Instalar e Renovar Certificado no FTD Gerenciado pelo FDM

Contents

Introdução

Este documento descreve como instalar, confiar e renovar certificados autoassinados e certificados assinados por uma CA de terceiros ou CA interna no FTD.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O registro manual do certificado requer acesso a uma Autoridade de Certificação (CA) de terceiros confiável. Exemplos de fornecedores de CA de terceiros incluem, entre outros, Entrust, Geotrust, GoDaddy, Thawte e VeriSign.
- Verifique se o Firepower Threat Defense (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:

- FTDv que executa 6.5.
- Para a criação de pares de chaves e CSR (Certificate Signing Request, Solicitação de assinatura de certificado), o OpenSSL é usado.

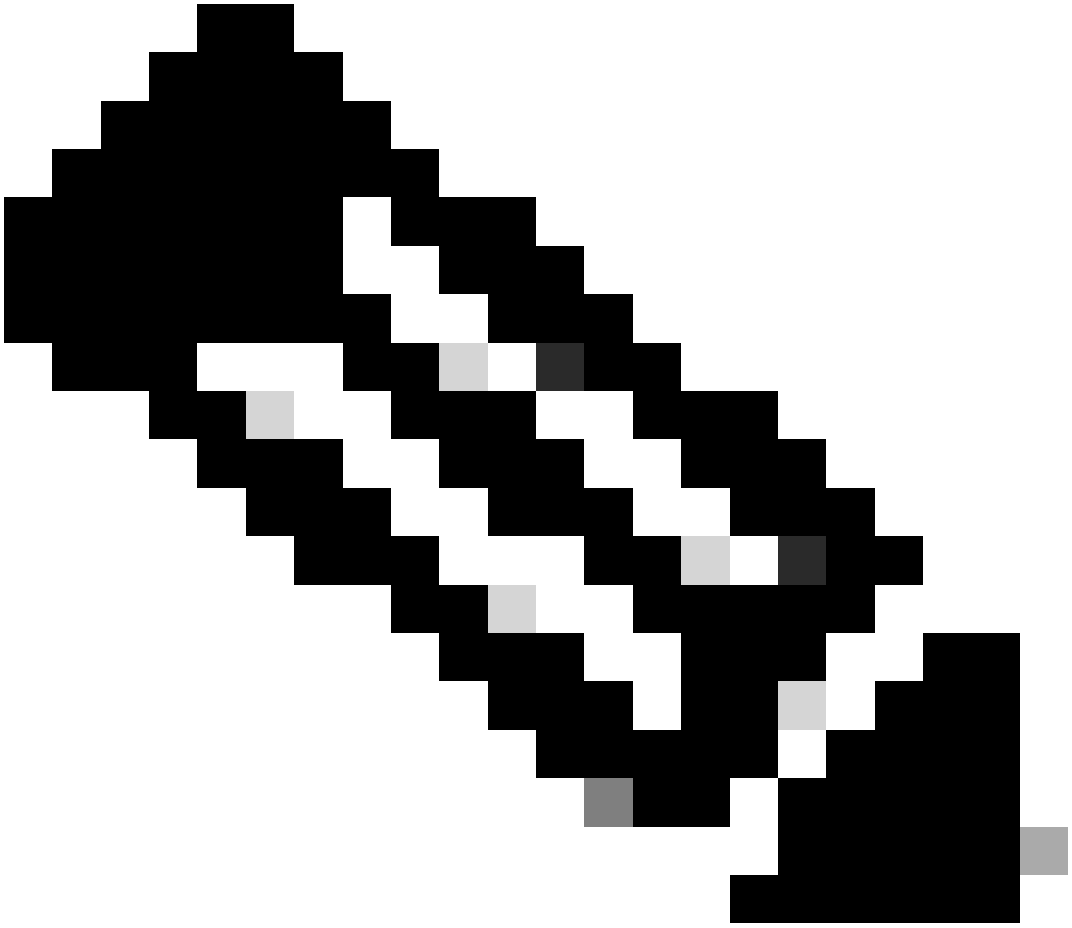
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Configurar

Instalação do certificado

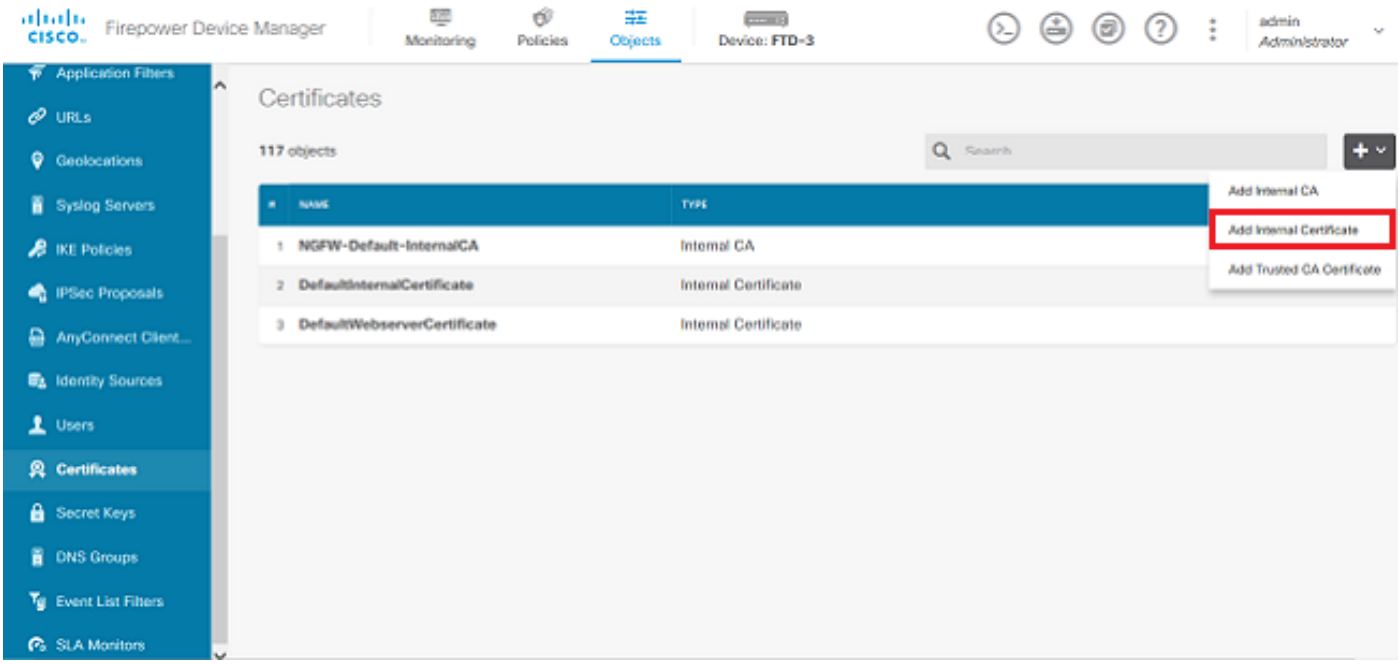
Inscrição com assinatura automática

Os certificados autoassinados são uma maneira fácil de obter um certificado com os campos apropriados adicionados ao dispositivo FTD. Embora não sejam confiáveis na maioria dos lugares, eles ainda podem oferecer benefícios de criptografia semelhantes aos de um certificado assinado por terceiros. Ainda assim, é recomendável ter um certificado assinado por CA confiável para que os usuários e outros dispositivos possam confiar no certificado apresentado pelo FTD.

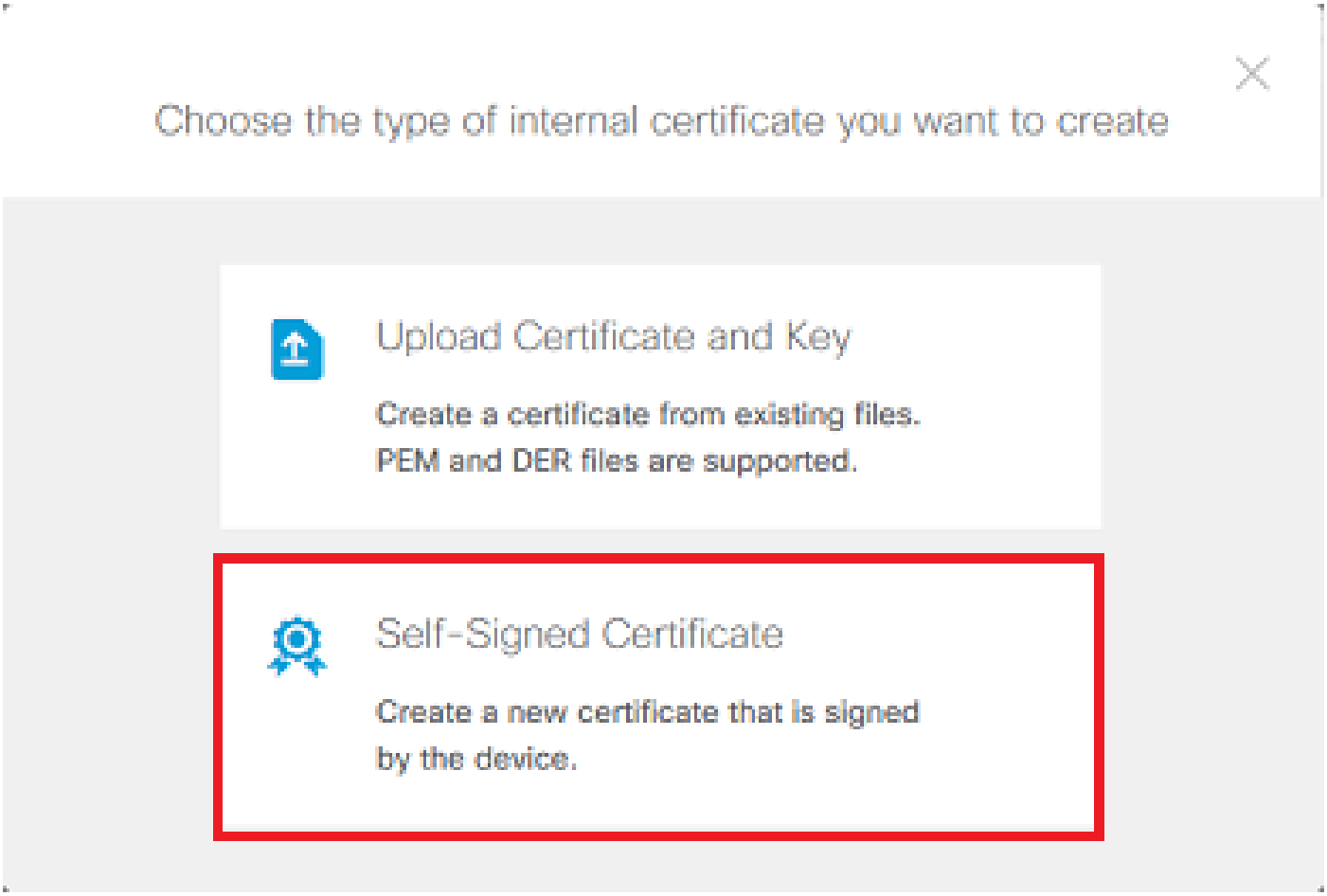


Observação: o Firepower Device Management (FDM) tem um certificado autoassinado padrão chamado DefaultInternalCertificate que pode ser usado para fins semelhantes.

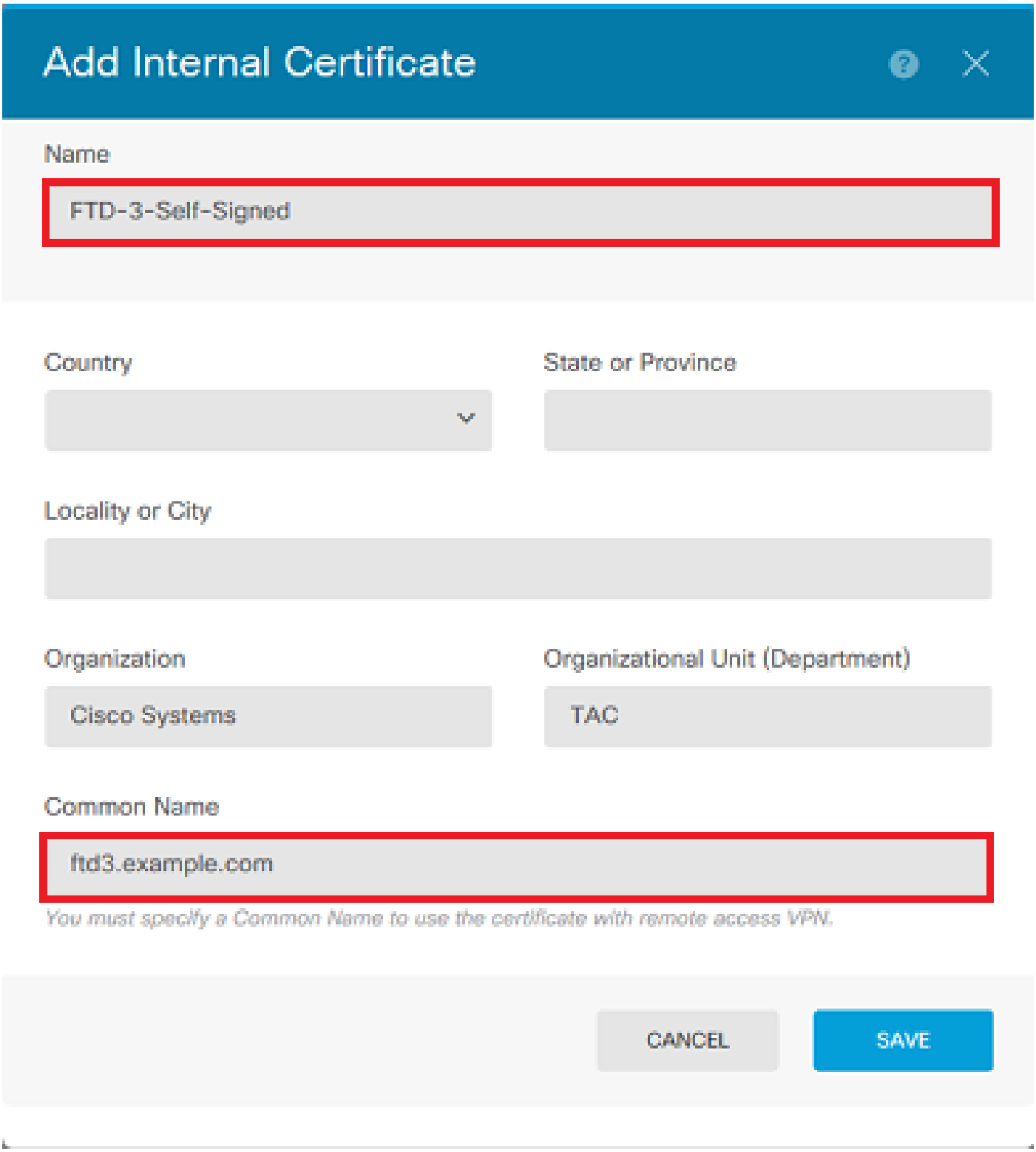
1. Navegue até Objetos > Certificados. Clique no símbolo + e escolha Adicionar certificado interno conforme mostrado na imagem.



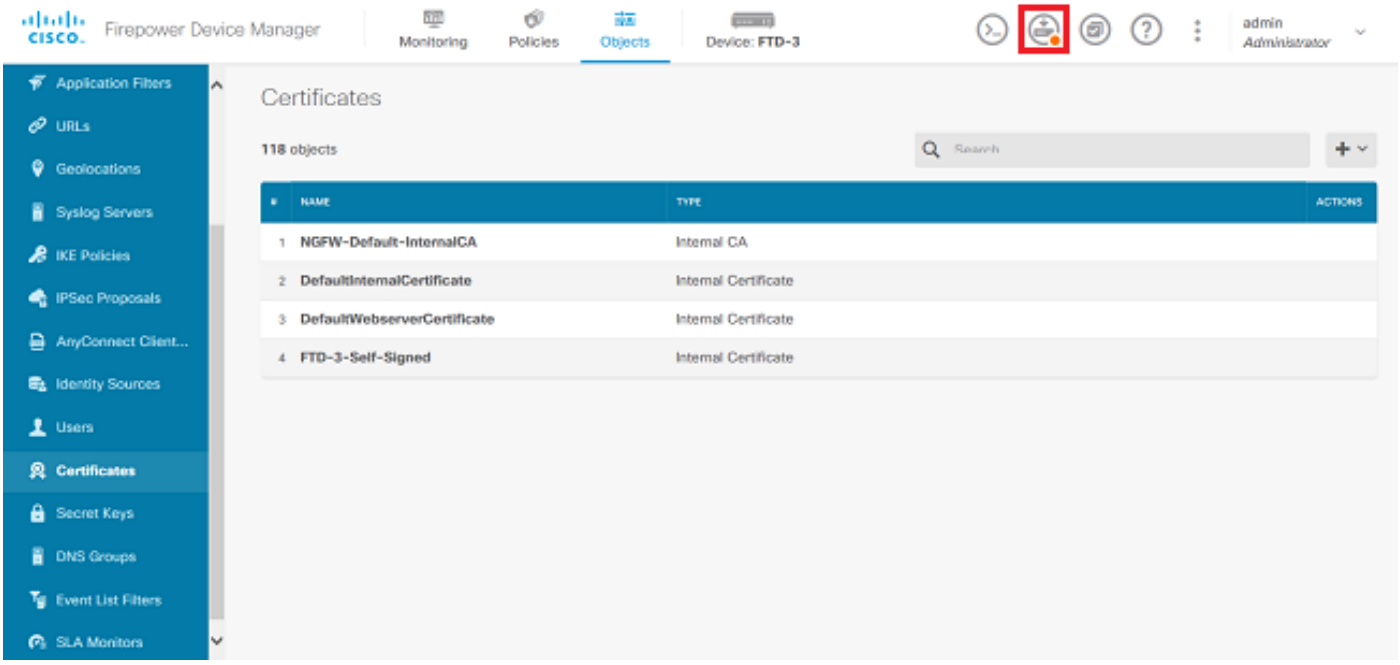
2. Escolha Certificado Autoassinado na janela pop-up, conforme mostrado na imagem.



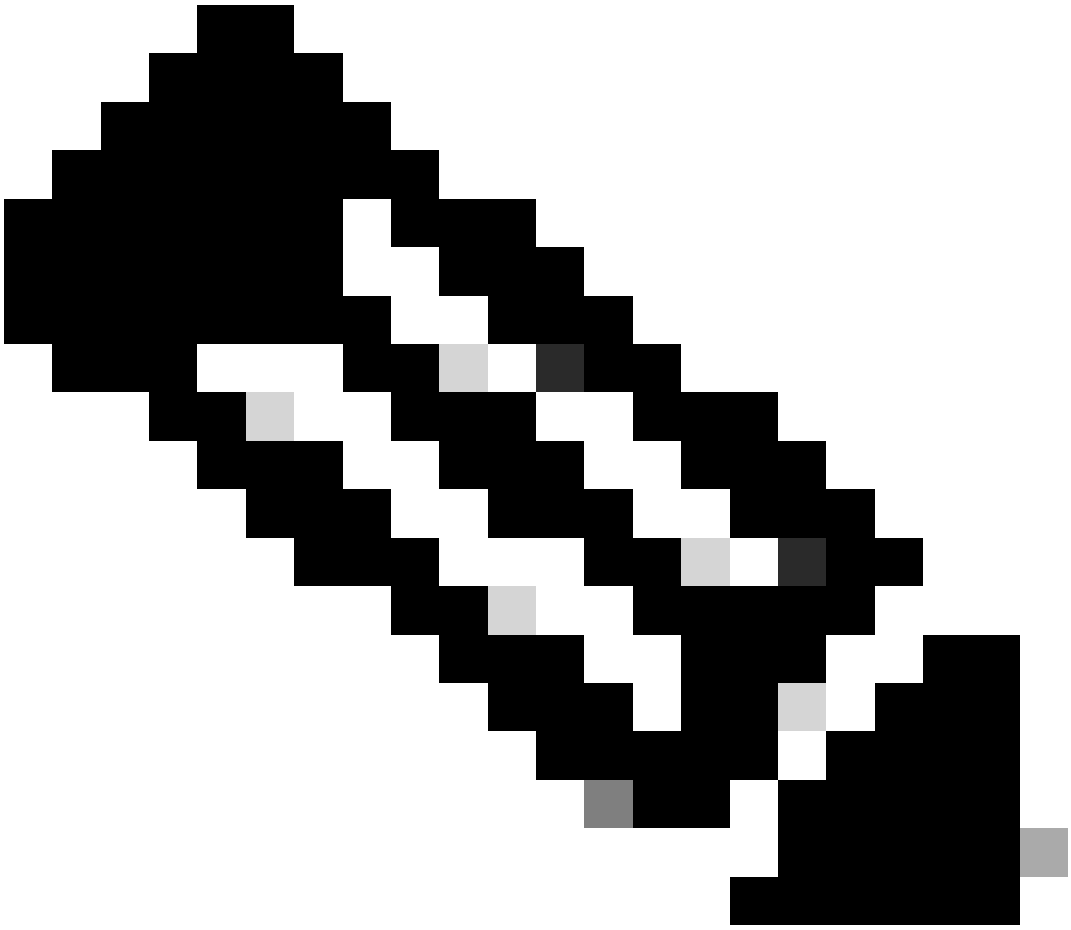
3. Especifique um Nome para o ponto confiável e preencha os campos de nome distinto do assunto. No mínimo, o campo Nome comum pode ser adicionado. Isso pode corresponder ao FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) ou ao endereço IP do serviço para o qual o certificado é usado. Clique em Salvar quando terminar, conforme mostrado na imagem.



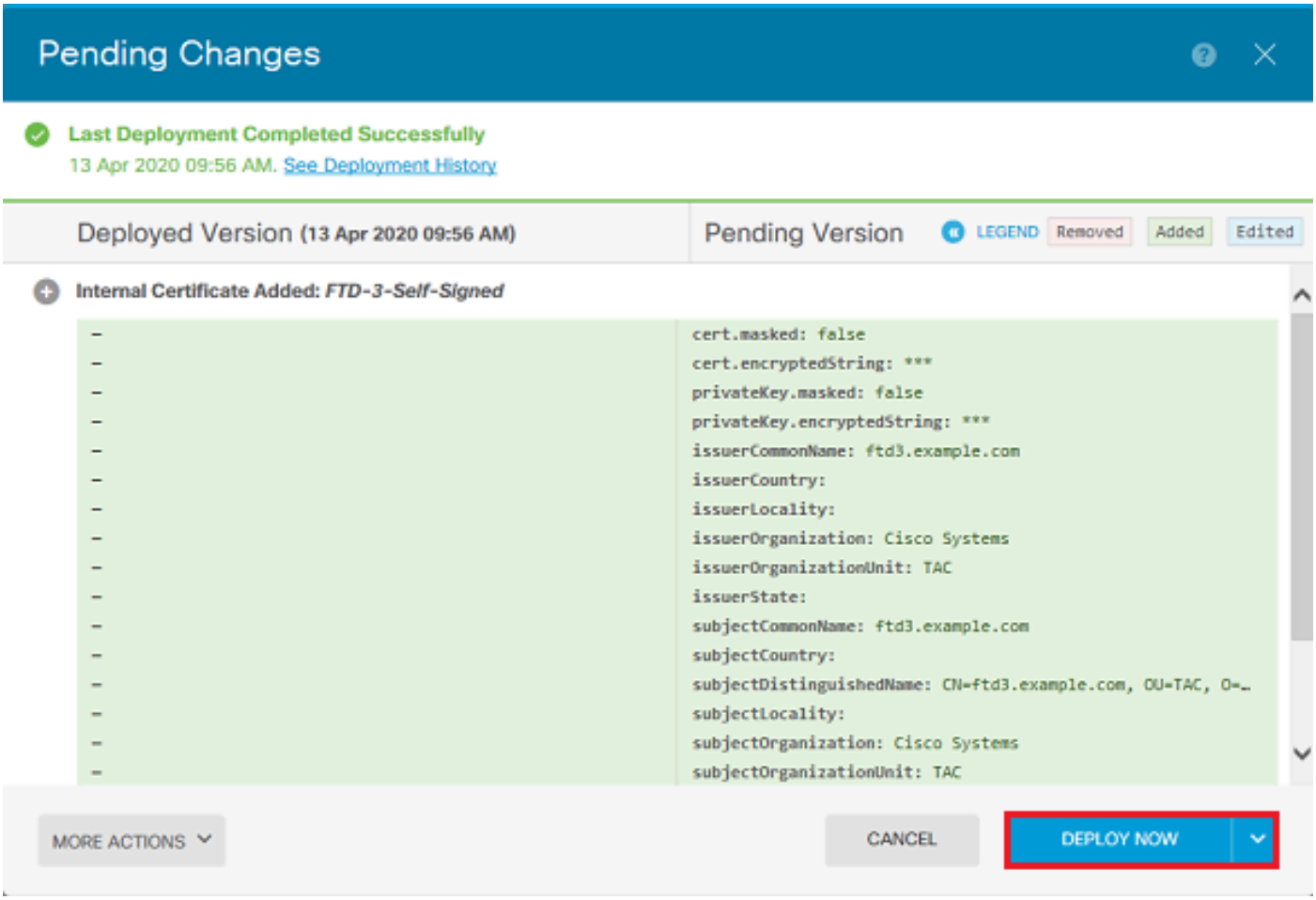
4. Clique no botão Alterações Pendentes na parte superior direita da tela, conforme mostrado na imagem.



5. Clique no botão Implantar Agora.



Observação: quando a implantação é concluída, o certificado não fica disponível para ser visto na CLI até que haja um serviço que o use, como o AnyConnect, como mostrado na imagem.



Inscrição manual

A Inscrição Manual pode ser usada para instalar um certificado emitido por uma CA confiável. O OpenSSL ou uma ferramenta semelhante pode ser usada para gerar a chave privada e o CSR necessários para receber um certificado assinado pela CA. Estas etapas abordam os comandos comuns do OpenSSL para gerar a chave privada e o CSR, bem como as etapas para instalar o certificado e a chave privada uma vez obtidas.

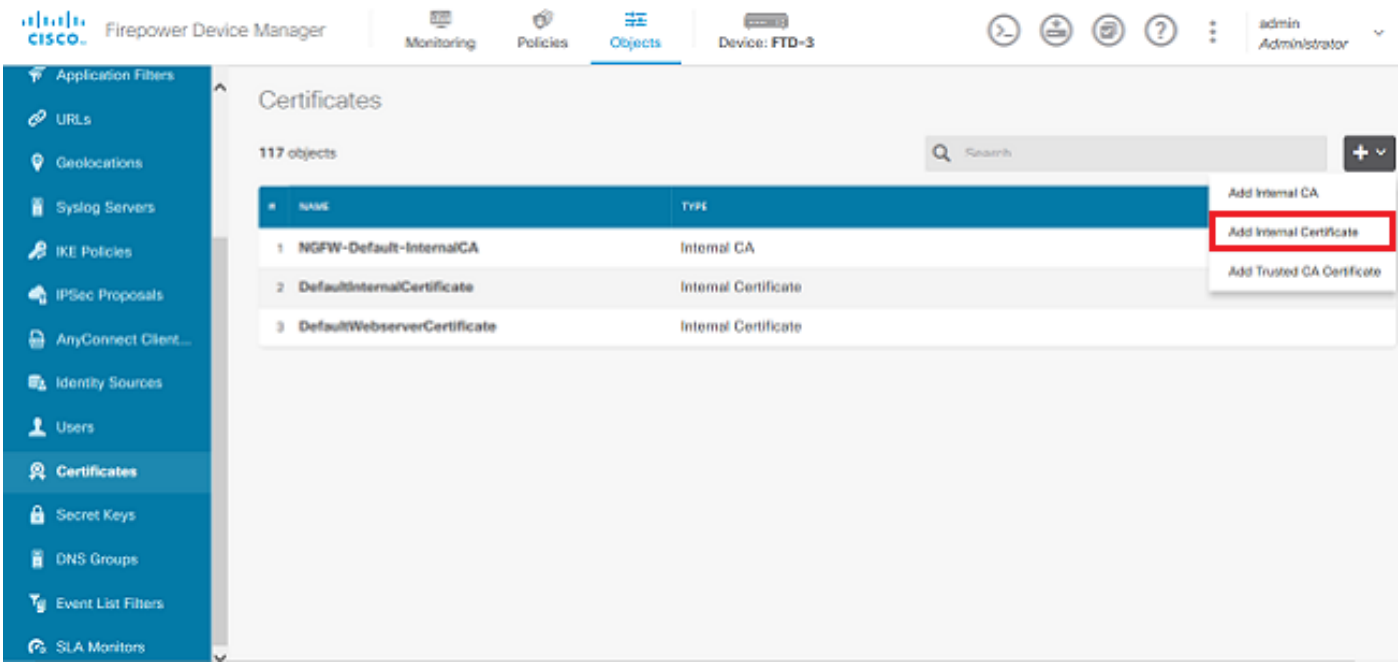
1. Com o OpenSSL ou um aplicativo semelhante, gere uma chave privada e uma CSR (Certificate Signing Request, Solicitação de assinatura de certificado). Este exemplo mostra uma chave RSA de 2048 bits chamada private.key e um CSR chamado ftd3.csr que é criado no OpenSSL.

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
.....................................+++
.....................................................................+++
writing new private key to 'private.key'
-----
```

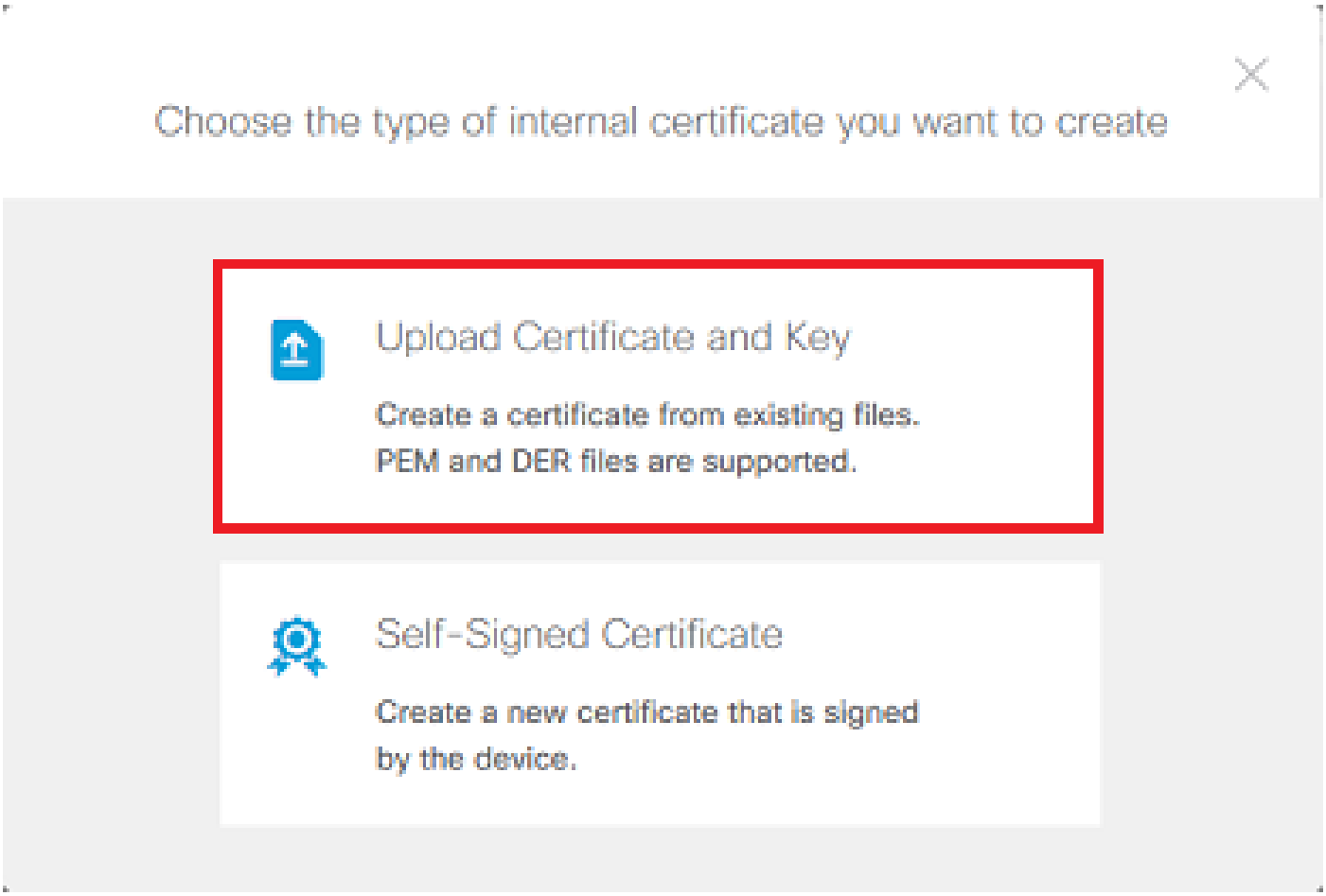
```
You are about to be asked to enter information that is incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', the 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) []:ftd3.example.com
Email Address []:.

Please enter the following '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.

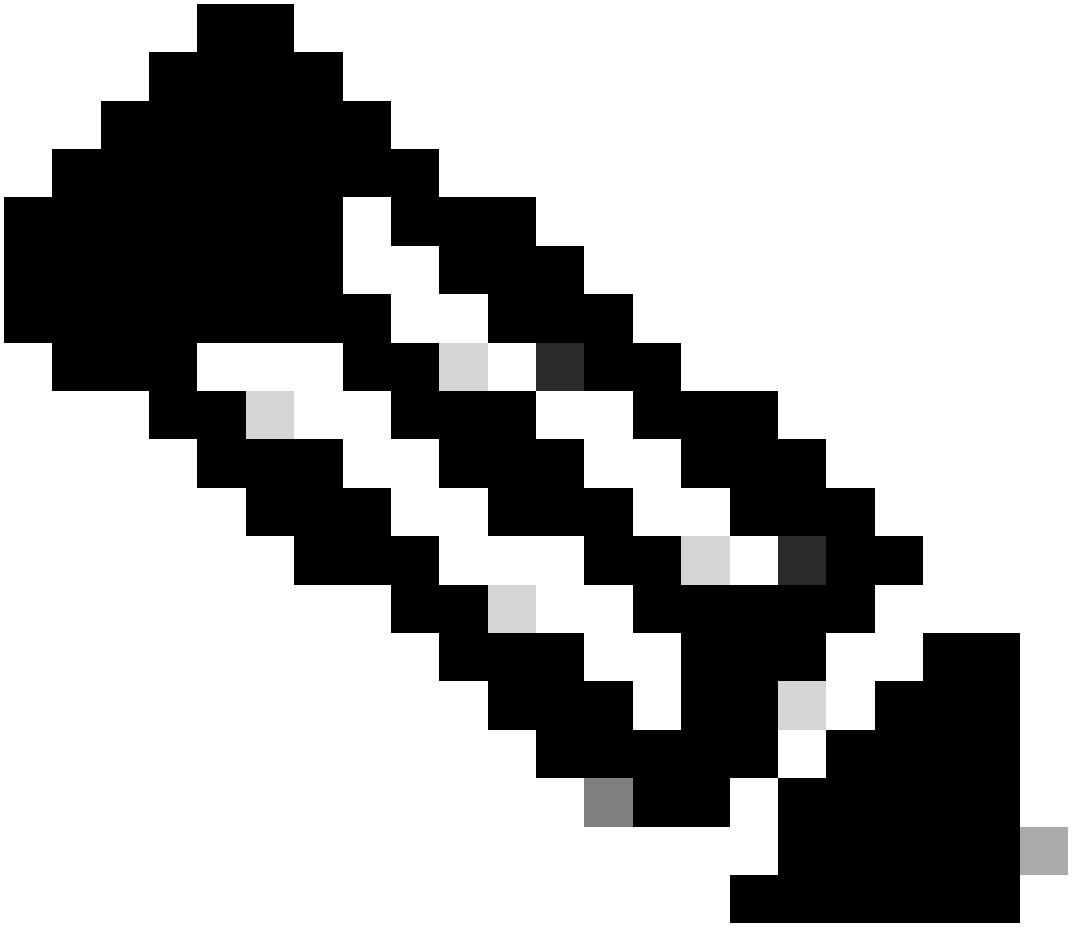
3. Navegue até Objetos > Certificados. Clique no símbolo + e escolha Adicionar certificado interno conforme mostrado na imagem.



4. Escolha Carregar Certificado e Chave na janela pop-up, conforme mostrado na imagem.

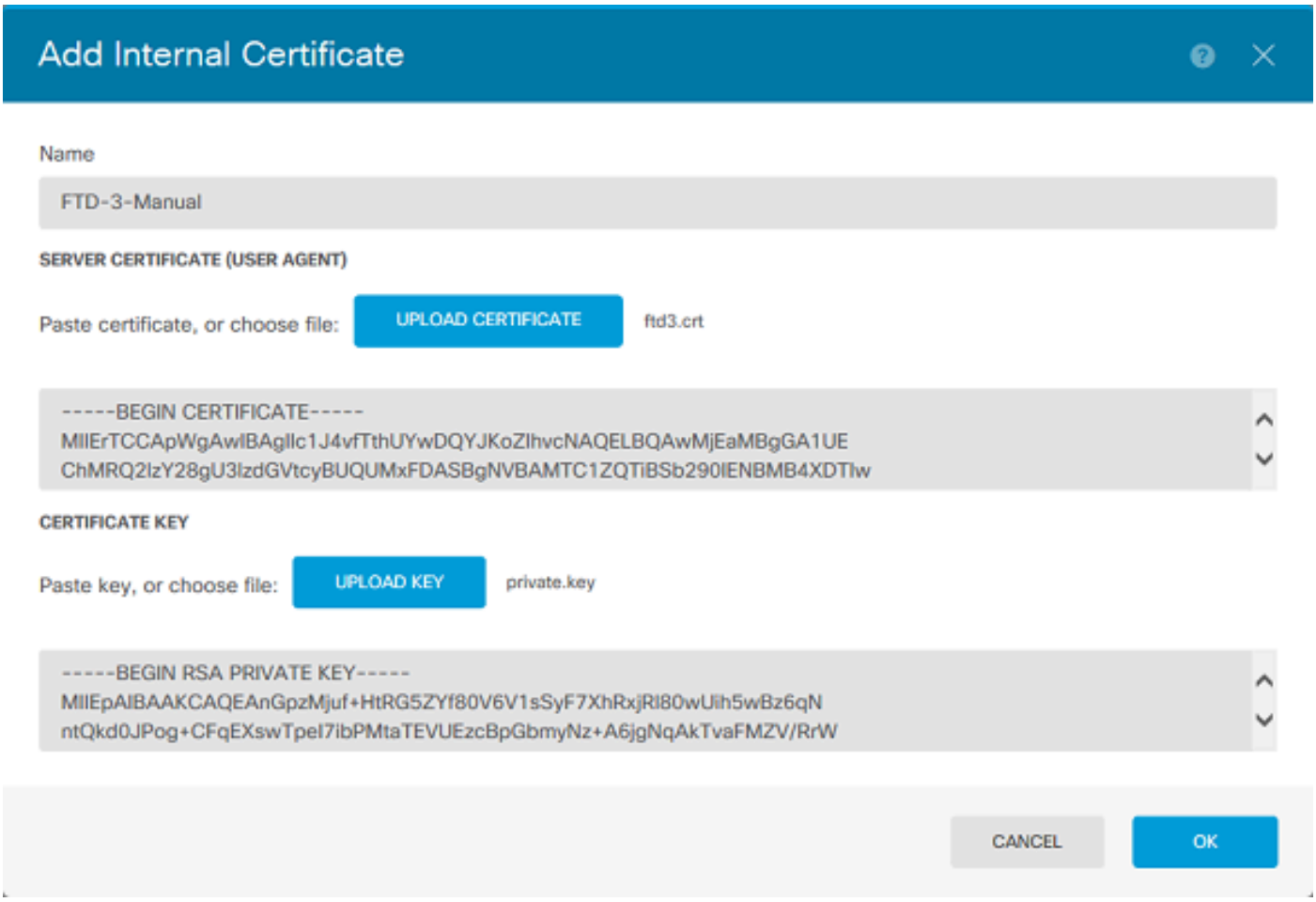


5. Especifique um Nome para o ponto confiável e, em seguida, carregue ou copie e cole o certificado de identidade e a chave privada no formato Privacy Enhanced Mail (PEM). Se a CA forneceu o certificado e a chave juntos em um único PKCS12, navegue para a seção intitulada Extraindo o certificado de identidade e a chave privada do arquivo PKCS12 mais adiante neste documento para separá-los.

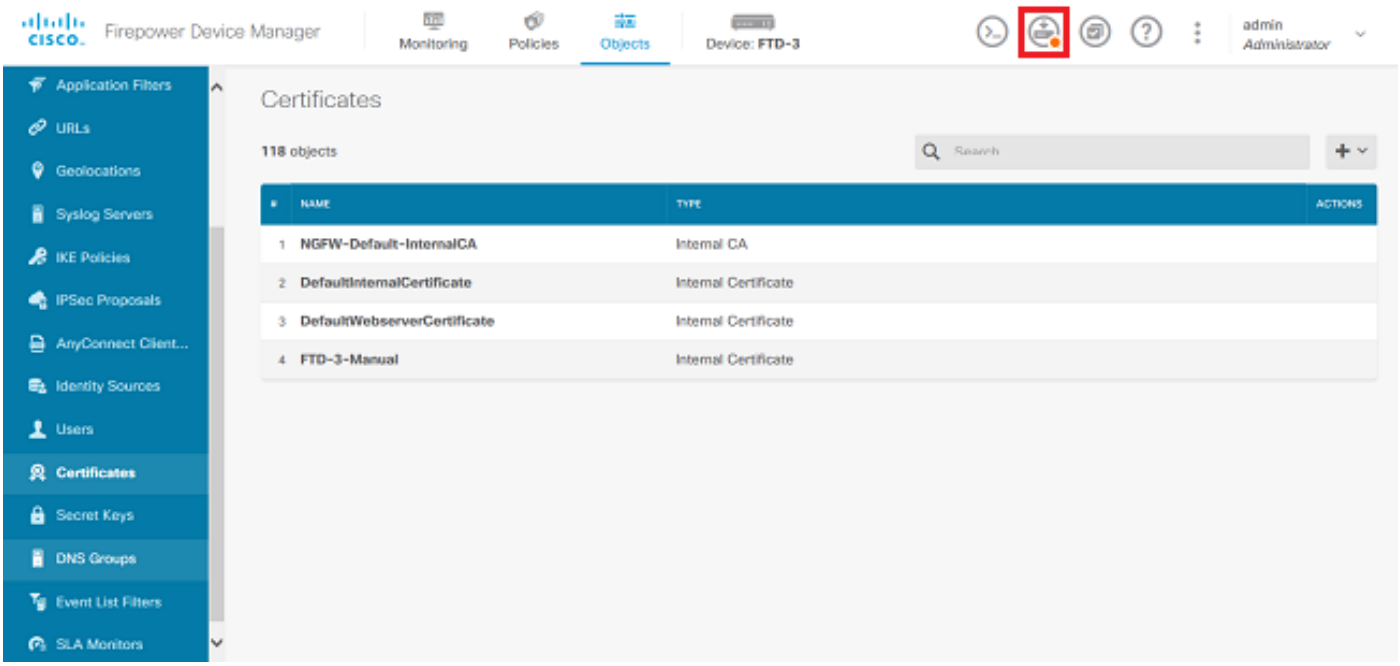


Observação: os nomes de arquivo não podem ter espaços ou o FDM não os aceita. Além disso, a chave privada não deve ser criptografada.

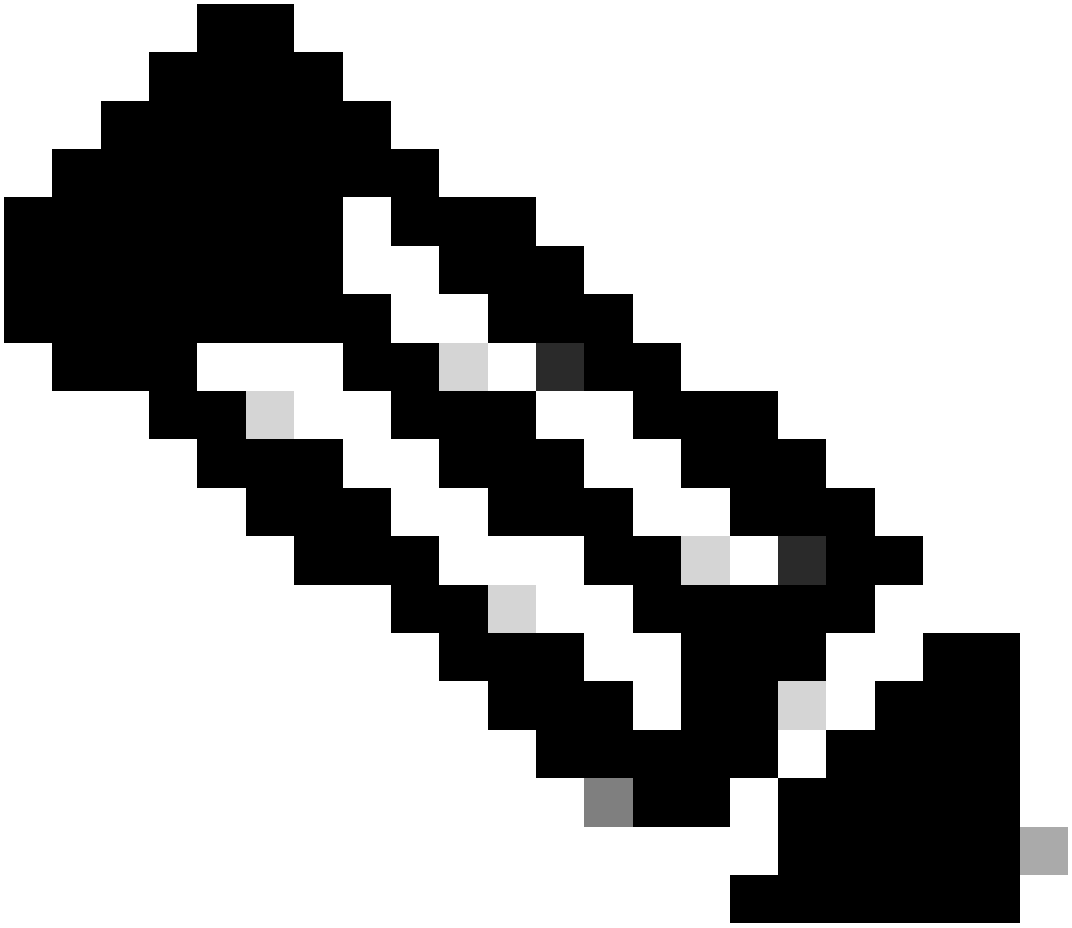
Clique em OK quando terminar, conforme mostrado na imagem.



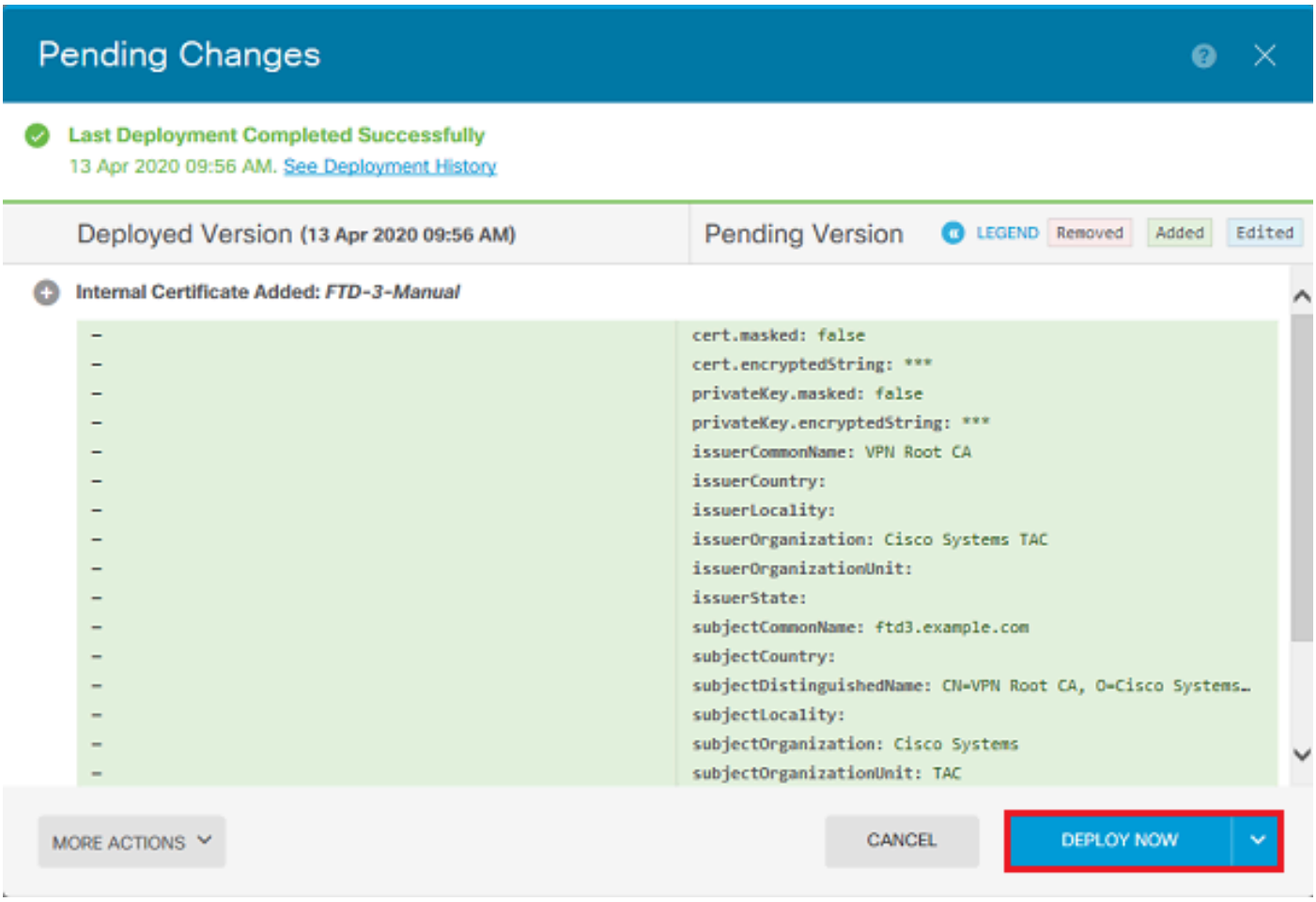
6. Clique no botão Alterações Pendentes na parte superior direita da tela, conforme mostrado na imagem.



7. Clique no botão Implantar Agora.



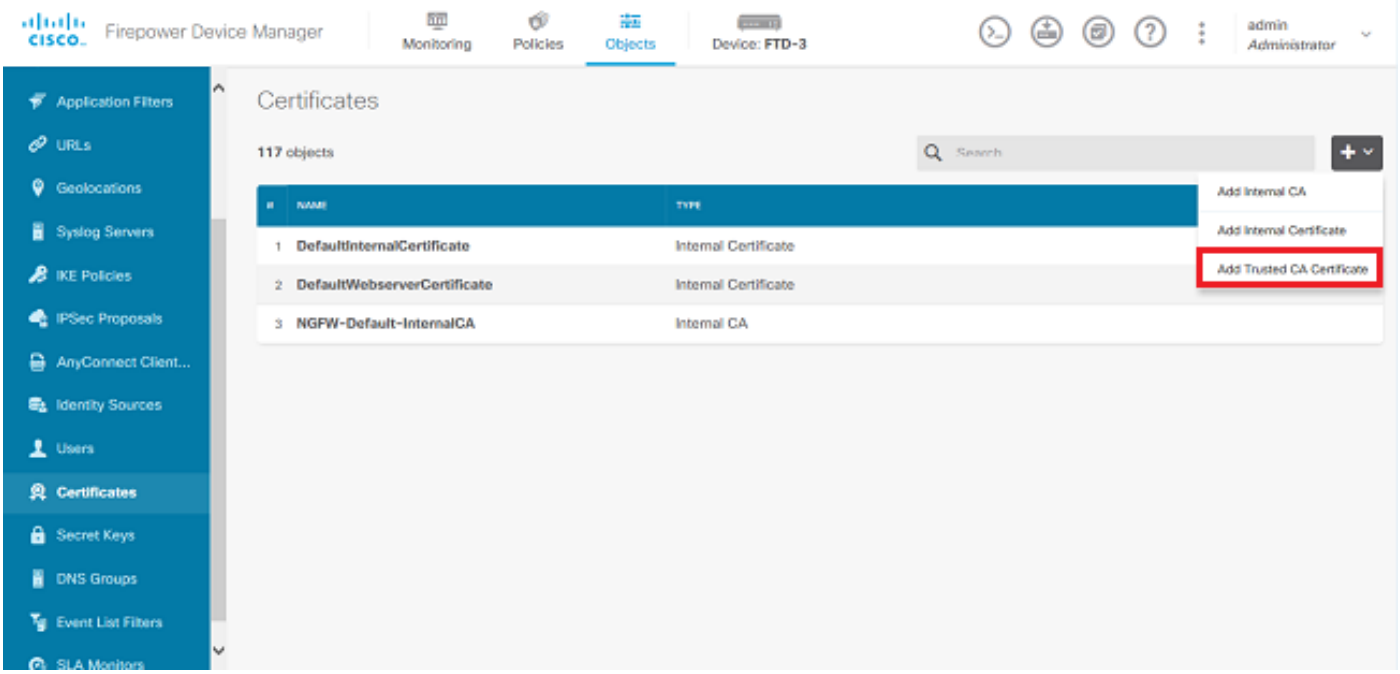
Observação: quando a implantação é concluída, o certificado não fica disponível para ser visto na CLI até que haja um serviço que o use, como o AnyConnect, como mostrado na imagem.



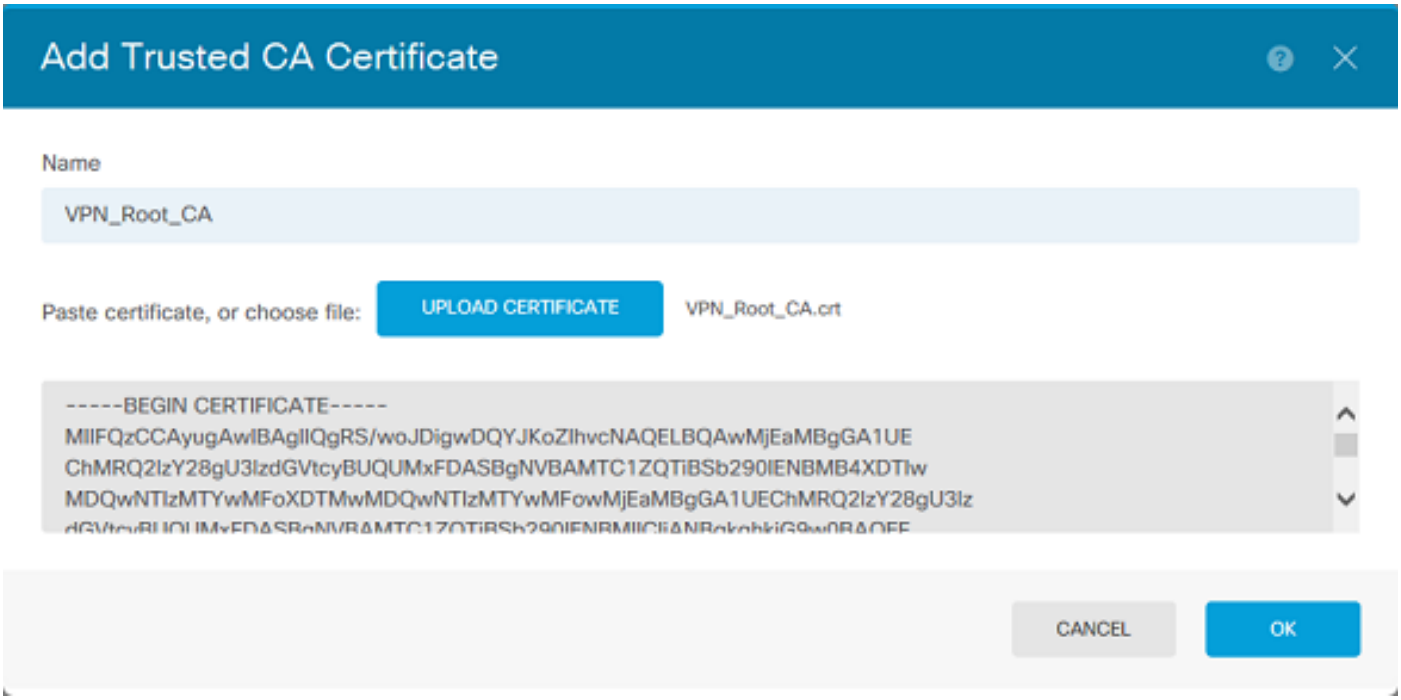
Instalação de Certificado de Autoridade de Certificação Confiável

Quando você instala um certificado de CA confiável, ele é necessário para autenticar com êxito usuários ou dispositivos que apresentam certificados de identidade ao FTD. Exemplos comuns disso incluem a autenticação de certificado do AnyConnect e a autenticação de certificado VPN S2S. Estas etapas abordam como confiar em um certificado de CA para que os certificados emitidos por essa CA também sejam confiáveis.

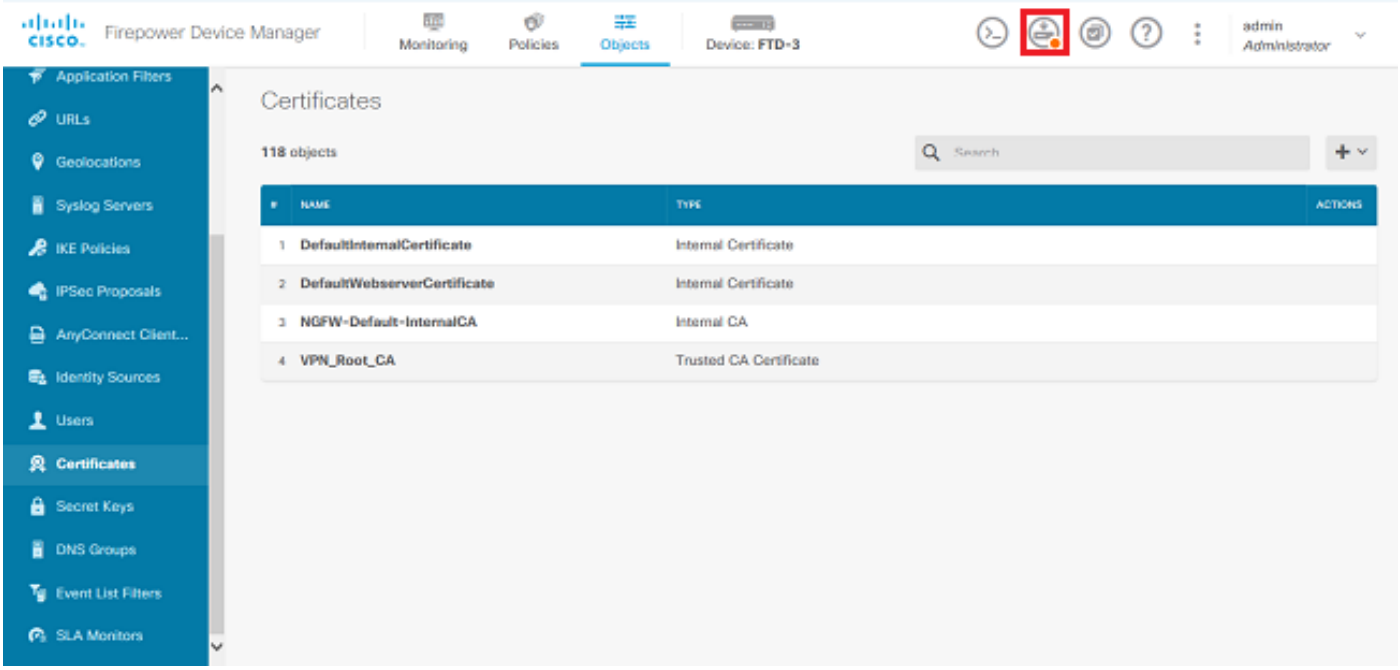
1. Navegue até Objetos > Certificados. Clique no símbolo + e escolha Add Trusted CA Certificate como mostrado na imagem.



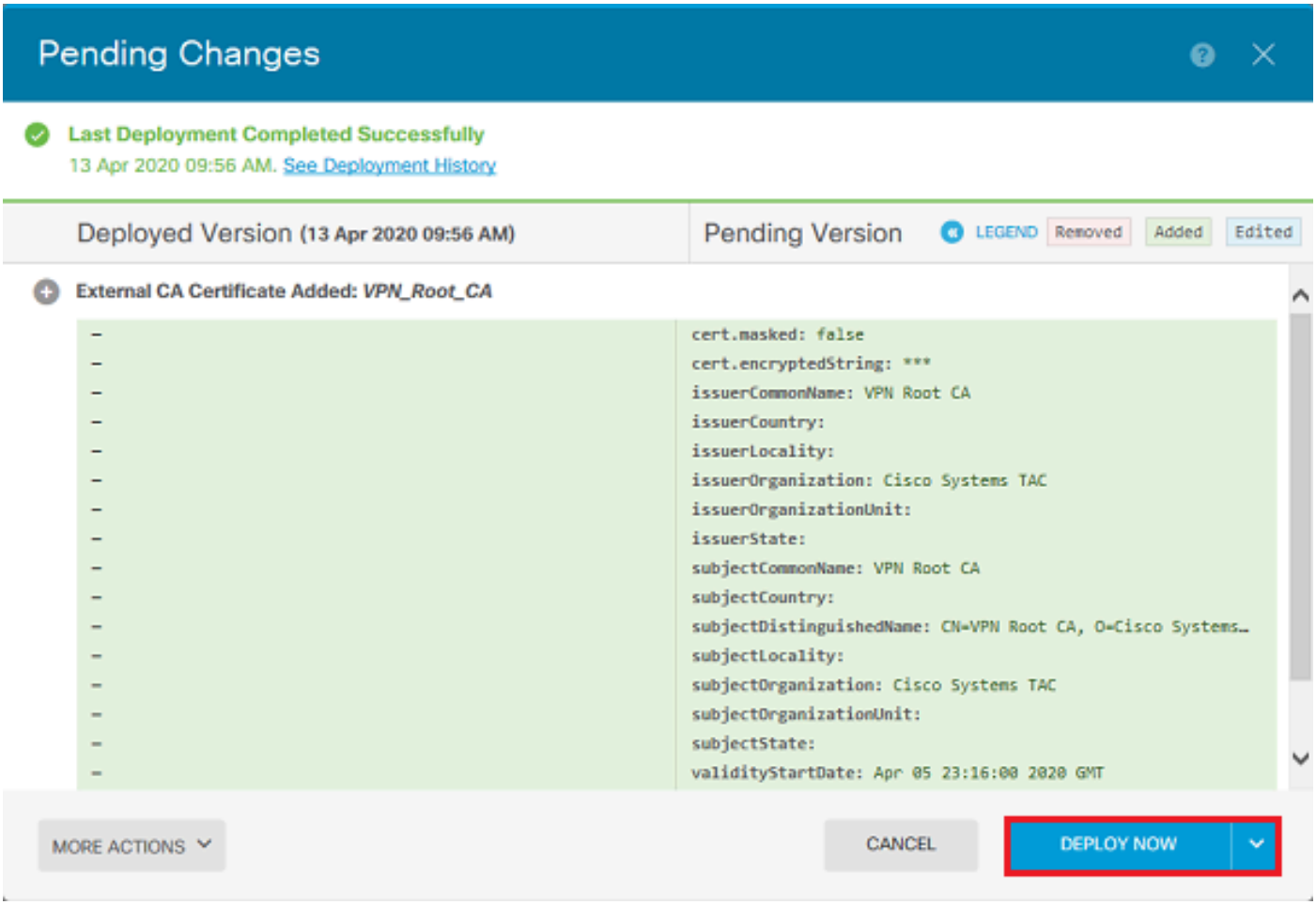
2. Especifique um Nome para o ponto confiável. Em seguida, carregue ou copie e cole o certificado CA no formato PEM. Clique em OK quando terminar, conforme mostrado na imagem.



3. Clique no botão Alterações Pendentes na parte superior direita da tela, conforme mostrado na imagem.



4. Clique no botão Implantar Agora como mostrado na imagem.



Renovação de certificado

A renovação de certificado em um FTD gerenciado pelo FDM envolve a substituição do certificado anterior e, possivelmente, da chave privada. Se você não tiver o CSR original e a chave privada

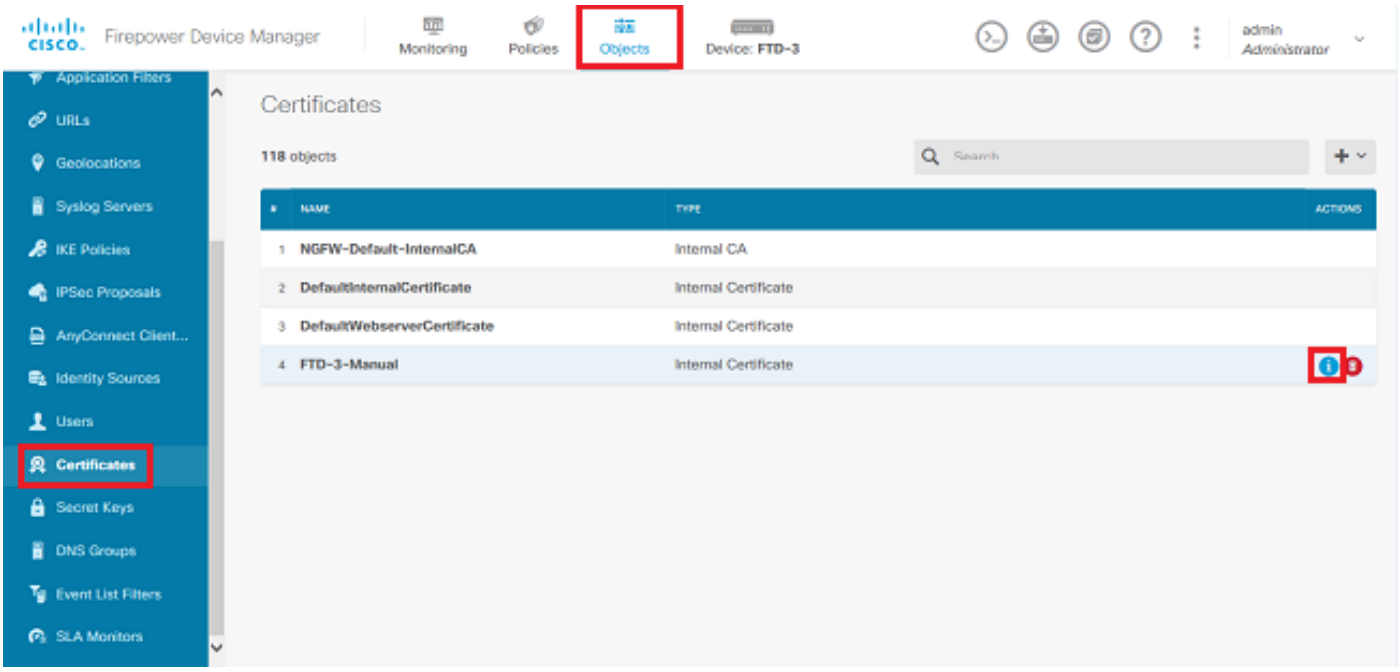
usados para criar o certificado original, será necessário criar um novo CSR e uma nova chave privada.

1. Se você tiver o CSR original e a chave privada, esta etapa poderá ser ignorada. Caso contrário, será necessário criar uma nova chave privada e CSR. Use o OpenSSL ou um aplicativo semelhante para gerar uma chave privada e CSR. Este exemplo mostra uma chave RSA de 2048 bits chamada private.key e um CSR chamado ftd3.csr que é criado no OpenSSL.

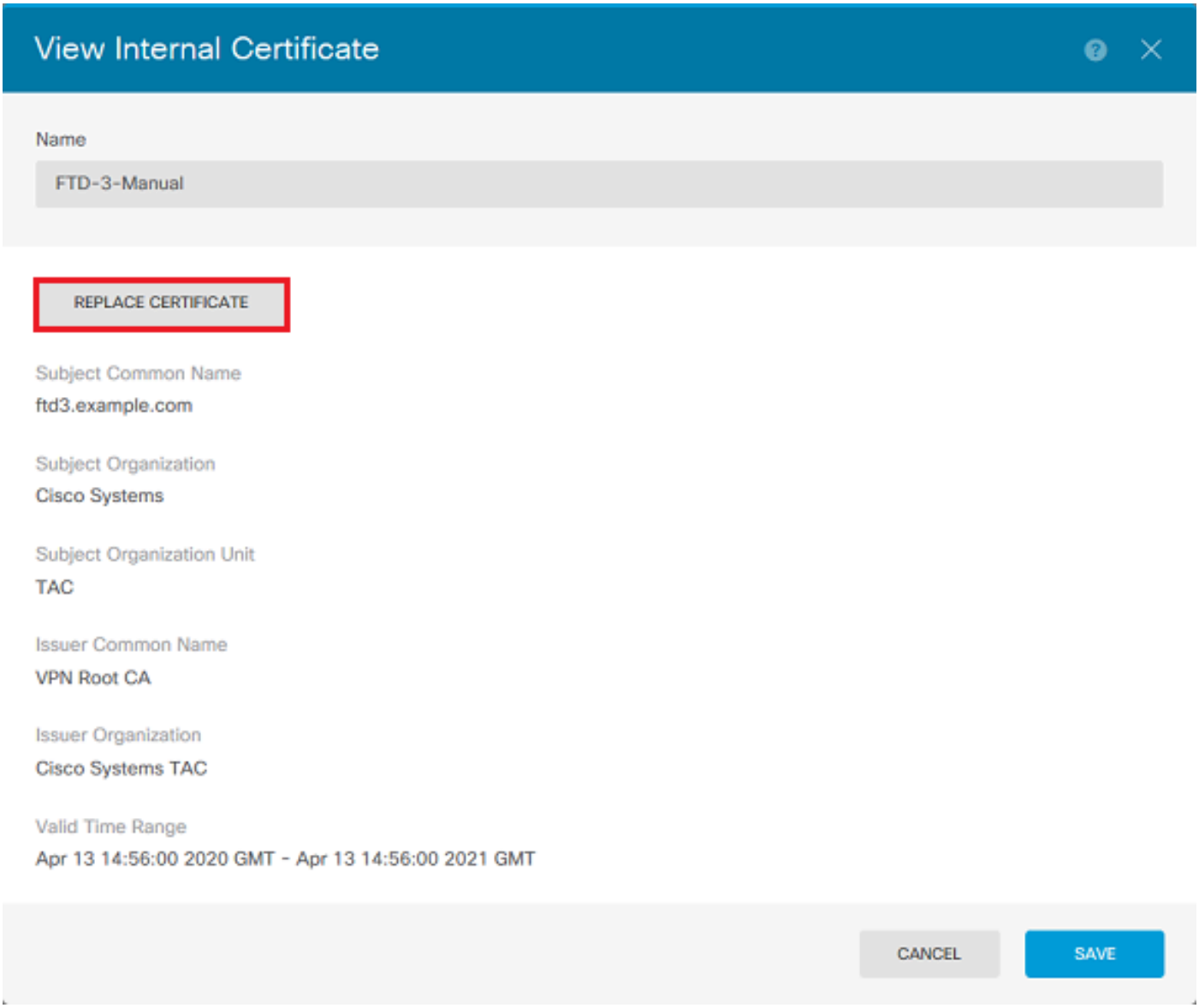
```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
.....................................+++
.....................................................................................+++
writing new private key to 'private.key'
-----
You are 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 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) []:ftd3.example.com
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

2. Envie o CSR gerado ou o CSR original para uma Autoridade de Certificação. Uma vez assinado o CSR, é fornecido um certificado de identidade renovado.

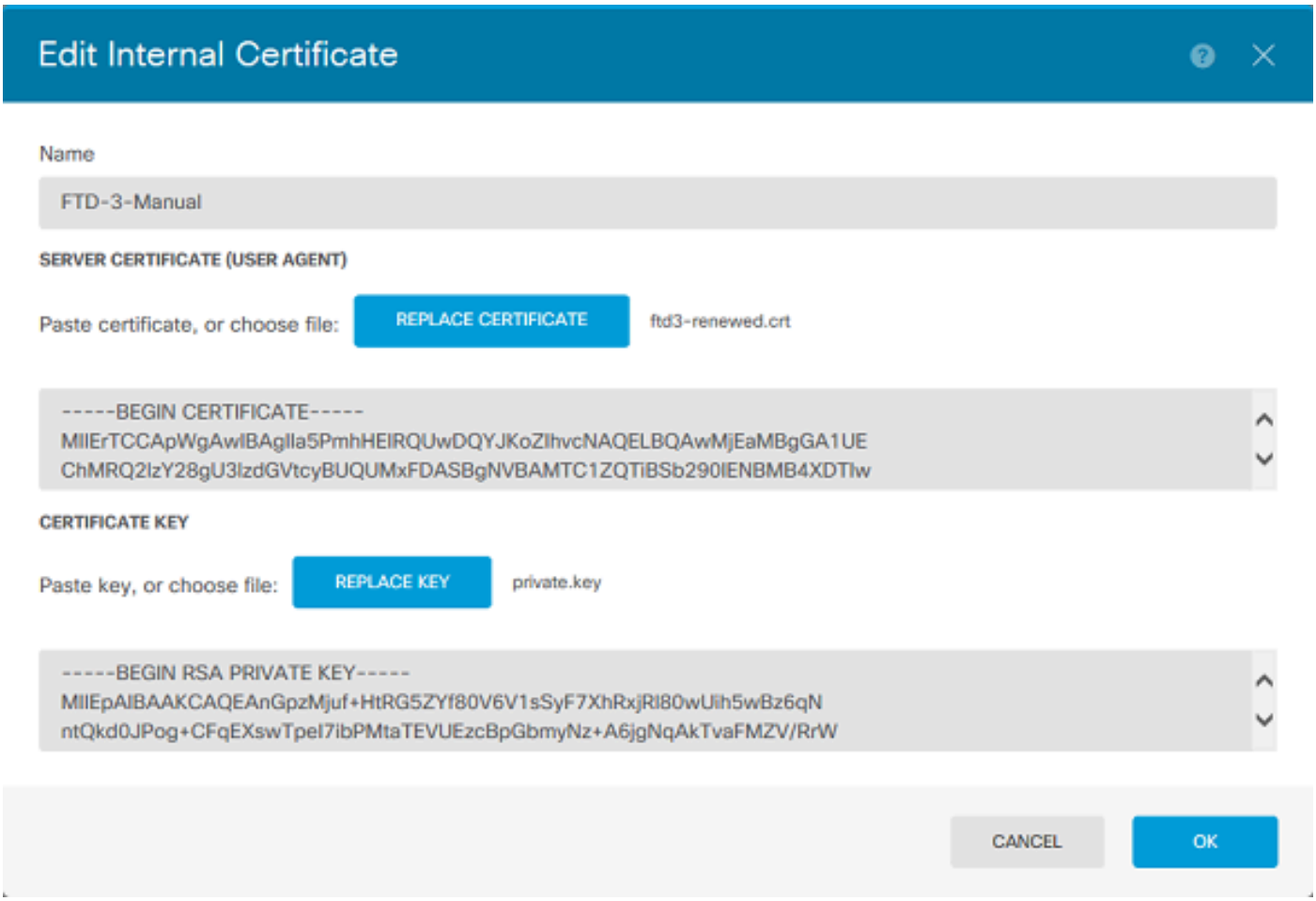
3. Navegue até Objetos > Certificados. Passe o mouse sobre o certificado que deseja renovar e clique no botão View, conforme mostrado na imagem.



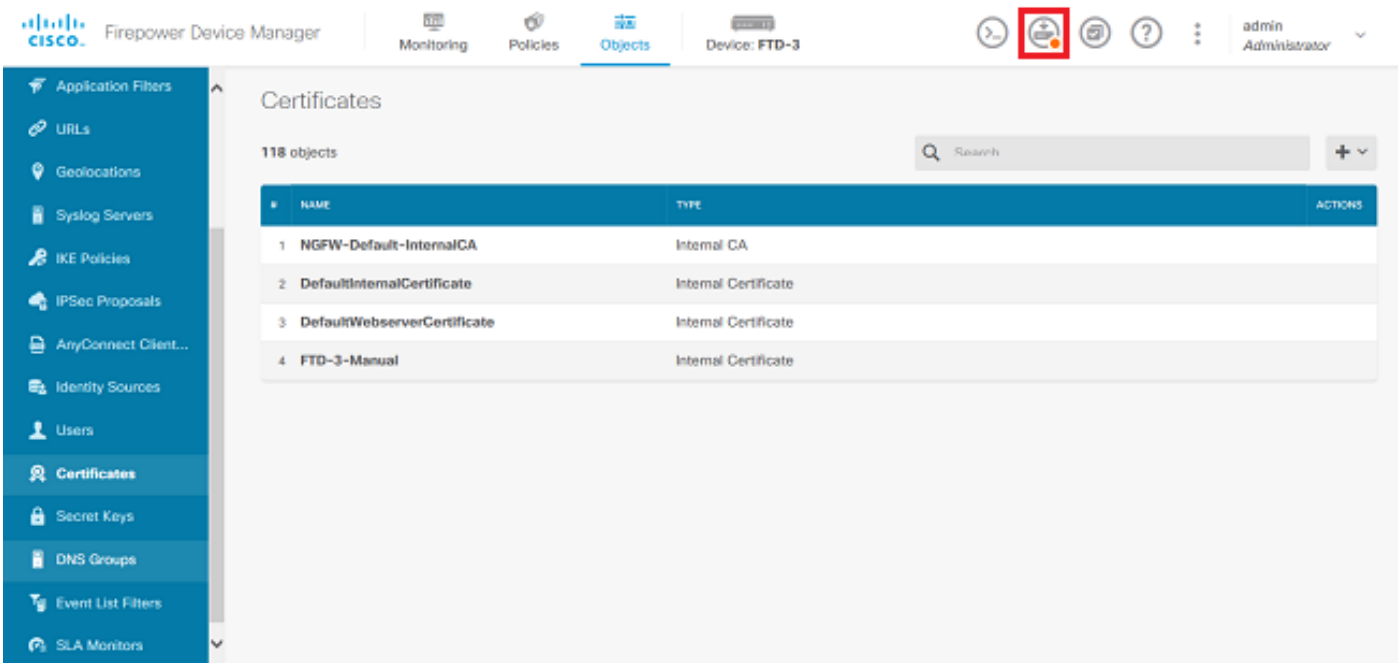
4. Na janela pop-up, clique em Substituir certificado conforme mostrado na imagem.



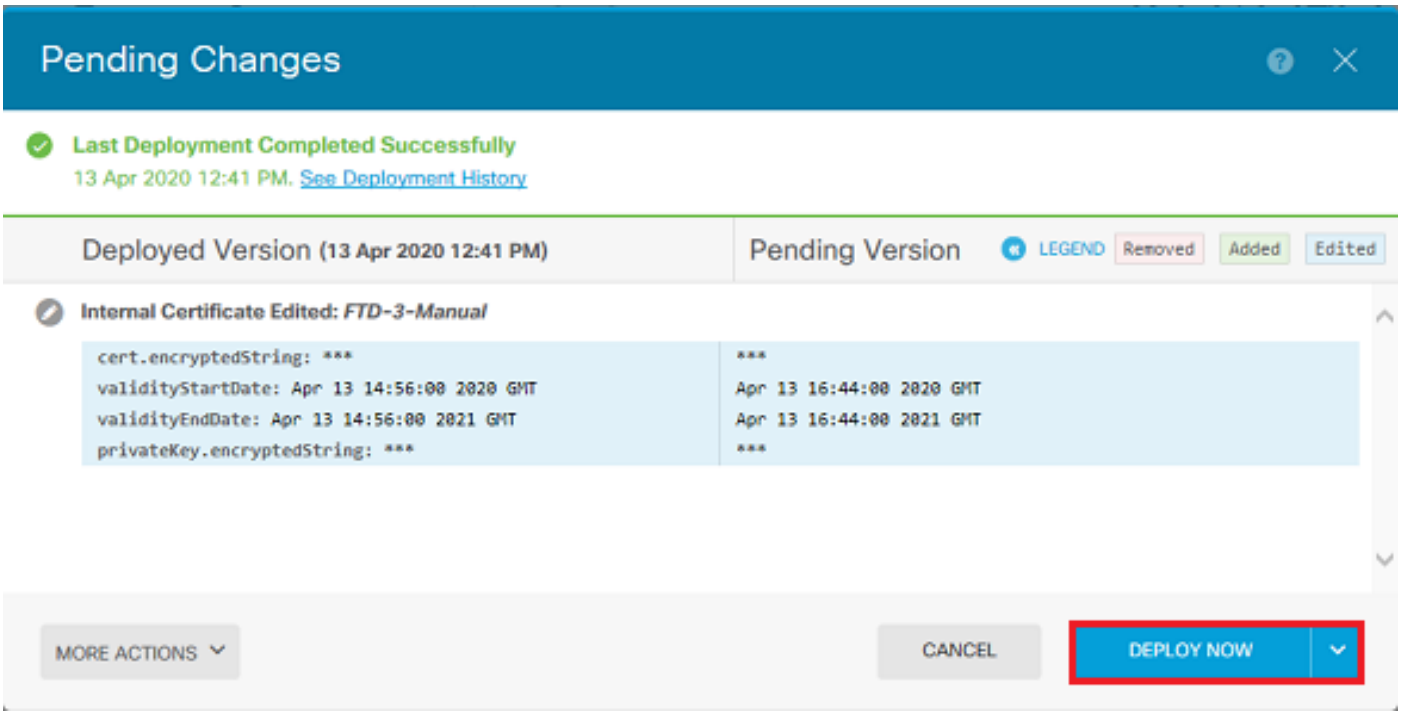
5. Faça upload ou copie e cole o certificado de identidade e a chave privada no formato PEM. Clique em OK quando terminar, conforme mostrado na imagem.



6. Clique no botão Alterações Pendentes na parte superior direita da tela, conforme mostrado na imagem.



7. Clique no botão Implantar Agora como mostrado na imagem.



Operações comuns do OpenSSL

Extrair certificado de identidade e chave privada do arquivo PKCS12

Um administrador pode receber um arquivo PKCS12 que precisa ser importado para o FTD. No momento, o FDM não oferece suporte à importação de arquivos PKCS12. Para importar os certificados e a chave privada contidos no arquivo PKCS12, os arquivos individuais devem ser extraídos do PKCS12 com o uso de uma ferramenta como o OpenSSL. Você precisa da senha usada para criptografar o PKCS12.

```
openssl pkcs12 -info -in pkcs12file.pfx
Enter Import Password: [PKCS12-passcode]
MAC Iteration 1
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    localKeyID: 28 20 C1 B4 08 1E 65 2E 4D 1D F9 F3 25 07 62 F7 D9 96 A7 F4
    friendlyName: ftd3.example.com
subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIErTCCApWgAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQxMzE2NDQwMFoXDTIxMDQxMzE2NDQwMFowQTEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEMMAoGA1UECxMDVEFDMRkwFwYDVQQDExBmdGQzLmV4YW1wbGUuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnGpzMjuf+HtRG5ZYf8OV6V1s
SyF7XhRxjRl8OwUih5wBz6qNntQkdOJPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZOIcpzVqL6hOziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS5O
QpQDTgvIiD1bYpPiWKpSOg1PZDnX8b74Os0pVKVXTsujQqSqH1va9BB6hK1JCoZa
HrP9YOxO9+MpVMH33R9vRl3SOEF6kpZ6VEdGI4s6/IRvaM1zlBcK1ON/N2+mjwID
AQABo4G3MIG0MAkGA1UdEwQCMAAwHQYDVR0OBBYEFMcvjLOXiSTzNADJ/ptNb/cd
```

```
zB8wMB8GA1UdIwQYMBaAFHekzDnhi4O727mjLXuwCRVFgyguMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwGwYDVR0RBBQwEoIQZnRk
My5leGFtcGxlLmNvbTAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMA0G
CSqGSIb3DQEBCwUAA4ICAQCjjrMjruGH5fpcFND8qfuVU0hkszCwq2O1oMqMrvXn
gENKcXxxT27z6AHnQXeX3vhDcY3zs+FzFSoP5tRRPmy/413HAN+QEP2L9MQVD9PH
f5OrQ/Ke5c16hMOJO8daR7wNzvFkcbicKCLRH0EvEoIOSPKsLyGSSxGmh6QXfZcM
GX3jG9Krglugp2UEqOug9HPTpgsbuNcHw8xXgFp6IAlOLrytwrLeMIh5V+Vh5pll
yTl9wo5VADoYKgN4O8D21TeJIj6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwfMXM4Tl
Rk3EOdSTENqzq2ZwnqJ4HCoqar7ASlQ5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBUlbadlnEfi5Jl8G+/vZl6ykcmXe9hokKYxY8cg/U717On/FbAmdYwRYgMAE4
RWfBpOvoNzn97cG+qzogo7j/OkTfYu3O9DzdU3uy+R8JJkBrerktrZR7w7OfP61O
IAs86N5Zb18U14Gfc9mOeXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2Px0yam/bROn0FoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJFOiVOGV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfpMwTiT47I
ng==
-----END CERTIFICATE-----
Certificate bag
Bag Attributes: <No Attributes>
subject=/O=Cisco Systems TAC/CN=VPN Root CA
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQwNTIzMTYwMFoXDTMwMDQwNTIzMTYwMFowMjEaMBgGA1UEChMRQ2lzY28gU3lz
dGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAxhTBKiB1xzLg2Jr48h/2u84RcWahOTmPYCNGYZg0PvSf
JOpKvAu5tz4z625Yx1nBtjSsEgzF+qETpSplEhjW2NxIclxuNirfrmSJQfIw51yT
PaFv7u+VhgyYbYsSxGAB/m6RWWpiNbg8SDoUACU7R/bvp1Rb8W6tXk/rsTljc7L2
c/G5MeDLNmc/i/M1zuMjhjOtCphsJPhvNII7lcNj6KOpvg2yB/Md7PXOZnLaz9pf
GgpjpHOzzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXmlHQcgp
g5BgZMGqroOl5rcqOPjtK9Tqg7qO13Vf0kMlsofMp+Bu1CiFDpawF/j8uSPuswEs
rzvJ+8GbOY1WEHtohgNGjPOOq8wnKQu0C47Ft1UMpdSwUsMMze0X43dyp/WoZtLW
4v/Pn/NibE3aoPOaMhIo4CdwSBHZOgVag4INqVsuFX1uPKD25WhrlO9LQ93P/sN3
FhoAh98HKOcuQ64Ua3AaShdzornD+G2J2pd1Nf1DahlzlskIMtlURSWdLjsHLKft
JqSOoLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/lyNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cxl1jIN0LdB+/jQqkfzmx9ziB1PXnIshNRbflLLrNfdDO9agqQsvsC
AwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDKC4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDKC4wCwYDVR0PBAQD
AgEGMA0GCSqGSIb3DQEBCwUAA4ICAQC6B+Y3obatEZqv0RQz1MS6oOumCgNWGi8d
kcRDxkY2F+zw3pBFa54Sin1OfRPJvZvLNJV5OdXmvH5luh6KJDMVrLMWNiSgI7Tn
OipqKraokS2Oo0STwQ7Q9Wk1xCrwxMfTuDJFMe8OqabFAU557O5PDXPtFEutn0xz
Ou8VMLBRy+gDc+0WARsjFj+0gUOc2Wj3gQ81GlyoPYgufWRnztN5rQxWzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AydsGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p7O2FZly5lxuzuA/wPnR89HiIkSF13OMTpnOIl3d6dO7s3bwyNja8JikYTCflle5
2CSsz4Cn/BlwfWyAcLN3HxUjG4Ev2818fWWpkYmuxujpKDFFzFOskpKAK53tNKPf
pn4+w5FyLo18o0AydtPoKjYkDqbvG/SRPbt92mdTIF7E6J+o8J6OV3YL+IyrZ+u0
MYqPd45Oi4cgHdMFICAndN3PYScrrGYHawfVxp+R+G4dTJWdMvthh3ftSOmkiKJ8
m1NH7WYST1kYcTbcokZiOIcZa+VVv5UOLIt/hDOVG7xqZOlpMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpxTIsmDv9rQzxBjuCyKn+23FkkUhFJt0D989UUypO8H9vDoJr
yzm9JOpMrg==
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    localKeyID: 28 20 C1 B4 08 1E 65 2E 4D 1D F9 F3 25 07 62 F7 D9 96 A7 F4
    friendlyName: ftd3.example.com
Key Attributes: <No Attributes>
Enter PEM pass phrase: [private-key-passcode]
Verifying - Enter PEM pass phrase: [private-key-passcode]
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIScA8TOogup4CAggA
MBQGCCqGSIb3DQMHBAgKqoTuZzoXsASCBMgOTEb24ENJl4/qh3GpsE2C2OCnJeid
```

```
ptDDIFdyOV4A+su3OJWzlnHrCuIhjR8+/p/NOWlA73x47R4T6+u4w4/ctHkvEbQj
gZJZzFWTed9HqidhcKxxOoM/w6/uDv/opc6/rlIZiaKp6FO9hOibqlGI9kjxkWQC
EQR8cM1U2yi0vagL8pOYdeujCrzBtorRp9BMJelCP1Mw9t0EbAC4mmuedzs+86r1
xadK7qHBuWUJcO3SLXLCmX5yLSGteWcoaPZnIKO9UhLxpUSJTkWLHr2VtE1ACMRc
RlPBXMLb7OnMtPTqctl58+Q/axtQCWUs8caHs3LvVfOnRG+War49/F8Ii8mqnNnb
M6ZTwTOZ1sn0f4ohVePrW/kkdlQavJbPa+0dzjZvs88ClEXAJ/XIegfSWifJAXqP
3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jjlKgfoxubtnuFq
un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZHOBuFls+wZEmzYqw+cuc+I8XEFVOMl8
P3ah28Nno0jXMk4MpfFJlYMCmMq66xj5gZtcVZxOGCOswOCKU0JiFFQTEmmVf9/C
65a96np7YCI8s6UnUWi5Zp/NrbN31HkPOwt7+1DFGFit1pTTGvOFchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG1l5NSslwKbTGiiwCYwON8c09TXQb04rMomFDAv8
aef1aBsjMqEUkzOZK0U2ZgTxMline8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubp0
qtmFX/DtSu9J2yevfV+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc4O
w94fQH/DJ/lKsmSVwBLQLEKRl/nIDz36kmA27+1nVtX42PbEaIaFgucU4xHKx3zN
mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaq8
fNl7vEB+aret+PmqCiQYlHqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUROTuBHQhRK
3XpHfGXpe/OOGdW3LeifNLvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP
VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzdOcJ3aGCeAl84XuPRfQhHe/Aj7q6l6uqB
W3Kt+kMJ9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/
QCyhIRk3mx+8a1YLqK+hOMjWWBDEHX2mvbdKickK/jhwRdR/WmFOALq51phgtZlz
Zedl5UbPqWahJsjoO9N5pp7Uq5iV0/xq4Ml+/xQIYo2GIrqyat4AdB2B6K8K3xQd
Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTfzH5zgneUwLwnuBAbGT3oMSQ/
OKXnhcmUGu8XvLEfU/PITvGzKrO6o12/hHJtzXQ8eNPDJbvcD/okRRKZpmjH+ijp
FPD/WgQ/vmO9HdCWW3flhqceqfHff8ClCJYFLxsgZp4M3G+WyQTky4J8+6uTn/mj
yyZ5JCZdlt42haSNqU/ynioCjh5XY4m8WMZsOJBNPjKZiUX/vqVcc+/nodl7VRZy
ELk=
-----END ENCRYPTED PRIVATE KEY-----
```


pkcs12file.pfx é um arquivo PKCS12 que precisa ser desempacotado.

Neste exemplo, três arquivos separados são criados:

Um para o Certificado de Identidade. Você pode dizer que este é o certificado de identidade devido ao assunto=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com.


```
subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIErTCCApWgAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQxMzE2NDQwMFoXDTIxMDQxMzE2NDQwMFowQTEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEMMAoGA1UECxMDVEFDMRkwFwYDVQQDExBmdGQzLmV4YW1wbGUuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnGpzMjuf+HtRG5ZYf80V6V1s
SyF7XhRxjRl8OwUih5wBz6qNntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZOIcpzVqL6hOziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50
QpQDTgvIiD1bYpPiWKpS0g1PZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZa
HrP9Y0xO9+MpVMH33R9vRl3SOEF6kpZ6VEdGI4s6/IRvaM1zlBcK1ON/N2+mjwID
AQABo4G3MIG0MAkGA1UdEwQCMAAwHQYDVR0OBBYEFMcvjL0XiSTzNADJ/ptNb/cd
zB8wMB8GA1UdIwQYMBaAFHekzDnhi4O727mjLXuwCRVFgyguMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwGwYDVR0RBBQwEoIQZnRk
My5leGFtcGxlLmNvbTAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMA0G
CSqGSIb3DQEBCwUAA4ICAQCjjrMjruGH5fpcFND8qfuVU0hkszCwq2O1oMqMrvXn
gENKcXxxT27z6AHnQXeX3vhDcY3zs+FzFSoP5tRRPmy/413HAN+QEP2L9MQVD9PH
f5OrQ/Ke5c16hMOJO8daR7wNzvFkcbicKCLRH0EvEoIOSPKsLyGSSxGmh6QXfZcM
GX3jG9Krglugp2UEqOug9HPTpgsbuNcHw8xXgFp6IAlOLrytwrLeMIh5V+Vh5pll
yTl9wo5VADoYKgN4O8D21TeJIj6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwfMXM4Tl
```

```
Rk3EOdSTENqzq2ZwnqJ4HCoqar7ASlQ5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBUlbadlnEfi5Jl8G+/vZl6ykcmXe9hokKYxY8cg/U717On/FbAmdYwRYgMAE4
RWfBpOvoNzn97cG+qzogo7j/OkTfYu3O9DzdU3uy+R8JJkBrerktrZR7w7OfP61O
IAs86N5Zb18U14Gfc9mOeXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2PxOyam/bROnOFoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJFOiVOGV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfpMwTiT47I
ng==
-----END CERTIFICATE-----
```

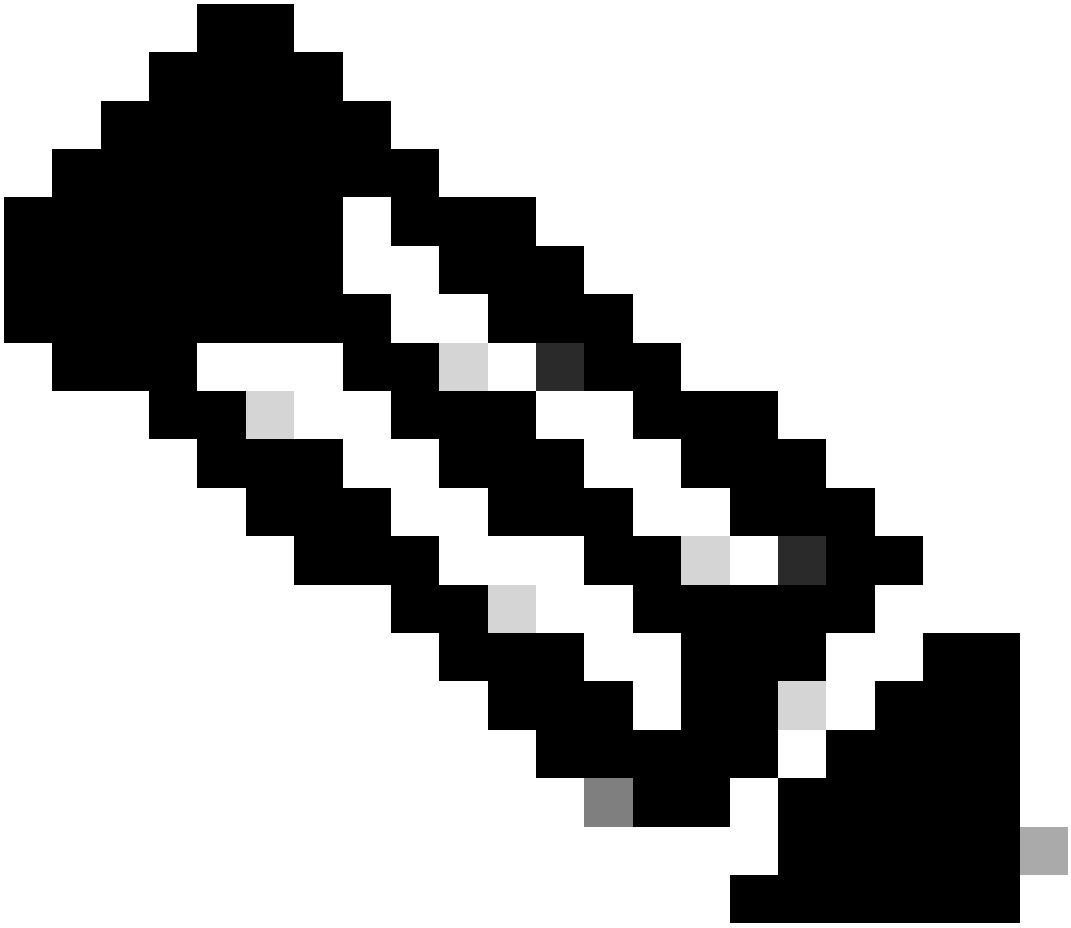
Uma para o Certificado de CA Emissor. Você pode dizer que este é o certificado de identidade devido ao assunto=/O=Cisco Systems TAC/CN=VPN Root CA. Este é o mesmo valor que o emissor no Certificado de Identidade visto anteriormente:

```
subject=/O=Cisco Systems TAC/CN=VPN Root CA
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQwNTIzMTYwMFoXDTMwMDQwNTIzMTYwMFowMjEaMBgGA1UEChMRQ2lzY28gU3lz
dGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAxhTBKiB1xzLg2Jr48h/2u84RcWahOTmPYCNGYZg0PvSf
JOpKvAu5tz4z625Yx1nBtjSsEgzF+qETpSplEhjW2NxIclxuNirfrmSJQfIw51yT
PaFv7u+VhgyYbYsSxGAB/m6RWWpiNbg8SDoUACU7R/bvp1Rb8W6tXk/rsTljc7L2
c/G5MeDLNmc/i/M1zuMjhj0tCphsJPhvNII7lcNj6KOpvg2yB/Md7PXOZnLaz9pf
GgpjpH0zzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXmlHQcgp
g5BgZMGqro0l5rcq0PjtK9Tqg7qO13Vf0kMlsofMp+Bu1CiFDpawF/j8uSPuswEs
rzvJ+8GbOY1WEHtohgNGjPOOq8wnKQuOC47Ft1UMpdSwUsMMze0X43dyp/WoZtLW
4v/Pn/NibE3aoPOaMhIo4CdwSBHZOgVag4INqVsuFX1uPKD25WhrlO9LQ93P/sN3
FhoAh98HKOcuQ64Ua3AaShdzornD+G2J2pd1Nf1DahlzlskIMtlURSWdLjsHLKft
JqSOoLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/lyNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cxl1jIN0LdB+/jQqkfzmx9ziB1PXnIshNRbflLLrNfdDO9agqQsvsC
AwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDKC4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDKC4wCwYDVR0PBAQD
AgEGMA0GCSqGSIb3DQEBCwUAA4ICAQC6B+Y3obatEZqv0RQz1MS6oOumCgNWGi8d
kcRDxkY2F+zw3pBFa54Sin1OfRPJvZvLNJV5OdXmvH5luh6KJDMVrLMWNiSgI7Tn
0ipqKraokS2Oo0STwQ7Q9Wk1xCrwxMfTuDJFMe8OqabFAU557O5PDXPtFEutn0xz
Ou8VMLBRy+gDc+0WARsjFj+0gUOc2Wj3gQ81GlyoPYgufWRnztN5rQxWzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AydsGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p7O2FZly5lxuzuA/wPnR89HiIkSF13OMTpnOIl3d6dO7s3bwyNja8JikYTCflle5
2CSsz4Cn/BlwfWyAcLN3HxUjG4Ev2818fWWpkYmuxujpKDFFzF0skpKAK53tNKPf
pn4+w5FyLo18o0AydtPoKjYkDqbvG/SRPbt92mdTIF7E6J+o8J6OV3YL+IyrZ+u0
MYqPd45Oi4cgHdMFICAndN3PYScrrGYHawfVxp+R+G4dTJWdMvthh3ftSOmkiKJ8
m1NH7WYST1kYcTbcokZiOIcZa+VVv5UOLIt/hDOVG7xqZOlpMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpxTIsmDv9rQzxBjuCyKn+23FkkUhFJtOD989UUyp08H9vDoJr
yzm9JOpMrg==
-----END CERTIFICATE-----
```

E uma para a chave privada:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIScA8TOogup4CAggA
MBQGCCqGSIb3DQMHBAgKqoTuZzoXsASCBMgOTEb24ENJl4/qh3GpsE2C2OCnJeid
ptDDIFdyOV4A+su3OJWzlnHrCuIhjR8+/p/N0WlA73x47R4T6+u4w4/ctHkvEbQj
```

```
gZJZzFWTed9HqidhcKxxOoM/w6/uDv/opc6/rlIZiaKp6FO9hOibqlGI9kjxkWQC
EQR8cM1U2yi0vagL8pOYdeujCrzBtorRp9BMJelCP1Mw9t0EbAC4mmuedzs+86r1
xadK7qHBuWUJcO3SLXLCmX5yLSGteWcoaPZnIKO9UhLxpUSJTkWLHr2VtE1ACMRc
RlPBXMLb7OnMtPTqctl58+Q/axtQCWUs8caHs3LvVf0nRG+War49/F8Ii8mqnNnb
M6ZTwTOZ1sn0f4ohVePrW/kkdlQavJbPa+0dzjZvs88ClEXAJ/XIegfSWifJAXqP
3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jjlKgfoxubtnuFq
un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZHOBuFls+wZEmzYqw+cuc+I8XEFVOMl8
P3ah28Nno0jXMk4MpfFJlYMCmMq66xj5gZtcVZxOGCOswOCKU0JiFFQTEmmVf9/C
65a96np7YCI8s6UnUWi5Zp/NrbN31HkPOwt7+1DFGFit1pTTGvOFchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG1l5NSslwKbTGiiwCYw0N8cO9TXQbO4rMomFDAv8
aef1aBsjMqEUkzOZKOU2ZgTxMline8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubp0
qtmFX/DtSu9J2yevfV+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc4O
w94fQH/DJ/lKsmSVwBLQLEKRl/nIDz36kmA27+1nVtX42PbEaIaFgucU4xHKx3zN
mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaq8
fNl7vEB+aret+PmqCiQYlHqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUROTuBHQhRK
3XpHfGXpe/OOGdW3LeifNLvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP
VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzdOcJ3aGCeAl84XuPRfQhHe/Aj7q6l6uqB
W3Kt+kMJ9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/
QCyhIRk3mx+8a1YLqK+hOMjWWBDEHX2mvbdKickK/jhwRdR/WmFOALq51phgtZlz
Zedl5UbPqWahJsjoO9N5pp7Uq5iVO/xq4Ml+/xQIYo2GIrqyat4AdB2B6K8K3xQd
Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTfzH5zgneUwLwnuBAbGT3oMSQ/
OKXnhcmUGu8XvLEfU/PITvGzKrO6o12/hHJtzXQ8eNPDJbvcD/okRRKZpmjH+ijp
FPD/WgQ/vmO9HdCWW3flhqceqfHff8ClCJYFLxsgZp4M3G+WyQTky4J8+6uTn/mj
yyZ5JCZdlt42haSNqU/ynioCjh5XY4m8WMZsOJBNPjKZiUX/vqVcc+/nodl7VRZy
ELk=
-----END ENCRYPTED PRIVATE KEY-----
```



Observação: a chave privada é criptografada e o FDM não aceita chaves privadas criptografadas.

Para descriptografar a chave privada, copie a chave privada criptografada para um arquivo e execute este comando openssl:

```
openssl rsa -in encrypted.key -out unencrypted.key
Enter pass phrase for encrypted.key: [private-key passphrase]
writing RSA key
```

- encrypted.key é o nome do arquivo que contém a chave privada criptografada.
- unencrypted.key é o nome do arquivo que tem a chave não criptografada.

A chave privada não criptografada pode mostrar -----BEGIN RSA PRIVATE KEY----- em vez de -----BEGIN ENCRYPTED PRIVATE KEY----- como visto neste exemplo:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnGpzMjuf+HtRG5ZYf8OV6V1sSyF7XhRxjRl8OwUih5wBz6qN
ntQkdOJPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGbmyNz+A6jgNqAkTvaFMZV/RrW
qCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqNBqotoz3/8CrZOIcpzVqL6hOz
iJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS5OQpQDTgvIiD1bYpPiWKpSOg1P
ZDnX8b74Os0pVKVXTsujQqSqH1va9BB6hK1JCoZaHrP9YOxO9+MpVMH33R9vRl3S
OEF6kpZ6VEdGI4s6/IRvaM1zlBcK1ON/N2+mjwIDAQABAoIBAEQzCd1KMBrosdmk
eRvoMPiaemBbze2cXlJWXZ2orICSXhvMOokBGJFDQXN47ZCuVqYAqOecjU9RzGgE
NbXYfUsD6+P91k+/Gj1RiCNLBHBwdgewzw1quTxP54zSpAVlIXyQ+FolTzjH1yfW
7iHhuSujYsAYLWPy4Yg3NpU2IdzeQoK5ViuSTTNx8LHYBKw1Qf7HVaQTfmsWOAyg
/vjZqjRkukqKM41srgkO/HjPnEBDuUWVTehzMCk1etijENc7ttISzYIEMNPthe6O
NpidXAHoJ1lJM6HB9ZraBH5fu7MZJZOOn6YVKQuCdWOWfnKiNQCDsXq7X5EWsaj3
cgyjWlkCgYEAy33k1wxp7WEqg1zEwqOVq7AtoL6i4V9QCenMThQAHwNAAUGGOSIF
JhpKyApm/BUogSIOMzIPse+NgAA66TRn4qfkbpvTI98CeCUxiUPcbRmqZnYxC0fp
Pzosv5OnBLltoIOprIO2S5a261w6JGNAfD95tCjCYYrB8Cw/HbZOLPUCgYEAxMbZ
KVyosBxaAIFQinHaff3fVSTsEOZFpLCBbLybgLcP8LsLdahBsj6HK/hAffKXOdvM
35CAM7ZL/WCI1Jb+dx4YcD9q8lbVMu4HTvSl2deTZoZrBG2iFX6OSsn2rLKAH+cH
uLSHCNAj9cj9syldZErGLZtBQpJPtpLRd6iyOvMCgYBP/zoLYJHOBBLWeY3QioLO
cABABTG7L+EjRIpQ14QErR5oX/4IT9t+Uy+63HwH9blqqpyye6e359jUzUJbk4KT
lDU1VoT2wSETYmvK7qalLUXT6fr12FtVw+T7m2w5azwxshDuBQmRRbq7ZBJnY61i
KwIJVUy1U/tSE9LsN1McUQKBgQClc4ykeoRbj3sdcZ2GyrQru4pMzP6wNu3Xy5EH
HI6ja0i74ImCJDcY5/o/vjx7qb39qBJa5+TjliPOp5xlI5BSF7vOpV4G5XvdlsYO
XSYWRGxriBnzXzspV3/M4oPGMVAJgve7Fg9OGY4i2xx1yBH+geCf+CqnDt53ZHs7
YVz6gQKBgQDG42tZZ1kNAnOx/k1lUlZrEeF8iqdsyVcRf4fAvqsPbY3+kdae+8Or
+cQpVoeWzOQLUkA6eMsiTLmcWYb62qMgdpluyKoOciPG9+2AGNTvQp/ig34pF2F/
9OGuVYlA1p7mkP8Vb1Mo1ugVOzUqAIjHKiGUzBWVsxOZsGa+SY47uw==
-----END RSA PRIVATE KEY-----
```

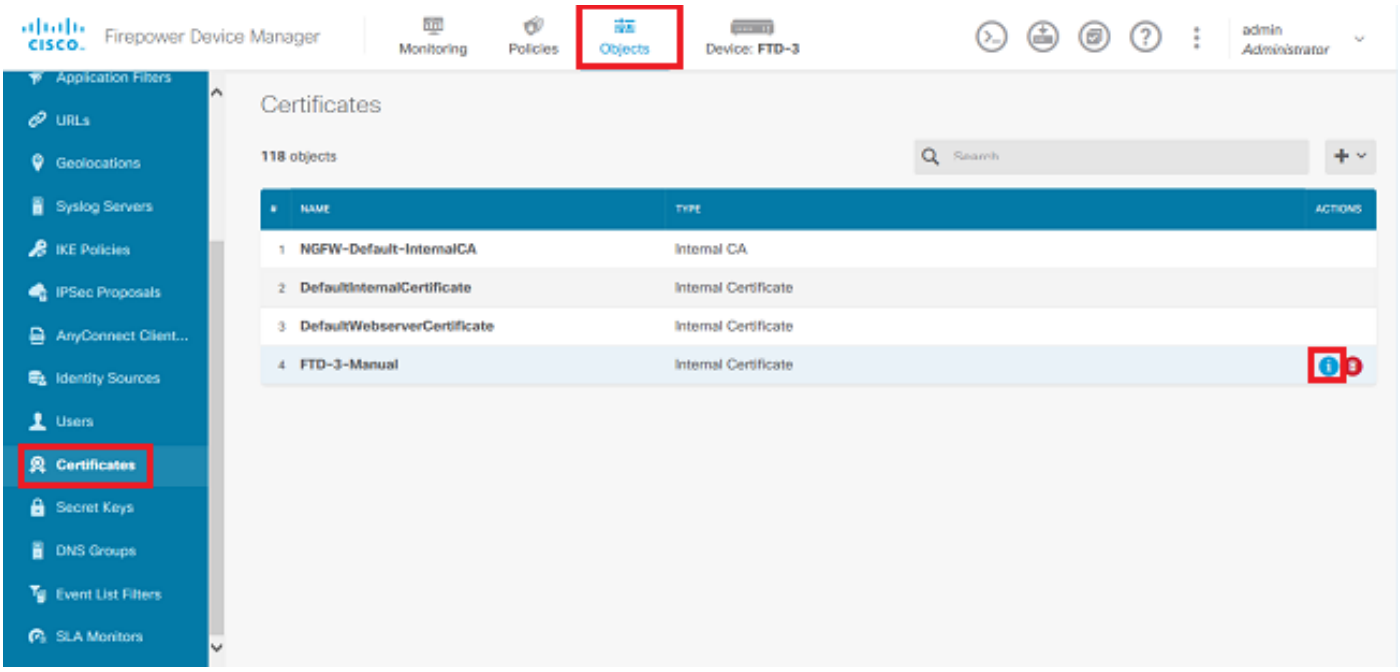
Depois que a chave privada for descriptografada, o arquivo de identidade e chave privada poderá ser carregado, ou copiado e colado no FDM com a Etapa 3 na seção Inscrição Manual mencionada anteriormente. A CA emissora pode ser instalada com o uso das etapas de Instalação de Certificado de CA Confiável mencionadas anteriormente.

Verificar

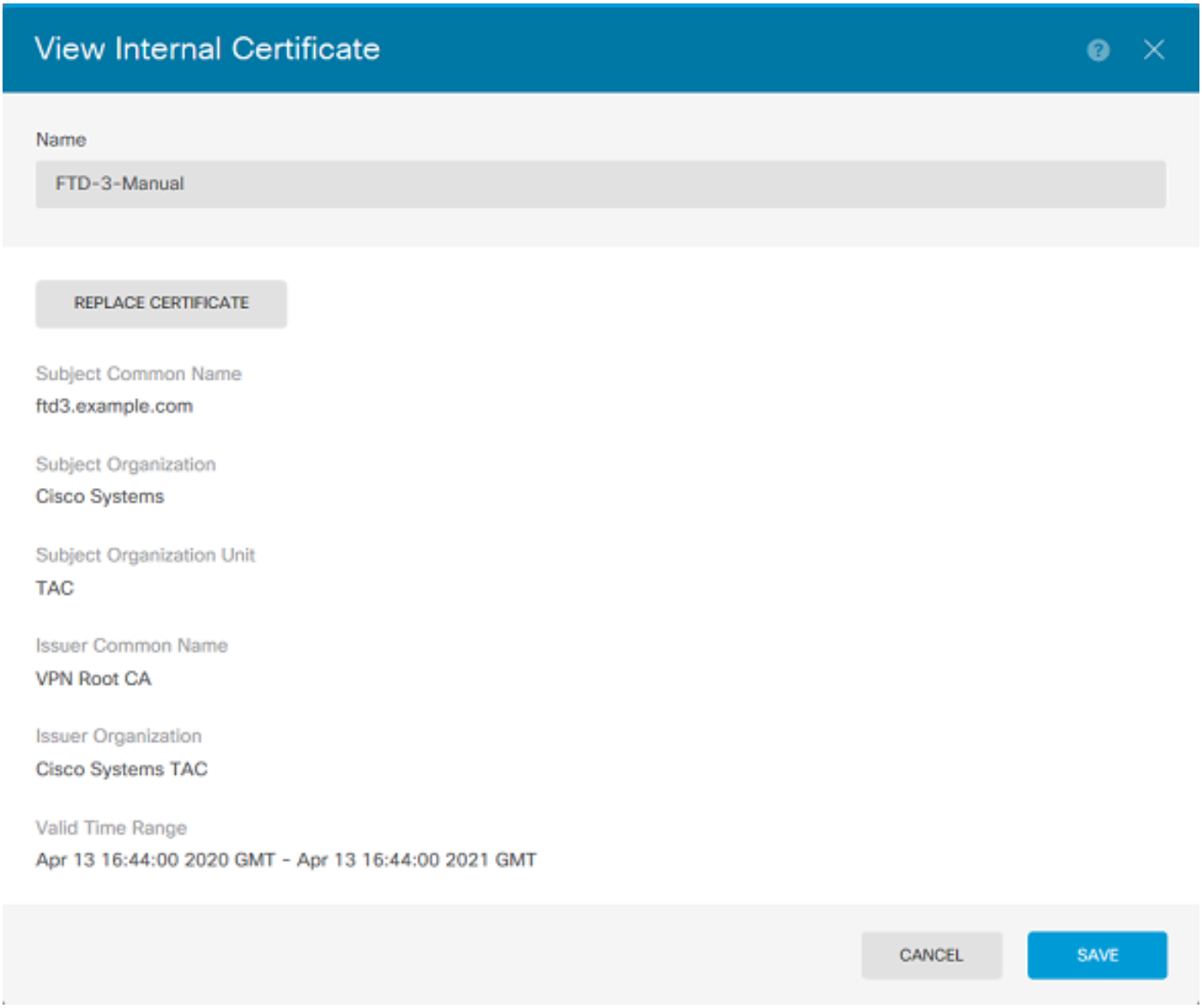
Use esta seção para confirmar se a sua configuração funciona corretamente.

Exibir Certificados Instalados no FDM

1. Navegue até Objetos > Certificados. Passe o mouse sobre o certificado que deseja verificar e clique no botão view, conforme mostrado na imagem.



2. A janela pop-up fornece detalhes adicionais sobre o certificado, conforme mostrado na imagem.

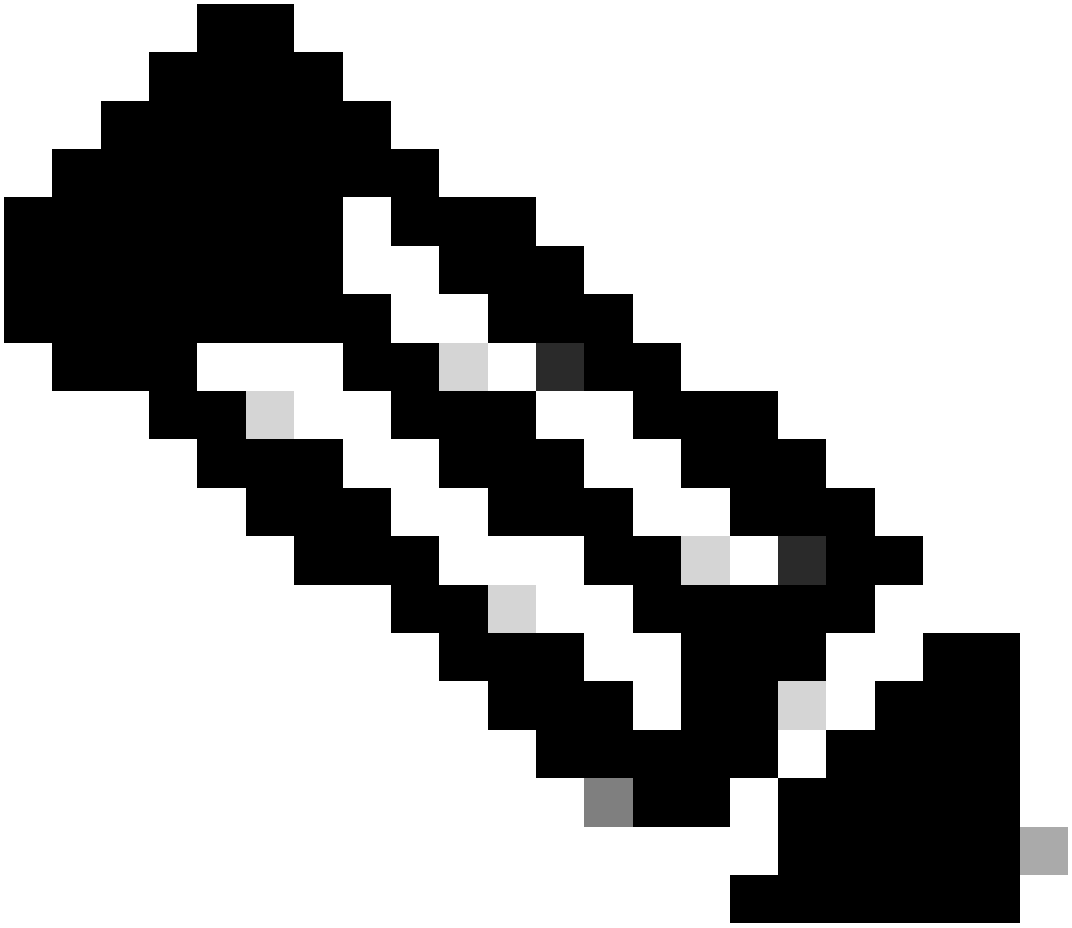


Exibir certificados instalados na CLI

Você pode usar o Console CLI no FDM ou SSH no FTD e executar o comando show crypto ca certificates para verificar se um certificado foi aplicado ao dispositivo como mostrado na imagem.

Saída de exemplo:

```
> show crypto ca certificates

Certificate
  Status: Available
  Certificate Serial Number: 6b93e68471084505
  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=ftd3.example.com
    ou=TAC
    o=Cisco Systems
  Validity Date:
    start date: 16:44:00 UTC Apr 13 2020
    end   date: 16:44:00 UTC Apr 13 2021
  Storage: config
  Associated Trustpoints: FTD-3-Manual
```



Observação: os certificados de identidade só são exibidos na CLI quando são usados com um serviço como o AnyConnect. Os certificados CA confiáveis são exibidos após a implantação.

Troubleshooting

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

Comandos debug

As depurações podem ser executadas na CLI de diagnóstico depois que você conectar o FTD 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

Importar ASA exportado PKCS12

Ao tentar extrair o certificado de identidade e a chave privada de um ASA PKCS12 exportado no OpenSSL, você poderá receber um erro semelhante a este:

```
openssl pkcs12 -info -in asaexportedpkcs12.p12
6870300:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1220:
6870300:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:386:Type=PK
```

Para contornar esse problema, o arquivo pkcs12 deve primeiro ser convertido para o formato DER:

```
openssl enc -base64 -d -in asaexportedpkcs12.p12 -out converted.pfx
```

Depois que isso for feito, os passos da seção Extraindo o certificado de identidade e a chave privada do arquivo PKCS12 anteriormente neste documento podem ser seguidos para importar o certificado de identidade e a chave privada.

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.