Installer et renouveler le certificat sur le FTD géré par FDM

Table des matières

Introduction

Ce document décrit comment installer, approuver et renouveler des certificats auto-signés et des certificats signés par une autorité de certification tierce ou interne sur FTD.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- L'inscription manuelle des certificats nécessite l'accès à une autorité de certification tierce approuvée. Les exemples de fournisseurs CA tiers incluent, sans s'y limiter, Entrust, Geotrust, GoDaddy, Thawte et VeriSign.
- Vérifiez que Firepower Threat Defense (FTD) dispose de l'heure, de la date et du fuseau horaire corrects. Avec l'authentification de certificat, il est recommandé d'utiliser un serveur NTP (Network Time Protocol) pour synchroniser l'heure sur le FTD.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FTDv qui exécute 6.5.
- Pour la création de paire de clés et de demande de signature de certificat (CSR), OpenSSL est utilisé.

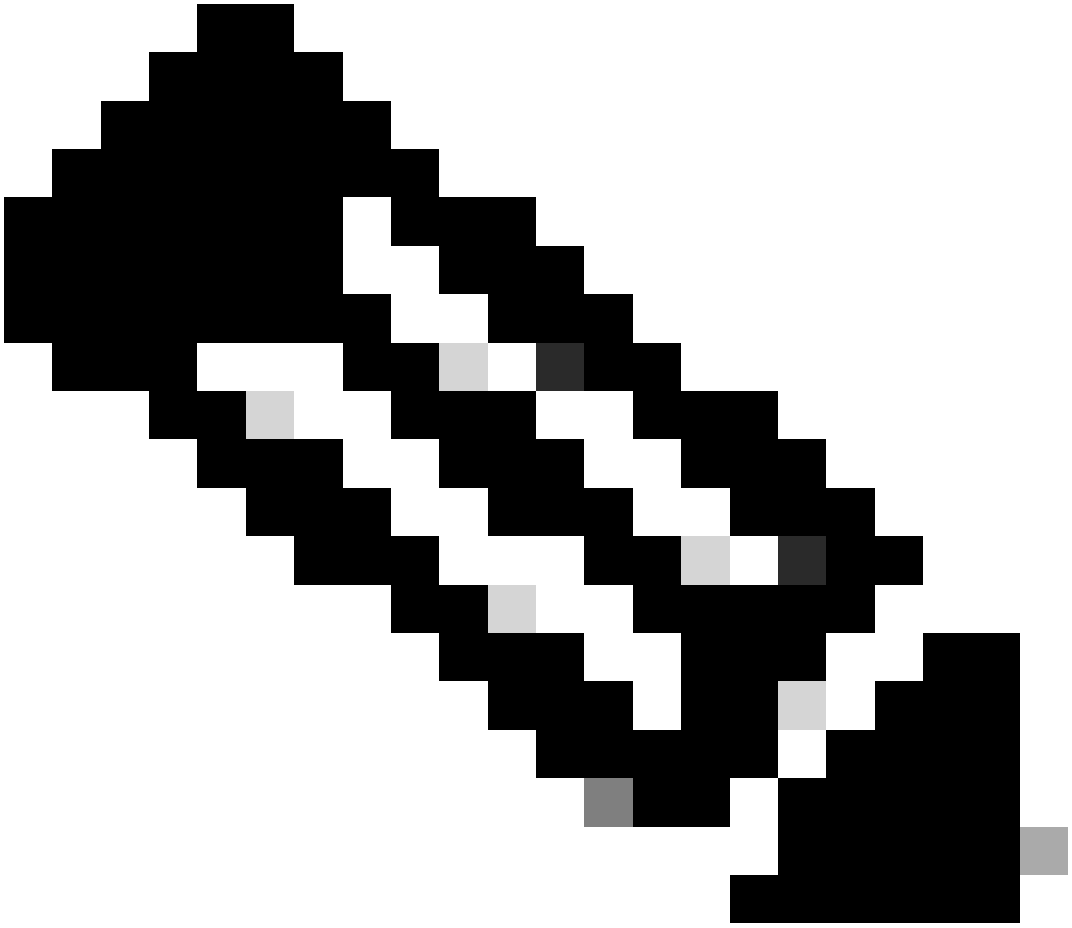
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Installation du certificat

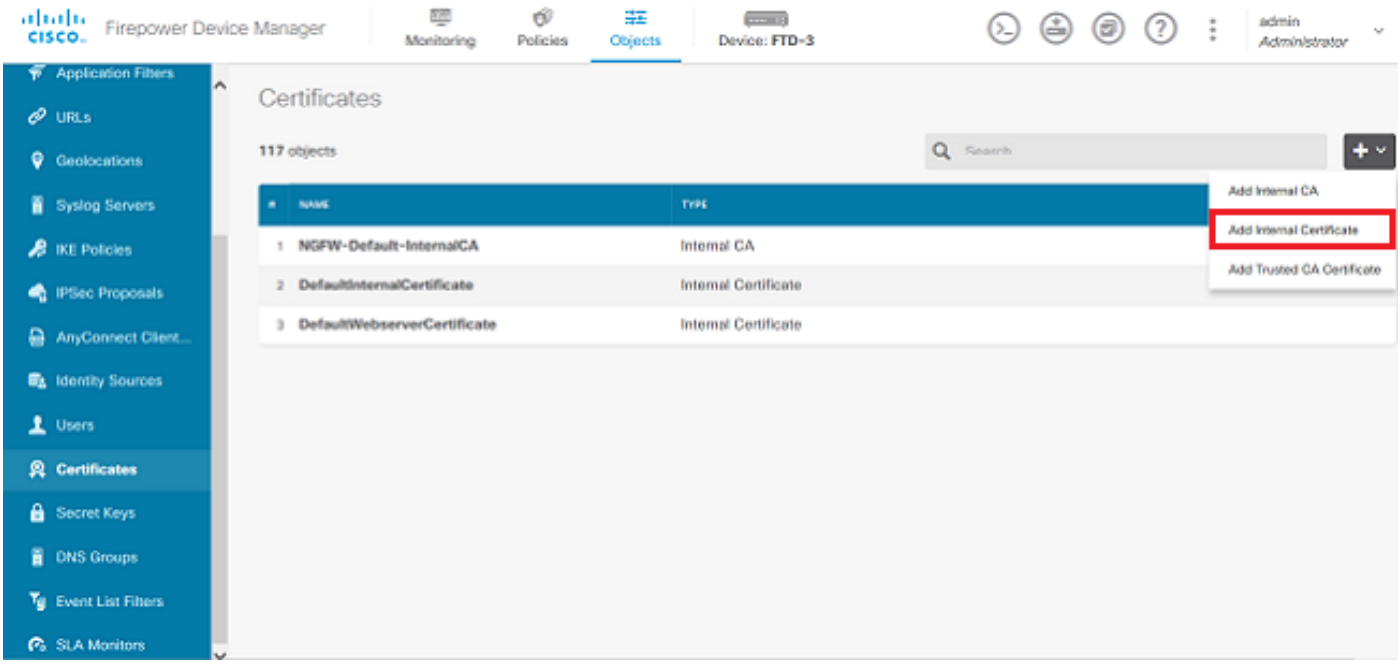
Inscription auto-signée

Les certificats auto-signés sont un moyen facile d'obtenir un certificat avec les champs appropriés ajoutés au périphérique FTD. Bien qu'ils ne soient pas fiables dans la plupart des pays, ils peuvent néanmoins fournir des avantages de cryptage similaires à ceux d'un certificat signé par un tiers. Cependant, il est recommandé d'avoir un certificat approuvé signé par l'autorité de certification afin que les utilisateurs et les autres périphériques puissent faire confiance au certificat présenté par le FTD.

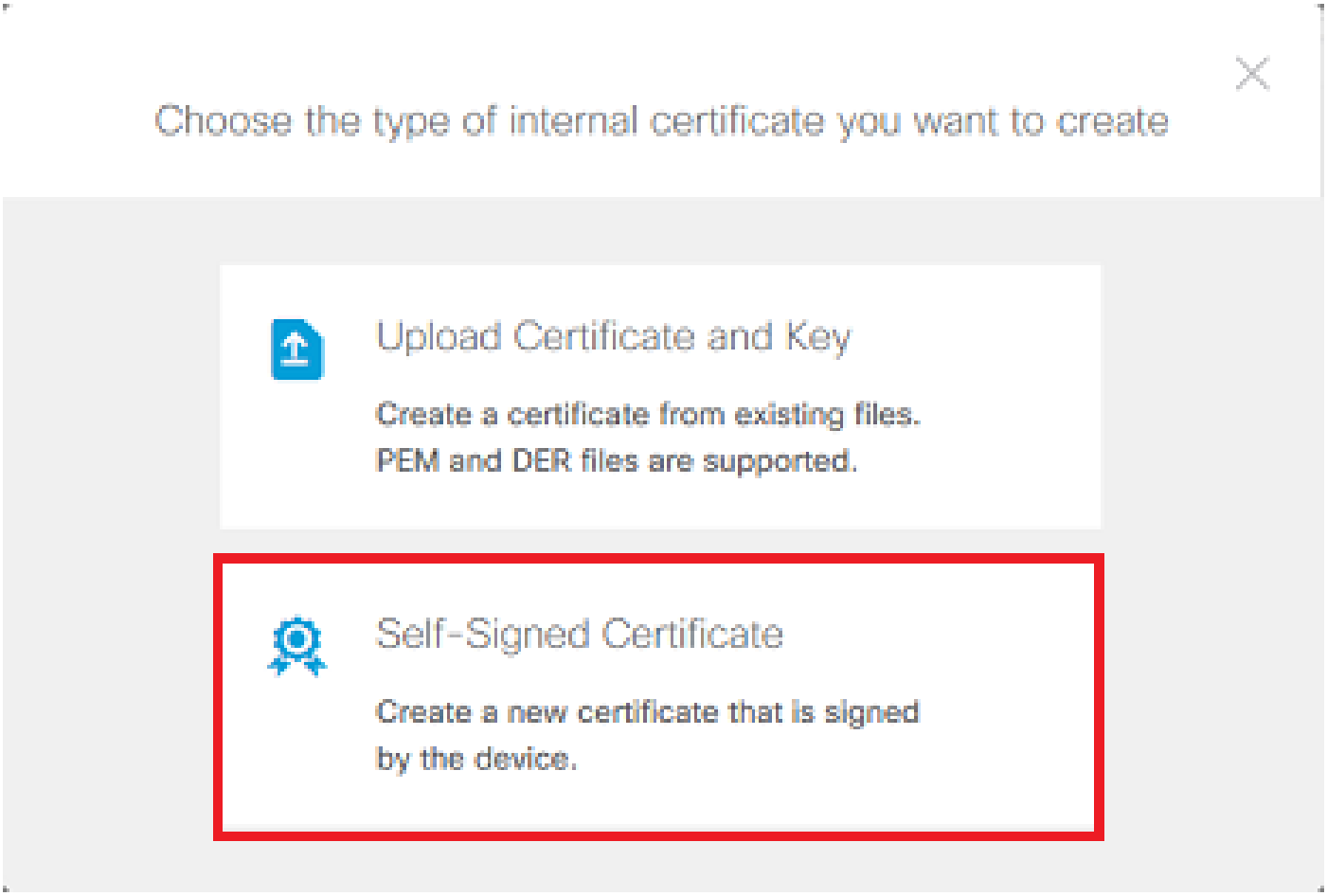


Remarque : Firepower Device Management (FDM) ne dispose pas d'un certificat auto-signé par défaut nommé DefaultInternalCertificate qui peut être utilisé à des fins similaires.

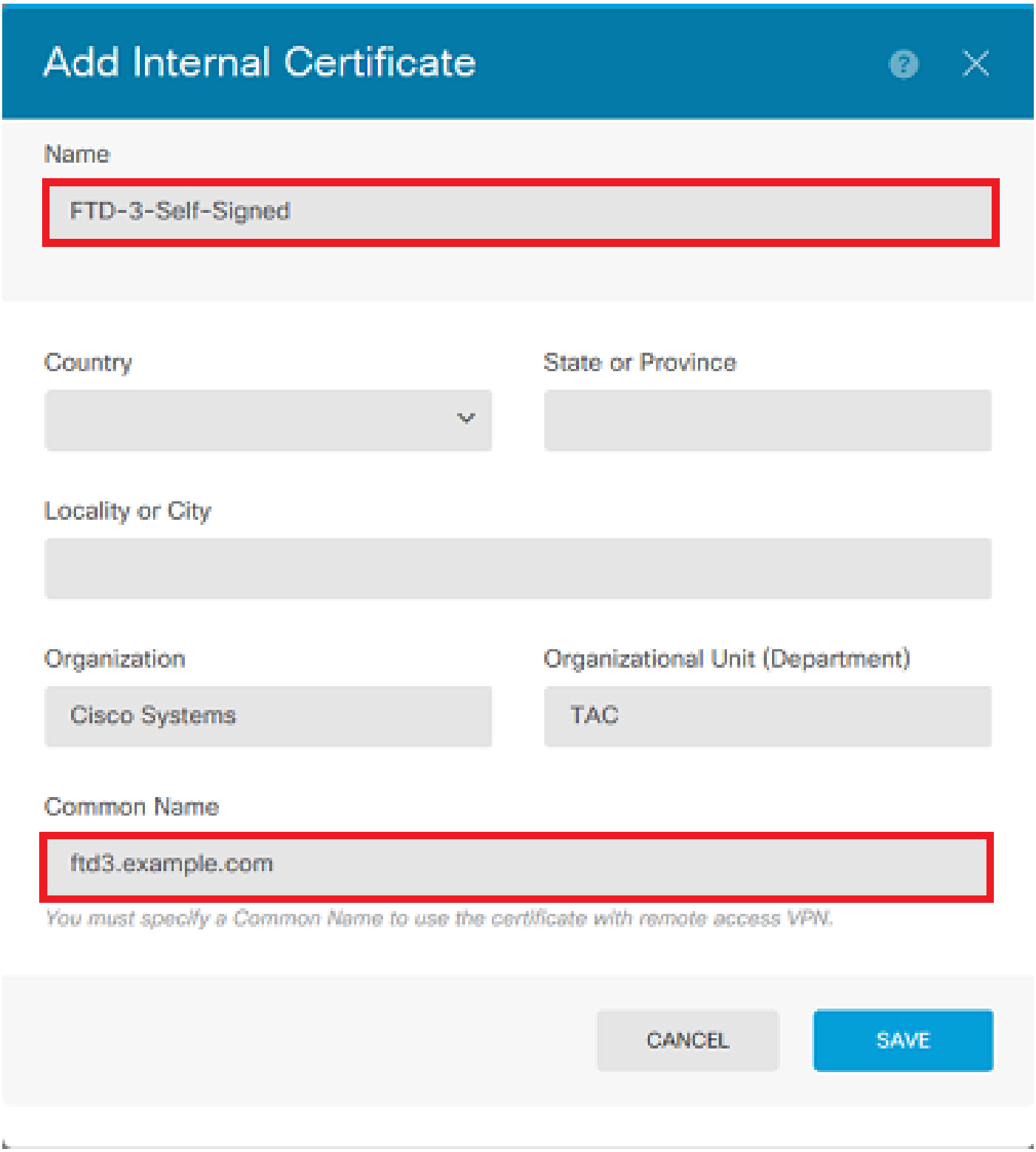
1. Accédez à Objets > Certificats. Cliquez sur le symbole +, puis choisissez Add Internal Certificate comme illustré dans l'image.



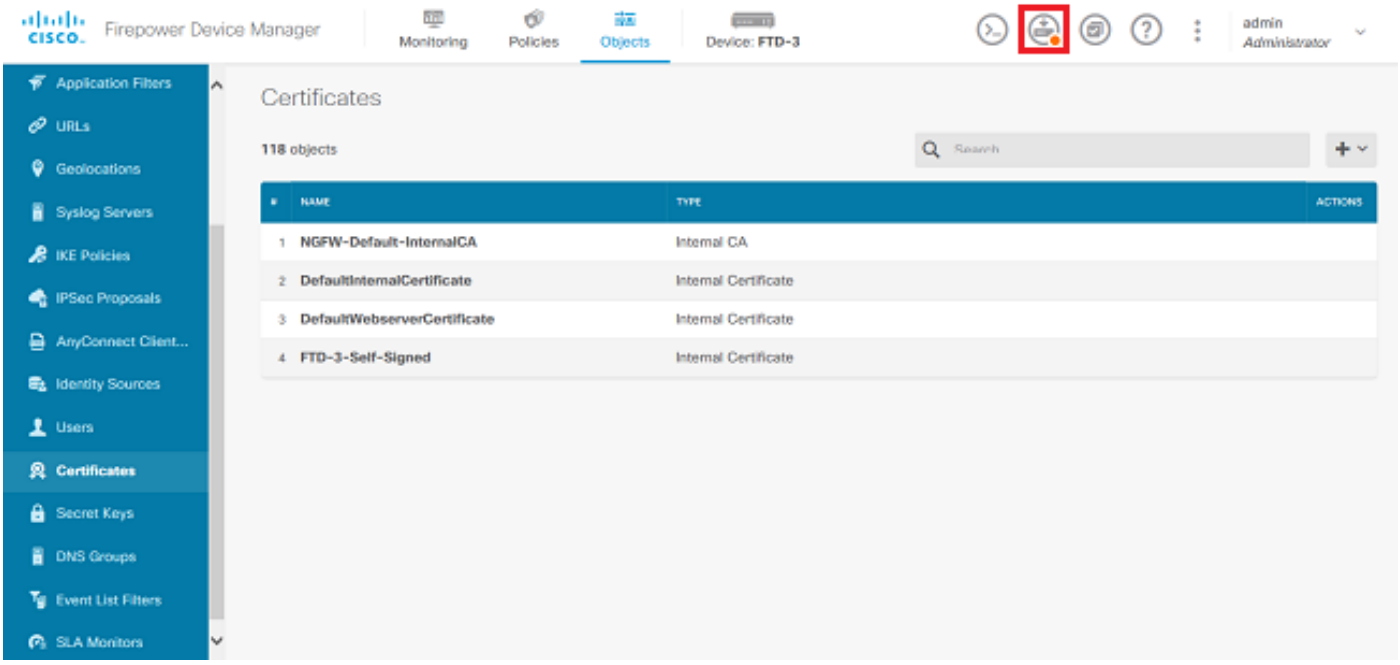
2. Choisissez Certificat auto-signé dans la fenêtre contextuelle comme indiqué dans l'image.



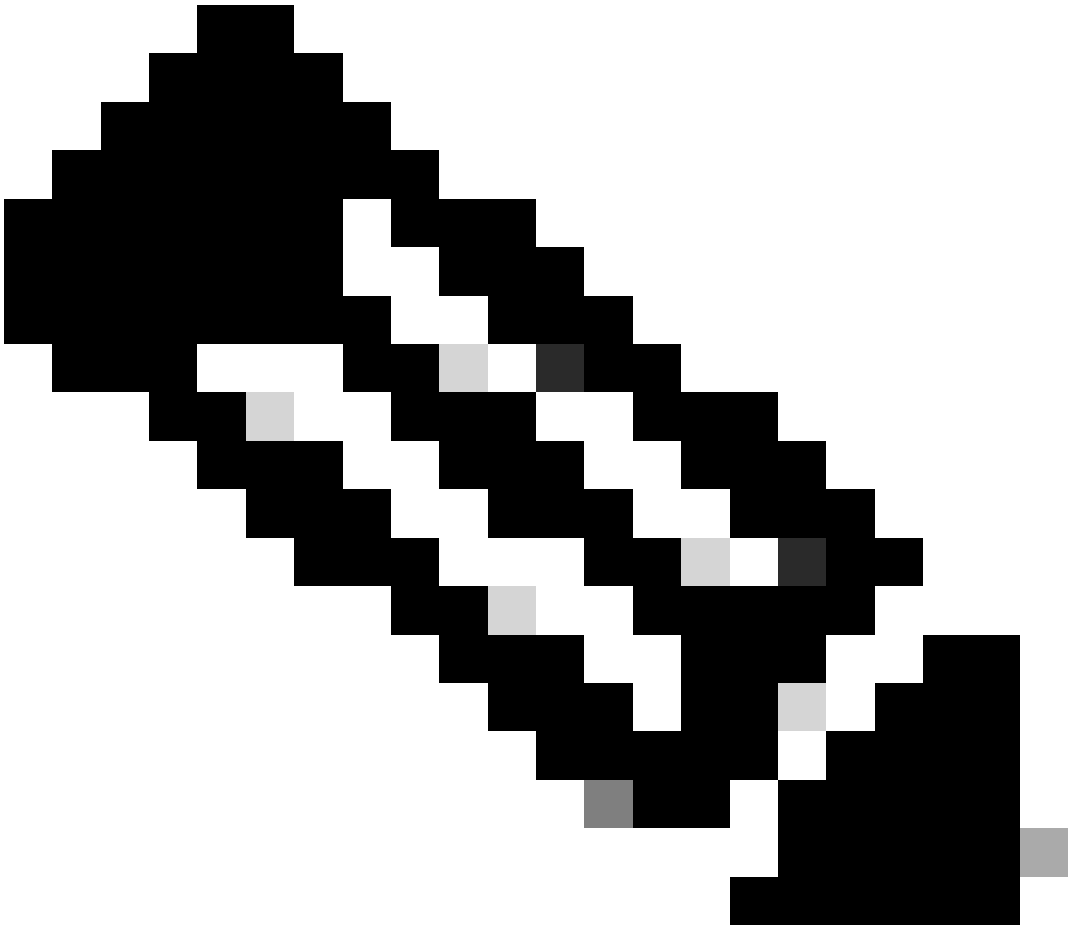
3. Spécifiez un nom pour le point de confiance, puis renseignez les champs de nom distinctif de l'objet. Au minimum, le champ Nom commun peut être ajouté. Cela peut correspondre au nom de domaine complet (FQDN) ou à l'adresse IP du service pour lequel le certificat est utilisé. Cliquez sur Save lorsque vous avez terminé comme indiqué dans l'image.



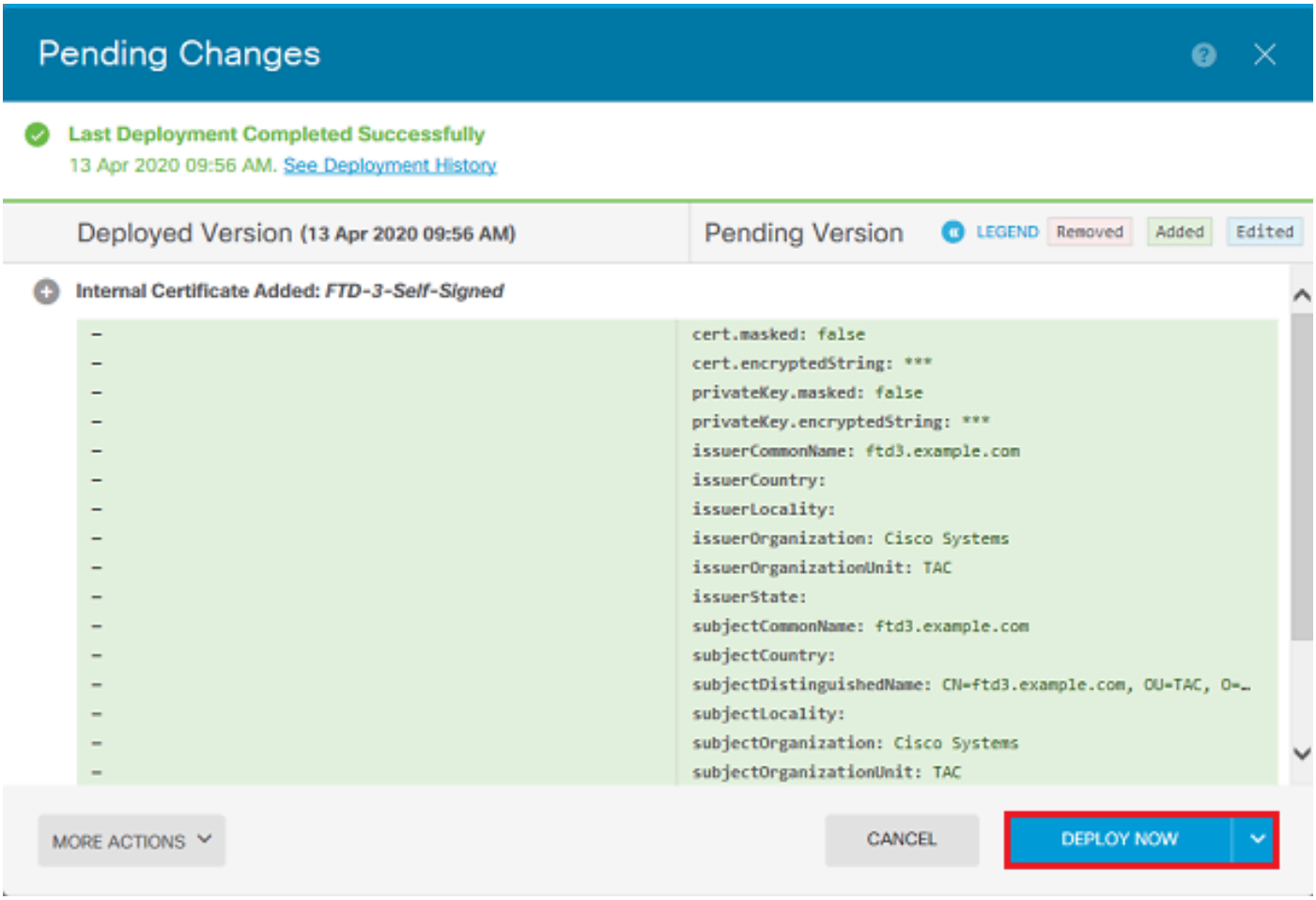
4. Cliquez sur le bouton Modifications en attente en haut à droite de l'écran, comme illustré dans l'image.



5. Cliquez sur le bouton Déployer maintenant.



Remarque : une fois le déploiement terminé, le certificat n'est pas visible dans l'interface de ligne de commande tant qu'un service ne l'utilise pas, tel qu'AnyConnect, comme illustré dans l'image.



Inscription manuelle

L'inscription manuelle peut être utilisée pour installer un certificat émis par une autorité de certification approuvée. OpenSSL ou un outil similaire peut être utilisé pour générer la clé privée et le CSR requis pour recevoir un certificat signé par une autorité de certification. Ces étapes couvrent les commandes OpenSSL courantes afin de générer la clé privée et CSR ainsi que les étapes pour installer le certificat et la clé privée une fois obtenus.

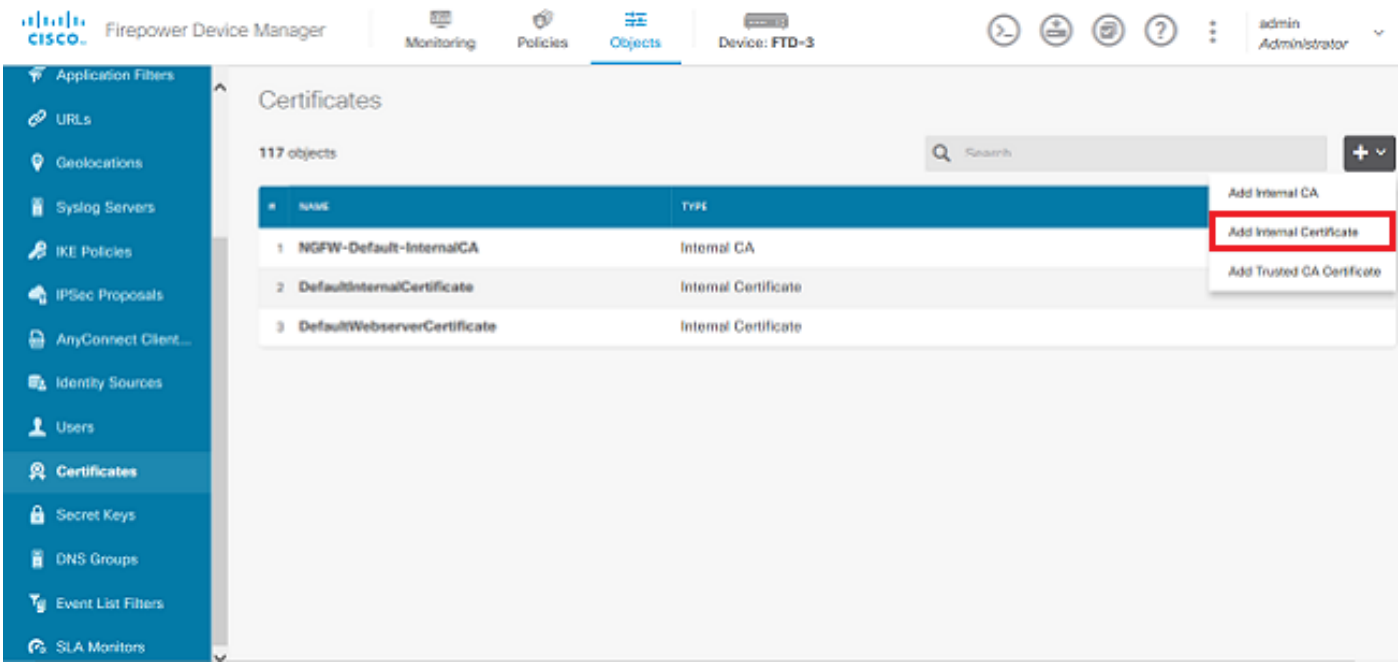
1. Avec OpenSSL ou une application similaire, générez une clé privée et une demande de signature de certificat (CSR). Cet exemple montre une clé RSA de 2048 bits nommée private.key et un CSR nommé ftd3.csr qui est créé dans OpenSSL.

```
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'
-----
```

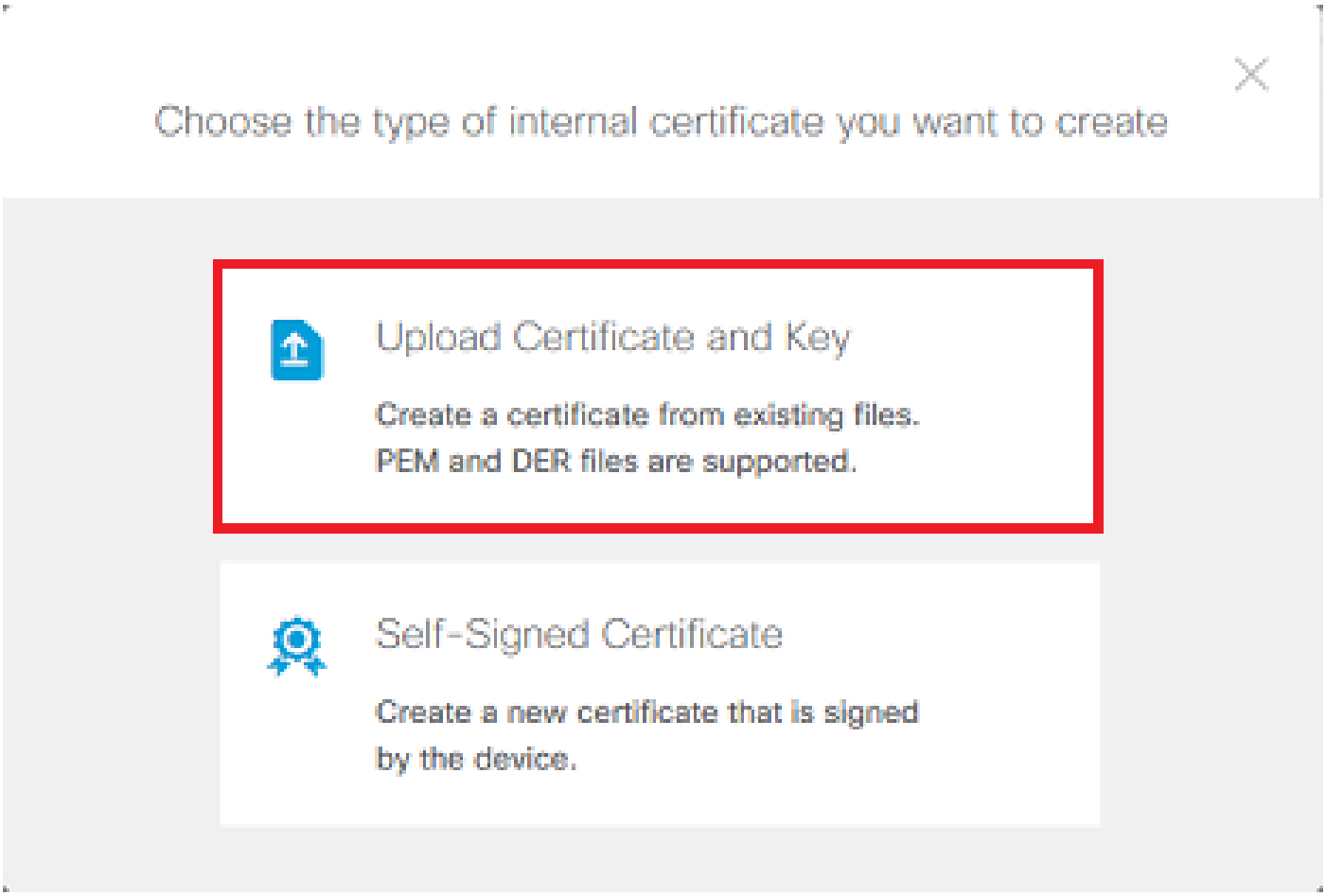
```
You are about to be asked to enter information that is incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', the 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. Copiez le CSR généré et envoyez-le à une autorité de certification. Une fois le CSR signé, un certificat d'identité est fourni.

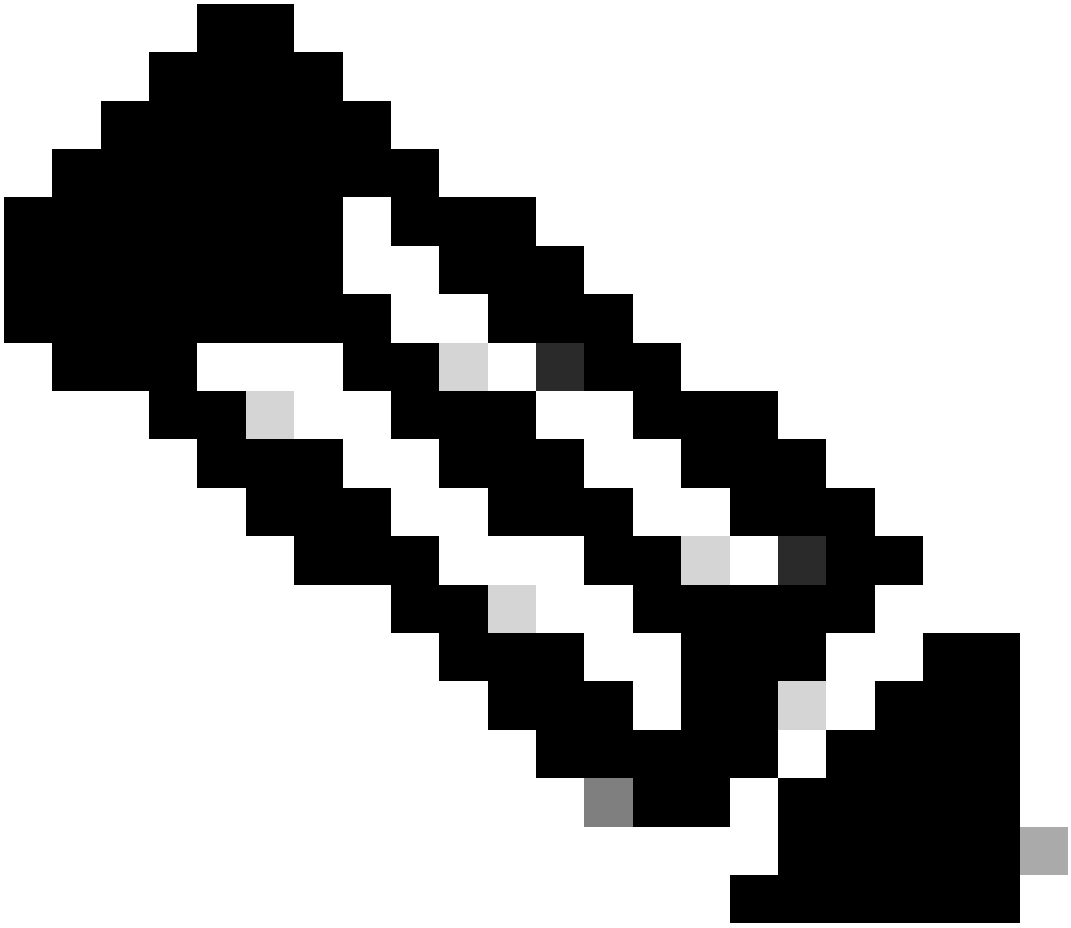
3. Accédez à Objets > Certificats. Cliquez sur le symbole +, puis choisissez Add Internal Certificate comme illustré dans l'image.



4. Choisissez Upload Certificate and Key dans la fenêtre contextuelle, comme indiqué dans l'image.

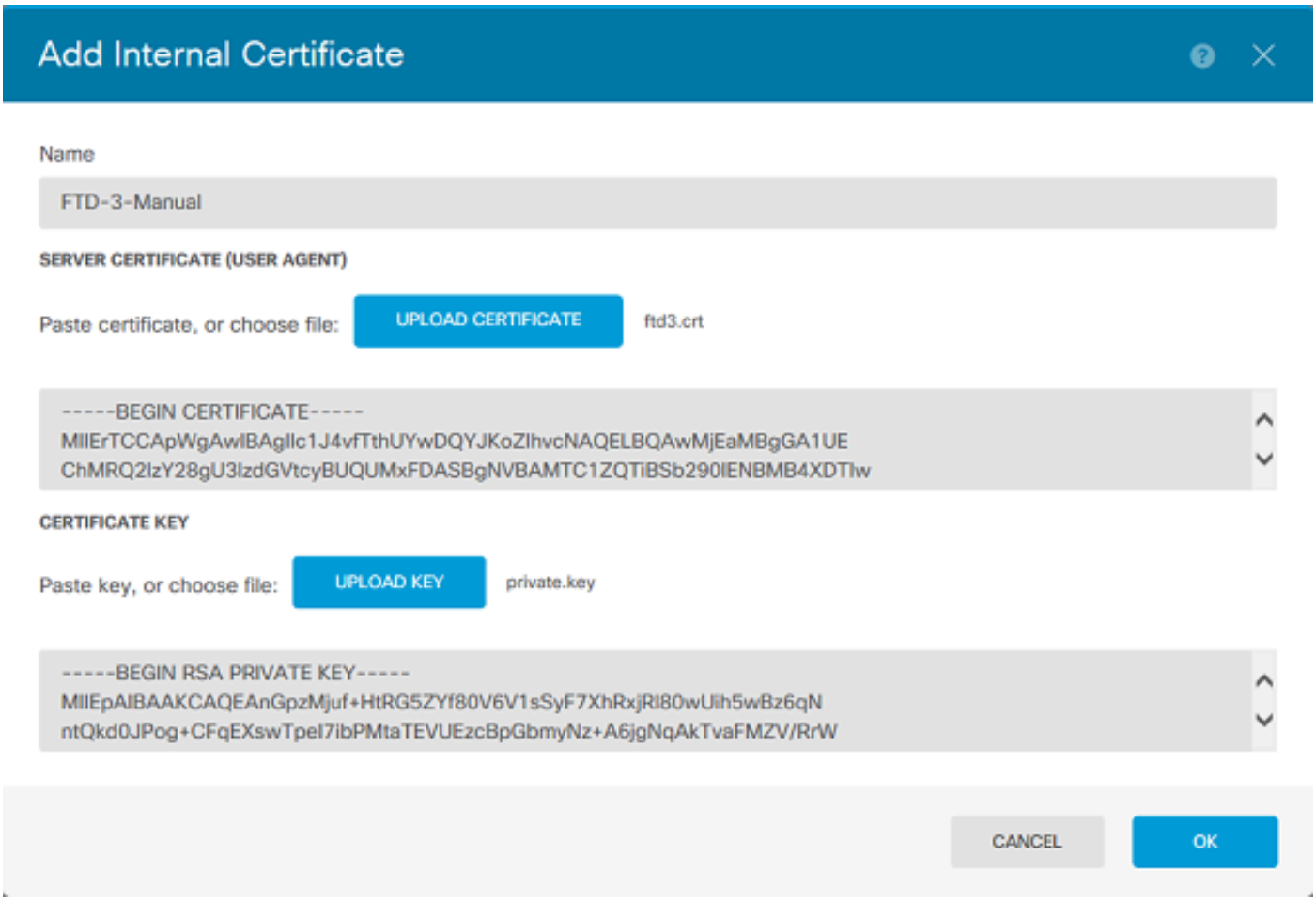


5. Spécifiez un nom pour le point de confiance, puis téléchargez, ou copiez et collez le certificat d'identité et la clé privée au format PEM (Privacy Enhanced Mail). Si l'autorité de certification a fourni le certificat et la clé ensemble dans un seul PKCS12, accédez à la section intitulée Extraction du certificat d'identité et de la clé privée à partir du fichier PKCS12 plus loin dans ce document afin de les séparer.

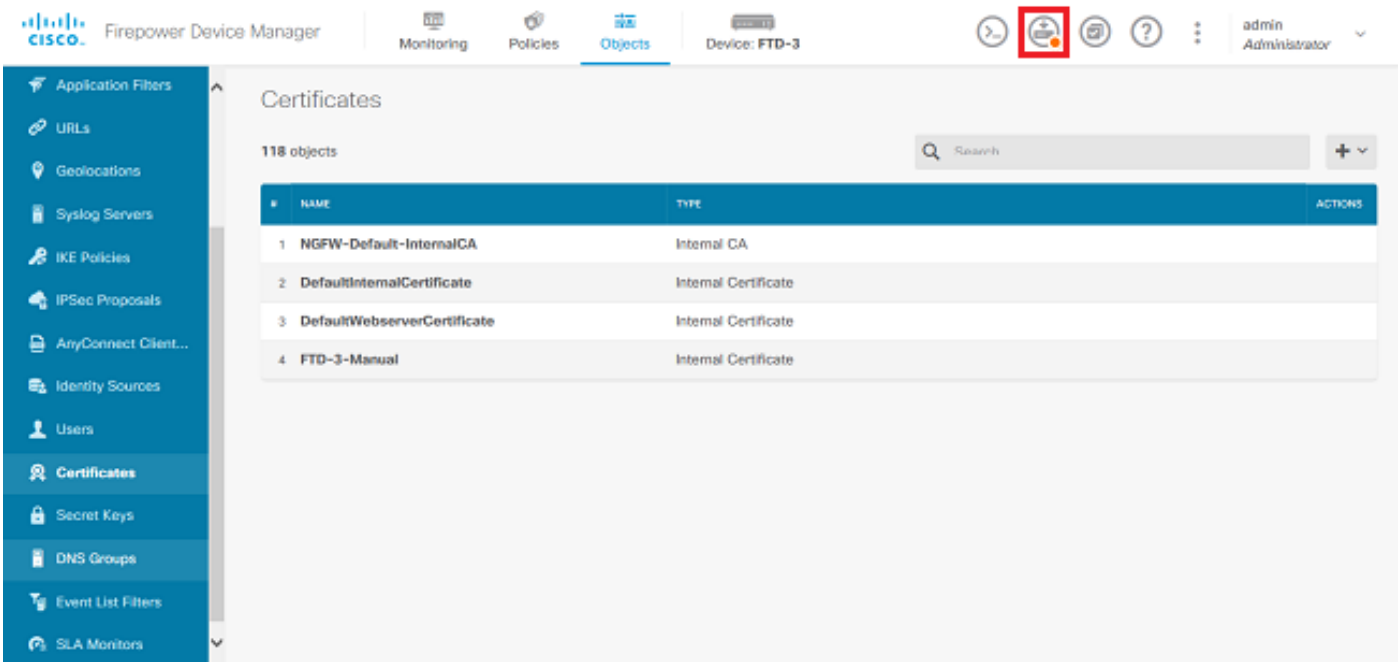


Remarque : les noms de fichiers ne peuvent pas contenir d'espaces ou FDM ne les accepte pas. En outre, la clé privée ne doit pas être chiffrée.

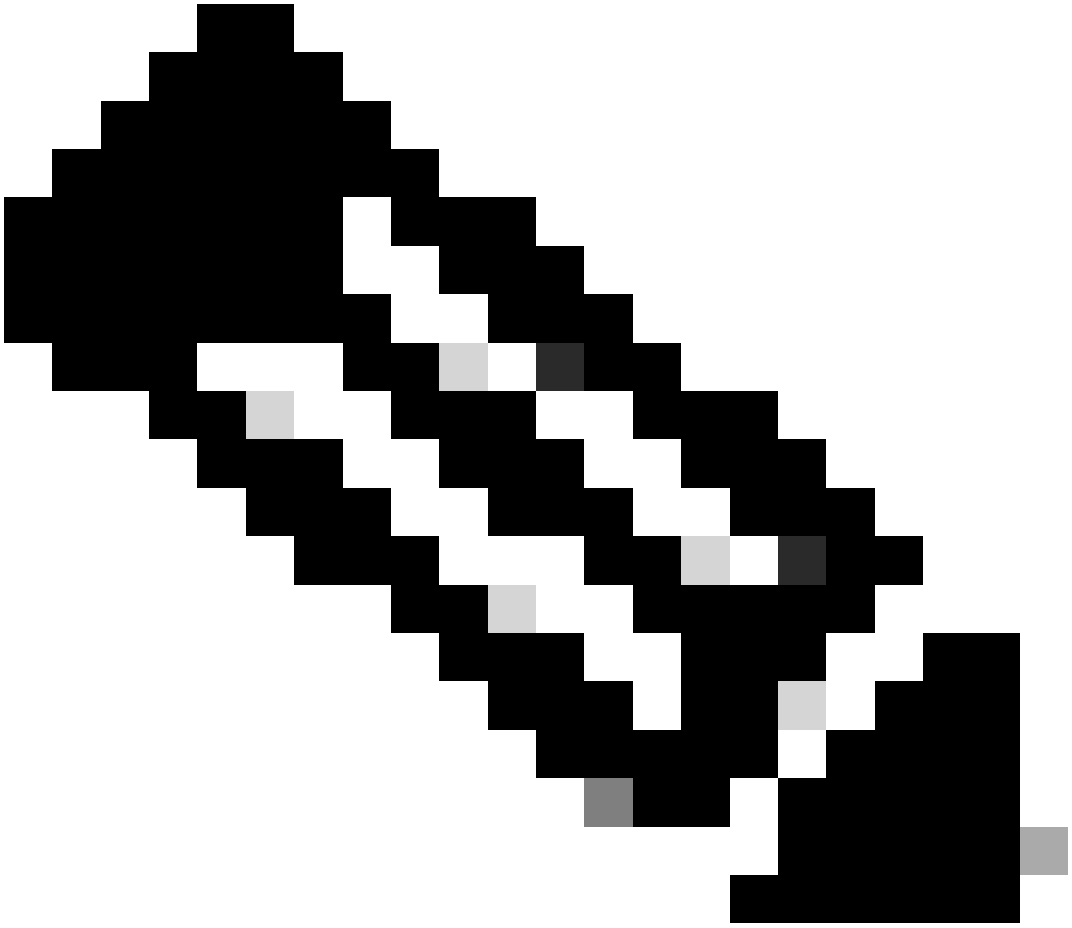
Cliquez sur OK lorsque vous avez terminé, comme illustré dans l'image.



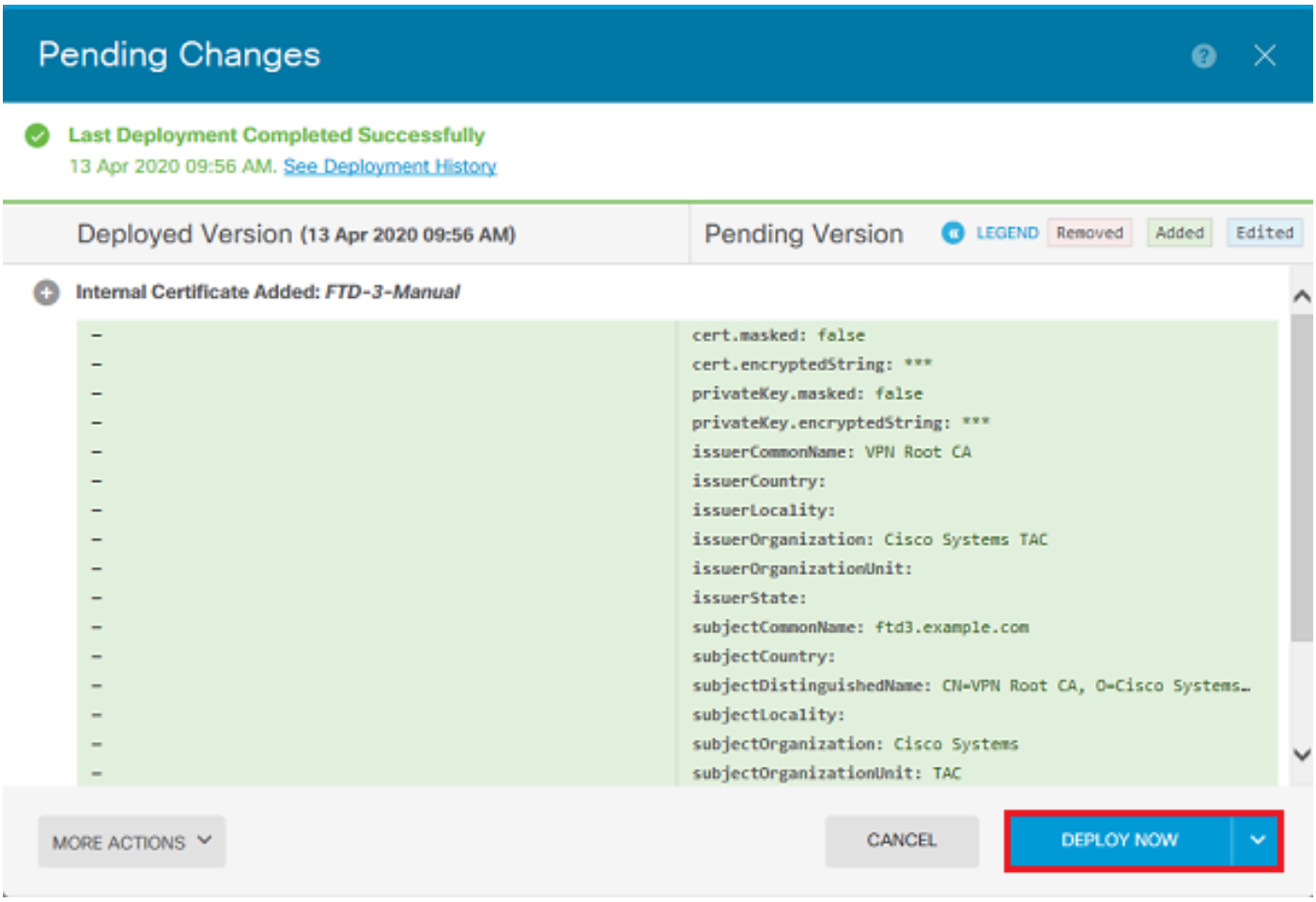
6. Cliquez sur le bouton Modifications en attente en haut à droite de l'écran, comme illustré dans l'image.



7. Cliquez sur le bouton Déployer maintenant.



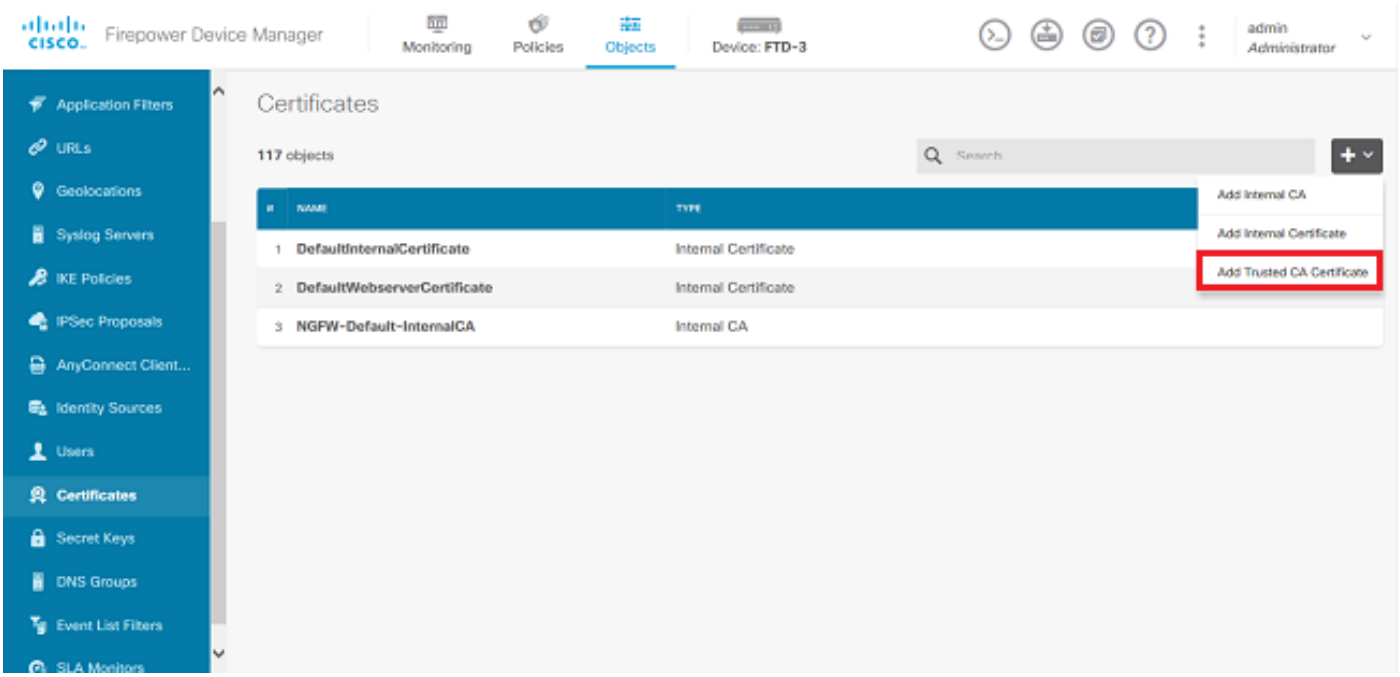
Remarque : une fois le déploiement terminé, le certificat n'est pas visible dans l'interface de ligne de commande tant qu'un service ne l'utilise pas, tel qu'AnyConnect, comme illustré dans l'image.



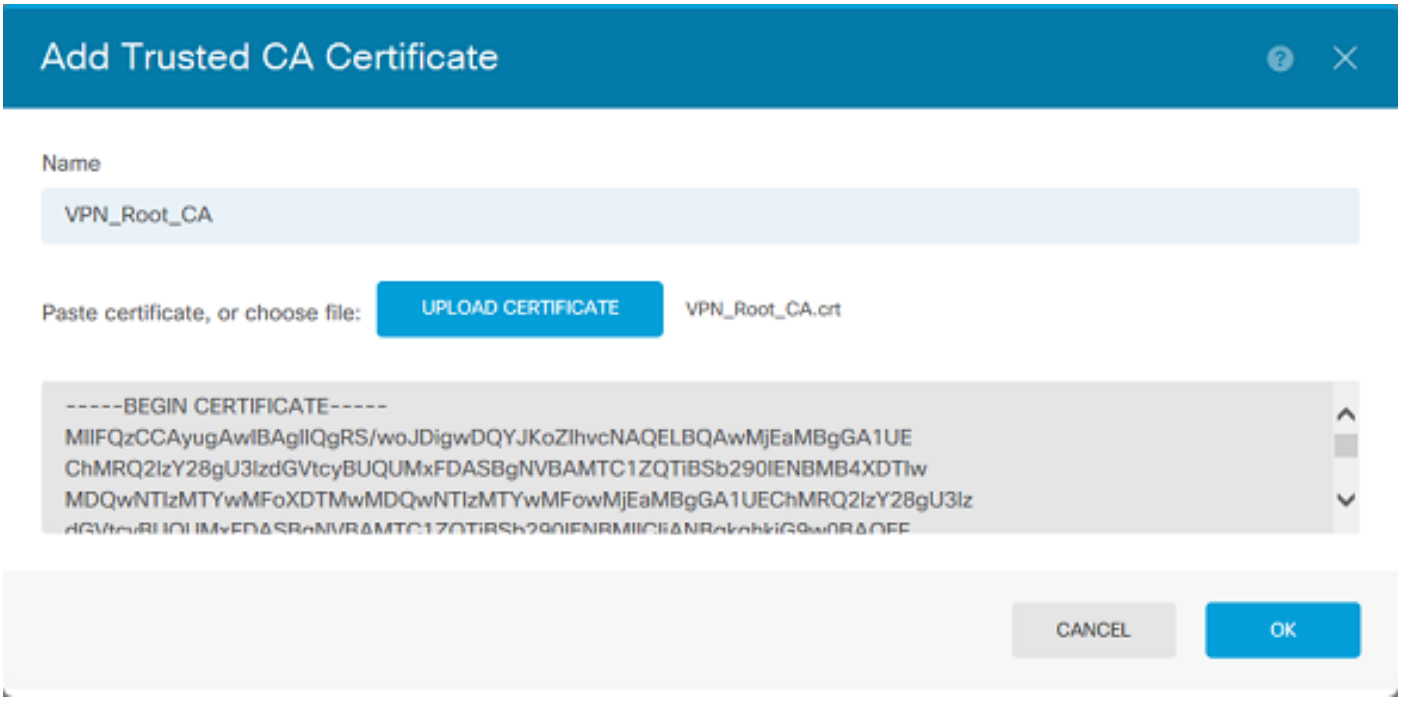
Installation du certificat CA approuvé

Lorsque vous installez un certificat CA approuvé, il est nécessaire, afin d'authentifier avec succès les utilisateurs ou les périphériques qui présentent des certificats d'identité au FTD. L'authentification de certificat AnyConnect et l'authentification de certificat VPN S2S en sont des exemples courants. Ces étapes décrivent comment faire confiance à un certificat d'autorité de certification afin que les certificats émis par cette autorité de certification soient également approuvés.

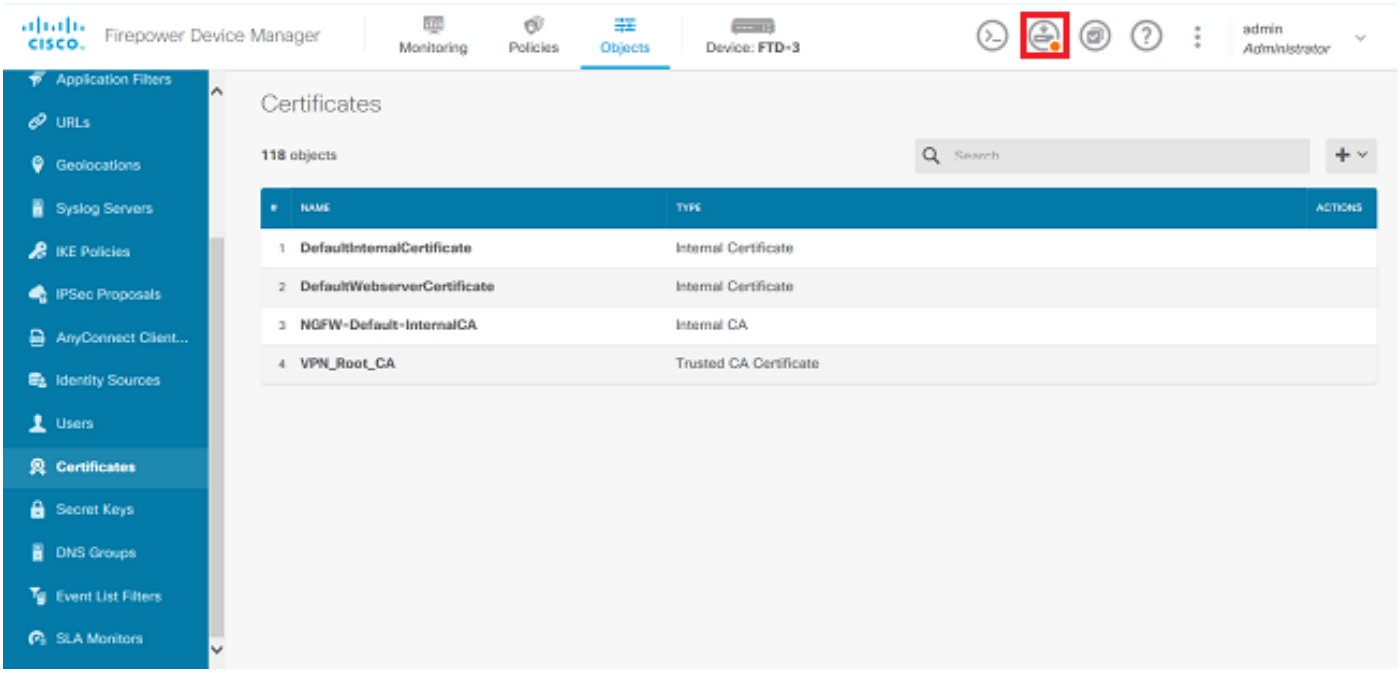
1. Accédez à Objets > Certificats. Cliquez sur le symbole +, puis choisissez Add Trusted CA Certificate comme indiqué dans l'image.



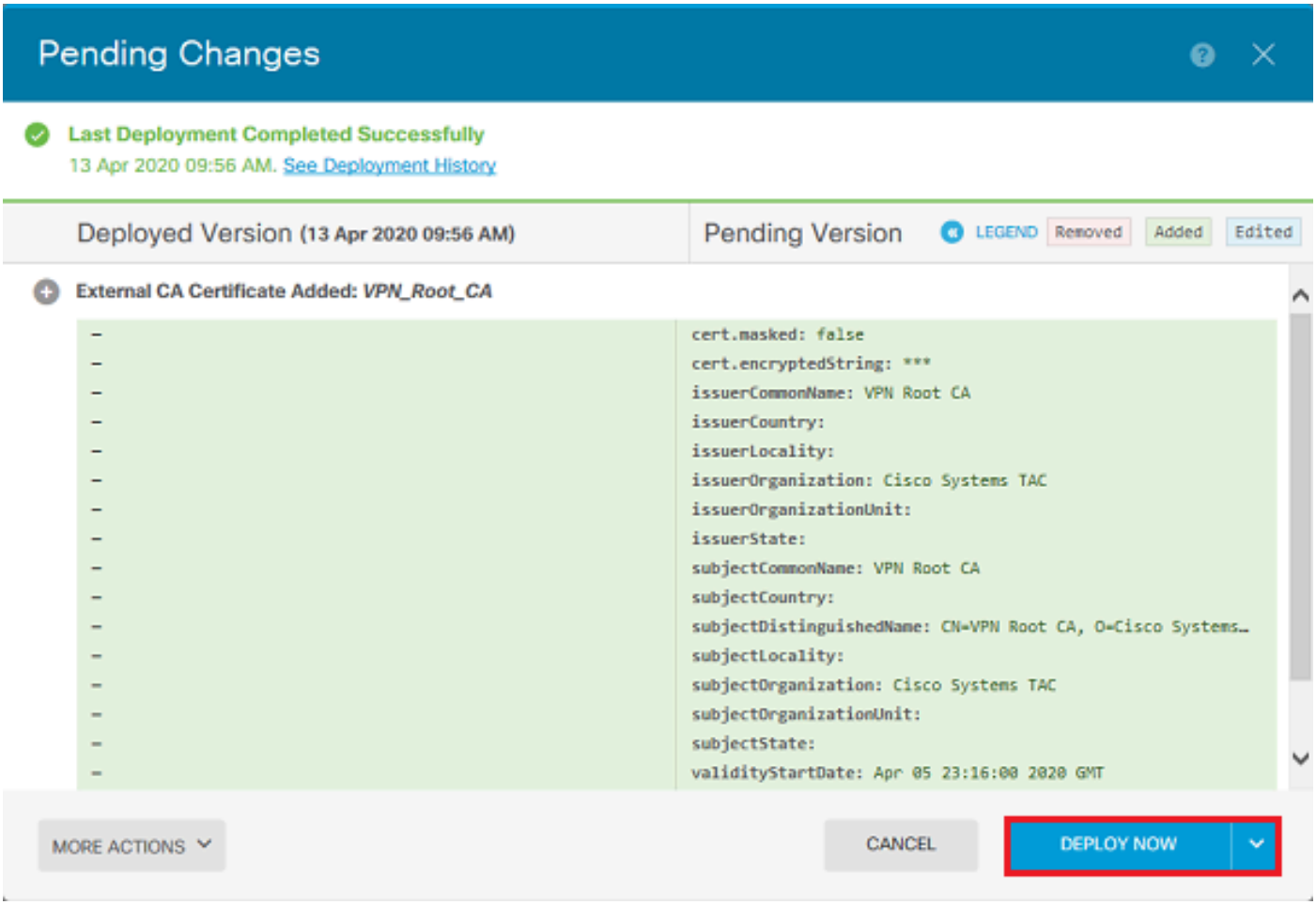
2. Spécifiez un nom pour le point de confiance. Ensuite, téléchargez ou copiez et collez le certificat CA au format PEM. Cliquez sur OK lorsque vous avez terminé, comme illustré dans l'image.



3. Cliquez sur le bouton Modifications en attente en haut à droite de l'écran, comme illustré dans l'image.



4. Cliquez sur le bouton Déployer maintenant comme illustré dans l'image.



Renouvellement du certificat

Le renouvellement de certificat sur un FTD géré par FDM implique le remplacement du certificat précédent et potentiellement de la clé privée. Si vous ne disposez pas de la clé CSR et privée

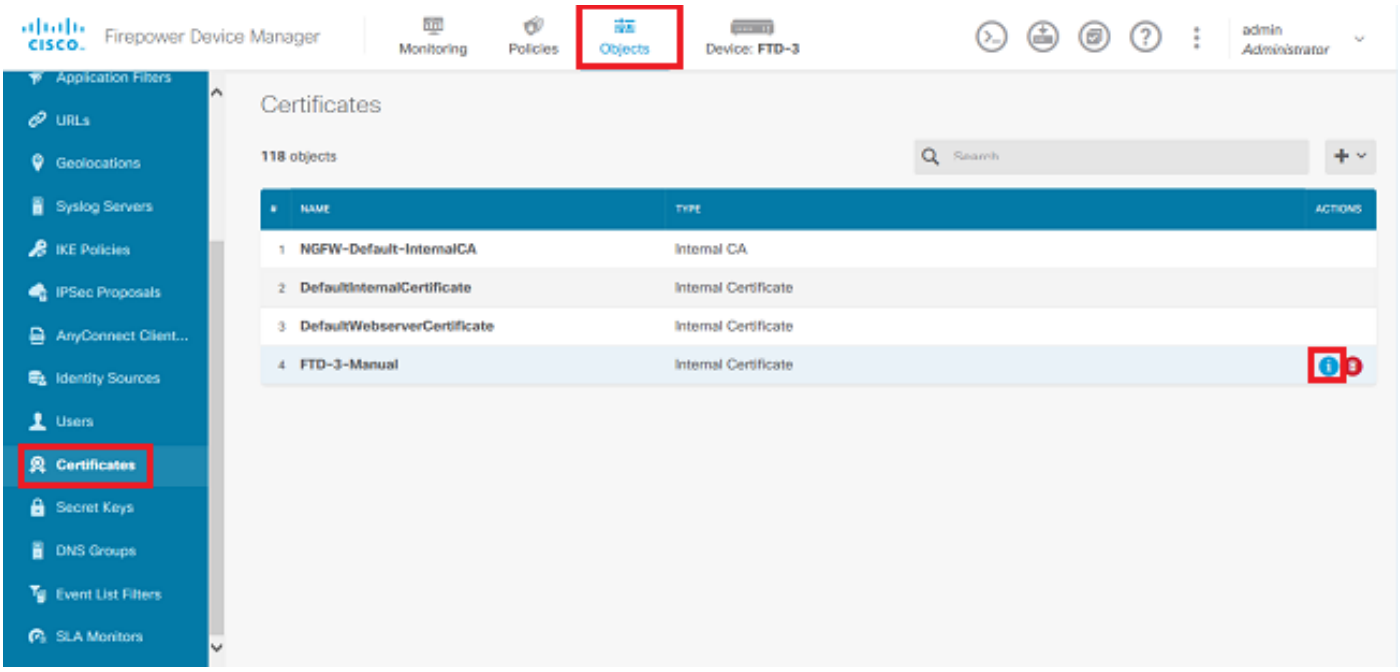
d'origine utilisée pour créer le certificat d'origine, vous devez créer une nouvelle clé CSR et privée.

1. Si vous disposez du CSR et de la clé privée d'origine, cette étape peut être ignorée. Sinon, une nouvelle clé privée et une nouvelle CSR doivent être créées. Utilisez OpenSSL, ou une application similaire, pour générer une clé privée et un CSR. Cet exemple montre une clé RSA de 2048 bits nommée private.key et un CSR nommé ftd3.csr qui est créé dans OpenSSL.

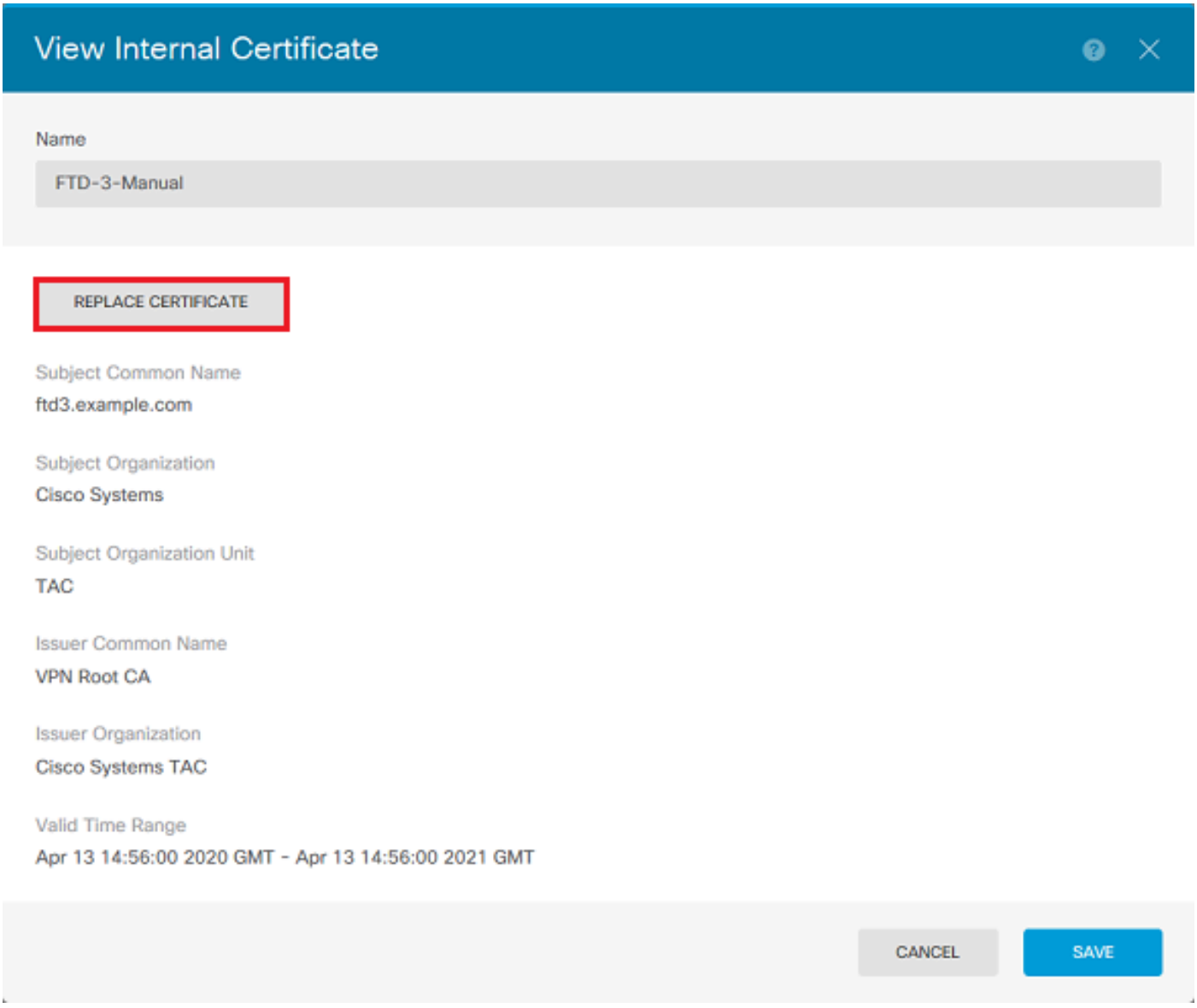
```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
.....................................+++
.....................................................................+++
writing new private key to 'private.key'
-----
You are about to be asked 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. Envoyez le CSR généré ou le CSR d’origine à une autorité de certification. Une fois le CSR signé, un certificat d'identité renouvelé est fourni.

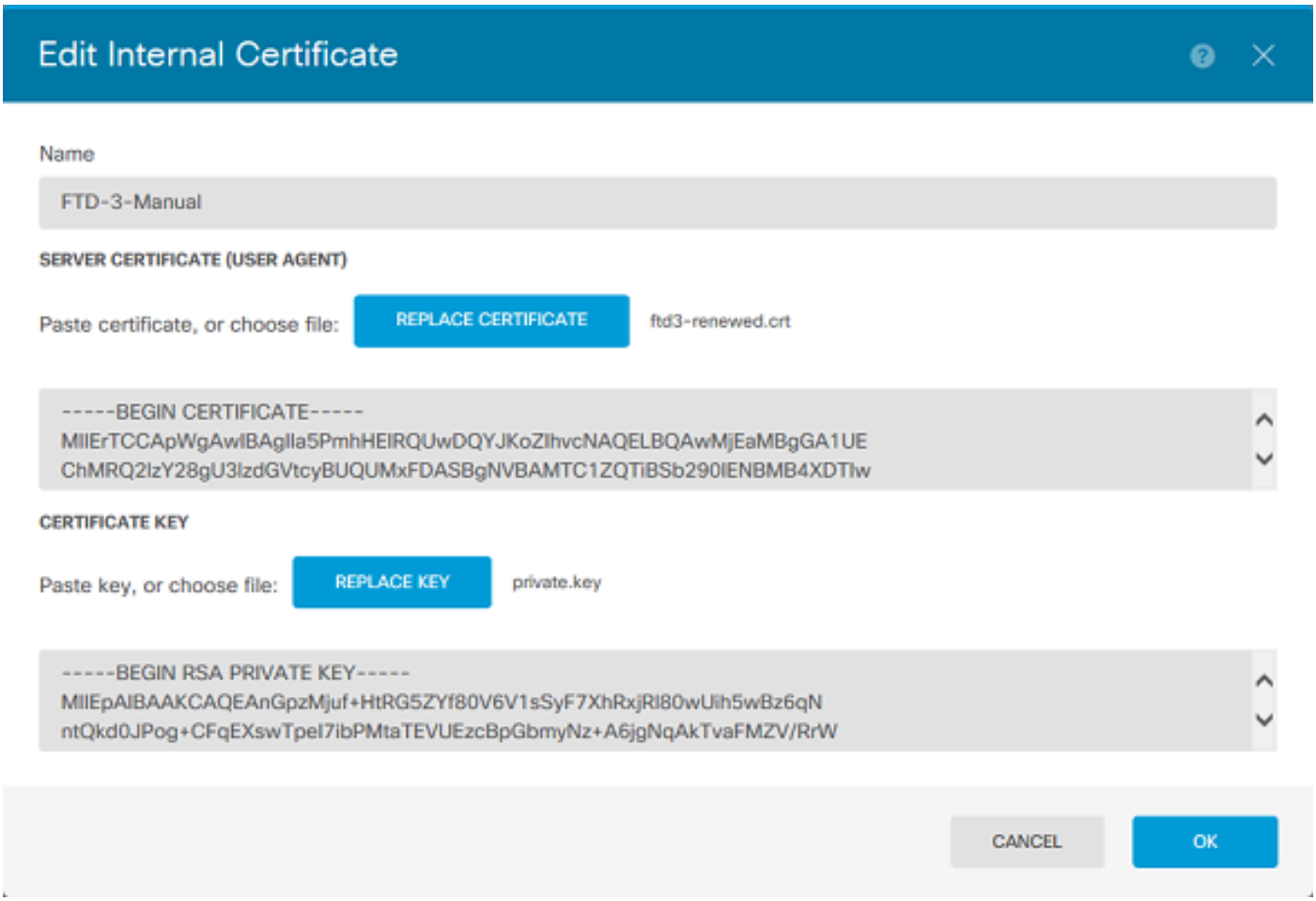
3. Accédez à Objets > Certificats. Passez le curseur sur le certificat que vous voulez renouveler, et cliquez sur le bouton View comme indiqué dans l'image.



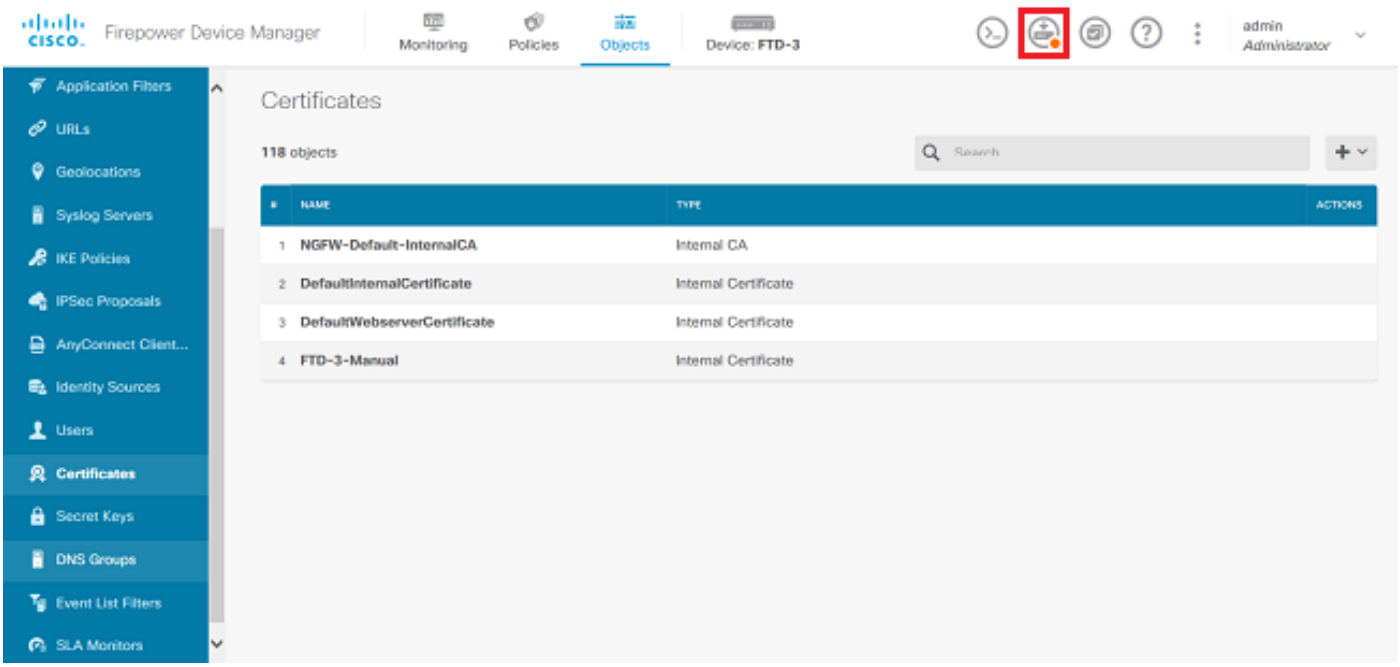
4. Dans la fenêtre contextuelle, cliquez sur Remplacer le certificat comme indiqué dans l'image.



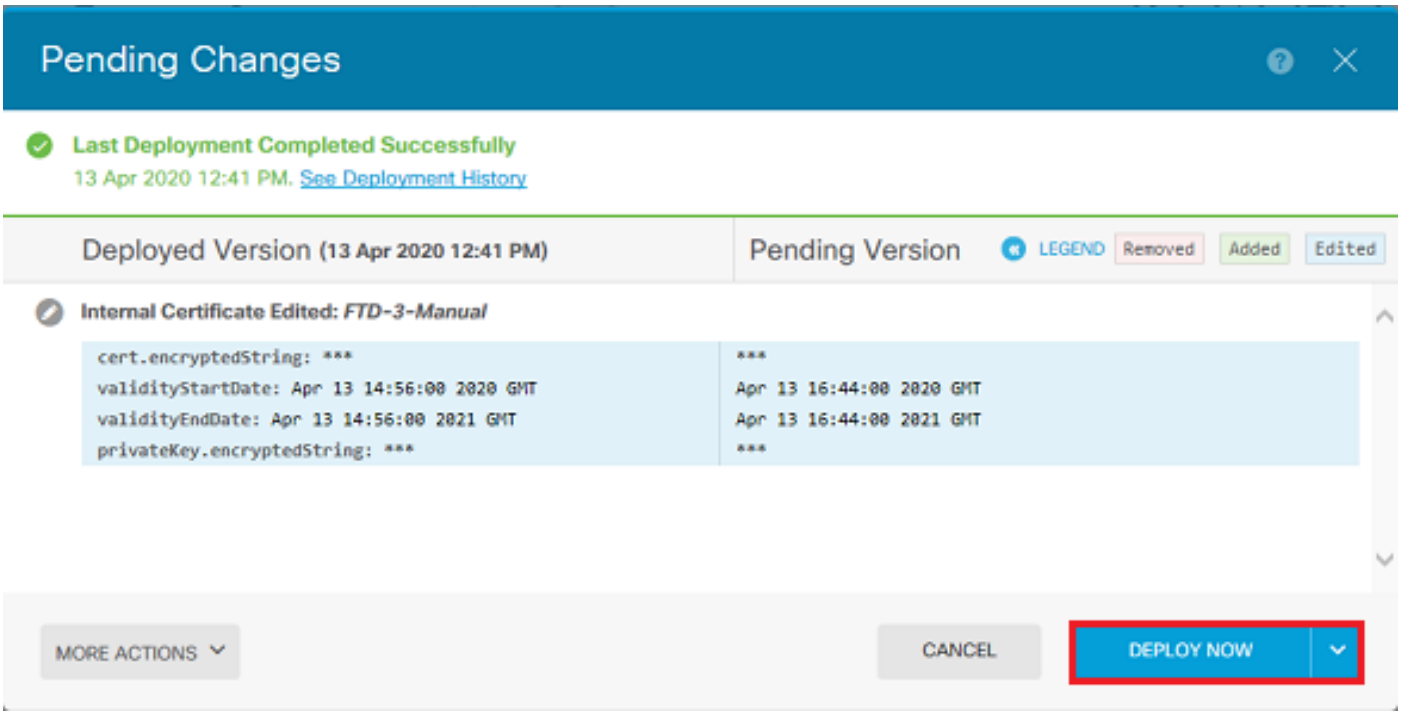
5. Téléchargez ou copiez et collez le certificat d'identité et la clé privée au format PEM. Cliquez sur OK lorsque vous avez terminé, comme illustré dans l'image.



6. Cliquez sur le bouton Modifications en attente en haut à droite de l'écran, comme illustré dans l'image.



7. Cliquez sur le bouton Déployer maintenant comme illustré dans l'image.



Opérations OpenSSL courantes

Extraire le certificat d'identité et la clé privée du fichier PKCS12

Un administrateur peut recevoir un fichier PKCS12 qui doit être importé sur le FTD. FDM ne prend actuellement pas en charge l'importation de fichiers PKCS12. Afin d'importer les certificats et la clé privée contenus dans le fichier PKCS12, les fichiers individuels doivent être extraits de PKCS12 à l'aide d'un outil tel qu'OpenSSL. Vous avez besoin du code secret utilisé pour chiffrer le 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
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
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
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-----
```

pkcs12file.pfx est un fichier PKCS12 qui doit être décompressé.

Dans cet exemple, trois fichiers distincts sont créés :

Une pour le certificat d'identité. Vous pouvez voir qu'il s'agit du certificat d'identité dû à subject=/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-----
```

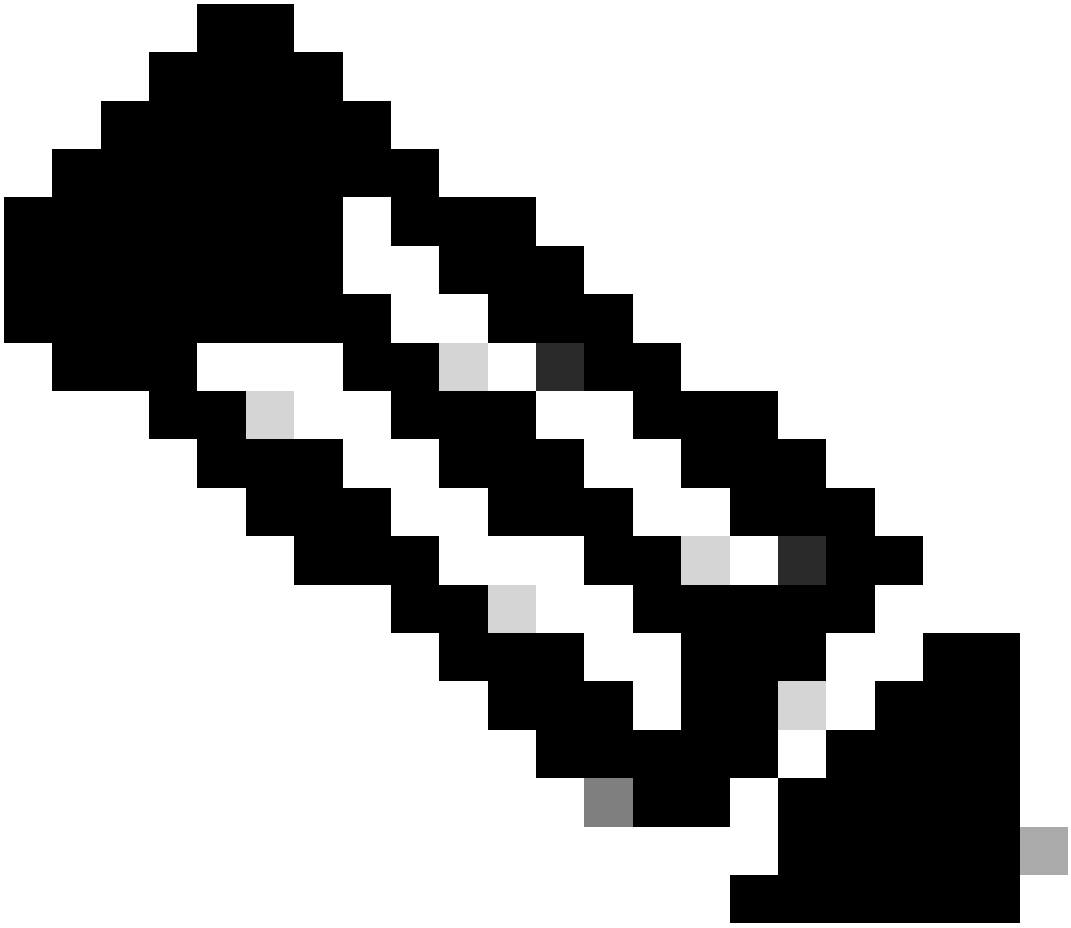
Une pour le certificat CA émetteur. Vous pouvez dire qu'il s'agit du certificat d'identité dû à l'autorité de certification racine subject=/O=Cisco Systems TAC/CN=VPN. Il s'agit de la même valeur que l'émetteur dans le certificat d'identité qui est vu précédemment :

```
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-----
```

Et un pour la clé privée :

```
-----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-----
```



Remarque : la clé privée est chiffrée et FDM n'accepte pas les clés privées chiffrées.

Afin de déchiffrer la clé privée, copiez la clé privée chiffrée dans un fichier, puis exécutez cette commande openssl :

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

- encryption.key est le nom du fichier qui contient la clé privée chiffrée.
- unencryption.key est le nom du fichier qui a la clé non chiffrée.

La clé privée non chiffrée peut afficher -----BEGIN RSA PRIVATE KEY----- au lieu de -----BEGIN ENCRYPTED PRIVATE KEY----- comme indiqué dans cet exemple :

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnGpzMjuf+HtRG5ZYf8OV6V1sSyF7XhRxjRl8OwUih5wBz6qN
ntQkdOJPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGbmyNz+A6jgNqAkTvaFMZV/RrW
qCNktO8ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqNBqotoz3/8CrZOIcpzVqL6hOz
iJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS5OQpQDTgvIiD1bYpPiWKpSOg1P
ZDnX8b74Os0pVKVXTsujQqSqH1va9BB6hK1JCoZaHrP9YOxO9+MpVMH33R9vRl3S
OEF6kpZ6VEdGI4s6/IRvaM1zlBcK1ON/N2+mjwIDAQABAoIBAEQzCd1KMBrosdmk
eRvoMPiaemBbze2cXlJWXZ2orICSXhvMOokBGJFDQXN47ZCuVqYAqOecjU9RzGgE
NbXYfUsD6+P91k+/Gj1RiCNLBHBwdgewzw1quTxP54zSpAVlIXyQ+FolTzjH1yfW
7iHhuSujYsAYLWPy4Yg3NpU2IdzeQoK5ViuSTTNx8LHYBKw1Qf7HVaQTfmsWOAyg
/vjZqjRkukqKM41srgkO/HjPnEBDuUWVTehzMCk1etijENc7ttISzYIEMNPthe6O
NpidXAHoJ1lJM6HB9ZraBH5fu7MZJZOOn6YVKQuCdWOWfnKiNQCDsXq7X5EWsaj3
cgyjWlkCgYEAy33k1wxp7WEqg1zEwqOVq7AtoL6i4V9QCenMThQAHwNAAUGGOSIF
JhpKyApm/BUogSIOMzIPse+NgAA66TRn4qfkbpvTI98CeCUxiUPcbRmqZnYxCOfp
Pzosv5OnBLltoIOprIO2S5a261w6JGNAfD95tCjCYYrB8Cw/HbZOLPUCgYEAxMbZ
KVyosBxaAIFQinHaff3fVSTsEOZFpLCBbLybgLcP8LsLdahBsj6HK/hAffKXOdvM
35CAM7ZL/WCI1Jb+dx4YcD9q8lbVMu4HTvSl2deTZoZrBG2iFX6OSsn2rLKAH+cH
uLSHCNAj9cj9syldZErGLZtBQpJPtpLRd6iyOvMCgYBP/zoLYJHOBBLWeY3QioLO
cABABTG7L+EjRIpQ14QErR5oX/4IT9t+Uy+63HwH9blqqpyye6e359jUzUJbk4KT
lDU1VoT2wSETYmvK7qalLUXT6fr12FtVw+T7m2w5azwxshDuBQmRRbq7ZBJnY61i
KwIJVUy1U/tSE9LsN1McUQKBgQClc4ykeoRbj3sdcZ2GyrQru4pMzP6wNu3Xy5EH
HI6ja0i74ImCJDcY5/o/vjx7qb39qBJa5+TjliPOp5xlI5BSF7v0pV4G5XvdlsYO
XSYWRGxriBnzXzspV3/M4oPGMVAJgve7Fg9OGY4i2xx1yBH+geCf+CqnDt53ZHs7
YVz6gQKBgQDG42tZZ1kNAnOx/k1lUlZrEeF8iqdsyVcRf4fAvqsPbY3+kdae+8Or
+cQpVoeWzOQLUkA6eMsiTLmcWYb62qMgdpluyKoOciPG9+2AGNTvQp/ig34pF2F/
9OGuVYlA1p7mkP8Vb1Mo1ugVOzUqAIjHKiGUzBWVsxOZsGa+SY47uw==
-----END RSA PRIVATE KEY-----
```

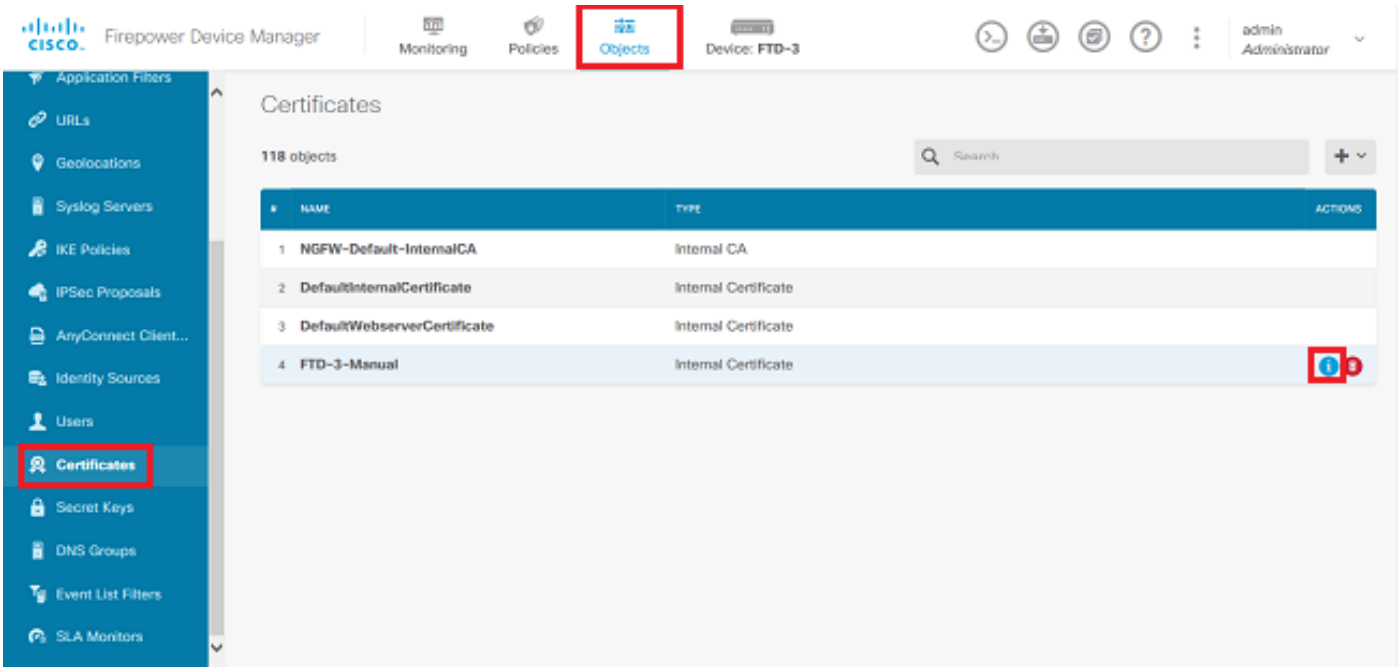
Une fois la clé privée déchiffrée, le fichier d'identité et de clé privée peut être téléchargé, ou copié et collé dans FDM à l'étape 3 de la section Inscription manuelle mentionnée précédemment. L'autorité de certification émettrice peut être installée en suivant les étapes d'installation du certificat d'autorité de certification approuvée mentionnées précédemment.

Vérifier

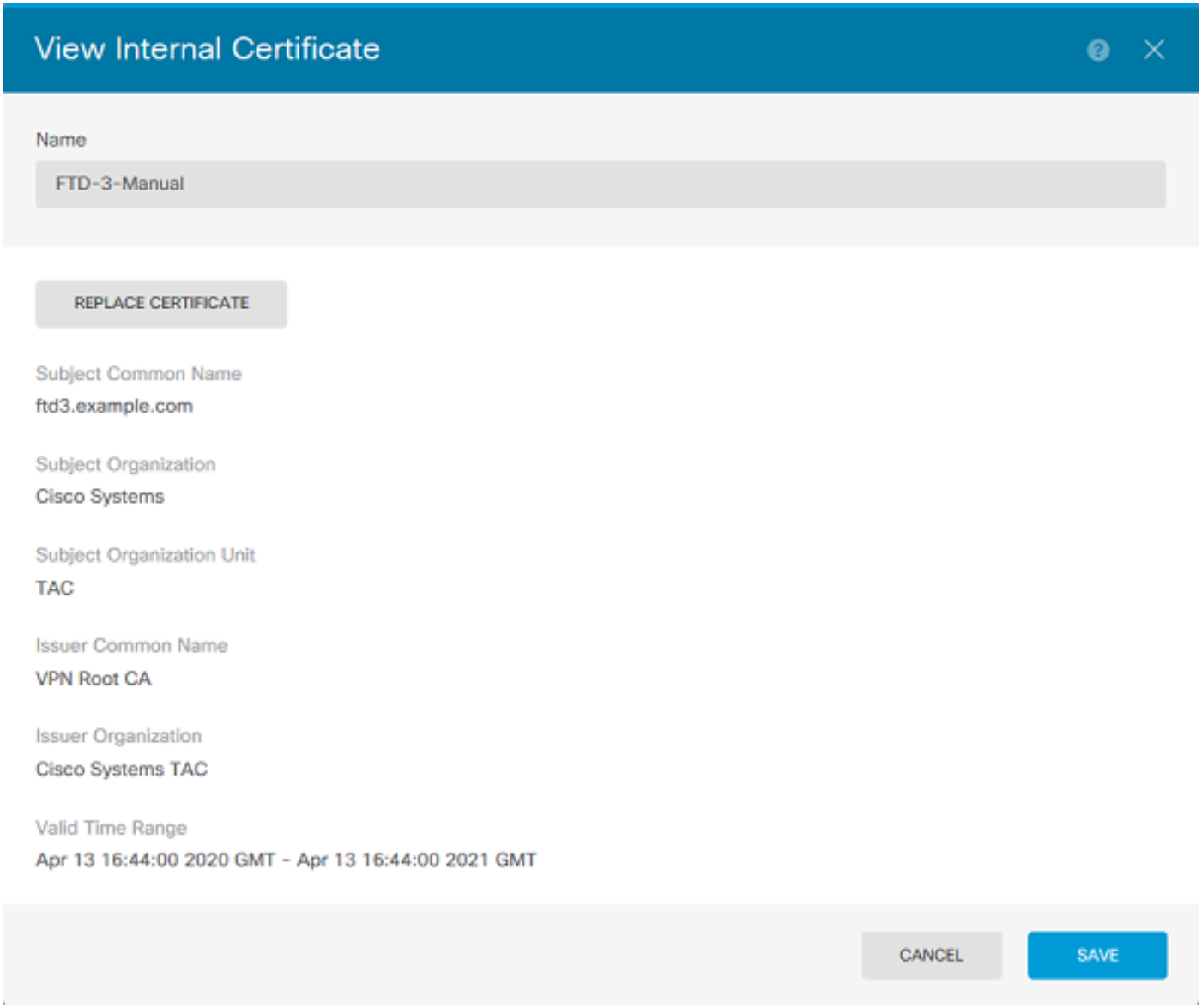
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Afficher les certificats installés dans FDM

1. Accédez à Objets > Certificats. Passez le curseur sur le certificat que vous voulez vérifier, et cliquez sur le bouton view comme montré dans l'image.



2. La fenêtre contextuelle fournit des détails supplémentaires sur le certificat, comme indiqué dans l'image.

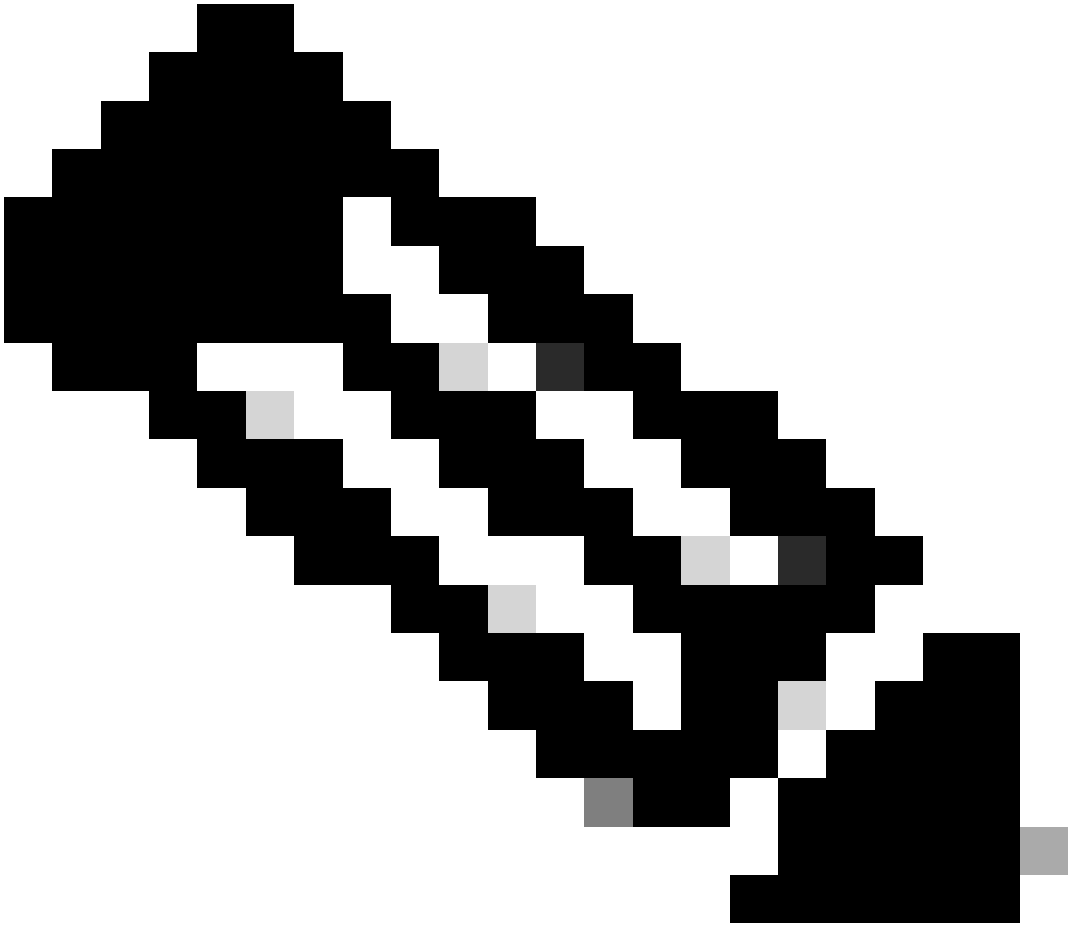


Afficher les certificats installés dans CLI

Vous pouvez utiliser la console CLI dans FDM ou SSH dans le FTD et exécuter la commande show crypto ca certificates afin de vérifier qu'un certificat est appliqué au périphérique comme indiqué dans l'image.

Exemple de rapport :

```
> 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
```



Remarque : les certificats d'identité s'affichent uniquement dans l'interface de ligne de commande lorsqu'ils sont utilisés avec un service tel qu'AnyConnect. Les certificats d’autorité de certification approuvés apparaissent une fois déployés.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Commandes de débogage

Les débogages peuvent être exécutés à partir de l'interface de ligne de commande de diagnostic après que vous ayez connecté le FTD via SSH dans le cas d'un échec d'installation de certificat SSL : debug crypto ca 14

Dans les versions antérieures de FTD, ces débogages sont disponibles et recommandés pour le dépannage :

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 25

Problèmes courants

Importer PKCS exporté par ASA12

Lorsque vous tentez d'extraire le certificat d'identité et la clé privée d'une ASA PKCS12 exportée dans OpenSSL, vous pouvez recevoir une erreur similaire à celle-ci :

```
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
```

Pour contourner ce problème, le fichier pkcs12 doit d'abord être converti au format DER :

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

Une fois cela fait, les étapes de la section Extraction du certificat d'identité et de la clé privée à partir du fichier PKCS12 plus haut dans ce document peuvent être suivies afin d'importer le certificat d'identité et la clé privée.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.