

# Installer et renouveler des certificats sur le FTD géré par FMC

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Fond](#)

[Configurer](#)

[Installation du certificat](#)

[Inscription auto-signée](#)

[Inscription manuelle](#)

[Inscription PKCS12](#)

[Renouvellement du certificat](#)

[Renouvellement de certificat auto-signé](#)

[Renouvellement manuel des certificats](#)

[Renouvellement PKCS12](#)

[Création PKCS12 avec OpenSSL](#)

[Vérifier](#)

[Afficher les certificats installés dans FMC](#)

[Afficher les certificats installés dans CLI](#)

[Dépannage](#)

[Commandes de débogage](#)

[Problèmes courants](#)

---

## Introduction

Ce document décrit comment installer, approuver et renouveler des certificats sur un FTD géré par FMC.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- L'inscription manuelle des certificats nécessite l'accès à une autorité de certification tierce approuvée.
- Les exemples de fournisseurs CA tiers incluent, sans s'y limiter, Entrust, Geotrust, GoDaddy, Thawte et VeriSign.

- Vérifiez que le FTD dispose de l'heure, de la date et du fuseau horaire corrects. Avec l'authentification de certificat, il est recommandé d'utiliser un serveur NTP (Network Time Protocol) pour synchroniser l'heure sur le FTD.

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FMCv 6.5
- FTDv 6.5
- Pour la création de PKCS12, OpenSSL est utilisé

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Fond

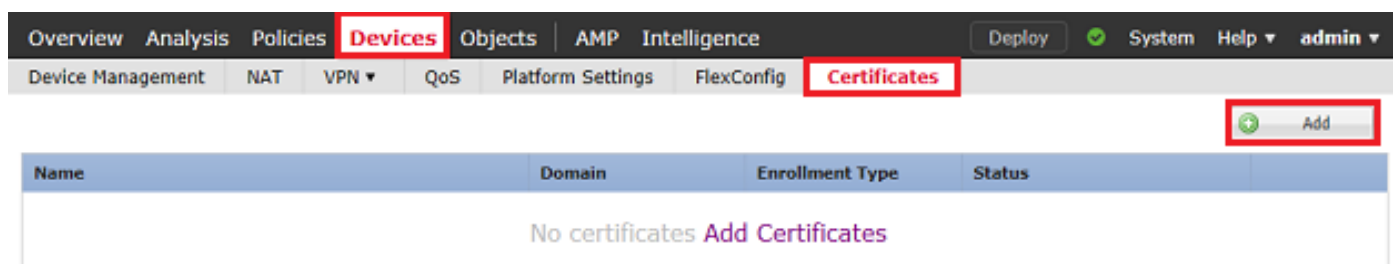
Ce document décrit comment installer, approuver et renouveler des certificats auto-signés et des certificats signés par une autorité de certification tierce ou une autorité de certification interne sur un pare-feu Firepower Threat Defense (FTD) géré par Firepower Management Center (FMC).

## Configurer

### Installation du certificat

#### Inscription auto-signée

1. Accédez à Périphériques > Certificats, puis cliquez sur Ajouter comme indiqué dans l'image.




2. Sélectionnez le périphérique et le certificat est ajouté à dans la liste déroulante Périphérique\*. Cliquez ensuite sur le symbole vert + comme illustré dans l'image.

### 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. Spécifiez un nom pour le point de confiance et sous l'onglet Informations sur l'autorité de certification, sélectionnez Type d'inscription : Certificat auto-signé comme indiqué dans l'image.


### Add Cert Enrollment ? X

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. Sous l'onglet Paramètres du certificat, entrez un nom commun pour le certificat. Elle doit

correspondre à l'adresse fqdn ou IP du service pour lequel le certificat est utilisé, comme indiqué dans l'image.

### Add Cert Enrollment

? X

The screenshot shows the 'Add Cert Enrollment' dialog box with the 'Certificate Parameters' tab selected. The 'Name\*' field contains 'FTD-1-Self-Signed'. The 'Description' field is empty. The 'Certificate Parameters' section includes the following fields:

- Include FQDN: Use Device Hostname as FQDN (dropdown menu)
- Include Device's IP Address: (empty text field)
- Common Name (CN): ftd1.example.com (text field, highlighted with a red border)
- Organization Unit (OU): Cisco Systems (text field)
- Organization (O): TAC (text field)
- Locality (L): (empty text field)
- State (ST): (empty text field)
- Country Code (C): Comma separated country codes (text field)
- Email (E): (empty text field)
- Include Device's Serial Number

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

5. (Facultatif) Sous l'onglet Key, le type, le nom et la taille de la clé privée utilisée pour le certificat peuvent être spécifiés. Par défaut, la clé utilise une clé RSA avec le nom <Default-RSA-Key> et une taille de 2048 ; cependant, il est recommandé d'utiliser un nom unique pour chaque certificat, afin qu'ils n'utilisent pas la même paire de clés privée/publique que celle illustrée dans l'image.

## 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. Une fois fait, cliquez sur Enregistrer, puis cliquez sur Ajouter comme indiqué dans l'image.

### 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. Une fois terminé, le certificat auto-signé s'affiche dans l'image.

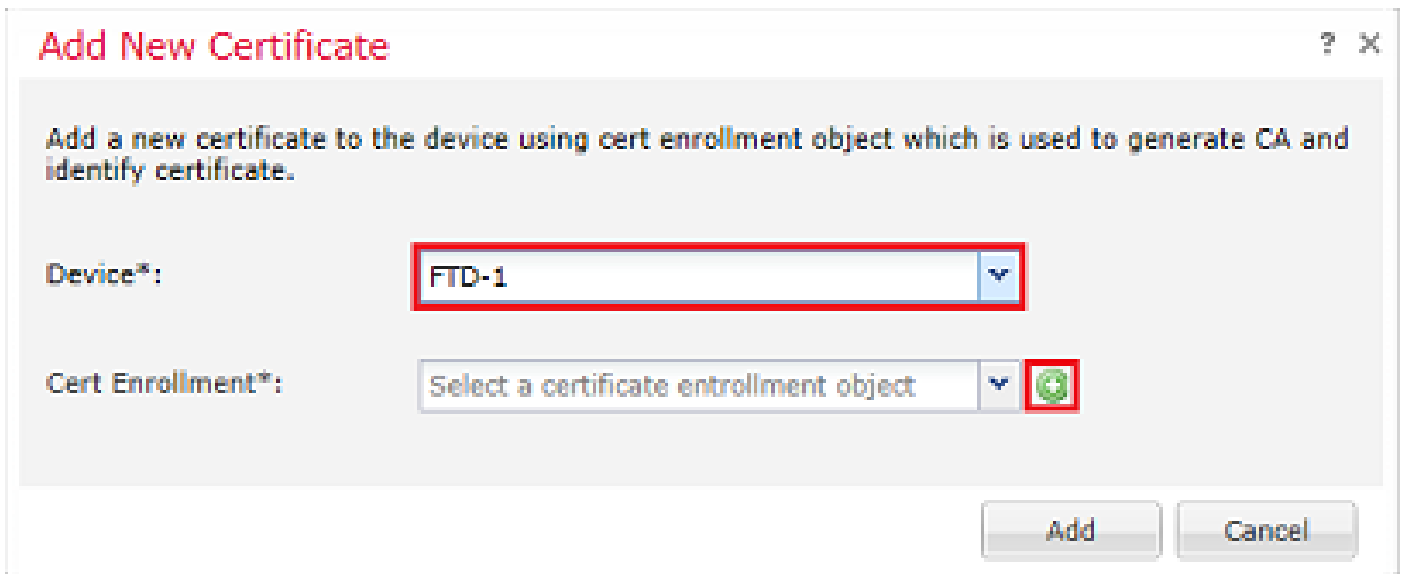
Overview Analysis Policies <b>Devices</b> Objects AMP Intelligence <span style="float: right;">Deploy System Help admin</span>			
Device Management NAT VPN QoS Platform Settings FlexConfig <b>Certificates</b>			
Add			
Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA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

### Inscription manuelle

1. Accédez à Périphériques > Certificats, puis cliquez sur Ajouter, comme indiqué dans l'image.

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. Sélectionnez le périphérique auquel le certificat est ajouté dans la liste déroulante Périphérique\*, puis cliquez sur le + symbole vert comme illustré dans l'image.



3. Spécifiez un nom pour le point de confiance et sous l'onglet Informations sur l'autorité de certification, sélectionnez Type d'inscription : Manuel. Saisissez le certificat de format pem de l'autorité de certification qui est utilisé pour signer le certificat d'identité. Si ce certificat n'est pas disponible ou connu à ce stade, ajoutez un certificat d'autorité de certification en tant qu'espace réservé et, une fois le certificat d'identité émis, répétez cette étape pour ajouter l'autorité de certification émettrice réelle, comme indiqué dans l'image.

## Add Cert Enrollment



Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:\*  
-----BEGIN CERTIFICATE-----  
MIIESzCCAjOgAwIBAgIIIItsWeBSsr5QwDQYJKoZIhvcNAQELBQAw  
MjEaMBgGA1UE  
ChMRQ2lzY28gU3lzdGVtcyBUQUxhZDAsBgNVBAMTC1ZQTiBSb29  
O1ENBMB4XDTIw  
MDQwNTIzMjkwMFoXDTEwMDQwNTIzMjkwMFowOjEaMBgGA1UE  
ChMRQ2lzY28gU3lz  
dGVtcyBUQUxhZDAsBgNVBAMTE1ZQTiBjb3RlcmlZGldGUGuQ0E  
wggEIMA0GCSqG  
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCII/m7uyjRUoyjyob7sWS  
AUVmnUMtovHen  
9VbgjowZs0hVcig/Lp2YyuawWRJhW99nagUBYTMyvY744sRw7AK  
AwlyROO1J6IT  
Is5suK60Yryz7JG3eNDqAroqJg/VeDeAjprpCW0YhHHYXAI0s7GXjHI  
S6nGIy/qP  
SRcPLdqx4/aFXw+DONJYHL0e5FIsfknrOeketnbABjkAkmOauNpS  
zN4FAISIk4  
DU3yX7d31GD4BBhxI7IPsDH933AUm6zxntC9AxK6gHAY8/8pUPv

Allow Overrides

Save Cancel

4. Sous l'onglet Paramètres du certificat, entrez un nom commun pour le certificat. Elle doit correspondre à l'adresse fqdn ou IP du service pour lequel le certificat est utilisé, comme indiqué dans l'image.



## 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. (Facultatif) Sous l'onglet Clé, le type, le nom et la taille de la clé privée utilisée pour le certificat peuvent éventuellement être spécifiés. Par défaut, la clé utilise une clé RSA avec le nom <Default-RSA-Key> et une taille de 2048 ; cependant, il est recommandé d'utiliser un nom unique pour chaque certificat afin qu'ils n'utilisent pas la même paire de clés privée/publique comme illustré dans l'image.

## Add Cert Enrollment

? X

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. (Facultatif) Sous l'onglet Revocation, la révocation de la liste de révocation de certificats (CRL) ou du protocole Online Certificate Status Protocol (OCSP) est cochée et peut être configurée. Par défaut, aucune des deux options n'est cochée comme illustré dans l'image.

## Add Cert Enrollment



Name\*

Description

CA Information Certificate Parameters Key **Revocation**

Enable Certificate Revocation Lists (CRL)

Use CRL distribution point from the certificate

Use 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. Une fois fait, cliquez sur Enregistrer, puis cliquez sur Ajouter comme indiqué dans l'image.

### 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. Après avoir traité la demande, FMC vous propose d'ajouter un certificat d'identité. Cliquez sur le bouton ID comme illustré dans l'image.

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-Manual	Global	Manual	Identity certificate import required

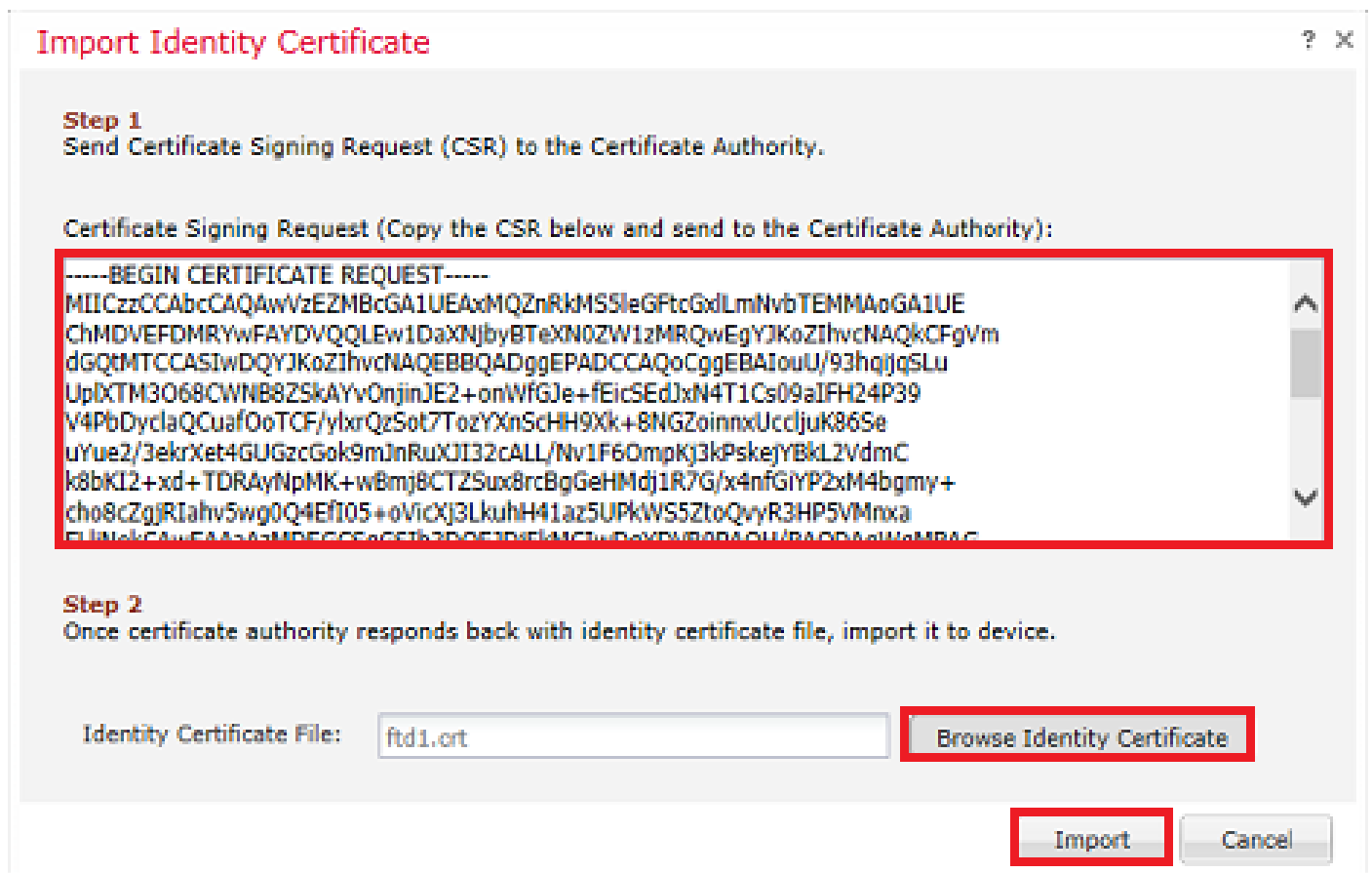
9. Une fenêtre s'affiche pour vous informer qu'un CSR est généré. Cliquez sur Yes comme indiqué dans l'image.

## Warning

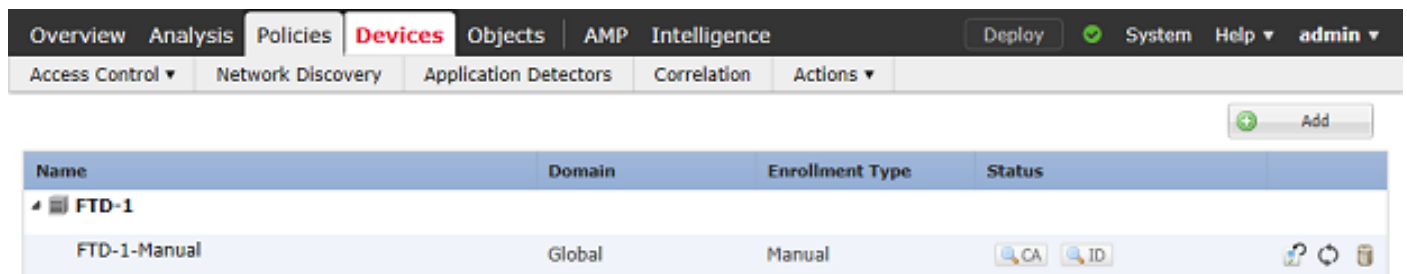
This operation will generate Certificate Signing Request do you want to continue?

10. Ensuite, un CSR est généré et peut être copié et envoyé à une autorité de certification. Une

fois le CSR signé, un certificat d'identité est fourni. Recherchez le certificat d'identité fourni et sélectionnez-le, puis cliquez sur Importer, comme indiqué dans l'image.

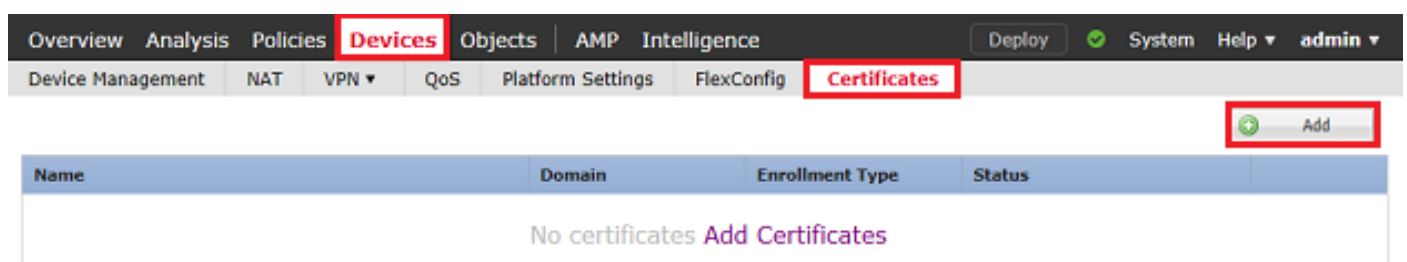


11. Une fois terminé, le certificat manuel s'affiche comme dans l'image.



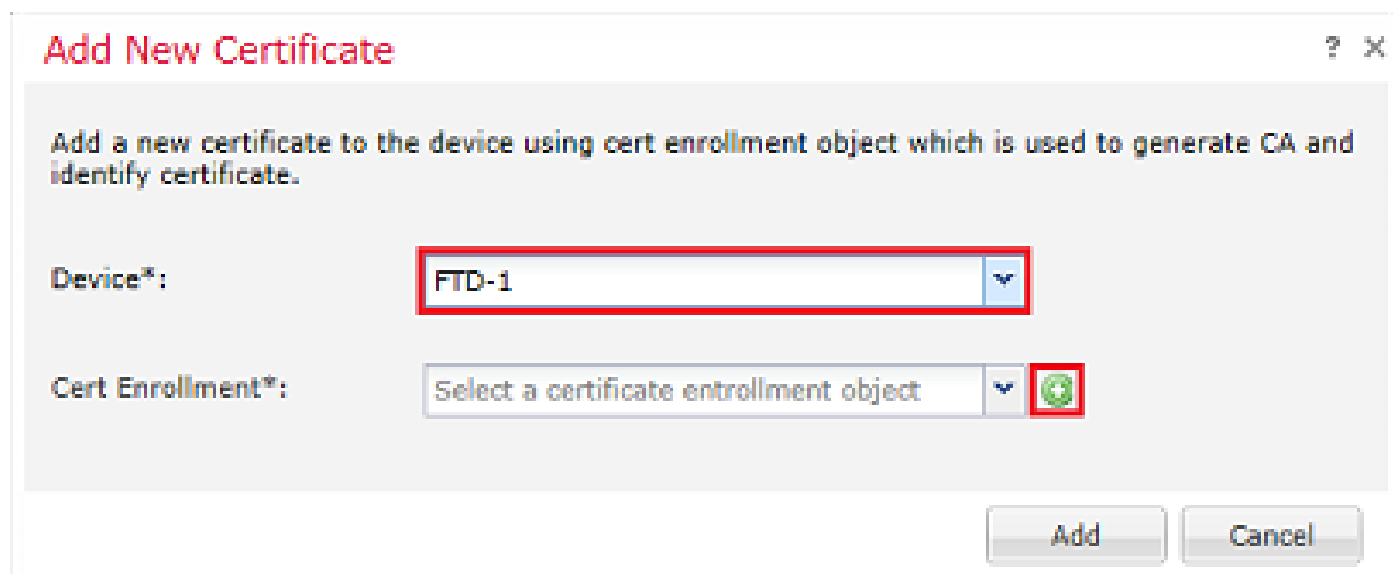
## Inscription PKCS12

1. Afin d'installer un fichier PKCS12 reçu ou créé, naviguez vers Devices > Certificates puis cliquez sur Add comme indiqué dans l'image.



2. Sélectionnez le périphérique auquel le certificat est ajouté dans la liste déroulante

Périphérique\*, puis cliquez sur le + symbole vert comme illustré dans l'image.



**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\*: FTD-1

Cert Enrollment\*: Select a certificate enrollment object

Add Cancel

3. Spécifiez un nom pour le point de confiance et sous l'onglet Informations sur l'autorité de certification, sélectionnez Type d'inscription : Fichier PKCS12. Recherchez le fichier PKCS12 créé et sélectionnez-le. Saisissez le code secret utilisé lors de la création de PKCS12, comme illustré dans l'image.

## Add Cert Enrollment



Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

PKCS12 File\*:

Passphrase:

Allow Overrides

4. (Facultatif) Les onglets Certificate Parameters et Key sont grisés car ils sont déjà créés avec PKCS12. Cependant, l'onglet Revocation pour activer la vérification de la révocation de la liste de révocation de certificats et/ou de la révocation du protocole OCSP peut être modifié. Par défaut, aucune des deux options n'est cochée comme illustré dans l'image.

## 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

5. Une fois fait, cliquez sur Enregistrer, puis cliquez sur Ajouter sur cette fenêtre comme indiqué dans l'image.



### 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

**Add**

6. Une fois terminé, le certificat PKCS12 s'affiche comme illustré dans l'image.

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID

## Renouvellement du certificat

### Renouvellement de certificat auto-signé

1. Appuyez sur le bouton Réinscrire le certificat comme illustré dans l'image.

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA ID <b>?</b>

2. Une fenêtre vous invite à supprimer et à remplacer le certificat auto-signé. Cliquez sur Yes comme indiqué dans l'image.

## 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. Une nouvelle signature automatique est envoyée au FTD. Cela peut être vérifié lorsque vous cliquez sur le bouton ID et que vous cochez la case Valid time.

### Renouvellement manuel des certificats

1. Appuyez sur le bouton Réinscrire le certificat comme illustré dans l'image.

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

2. Une fenêtre vous invite à générer une demande de signature de certificat. Cliquez sur Yes comme indiqué dans l'image.

## Warning

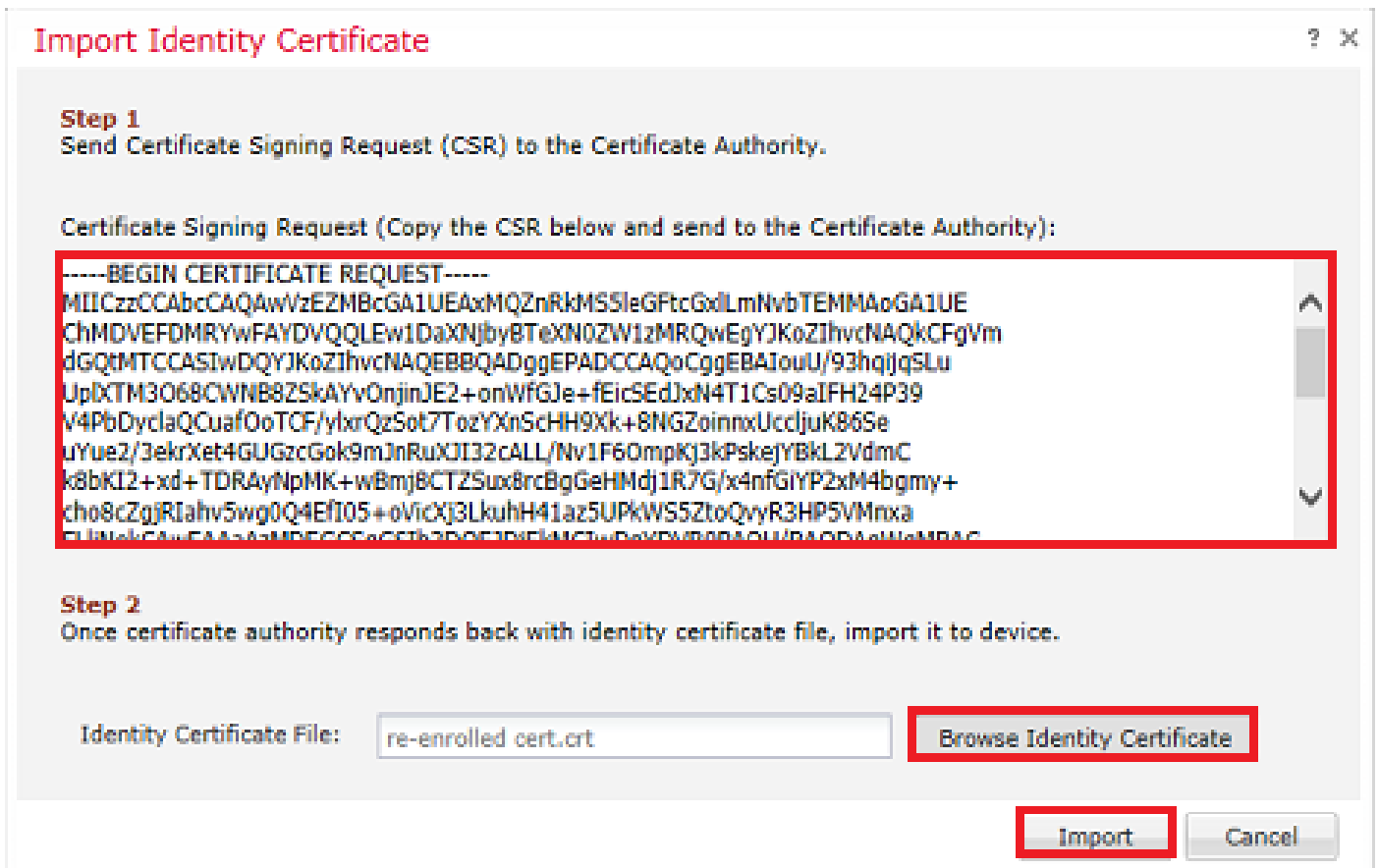


This operation will generate Certificate Signing Request do you want to continue?

Yes

No

3. Dans cette fenêtre, un CSR est généré qui peut être copié et envoyé à la même autorité de certification qui a signé le certificat d'identité précédemment. Une fois le CSR signé, le certificat d'identité renouvelé est fourni. Recherchez le certificat d'identité fourni et sélectionnez-le, puis cliquez sur Importer, comme indiqué dans l'image.



4. Un certificat manuel renouvelé est envoyé au FTD. Cela peut être vérifié lorsque vous cliquez sur le bouton ID et que vous cochez la case Valid time.

## Renouvellement PKCS12

Si vous cliquez sur le bouton Réinscrire le certificat, il ne renouvelle pas le certificat. Afin de renouveler un fichier PKCS12, un nouveau fichier PKCS12 doit être créé et téléchargé à l'aide des méthodes mentionnées précédemment.

## Création PKCS12 avec OpenSSL

1. Avec l'utilisation d'OpenSSL ou d'une application similaire, générez une clé privée et une demande de signature de certificat (CSR). Cet exemple montre une clé RSA de 2048 bits nommée private.key et un CSR nommé ftd1.csr qui est créé dans OpenSSL :

```
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 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. Copiez le CSR généré et envoyez-le à une autorité de certification. Une fois le CSR signé, un certificat d'identité est fourni. Généralement, le ou les certificats d'autorité de certification sont également fournis. Afin de créer un PKCS12, exécutez l'une de ces commandes dans OpenSSL :

Afin d'inclure uniquement le certificat CA émis dans le PKCS12, utilisez cette commande :

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

- ftd.pfx est le nom du fichier pkcs12 (au format der) qui est exporté par openssl.
- ftd.crt est le nom du certificat d'identité signé émis par l'autorité de certification au format pem.
- private.key est la paire de clés créée à l'étape 1.
- ca.crt est le certificat de l'autorité de certification émettrice au format pem.

Si le certificat fait partie d'une chaîne avec une autorité de certification racine et une ou plusieurs autorités de certification intermédiaires, cette commande peut être utilisée pour ajouter la chaîne complète dans le PKCS12 :

```
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 est le nom du fichier pkcs12 (au format der) qui est exporté par OpenSSL.
- ftd.crt est le nom du certificat d'identité signé émis par l'autorité de certification au format pem.
- private.key est la paire de clés créée à l'étape 1.
- cachain.pem est un fichier qui contient les certificats d'autorité de certification dans la chaîne qui commencent par l'autorité de certification intermédiaire émettrice et se terminent par l'autorité de certification racine au format pem.

Si un fichier PKCS7 (.p7b, .p7c) est retourné, ces commandes peuvent également être utilisées pour créer le PKCS12. Si le p7b est au format der, assurez-vous d'ajouter -inform der aux arguments, sinon ne l'incluez pas :

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

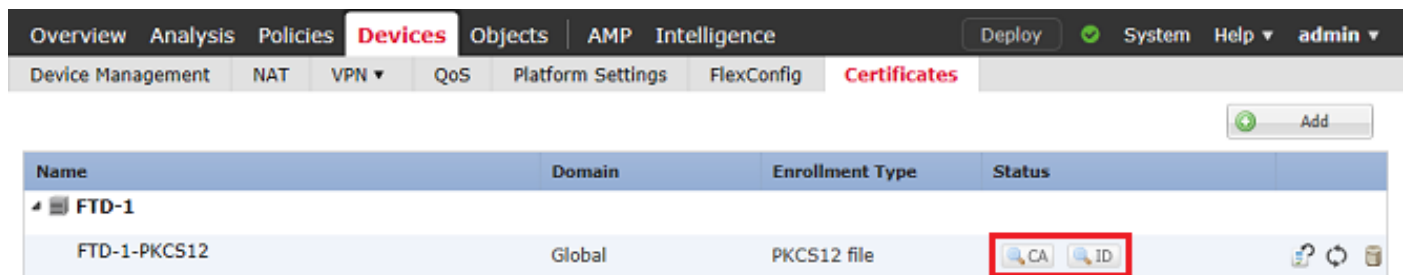
- ftd.p7b est le PKCS7 renvoyé par l'autorité de certification contenant le certificat d'identité signé et la chaîne de l'autorité de certification.
- ftdpem.crt est le fichier p7b converti.
- ftd.pfx est le nom du fichier pkcs12 (au format der) qui est exporté par OpenSSL.
- private.key est la paire de clés créée à l'étape 1.

## Vérifier

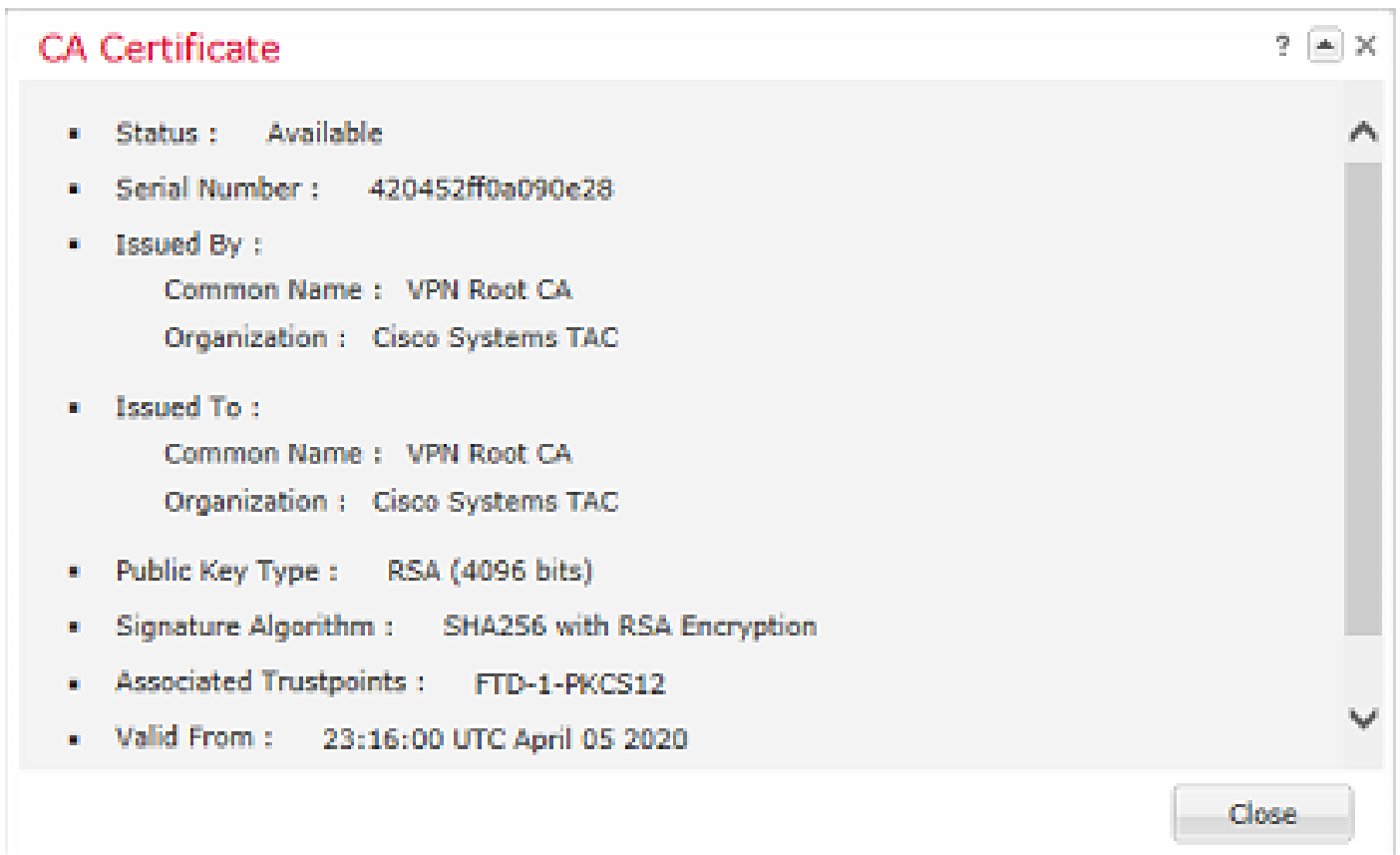
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

### Afficher les certificats installés dans FMC

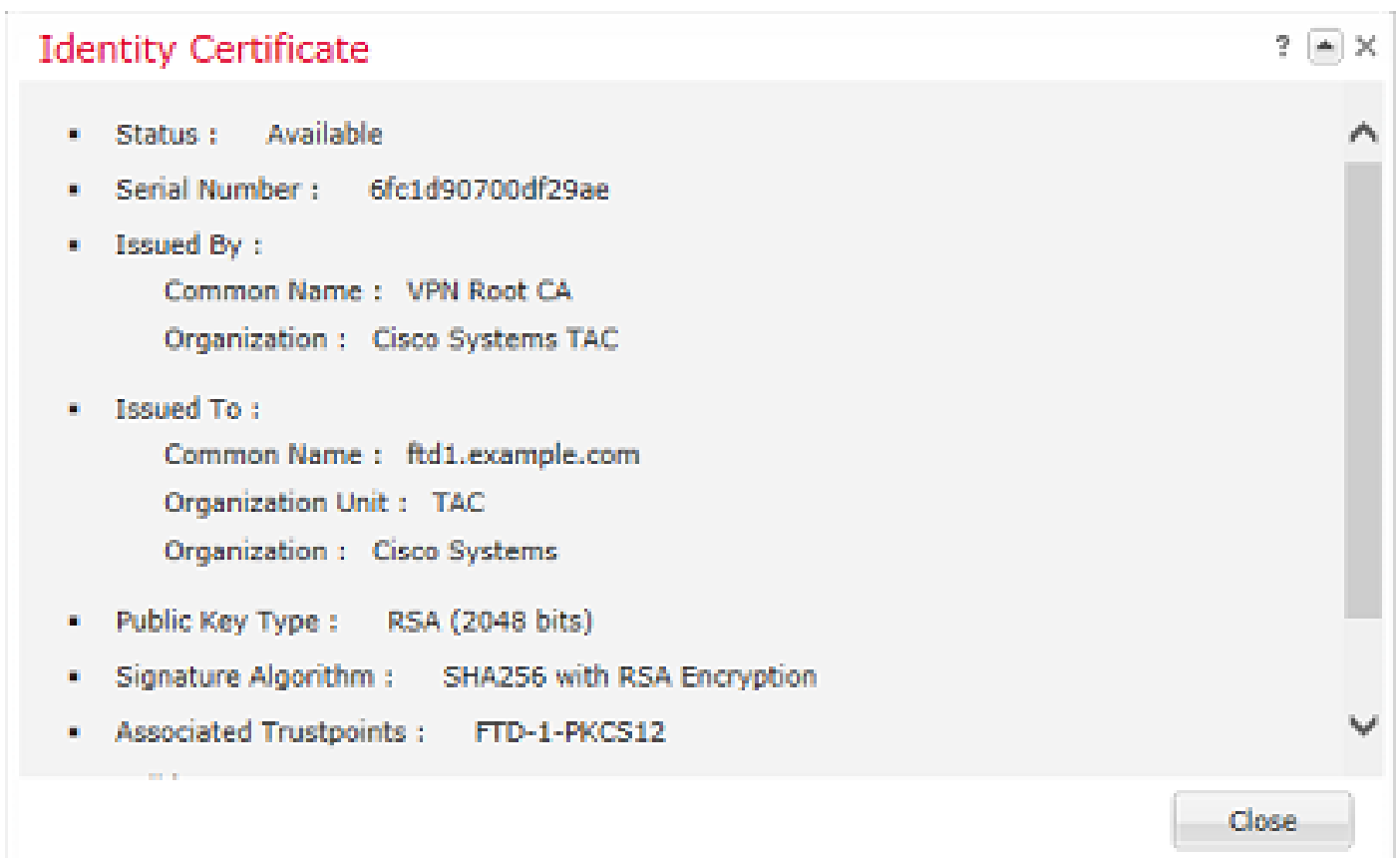
Dans FMC, accédez à Périphériques > Certificats. Pour le point de confiance approprié, cliquez sur l'AC ou l'ID pour afficher plus de détails sur le certificat comme indiqué dans l'image.



Vérifiez le certificat CA comme indiqué dans l'image.



Vérifiez le certificat d'identité comme indiqué dans l'image.



Afficher les certificats installés dans CLI

Envoyez SSH au FTD et entrez la commande 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
```

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

### Commandes de débogage

Les débogages peuvent être exécutés à partir de l'interface de ligne de commande de diagnostic après la connexion du FTD via SSH en cas d'échec de l'installation du certificat SSL :

```
debug crypto ca 14
```

Dans les versions antérieures de FTD, ces débogages sont disponibles et recommandés pour le dépannage :

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 25

## Problèmes courants

Le message « Identity certificate import required » (Importation de certificat d'identité requise) s'affiche toujours après l'importation du certificat d'identité émis.

Cela peut se produire en raison de deux problèmes distincts :

### 1. Le certificat de CA émetteur n'a pas été ajouté lors de l'inscription manuelle

Lorsque le certificat d'identité est importé, il est comparé au certificat d'autorité de certification ajouté sous l'onglet Informations sur l'autorité de certification lors de l'inscription manuelle. Parfois, les administrateurs réseau ne disposent pas du certificat d'autorité de certification utilisé pour signer leur certificat d'identité. Dans cette situation, il est nécessaire d'ajouter un certificat CA d'espace réservé lorsque vous effectuez une inscription manuelle. Une fois que le certificat d'identité a été émis et que le certificat CA a été fourni, une nouvelle inscription manuelle peut être effectuée avec le certificat CA correct. Lorsque vous parcourez à nouveau l'assistant d'inscription manuelle, veillez à spécifier le même nom et la même taille pour la paire de clés que lors de l'inscription manuelle d'origine. Une fois cette opération effectuée, au lieu de transmettre à nouveau le CSR à l'autorité de certification, le certificat d'identité précédemment émis peut être importé dans le point de confiance nouvellement créé avec le certificat d'autorité de certification correct.

Pour vérifier si le même certificat CA a été appliqué lors de l'inscription manuelle, cliquez sur le bouton CA comme spécifié dans la section Vérifier ou vérifiez la sortie de show crypto ca certificates. Les champs tels que Délivré à et Numéro de série peuvent être comparés aux champs du certificat CA fourni par l'autorité de certification.

### 2. La paire de clés dans le point de confiance créé est différente de la paire de clés utilisée lorsque le CSR est créé pour le certificat émis.

Avec l'inscription manuelle, lorsque la paire de clés et le CSR sont générés, la clé publique est ajoutée au CSR afin qu'elle puisse être incluse dans le certificat d'identité émis. Si, pour une raison quelconque, la paire de clés du FTD est modifiée ou si le certificat d'identité émis inclut une clé publique différente, le FTD n'installe pas le certificat d'identité émis. Pour vérifier si cela s'est produit, il existe deux tests différents :

Dans OpenSSL, ces commandes peuvent être émises pour comparer la clé publique dans le CSR à la clé publique dans le certificat émis :

```
openssl req -noout -modulus -in ftd.csr
```

```
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEB096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
```



```
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C  
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B  
B966DA10BF24771CFE55327C5A14B96235E9
```

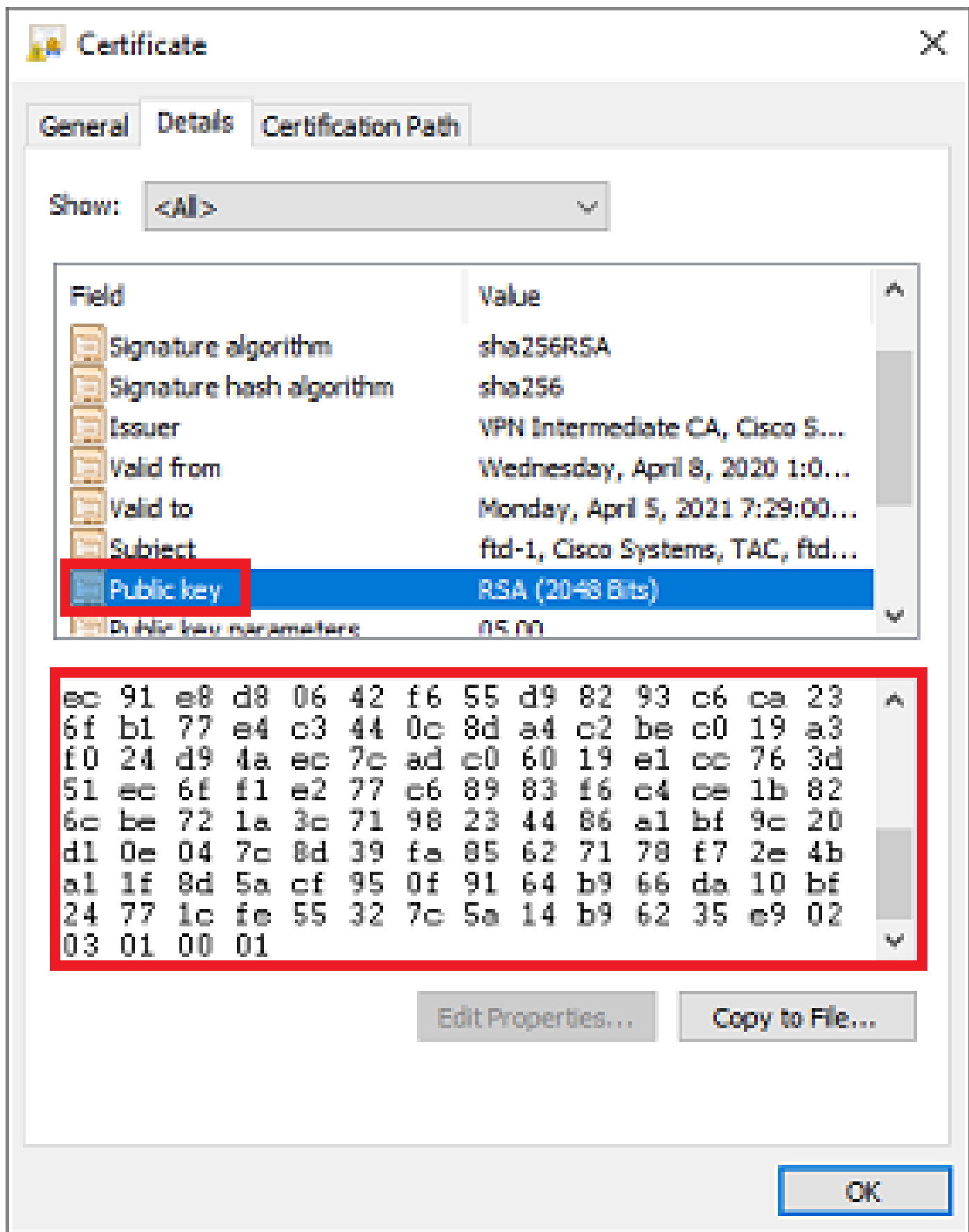
```
openssl x509 -noout -modulus -in id.crt
```

```
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEB096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE  
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9  
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C  
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B  
B966DA10BF24771CFE55327C5A14B96235E9
```

- ftd.csr est le CSR copié depuis FMC lors de l'inscription manuelle.
- id.crt est le certificat d'identité signé par l'autorité de certification.

En variante, la valeur de clé publique sur le FTD peut également être comparée à la clé publique dans le certificat d'identité émis. Notez que les premiers caractères du certificat ne correspondent pas à ceux de la sortie FTD en raison du remplissage :

Certificat d'identité émis ouvert sur le PC Windows :



Sortie de clé publique extraite du certificat d'identité :

```
f6e0fdfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b8af3a491b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8da4c2bec0e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f8d5acf955327c5a14b96235e90203010001
```

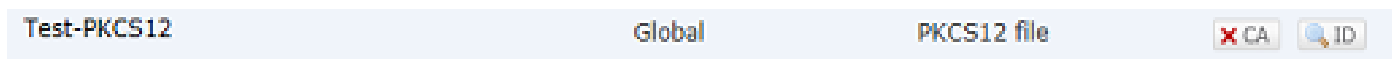
Afficher la sortie crypto key mypubkey rsa du FTD. Une fois l'inscription manuelle effectuée, la <Default-RSA-Key> a été utilisée pour créer le CSR. La section en gras correspond à la sortie de clé publique extraite du certificat d'identité.

```
> 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
```

X rouge à côté de CA dans FMC

Cela peut se produire avec l'inscription PKCS12 car le certificat CA n'est pas inclus dans le package PKCS12.



Pour résoudre ce problème, le certificat CA doit être ajouté à PKCS12.

Émettez ces commandes afin d'extraire le certificat d'identité et la clé privée. Le mot de passe utilisé lors de la création de PKCS12 et la clé privée sécurisée sont nécessaires :

```
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
ChMRQ2l2Yz28gU3lzdGVtcyBUQUUMxHDAaBgNVBAMTE1ZQTiBJbnR1cm1lZG1hdGUg
Q0EwHhcNMjAwNDA4MjY1ODAwWhcNMjEwNDA1MjMyOTAwWjAbMRkwFwYDVQQDExBm
dGQxLmV4Yw1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
043eLVP18K0jnYfHCBZuFUyRXTTB28Z1ouIJ5yYrDzCN781GFrHb/wCczRx/jW4n
pF9q2z7FHR5bQCI4oSUSX40UQfr0/uOK5riI1uZumPUx1Vp1zVkYuqDd/i1r0+0j
PyS7BmyGfV7aebYWZnr8R9ebDsnC2U3nKjP5RaE/wNdVGTs/180H1rIjMpcFMXps
LwxixiEz0hCmDm9RC+7uWZQd1wZ9oNANcbQC0px/Zikj9Dz70RhhbzBTeUNKD3p
sN3VqdDPvGZHFGLPcnhKyyZ79+6p+CHC8X8BFjuTJYoo176uGgiB4Jz2Y9ZeFSQz
Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBg1ghkgBhvCAQOEERYPeGnhIGN1
cnRpZm1jYXR1MA0GCsQGSiB3DQEBcWUAA4IBAQCv/MgshWxXtwpwmMF/6KqEj8nB
S1jbfz1zNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRY54taRI27W+gLneCbQAux
9amxXuhpxP5E0hnc+tsY9eriAKpHuS1Y/2uwn92fHIb3HEXPO1HBJueI8PH3ZK
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
MBQGccqGSiB3DQMhBAgCm0qRxx/dcWScBmiF7BpgJNIPhdU5Zorn1jm3pmsI/XkJ
MRHc1Ree10ziSLCZOSTr84JFQxNpbThXLhsHC9WhpPy5sNXIvXS7Gu+U10/V1NSA
rW1X6SPftAYiFq5QxyEutSHdZZwgQIqpj97seu3Px0agvI0bw1Lo8or51SydnMjp
Ptv50Ko95BSHwWycqkTAia4ZKxytyIc/mIu5m72LucOFmoRB05JZu1avWXjbCAA+
k2ebkb1FT0YRQT1Z4tZHSqX1LFPZe170NZEUG7rIcWak1Yw7XNUPhOn6FHL/ieIZ
IhvIfj+IqQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E
Gnh8r31903A1kPMBkMdx0q1pzo2naIy2KGrUnOSHajVwclR9dTPWIDyjd95YoeS
IUE7Ma00pjJc02FNbWyxRrYt+4hp3aJt0ZW83FHiS1B5UIzGrBMAgKJc2Hb2RTV
9gxZGve1cRco1LeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShn0wHzridF8Zn
F06XvBDSyXVSpkxwAd1Twxq62tUnLIkyRXo2CSz8z8W29UXmF04o3G67n28//LJ
Ku8wj1jeq1vFgXSQiWLADNH772RNwzCMeobfxG1BprF9DPT8yvyBdQviUIuFpJ
nNs5FYbLTv9ygZ1S9xwQpTcqEu+y4F5BJuYLMHqcZ+VpFA4nM0YHhZ5M3sccRSR4
1L+a3BPJJsh1TIJQg0TixDaveCfpDcpS+ydUgS6WY8xw17v0+1f7y5z1t4TkZrt
ItBHHA6yDzR0Cn0/ZH3y88a/asDcukw6bsRaY5iT8nAWGTQved3xXj+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/tJDLV1jyTqWajHnWIZCc+P2AXgn1LzG
HVVfxs0c8FGUJJPQHAtXYd7worWCxszaufJ99E4PaoZnAOYUFW2jaZEwo0NBpBD1
AjQ8aciuosv0FKpp/jXDI78/aYAEk662tPsfGmxvAWB+UMFarA9ZTiihK3x/tDPy
GZ6ByGWJYp/0tNNmJRCFhcAyy83EtzHK9h+8LatFA6WrJ4j3dhceUPzrPXjMffNN
0Yg=
-----END ENCRYPTED PRIVATE KEY-----
```

Une fois terminé, le certificat d'identité et la clé privée peuvent être placés dans des fichiers

séparés et le certificat d'autorité de certification peut être importé dans un nouveau fichier PKCS12 en suivant les étapes mentionnées à l'étape 2. de la création de PKCS12 avec OpenSSL.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.