FMCでの証明書エラー"Fail to Configure CA Certificate"；のトラブルシューティング

内容

はじめに

このドキュメントでは、FMCによって管理されているFirepower Threat Defense(FTD)デバイスの認証局(CA)インポートエラーをトラブルシューティングし、修正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。

- 公開キー インフラストラクチャ（PKI）
- Firepower Management Center（FMC）
- Firepower Threat Defense（FTD）
- OpenSSL

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- MacOS x 10.14.6

- FMC 6.4
- OpenSSL

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

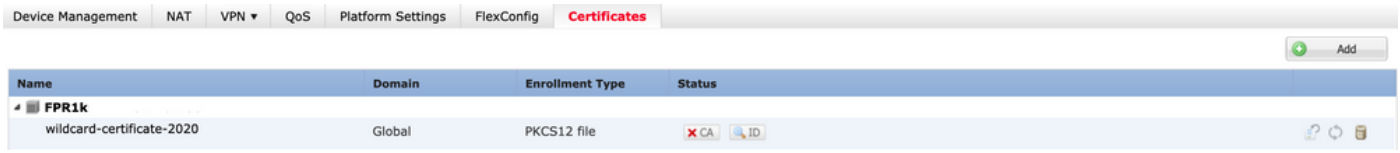
背景説明

注:FTDデバイスでは、証明書署名要求(CSR)を生成する前にCA証明書が必要です。

- CSRが外部サーバ（Windows ServerやOpenSSLなど）で生成される場合、FTDはキーの手動登録をサポートしないため、手動登録メソッドは失敗します。PKCS12など、別の方式を使用する必要があります。

問題

この特定のシナリオでは、図に示すように、FMCのCA証明書ステータスに赤い十字が表示されます。これは、証明書の登録がCA証明書のインストールに失敗したことを示します。このエラーは、証明書が正しくパッケージされていない場合、または図に示すようにPKCS12ファイルに正しい発行者証明書が含まれていない場合によく発生します。



注：新しいFMCバージョンでは、この問題は、.pfx証明書の信頼チェーンに含まれるルートCAを使用して追加のトラストポイントを作成するASAの動作と一致するように対処されています。

解決方法

ステップ 1：.pfx証明書の検索

FMC GUIに登録されたpfx証明書を取得し、保存してMac Terminal(CLI)でファイルを見つけます。

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

ls

ステップ 2：.pfxファイルからの証明書とキーの抽出

CA証明書ではなく、クライアント証明書をpfxファイルから抽出します（.pfxファイルの生成に使用したパスフレーズが必要です）。

```
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
```

IDエクスポート

CA証明書（クライアント証明書ではない）を抽出します。

```
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
```

cacertsエクスポート

pfxファイルから秘密キーを抽出します（ステップ2と同じパスフレーズが必要です）。

```
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:
```

キーエクスポート

cert.pfx（元のpfxバンドル）、certs.pem（CA証明書）、id.pem（クライアント証明書）、key.pem（秘密キー）の4つのファイルが存在します。

```
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#
```

エクスポート後のLS

ステップ 3：テキストエディタでの証明書の確認

テキストエディタ（nano certs.pemなど）を使用して証明書を確認します。

この特定のシナリオでは、certs.pemには下位CA（発行側CA）のみが含まれていました。

この記事では、ステップ5以降で、ファイルcerts.pemに2つの証明書（1つのルートCAと1つのサブCA）が含まれているシナリオの手順について説明します。

```
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
IFJvb3QgQ0EwHhcNMjIwMjAyMDc1MDQ4WhcNMzIwMTMxMDc1MDQ4WjB+MQswCQYD
VQQGEwJNWDENMAsGA1UECAwEQ0RNWDESMBAGA1UECgwJVW5ndSBDb3JwMSgwJgYD
VQQLDB9Vbmd1IENvcnAgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSIwIAYDVQQDDBlV
bmd1IENvcnAgSW50ZXJtZWRpYXRlIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAt9zB5lbrhMTEEyGmRVRnuQ+mt86axF3QZEeSYCfV5gZs9R25cw+N
L7U9agbL/bNfvR0ON8I8ywVahiTWJP9kuzGksEDaUzyHXybDslYpHUNt0fYn5zFi
GGa8lr9OKmxSpsXeQB+GB0D8wezA1bAAGSKDiQymtBdQQMpnKTCmCRCjcPD1rBq1
EwiO/7ePWhHK4KhtBBfSmjqxZYb1QIG5DBWCKA4q2DlME9/o+pL944Utw+HMLrAH
4bT86kT7cYQVbeVSmoCastuN+1jux2aJ+4jT0GJM44yn0KzVANolgEjw/DPhW460
u9I1oJGMCh4j7EfL8bYvHTd+8yEejmHR+ASycsy+8qoymWq3wIPiWJA0r160Hn2c
JOZpu2oQQs+9O+wBrzn/yV7aZmVDdbEJSXKHJkIGA7k5VWe/CvXbfExHSCfdZ5EV
uIx4AixdgwEddOrgpHvYOGS1IHBmXNKoPp6s41oLMsmSr8lgZqm5mgdDlUKNA8tG
OjVrURiHLalHhyynoYHHVihEjhPRjNL9T26Dq9iAhX6yMClIXB1QG/QUxef7ALO7
nzIBA5rYnAEv+TvgYkRE4Z9gVKxYhNLpxnVgOycHiZbco2IcQzqIWdQAqQS2LRWP
8eNuPd9l+5BgsSYgK3NxQPzMXZwmMXgnGye3lueBUL9DSkuknxOaFVMCAwEAAaNj
MGEwHQYDVR0OBBYEFE/DAVTSyUoHThBtxlvip1L0TEQoMB8GA1UdIwQYMBaAFJMO
DF6TWo6EkboLkLC0t59zO1QwMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgGGMA0GCSqGSIb3DQEBCwUAA4ICAQBUNUuk9jMTGmcP6j/tqBFM3Inhj/84ABMY
T4RBdtxi1v5HPjtknyEIp1B31QxrWi4pLiyh0ILb181mNxnawZDOMvzv7Bsxepvx
xHrGhGac2y4yT72vGcIp/++8H2LatFaGAGePIssCjzTcLG9bruPB/MXYJ3MrlGXl
FbqvTdDJS5qBO+jRnMbACbV/nTUVXl6f6vb3AW2ZyO/u0+S6VoiB5Uk4xLZuhrwl
IXxSTghQWLqK4FBLj+XxyK2u+10iR3+6JGkkaIbb62zJsklnSJ+gVHgsMhEjATto
HOZw5+uoJQyl/pa4ukOUaRPksIcH82p+4gPeCg5cEQAcI4niqJgIH0oPYJQszRwD
IB2w3nTAaNMTDyH6Ih/N/MvPiBhaYI3jynGEmJmansw8zcBPoeak4bTsEx3hu7a/
kWddLmv2TscsfkGCL0XLOfcJLcW4R6QvsZaj3Ia0AsX/Lm0eYb7RnXfjPHenp3rA
a9IOLNe9/AyQrAqp3hQ4XSNs3zgScCja40ZcXiSgJcf1XIs8Ml2phT4bob89vY+u
xIawv6bXItQE7P2RBUeJWPMFcJ75JMplRYsj2xogkneMiPpc9w5moZLxZpvznqgy
aCi37m1d+CT6hYTWxe3HztS03VJ+24IqEr+wmi+FB04VHZtqc/BpajbOTpGBUGex
wxMFkoFWSA==
-----END CERTIFICATE-----
```

certsビュー

ステップ 4：メモ帳での秘密キーの確認

テキストエディタ（nano certs.pemなど）を使用して、key.pemファイルの内容を確認します。

```
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
MBQGCCqGSIb3DQMHBAjnRV9YTIYsSwSCBMjqflLhs3v0RL0DHkvi7yvWSd3xWLMn
jt1hgOLsU1TDmBAWp/LXpqSP27c4XCQiZcOeiFDqm8aKw9xTDjgkEUBVactZs+Sz
yCE1gcG6NRH9lZFiwOYy+MCR4EPYh06DJPQ+MxLvtjjHrErruyXlAlywfAtrAcQk
E5tJniCaNTppwfVOfLpd/oHa2tFOkBMVVjS3HyxAXEfNThmzMwKRygsLPUKShtfb
iv0bu8zI6fVfB4db3J/FjqikoiCHKXbWetm/GewZO71H3DW0HamtPw3InUuvYuzv
SM08x+NJi6uo7gtrQ6Rld2z5fN6vTtAw3xlOAHjxm+vfOxt95zXhABYkMg2zHaQg
0djTHYFWdHwpdmSSNWM8hWnY8AvFxdjXURp/5MNP+v6ty5W/ETVe6o+Dh1sa9i7v
PzUwIDWs6kt0rxp0v82O0lmqSKD6C4UnDlVf2hH7AyMuwRpYamOEIuPtg8GgeiHJ
6vxpIJ3dY9/s0eyElkvKimZgiXpexBV/nDnksCLJTGyR08AE56iq2+XiBkwIoUai
QTZNi3S+PmPf8glHFtVKR8V6Zk4u8xov3reNTTmKXxXcH3mHPaMU/Nhdldn8fpx+
phTzULmdtIpD3rlHknh0uMvjrw0RYTLp1WGiEo5DU1SyI5jrMCYa0mhufOI7vtPp
rQqXNo6JleXuBteWSIHDqFynrtIdLyUVhK5QwF4Om9+OvGkXNuqMDv4fH4+7nv9l
KqK2NS4yUXW1KjbAFe+Cxz9E7stt4Nyvwx56l/FpYLHymYDjQA3kFrC3tPHeULjT
fp95fJ+6g2ROnr4yKerHbV5BAaiOV3rRVpBWhgzBK5o3w4+C+QIH6tgD1f2Jp9YA
TZLj/BDxIc4OQ6AORATjWcbE1fvuNmNvMEQpDFMOgP8mlqnnBGzc5mwxC1xTNcQD
nmaFYykWVxYCzsvQAgwkvyzzZw2mPNQpj3lVIOVRdZy8NWVkKCBLpq2XTSA6AQIK
mnJLY+rSAEi6miVnHeUW683un8KND9+HQlYZbpKDK+JGcwkP/KhEHKmipEoHS8b5
MLby4tL7qrA3sfddMooJJYsCC372WYrd8xPrDZ9kYJ0N64ks9sYhvRUxRMJaxqaY
Int7b6p9Oi1r0LpielhUUrEvbuOCudM4sLDyXq8Fqf9G5u8dMuchCjXrEPGhmf4Y
ZhTfQF3xxQYtLBbLfWeQUFt6GBsJMLGZFTFPM06/e3vToRu/Opw4Z9hrA6zBfQWa
bcT868DNME+UQxoT825SLwsFFPcjOpixn21FSm6baiq6QWvTV9+5797+AEPnG23i
1x/KKsvTEuwyHGgAX6p9Z0bfPOVcikMZkO9MvMDU5MOUm0lbnb0zINrrblG0qmRX
SYNNoL7lJ3joAKzv056KURWAMk9tQE8hAefWAZHSlPacwgUIWxOSAszRMkneptiR
VCm5UvzbYiMIAOrJjx6PTakuPIhdfokLyWfMI74ETao0Hl7KdDD1i/w11fAWFqtN
2gzfPw7QO2F7iZiYtxV9ryVBnH4wqut9pFjPYGu2oXC5q4Y7lJ1DrMzc879vAchM
C1dBcaJLWdpdTmrg2WNiao/rv3A20JjPOzAOeUwRo9r5OS0oF9ez1ghBpAAtehyi
FGY=
-----END ENCRYPTED PRIVATE KEY-----
```

ステップ 5：CA証明書の分割

certs.pemファイルに2つの証明書（1つのルートCAと1つのサブCA）がある場合、検証のためにチェーンにサブCAだけを残してFMCにpfx形式の証明書をインポートできるようにするには、ルートCAを信頼チェーンから削除する必要があります。

certs.pemを複数のファイルに分割し、次のコマンドでcertsの名前をcacert-XXに変更します。

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

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

分割

```
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#
```

分割後のLS

次に説明するコマンドを使用して、これらの新しいファイルに.pem拡張子を追加します。

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

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

スクリプト名の変更

2つの新しいファイルを確認し、説明したコマンドを使用して、ルートCAとサブCAを含むファイルを決定します。

まず、id.pemファイル（ID証明書）の発行者を見つけます。

```
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
```

発行者ビュー

次に、2つのcacert – ファイル（CA証明書）のサブジェクトを見つけます。

```
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
```

件名チェック

前の図に示すように、id.pemファイルの発行者とSubjectが一致するcacertファイルは、後でPFX証明書の作成に使用されるサブCAです。

Subjectが一致しないcacertファイルを削除します。この場合、その証明書はcacert-aa.pemです。

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

手順 6：PKCS12ファイルでの証明書のマージ

サブCA証明書（この例では名前はcacert-ab.pem）と、ID証明書(id.pem)および秘密キー(key.pem)を新しいpfxファイルにマージします。このファイルはパスフレーズで保護する必要があります。必要に応じて、 cacert-ab.pemファイル名をファイル名に一致するように変更します。

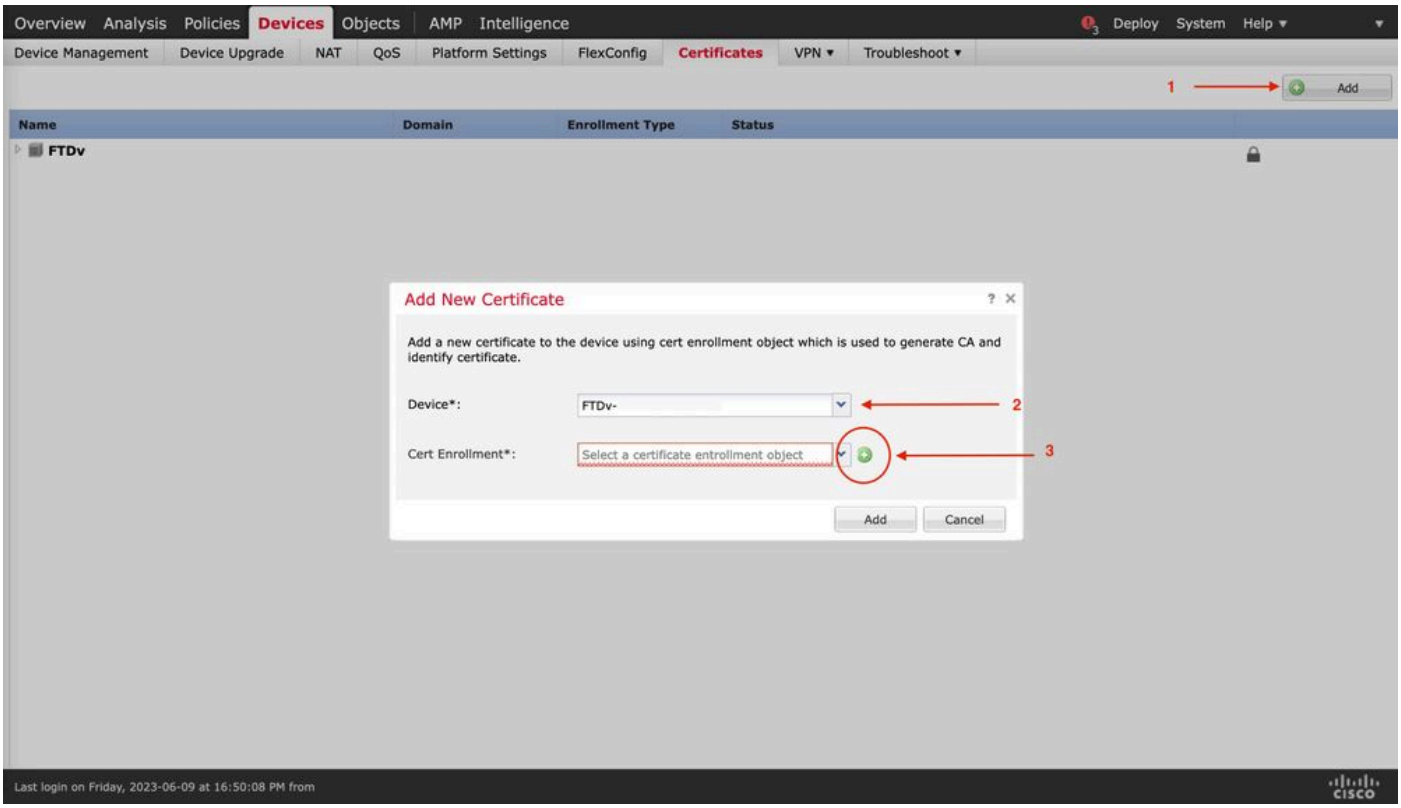
```
openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
```

```
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作成

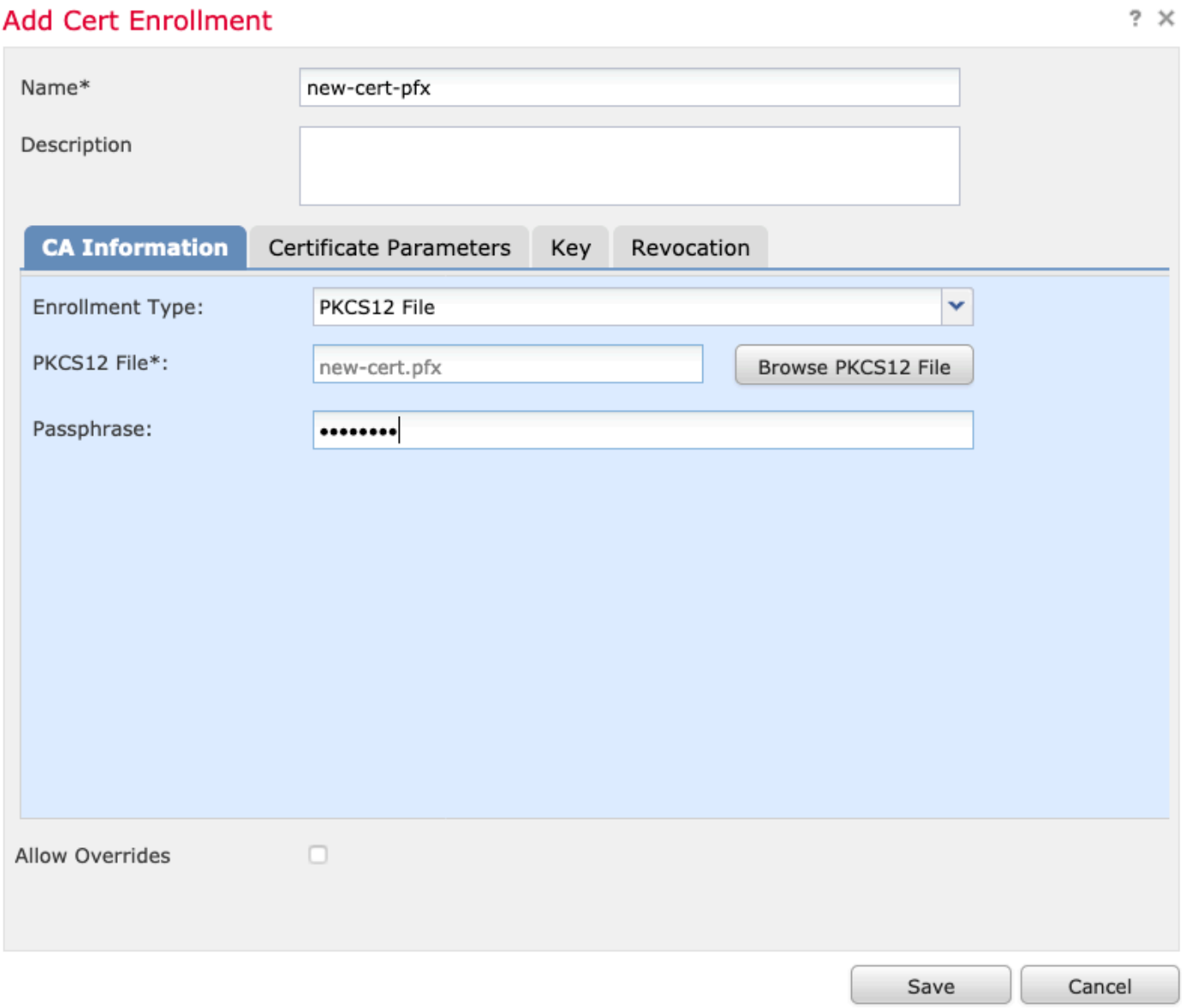
手順 7：FMCでのPKCS12ファイルのインポート

図に示すように、FMCでDevice > Certificatesの順に移動し、目的のファイアウォールに証明書をインポートします。



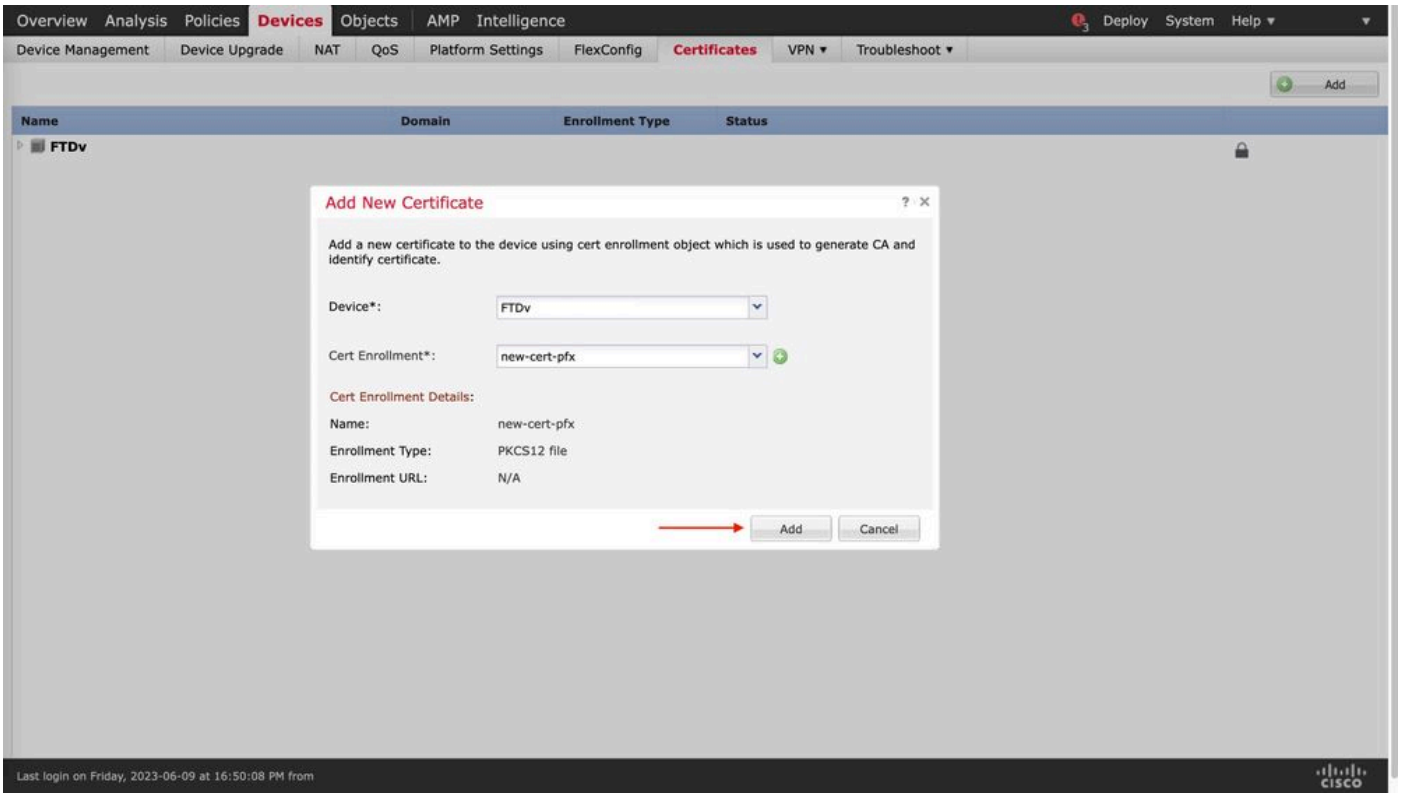
証明書の登録

新しい証明書の名前を挿入します。



登録

新しい証明書を追加し、登録プロセスによって新しい証明書がFTDに展開されるまで待機します。



新しい証明書

新しい証明書は、CAフィールドに赤い十字なしで表示される必要があります。

確認

このセクションでは、設定が正常に動作していることを確認します。

Windowsでは、.pfxファイルにID証明書のみが含まれていても、OSが証明書のチェーン全体を表示するという問題が発生する場合があります。この場合、ストアにsubCA、CAチェーンが含まれています。

.pfxファイル内の証明書のリストを確認するには、certutilやopensslなどのツールを使用できます。

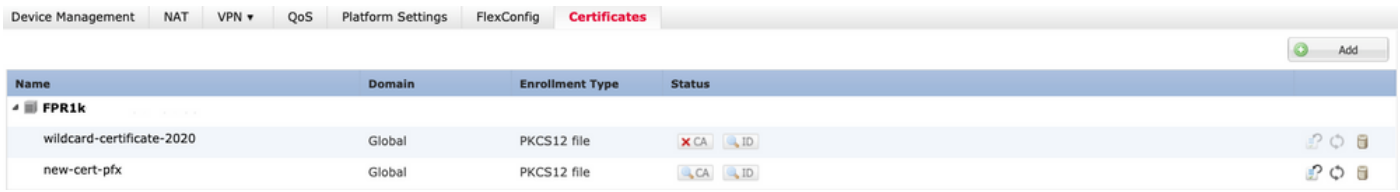
```
certutil -dump cert.pfx
```

certutilは、.pfxファイル内の証明書の一覧を提供するコマンドラインユーティリティです。ID、SubCA、CAが含まれているチェーン全体を確認する必要があります（存在する場合）。

または、次のコマンドに示すように、openssl コマンドを使用できます。

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

CAおよびID情報とともに証明書のステータスを確認するには、アイコンを選択して、正常にインポートされたことを確認します。



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。