

Dépannage de l'erreur de certificat " ; Échec de la configuration du certificat AC" ; sur FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Problème](#)

[Solution](#)

[Étape 1. Rechercher le certificat .pfx](#)

[Étape 2. Extraire les certificats et la clé du fichier .pfx](#)

[Étape 3. Vérification des certificats dans un éditeur de texte](#)

[Étape 4. Vérification de la clé privée dans un bloc-notes](#)

[Étape 5. Fractionner les certificats CA](#)

[Étape 6. Fusionner les certificats dans un fichier PKCS12](#)

[Étape 7. Importer le fichier PKCS12 dans FMC](#)

[Vérifier](#)

Introduction

Ce document décrit comment dépanner et corriger l'erreur d'importation de l'autorité de certification (CA) sur les périphériques Firepower Threat Defense gérés par FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Infrastructures à clé publique (PKI)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- OpenSSL

Composants utilisés


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

- MacOS x 10.14.6

- FMC 6,4
- OpenSSL

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

 Remarque : sur les périphériques FTD, le certificat CA est nécessaire avant la génération de la demande de signature de certificat (CSR).


- Si le CSR est généré sur un serveur externe (tel que Windows Server ou OpenSSL), la méthode d'inscription manuelle est censée échouer, car FTD ne prend pas en charge l'inscription manuelle des clés. Une autre méthode doit être utilisée, telle que PKCS12.

Problème

Dans ce scénario particulier, le FMC affiche une croix rouge dans l'état du certificat CA (comme illustré dans l'image), qui indique que l'inscription du certificat n'a pas réussi à installer le certificat CA. Cette erreur se produit généralement lorsque le certificat n'a pas été correctement emballé ou que le fichier PKCS12 ne contient pas le certificat d'émetteur correct, comme illustré dans l'image.



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

 Remarque : dans les versions FMC plus récentes, ce problème a été résolu pour faire correspondre le comportement ASA qui crée un point de confiance supplémentaire avec l'autorité de certification racine incluse dans la chaîne de confiance du certificat .pfx.

Solution

Étape 1. Rechercher le certificat .pfx

Obtenez le certificat pfx qui était inscrit dans l'interface graphique FMC, enregistrez-le et localisez le fichier dans le terminal Mac (CLI).

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

Étape 2. Extraire les certificats et la clé du fichier .pfx

Extrayez le certificat client (et non les certificats CA) du fichier pfx (la phrase de passe utilisée pour générer le fichier .pfx est requise).

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

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

exportation d'identité

Extrayez les certificats CA (et non les certificats clients).

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

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

exportation de cacerts

Extrayez la clé privée du fichier pfx (la même phrase de passe de l'étape 2 est requise).

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

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

exportation de clé

Il existe désormais quatre fichiers : cert.pfx (le bundle pfx d'origine), certs.pem (les certificats CA), id.pem (certificat client) et key.pem (la clé privée).

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

ls après exportation

Étape 3. Vérification des certificats dans un éditeur de texte

Vérifiez les certificats à l'aide d'un éditeur de texte (par exemple nano certs.pem).

Pour ce scénario particulier, certs.pem ne contenait que la sous-CA (CA émettrice).

À partir de l'étape 5, cet article traite de la procédure pour le scénario où le fichier certs.pem contient 2 certificats (une autorité de certification racine et une sous-autorité de certification).

```
Bag Attributes: <No Attributes>
subject=/C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Intermediate CA
issuer=/C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Root CA
-----BEGIN CERTIFICATE-----
MIIF0zCCA7ugAwIBAgICEAUwDQYJKoZIhvcNAQELBQAwdjELMAkGA1UEBhMCTVgx
DTALBgNVBAGMBENETVgxEjAQBGNVBAoMCVVuZ3UgQ29ycDEoMCYGA1UECwwfVW5n
dSBDb3JwIENlcnRpZmljYXRlIEF1dGhvcml0eTEaMBGGA1UEAwwRVW5ndSBDb3Jw
IFJvb3QgQ0EwHhcNMjIwMDQ0WhcNMzIwMTMxMDEwMDQ0WjB+MQswCQYD
VQQGEwJNWDENMA5GA1UECAwEQ0RNVDESMBAGA1UECgwJVW5ndSBDb3JwMSgwJgYD
VQQLDB9Vbmd1IENvcnAgQ2VydgGmaWNhdGUgQXV0aG9yaXR5MSIwIAYDVQDDb1V
bmd1IENvcnAgSW50ZXJtZWZlYXRlIENBMiICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAt9zB5lbrhMTEEyGmRVRnuQ+mt86axF3QZEeSYCfV5gzS9R25cw+N
L7U9agbL/bnfvr00N8I8ywVahiTWJP9kuzGksEDAUzyHXybdSlyPHUNt0fYn5zFi
GGa8lr90KmxSpsXeQB+GB0D8wezA1bAAGSKDiQymtBdQQMpnKTCmCRCjcPD1rBq1
Ewi0/7ePWhHK4KhtBBfSmjxqZYb1QIG5DBWCKA4q2D1ME9/o+pL944Utw+HMLrAH
4bT86kT7cYQVbeVsmoCastuN+1jux2aJ+4jT0GJM44yn0KzVANolGEjw/DPhW460
u9I1oJGMCh4j7Efl8bYvHTd+8yEejmHR+ASysy+8qoymWq3wIPiWJA0r160Hn2c
J0Zpu2oQQs+90+wBrzn/yV7aZmVdDbEJSXKHJkIGA7k5VWe/CvXbfExHSCfdZ5EV
uIx4AixdgwEdd0rghVYOGS1IHBmXNkoPp6s41oLmSmSr8lgZqm5mgdD1UKNA8tG
0jVrURiHLalHhyynYHHVihEjhPRjNL9T26Dq9iAhX6yMClIXB1QG/QUxef7AL07
nzIBASrYnAEv+TvgYkRE4Z9gVKxYhNLpxnVg0ycHiZbco2IcQzqIwdQAqS2LRWP
8eNuPd9l+5BgsSYgK3NxQPzMXZwmMXgnGye3lueBUL9DSkuknx0aFVMCAwEAAAnj
MGEWhQYDVR00BBYEFE/DAVTSyUoHTbTxlvip1L0TEQoMB8GA1UdIwQYMBaAFJMO
DF6TWO6EkboLkLC0t59z01QwMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgGGA0GCSqGSIb3DQEBwUAA4ICAQBUNUuk9jMTGmcP6j/tqBFM3Inhj/84ABMY
T4Rbdtxi1v5HPjtknyEip1B31QxrWi4pLiyh0ILb181mNxnawZDOMvzv7Bsxpvx
xHrGhGac2y4yT72vGcIp/+8H2LatFaGAGEPIssCjzTcLG9brubPB/MXYJ3MrlGXl
FbqvTdDJS5qB0+jRnMbACbV/nTUVXl6f6vb3AW2Zy0/u0+S6VoiB5Uk4xLZuhrwL
IXxSTghQWLqK4FBLj+XxyK2u+10iR3+6JGkkaIbb62zJsklnSJ+gVHgsMhEjATto
H0Zw5+uoJQyl/pa4uk0UaRpKsIcH82p+4gPeCg5cEQAcI4niqJgIH0oPYJQszRwD
IB2w3nTAaNMtDyH6Ih/N/MvPiBhaYI3jynGEmJmansw8zcBPoeak4bTsEx3hu7a/
kWddLmv2TscsfkGL0XL0fclLcW4R6QvsZaj3Ia0AsX/Lm0eYb7RnXfjPHenp3rA
a9IOLNe9/AyQrAqp3hQ4XSNs3zgScCja40ZcXiSgJcf1XIs8Ml2phT4bob89vY+u
xIawv6bXIQtE7P2RBUEJWPMFCJ75JMplRYSj2xogkneMiPpc9w5moZLxZpvznqgy
aCi37m1d+CT6hYTWxe3HztS03VJ+24IqEr+wmi+FB04VHztqc/Bpajb0TpGBUGex
wxMFkoFWSA==
-----END CERTIFICATE-----
```

vue certs

Étape 4. Vérification de la clé privée dans un bloc-notes

Vérifiez le contenu du fichier key.pem à l'aide d'un éditeur de texte (par exemple nano certs.pem).

```
Bag Attributes
  localKeyID: 4B ED BA 56 76 3A C9 22 C3 75 54 A7 0A 1A F1 7D 3B 5E B0 D8
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI9vQUkrEl0MMCAggA
MBQGCCqGSIB3DQMHBajnRV9YTIYsSwSCBMjqf1Lhs3v0RL0DHkvi7yvWSd3xWLMn
jt1hg0LsU1TDmBAWp/LXpqSP27c4XCQiZc0eiFDqm8aKw9xTDjgkEUBVactZs+Sz
yCE1gcG6NRH91ZFiw0Yy+MCR4EPYh06DJPQ+MxLvTjjHrErruyX1AlywfAtrAcQk
E5tJniCaNTppwfVOfLpd/oHa2tFOkBMVVjS3HyxAXEfNThmzMwKRYgsLPUKShTfb
iv0bu8zI6fVfB4db3J/FjqikoiCHKXbWetm/GewZ071H3DW0HamtPw3InUuvYuzv
SM08x+NJi6uo7gtrQ6Rld2z5fN6vTtAw3x10AHjxm+vf0xt95zXhABYkMg2zHaQg
0djTHYFwDhwpdmSSNWm8hWnY8AvFxdjXURp/5MNP+v6ty5W/ETVe6o+Dh1sa9i7v
PzUwIDWs6kt0rxp0v8200lmqSKD6C4UnD1Vf2hH7AyMuwRpYamOEIuPtg8GgeiHJ
6vxpIJ3dY9/s0eyElkvKimZgiXpexBV/nDnksCLJTgyR08AE56iq2+XiBkwIoUai
QTZNi3S+PmPf8glHFtVKR8V6Zk4u8xov3reNTTmKXxXcH3mHPaMU/Nhdldn8fpx+
phTzULmdtIpD3r1Hknh0uMvjrw0RYTLp1WGiEo5DU1SyI5jrMCYa0mhufOI7vtPp
rQqXNo6JleXuBteWSIHdqFynrtIdLyUVhK5QwF40m9+OvGkXNuqMDv4fH4+7nv9l
KqK2NS4yUXW1KjbaFe+Cxz9E7stt4Nyvwx56l/FpYlHymYDjQA3kFrC3tPHeULjT
fp95fJ+6g2R0nr4yKerHbV5BAai0V3rRVpBWhgzBK5o3w4+C+QIH6tgD1f2Jp9YA
TZLj/BDxIc40Q6AORATjWcbE1fvuNmNvMEQpDFM0gP8mlqnnBGzc5mwxC1xTncQD
nmaFYykwVxYCzsvQAgwkvzyzzZw2mPNQpj3lVIOVRdZy8NWVkkCBLpq2XTSA6AQIK
mnJLY+rSAEi6miVnHeUW683un8KND9+HQ1YZbpKDK+JGcwKp/KhEHK mipEoHS8b5
MLby4tL7qrA3sfddMooJJYsCC372WYrd8xPrDZ9kYJ0N64ks9sYhvRUxRMJaxqAY
Int7b6p90i1r0LpielhUUrEvbu0CudM4sLDyXq8Fqf9G5u8dMuchCjXrEPGhmf4Y
ZhTfQF3xxQYtLBbLfWeQUFt6GBsJMLGZFTFPM06/e3vToRu/Opw4Z9hrA6zBfQWa
bcT868DNME+UQxoT825SLwsFFPcjOpixn21FSm6baiq6QWvTV9+5797+AEPnG23i
1x/KKsvTEuwyHGgAX6p9Z0bfP0VcikMzk09MvMDU5MOUm01bnb0zINrrblG0qmRX
SYNNoL71J3joAKzv056KURWAMk9tQE8hAefWAZHS1PacwgUIWx0SAszRMkneptiR
VCm5UvzbYiMIAOrJjx6PTakuPIhdfokLyWfMI74ETao0H17KdDD1i/w11fAWFqtN
2gzfPw7Q02F7iZiYtxV9ryVBnH4wqut9pFjPYGu2oXC5q4Y71J1DrMzc879vAchM
C1dBcaJLWdpdTmrg2WNiao/rv3A20JjP0zAOeUwRo9r50S0oF9ez1ghBpAAtehyi
FGY=
-----END ENCRYPTED PRIVATE KEY-----
```

Étape 5. Fractionner les certificats CA

Dans le cas où le fichier certs.pem a 2 certificats (1 CA racine et 1 sous-CA), la CA racine doit être supprimée de la chaîne de confiance afin de pouvoir importer le certificat formaté pfx dans le FMC, laissant seulement la sous-CA dans la chaîne à des fins de validation.

Fractionnez le fichier certs.pem en plusieurs fichiers, la commande suivante renomme les certs cacert-XX.

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

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

fente traversante

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

ls après division

Ajoutez l'extension .pem à ces nouveaux fichiers à l'aide de la commande décrite ci-dessous.

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

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

renommer le script

Passez en revue les deux nouveaux fichiers et déterminez lequel contient l'autorité de certification racine et lequel contient la sous-autorité de certification avec les commandes décrites.

Recherchez d'abord l'émetteur du fichier id.pem (qui est le certificat d'identité).

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

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

point de vue de l'émetteur

Maintenant, recherchez l'objet des deux fichiers cacert (certificats CA).

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

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

contrôle par sujets

Le fichier cacert qui fait correspondre l'objet avec l'émetteur du fichier id.pem (comme illustré dans les images précédentes) est l'autorité de certification secondaire qui est utilisée ultérieurement pour créer le certificat PFX.

Supprimez le fichier cacert qui ne contient pas l'objet correspondant. Dans ce cas, ce certificat était cacert-aa.pem.

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

Étape 6. Fusionner les certificats dans un fichier PKCS12

Fusionnez le certificat de sous-autorité de certification (dans ce cas, le nom était cacert-ab.pem) avec le certificat d'ID (id.pem) et la clé privée (key.pem) dans un nouveau fichier pfx. Vous devez protéger ce fichier avec une phrase de passe. Si nécessaire, modifiez le nom du fichier cacert-ab.pem pour qu'il corresponde à votre fichier.

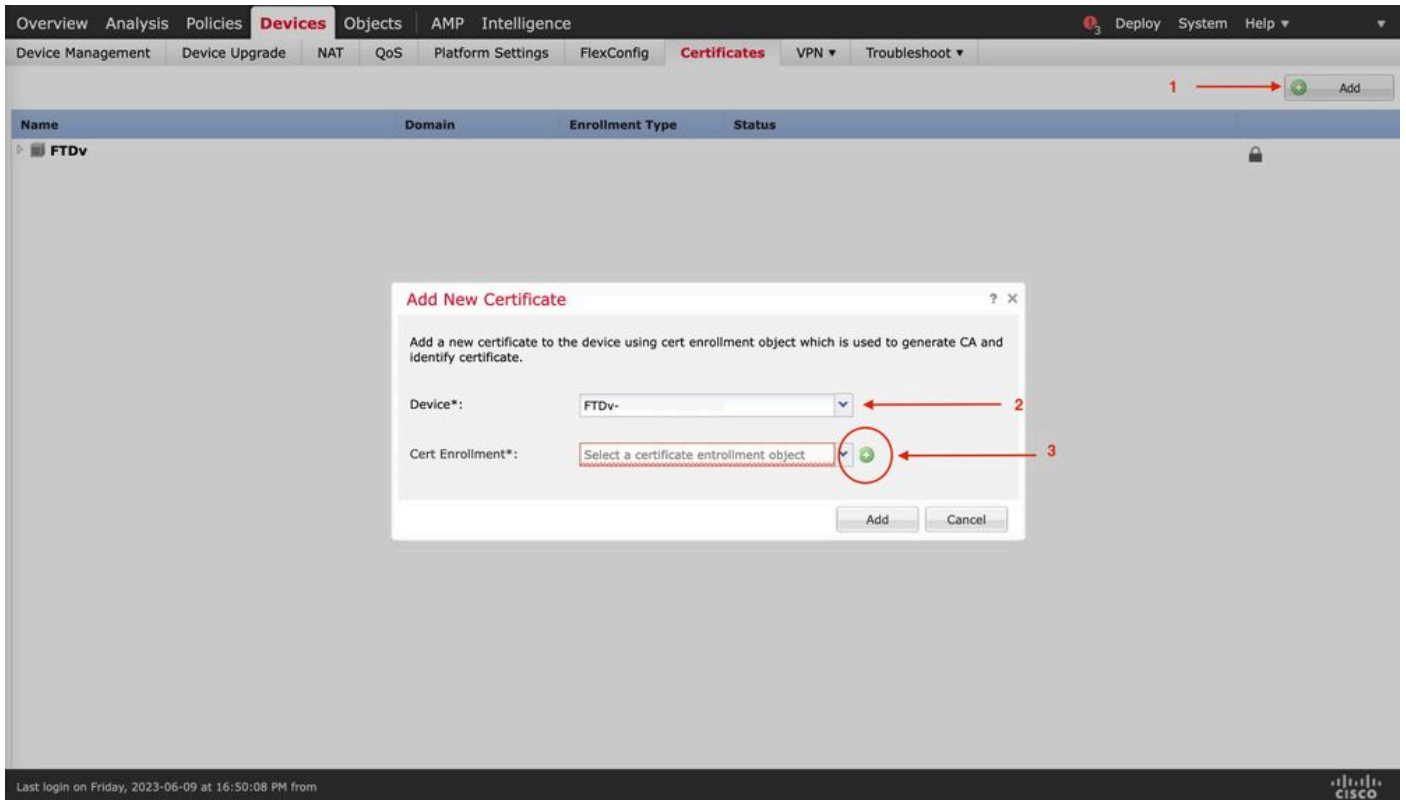
```
openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
```

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

pfx-creation

Étape 7. Importer le fichier PKCS12 dans FMC

Dans le FMC, accédez à Device > Certificates et importez le certificat dans le pare-feu souhaité comme indiqué dans l'image.



inscription au certificat

Insérez un nom pour le nouveau certificat.

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

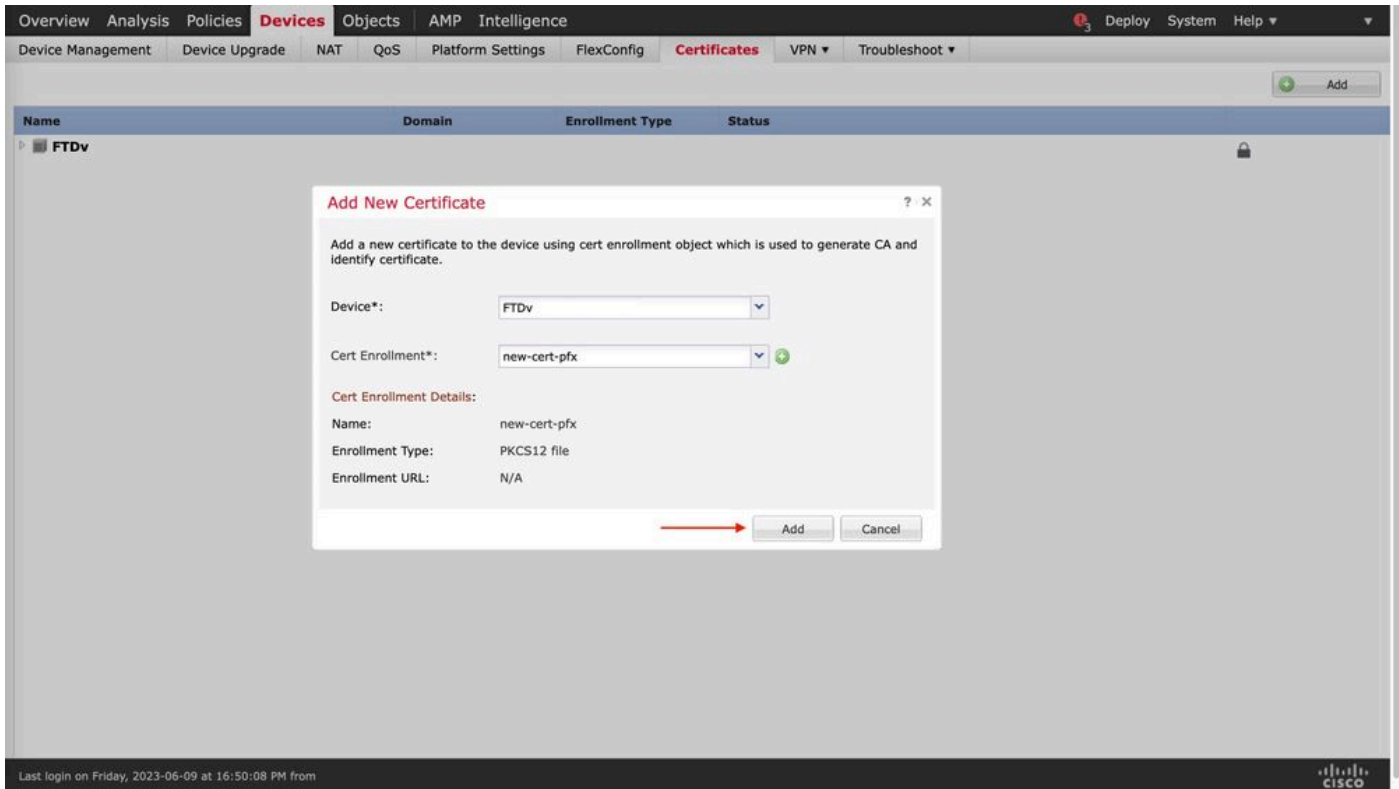
PKCS12 File*:

Passphrase:

Allow Overrides

Inscription

Ajoutez le nouveau certificat et attendez que le processus d'inscription déploie le nouveau certificat sur le FTD.



new-cert

Le nouveau certificat doit être visible sans croix rouge dans le champ AC.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Sous Windows, vous pouvez rencontrer un problème où le système d'exploitation affiche la chaîne entière pour le certificat même si le fichier .pfx ne contient que le certificat d'ID, dans le cas où il a la sous-CA, chaîne CA dans son magasin.

Afin de vérifier la liste des certificats dans un fichier .pfx, des outils comme certutil ou openssl peuvent être utilisés.

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

Le certutil est un utilitaire de ligne de commande qui fournit la liste des certificats dans un fichier .pfx. Vous devez voir toute la chaîne avec ID, SubCA, CA inclus (le cas échéant).

Vous pouvez également utiliser une commande openssl, comme indiqué dans la commande ci-dessous.

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

Afin de vérifier l'état du certificat ainsi que les informations d'autorité de certification et d'ID, vous pouvez sélectionner les icônes et confirmer qu'il a été importé avec succès :

Name	Domain	Enrollment Type	Status
FPR1k			
wildcard-certificate-2020	Global	PKCS12 file	CA
new-cert-pfx	Global	PKCS12 file	CA

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.