# Solucionar errores de certificados en FMC

## Contenido



## Introducción

Este documento describe cómo resolver problemas y corregir el error de importación de la autoridad certificadora (CA) en los dispositivos Firepower Threat Defence administrados por FMC.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Public Key Infrastructure (PKI)
- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)
- OpenSSL

### Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- MacOS x 10.14.6
- CSP 6.4
- OpenSSL

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

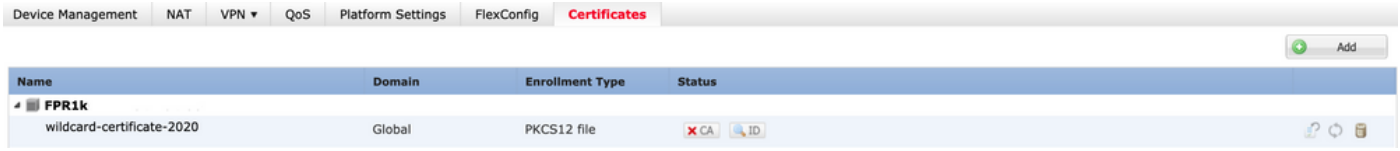
# Antecedentes

Nota: en los dispositivos gestionados mediante FTD, se requiere el certificado de CA antes de generar la solicitud de firma de certificado (CSR).

- Si el CSR se genera en un servidor externo (como Windows Server u OpenSSL), el método de inscripción manual tiene la intención de fallar, ya que FTD no admite la inscripción manual de claves. Se debe utilizar un método diferente, como PKCS12.

# Problema

En este escenario en particular, el FMC muestra una cruz roja en el estado del certificado de la CA (como se muestra en la imagen), que indica que la inscripción del certificado no pudo instalar el certificado de la CA con el mensaje: "Fail to configure CA certificate" (Error al configurar el certificado de la CA). Este error se observa comúnmente cuando el certificado no se ha empaquetado correctamente o el archivo PKCS12 no contiene el certificado de emisor correcto como se muestra en la imagen.




Nota: en las versiones más recientes de FMC, este problema se ha solucionado para que coincida con el comportamiento de ASA que crea un punto de confianza adicional con la CA raíz incluida en la cadena de confianza del certificado .pfx.

# Solución

## Paso 1. Localice el certificado .pfx

Obtenga el certificado pfx que estaba inscrito en la GUI de FMC, guárdelo y localice el archivo en la Terminal Mac (CLI).

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

ls

## Paso 2. Extraiga los certificados y la clave del archivo .pfx

Extraiga el certificado de cliente (no los certificados de CA) del archivo pfx (se requiere la frase de contraseña que se utilizó para generar el archivo .pfx).

```
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
```

exportación de identidad

Extraiga los certificados de CA (no los certificados de cliente).

```
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
```

exportación de cacerts

Extraiga la clave privada del archivo pfx (se requiere la misma frase de contraseña del paso 2).

```
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:
```

exportación de claves

Ahora existen cuatro archivos: cert.pfx (el paquete pfx original), certs.pem (los certificados de CA), id.pem (certificado de cliente) y key.pem (la clave privada).

```
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 después de exportar

## Paso 3. Verificar los certificados en un editor de texto

Verifique los certificados con el uso de un editor de texto (por ejemplo: nano certs.pem).

Para este escenario en particular, certs.pem sólo contenía la CA secundaria (CA emisora).

Comenzando en el paso 5, este artículo trata el procedimiento para el escenario donde el archivo certs.pem contiene 2 certificados (una CA raíz y una CA secundaria).

```
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-----
```

vista de certificados

## Paso 4. Comprobar la clave privada en un Bloc de notas

Verifique el contenido del archivo key.pem con el uso de un editor de texto (por ejemplo: 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-----
```

## Paso 5. Dividir los certificados de CA

En el caso de que el archivo certs.pem tenga 2 certificados (1 CA raíz y 1 CA secundaria), la CA raíz debe eliminarse de la cadena de confianza para poder importar el certificado con formato pfx en el FMC, dejando solo la CA secundaria en la cadena para fines de validación.

Divida el certs.pem en varios archivos, el siguiente comando renombra los certs como cacert-XX.

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

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

```
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#
```

splitls después de split

Agregue la extensión .pem a estos nuevos archivos con el comando que se describe a continuación.

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

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

cambiar nombre de script

Revise los dos archivos nuevos y determine cuál contiene la CA raíz y cuál contiene la CA secundaria con los comandos descritos.

Primero, busque el emisor del archivo id.pem (que es el certificado de identidad).

```
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
```

vista del emisor

Ahora, busque el asunto de los dos archivos cacert- (certificados de 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
```

comprobación del asunto

El archivo cacert que coincide con el Asunto con el Emisor del archivo id.pem (como se muestra en las imágenes anteriores) es la CA secundaria que se utiliza más adelante para crear el certificado PFX.

Elimine el archivo cacert que no tenga el Asunto coincidente. En este caso, ese certificado era cacert-aa.pem.

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

## Paso 6. Fusionar los certificados en un archivo PKCS12

Combine el certificado de la CA secundaria (en este caso, el nombre era cacert-ab.pem) junto con el certificado de ID (id.pem) y la clave privada (key.pem) en un nuevo archivo pfx. Debe proteger este archivo con una frase de contraseña. Si es necesario, cambie el nombre del archivo cacert-ab.pem para que coincida con el suyo.

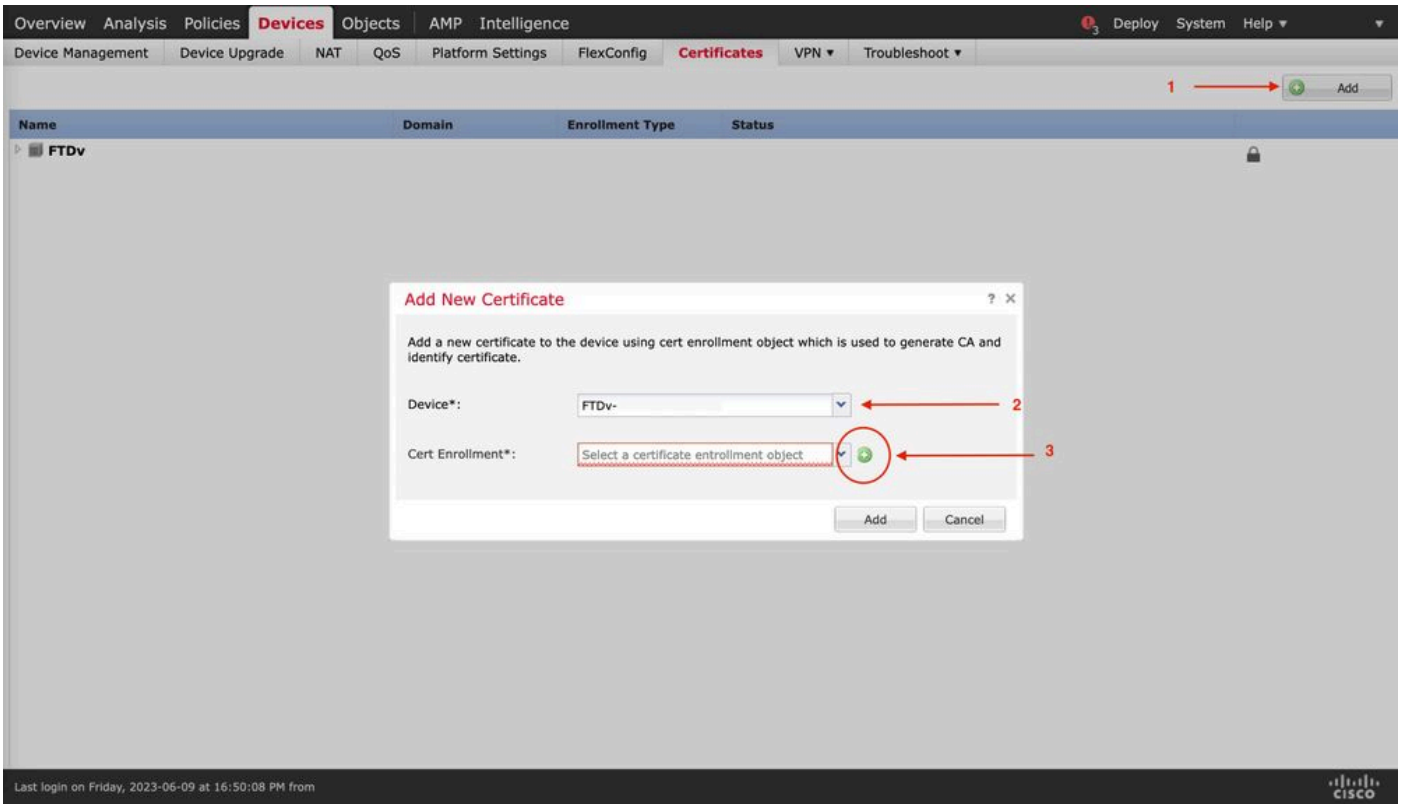
```
openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
```

```
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

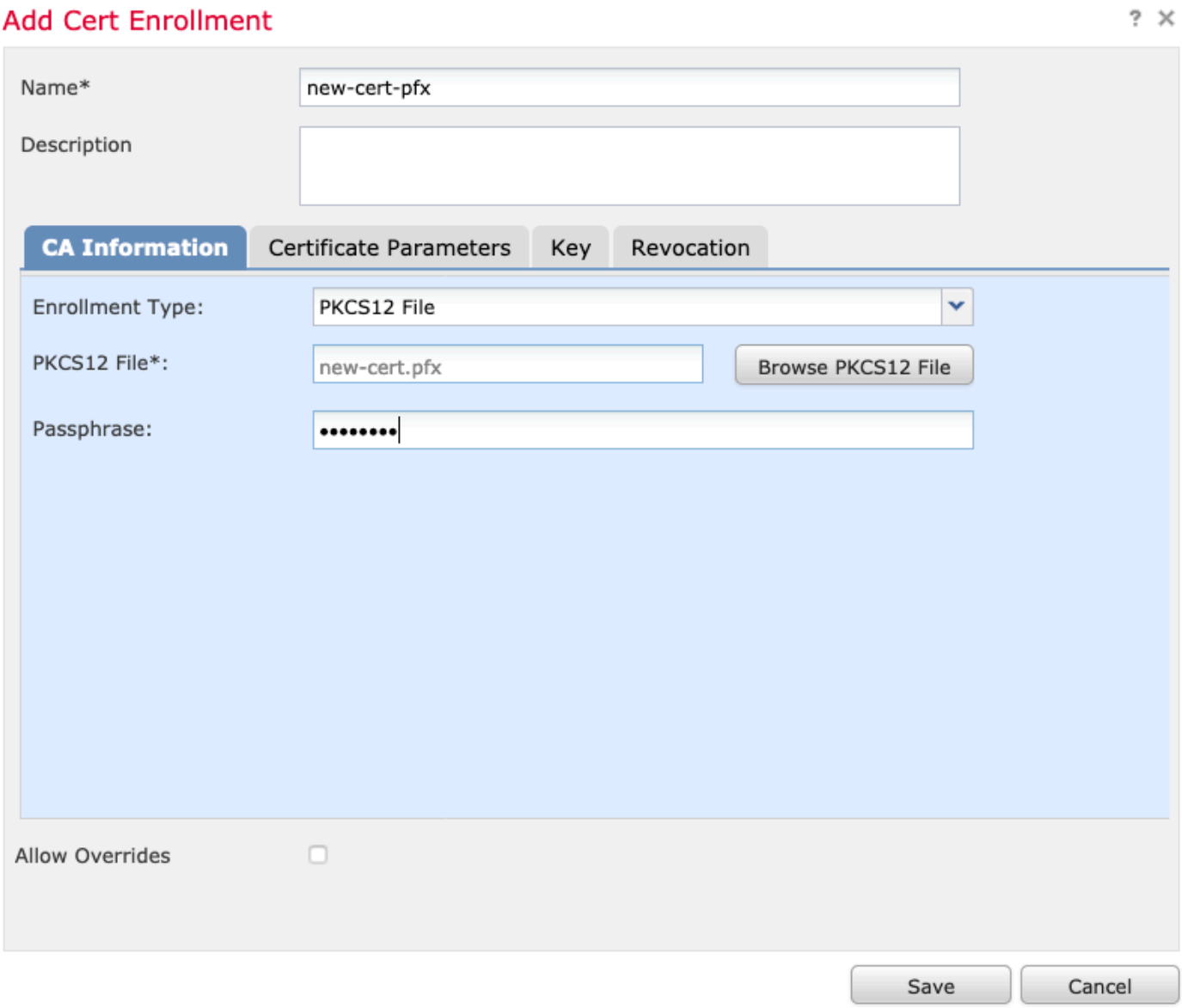
## Paso 7. Importe el archivo PKCS12 en el FMC

En el FMC, navegue hasta Device > Certificates e importe el certificado al firewall deseado como se muestra en la imagen.



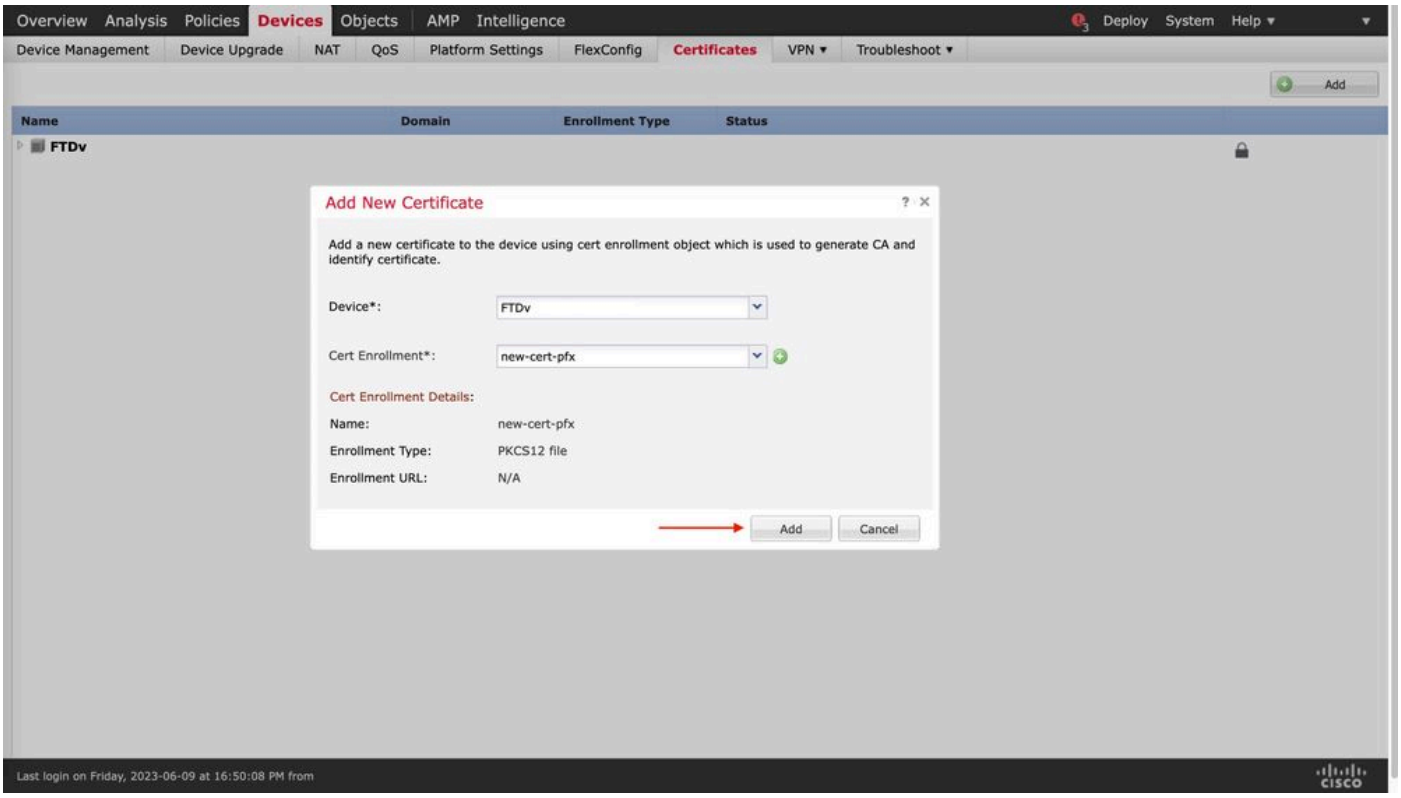

inscripción de certificados

Inserte un nombre para el nuevo certificado.




Inscripción

Agregue el nuevo certificado y espere al proceso de inscripción para implementar el nuevo certificado en el FTD.




de nueva certificación

El nuevo certificado debe estar visible sin una cruz roja en el campo CA.

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

En Windows, puede encontrar un problema en el que el sistema operativo muestre la cadena completa del certificado, aunque el archivo .pfx sólo contenga el certificado de ID, en el caso de que tenga la cadena subCA, CA en su almacén.

Para verificar la lista de certificados en un archivo .pfx, se pueden utilizar herramientas como certutil o openssl.

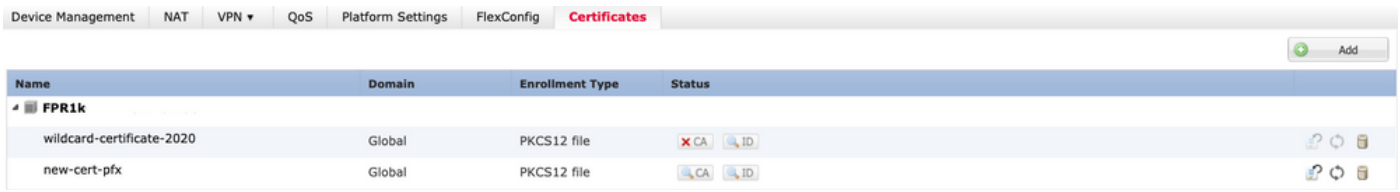
```
certutil -dump cert.pfx
```

El certutil es una utilidad de línea de comandos que proporciona la lista de certificados de un archivo .pfx. Debe ver toda la cadena con ID, SubCA, CA incluido (si lo hubiera).

Alternativamente, puede utilizar un comando openssl, como se muestra en el siguiente comando.

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

Para verificar el estado del certificado junto con la información de CA e ID, puede seleccionar los iconos y confirmar que se importó correctamente:



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).