

# Instalación y renovación de certificados en FTD gestionados por FMC

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Background](#)

[Configurar](#)

[Instalación de certificados](#)

[Inscripción con firma automática](#)

[Inscripción manual](#)

[Inscripción en PKCS12](#)

[Renovación de certificados](#)

[Renovación de certificado autofirmado](#)

[Renovación manual de certificados](#)

[Renovación PKCS12](#)

[Creación de PKCS12 con OpenSSL](#)

[Verificación](#)

[Ver certificados instalados en FMC](#)

[Ver certificados instalados en CLI](#)

[Troubleshoot](#)

[Comandos de Debug](#)

[Problemas comunes](#)

---

## Introducción

Este documento describe cómo instalar, confiar y renovar certificados en un FTD administrado por FMC.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- La inscripción manual de certificados requiere acceso a una CA de terceros de confianza.
- Algunos ejemplos de proveedores de CA de terceros son, entre otros, Entrust, Geotrust, GoDaddy, Thawte y VeriSign.
- Verifique que el FTD tenga la hora del reloj, la fecha y la zona horaria correctas. Con la

autenticación de certificados, se recomienda utilizar un servidor de protocolo de tiempo de la red (NTP) para sincronizar la hora en el FTD.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FMCv con 6.5
- FTDv con 6.5
- Para la creación de PKCS12, se utiliza 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). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Background

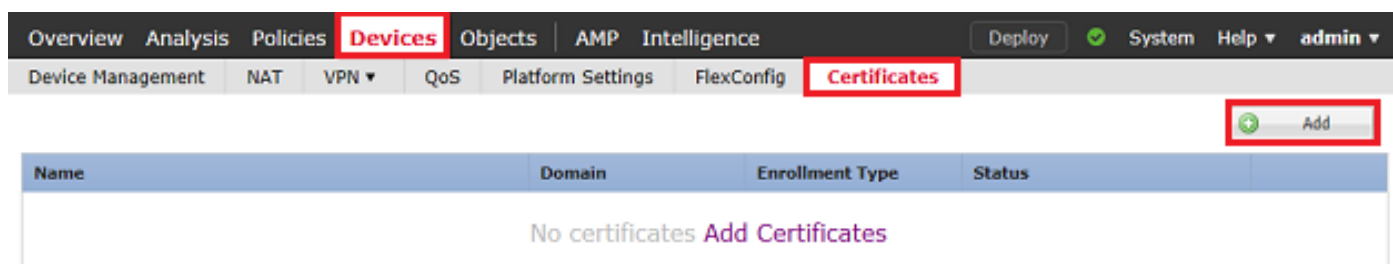
Este documento describe cómo instalar, confiar y renovar certificados autofirmados y certificados firmados por una autoridad de certificación (CA) de terceros o una CA interna en un Firepower Threat Defense (FTD) administrado por Firepower Management Center (FMC).

## Configurar

### Instalación de certificados

#### Inscripción con firma automática

1. Navegue hasta Dispositivos > Certificados, luego haga clic en Agregar como se muestra en la imagen.




2. Seleccione el dispositivo y el certificado se agregará a en el menú desplegable Device\*. A continuación, haga clic en el símbolo + verde que se muestra en la imagen.

### 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. Especifique un Nombre para el punto de confianza y, en la pestaña Información de CA, seleccione Tipo de Inscripción: Certificado Firmado Automáticamente como se muestra en la imagen.


### 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. En la pestaña Parámetros de Certificado, introduzca un nombre común para el certificado. Debe coincidir con la dirección fqdn o IP del servicio para el que se utiliza el certificado, como se muestra en la imagen.

**Add Cert Enrollment** ? X

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

5. (Opcional) En la pestaña Key, se puede especificar el tipo, el nombre y el tamaño de la clave privada utilizada para el certificado. De forma predeterminada, la clave utiliza una clave RSA con el nombre <Default-RSA-Key> y un tamaño de 2048; sin embargo, se recomienda utilizar un nombre único para cada certificado, de modo que no utilicen el mismo par de claves privada/pública que se muestra en la imagen.

## 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. Una vez hecho, haga clic en Guardar y luego haga clic en Agregar como se muestra en la imagen.

## 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. Una vez completado, el certificado autofirmado se muestra en la imagen.

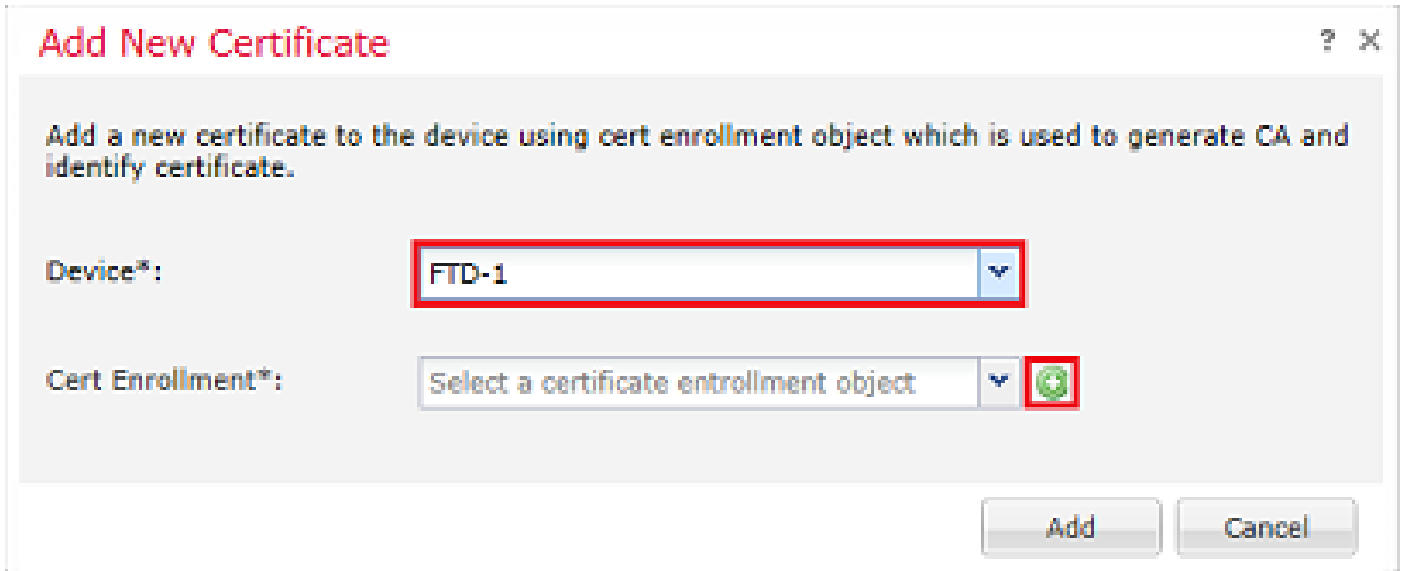
Overview Analysis Policies <b>Devices</b> Objects AMP Intelligence <span style="float: right;">Deploy System Help admin</span>			
Device Management NAT VPN QoS Platform Settings FlexConfig <b>Certificates</b>			
<span style="color: green;">+</span> Add			
Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed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

### Inscripción manual

1. Navegue hasta Dispositivos > Certificados y luego haga clic en Agregar como se muestra en la imagen.

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>			
<span style="color: green;">+</span> Add			
Name	Domain	Enrollment Type	Status
No certificates <a href="#">Add Certificates</a>			

2. Seleccione el dispositivo al que se agrega el certificado en el menú desplegable Device\* y, a continuación, haga clic en el símbolo verde+ como se muestra en la imagen.



3. Especifique un Nombre para el punto de confianza y, en la pestaña Información de la CA, seleccione Tipo de Inscripción: Manual. Introduzca el certificado con formato pem de la CA que se utiliza para firmar el certificado de identidad. Si este certificado no está disponible o no se conoce en este momento, agregue cualquier certificado de CA como marcador de posición y, una vez emitido el certificado de identidad, repita este paso para agregar la CA emisora real, como se muestra en la imagen.

## Add Cert Enrollment



Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:\*  
-----BEGIN CERTIFICATE-----  
MIIESzCCAjOgAwIBAgIIIItsWeBSsr5QwDQYJKoZIhvcNAQELBQAw  
MjEaMBgGA1UE  
ChMRQ2lzY28gU3lzdGVtcyBUQUxkFDASBgNVBAMTC1ZQTiBSb29  
O1ENBMB4XDTIw  
MDQwNTIzMjkwMFoXDTEwMDQwNTIzMjkwMFowOjEaMBgGA1UE  
ChMRQ2lzY28gU3lz  
dGVtcyBUQUxkHDAaBgNVBAMTE1ZQTiBjb3Rlcm1lZGlhdGUgQ0E  
wggEiMA0GCSqG  
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDII/m7uyjRUoyjyob7sWS  
AUVmnUMtovHen  
9VbgjowZs0hVcig/Lp2YYuawWRJhW99nagUBYtMyvY744sRw7AK  
AwlyROO1J6IT  
Is5suK60Yryz7JG3eNDqAroqJg/VeDeAjprpCW0YhHHYXAI0s7GXjHI  
S6nGIy/qP  
5RcPLdqx4/aFXw+DONJYHL0E5FlsfnrOeketnbABjkAkmOauNpS  
zN4FAISIk4  
DU3yX7d31GD4BBhxI7IPsDH933AUm6zxntC9AxK6gHAY8/8pUPv

Allow Overrides

Save Cancel

4. En la pestaña Parámetros de Certificado, introduzca un nombre común para el certificado. Debe coincidir con la dirección fqdn o IP del servicio para el que se utiliza el certificado, como se muestra en la imagen.



## 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. (Opcional) En la pestaña Clave, opcionalmente se puede especificar el tipo, el nombre y el tamaño de la clave privada utilizada para el certificado. De forma predeterminada, la clave utiliza una clave RSA con el nombre <Default-RSA-Key> y un tamaño de 2048; sin embargo, se recomienda utilizar un nombre único para cada certificado para que no utilicen el mismo par de claves privada/pública que se muestra en la imagen.

## 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. (Opcional) En la pestaña Revocación, la revocación de la Lista de revocación de certificados (CRL) o del Protocolo de estado de certificados en línea (OCSP) está activada y se puede configurar. De forma predeterminada, ninguna de las opciones está marcada como se muestra en la imagen.

## 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. Una vez hecho, haga clic en Guardar y luego haga clic en Agregar como se muestra en la imagen.

### 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. Después de procesar la solicitud, FMC presenta la opción de añadir un certificado de identidad. Haga clic en el botón ID como se muestra en la imagen.

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Manual	Global	Manual	<input type="button" value="CA"/> <input type="button" value="ID"/> <input type="button" value="Identity certificate import required"/>

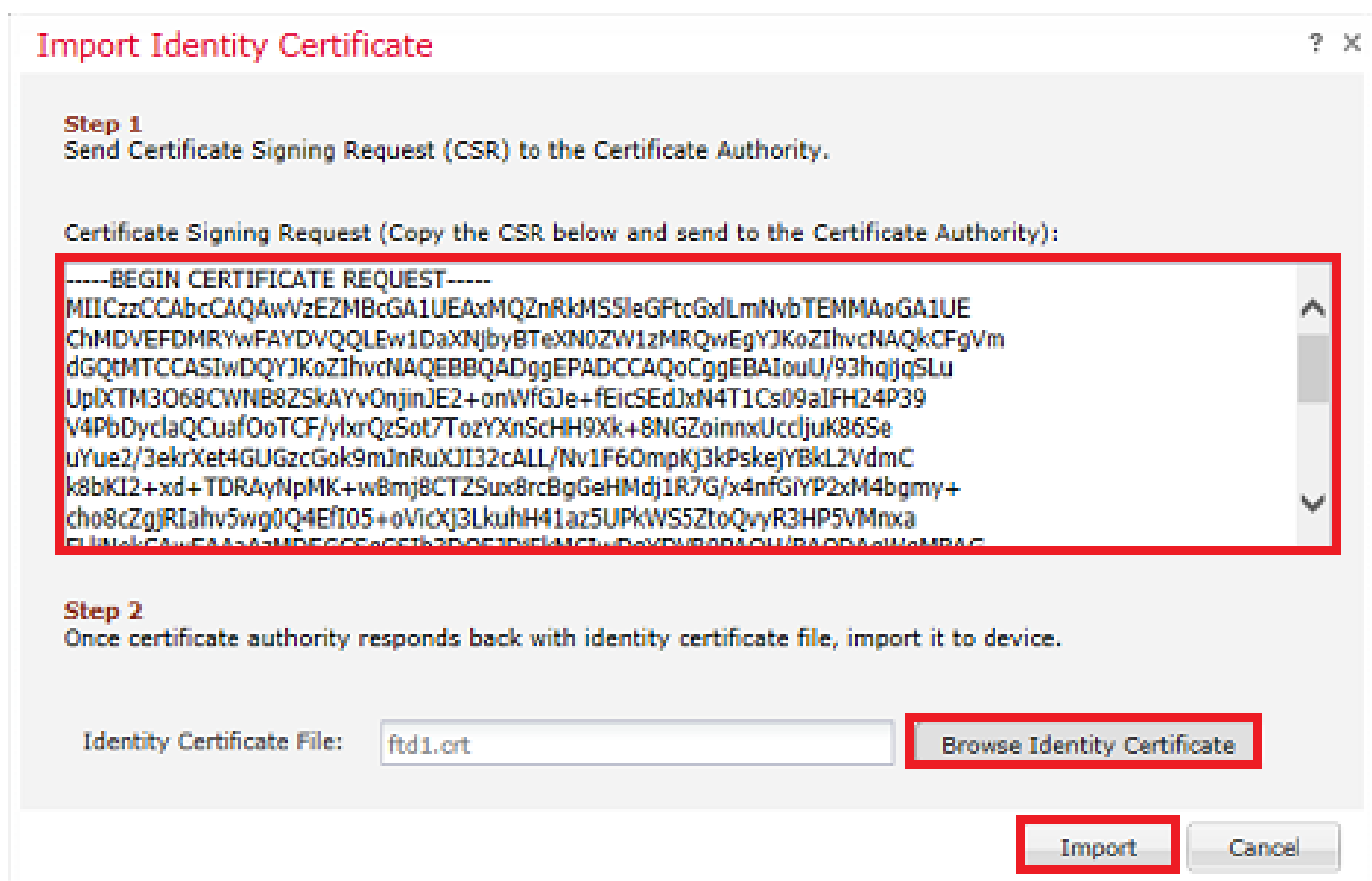
9. Aparece una ventana que informa de que se ha generado una CSR. Haga clic en Yes como se muestra en la imagen.

## Warning

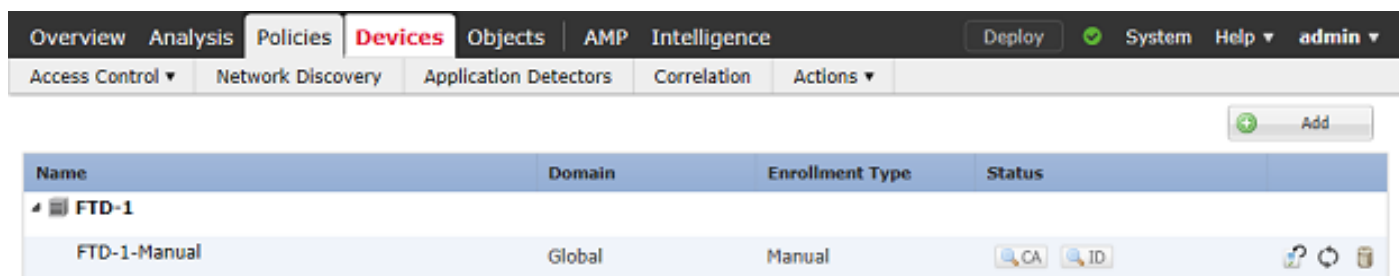
**This operation will generate Certificate Signing Request do you want to continue?**

10. A continuación, se genera una CSR que se puede copiar y enviar a una CA. Una vez firmado

el CSR, se proporciona un certificado de identidad. Busque el certificado de identidad proporcionado, selecciónelo y haga clic en Importar como se muestra en la imagen.

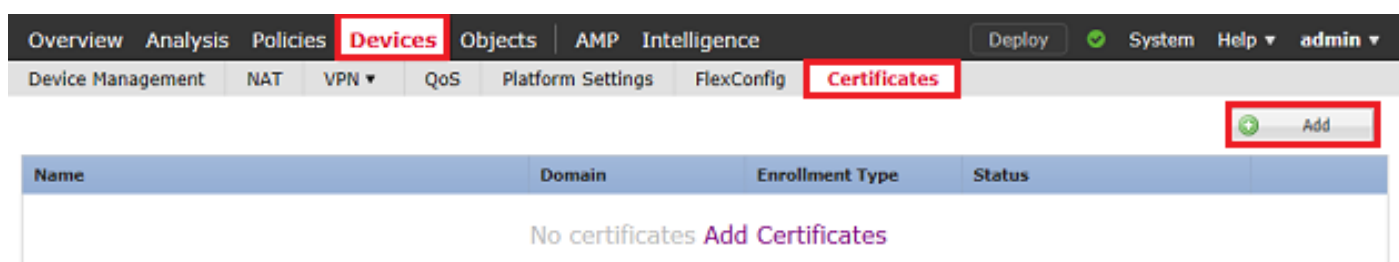


11. Una vez completado, el certificado manual se muestra como en la imagen.



## Inscripción en PKCS12

1. Para instalar un archivo PKCS12 recibido o creado, navegue hasta Dispositivos > Certificados y luego haga clic en Agregar como se muestra en la imagen.



2. Seleccione el dispositivo al que se agrega el certificado en el menú desplegable Device\* y, a

continuación, haga clic en el símbolo verde+ como se muestra en la imagen.

**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. Especifique un Nombre para el punto de confianza y, en la pestaña Información de CA, seleccione Tipo de Inscripción: Archivo PKCS12. Busque el archivo PKCS12 creado y selecciónelo. Introduzca el código de acceso utilizado al crear el PKCS12, como se muestra en la imagen.

## Add Cert Enrollment



Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

PKCS12 File\*:

Passphrase:

Allow Overrides

4. (Opcional) Las pestañas Parámetros de certificado y Clave están atenuadas, ya que se han creado con PKCS12. Sin embargo, la pestaña Revocación para habilitar la comprobación de revocación de CRL o OCSP se puede modificar. De forma predeterminada, ninguna de las opciones está marcada como se muestra en la imagen.

## 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

5. Una vez hecho, haga clic en Guardar y luego haga clic en Agregar en esta ventana como se muestra en la imagen.



### 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** **Cancel**

6. Una vez completado, el certificado PKCS12 se ve como se muestra en la imagen.

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

## Renovación de certificados

### Renovación de certificado autofirmado

1. Presione el botón Re-enroll certificate (Reinscribir certificado) como se muestra en la imagen.

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

2. Una ventana le indica que el certificado autofirmado se elimina y reemplaza. Haga clic en Yes como se muestra en la imagen.

## 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. Se envía al FTD un documento firmado automáticamente renovado. Esto puede verificarse al hacer clic en el botón ID (ID) y comprobar la hora válida.

### Renovación manual de certificados

1. Presione el botón Re-enroll certificate (Reinscribir certificado) como se muestra en la imagen.

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

2. Una ventana solicita que se genere una solicitud de firma de certificado. Haga clic en Yes como se muestra en la imagen.

## Warning

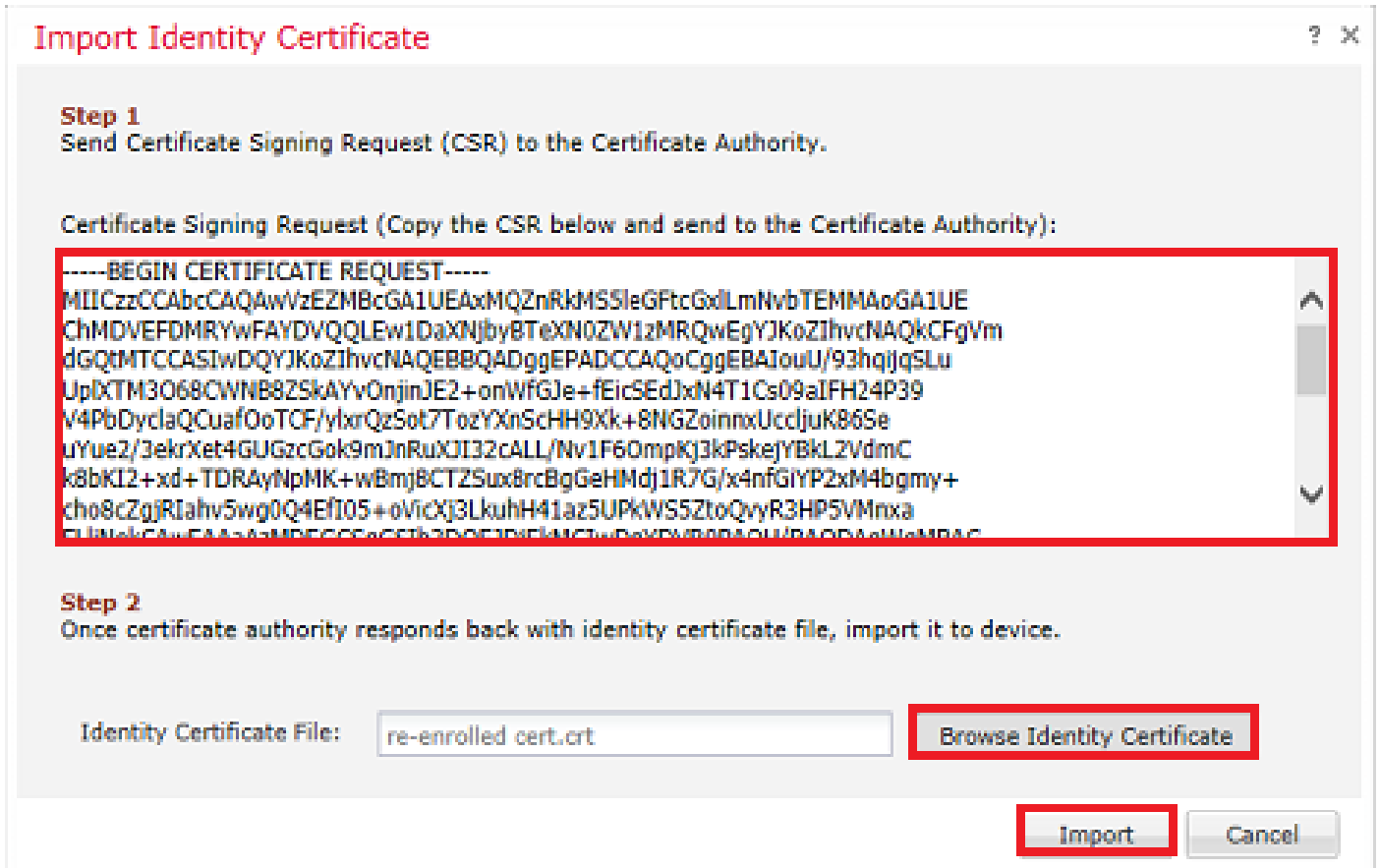


This operation will generate Certificate Signing Request do you want to continue?

Yes

No

3. En esta ventana, se genera una CSR que se puede copiar y enviar a la misma CA que firmó el certificado de identidad anteriormente. Una vez firmado el CSR, se proporciona el certificado de identidad renovado. Busque el certificado de identidad proporcionado, selecciónelo y haga clic en Importar como se muestra en la imagen.



4. Se envía un certificado manual renovado al FTD. Esto puede verificarse al hacer clic en el botón ID (ID) y comprobar la hora válida.

### Renovación PKCS12

Si hace clic en el botón Volver a inscribir certificado, el certificado no se renovará. Para renovar un PKCS12, es necesario crear y cargar un nuevo archivo PKCS12 con el uso de los métodos mencionados anteriormente.

### Creación de PKCS12 con OpenSSL

1. Con el uso de OpenSSL o una aplicación similar, genere una clave privada y una solicitud de firma de certificado (CSR). Este ejemplo muestra una clave RSA de 2048 bits denominada private.key y una CSR denominada ftd1.csr que se crea en 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 be 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. Copie el CSR generado y envíelo a una CA. Una vez firmado el CSR, se proporciona un certificado de identidad. Normalmente, también se proporcionan los certificados de CA. Para crear un PKCS12, ejecute uno de estos comandos en OpenSSL:

Para incluir solamente el certificado de CA emitido dentro de PKCS12, utilice este comando:

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

- ftd.pfx es el nombre del archivo pkcs12 (en formato der) exportado por openssl.
- ftd.crt es el nombre del certificado de identidad firmado emitido por la CA en formato pem.
- private.key es el par de claves creado en el paso 1.
- ca.crt es el certificado de la autoridad certificadora emisora en formato pem.

Si el certificado es parte de una cadena con una CA raíz y 1 o más CA intermedias, este comando se puede utilizar para agregar la cadena completa en el 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 es el nombre del archivo pkcs12 (en formato der) exportado por OpenSSL.
- ftd.crt es el nombre del certificado de identidad firmado emitido por la CA en formato pem.
- private.key es el par de claves creado en el paso 1.
- cachain.pem es un archivo que contiene los certificados de CA de la cadena que comienzan con la CA intermedia emisora y terminan con la CA raíz en formato pem.

Si se devuelve un archivo PKCS7 (.p7b, .p7c), estos comandos también se pueden utilizar para crear el PKCS12. Si el p7b está en formato der, asegúrese de agregar -inform der a los argumentos; de lo contrario, no lo incluya:

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

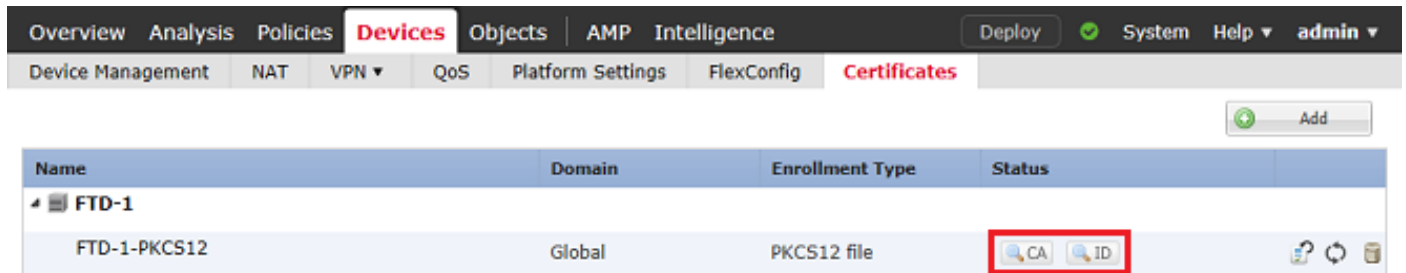
- ftd.p7b es el PKCS7 devuelto por la CA que contiene el certificado de identidad firmado y la cadena de CA.
- ftdpem.crt es el archivo p7b convertido.
- ftd.pfx es el nombre del archivo pkcs12 (en formato der) exportado por OpenSSL.
- private.key es el par de claves creado en el paso 1.

## Verificación

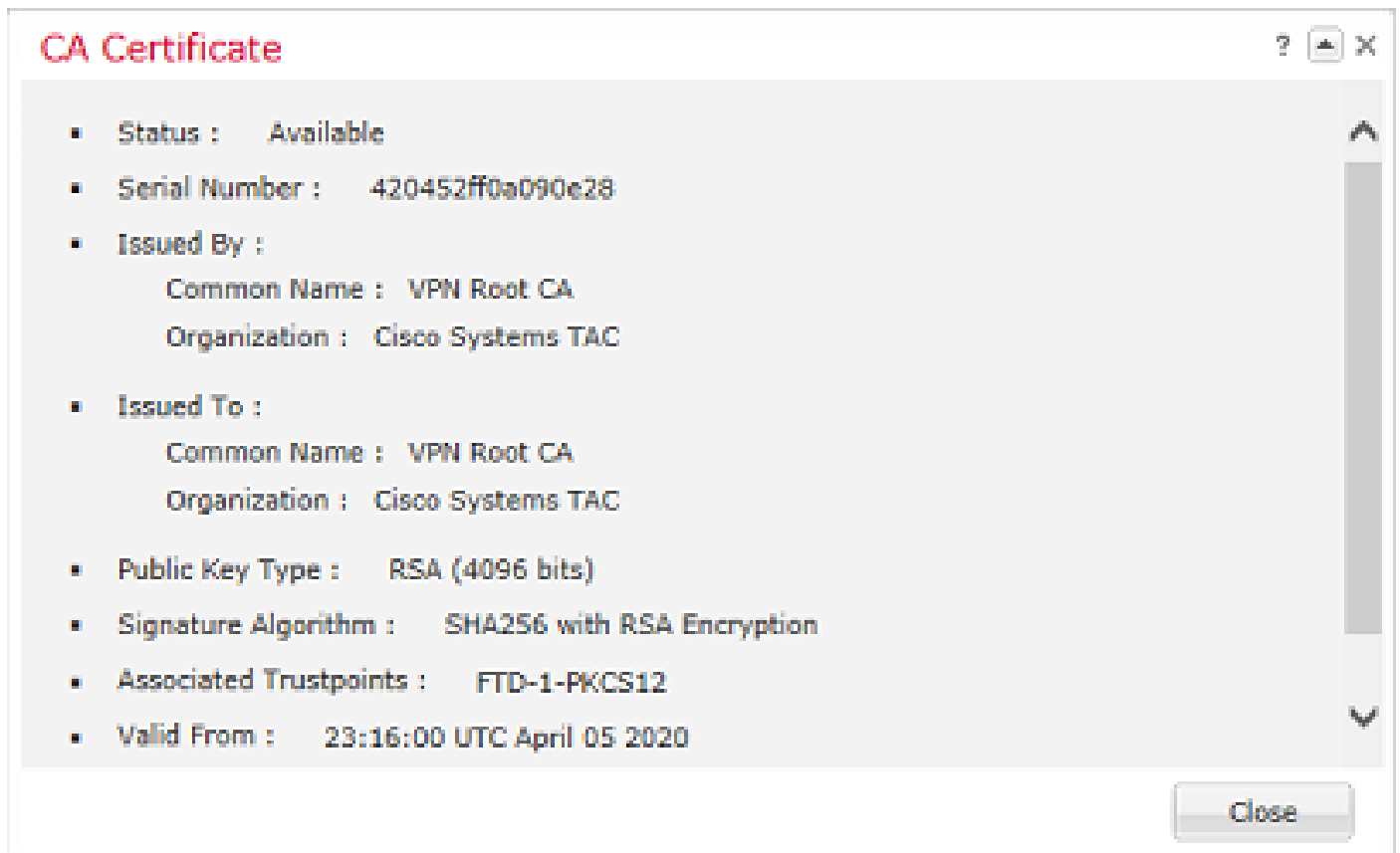
Utilice esta sección para confirmar que su configuración funcione correctamente.

### Ver certificados instalados en FMC

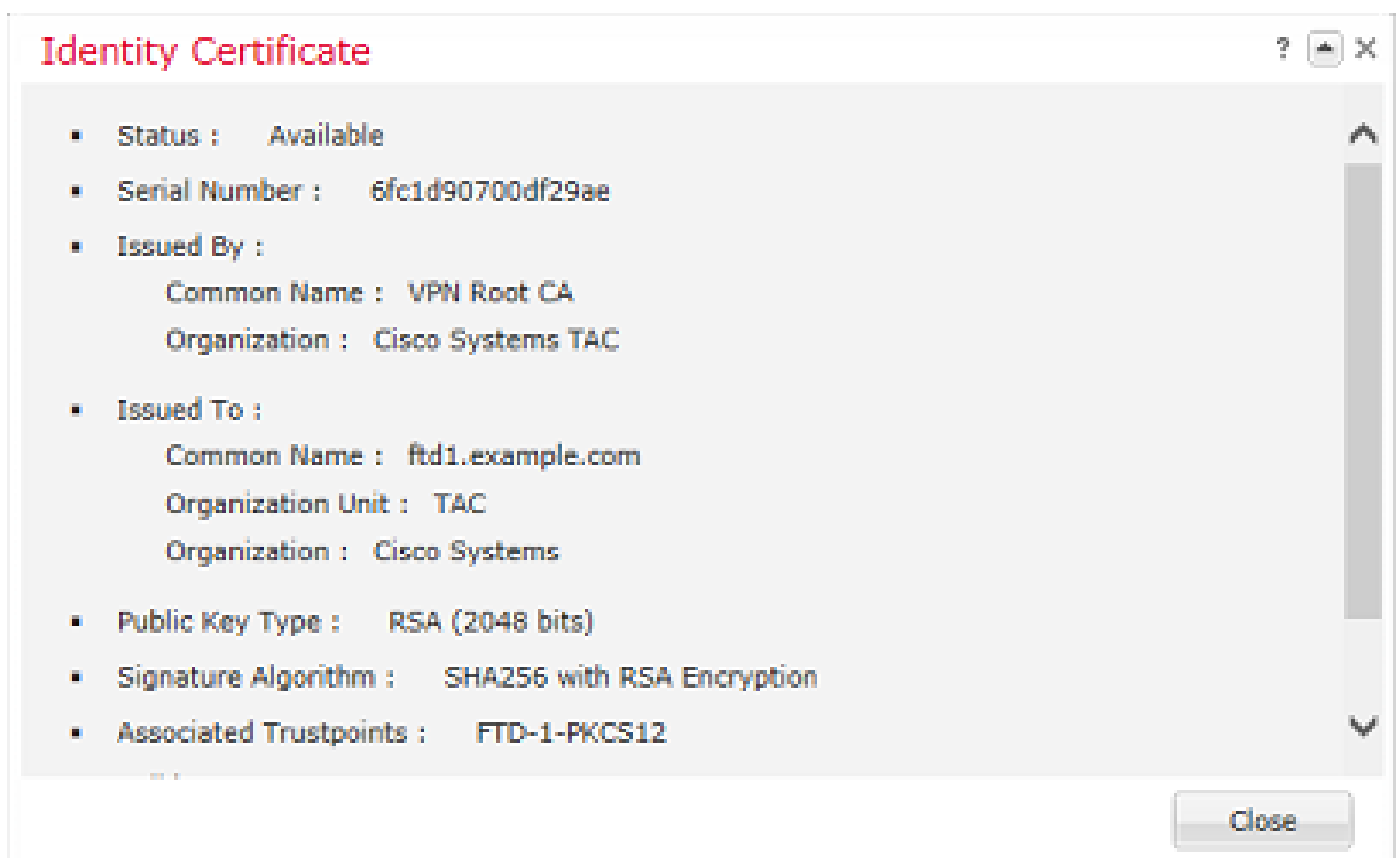
En FMC, vaya a Devices > Certificates. Para el punto de confianza relevante, haga clic en la CA o ID para ver más detalles sobre el certificado como se muestra en la imagen.



Verifique el certificado de la CA como se muestra en la imagen.



Verifique el certificado de identidad como se muestra en la imagen.



Ver certificados instalados en CLI

SSH al FTD e ingrese el comando 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
```

## Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

### Comandos de Debug

Las depuraciones se pueden ejecutar desde la CLI de diagnóstico después de que el FTD se conecte a través de SSH en el caso de una falla en la Instalación del Certificado SSL:

```
debug crypto ca 14
```

En las versiones anteriores de FTD, estos debugs están disponibles y se recomiendan para la

solución de problemas:

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 255

## Problemas comunes

Sigue apareciendo el mensaje "Se requiere la importación del certificado de identidad" después de importar el certificado de identidad emitido.

Esto puede ocurrir debido a dos problemas separados:

1. El certificado de CA emisor no se agregó en la inscripción manual

Cuando se importa el certificado de identidad, se compara con el certificado de CA agregado en la ficha Información de CA en la inscripción manual. A veces, los administradores de red no tienen el certificado de CA para la CA que se utiliza para firmar su certificado de identidad. En esta situación, es necesario agregar un certificado de CA de marcador de posición al realizar la inscripción manual. Una vez emitido el certificado de identidad y proporcionado el certificado de CA, se puede realizar una nueva inscripción manual con el certificado de CA correcto. Cuando vuelva a utilizar el asistente de inscripción manual, asegúrese de especificar el mismo nombre y tamaño para el par de claves que en la inscripción manual original. Una vez hecho esto, en lugar de reenviar el CSR a la CA de nuevo, el certificado de identidad emitido anteriormente se puede importar al punto de confianza recién creado con el certificado de CA correcto.

Para comprobar si se aplicó el mismo certificado de CA en la inscripción manual, haga clic en el botón CA como se especifica en la sección Verify o compruebe la salida de show crypto ca certificates. Los campos como Emitido para y Número de serie se pueden comparar con los campos del certificado de CA proporcionado por la autoridad de certificación.

2. El par de claves del punto de confianza creado es diferente del par de claves utilizado cuando se crea el CSR para el certificado emitido.

Con la inscripción manual, cuando se generan el par de claves y la CSR, la clave pública se agrega a la CSR para que se pueda incluir en el certificado de identidad emitido. Si por alguna razón se modifica el par de claves del FTD o si el certificado de identidad emitido incluye una clave pública diferente, el FTD no instala el certificado de identidad emitido. Para comprobar si esto ha ocurrido, hay dos pruebas diferentes:

En OpenSSL, estos comandos se pueden ejecutar para comparar la clave pública en el CSR con la clave pública en el certificado emitido:

```
openssl req -noout -modulus -in ftd.csr
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEB096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C
```



C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B  
B966DA10BF24771CFE55327C5A14B96235E9

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

```
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE  
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9  
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C  
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B  
B966DA10BF24771CFE55327C5A14B96235E9
```

- ftd.csr es la CSR copiada de FMC en la inscripción manual.
- id.crt es el certificado de identidad firmado por la CA.

Alternativamente, el valor de la clave pública en el FTD también puede compararse con la clave pública en el certificado de identidad emitido. Tenga en cuenta que los primeros caracteres del certificado no coinciden con los de la salida de FTD debido al relleno:

Certificado de identidad emitido abierto en PC con Windows:

**Certificate** [X]

General Details Certification Path

Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	VPN Intermediate CA, Cisco S...
Valid from	Wednesday, April 8, 2020 1:0...
Valid to	Monday, April 5, 2021 7:29:00...
Subject	ftd-1, Cisco Systems, TAC, ftd...
<b>Public key</b>	<b>RSA (2048 Bits)</b>
Public key parameters	05 00

```

ec 91 e8 d8 06 42 f6 55 d9 82 93 c6 ca 23
6f b1 77 e4 c3 44 0c 8d a4 c2 be c0 19 a3
f0 24 d9 4a ec 7c ad c0 60 19 e1 cc 76 3d
51 ec 6f f1 e2 77 c6 89 83 f6 c4 ce 1b 82
6c be 72 1a 3c 71 98 23 44 86 a1 bf 9c 20
d1 0e 04 7c 8d 39 fa 85 62 71 78 f7 2e 4b
a1 1f 8d 5a cf 95 0f 91 64 b9 66 da 10 bf
24 77 1c fe 55 32 7c 5a 14 b9 62 35 e9 02
03 01 00 01

```

Edit Properties... Copy to File...

OK

Salida de clave pública extraída del certificado de identidad:

```
f6e0fdfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b8af3a491b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8da4c2bec0e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f8d5acf955327c5a14b96235e90203010001
```

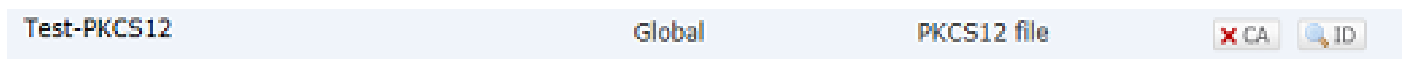
Muestra la salida rsa de la clave crypto mypubkey desde el FTD. Cuando se realizó la inscripción manual, se utilizó la <Default-RSA-Key> para crear el CSR. La sección en negrita coincide con la salida de clave pública extraída del certificado de identidad.

```
> 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 roja junto a CA en FMC

Esto puede ocurrir con la inscripción PKCS12 porque el certificado de CA no está incluido en el paquete PKCS12.



Para solucionar este problema, PKCS12 necesita que se agregue el certificado de CA.

Ejecute estos comandos para extraer el certificado de identidad y la clave privada. La contraseña que se utiliza en el momento de la creación de PKCS12 y la clave privada segura son necesarias:

```
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+CHC8X8BFjuTJYoo116uGgiB4Jz2Y9ZeFSQz
Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBg1ghkgBhvCAQOEERYPeGnhIGN1
cnRpZmljYXR1MA0GCsQGSiB3DQEBcWUAA4IBAQCv/MgshWxXtwpwmMF/6KqEj8nB
S1jbfz1zNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRY54taRI27W+gLneCbQAux
9amxXuhpxP5E0hnc+tsYS9eriAKpHuS1Y/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+
k2ebkb1FT0YRQT1Z4tZHSqX1LFPZe170NZEUG7rIcWak1Yw7XNUPh0n6FHL/ieIZ
IhvIfj+IgQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E
Gnh8r31903A1kPMBkMdx0q1pzo2naIy2KGrUnOSHajVwclR9dTPWIDyjd95YoeS
IUE7Ma00pjJc02FNbWyxNrxRyt+4hp3aJt0ZW83FHiS1B5UIzGrBMAgKJc2Hb2RTV
9gxZGve1cRco1LeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShn0wHzridF8Zn
F06XvBDSyXVSpkxwAd1Twxq62tUnLIkyRXo2CSz8z8W29UXmF04o3G67n28//LJ
Ku8wj1jeq1vFgXSQiWLADNH772RNwzCMeobfxG1BprF9DPT8yvyBdQviUIuFpJ
nNs5FYbLTv9ygZ1S9xwQpTcqEu+y4F5BJuYlMhqcZ+VpFA4nM0YHhZ5M3sccRSR4
1L+a3BPJJsh1TIJQg0TixDaveCfpDcpS+ydUgS6WY8xw17v0+1f7y5z1t4TkZrt
ItBHHA6yDzR0Cn0/ZH3y88a/asDcuw6bsRaY5iT8nAWGTQved3xXj+EgeRs25HB
dIBX5gTvqN7qDanhkaPUcEawj1/38M0pAYULei3e1fKKrhWaysBFaV/BeUMWuNW
BmKprkKKQv/JdWnoJ149KcS4bfa3GHG9Xxnyvbg8HxopcYFMTEjao+wLZH9agqKe
Y0jyoHFN6ccBBC7vn7u12tmXOM5RcnPLmaDaBFDSBBFS8Y8VkeHn3P0q7+sEQ26d
vL807WdgLH/wKqovoJRYxwzz+TryRq9cd5BNyyLaABESa1sWRhk81C2P+B+Jdg9w
d6RsvJ2dt3pd1/+pUR3CdC0b8qRZOoL03+onUIUoEsCCndp0x8Yj/mvc6ReXtOKB
2qVmhVMYseiU1rOAGt7XMe1UuiJ+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-----
```

Una vez completados, el certificado de identidad y la clave privada se pueden colocar en archivos

separados y el certificado de CA se puede importar en un nuevo archivo PKCS12 con el uso de los pasos mencionados en el paso 2 de la creación de PKCS12 con OpenSSL.

## 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).

## 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).