

# Instalar e Renovar Certificados no FTD Gerenciado pelo FMC

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Background](#)

[Configurar](#)

[Instalação do certificado](#)

[Inscrição com assinatura automática](#)

[Inscrição manual](#)

[Inscrição PKCS12](#)

[Renovação de certificado](#)

[Renovação de certificado autoassinado](#)

[Renovação manual de certificado](#)

[Renovação de PKCS12](#)

[Criação de PKCS12 com OpenSSL](#)

[Verificar](#)

[Exibir certificados instalados no FMC](#)

[Exibir certificados instalados na CLI](#)

[Troubleshooting](#)

[Comandos debug](#)

[Problemas comuns](#)

---

## Introdução

Este documento descreve como instalar, confiar e renovar certificados em um FTD gerenciado pelo FMC.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O registro manual do certificado requer acesso a uma CA de terceiros confiável.
- Exemplos de fornecedores de CA de terceiros incluem, entre outros, Entrust, Geotrust, GoDaddy, Thawte e VeriSign.
- Verifique se o FTD tem a hora, a data e o fuso horário corretos. Com a autenticação do

certificado, é recomendável usar um servidor Network Time Protocol (NTP) para sincronizar a hora no FTD.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FMCv executando 6.5
- FTDv executando 6.5
- Para a criação de PKCS12, o OpenSSL é usado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Background

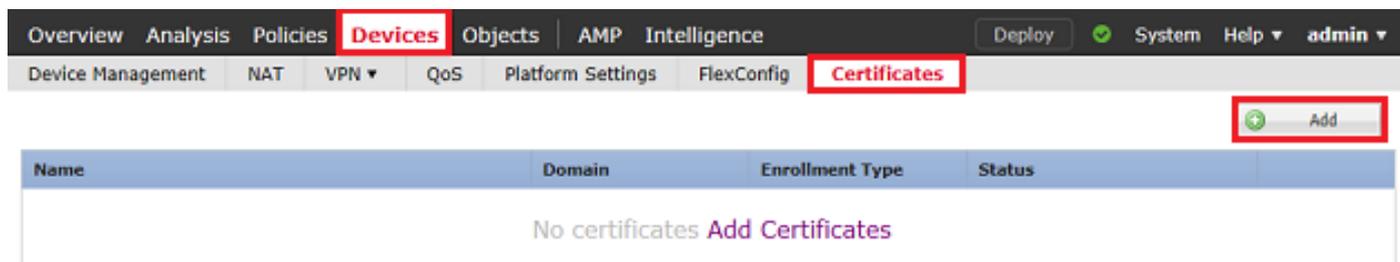
Este documento descreve como instalar, confiar e renovar certificados autoassinados e certificados assinados por uma CA (Certificate Authority, autoridade de certificação) de terceiros ou CA interna em um FTD (Threat Defense, defesa contra ameaças) do Firepower gerenciado pelo FMC (Firepower Management Center, centro de gerenciamento do Firepower).

## Configurar

### Instalação do certificado

#### Inscrição com assinatura automática

1. Navegue até Devices > Certificates e clique em Add conforme mostrado na imagem.



2. Selecione o dispositivo ao qual o certificado será adicionado no menu suspenso Device\*. Em seguida, clique no símbolo verde +, conforme mostrado na imagem.

### 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\*:

3. Especifique um Nome para o ponto de confiança e, na guia Informações da CA, selecione Tipo de Registro: Certificado Autoassinado conforme mostrado na imagem.

### Add Cert Enrollment

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. Na guia Parâmetros do Certificado, informe um Nome Comum para o certificado. Ele deve

corresponder ao fqdn ou ao endereço IP do serviço para o qual o certificado é usado, conforme mostrado na imagem.

### 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) Na guia Chave, o tipo, o nome e o tamanho da chave privada usada para o certificado podem ser especificados. Por padrão, a chave usa uma chave RSA com o nome de <Default-RSA-Key> e um tamanho de 2048; no entanto, é recomendável usar um nome exclusivo para cada certificado, para que eles não usem o mesmo par de chaves privadas/públicas como mostrado na imagem.

## 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

6. Depois de concluir, clique em Salvar e em Adicionar, conforme mostrado na imagem.

### 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. Depois de concluído, o certificado autoassinado é mostrado na imagem.

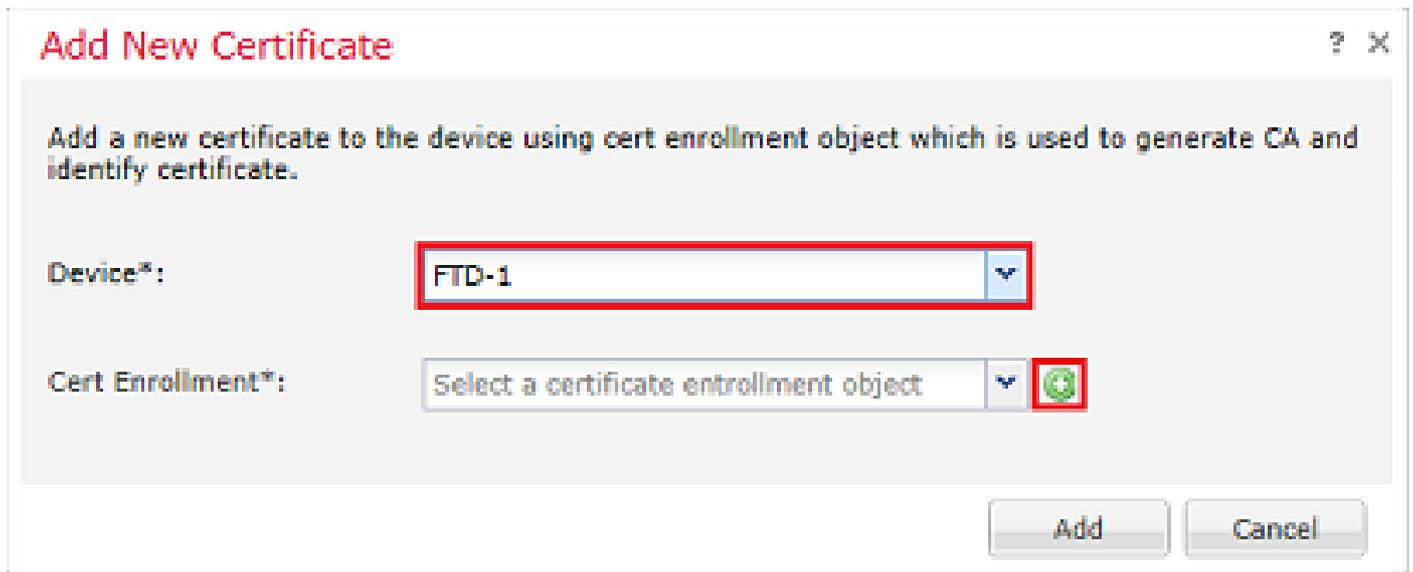
Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA ID

### Inscrição manual

1. Navegue até Devices > Certificates e clique em Add conforme mostrado na imagem.

Name	Domain	Enrollment Type	Status
No certificates <a href="#">Add Certificates</a>			

2. Selecione o dispositivo ao qual o certificado é adicionado no menu suspenso Device\* e clique no símbolo + verde conforme mostrado na imagem.



3. Especifique um Nome para o ponto de confiança e, na guia Informações da CA, selecione Tipo de Inscrição: Manual. Insira o certificado de formato pem da autoridade de certificação usada para assinar o certificado de identidade. Se este certificado não estiver disponível ou não for conhecido no momento, adicione qualquer certificado CA como um espaço reservado e, uma vez que o certificado de identidade seja emitido, repita esta etapa para adicionar a CA emissora real, como mostrado na imagem.



## 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) Na guia Chave, o tipo, o nome e o tamanho da chave privada usada para o certificado podem ser especificados opcionalmente. Por padrão, a chave usa uma chave RSA com o nome de <Default-RSA-Key> e um tamanho de 2048; no entanto, é recomendável usar um nome exclusivo para cada certificado para que ele não use o mesmo par de chaves privadas/públicas como mostrado na imagem.

## Add Cert Enrollment

? X

The screenshot shows the 'Add Cert Enrollment' dialog box with the 'Key' tab selected. The 'Name' field contains 'FTD-1-Manual'. The 'Description' field is empty. The 'Key Type' is set to 'RSA'. The 'Key Name' is '<Default-RSA-Key>'. The 'Key Size' is '2048'. The 'Advanced Settings' section is expanded, showing the 'Ignore IPsec Key Usage' checkbox, which is unchecked. Below this, there is a note: 'Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.' At the bottom left, the 'Allow Overrides' checkbox is also unchecked. At the bottom right, there are 'Save' and 'Cancel' buttons.

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) Na guia Revogação, a revogação da Lista de Revogação de Certificados (CRL) ou do Protocolo de Status de Certificados On-line (OCSP) está marcada e pode ser configurada. Por padrão, nenhuma dessas opções é marcada como mostrado na imagem.

## Add Cert Enrollment



Name\*

Description

CA Information Certificate Parameters Key **Revocation**

Enable Certificate Revocation Lists (CRL)

- Use CRL distribution point from the certificate
- User 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. Depois de concluir, clique em Salvar e em Adicionar, conforme mostrado na imagem.

### 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-Manual

Enrollment Type: Manual

SCEP URL: NA

8. Após processar a solicitação, o FMC apresenta a opção de adicionar um certificado de identidade. Clique no botão ID conforme mostrado na imagem.

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"/>

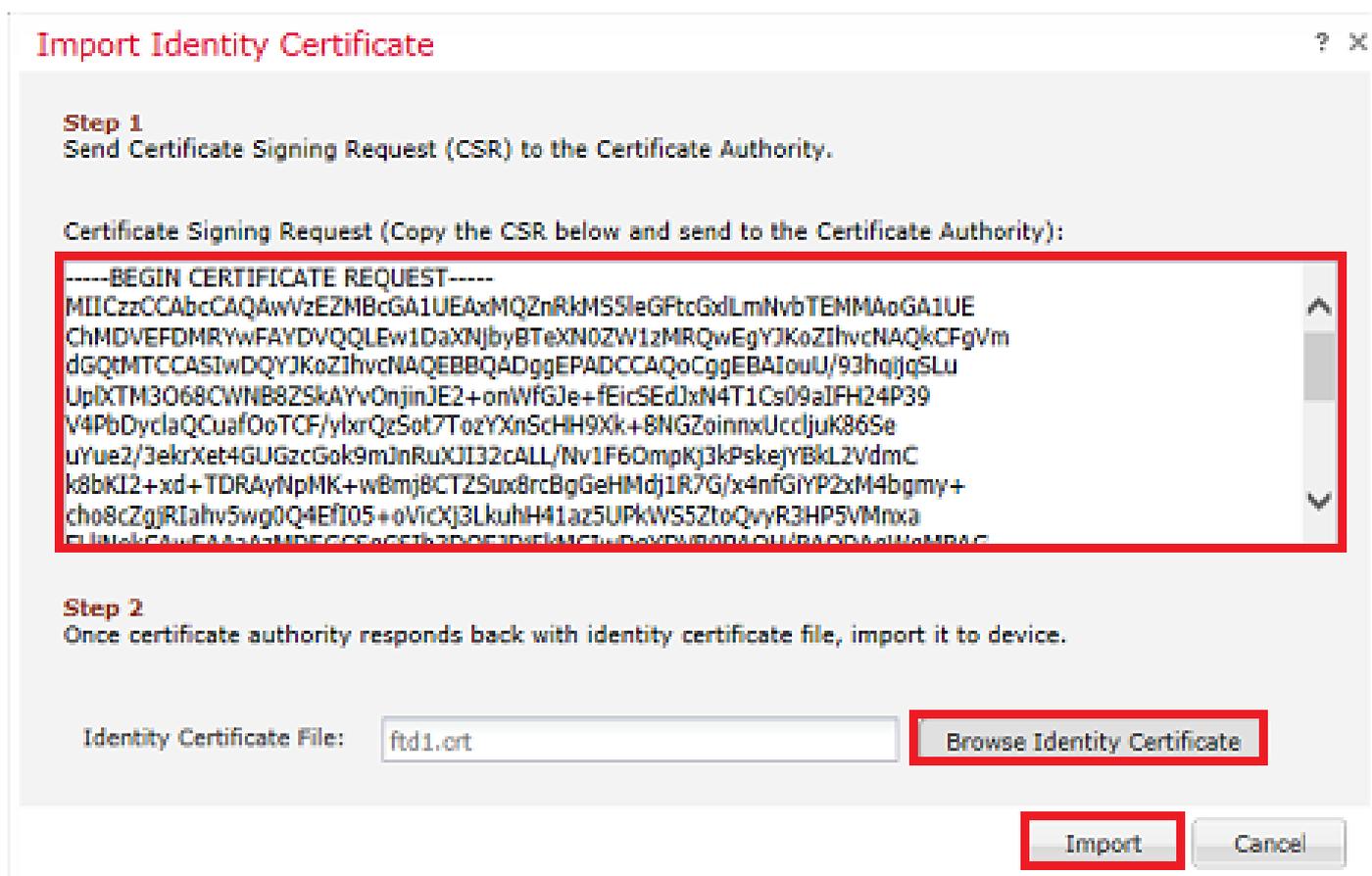
9. Será exibida uma janela informando que um CSR foi gerado. Clique em Sim como mostrado na imagem.

## Warning

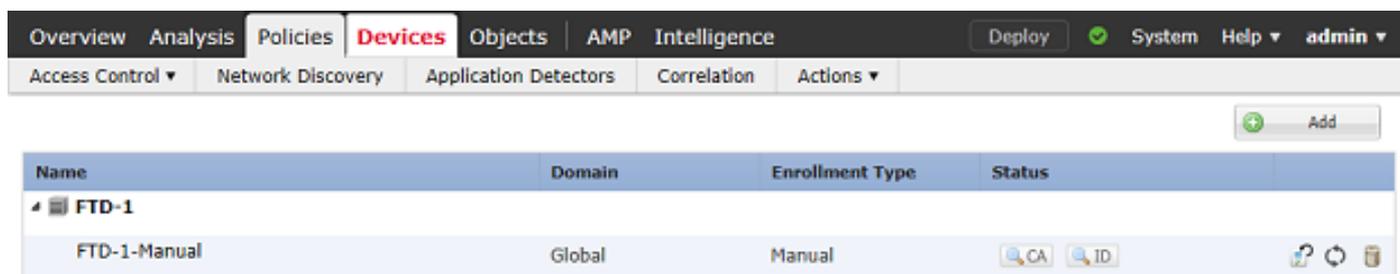
This operation will generate Certificate Signing Request do you want to continue?

10. Em seguida, é gerado um CSR que pode ser copiado e enviado para uma CA. Depois que o

CSR for assinado, um certificado de identidade será fornecido. Navegue até o certificado de identidade fornecido, selecione-o e clique em Importar conforme mostrado na imagem.

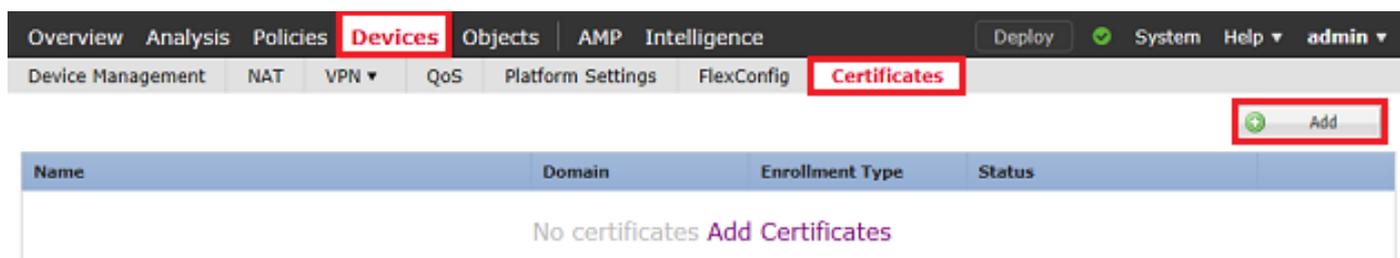


11. Uma vez concluído, o certificado manual é mostrado como na imagem.



## Inscrição PKCS12

1. Para instalar um arquivo PKCS12 recebido ou criado, navegue para Devices > Certificates e clique em Add conforme mostrado na imagem.



2. Selecione o dispositivo ao qual o certificado é adicionado no menu suspenso Device\* e clique

no símbolo + verde conforme mostrado na imagem.

**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 um Nome para o ponto de confiança e, na guia Informações da CA, selecione Tipo de Registro: Arquivo PKCS12. Navegue até o arquivo PKCS12 criado e selecione-o. Digite a senha usada ao criar o PKCS12 como mostrado na imagem.

## Add Cert Enrollment



Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

PKCS12 File\*:

Passphrase:

Allow Overrides

4. (Opcional) As guias Parâmetros do Certificado e Chave estão acinzentadas, pois elas já foram criadas com o PKCS12, no entanto, a guia Revogação para ativar a verificação de revogação de CRL e/ou OCSP pode ser modificada. Por padrão, nenhuma das opções é verificada conforme mostrado na imagem.

## 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

5. Depois de concluir, clique em Salvar e em Adicionar nesta janela, conforme mostrado na imagem.

### 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**

6. Uma vez concluído, o certificado PKCS12 parece como mostrado na imagem.

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

## Renovação de certificado

### Renovação de certificado autoassinado

1. Pressione o botão Reenrolar certificado como mostrado na imagem.

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

2. Uma janela avisará que o certificado autoassinado será removido e substituído. Clique em Sim como mostrado na imagem.

## 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. Uma assinatura automática renovada é enviada para o FTD. Isso pode ser verificado quando você clica no botão ID e marca a hora válida.

### Renovação manual de certificado

1. Pressione o botão Reenrolar certificado como mostrado na imagem.

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

2. Uma janela solicita que uma solicitação de assinatura de certificado seja gerada. Clique em Sim como mostrado na imagem.

## Warning

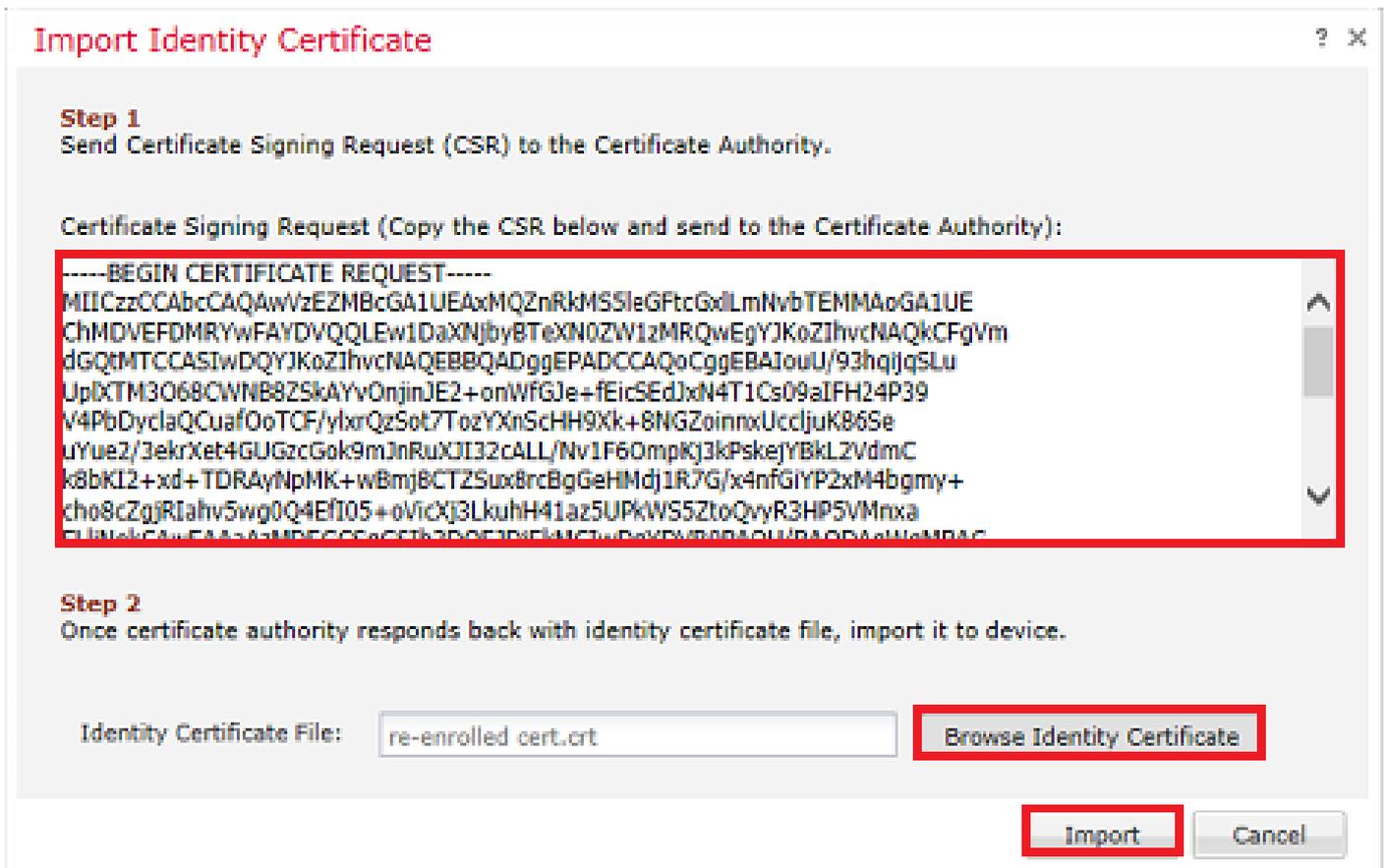


This operation will generate Certificate Signing Request do you want to continue?

Yes

No

3. Nessa janela, é gerado um CSR que pode ser copiado e enviado para a mesma CA que assinou o certificado de identidade anteriormente. Após a assinatura do CSR, o certificado de identidade renovado é fornecido. Navegue até o certificado de identidade fornecido, selecione-o e clique em Importar conforme mostrado na imagem.



4. Um certificado manual renovado é enviado para o DTF. Isso pode ser verificado quando você clica no botão ID e marca a hora válida.

### Renovação de PKCS12

Se você clicar no botão "reinscrever certificado", o certificado não será renovado. Para renovar um PKCS12, um novo arquivo PKCS12 precisa ser criado e carregado com o uso dos métodos mencionados anteriormente.

### Criação de PKCS12 com OpenSSL

1. Com o uso do OpenSSL ou de um aplicativo semelhante, gere uma chave privada e uma CSR (Certificate Signing Request, Solicitação de assinatura de certificado). Este exemplo mostra uma chave RSA de 2048 bits chamada private.key e um CSR chamado ftd1.csr que é criado no 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 o CSR gerado e envie-o para um CA. Depois que o CSR for assinado, um certificado de identidade será fornecido. Normalmente, o(s) certificado(s) da CA também é(são) fornecido(s). Para criar um PKCS12, execute um destes comandos no OpenSSL:

Para incluir apenas o certificado CA emitido dentro do PKCS12, use 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 é o nome do arquivo pkcs12 (no formato der) exportado pelo openssl.
- ftd.crt é o nome do certificado de identidade assinado emitido pela CA no formato pem.
- private.key é o par de chaves criado na Etapa 1.
- ca.crt é o certificado da Autoridade de Certificação emissora no formato pem.

Se o certificado for uma parte de uma cadeia com uma CA raiz e uma ou mais CAs intermediárias, este comando pode ser usado para adicionar a cadeia completa no 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 é o nome do arquivo pkcs12 (no formato der) que é exportado pelo OpenSSL.
- ftd.crt é o nome do certificado de identidade assinado emitido pela CA no formato pem.
- private.key é o par de chaves criado na Etapa 1.
- cachain.pem é um arquivo que contém os certificados CA na cadeia que começa com a CA intermediária de emissão e termina com a CA raiz no formato pem.

Se um arquivo PKCS7 (.p7b, .p7c) for retornado, esses comandos também poderão ser usados para criar o PKCS12. Se o p7b estiver no formato der, certifique-se de adicionar -inform der aos

argumentos, caso contrário não o inclua:

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

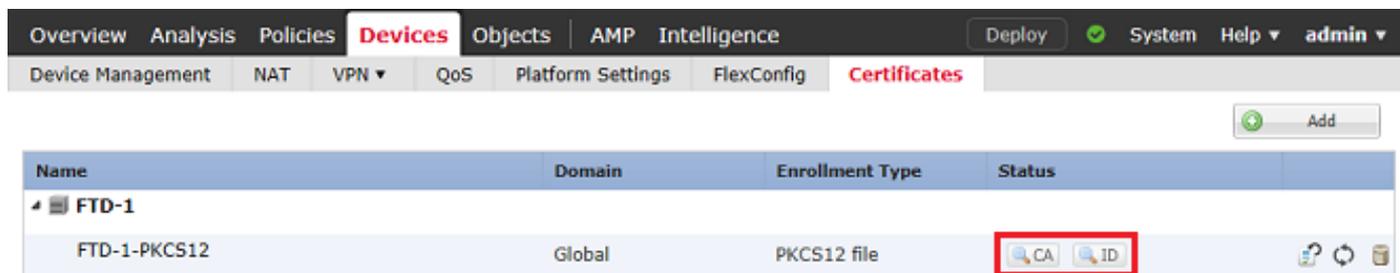
- ftd.p7b é o PKCS7 retornado pela CA que contém o certificado de identidade assinado e a cadeia de CA.
- ftdpem.crt é o arquivo p7b convertido.
- ftd.pfx é o nome do arquivo pkcs12 (no formato der) que é exportado pelo OpenSSL.
- private.key é o par de chaves criado na Etapa 1.

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

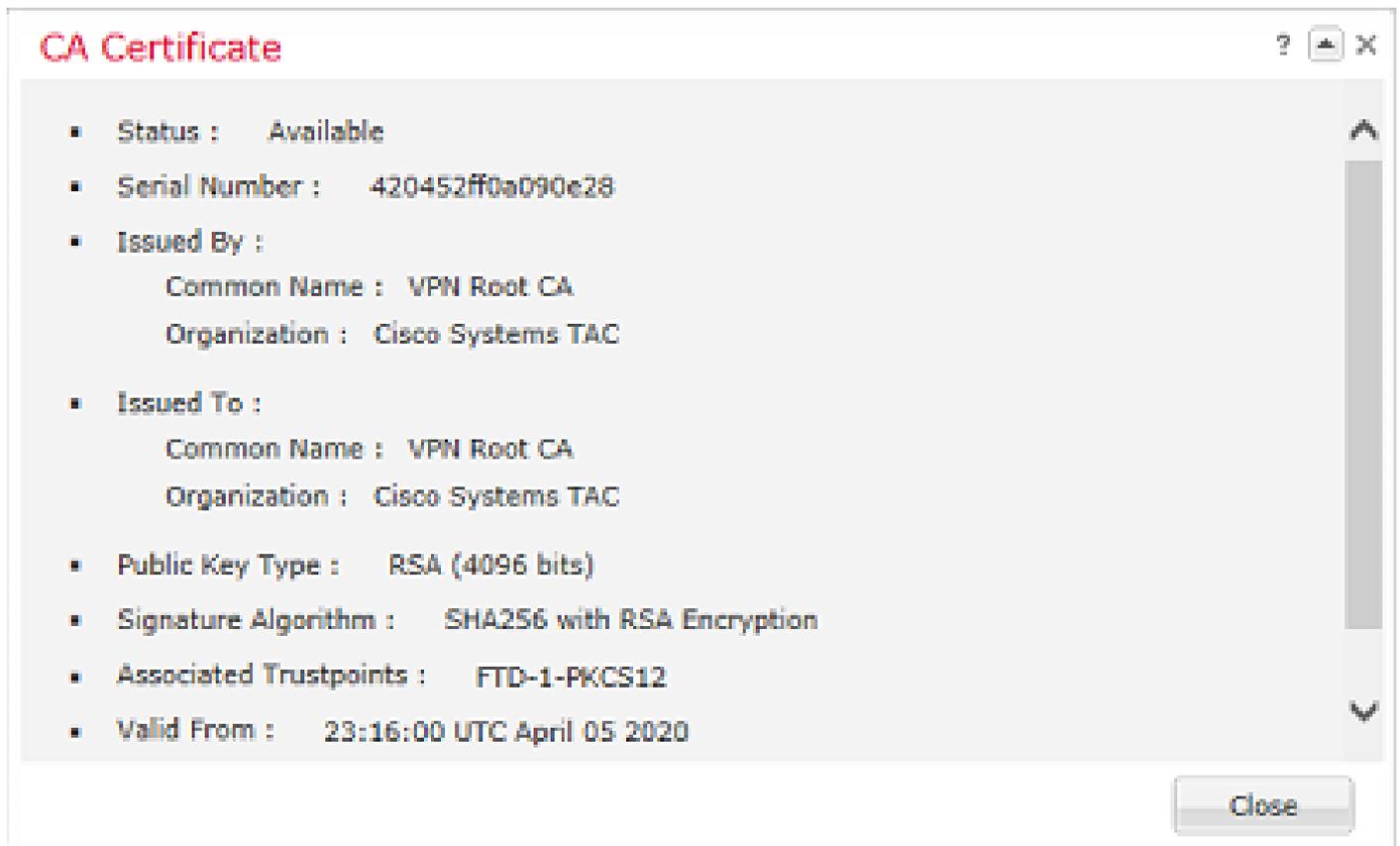
### Exibir certificados instalados no FMC

No FMC, navegue até Devices > Certificates. Para o ponto confiável relevante, clique na CA ou na ID para exibir mais detalhes sobre o certificado, como mostrado na imagem.

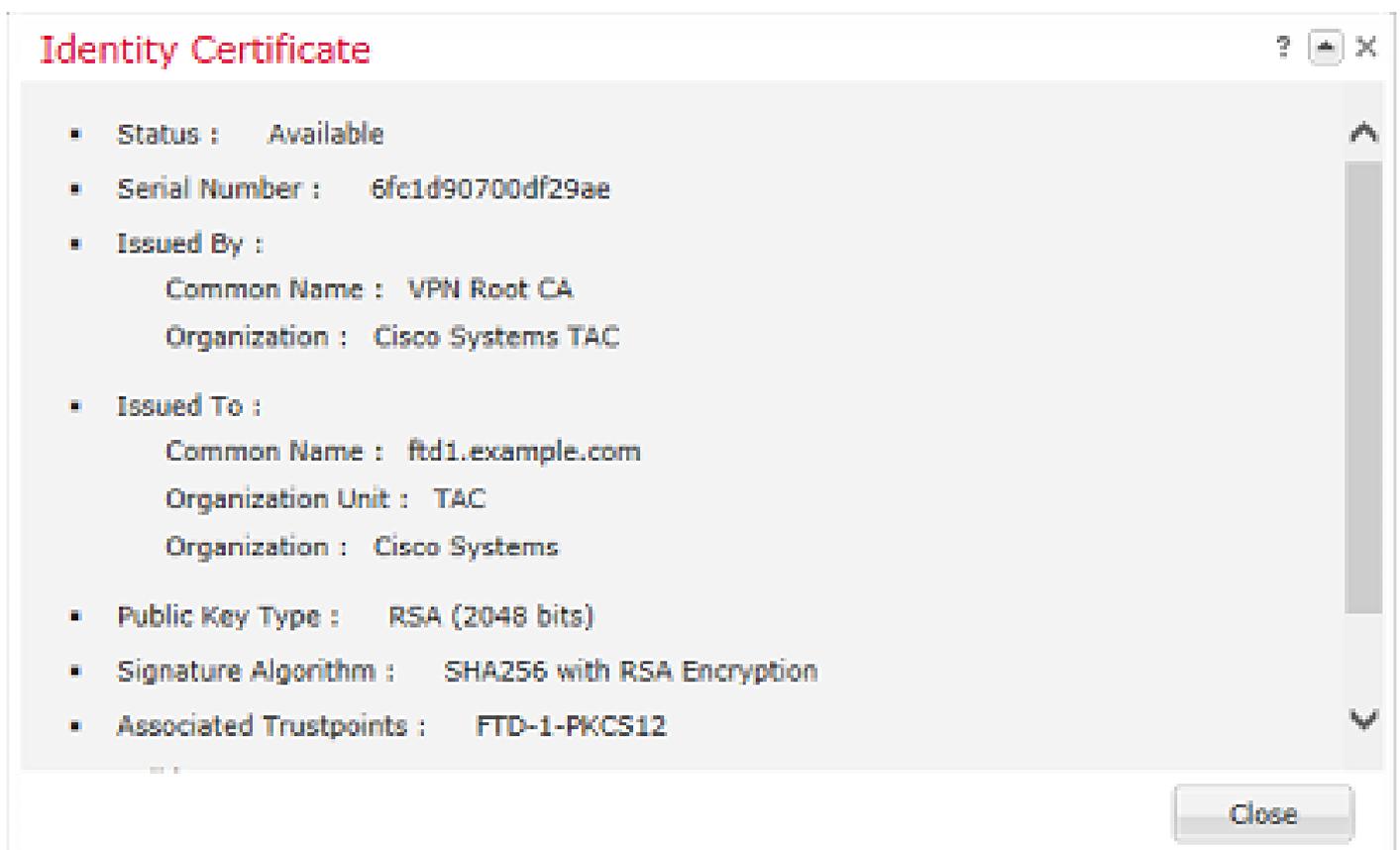


Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID

Verifique o Certificado CA conforme mostrado na imagem.



Verifique o certificado de identidade conforme mostrado na imagem.



Exibir certificados instalados na CLI

Use SSH para acessar o FTD e insira o 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
```

## Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

### Comandos debug

As depurações podem ser executadas a partir da CLI de diagnóstico depois que o FTD é conectado via SSH no caso de uma falha de instalação de certificado SSL:

```
debug crypto ca 14
```

Em versões mais antigas do FTD, essas depurações estão disponíveis e são recomendadas para

solução de problemas:

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 255

## Problemas comuns

Você ainda verá a mensagem "Importação de certificado de identidade necessária" após importar o certificado de identidade emitido.

Isso pode ocorrer devido a dois problemas separados:

### 1. O certificado CA emissor não foi adicionado na inscrição manual

Quando o certificado de identidade é importado, ele é comparado com o certificado CA adicionado na guia Informações da CA no registro manual. Às vezes, os administradores de rede não têm o certificado CA para a CA que é usada para assinar seu certificado de identidade. Nessa situação, é necessário adicionar um certificado CA de espaço reservado quando você faz a inscrição manual. Depois que o certificado Identity tiver sido emitido e o certificado CA tiver sido fornecido, uma nova inscrição Manual poderá ser feita com o certificado CA correto. Quando passar pelo assistente de registro manual novamente, certifique-se de especificar o mesmo nome e tamanho para o par de chaves como foi feito no registro manual original. Depois de concluído, em vez do CSR encaminhado para a CA novamente, o certificado de identidade emitido anteriormente pode ser importado para o ponto confiável recém-criado com o certificado de CA correto.

Para verificar se o mesmo certificado CA foi aplicado na inscrição manual, clique no botão CA conforme especificado na seção Verify ou verifique a saída de show crypto ca certificates. Campos como Emitido para e Número de série podem ser comparados com os campos no certificado CA fornecido pela autoridade de certificação.

### 2. O par de chaves no ponto confiável criado é diferente do par de chaves usado quando o CSR é criado para o certificado emitido.

Com a inscrição manual, quando o par de chaves e o CSR são gerados, a chave pública é adicionada ao CSR para que possa ser incluída no certificado de identidade emitido. Se, por algum motivo, o par de chaves no FTD for modificado ou o certificado de identidade emitido incluir uma chave pública diferente, o FTD não instalará o certificado de identidade emitido. Para verificar se isso ocorreu, há dois testes diferentes:

No OpenSSL, estes comandos podem ser emitidos para comparar a chave pública no CSR com a chave pública no certificado emitido:

```
openssl req -noout -modulus -in ftd.csr
```

```
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
```

```
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9  
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C  
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B  
B966DA10BF24771CFE55327C5A14B96235E9
```

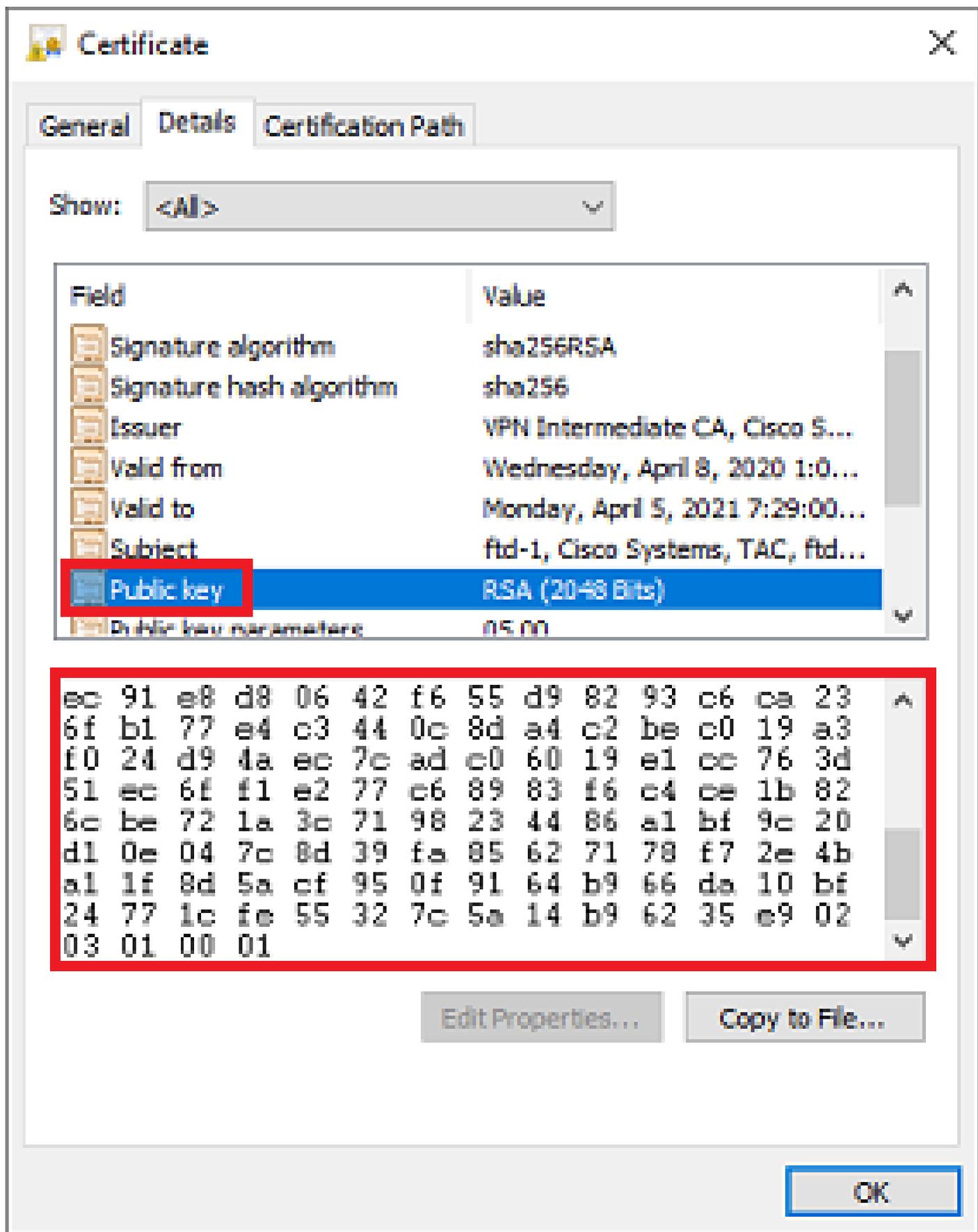
```
openssl x509 -noout -modulus -in id.crt
```

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

- ftd.csr é o CSR copiado do FMC na inscrição manual.
- id.crt é o certificado de identidade assinado pela CA.

Em alternativa, o valor da chave pública no DTF pode também ser comparado com a chave pública no certificado de identidade emitido. Observe que os primeiros caracteres no certificado não correspondem àqueles na saída FTD devido ao preenchimento:

Certificado de Identidade Emitido aberto no PC com Windows:



Saída de chave pública extraída do certificado de identidade:

```
f6e0fdfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b8af3a491b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8da4c2bec0e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f8d5acf955327c5a14b96235e90203010001
```

Mostrar saída crypto key mypubkey rsa do FTD. Quando o registro manual foi feito, o <Default-RSA-Key> foi usado para criar o CSR. A seção em negrito corresponde à saída de chave pública extraída do certificado de identidade.

```
> 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 vermelho próximo à CA no FMC

Isso pode ocorrer com o registro PKCS12 porque o certificado CA não está incluído no pacote PKCS12.



Para corrigir isso, o PKCS12 precisa que o certificado CA seja adicionado.

Execute estes comandos para extrair o certificado de identidade e a chave privada. A senha usada no momento da criação do PKCS12 e a chave privada segura são necessárias:

```
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
ChMRQ2l2YzY28gU3lzdGVtcyBUQUUMxHDAaBgNVBAMTE1ZQTiBJbnR1cm1lZG1hdGUg
Q0EwHhcNMjAwNDA0MTY1ODAwWhcNMjEwNDA1MjMyOTAwWjAbMRkwFwYDVQQDExBm
dGQxLmV4Yw1wbGUuY292tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
043eLVP18K0jnYfHCBZuFUyRXTTB28Z1ouIJ5yYrDzCN781GFrHb/wCczRx/jW4n
pF9q2z7FHR5bQCI4oSUSX40UQfr0/uOK5riI1uZumPUx1Vp1zVkYuqDd/i1r0+0j
PyS7BmyGfV7aebYWZnr8R9ebDsnC2U3nKjP5RaE/wNdVGTs/180H1rIjMpcFMXps
LwxdxiEz0hCmDm9RC+7uWZQd1wZ9oNANcbQC0px/Zikj9Dz70RhhbzBTuNKD3p
sN3VqdDPvGZHFGLPcnhKYyZ79+6p+CHC8X8BFjuTJYoo176uGgiB4Jz2Y9ZeFSQz
Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBg1ghkgBhvCAQOEERYPeGnhIGN1
cnRpZm1jYXR1MA0GCsQGSiB3DQEBcUAA4IBAQCv/MgshWxXtwpwmMF/6KqEj8nB
S1jbfz1zNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRY54taRI27W+gLneCbQAux
9amxXuhpxP5E0hkn+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
MBQGccqGSiB3DQMHBAGcm0qRKh/dcwSCBmiF7BpgJNIPhdU5Zorn1jm3pmsI/XkJ
MRHc1Ree10ziSLCZOSTr84JFQxNpbThXLhsHC9WhpPy5sNXIvXS7Gu+U10/V1NSA
rW1X6SPftAYiFq5QxyEutSHdZZwGQIqj97seu3Px0agvI0bw1Lo8or51SydnMjp
Ptv50Ko95BSHwWycqkTAia4ZKxytyIc/mIu5m72LucOFmoRB05JZu1avWXjbCAA+
k2ebkb1FT0YRQT1Z4tZHSqX1LFPZe170NZEUG7rIcWak1Yw7XNUPh0n6FHL/ieIZ
IhvIfj+IgQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E
Gnh8r31903A1kPMBkMdx0q1pzo2naIy2KGrUnOSHajVwclR9dTPWIDyjd95YoeS
IUE7Ma00pjJc02FNbWyxRrYt+4hp3aJt0ZW83FHiS1B5UIzGrBMAgKJc2Hb2RTV
9gxZGve1cRco1LeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShn0wHzridF8Zn
F06XvBDSyXVSpkxwAd1Twxq62tUnLIkyRXo2CSz8z8W29UXmF04o3G67n28//LJ
Ku8wj1jjeq1vFgXSQiWLADNH772RNwzCMeobfxG1BprF9DPT8yvyBdQviUIuFpJ
nNs5FYbLTv9ygZ1S9xwQpTcqEu+y4F5BJuYLMHqcZ+VpFA4nM0YHhZ5M3sccRSR4
1L+a3BPJJsh1TIJQg0TixDaveCfpDcpS+ydUgS6WY8xw17v0+1f7y5z1t4TkZrt
ItBHHA6yDzR0Cn0/ZH3y88a/asDcuKw6bsRaY5iT8nAWGTQved3xXj+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-----
```

Uma vez concluído, o certificado de identidade e a chave privada podem ser colocados em

arquivos separados e o certificado CA pode ser importado para um novo arquivo PKCS12 com o uso das etapas mencionadas na Etapa 2. da criação de PKCS12 com OpenSSL.

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.