および証明書をインストール、信頼、および更新する方法について説明します。

設定

証明書のインストール

自己署名証明書の登録

1. Devices > Certificatesの順に移動し、図に示すようにAddをクリックします。




2. デバイスを選択すると、Device*ドロップダウンに証明書が追加されます。次に、図に示すように、緑色の+記号をクリックします。

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*: 

3. トラストポイントの名前を指定し、図に示すように、CA InformationタブでEnrollment Type: Self Signed Certificate を選択します。


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. Certificate Parametersタブで、証明書のCommon Nameを入力します。これは、図に示すよう

に、証明書が使用されるサービスのfqdnまたはIPアドレスと一致する必要があります。

Add Cert Enrollment

The screenshot shows the 'Add Cert Enrollment' dialog box with the 'Certificate Parameters' tab selected. The 'Name' field is 'FTD-1-Self-Signed'. The 'Common Name (CN)' field is highlighted with a red box and contains 'ftd1.example.com'. Other fields include 'Include FQDN' (Use Device Hostname as FQDN), 'Include Device's IP Address', 'Organization Unit (OU)' (Cisco Systems), 'Organization (O)' (TAC), 'Locality (L)', 'State (ST)', 'Country Code (C)' (Comma separated country codes), and 'Email (E)'. There is an unchecked checkbox for 'Include Device's Serial Number' and an unchecked checkbox for 'Allow Overrides'. 'Save' and 'Cancel' buttons are at the bottom right.

5. (オプション) Keyタブで、証明書に使用する秘密キーのタイプ、名前、およびサイズを指定できます。デフォルトでは、キーは名前が<Default-RSA-Key>でサイズが2048のRSAキーを使用しますが、図に示すように同じ秘密/公開キーペアを使用しないように、各証明書に一意の名前を使用することをお勧めします。

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.完了したら、図に示すように、SaveをクリックしてからAddをクリックします。

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

7.完了すると、自己署名証明書が図に表示されます。

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA ID

手動登録

1. Devices > Certificatesの順に移動し、図に示すようにAddをクリックします。


Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

2. Device*ドロップダウンで証明書を追加するデバイスを選択し、図に示すように緑色の+記号をクリックします。

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. トラストポイントの名前を指定し、CA InformationタブでEnrollment Type: Manualを選択します。ID証明書の署名に使用するCAのpem形式の証明書を入力します。この証明書が使用できないか、現時点で判明していない場合は、プレースホルダとしてCA証明書を追加し、ID証明書が発行されたら、図に示すように、この手順を繰り返して実際の発行元CAを追加します。

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*
-----BEGIN CERTIFICATE-----
MIIESzCCAjOgAwIBAgIIItsWeBSsr5QwDQYJKoZIhvcNAQELBQAw
MjEaMBgGA1UE
ChMRQ2lzY28gU3lzZdGVtcyBUQUxkFDASBgNVBAMTC1ZQTiBSb29
O1ENBMB4XDTIw
MDQwNTIzMjkwMFoXDTEwMDQwNTIzMjkwMFowOjEaMBgGA1UE
ChMRQ2lzY28gU3lz
dGVtcyBUQUxkHDAaBgNVBAMTE1ZQTiBjbnRlcm1lZGlhdGUgQ0E
wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCII/m7uyjRUoyjyob7sWS
AUVmnUMtovHen
9VbgjowZs0hVcig/Lp2YYuawWRJhW99nagUBYtMyvY744sRw7AK
AwlyROO1J6IT
Is5suK60Yryz7JG3eNDqAroqJg/VeDeAjprpCW0YhHHYXAI0s7GXjHI
S6nGIy/qP
SRcPLdqx4/aFXw+DONJYHLoE5FlsfknrOeketnbABjkAkmOauNpS
zN4FAISIk4
DU3yX7d31GD4BBhxI7IPsDH933AUm6zxntC9AxK6gHAY8/8pUPv

Allow Overrides

Save Cancel

4. Certificate Parametersタブで、証明書のCommon Nameを入力します。これは、図に示すように、証明書が使用されるサービスのfqdnまたはIPアドレスと一致する必要があります。

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

- (オプション) Keyタブで、証明書に使用する秘密キーのタイプ、名前、およびサイズをオプションで指定できます。デフォルトでは、キーは名前が<Default-RSA-Key>でサイズが2048のRSAキーを使用しますが、図に示すように同じ秘密/公開キーペアを使用しないように、各証明書に一意の名前を使用することをお勧めします。

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. Below this, there is a note: 'Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.' At the bottom left, the 'Allow Overrides' checkbox is also unchecked. At the bottom right, there are 'Save' and 'Cancel' buttons.

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. (オプション) Revocationタブで、Certificate Revocation List(CRL ; 証明書失効リスト)または Online Certificate Status Protocol(OCSP ; オンライン証明書状態プロトコル)の失効がチェックされ、設定できます。デフォルトでは、どちらのチェックボックスもオンになっていません (図を参照)。

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.完了したら、図に示すようにSaveをクリックしてからAddをクリックします。

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. 要求を処理した後、FMCはID証明書を追加するオプションを提示します。図に示すように、IDボタンをクリックします。

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. CSRが生成されたことを通知するウィンドウが表示されます。図に示すように、Yesをクリックします。

Warning

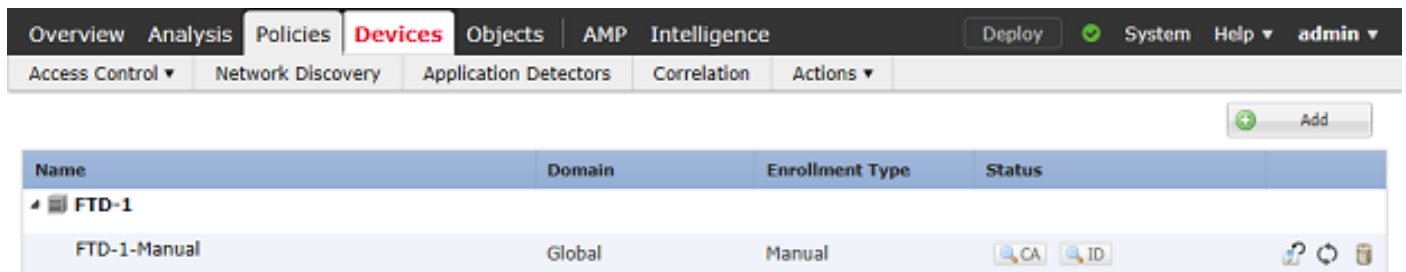
?
 This operation will generate Certificate Signing Request do you want to continue?

10. 次に、コピーしてCAに送信できるCSRが生成されます。CSRが署名されると、ID証明書が提

供されます。提供されたID証明書を参照して選択し、図に示すようにImportをクリックします。

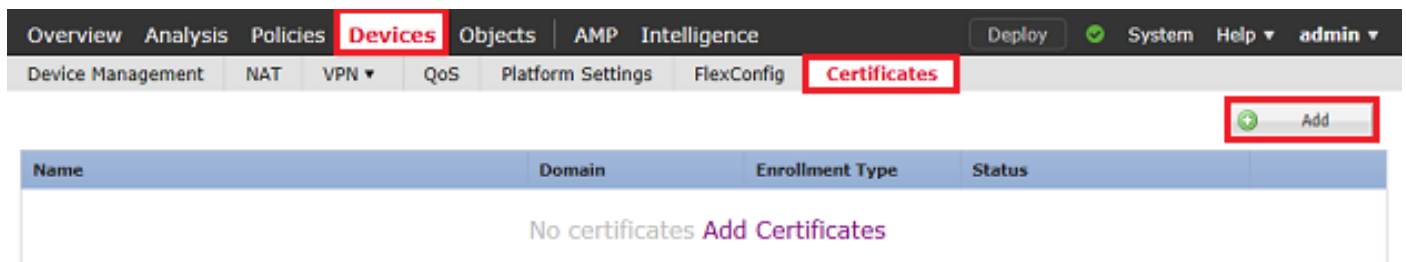


11.完了すると、次の図のように手動証明書が表示されます。



PKCS12登録

1.受信または作成したPKCS12ファイルをインストールするには、Devices > Certificatesに移動し、図に示すようにAddをクリックします。



2. Device*ドロップダウンで証明書を追加するデバイスを選択し、図に示すように緑色の+記号をクリックします。

Add New Certificate



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

Device*:

FTD-1

Cert Enrollment*:

Select a certificate enrollment object

Add

Cancel

3. トラストポイントの名前を指定し、CA InformationタブでEnrollment Type: PKCS12 Fileを選択します。作成したPKCS12ファイルを参照して選択します。図に示すように、PKCS12の作成時に使用するパスコードを入力します。

Add Cert Enrollment



Name*

FTD-1-PKCS12

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

PKCS12 File

PKCS12 File*:

PKCS12File.pfx

Browse PKCS12 File

Passphrase:

Allow Overrides

Save

Cancel

4. (オプション) Certificate ParametersタブとKeyタブは、PKCS12ですでに作成されているためグレー表示になりますが、CRLおよびOCSPの失効チェックを有効にするためのRevocationタブは変更できます。デフォルトでは、どちらのチェックボックスもオンになっていません(図を参照)。

Add Cert Enrollment

The screenshot shows the 'Add Cert Enrollment' dialog box with the 'Revocation' tab selected. The 'Name' field contains 'FTD-1-PKCS12'. The 'Description' field is empty. The 'Revocation' tab is active, showing the following options:

- 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: Gets OCSP URL from certificate if not provided
- Consider the certificate valid if revocation information can not be reached

At the bottom, there is an 'Allow Overrides' checkbox which is unchecked. The 'Save' and 'Cancel' buttons are visible at the bottom right.

5.完了したら、図に示すように、このウィンドウでSaveをクリックしてからAddをクリックします。

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-PKCS12

Enrollment Type: PKCS12 file

SCEP URL: NA

6.完了すると、PKCS12証明書は次の図のように表示されます。

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin			
Device Management NAT VPN QoS Platform Settings FlexConfig Certificates			
Add			
Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID

証明書の更新

自己署名証明書の更新

1.図に示すように、Re-enroll certificateボタンを押します。

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin			
Device Management NAT VPN QoS Platform Settings FlexConfig Certificates			
Add			
Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA ID Re-enroll

2.自己署名証明書を削除して置き換えるよう求めるウィンドウが表示されます。図に示すように、Yesをクリックします。

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.更新された自己署名がFTDにプッシュされます。これは、IDボタンをクリックして有効時間をチェックすると確認できます。

証明書の手動更新

1.図に示すように、Re-enroll certificateボタンを押します。

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

2.証明書署名要求が生成されたことを示すウィンドウが表示されます。図に示すように、Yesをクリックします。

Warning

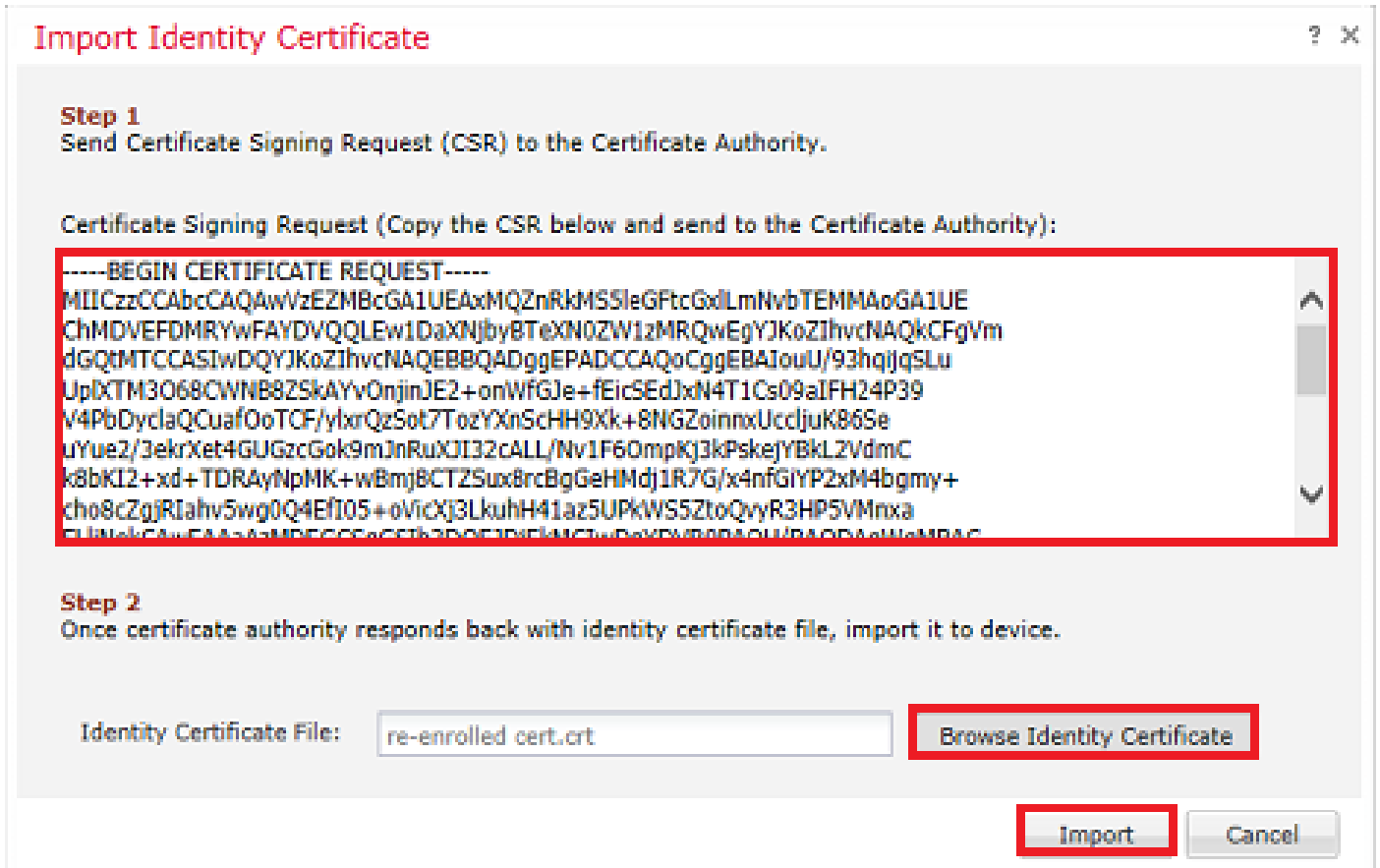


This operation will generate Certificate Signing Request do you want to continue?

Yes

No

3.このウィンドウでは、CSRが生成されます。このCSRは、前にID証明書に署名したのと同じCAにコピーして送信できます。CSRが署名されると、更新されたID証明書が提供されます。提供されたID証明書を参照して選択し、図に示すようにImportをクリックします。



4.更新された手動証明書がFTDにプッシュされます。これは、IDボタンをクリックして有効時間をチェックすると確認できます。

PKCS12更新

証明書の再登録ボタンをクリックしても、証明書は更新されません。PKCS12を更新するには、前述の方法を使用して新しいPKCS12ファイルを作成し、アップロードする必要があります。

OpenSSLでのPKCS12の作成

1. OpenSSLまたは同様のアプリケーションを使用して、秘密キーと証明書署名要求(CSR)を生成します。次の例は、OpenSSLで作成されたprivate.keyという名前の2048ビットRSAキーとftd1.csrという名前のCSRを示しています。

```
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.生成されたCSRをコピーしてCAに送信します。CSRが署名されると、ID証明書が提供されます。通常、CA証明書も提供されます。PKCS12を作成するには、OpenSSLで次のいずれかのコマンドを実行します。

PKCS12内で発行されたCA証明書のみを含めるには、次のコマンドを使用します。

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

- ftd.pfxは、opensslによってエクスポートされるpkcs12ファイル (der形式) の名前です。
- ftd.crtは、CAによってpem形式で発行された署名付きID証明書の名前です。
- private.keyはステップ1で作成したキーペアです。
- ca.crtは、pem形式の発行側の認証局(CA)の証明書です。

証明書がルートCAと1つ以上の中間CAを持つチェーンの一部である場合は、次のコマンドを使用してPKCS12にチェーン全体を追加できます。

```
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は、OpenSSLによってエクスポートされるpkcs12ファイル (der形式) の名前です。
- ftd.crtは、CAによってpem形式で発行された署名付きID証明書の名前です。
- private.keyはステップ1で作成したキーペアです。
- cachain.pemは、発行中間CAで始まり、pem形式のルートCAで終わるCA証明書をチェーンに含むファイルです。

PKCS7ファイル(.p7b、.p7c)が返された場合は、これらのコマンドを使用してPKCS12を作成することもできます。p7bがder形式の場合は、必ず-inform derを引数に追加してください。それ以外の場合は含めないでください。

```
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: *****
```

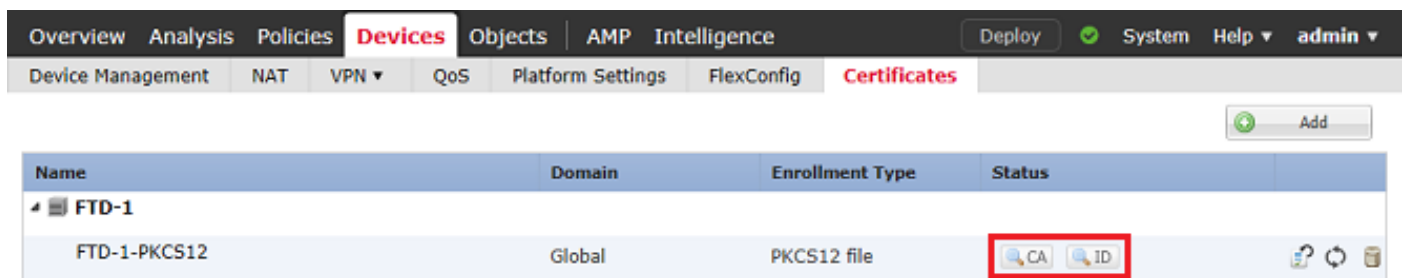
- ftd.p7bは、署名付きID証明書とCAチェーンを含むCAによって返されるPKCS7です。
- ftdpem.crtは変換後のp7bファイルです。
- ftd.pfxは、OpenSSLによってエクスポートされるpkcs12ファイル (der形式) の名前です。
- private.keyはステップ1で作成したキーペアです。

確認

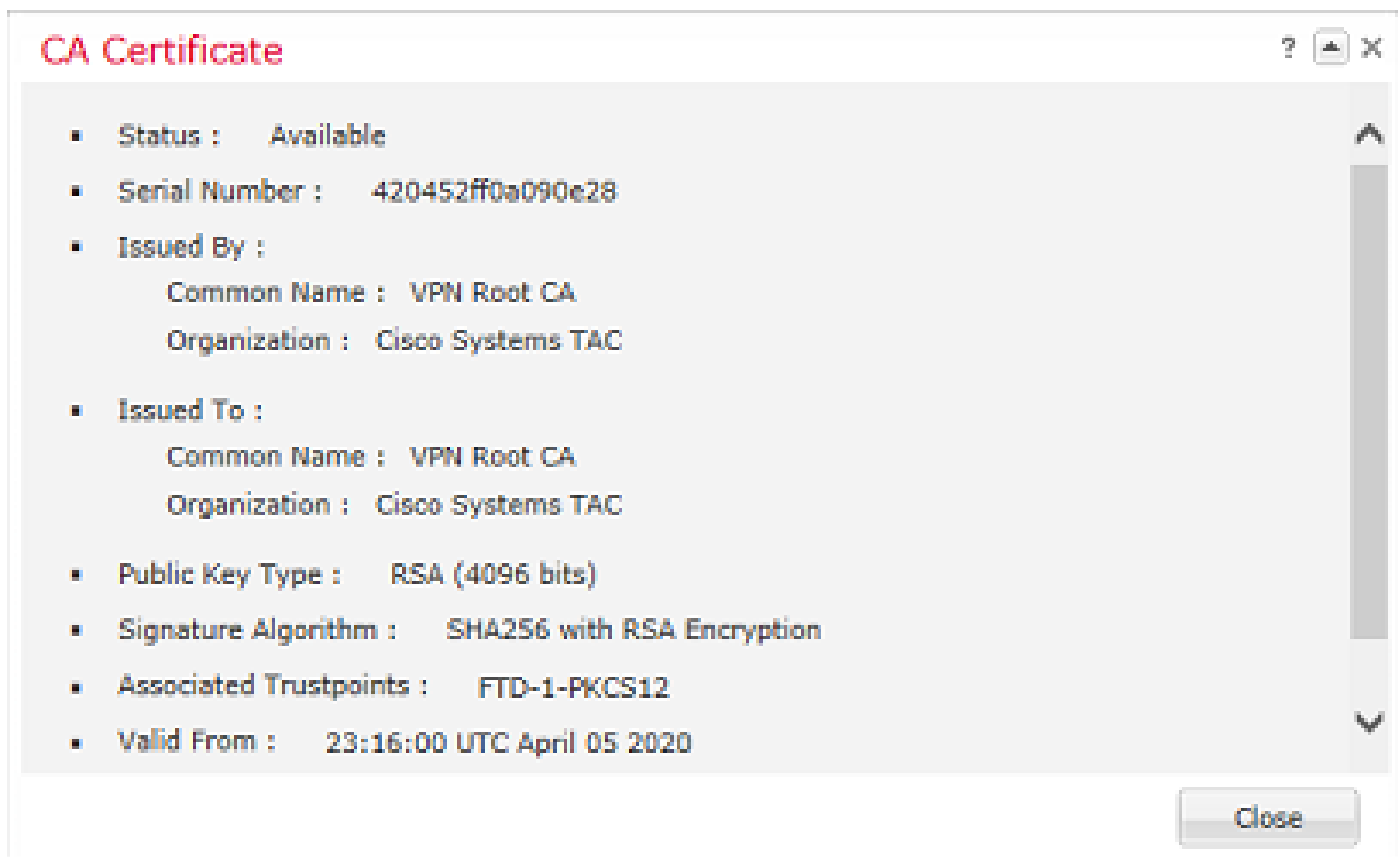
ここでは、設定が正常に機能しているかどうかを確認します。

FMCでインストールされた証明書を表示する

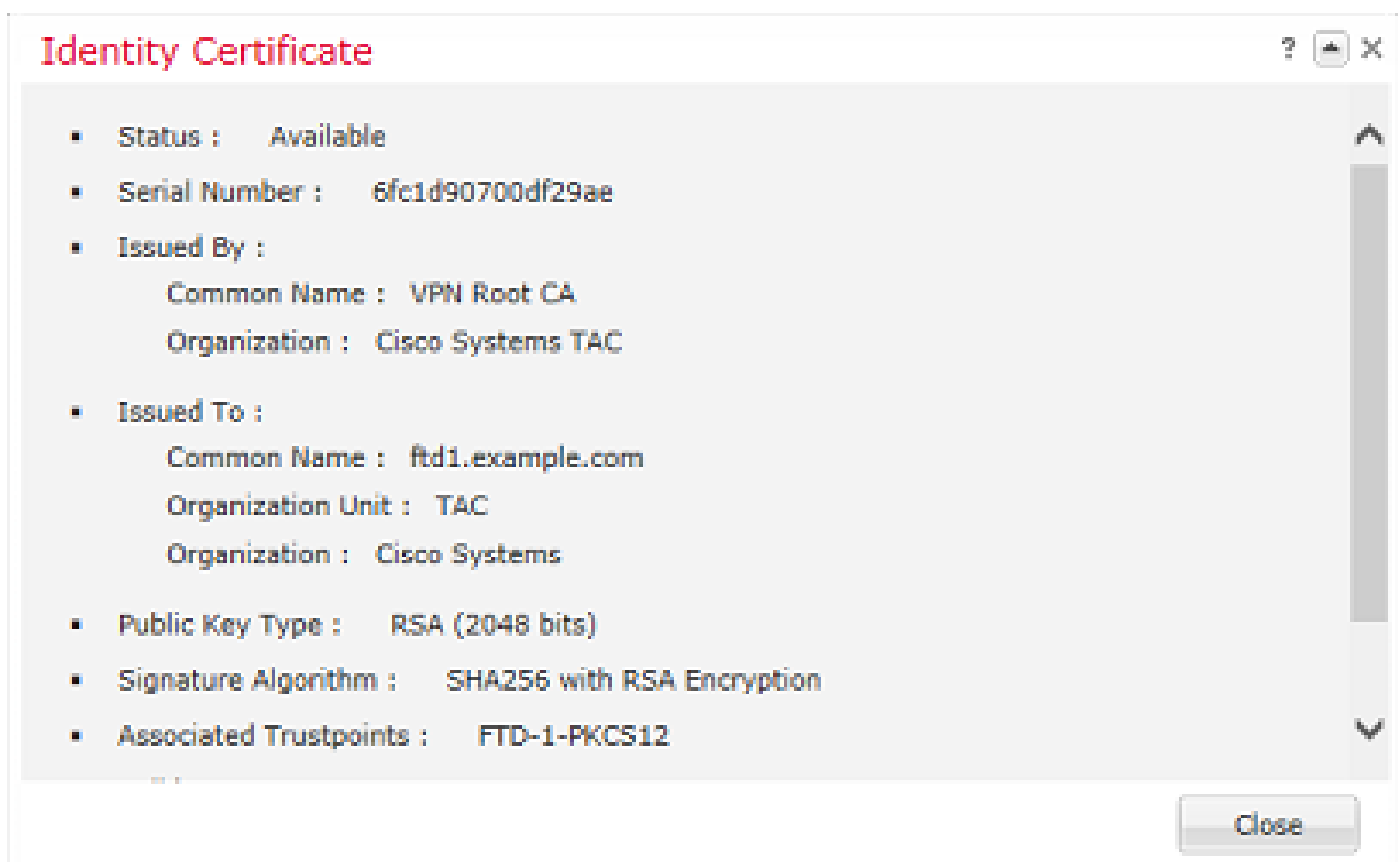
FMCで、Devices > Certificatesの順に移動します。該当するトラストポイントで、CAまたはIDをクリックすると、図に示すように、証明書の詳細が表示されます。



図に示すように、CA証明書を confirms します。



図に示すように、ID証明書を確認します。



CLIでのインストール済み証明書の表示

FTDにSSHで接続し、コマンドshow crypto ca certificateを入力します。

```
> 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
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

デバッグ コマンド

SSL証明書のインストールに失敗した場合、FTDがSSH経由で接続された後、診断CLIからデバッグを実行できます。

```
debug crypto ca 14
```

古いバージョンのFTDでは、次のデバッグが利用でき、トラブルシューティングに推奨されます。

。

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 255

一般的な問題

発行されたID証明書をインポートした後も、「ID証明書のインポートが必要です」というメッセージが表示されます。

これは、次の2つの問題が原因で発生する可能性があります。

1. 手動登録で発行側CA証明書が追加されなかった

ID証明書がインポートされると、手動登録時にCA Informationタブで追加されたCA証明書と照合されます。ネットワーク管理者が、ID証明書の署名に使用するCAのCA証明書を持っていない場合があります。この場合、手動登録を行う際には、プレースホルダCA証明書を追加する必要があります。ID証明書が発行され、CA証明書が提供されたら、正しいCA証明書を使用して新しい手動登録を行うことができます。手動登録ウィザードを再度実行する場合は、元の手動登録で行ったキーペアと同じ名前とサイズを指定してください。完了すると、CSRがCAに再度転送されるのではなく、以前に発行されたID証明書を、正しいCA証明書を使用して新しく作成されたトラストポイントにインポートできます。

同じCA証明書が手動登録時に適用されたかどうかを確認するには、「Verify」セクションで指定されているCAボタンをクリックするか、show crypto ca certificatesの出力を確認します。発行先やシリアル番号などのフィールドは、認証局から提供されるCA証明書内のフィールドと比較できます。

2. 作成されたトラストポイントのキーペアが、発行された証明書に対してCSRを作成するときに使用されるキーペアと異なる。

手動登録では、キーペアとCSRが生成されると、公開キーがCSRに追加され、発行済みID証明書に含まれるようになります。何らかの理由でFTDのキーペアが変更された場合、または発行されたID証明書に別の公開キーが含まれている場合、FTDは発行されたID証明書をインストールしません。これが発生しているかどうかを確認するには、2つの異なるテストがあります。

OpenSSLでは、次のコマンドを発行して、CSRの公開キーを発行済み証明書の公開キーと比較できます。

```
openssl req -noout -modulus -in ftd.csr
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C
C7CAD06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B
B966DA10BF24771CFE55327C5A14B96235E9
```

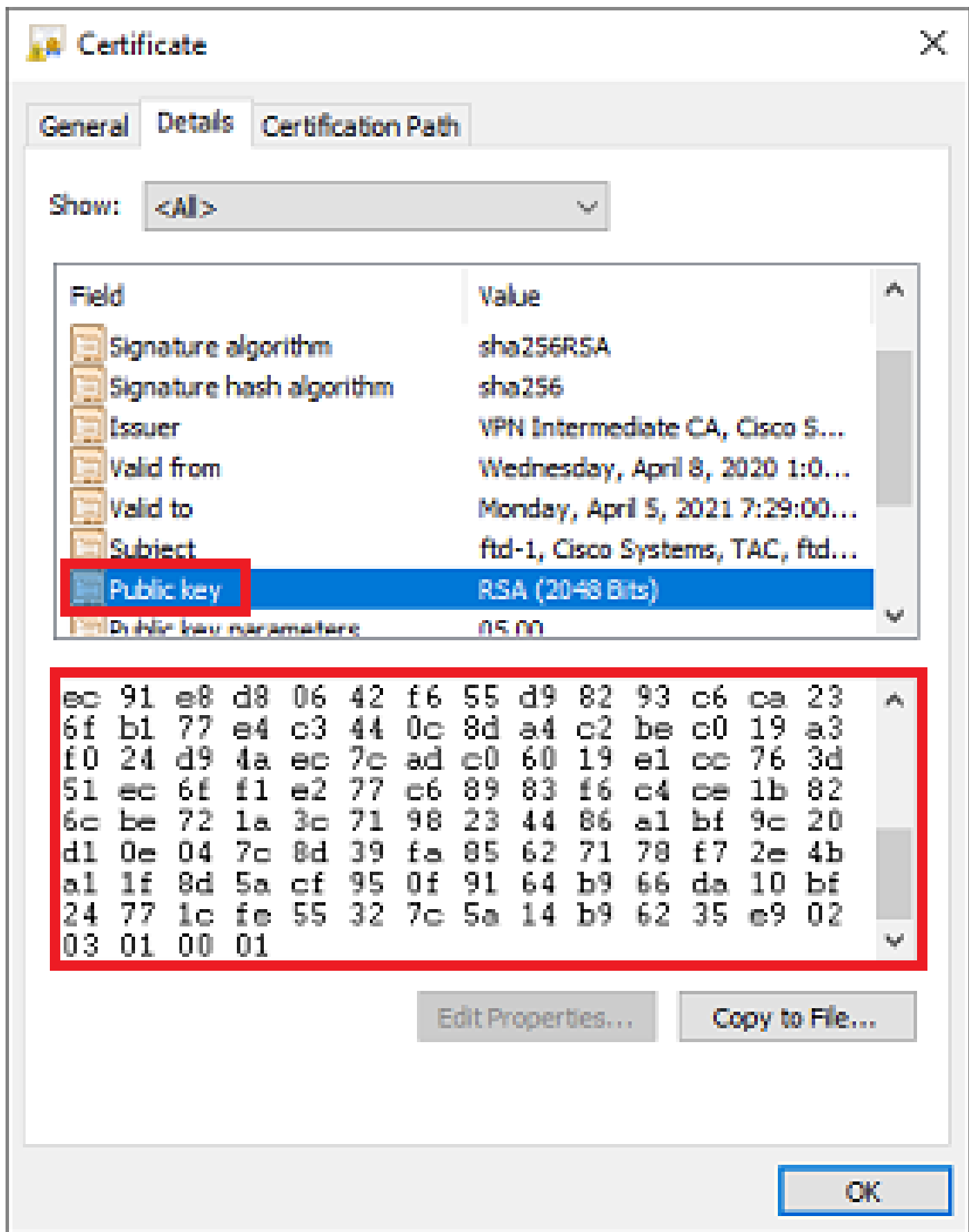
```
openssl x509 -noout -modulus -in id.crt
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
```

81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B
B966DA10BF24771CFE55327C5A14B96235E9

- ftd.csrは、手動登録時にFMCからコピーされるCSRです。
- id.crtは、CAによって署名されたID証明書です。

または、FTDの公開キーの値を、発行されたID証明書内の公開キーと比較することもできます。パディングが原因で、証明書の最初の文字がFTD出力の文字と一致しないことに注意してください。

Windows PCで開かれた発行済みID証明書：



ID証明書から抽出された公開キー出力：

```
f6e0fdfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b8af3a491b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8da4c2bec0e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f8d5acf955327c5a14b96235e90203010001
```

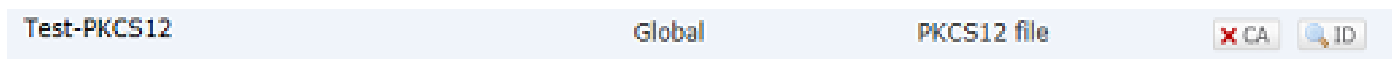
FTDからのshow crypto key mypubkey rsaの出力手動登録が行われると、<Default-RSA-Key>を使用してCSRが作成されました。太字の部分は、ID証明書から抽出された公開キーの出力と一致します。

```
> 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のCAの横の赤いX

これは、PKCS12登録で発生する可能性があります。これは、CA証明書がPKCS12パッケージに含まれていないためです。



これを修正するには、PKCS12にCA証明書を追加する必要があります。

ID証明書と秘密キーを抽出するには、次のコマンドを発行します。PKCS12の作成時に使用されるパスワードと保護された秘密キーが必要です。

```
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
ChMRQ2l2Yz8gU3lzdGVtcyBUQUUMxHDAaBgNVBAMTE1ZQTiBJbnR1cm1lZG1hdGUg
Q0EwHhcNMjAwNDA0MTY1ODAwWhcNMjEwNDA1MjMyOTAwWjAbMRkwFwYDVQQDExBm
dGQxLmV4Yw1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
043eLVP18K0jnYfHCBZuFUyRXTTB28Z1ouIJ5yYrDzCN781GFrHb/wCczRx/jW4n
pF9q2z7FHR5bQCI4oSUSX40UQfr0/uOK5riI1uZumPUx1Vp1zVkYuqDd/i1r0+0j
PyS7BmyGfV7aebYWZnr8R9ebDsnC2U3nKjP5RaE/wNdVGTs/180H1rIjMpcFMXps
LwxixiEz0hCmDm9RC+7uWZQd1wZ9oNANcbQC0px/Zikj9Dz70RhhbzBTeUNKD3p
sN3VqdDPvGZHFGLPcnhKYyZ79+6p+CHC8X8BFjuTJYoo116uGgiB4Jz2Y9ZeFSQz
Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBg1ghkgBhvCAQOEERYPeGnhIGN1
cnRpZmljYXR1MA0GCsQGSiB3DQEBcWUAA4IBAQCv/MgshWxXtwpwmMF/6KqEj8nB
S1jbfz1zNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRY54taRI27W+gLneCbQAux
9amxXuhpxP5E0hnc+tsYS9eriAKpHuS1Y/2uwn92fHIbh3HEXPO1HBJueI8PH3ZK
41rPKA9oIQPUW/uueHEF+xCbG4xCLi5H0GeHX+FTigGNqazaX5GM4RBUa4bk8jks
Ig53twvop71wE53COTH0EkSRCsVcW5mdJsd9BUZHjguhpw8Giv7Z36qWv18I/Owf
RhLhtsgenc25udglv9Sy5xK53a5Ieg8biRpWL9tIjgUgjxYZwtyVeHi32S7
-----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-----
MIIFDjBABGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI1KyWxk8cgTMCaggA
MBQGccqGSiB3DQMhBAgCm0qRKh/dcwSCBmiF7BpgJNIPhdU5Zorn1jm3pmsI/XkJ
MRHc1Ree10ziSLCZOStR84JFQxNpbThXLhshC9WhpPy5sNXIvXS7Gu+U10/V1NSA
rW1X6SPftAYiFq5QxyEutSHdZZwgQIqj97seu3Px0agvI0bw1Lo8or51SydnMjp
Ptv50Ko95BSHwWycqkTAia4ZKxytyIc/mIu5m72LucOFmoRB05JZu1avWXjbCAA+
k2ebkb1FT0YRQT1Z4tZHSqX1LFPZe170NZEUG7rIcWak1Yw7XNUPh0n6FHL/ieIZ
IhvIfj+IgQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E
Gnh8r31903A1kPMBkMdx0q1pzo2naIy2KGrUnOSHajVwclR9dTPWIDyjd95YoeS
IUE7Ma00pjJc02FNbWyxRrYt+4hp3aJt0ZW83FHiS1B5UIzGrBMAgKJc2Hb2RTV
9gxZGve1cRco1LeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShn0wHzridF8Zn
F06XvBDSyXVSpkxwAd1Twxq62tUnLIkyRXo2CSz8z8W29UXmF04o3G67n28//LJ
Ku8wj1jeq1vFgXSQiWLADNH772RNwzCMeobfxG1BprF9DPT8yvyBdQviUIuFpJ
nNs5FYbLTv9ygZ1S9xwQpTcqEu+y4F5BJuYlMhqcZ+VpFA4nM0YHhZ5M3sccRSR4
1L+a3BPJJsh1TIJQg0TixDaveCfpDcpS+ydUgS6YwY8xw17v0+1f7y5z1t4TkZrt
ItBHHA6yDzR0Cn0/ZH3y88a/asDcuw6bsRaY5iT8nAWGTQved3xXj+EgeRs25HB
dIBX5gTvqN7qDanhkaPUcEawj1/38M0pAYULei3e1fKKrhwaYsBFaV/BeUMWuNW
BmKprkKKQv/JdWnoJ149KcS4bfa3GHG9Xxnyvbg8HxopcYFMTEjao+wLZH9agqKe
Y0jyoHFN6ccBBC7vn7u12tmXOM5RcnPLmaDaBFDSBBFS8Y8VkeHn3P0q7+sEQ26d
vL807WdgLH/wKqovoJRyxwzz+TryRq9cd5BNyyLaABESa1sWRhk81C2P+B+Jdg9w
d6RsvJ2dt3pd1/+pUR3CdC0b8qRZOoL03+onUIUoEsCCndp0x8Yj/mvc6ReXtOKB
2qVmhVMYseiU1rOaQgt7XMe1UuiJ+dRnqcfAfbDGeOp+6epm1TK1BJL2ma1QWx51
73Qo4M7rR71aeq/dqob3o1PhcoMLa5z/Lo5vDe7S+LZMuAwjRkSfso0KQOY3kAP1
eZ2Eh2go4eJ7hHf5VFqBLL8Ci3rd3EOijRkNm3fAQmFJ1aFmooBM3Y2Ba+U8cMTH
1gjSFk11FAWpfxw9aSEECNCvEMm1Ghm6/tJDLV1jyTqawjHnWIZCc+P2AXgn1LzG
HVvfxs0c8FGUJJPQhatXYd7worWCxszaufJ99E4PaoZnAOYUFW2jaZEwo0NBpBD1
AjQ8aciuosv0FKpp/jXDI78/aYAEk662tPsfGmxvAWB+UMFarA9ZTiihK3x/tDPy
GZ6ByGWJYp/0tNNmJRCFhcAYY83EtzHK9h+8LatFA6WrJ4j3dhceUPzrPXjMffNN
0Yg=
-----END ENCRYPTED PRIVATE KEY-----
```

完了したら、「OpenSSLを使用したPKCS12の作成」のステップ2.で説明されている手順を使用

して、ID証明書と秘密キーを別々のファイルに入れ、CA証明書を新しいPKCS12ファイルにインポートできます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。