FDMで管理されるFTDでの証明書のインストールおよび更新

内容

はじめに

このドキュメントでは、FTDで自己署名証明書と、サードパーティCAまたは内部CAによって署名された証明書をインストール、信頼、および更新する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 証明書を手動で登録するには、信頼できるサードパーティの認証局(CA)にアクセスする必要があります。サードパーティCAベンダーの例としては、Entrust、Geotrust、GoDaddy、Thawte、およびVeriSignなどがありますが、これらに限定されるわけではありません。
- Firepower Threat Defense(FTD)のクロックの時刻、日付、およびタイムゾーンが正しいことを確認します。証明書認証では、ネットワークタイムプロトコル(NTP)サーバを使用してFTDの時刻を同期することをお勧めします。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 6.5が稼働するFTDv。
- キーペアと証明書署名要求(CSR)の作成には、OpenSSLが使用されます。

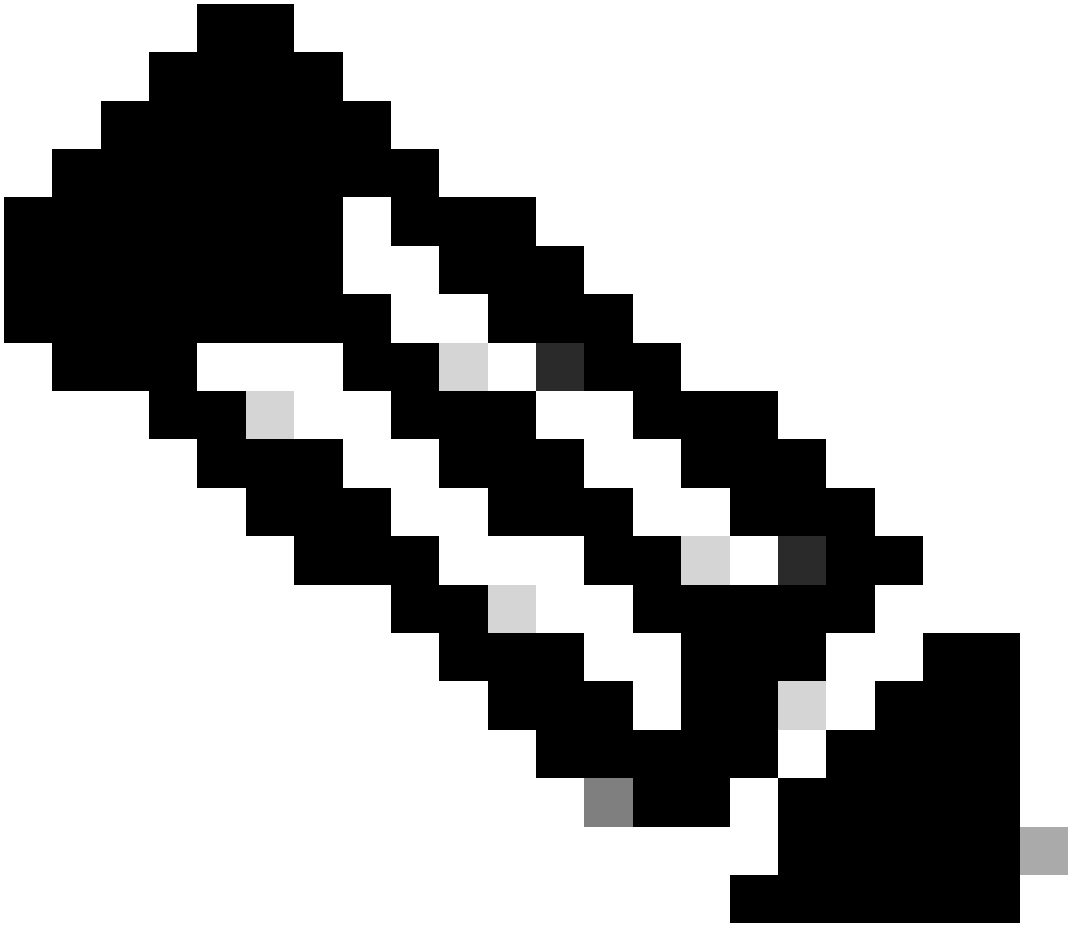
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

証明書のインストール

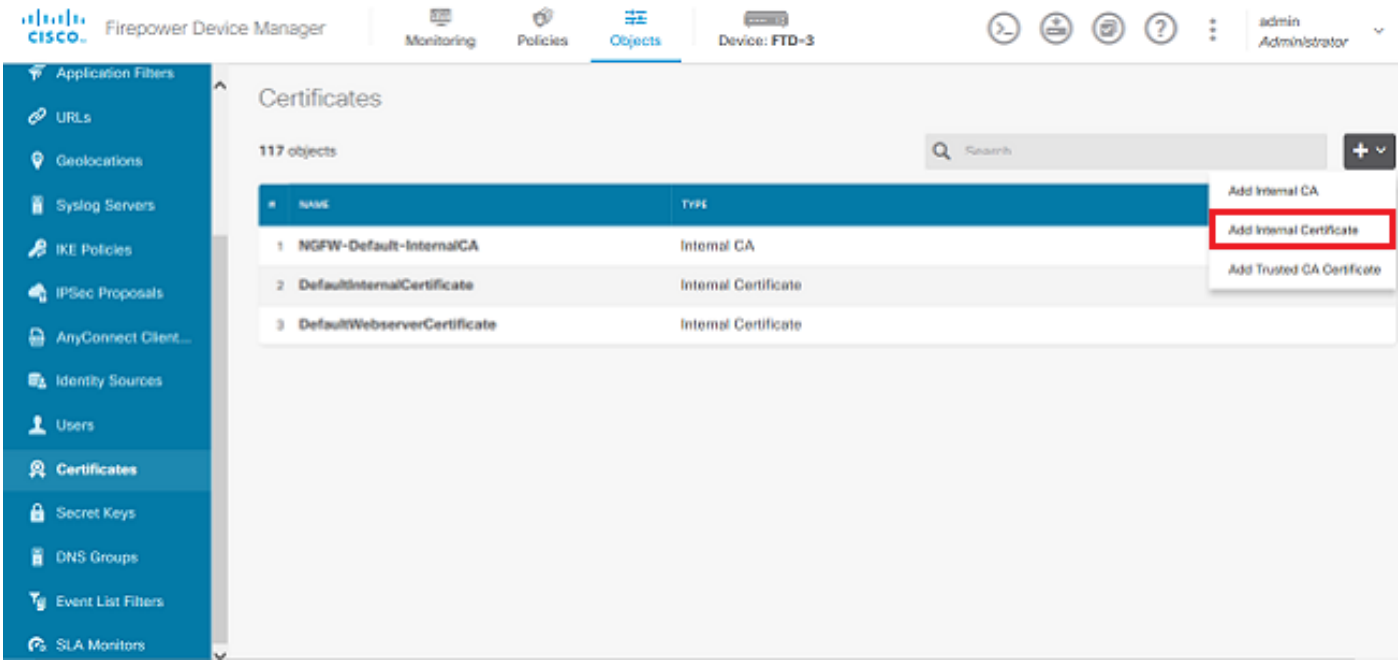
自己署名証明書の登録

自己署名証明書を使用すると、FTDデバイスに適切なフィールドが追加された証明書を簡単に取得できます。ほとんどの場所では信頼できませんが、サードパーティの署名付き証明書と同様の暗号化の利点を提供できます。それでも、ユーザや他のデバイスがFTDによって提示される証明書を信頼できるように、信頼できるCA署名付き証明書を用意することをお勧めします。

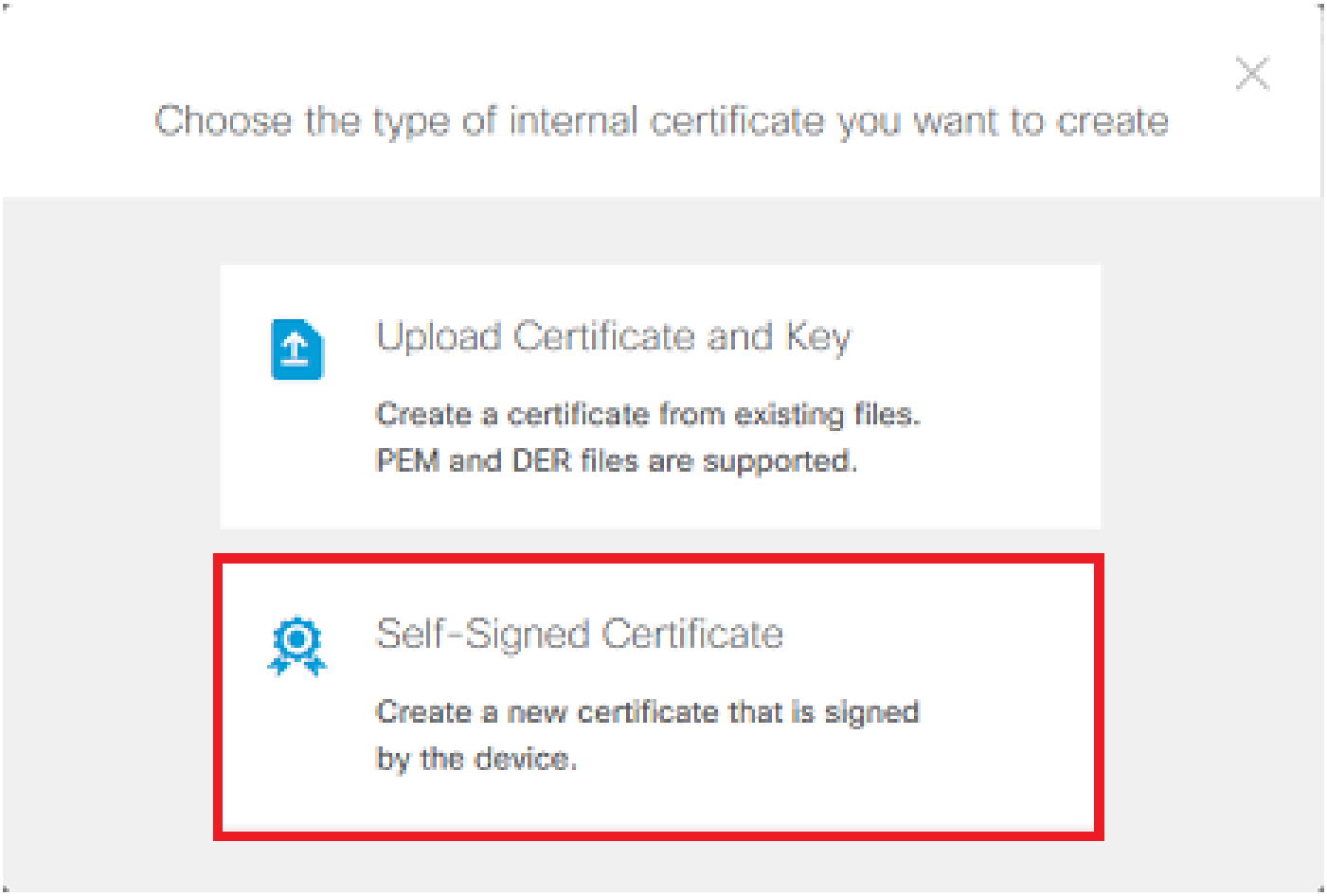


注:Firepower Device Management(FDM)には、同様の目的で使用できるDefaultInternalCertificateという名前のデフォルトの自己署名証明書があります。

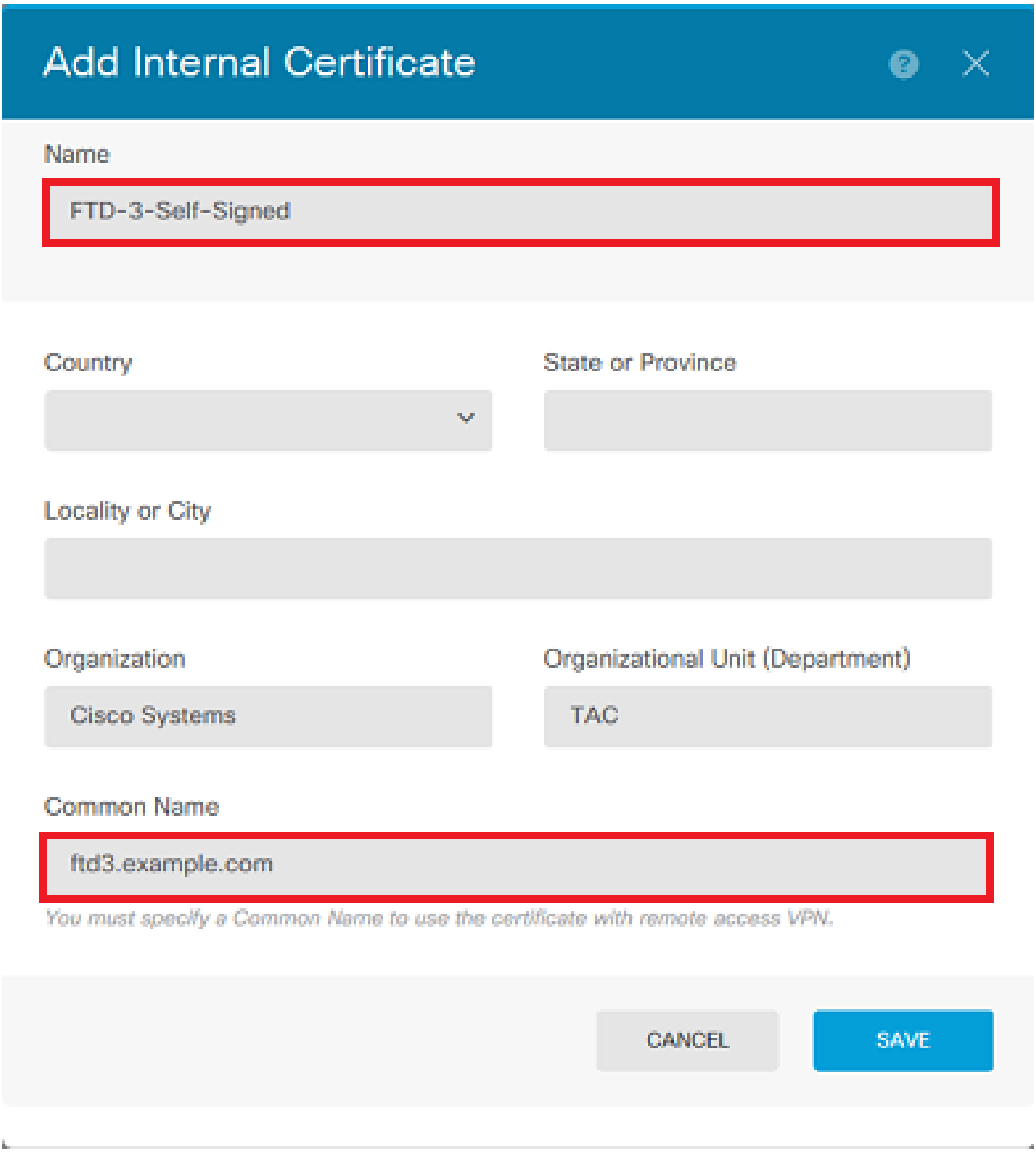
1. Objects > Certificatesの順に移動します。+記号をクリックし、図に示すようにAdd Internal Certificate を選択します。



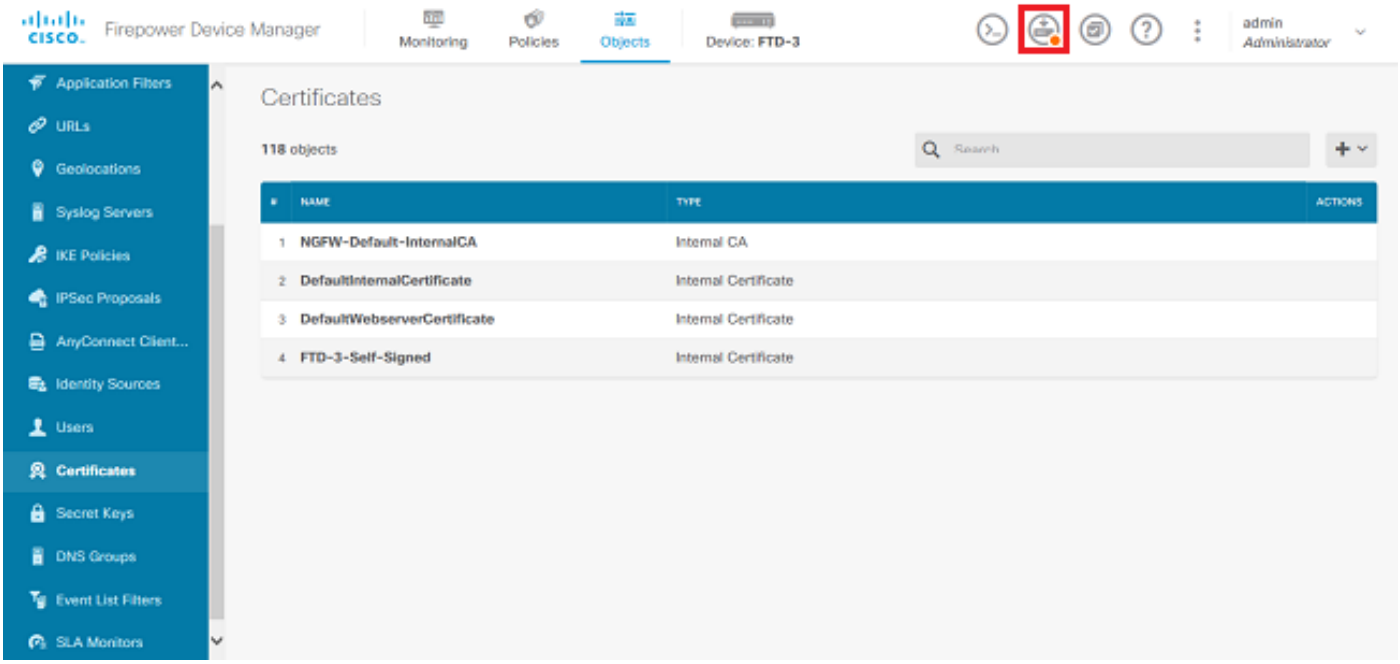
2. 図に示すように、ポップアップウィンドウでSelf-Signed Certificateを選択します。



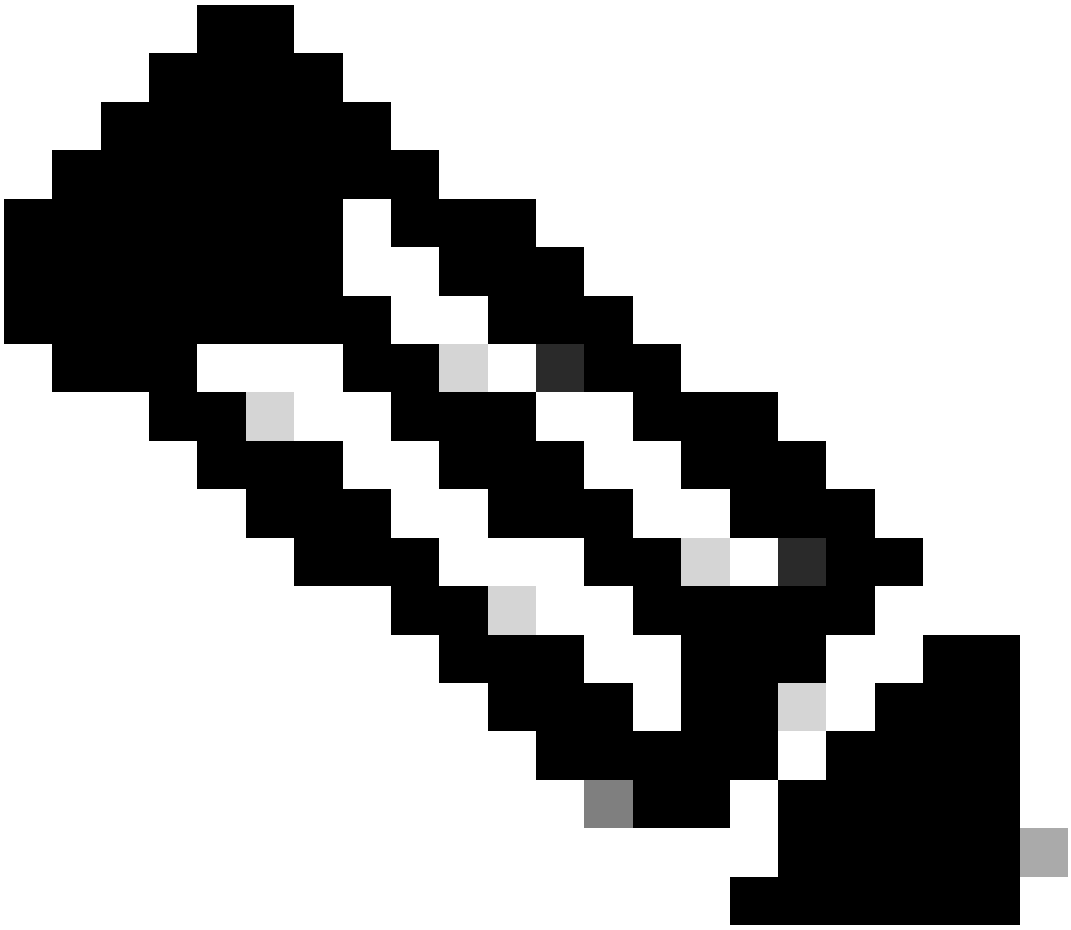
3. トラストポイントの名前を指定し、サブジェクトの識別名フィールドに入力します。少なくとも、Common Nameフィールドは追加できます。これは、証明書が使用されるサービスの完全修飾ドメイン名(FQDN)またはIPアドレスと一致する場合があります。 図に示すように、完了したらSaveをクリックします。



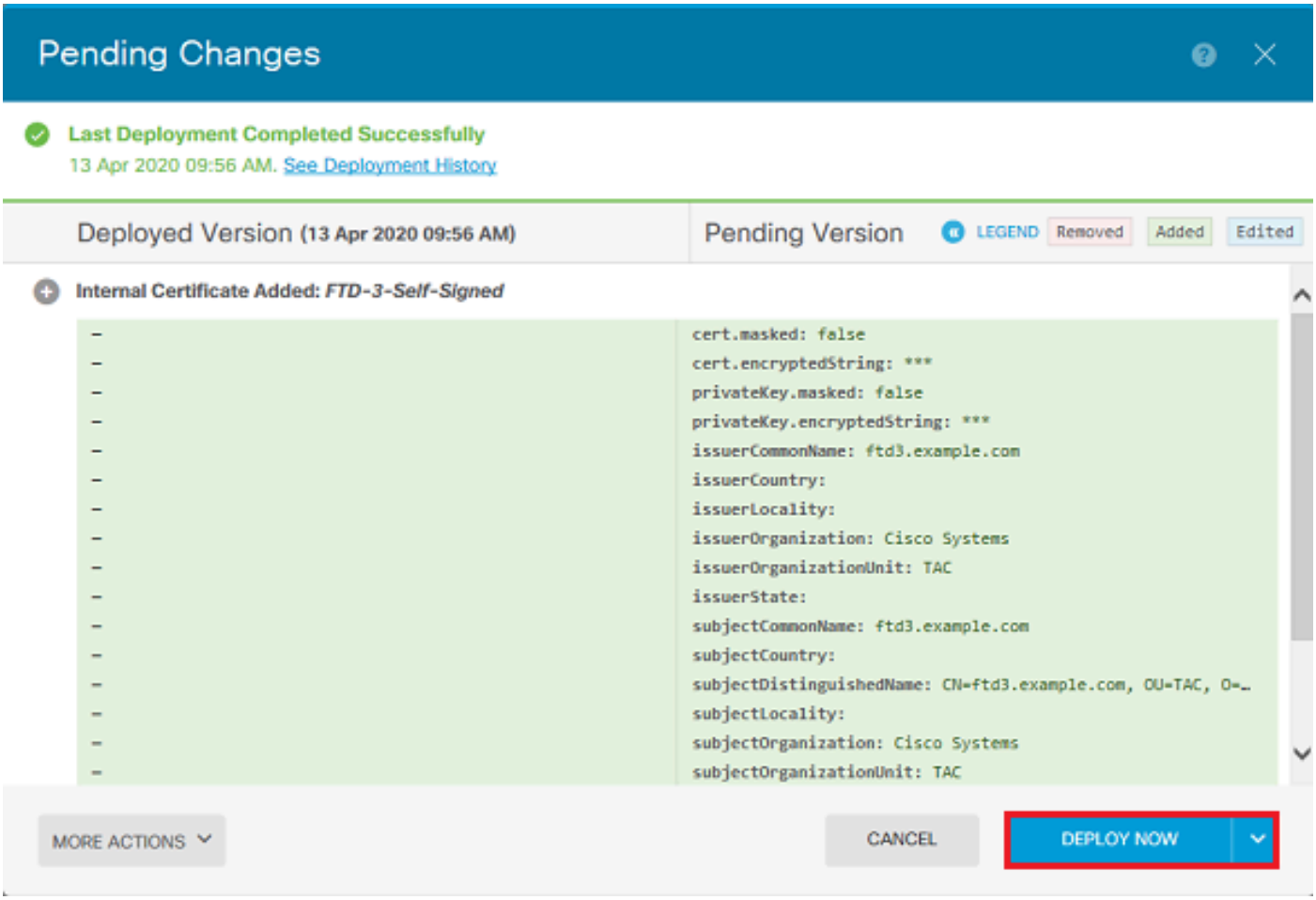
4. 図に示すように、画面右上のPending Changesボタンをクリックします。



5. 「今すぐ配置」ボタンをクリックします。



注：導入が完了すると、図に示すように、AnyConnectなどの証明書を使用するサービスが存在しない限り、証明書をCLIに表示することはできません。



手動登録

手動登録を使用すると、信頼できるCAによって発行された証明書をインストールできます。OpenSSLまたは同様のツールを使用して、CA署名付き証明書の受信に必要な秘密キーとCSRを生成できます。次の手順では、秘密キーとCSRを生成するための一般的なOpenSSLコマンド、および取得後に証明書と秘密キーをインストールする手順について説明します。

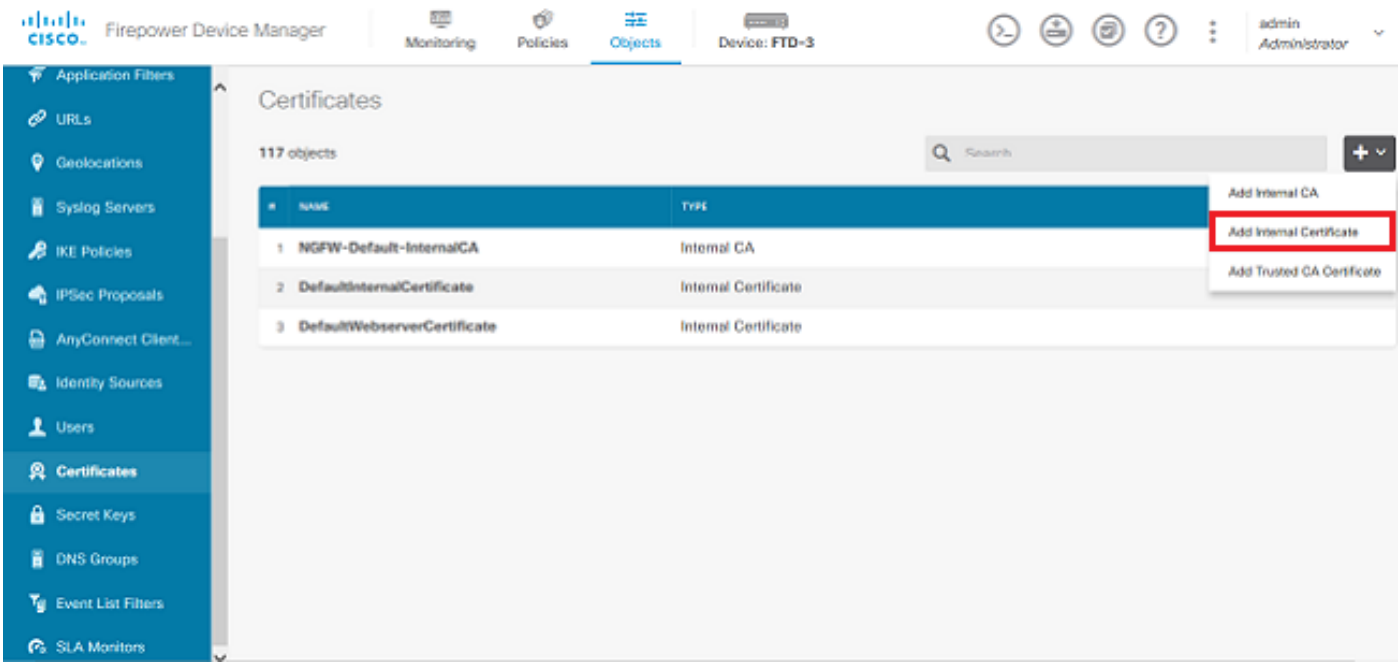
1. OpenSSLまたは同様のアプリケーションを使用して、秘密キーと証明書署名要求(CSR)を生成します。この例では、private.keyという名前の2048ビットRSAキーと、ftd3.csrという名前のCSRがOpenSSLで作成されます。

```
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.
```

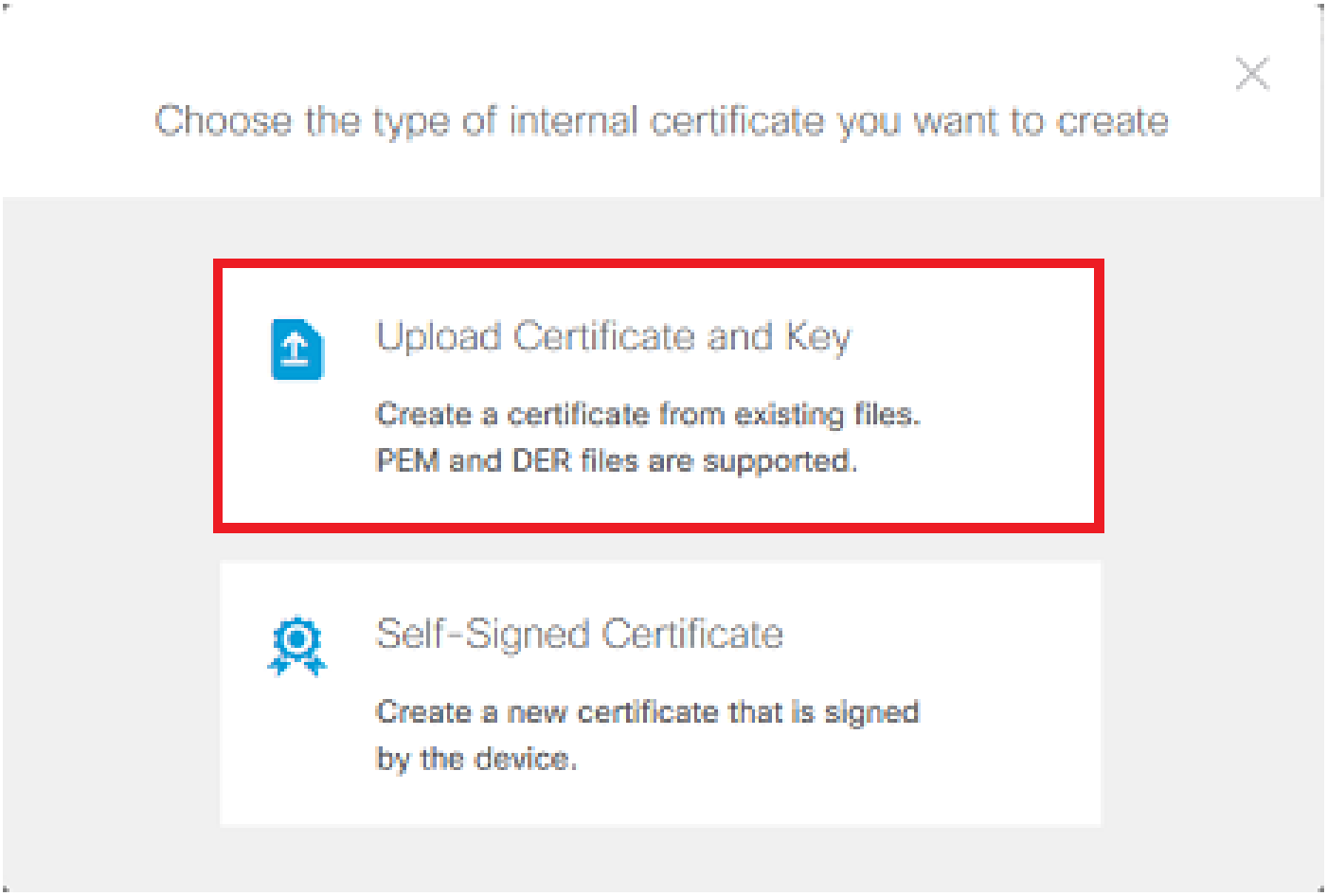
```
There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', the field is left blank.
-----
Country Name (2 letter code) [AU]:.
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [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. 生成されたCSRをコピーし、CAに送信します。CSRが署名されると、ID証明書が提供されます。

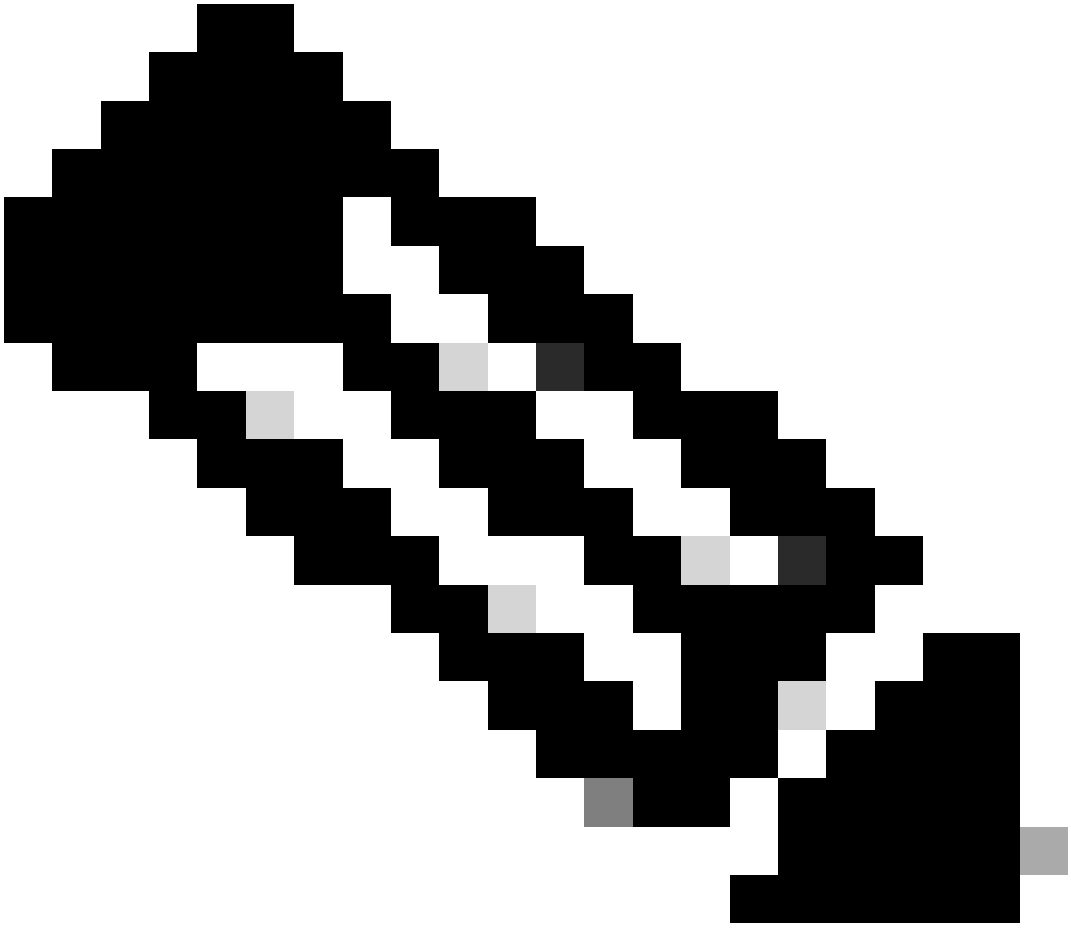
3. 「オブジェクト」>「証明書」にナビゲートします。 +記号をクリックし、図に示すように、Add Internal Certificate を選択します。



4. 図に示すように、ポップアップウィンドウでUpload Certificate and Keyを選択します。

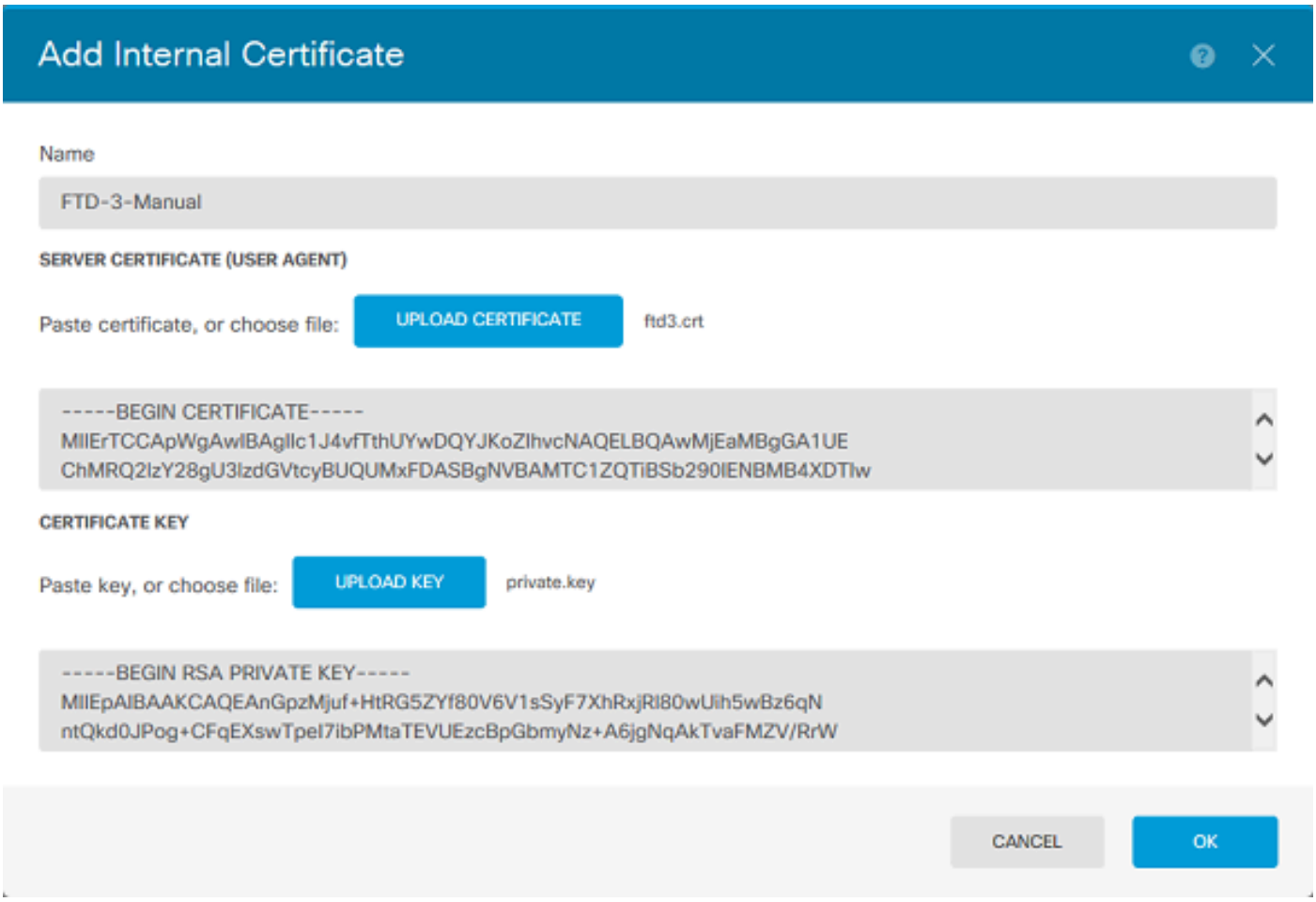


5. トラストポイントの名前を指定し、ID証明書と秘密キーをPrivacy Enhanced Mail(PEM)形式でアップロードするか、コピーアンドペーストします。CAが証明書と鍵を単一のPKCS12で提供している場合は、このドキュメントの後半にあるPKCS12ファイルからのID証明書と秘密鍵の抽出というタイトルのセクションに移動して、証明書と秘密鍵を分離します。

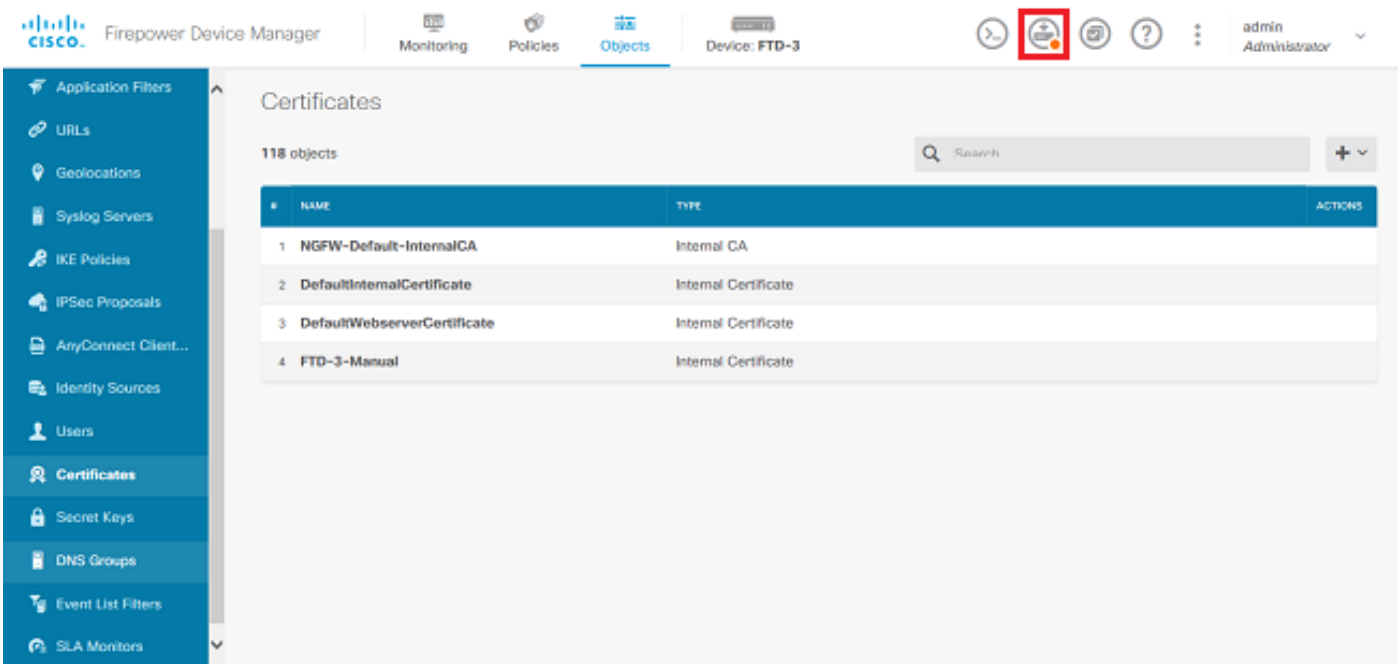


注意：ファイル名にスペースを含めることはできません。スペースを含めないと、FDMはスペースを受け入れません。また、秘密キーは暗号化しないでください。

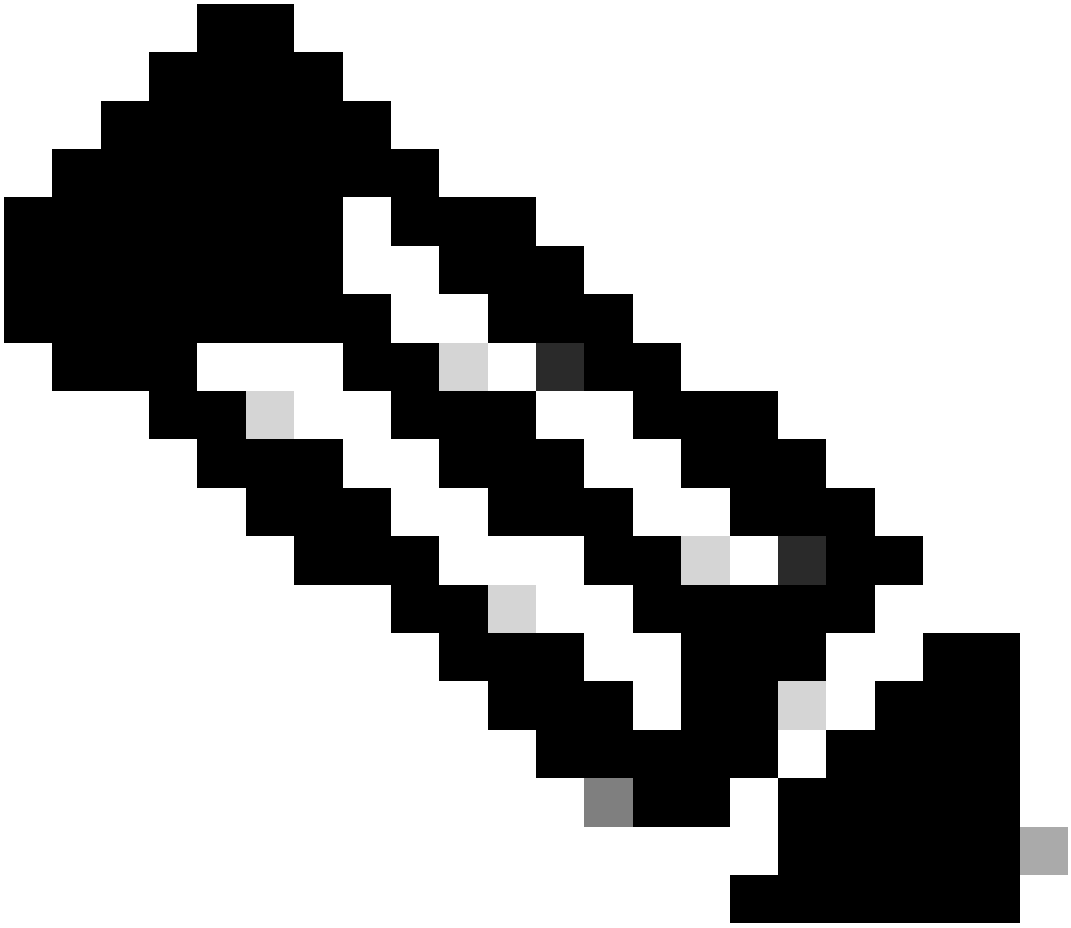
図に示すように、完了したらOKをクリックします。



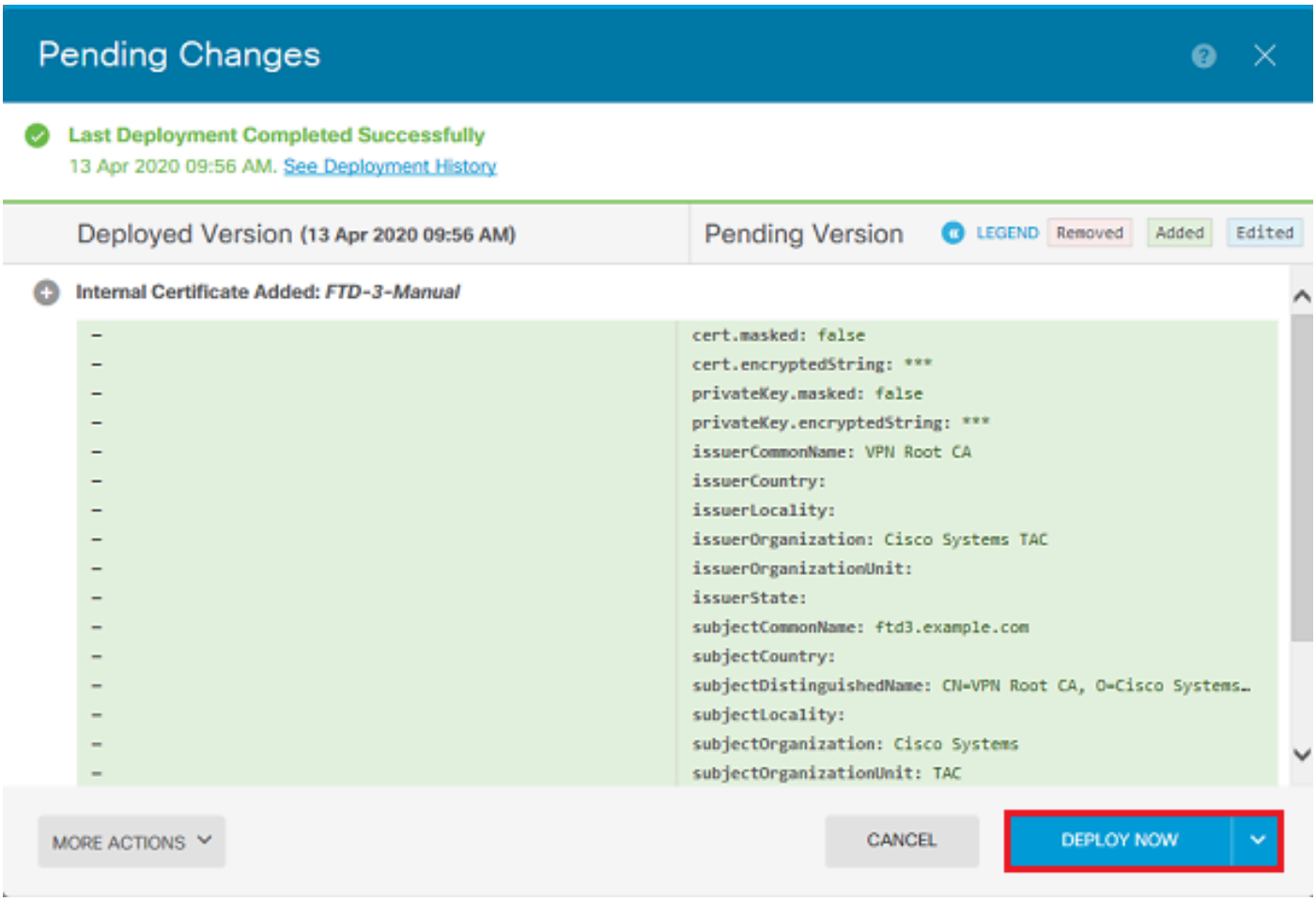
6. 図に示すように、画面右上のPending Changesボタンをクリックします。



7. 「今すぐ配置」ボタンをクリックします。



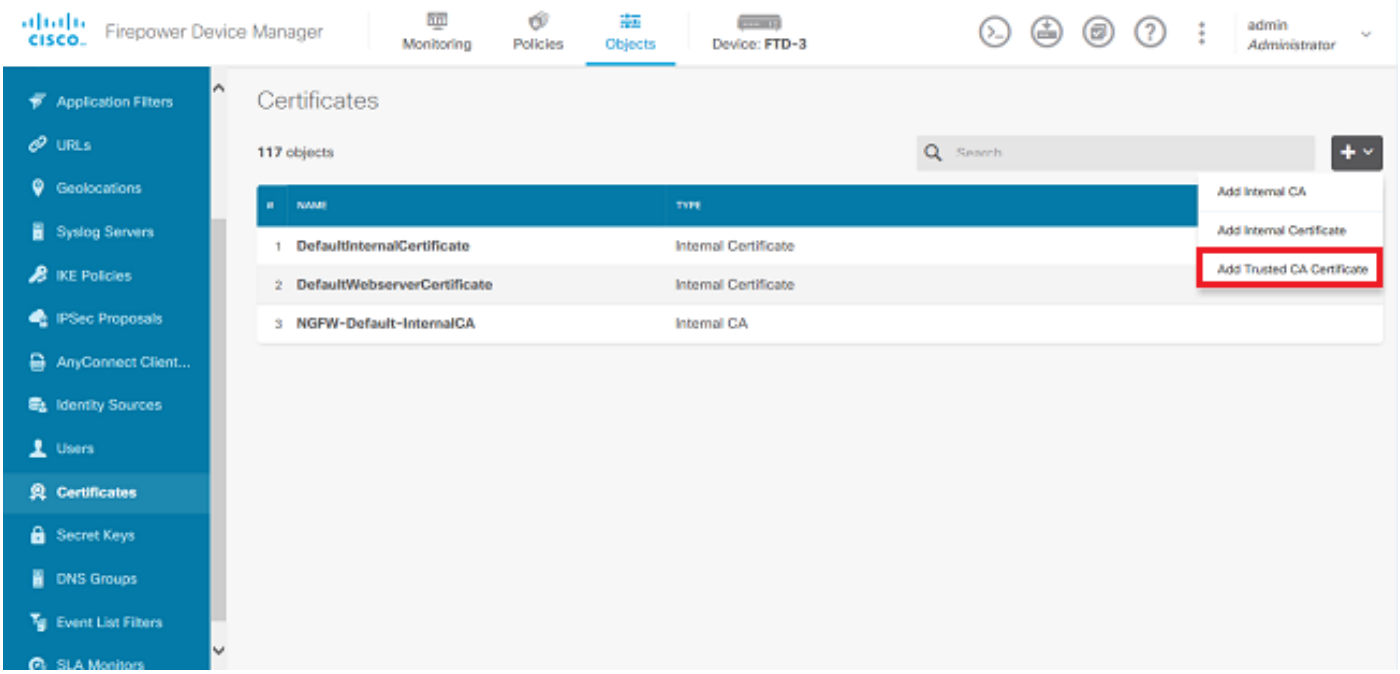
注：導入が完了すると、図に示すように、AnyConnectなどの証明書を使用するサービスが存在しない限り、証明書をCLIに表示することはできません。



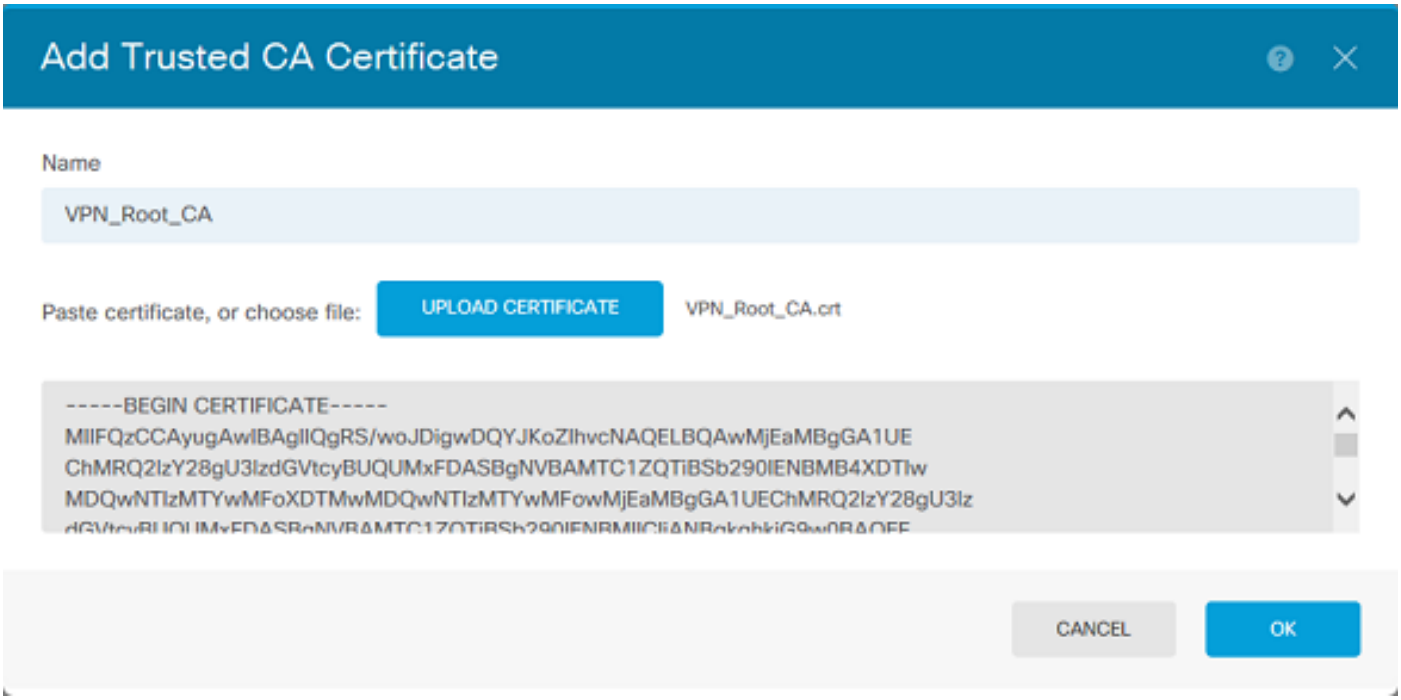
信頼済みCA証明書のインストール

信頼できるCA証明書をインストールする場合、FTDにID証明書を提示するユーザまたはデバイスを正常に認証するために必要です。この一般的な例としては、AnyConnect証明書認証やS2S VPN証明書認証などがあります。次の手順では、CA証明書を信頼し、そのCAによって発行された証明書も信頼する方法について説明します。

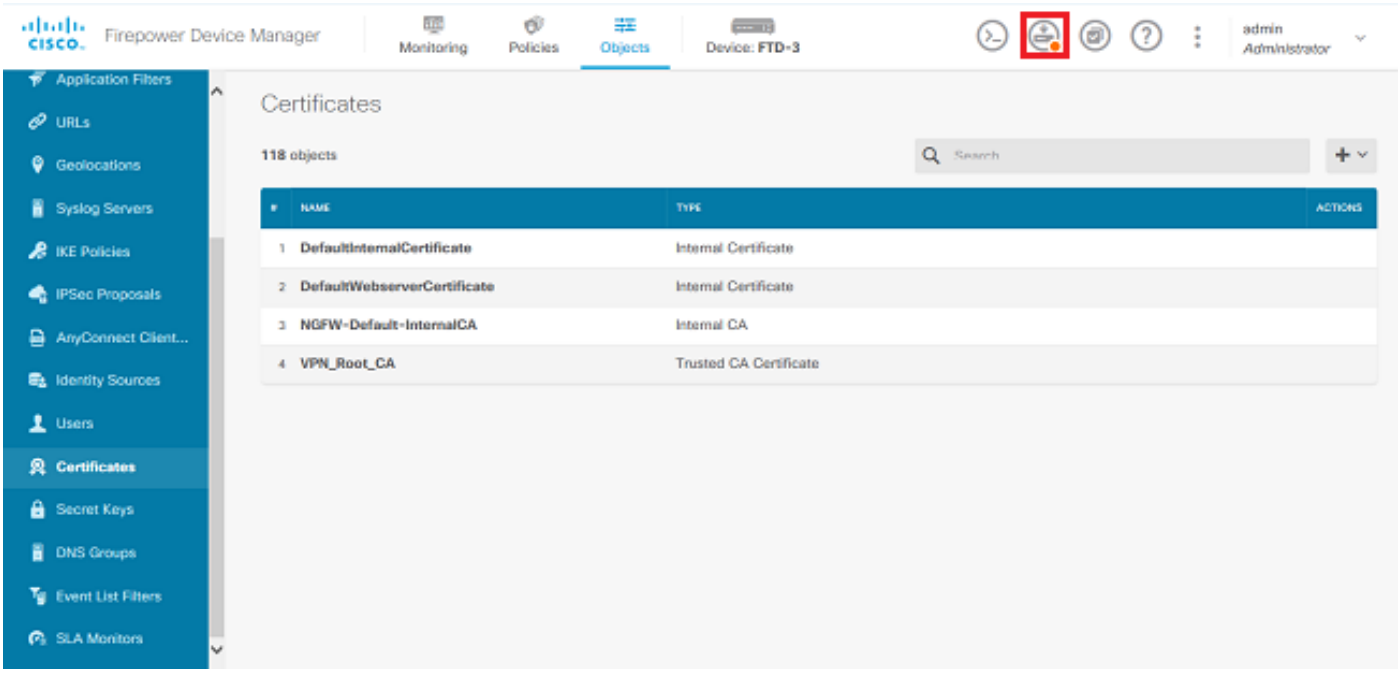
1. Objects > Certificatesの順に移動します。 +記号をクリックし、図に示すように、信頼できるCA証明書の追加を選択します。



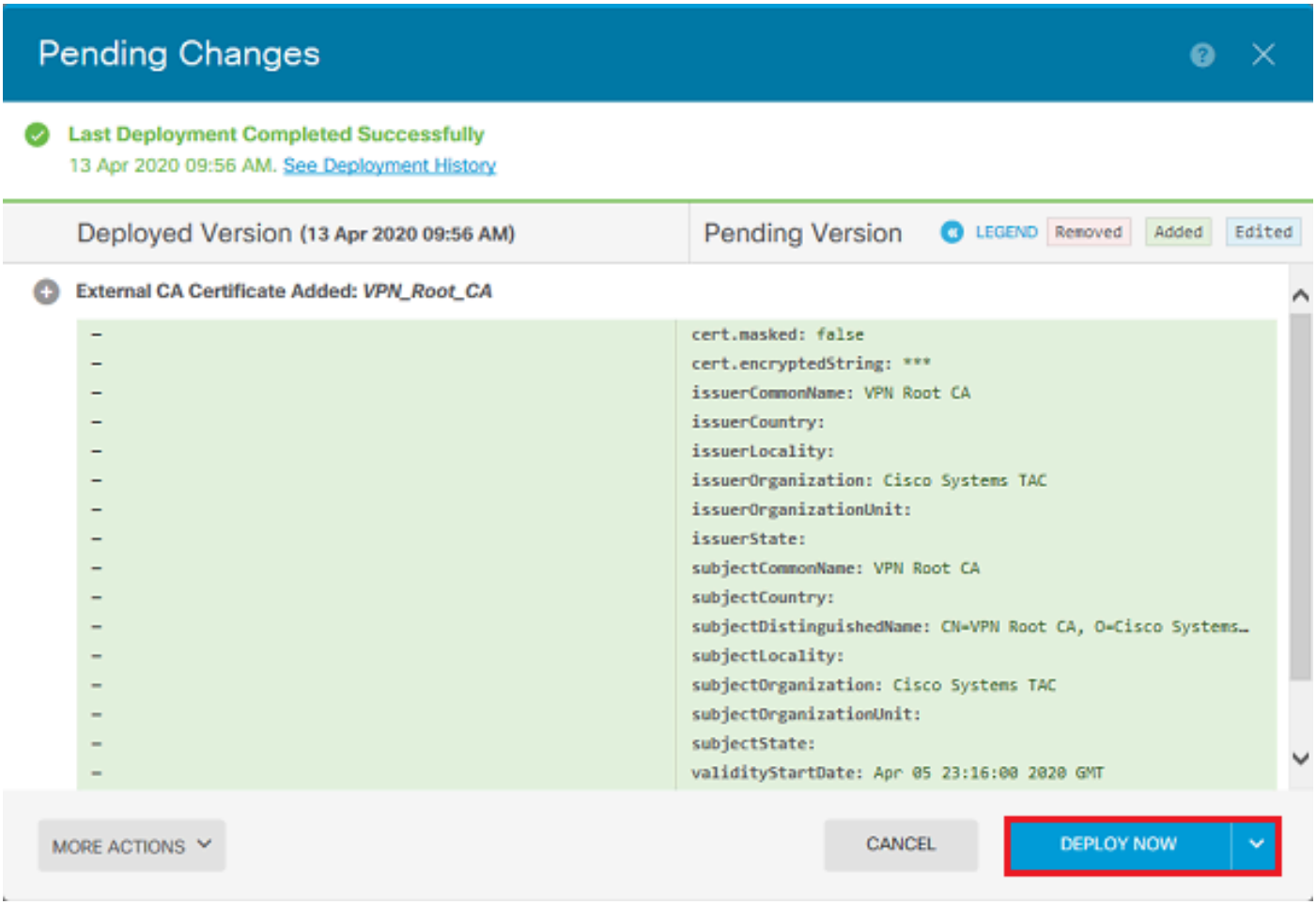
2. トラストポイントの名前を指定します。次に、PEM形式でCA証明書をアップロードするか、コピーアンドペーストします。図に示すように、完了したらOKをクリックします。



3. 図に示すように、画面右上のPending Changesボタンをクリックします。



4. 図に示すように、「今すぐ配備」ボタンをクリックします。



証明書の更新

FDMによって管理されるFTDの証明書の更新には、以前の証明書および場合によっては秘密キーの置き換えが含まれます。元の証明書の作成に使用した元のCSRと秘密キーがない場合は、新し

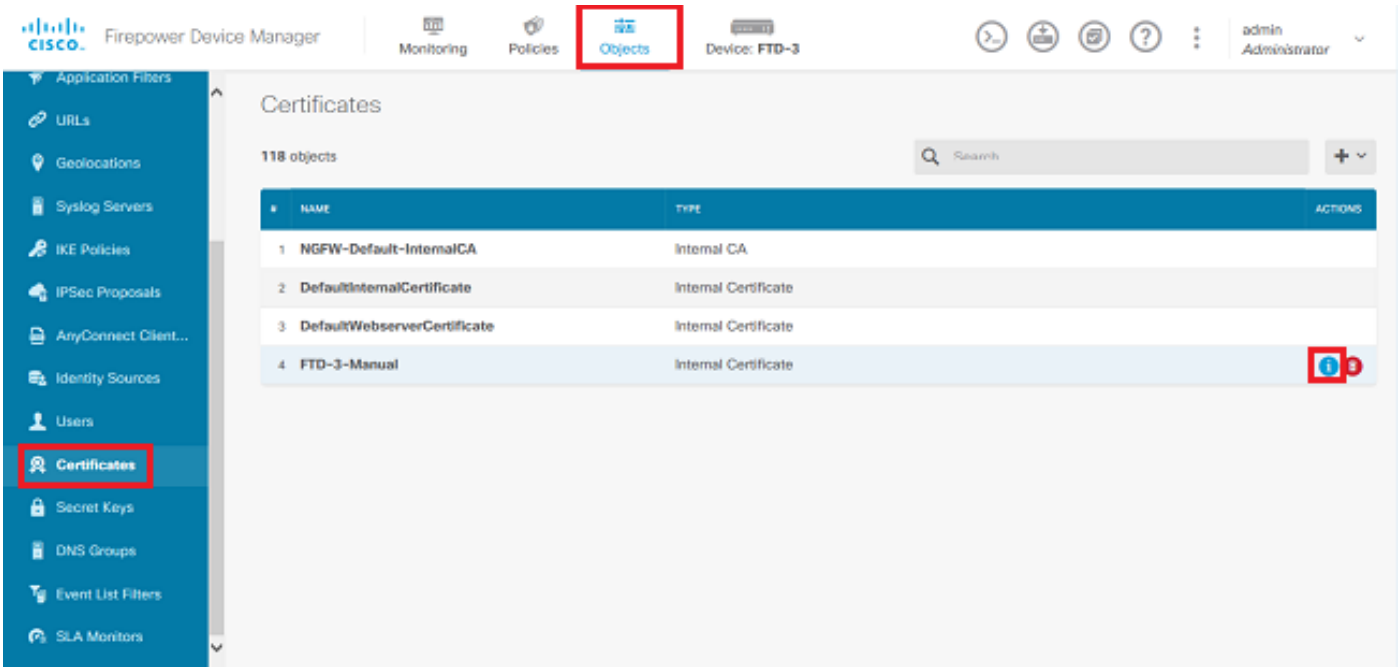
いCSRと秘密キーを作成する必要があります。

1. 元のCSRと秘密キーがある場合、この手順は無視できます。それ以外の場合は、新しい秘密キーとCSRを作成する必要があります。OpenSSLまたは同様のアプリケーションを使用して、秘密キーとCSRを生成します。この例では、private.keyという名前の2048ビットRSAキーと、ftd3.csrという名前のCSRがOpenSSLで作成されます。

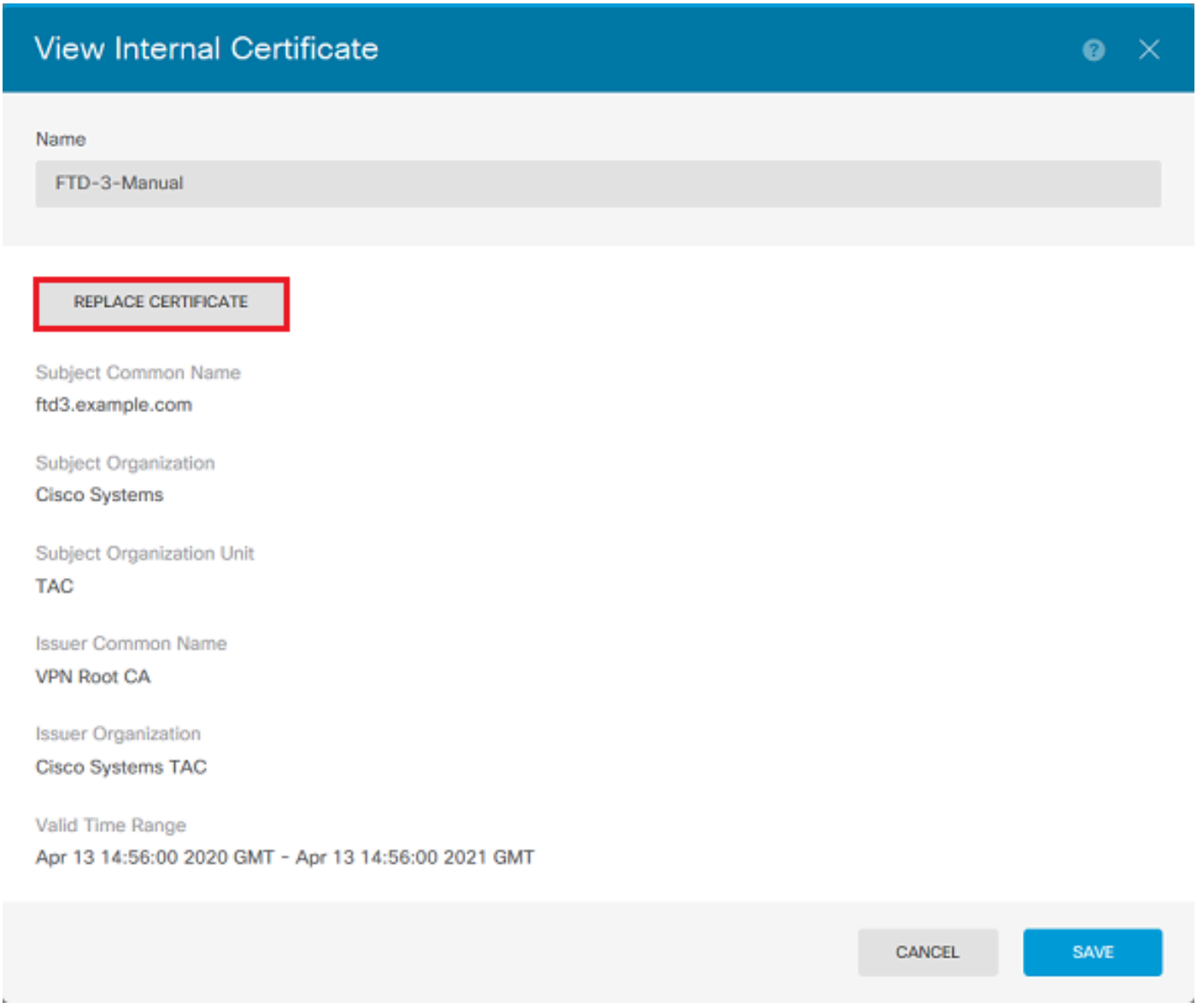
```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
.....................................+++
.....................................................................+++
writing new private key to 'private.key'
-----
You are about to be asked 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. 生成したCSRまたは元のCSRを認証局に送信します。CSRが署名されると、更新されたID証明書が提供されます。

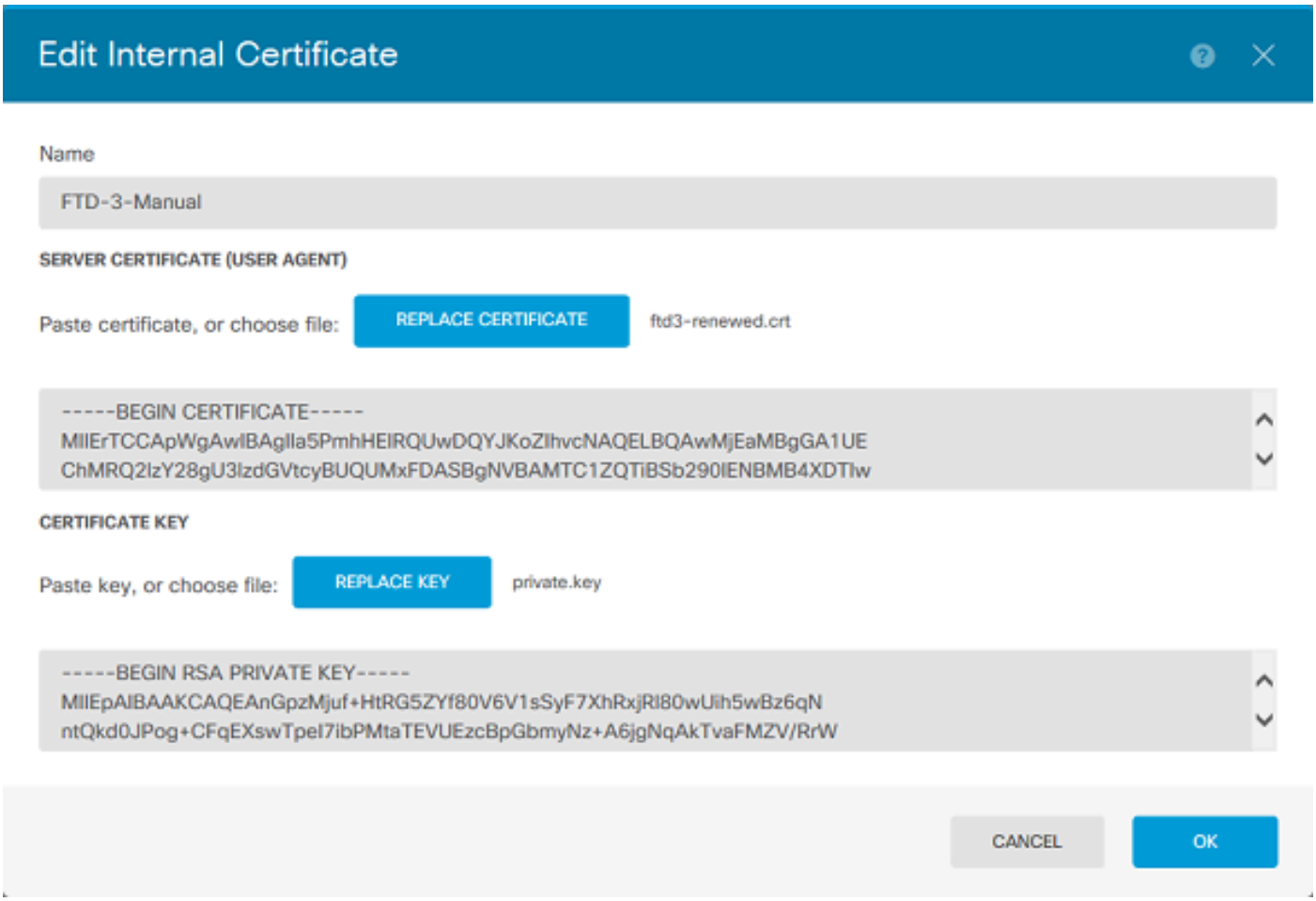
3. 「オブジェクト」>「証明書」にナビゲートします。 更新する証明書の上にカーソルを置き、図に示すようにViewボタンをクリックします。



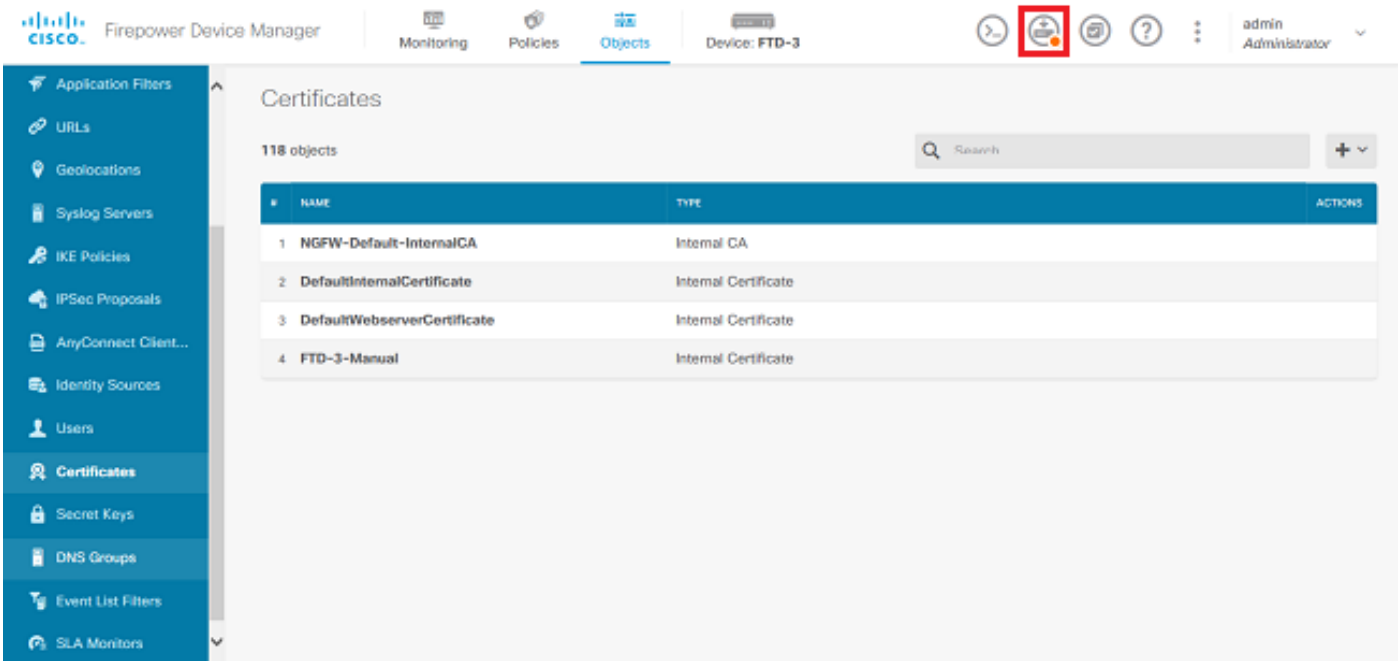
4. 図に示すように、ポップアップウィンドウでReplace Certificateをクリックします。



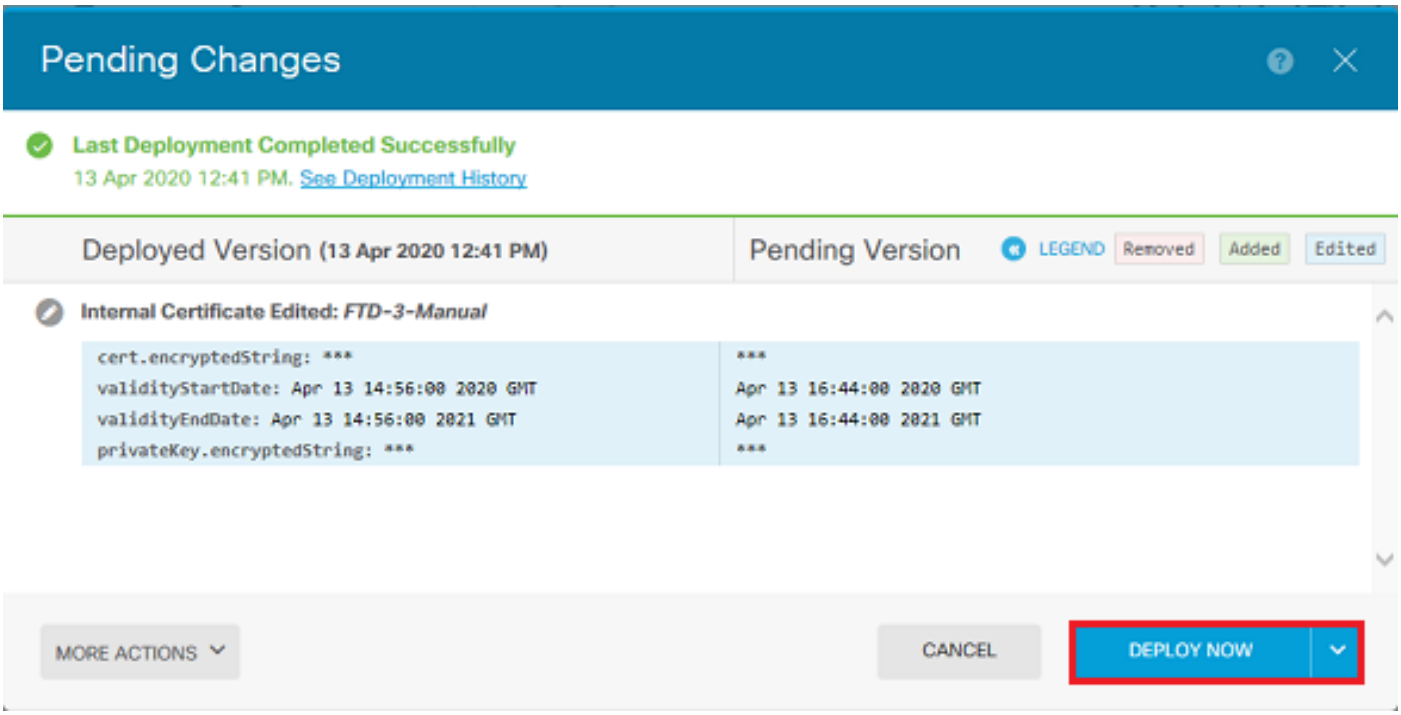
5. PEM形式のID証明書と秘密キーをアップロードするか、コピーアンドペーストします。図に示すように、完了したらOKをクリックします。



6. 図に示すように、画面右上のPending Changesボタンをクリックします。



7. 図に示すように、「今すぐ配備」ボタンをクリックします。



一般的なOpenSSL操作

PKCS12ファイルからのID証明書と秘密キーの抽出

管理者は、FTDにインポートする必要があるPKCS12ファイルを受信できます。FDMは現在、PKCS12ファイルのインポートをサポートしていません。PKCS12ファイルに含まれている証明書と秘密キーをインポートするには、OpenSSLなどのツールを使用してPKCS12から個々のファイルを抽出する必要があります。PKCS12の暗号化に使用するパスコードが必要です。

```
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+HtRG5ZYf80V6V1s
SyF7XhRxjRl80wUih5wBz6qNntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZOIcpzVqL6hOziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50
QpQDTgvIiD1bYpPiWKpS0g1PZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZa
HrP9YOxO9+MpVMH33R9vRl3SOEF6kpZ6VEdGI4s6/IRvaM1zlBcK1ON/N2+mjwID
AQABo4G3MIG0MAkGA1UdEwQCMAAwHQYDVR0OBBYEFMcvjL0XiSTzNADJ/ptNb/cd
zB8wMB8GA1UdIwQYMBaAFHekzDnhi4O727mjLXuwCRVFgyguMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwGwYDVR0RBBQwEoIQZnRk
```

```
My5leGFtcGxlLmNvbTAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMA0G
CSqGSIb3DQEBCwUAA4ICAQCjjrMjruGH5fpcFND8qfuVU0hkszCwq2O1oMqMrvXn
gENKcXxxT27z6AHnQXeX3vhDcY3zs+FzFSoP5tRRPmy/413HAN+QEP2L9MQVD9PH
f5OrQ/Ke5c16hMOJO8daR7wNzvFkcbicKCLRH0EvEoI0SPKsLyGSSxGmh6QXfZcM
GX3jG9Krglugp2UEqOug9HPTpgsbuNcHw8xXgFp6IAlOLrytwrLeMIh5V+Vh5pll
yTl9wo5VADoYKgN4O8D21TeJIj6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwfMXM4Tl
Rk3EOdSTENqzq2ZwnqJ4HCoqar7ASlQ5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBUlbadlnEfi5Jl8G+/vZl6ykcmXe9hokKYxY8cg/U717On/FbAmdYwRYgMAE4
RWfBpOvoNzn97cG+qzogo7j/0kTfYu3O9DzdU3uy+R8JJkBrerktrZR7w7OfP61O
IAs86N5Zb18U14Gfc9m0eXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2Px0yam/bROn0FoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJFOiV0GV+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/M1zuMjhj0tCphsJPhvNII7lcNj6K0pvg2yB/Md7PXOZnLaz9pf
GgpjpH0zzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXmlHQcgp
g5BgZMGqro0l5rcq0PjtK9Tqg7qO13Vf0kMlsofMp+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
0ipqKraokS2Oo0STwQ7Q9Wk1xCrwxMfTuDJFMe8OqabFAU557O5PDXPtFEutn0xz
Ou8VMLBRy+gDc+0WARsjFj+0gUOc2Wj3gQ81GlyoPYgufWRnztN5rQxWzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AydsGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p7O2FZly5lxuzuA/wPnR89HiIkSF13OMTpnOIl3d6dO7s3bwyNja8JikYTCflle5
2CSsz4Cn/BlwfWyAcLN3HxUjG4Ev2818fWWpkYmuxujpKDFFzF0skpKAK53tNKPf
pn4+w5FyLo18o0AydtPoKjYkDqbvG/SRPbt92mdTIF7E6J+o8J6OV3YL+IyrZ+u0
MYqPd45Oi4cgHdMFICAndN3PYScrrGYHawfVxp+R+G4dTJWdMvthh3ftS0mkiKJ8
m1NH7WYST1kYcTbcokZiOIcZa+VVv5UOLIt/hD0VG7xqZ0lpMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpxTIsmDv9rQzxBjuCyKn+23FkkUhFJt0D989UUyp08H9vDoJr
yzm9J0pMrg==
-----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
RlPBXMLb70nMtPTqctl58+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-----
```

pkcs12file.pfxは、パッケージ解除する必要があるaPKCS12ファイルです。

この例では、3つの個別のファイルが作成されます。

1つはID証明書用です。subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.comであるため、これがID証明書であることがわかります。

```
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
SyF7XhRxjRl8OwUih5wBz6qNntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZOIcpzVqL6hOziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50
QpQDTgvIiD1bYpPiWKpSOg1PZDnX8b74Os0pVKVXTsujQqSqH1va9BB6hK1JCoZa
HrP9YOxO9+MpVMH33R9vRl3SOEF6kpZ6VEdGI4s6/IRvaM1zlBcK1ON/N2+mjwID
AQABo4G3MIG0MAkGA1UdEwQCMAAwHQYDVR0OBBYEFMcvjL0XiSTzNADJ/ptNb/cd
zB8wMB8GA1UdIwQYMBaAFHekzDnhi4O727mjLXuwCRVFgyguMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwGwYDVR0RBBQwEoIQZnRk
My5leGFtcGxlLmNvbTAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMA0G
CSqGSIb3DQEBCwUAA4ICAQCjjrMjruGH5fpcFND8qfuVU0hkszCwq2O1oMqMrvXn
gENKcXxxT27z6AHnQXeX3vhDcY3zs+FzFSoP5tRRPmy/413HAN+QEP2L9MQVD9PH
f5OrQ/Ke5c16hMOJO8daR7wNzvFkcbicKCLRHOEvEoIOSPKsLyGSSxGmh6QXfZcM
GX3jG9Krglugp2UEqOug9HPTpgsbuNcHw8xXgFp6IAlOLrytwrLeMIh5V+Vh5pll
yTl9wo5VADoYKgN4O8D21TeJIj6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwfMXM4Tl
Rk3EOdSTENqzq2ZwnqJ4HCoqar7ASlQ5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBUlbadlnEfi5Jl8G+/vZl6ykcmXe9hokKYxY8cg/U717On/FbAmdYwRYgMAE4
```

```
RWfBpOvoNzn97cG+qzogo7j/OkTfYu3O9DzdU3uy+R8JJkBrerktrZR7w7OfP61O
IAs86N5Zb18U14Gfc9mOeXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2Px0yam/bROnOFoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJFOiVOGV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfpMwTiT47I
ng==
-----END CERTIFICATE-----
```

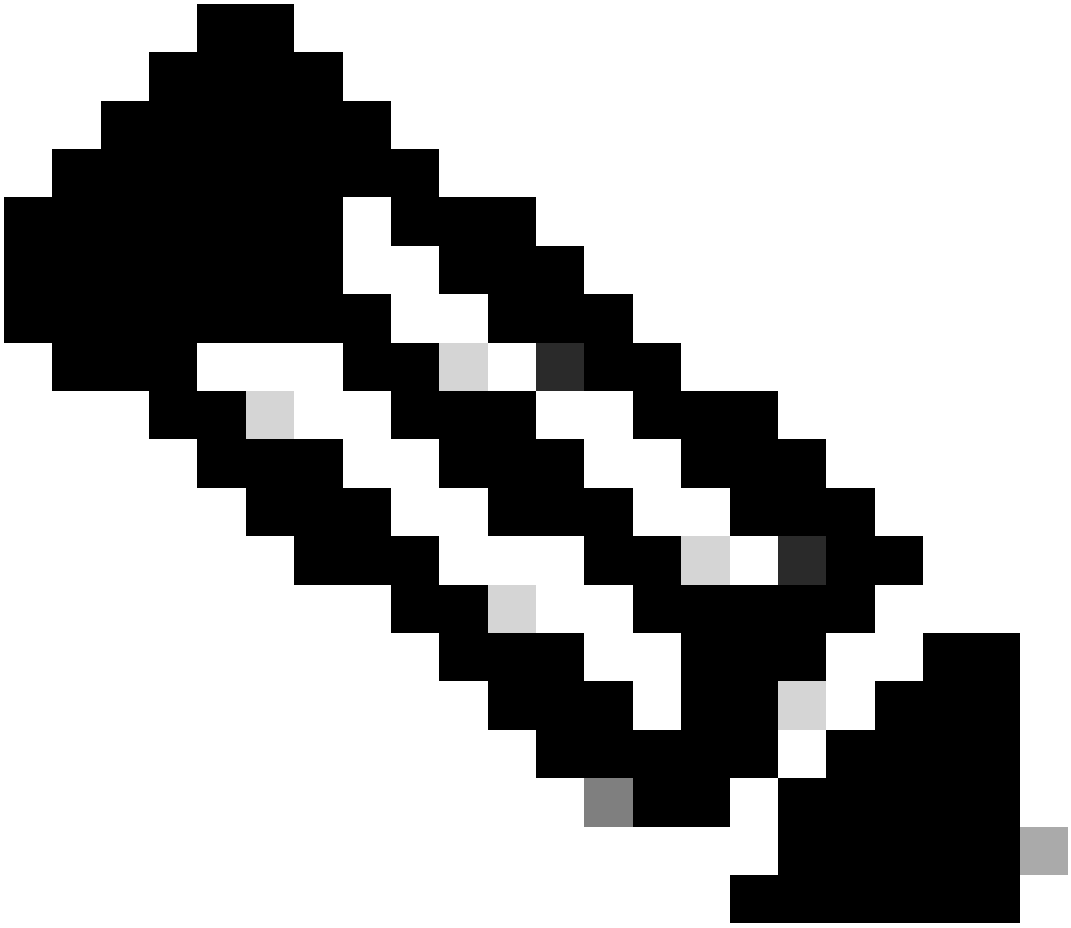
1つは発行側CA証明書用です。subject=/O=Cisco Systems TAC/CN=VPN Root CAであるため、これがID証明書であることがわかります。これは、前述のID証明書の発行者と同じ値です。

```
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
g5BgZMGqro0l5rcq0PjtK9Tqg7q013Vf0kMlsofMp+Bu1CiFDpawF/j8uSPuswEs
rzvJ+8GbOY1WEHtohgNGjPOOq8wnKQuOC47Ft1UMpdSwUsMMze0X43dyp/WoZtLW
4v/Pn/NibE3aoPOaMhIo4CdwSBHZOgVag4INqVsuFX1uPKD25WhrlO9LQ93P/sN3
FhoAh98HKOcuQ64Ua3AaShdzornD+G2J2pd1Nf1DahlzlskIMtlURSWdLjsHLKft
JqSOoLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/lyNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cxl1jINOLdB+/jQqkfzmx9ziB1PXnIshNRbflLLrNfdDO9agqQsvsC
AwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDKC4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDKC4wCwYDVR0PBAQD
AgEGMA0GCSqGSIb3DQEBCwUAA4ICAQC6B+Y3obatEZqv0RQz1MS6oOumCgNWGi8d
kcRDxkY2F+zw3pBFa54Sin1OfRPJvZvLNJV5OdXmvH5luh6KJDMVrLMWNiSgI7Tn
0ipqKraokS2Oo0STwQ7Q9Wk1xCrwxMfTuDJFMe8OqabFAU557O5PDXPtFEutn0xz
Ou8VMLBRy+gDc+OWARsjFj+OgUOc2Wj3gQ81GlyoPYgufWRnztN5rQxWzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AydsGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p7O2FZly5lxuzuA/wPnR89HiIkSF13OMTpnOIl3d6d07s3bwyNja8JikYTCflle5
2CSsz4Cn/BlwfWyAcLN3HxUjG4Ev2818fWWpkYmuxujpKDFFzFOskpKAK53tNKPf
pn4+w5FyLo18o0AydtPoKjYkDqbvG/SRPbt92mdTIF7E6J+o8J6OV3YL+IyrZ+u0
MYqPd45Oi4cgHdMFICAndN3PYScrrGYHawfVxp+R+G4dTJWdMvthh3ftSOmkiKJ8
m1NH7WYST1kYcTbcokZiOIcZa+VVv5UOLIt/hDOVG7xqZOlpMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpxTIsmDv9rQzxBjuCyKn+23FkkUhFJtOD989UUypO8H9vDoJr
yzm9JOpMrg==
-----END CERTIFICATE-----
```

秘密キー用に1つ：

```
-----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
M6ZTwTOZ1snOf4ohVePrW/kkdlQavJbPa+OdzjZvs88ClEXAJ/XIegfSWifJAXqP
3d37VonXX7YRocJ4kzhkuE/SUDsu1sMCOhbM81uZcWiBbDAT2jjlKgfoxubtnuFq
un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZHOBuFls+wZEmzYqw+cuc+I8XEFVOMl8
P3ah28NnoOjXMk4MpfFJlYMCmMq66xj5gZtcVZxOGCOswOCKUOJiFFQTEmmVf9/C
65a96np7YCI8s6UnUWi5Zp/NrbN31HkPOwt7+1DFGFit1pTTGvOFchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG1l5NSslwKbTGiiwCYwON8cO9TXQbO4rMomFDAv8
aef1aBsjMqEUkzOZKOU2ZgTxMline8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubp0
qtmFX/DtSu9J2yevfV+3/YCwnSRkrO2oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc4O
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-----
```



注意：秘密鍵は暗号化されており、FDMは暗号化された秘密鍵を受け入れません。

秘密キーの暗号化を解除するには、暗号化された秘密キーをファイルにコピーしてから、次のopensslコマンドを実行します。

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

- encrypted.keyは、暗号化された秘密キーを保持するファイルの名前です。
- unencrypted.keyは、暗号化されていないキーを持つファイルの名前です。

次の例に示すように、暗号化されていない秘密キーでは-----BEGIN ENCRYPTED PRIVATE KEY-----ではなく-----BEGIN RSA PRIVATE KEY-----と表示されます。

```
-----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/zoLYJH0BBLWeY3QioLO
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-----
```

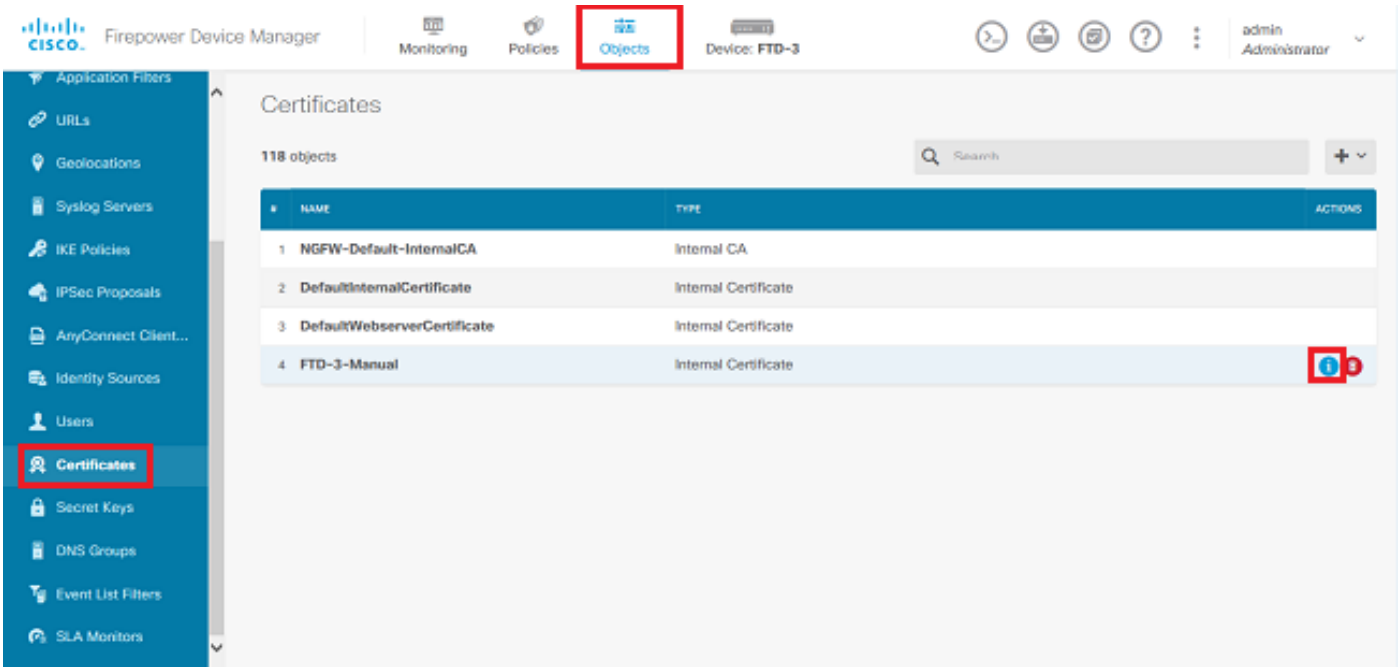
秘密鍵が暗号化されていない場合は、前述の「手動登録」セクションの手順3を使用して、IDおよび秘密鍵ファイルをアップロードするか、コピーしてFDMに貼り付けることができます。発行側CAは、前述の「信頼済みCA証明書のインストール」の手順を使用してインストールできます。

確認

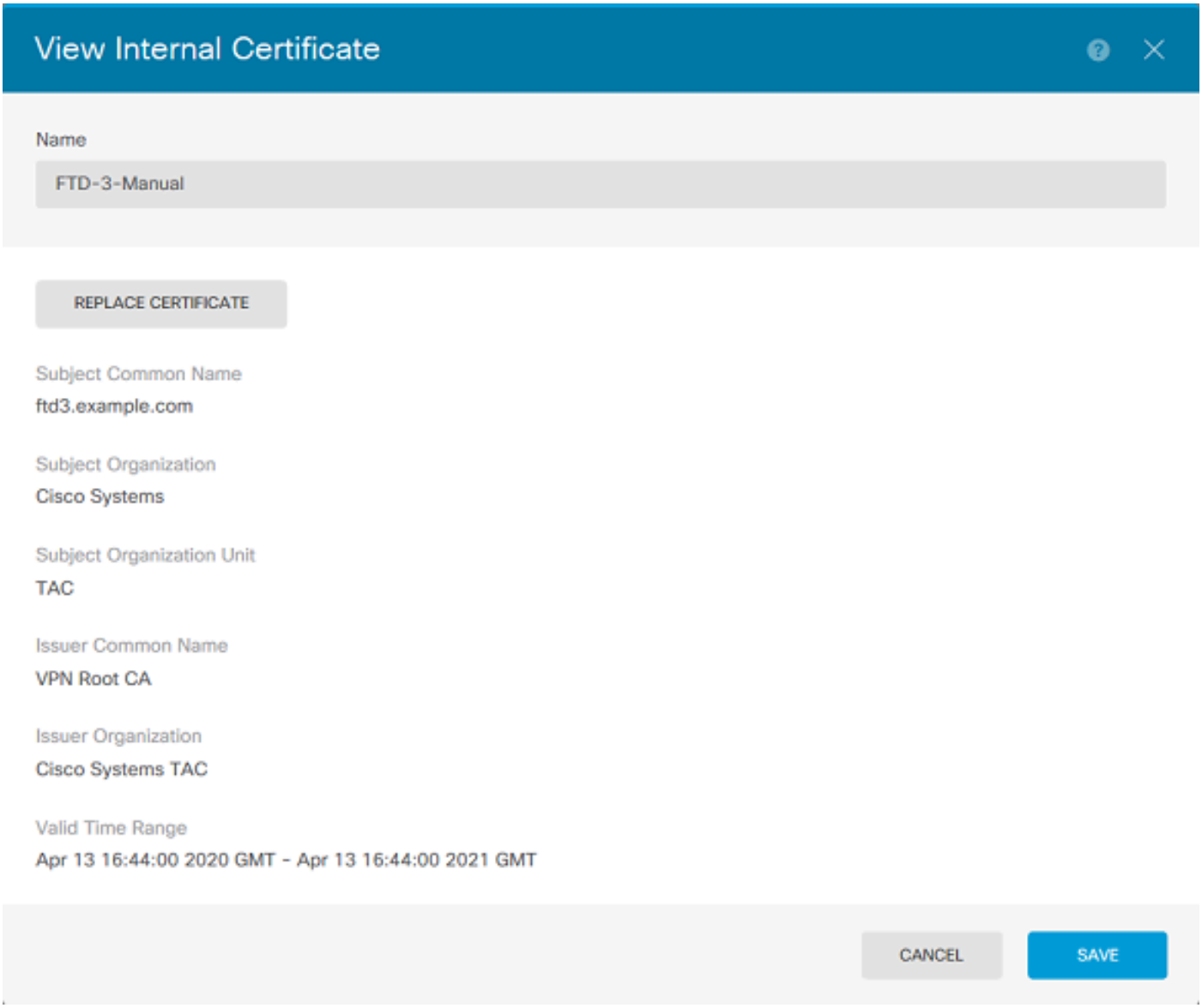
このセクションでは、設定が正常に動作していることを確認します。

FDMでのインストール済み証明書の表示

1. Objects > Certificatesの順に移動します。確認する証明書の上にカーソルを置き、図に示すようにviewボタンをクリックします。



2. 図に示すように、ポップアップウィンドウに証明書に関する詳細が表示されます。

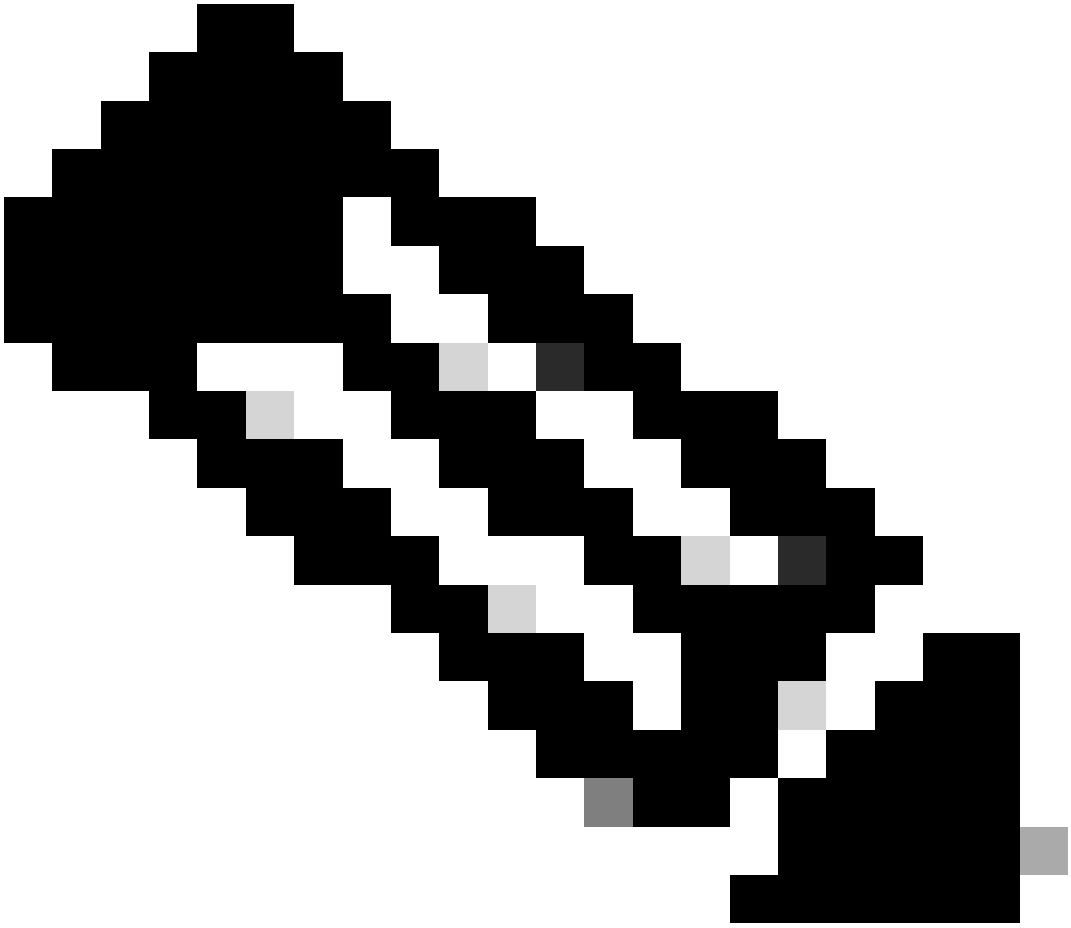


CLIでのインストール済み証明書の表示

FDMでCLIコンソールを使用するか、FTDにSSHで接続し、コマンドshow crypto ca certificatesを実行して、図のように証明書がデバイスに適用されていることを確認できます。

出力例：

```
> 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
```



注:ID証明書は、AnyConnectなどのサービスで使用される場合にのみCLIに表示されます。信頼されたCA証明書は、展開されると表示されます。

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

デバッグ コマンド

SSL証明書のインストールが失敗した場合、SSHを使用してFTDに接続した後、診断CLIからデバッグを実行できます。debug crypto ca 14

古いバージョンのFTDでは、次のデバッグが利用でき、トラブルシューティングに推奨されます。

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 255

一般的な問題

ASAエクスポートPKCS12のインポート

OpenSSLでエクスポートされたASA PKCS12からID証明書と秘密キーを抽出しようとすると、次のようなエラーが発生する場合があります。

```
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
```

この問題を解決するには、まずpkcs12ファイルをDER形式に変換する必要があります。

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

この作業が完了したら、前の「PKCS12ファイルからのID証明書と秘密キーの抽出」セクションの手順に従って、ID証明書と秘密キーをインポートできます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。