Troubleshoot Certificate Error on FMC pfx-creation

Contents

Introduction

Prerequisites

- Requirements
- Components used

Background information

Problem

Solution

- Step 1. Locate the .pfx Certificate
- Step 2. Extract the Certificates and Key from the .pfx File
- Step 3. Verify the Certificates in a Text Editor
- Step 4. Verify the Private Key in a Notepad
- Step 5. Split the CA Certs
- Step 6. Merge the Certificates in a PKCS12 File
- Step 7. Import the PKCS12 File in the FMC

Verify

Introduction

This document describes how to troubleshoot and fix the Certificate Authority (CA) import error on Firepower Threat Defense devices managed by FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Public Key Infrastructure (PKI)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- OpenSSL

Components used

The information in this document is based on these software versions:

- 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.

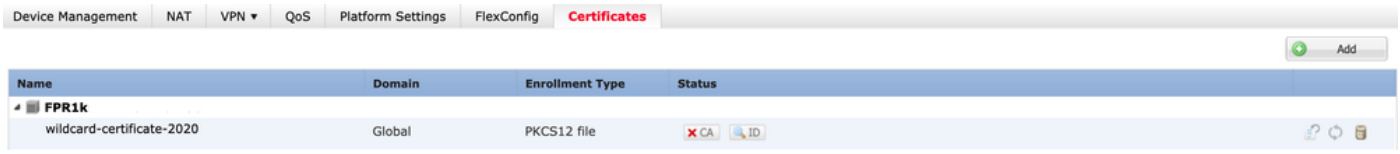
Background information

Note: On FTD-managed devices, the CA certificate is required before the Certificate Signing Request (CSR) is generated.

- If the CSR is generated in an external server (such as Windows Server or OpenSSL), the manual enrollment method is intended to fail, since FTD does not support manual key enrollment. A different method must be used such as PKCS12.

Problem

In this particular scenario, the FMC displays a red cross in the CA certificate status (as shown in the image), which states that the certificate enrollment failed to install the CA certificate with the message: "Fail to configure CA certificate." This error is commonly seen when the certificate has not been properly packaged or the PKCS12 file does not contain the correct issuer certificate as shown in the image.



Note: In newer FMC versions, this problem has been addressed to match the ASA behavior that creates an additional trustpoint with the root CA included in the chain of trust of the .pfx cert.

Solution

Step 1. Locate the .pfx Certificate

Get the pfx certificate that was enrolled in the FMC GUI, **save** it and locate the file in the Mac Terminal (CLI).

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

ls

Step 2. Extract the Certificates and Key from the .pfx File

Extract the client certificate (not CA certificates) from the pfx file (the passphrase that was used to generate the .pfx file is required).

```
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
```

identity export

Extract the CA certificates (not client Certificates).

```
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 export

Extract the private key from the pfx file (the same passphrase from Step 2 is required).

```
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:
```

key export

Four files now exist: cert.pfx (the original pfx bundle), certs.pem (the CA certificates), id.pem (client certificate), and key.pem (the private key).

```
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 after export

Step 3. Verify the Certificates in a Text Editor

Verify the certificates with the use of a text editor (for instance: nano certs.pem).

For this particular scenario, certs.pem only contained the sub CA (issuing CA).

Starting in step 5, this article addresses the procedure for the scenario where the file certs.pem contains 2

certificates (one root CA and one sub CA).

```
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 view

Step 4. Verify the Private Key in a Notepad

Verify the content of the key.pem file with the use of a text editor (for instance: 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
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-----
```

Step 5. Split the CA Certs

For the case that the certs.pem file has 2 certificates (1 root CA and 1 sub CA), the root CA needs to be removed from the chain of trust in order to be able to import the pfx-formatted certificate in the FMC, leaving only the sub-CA in the chain for validation purposes.

Split the certs.pem in multiple files, the next command renames the certs as cacert-XX.

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

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

split

```
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 after split

Add the .pem extension to these new files with the command described below.

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

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

rename script

Review the two new files and determine which one contains the root CA, and which contains the sub CA with the commands described.

First, find the issuer of the id.pem file (which is the identity certificate).

```
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
```

issuer view

Now, find the subject of the two cacert- files (CA certificates).

```
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
```

subject check

The cacert file that matches the Subject with the Issuer of the id.pem file (as shown in the previous images), is the Sub CA that is later used to create the PFX cert.

Delete the cacert file that does not have the matching Subject. In this case, that cert was cacert-aa.pem.

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

Step 6. Merge the Certificates in a PKCS12 File

Merge the sub CA certificate (for this case, the name was cacert-ab.pem) along with the ID certificate (id.pem) and private key (key.pem) in a new pfx file. You must protect this file with a passphrase. If needed, change the cacert-ab.pem file name to match your file.

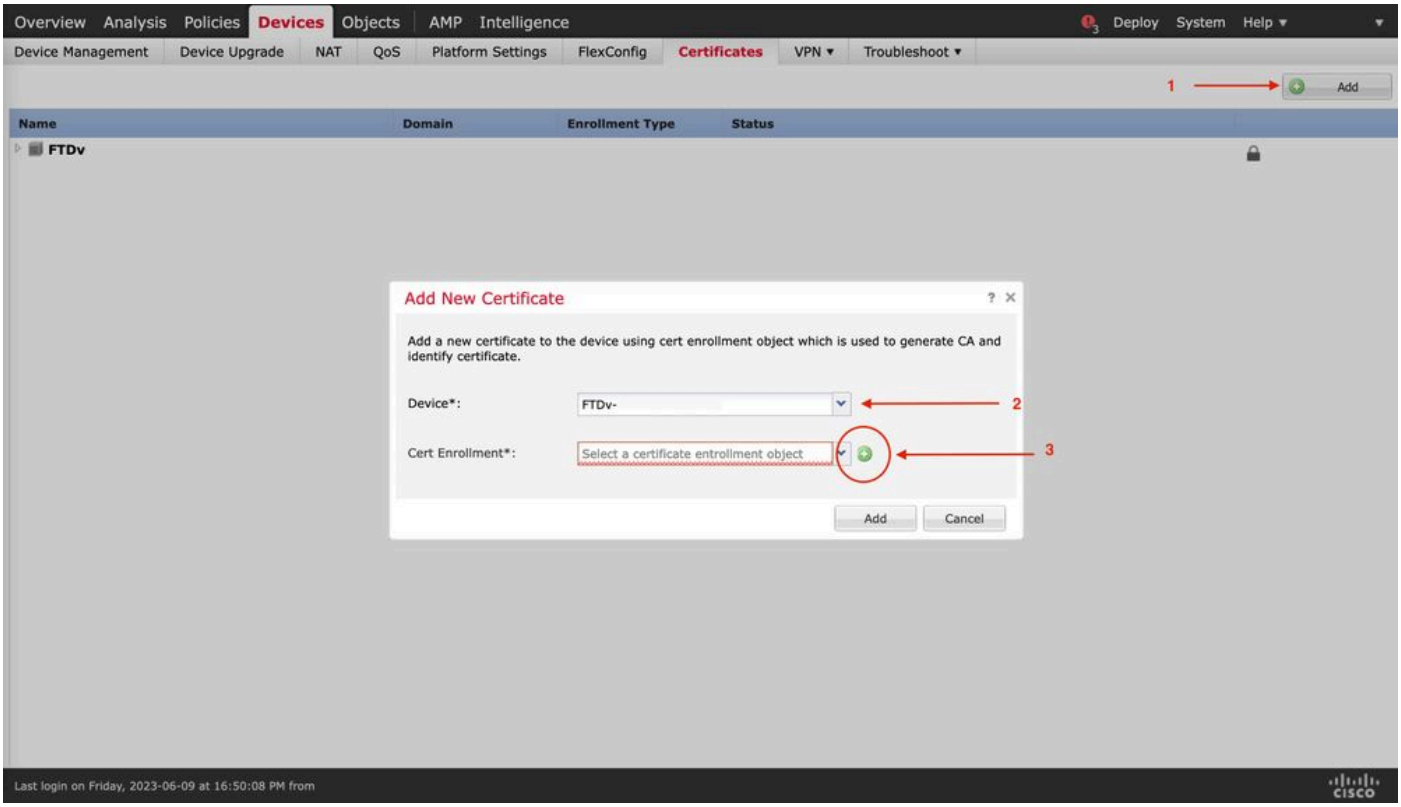
```
openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
```

```
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

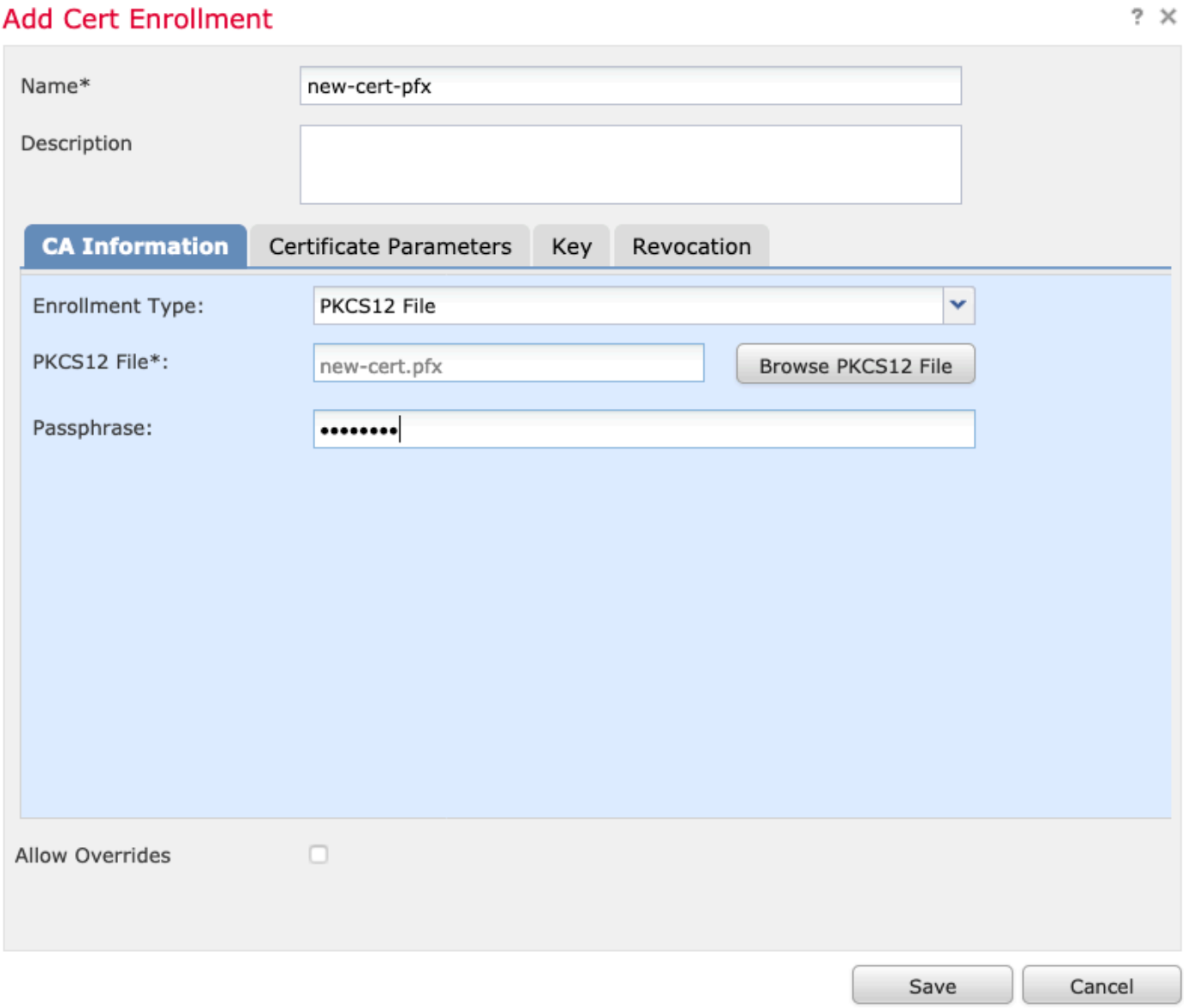
Step 7. Import the PKCS12 File in the FMC

In the FMC, navigate to **Device > Certificates** and import the certificate to the desired firewall as shown in the image.



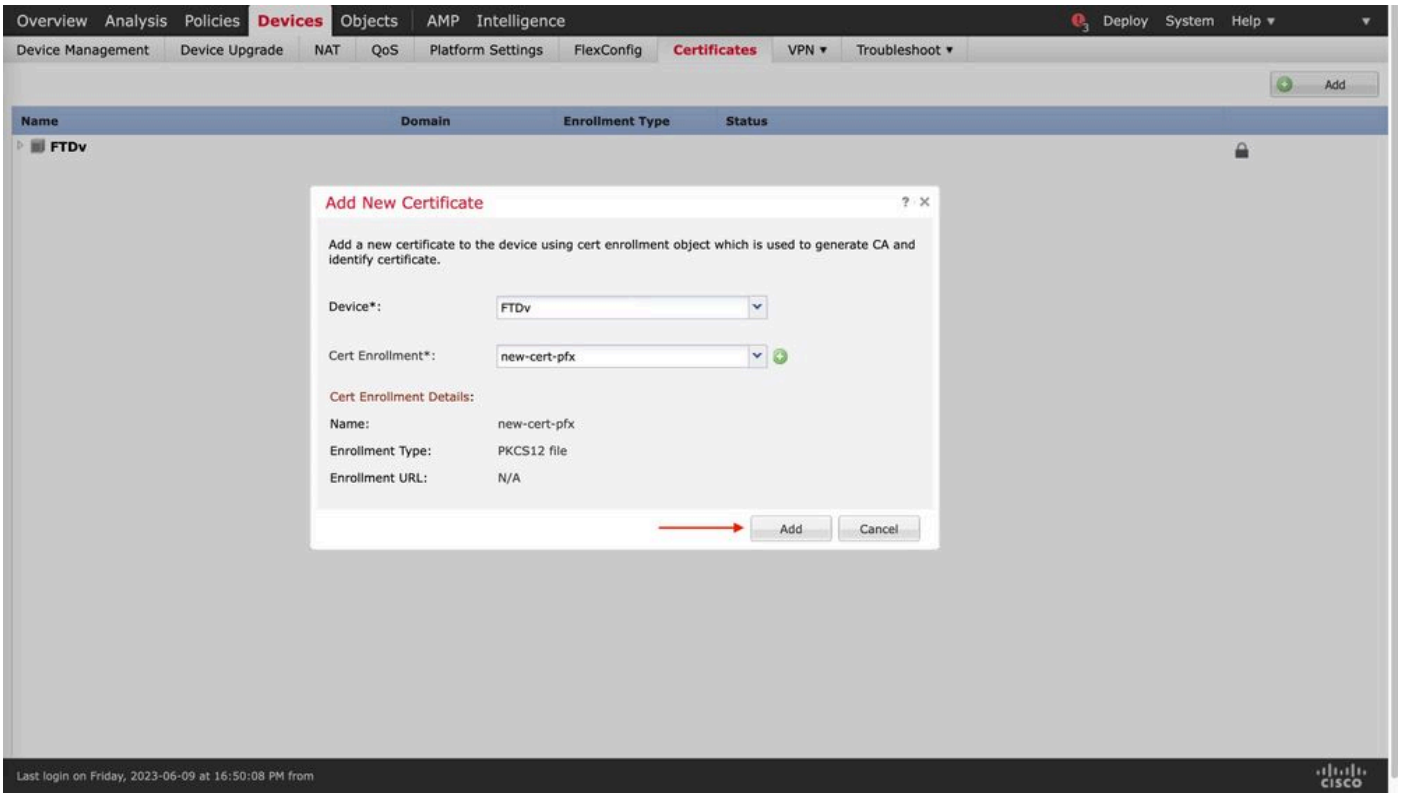
cert enrollment

Insert a **name** for the new cert.



Enrollment

Add the **new certificate**, and wait for the enrollment process to deploy the new cert to the FTD.



new-cert

The new certificate must be visible without a red cross in the CA field.

Verify

Use this section to confirm that your configuration works properly.

In Windows, you can encounter an issue where the OS displays the whole chain for the certificate even though the .pfx file only contains the ID certificate, in the case it has the subCA, CA chain in its store.

In order to check the list of the certificates in a .pfx file, tools like certutil or openssl can be used.

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

The certutil is a command line utility that provides the list of certificates in a .pfx file. You must see the whole chain with ID, SubCA, CA included (if any).

Alternatively, you can use an openssl command, as shown in the command below.

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

In order to verify the certificate status along with the CA and ID information, you can select the icons and

confirm it was successfully imported:

