Installieren und Verlängern des Zertifikats auf einem von FDM verwalteten FTD

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie selbstsignierte Zertifikate und Zertifikate, die von einer Drittanbieter-Zertifizierungsstelle oder internen Zertifizierungsstelle auf FTD signiert wurden, installiert, als vertrauenswürdig eingestuft und erneuert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Für die manuelle Zertifikatregistrierung ist der Zugriff auf eine vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA) eines Drittanbieters erforderlich. Zu den CA-Anbietern von Drittanbietern gehören u. a. Entrust, Geotrust, GoDaddy, Thawte und VeriSign.
- Überprüfen Sie, ob die FirePOWER Threat Defense (FTD) über die richtige Uhrzeit, das

richtige Datum und die richtige Zeitzone verfügt. Für die Zertifikatsauthentifizierung wird die Verwendung eines NTP-Servers (Network Time Protocol) empfohlen, um die Uhrzeit auf dem FTD zu synchronisieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FTDv mit 6.5.
- Für die Erstellung von Keypair und Certificate Signing Request (CSR) wird OpenSSL verwendet.

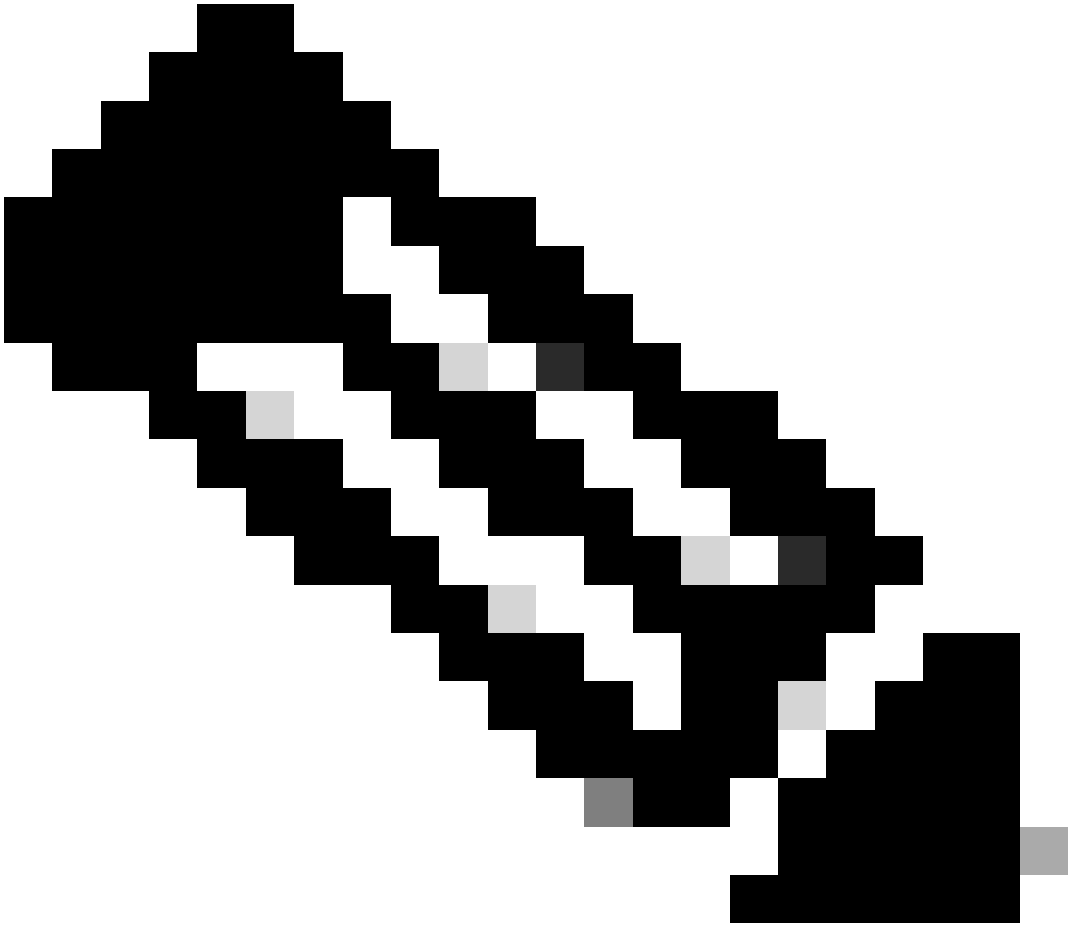
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Installation des Zertifikats

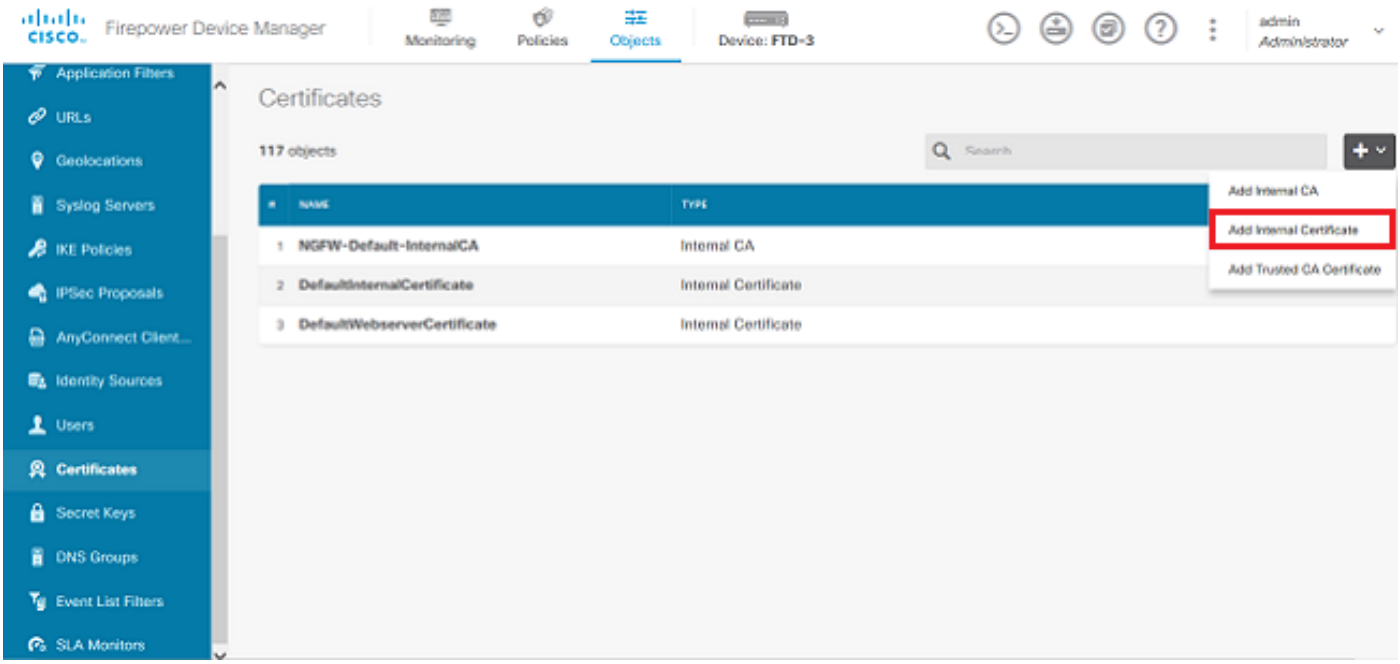
Selbstsignierte Registrierung

Selbstsignierte Zertifikate sind eine einfache Möglichkeit, ein Zertifikat mit den entsprechenden Feldern zu erhalten, die dem FTD-Gerät hinzugefügt werden. Obwohl sie an den meisten Orten nicht vertrauenswürdig sind, können sie dennoch ähnliche Verschlüsselungsvorteile bieten wie ein von einem Drittanbieter signiertes Zertifikat. Dennoch wird empfohlen, ein vertrauenswürdiges CA-signiertes Zertifikat zu haben, damit Benutzer und andere Geräte dem vom FTD vorgelegten Zertifikat vertrauen können.

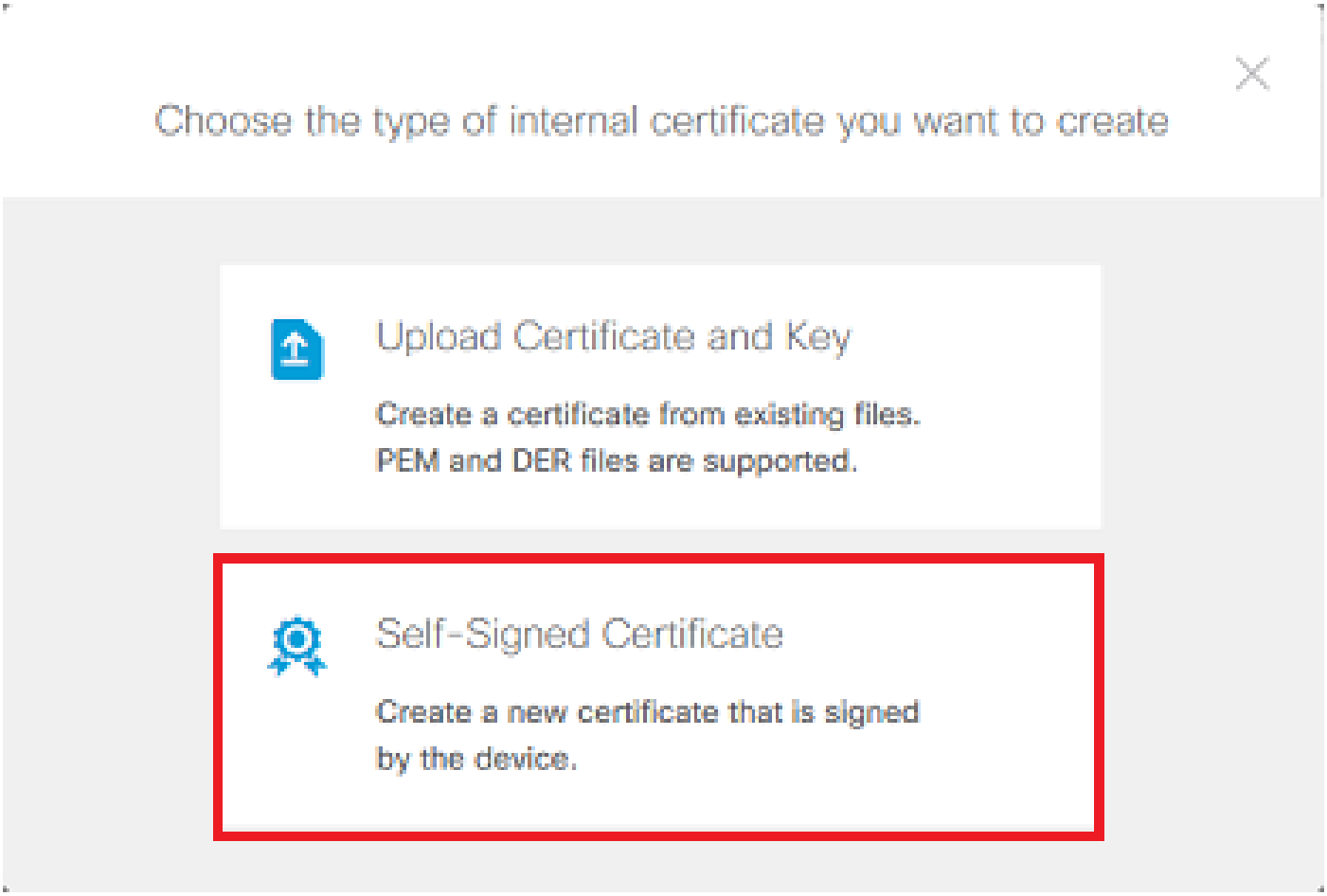


Hinweis: FirePOWER Device Management (FDM) verfügt über ein selbstsigniertes Standardzertifikat mit dem Namen DefaultInternalCertificate, das für ähnliche Zwecke verwendet werden kann.

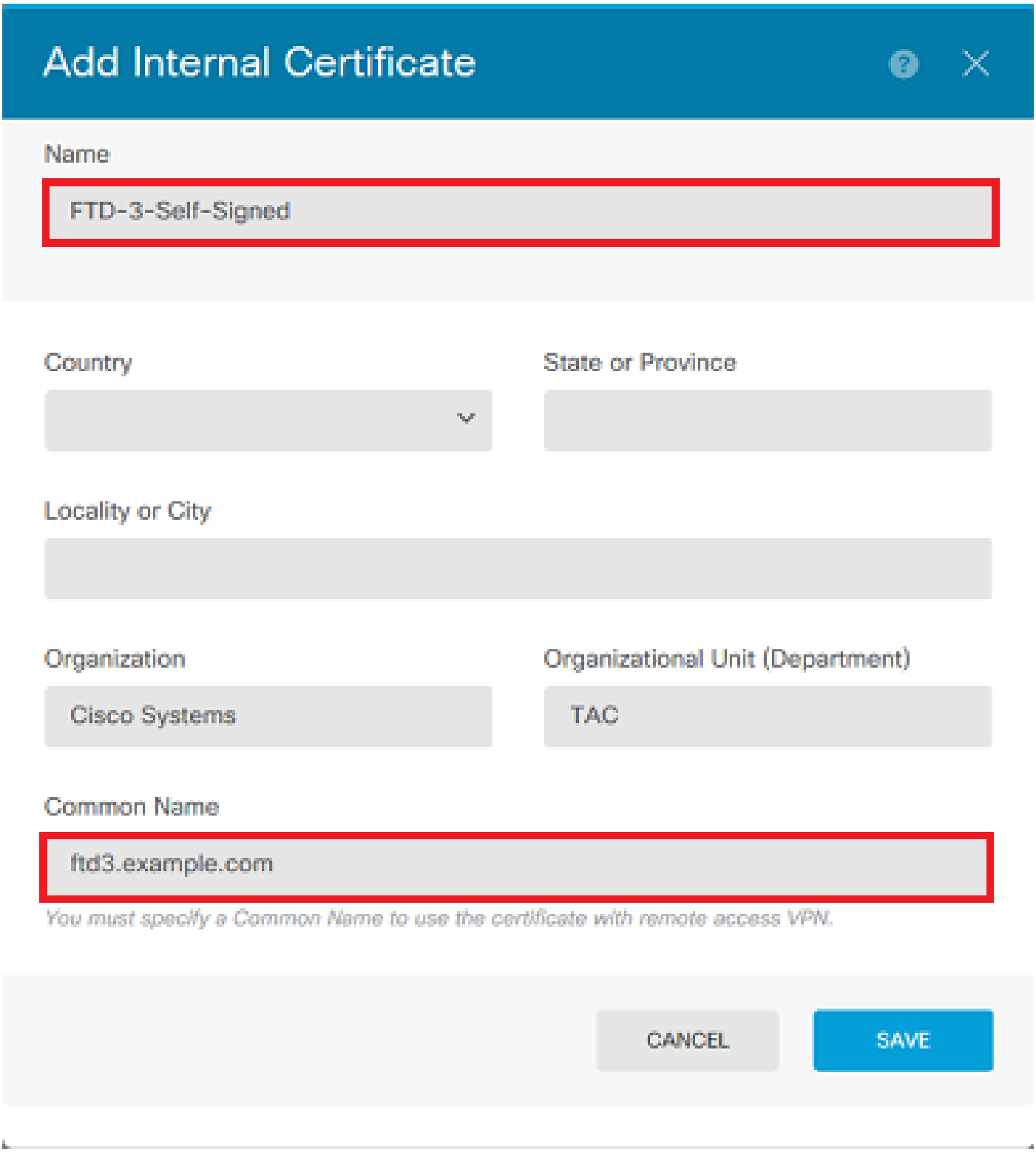
1. Navigieren Sie zu Objekte > Zertifikate. Klicken Sie auf das Symbol +, und wählen Sie dann Internes Zertifikat hinzufügen aus, wie im Bild dargestellt.



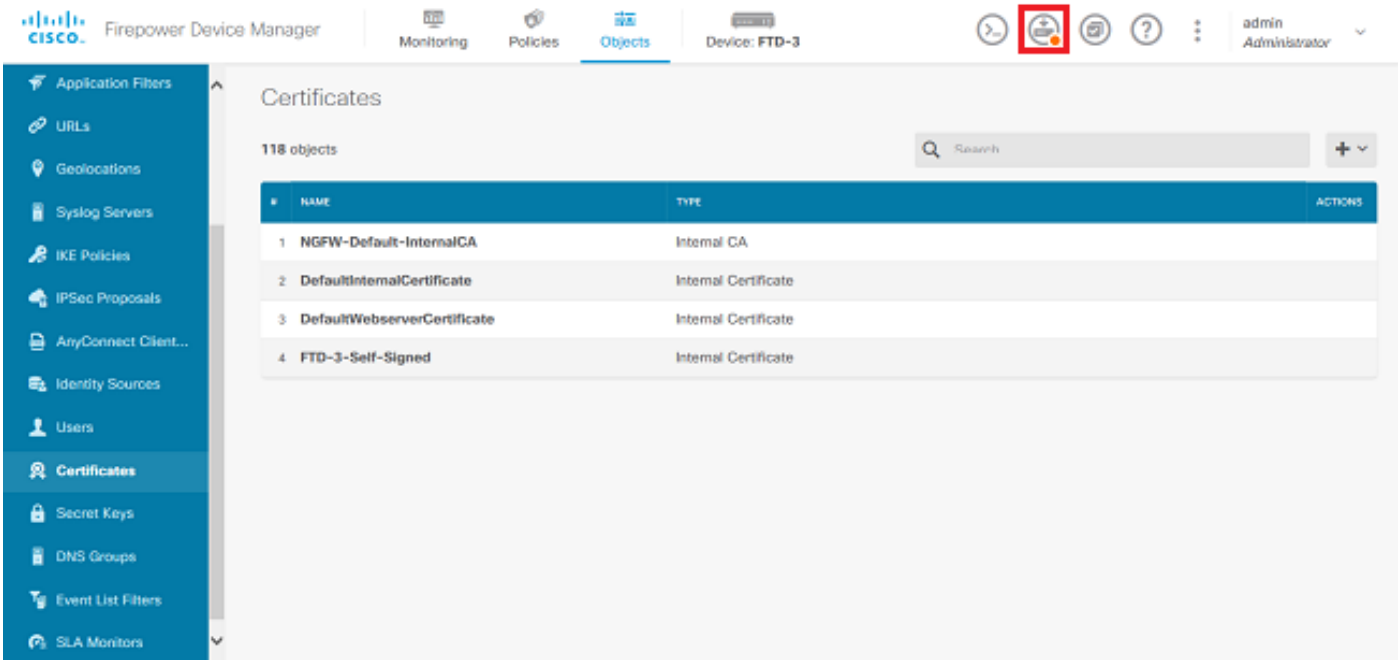
2. Wählen Sie Selbstsigniertes Zertifikat im Popup-Fenster, wie im Bild gezeigt.



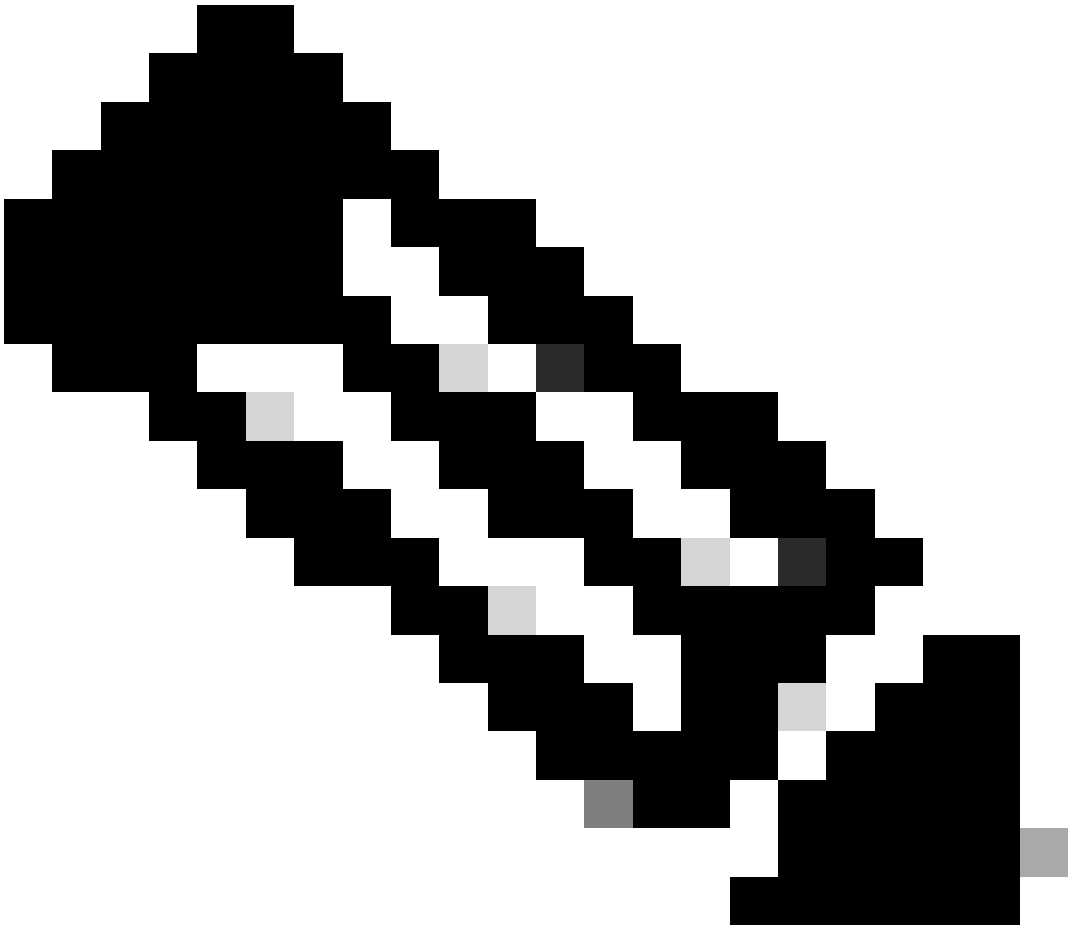
3. Geben Sie einen Namen für den Vertrauenspunkt an, und füllen Sie dann die Felder für den eindeutigen Betreffnamen aus. Das Feld Common Name kann mindestens hinzugefügt werden. Dies kann mit dem vollqualifizierten Domänennamen (FQDN) oder der IP-Adresse des Dienstes übereinstimmen, für den das Zertifikat verwendet wird. Klicken Sie anschließend auf Speichern.



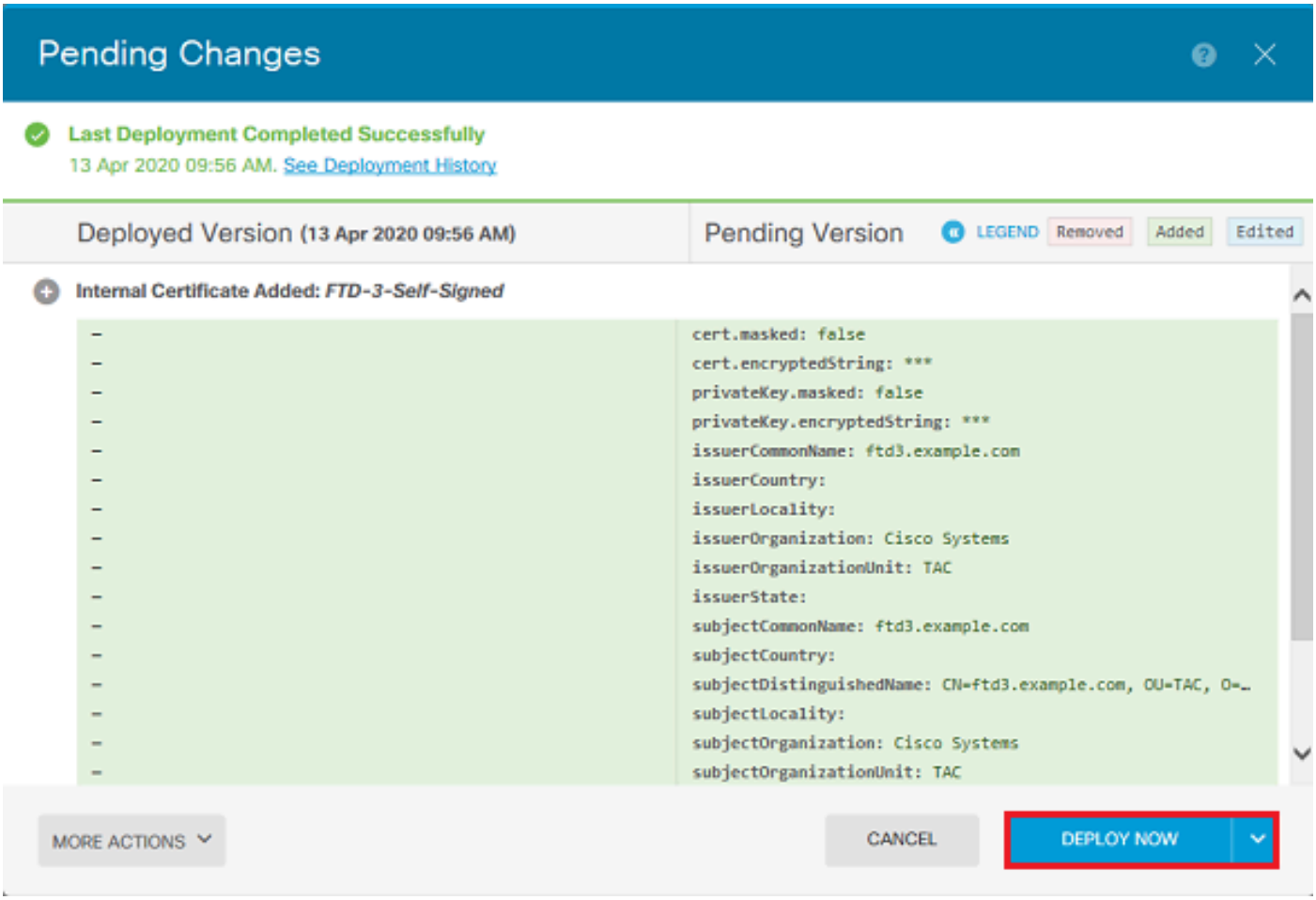
4. Klicken Sie auf die Schaltfläche Ausstehende Änderungen oben rechts auf dem Bildschirm, wie in der Abbildung dargestellt.



5. Klicken Sie auf die Schaltfläche Jetzt bereitstellen.



Hinweis: Nach Abschluss der Bereitstellung ist das Zertifikat erst dann in der CLI sichtbar, wenn es einen Dienst gibt, der es wie AnyConnect verwendet, wie im Abbild dargestellt.



Manuelle Registrierung

Die manuelle Registrierung kann verwendet werden, um ein von einer vertrauenswürdigen Zertifizierungsstelle ausgestelltes Zertifikat zu installieren. OpenSSL oder ein ähnliches Tool können verwendet werden, um den privaten Schlüssel und den CSR zu generieren, der für den Empfang eines CA-signierten Zertifikats erforderlich ist. Diese Schritte umfassen allgemeine OpenSSL-Befehle zum Generieren des privaten Schlüssels und der CSR sowie die Schritte zum Installieren des Zertifikats und des privaten Schlüssels nach dem Erhalt.

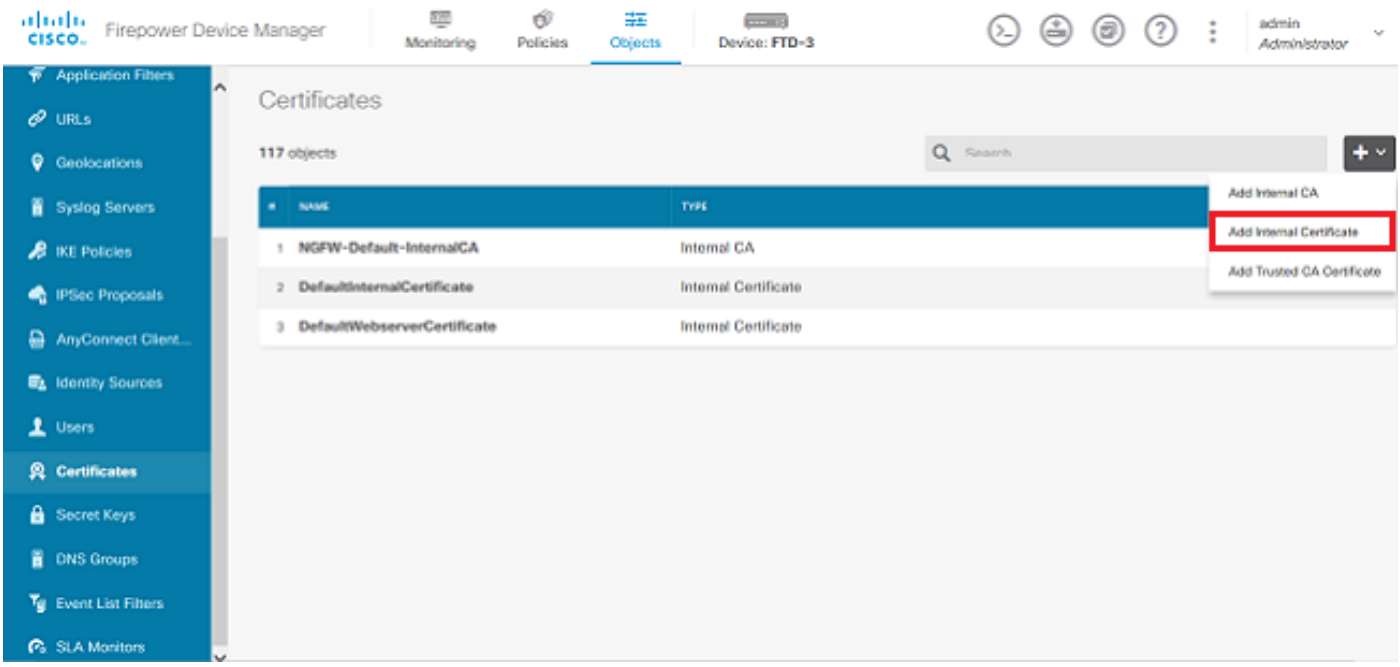
1. Generieren Sie mit OpenSSL oder einer ähnlichen Anwendung einen privaten Schlüssel und eine CSR-Anforderung (Certificate Signing Request). Dieses Beispiel zeigt einen 2048-Bit-RSA-Schlüssel mit dem Namen private.key und einen CSR mit dem Namen ftd3.csr, der in OpenSSL erstellt wird.

```
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'
```

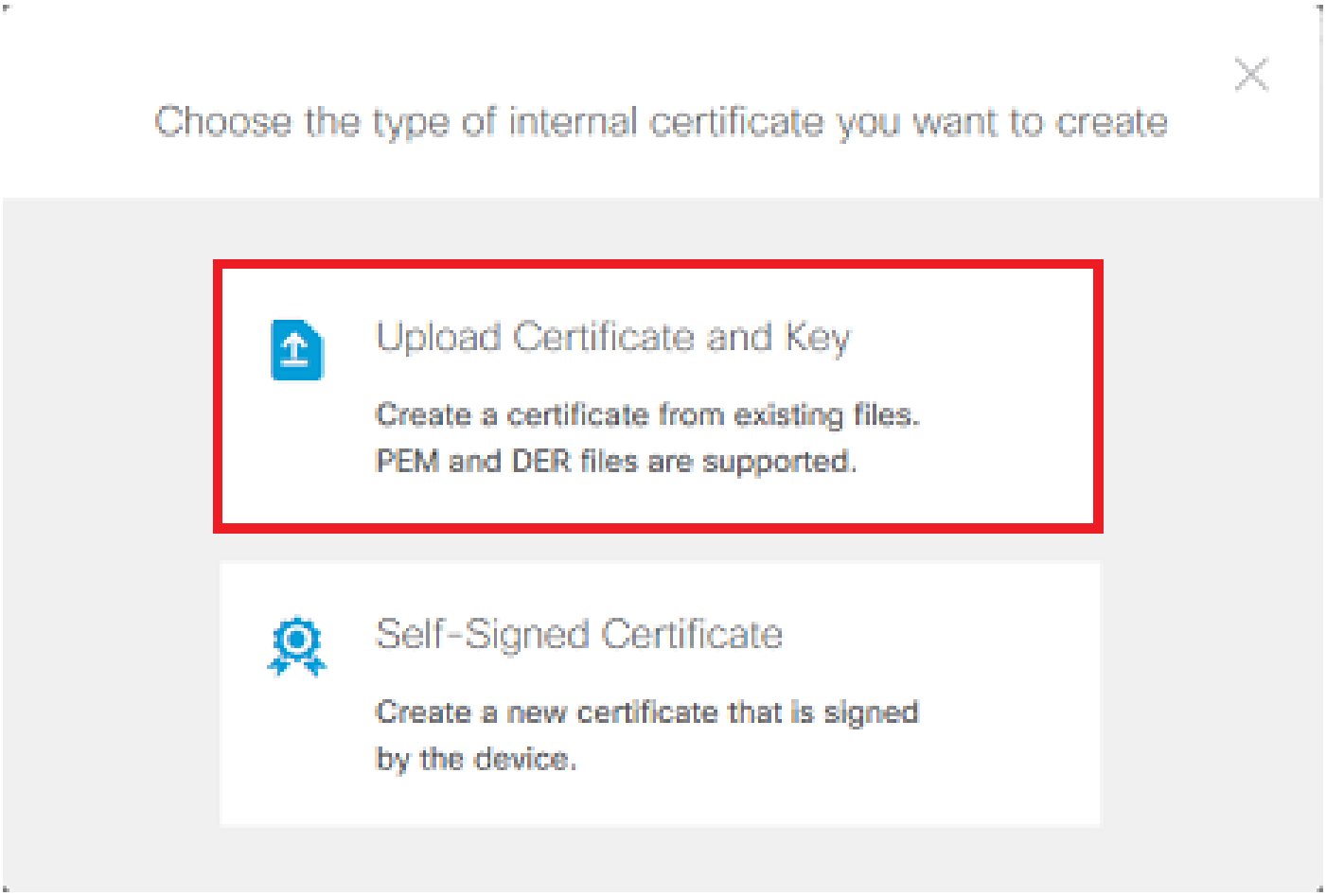
```
-----
You are about to be asked to enter information that is incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', 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. Kopieren Sie den erstellten CSR, und senden Sie ihn an eine Zertifizierungsstelle. Nach dem Signieren des CSR wird ein Identitätszertifikat bereitgestellt.

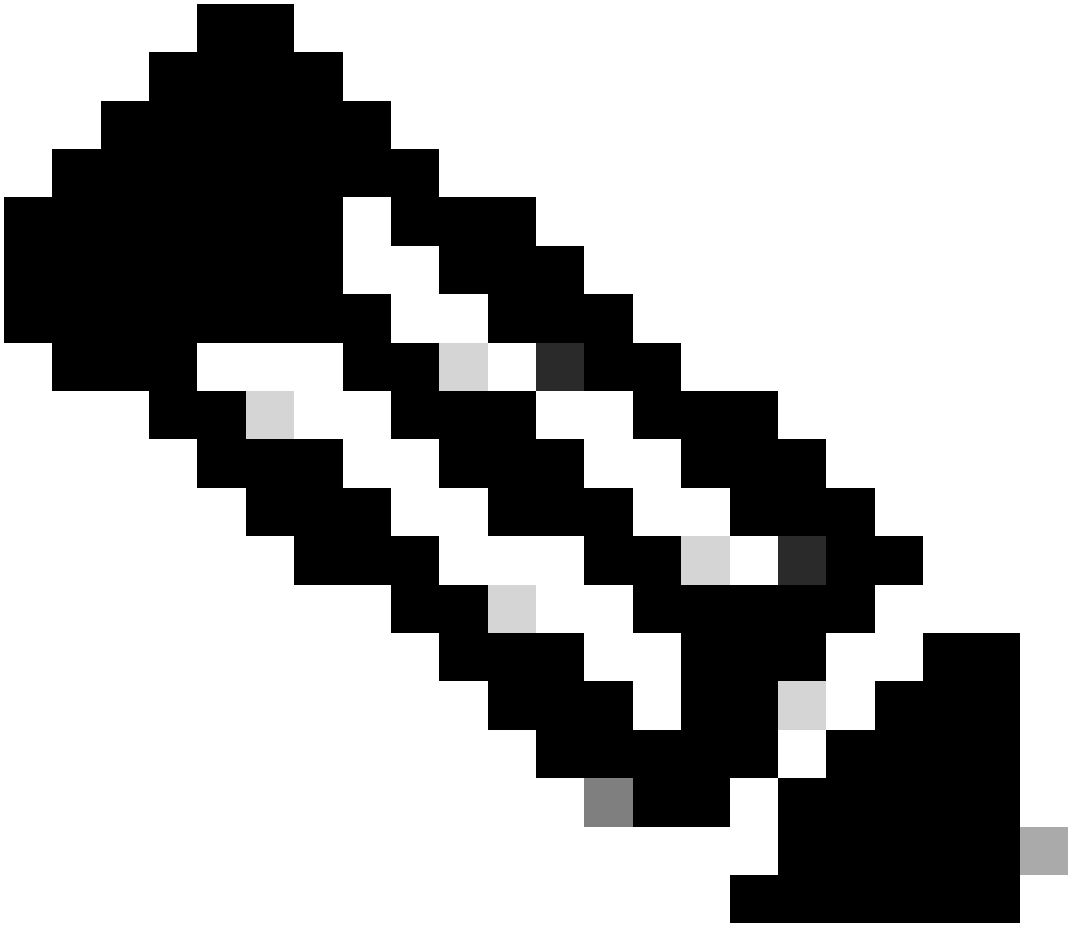
3. Navigieren Sie zu Objekte > Zertifikate. Klicken Sie auf das Symbol +, und wählen Sie dann Internes Zertifikat hinzufügen aus, wie im Bild dargestellt.



4. Wählen Sie im Popup-Fenster Zertifikat und Schlüssel hochladen, wie im Bild dargestellt.

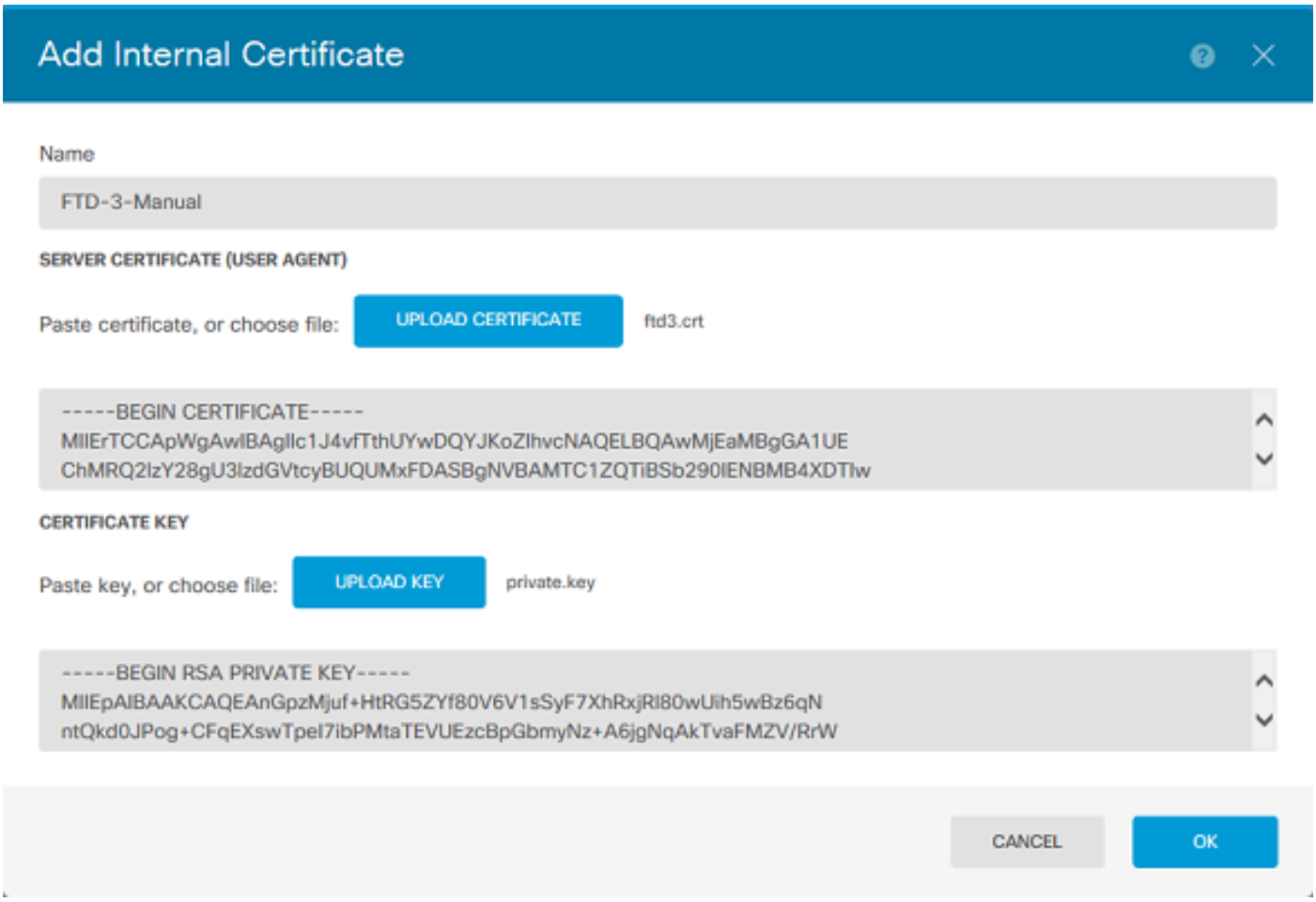


5. Geben Sie einen Namen für den Vertrauenspunkt an, und laden Sie dann das Identitätszertifikat und den privaten Schlüssel im PEM-Format (Privacy Enhanced Mail) hoch, oder kopieren Sie sie, und fügen Sie sie ein. Wenn die Zertifizierungsstelle das Zertifikat und den Schlüssel zusammen in einer einzigen PKCS12 bereitgestellt hat, navigieren Sie zu dem Abschnitt Extracting Identity certificate and private key from PKCS12 file weiter unten in diesem Dokument, um sie zu trennen.

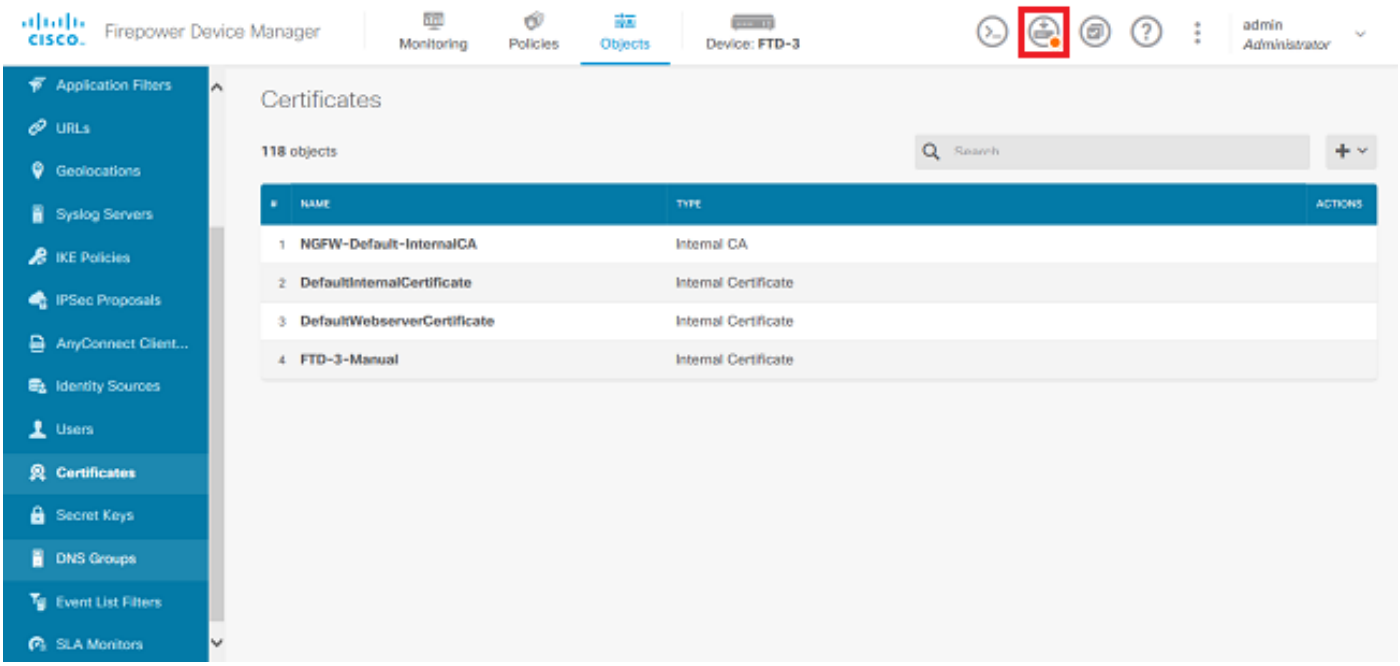


Hinweis: Die Dateinamen dürfen keine Leerzeichen enthalten, da sie von FDM nicht akzeptiert werden. Außerdem darf der private Schlüssel nicht verschlüsselt werden.

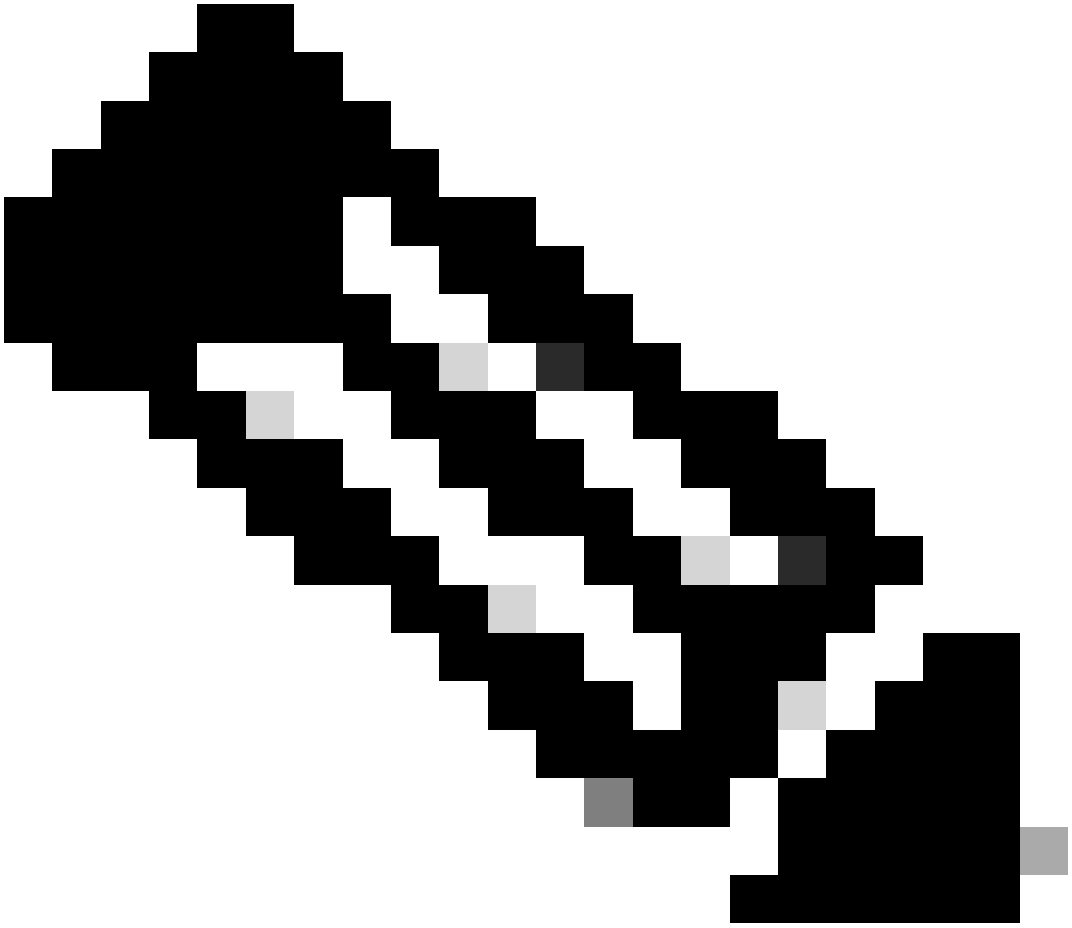
Klicken Sie auf OK, wenn Sie wie im Bild dargestellt fertig sind.



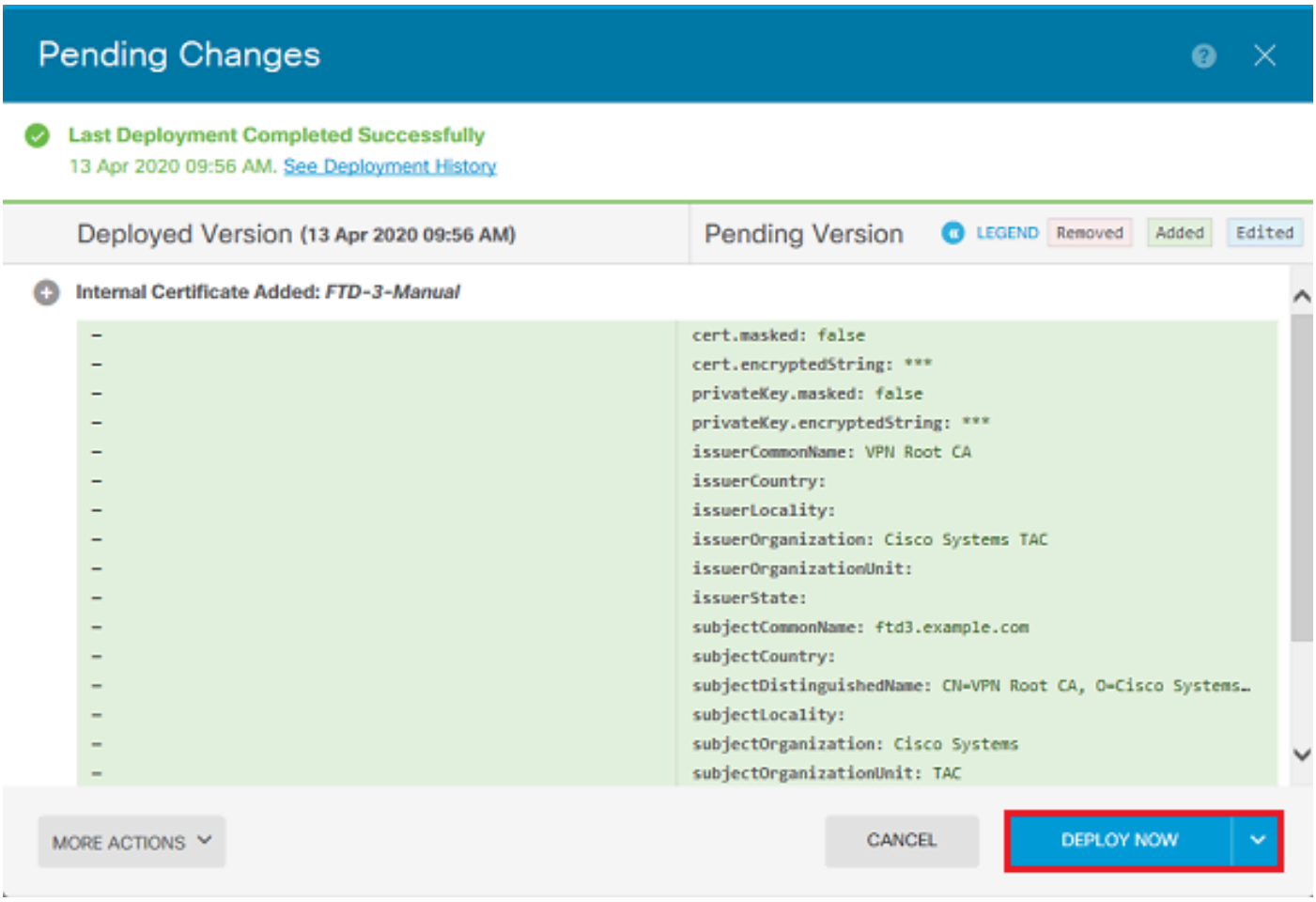
6. Klicken Sie auf die Schaltfläche Ausstehende Änderungen oben rechts auf dem Bildschirm, wie in der Abbildung dargestellt.



7. Klicken Sie auf die Schaltfläche Jetzt bereitstellen.



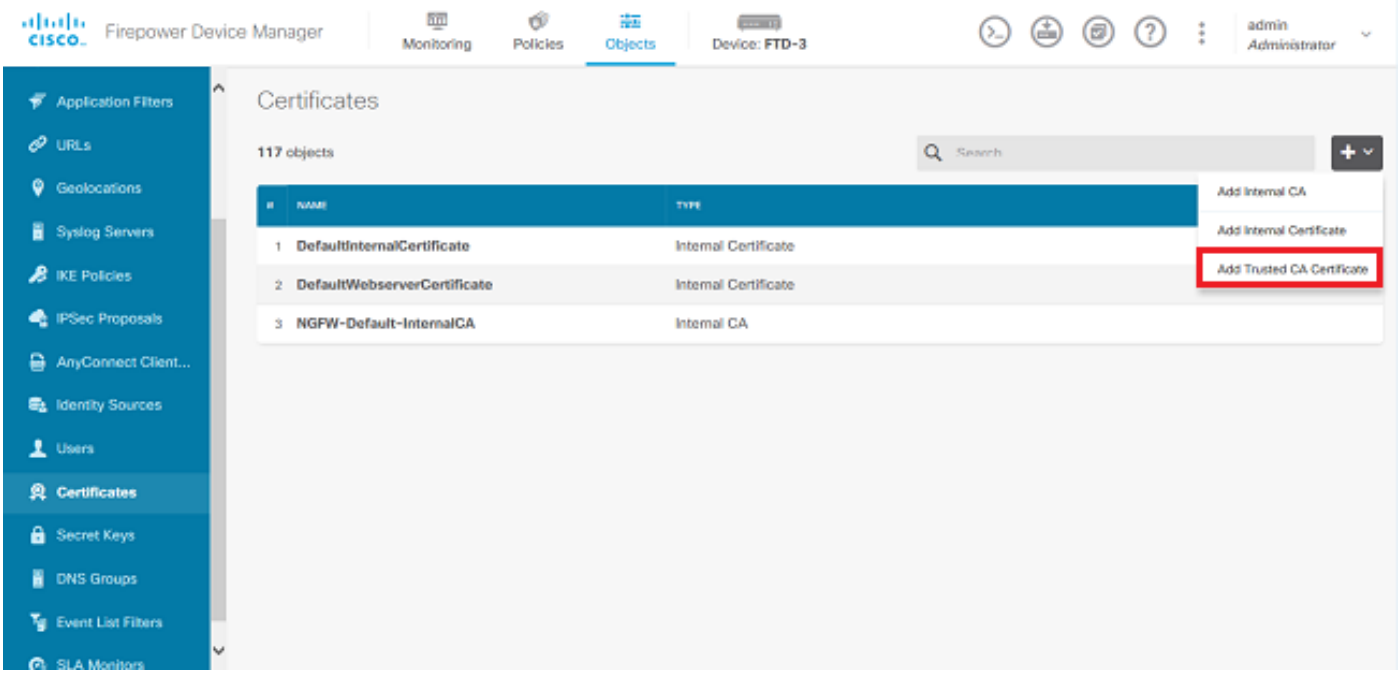
Hinweis: Nach Abschluss der Bereitstellung ist das Zertifikat erst dann in der CLI sichtbar, wenn es einen Dienst gibt, der es wie AnyConnect verwendet, wie im Abbild dargestellt.



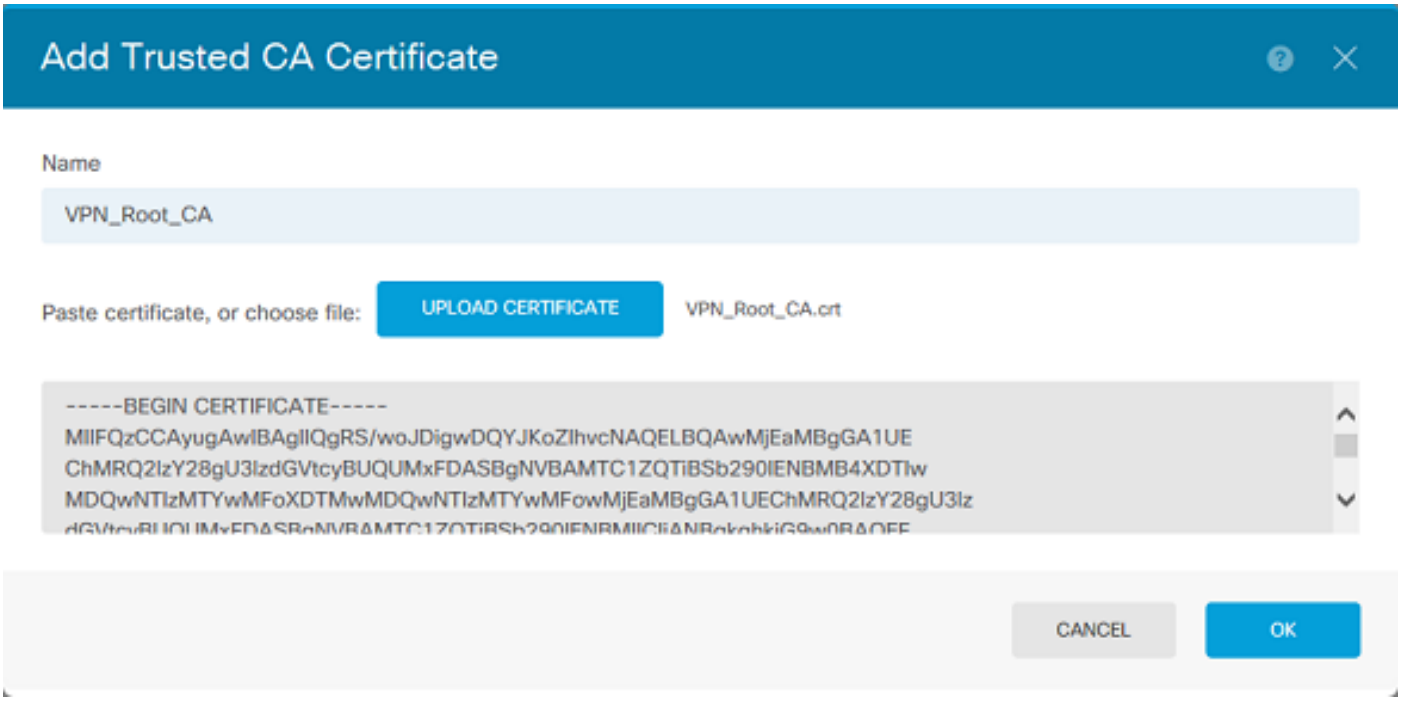
Installation des vertrauenswürdigen Zertifizierungsstellenzertifikats

Wenn Sie ein vertrauenswürdiges Zertifizierungsstellenzertifikat installieren, ist es erforderlich, um Benutzer oder Geräte, die dem FTD Identitätszertifikate vorlegen, erfolgreich zu authentifizieren. Beispiele hierfür sind die AnyConnect-Zertifikatauthentifizierung und die S2S-VPN-Zertifikatauthentifizierung. In diesen Schritten wird beschrieben, wie Sie einem Zertifizierungsstellenzertifikat vertrauen, damit von dieser Zertifizierungsstelle ausgestellte Zertifikate ebenfalls vertrauenswürdig sind.

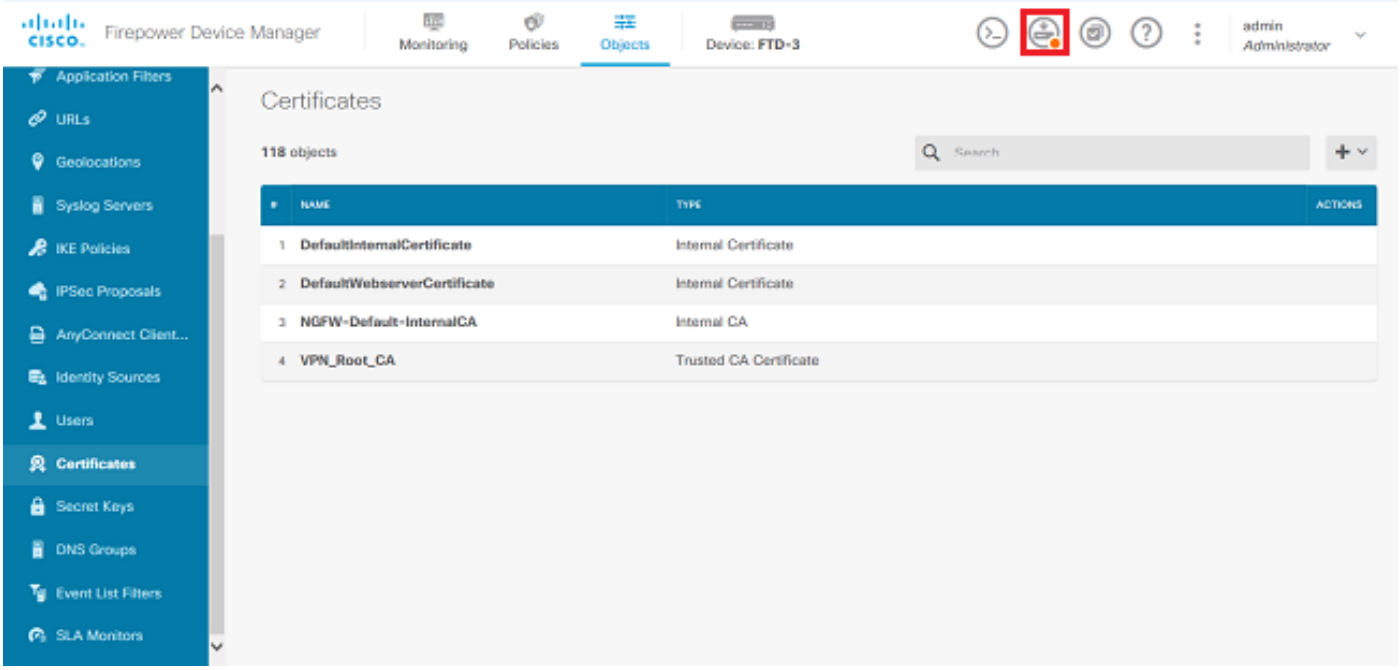
1. Navigieren Sie zu Objekte > Zertifikate. Klicken Sie auf das Symbol +, und wählen Sie dann Vertrauenswürdiges Zertifizierungsstellenzertifikat hinzufügen aus, wie im Bild gezeigt.



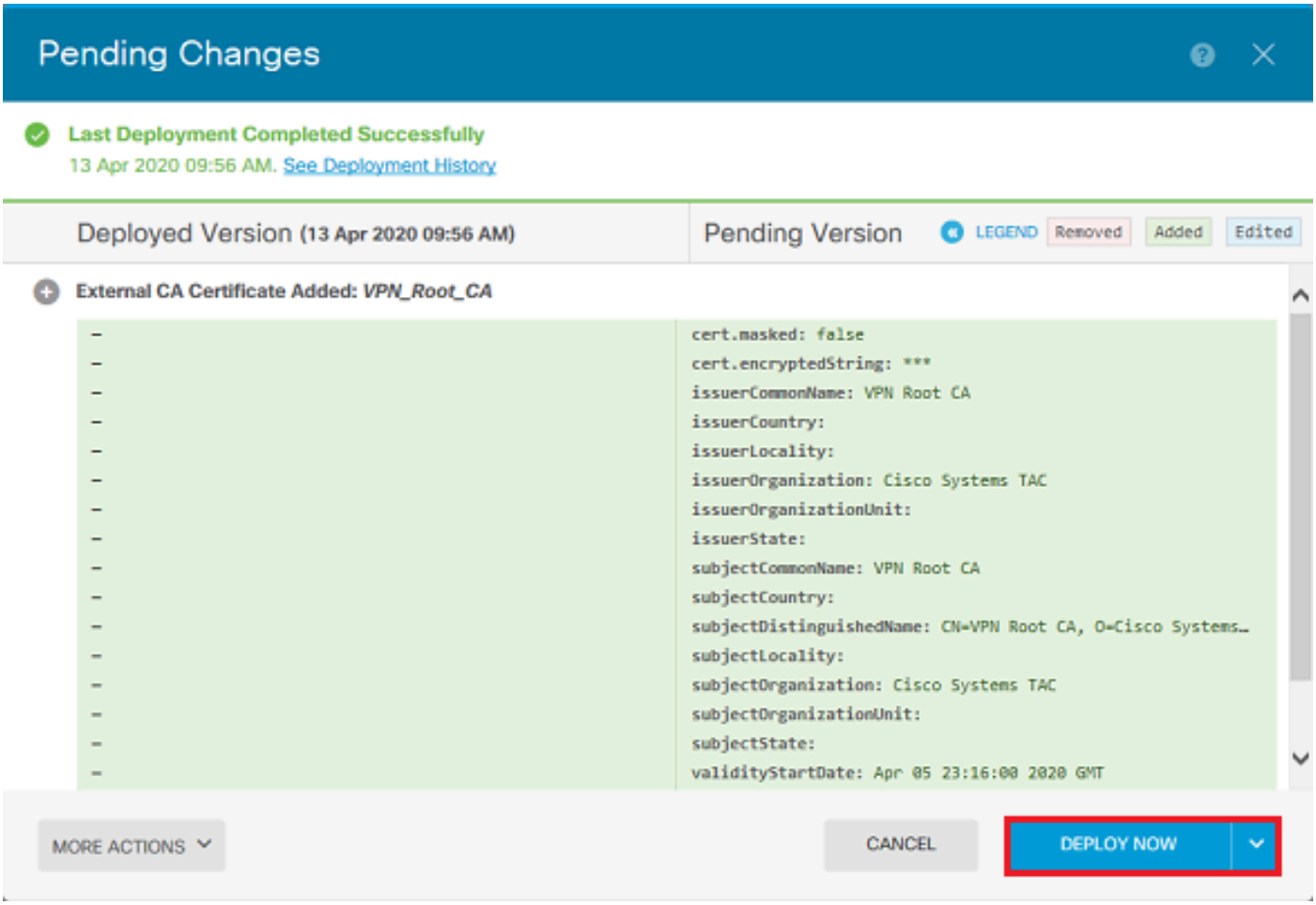
2. Geben Sie einen Namen für den Vertrauenspunkt an. Laden Sie das CA-Zertifikat dann hoch, oder kopieren Sie es, und fügen Sie es im PEM-Format ein. Klicken Sie auf OK, wenn Sie wie im Bild dargestellt fertig sind.



3. Klicken Sie auf die Schaltfläche Ausstehende Änderungen oben rechts auf dem Bildschirm, wie in der Abbildung dargestellt.



4. Klicken Sie auf die Schaltfläche Jetzt bereitstellen, wie in der Abbildung dargestellt.



Erneuerung des Zertifikats

Bei der Erneuerung eines von FDM verwalteten FTD werden das vorherige Zertifikat und möglicherweise der private Schlüssel ersetzt. Wenn Sie den ursprünglichen CSR und privaten

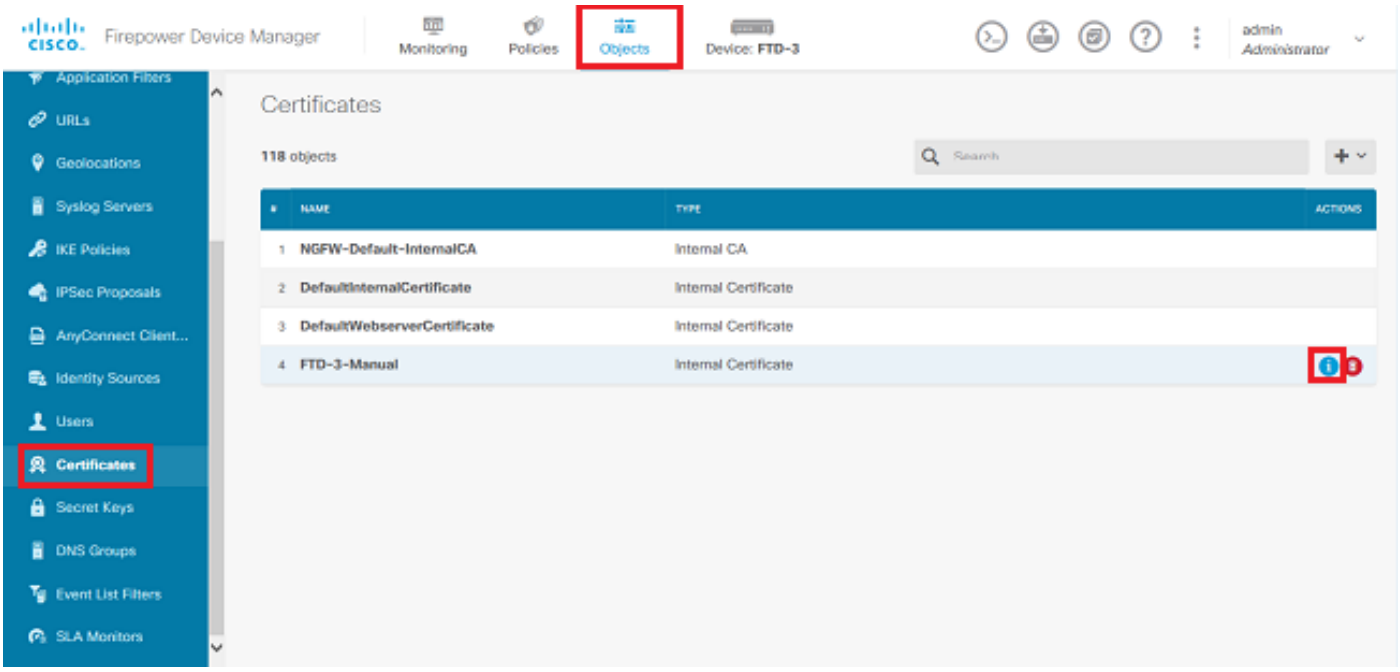
Schlüssel nicht zum Erstellen des ursprünglichen Zertifikats verwendet haben, müssen Sie einen neuen CSR und privaten Schlüssel erstellen.

1. Wenn Sie den ursprünglichen CSR und privaten Schlüssel haben, kann dieser Schritt ignoriert werden. Andernfalls müssen ein neuer privater Schlüssel und ein CSR erstellt werden. Verwenden Sie OpenSSL oder eine ähnliche Anwendung, um einen privaten Schlüssel und eine CSR-Anfrage zu erstellen. Dieses Beispiel zeigt einen 2048-Bit-RSA-Schlüssel mit dem Namen private.key und einen CSR mit dem Namen ftd3.csr, der in OpenSSL erstellt wird.

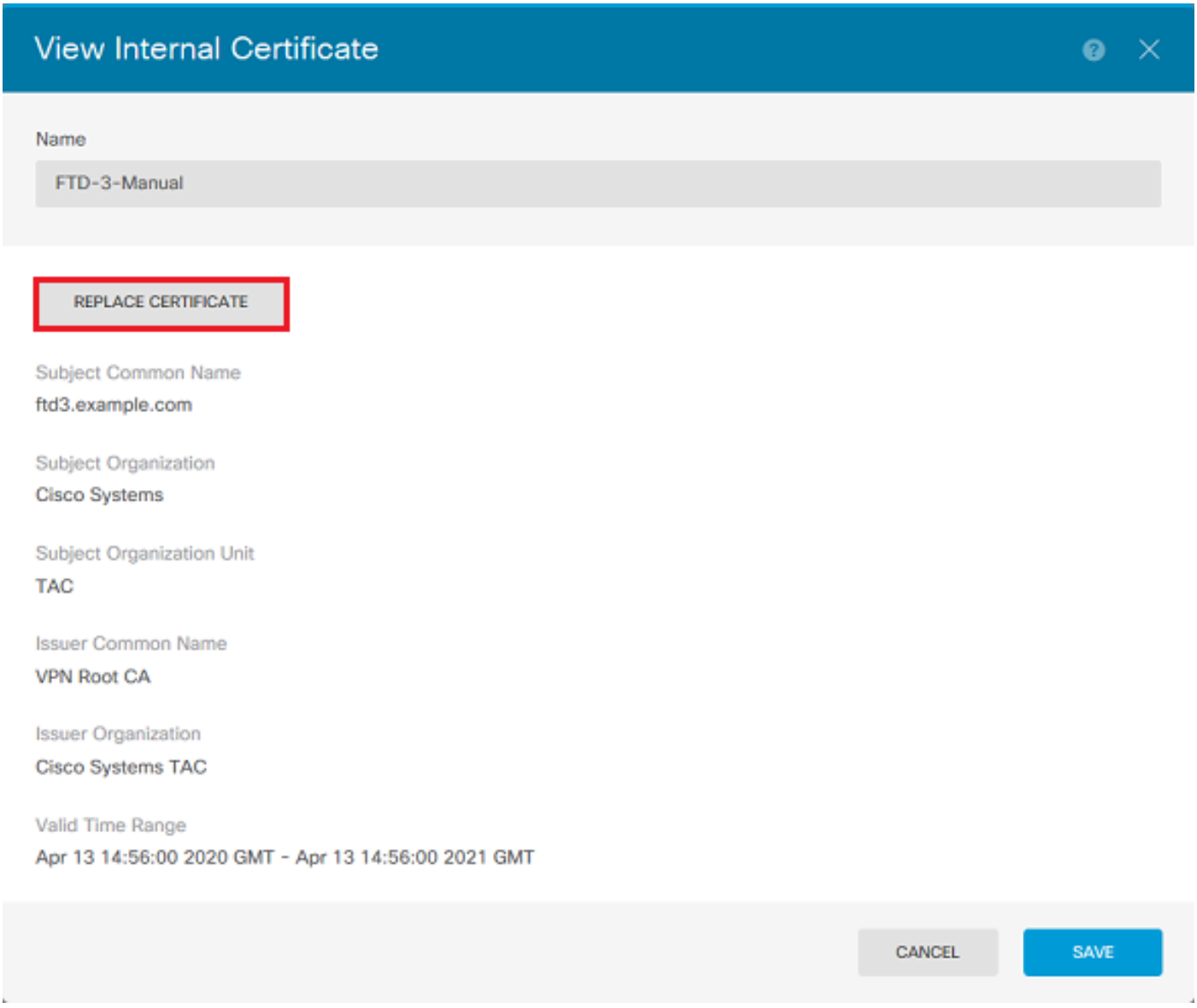
```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
.....................................+++
.....................................................................+++
writing new private key to 'private.key'
-----
You are about to be asked 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. Senden Sie die erstellte CSR oder die ursprüngliche CSR an eine Zertifizierungsstelle. Nach der Signatur des CSR wird ein neues Identitätszertifikat bereitgestellt.

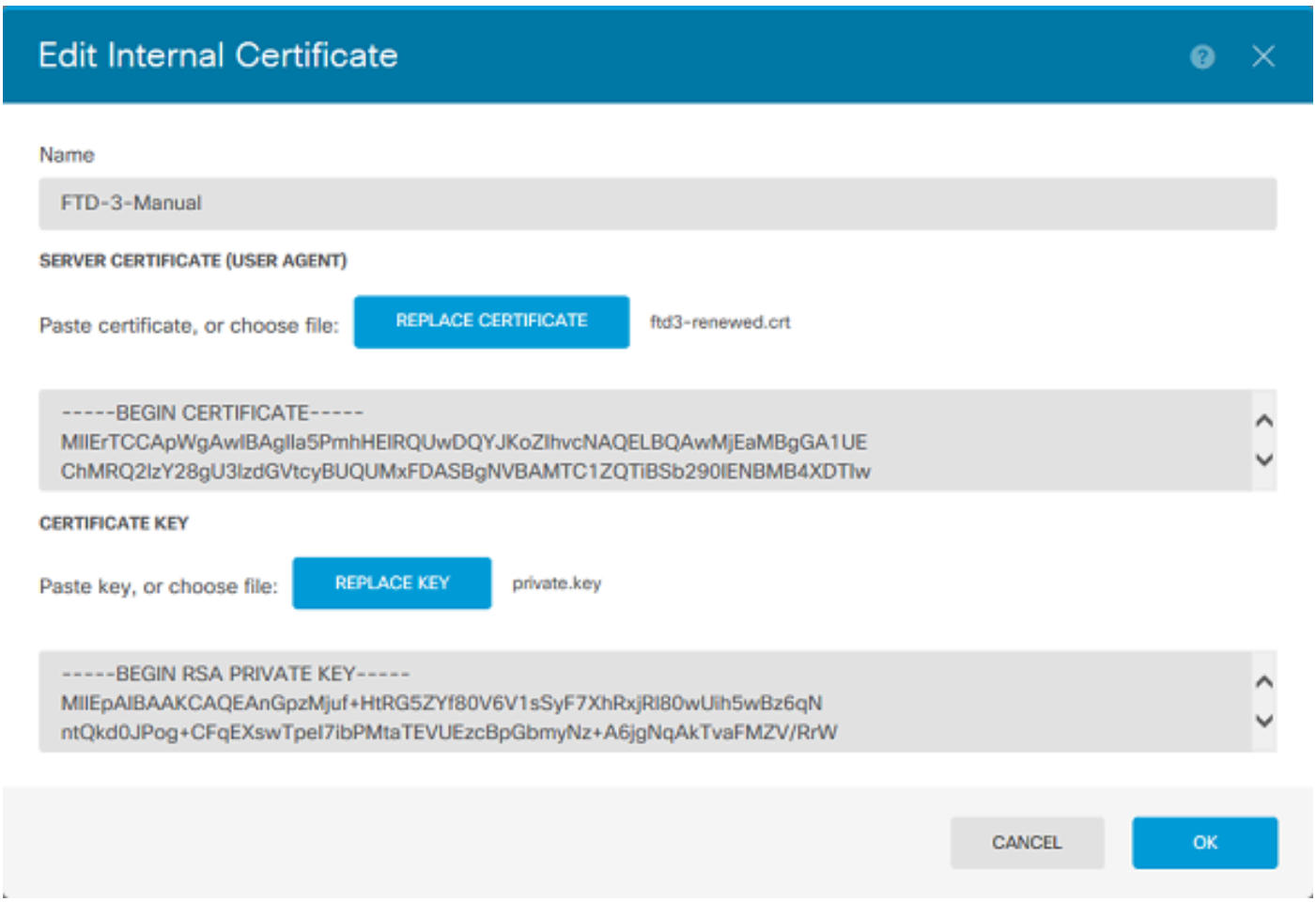
3. Navigieren Sie zu Objekte > Zertifikate. Bewegen Sie den Mauszeiger über das zu verlängernde Zertifikat, und klicken Sie auf die Schaltfläche Anzeigen, wie im Bild dargestellt.



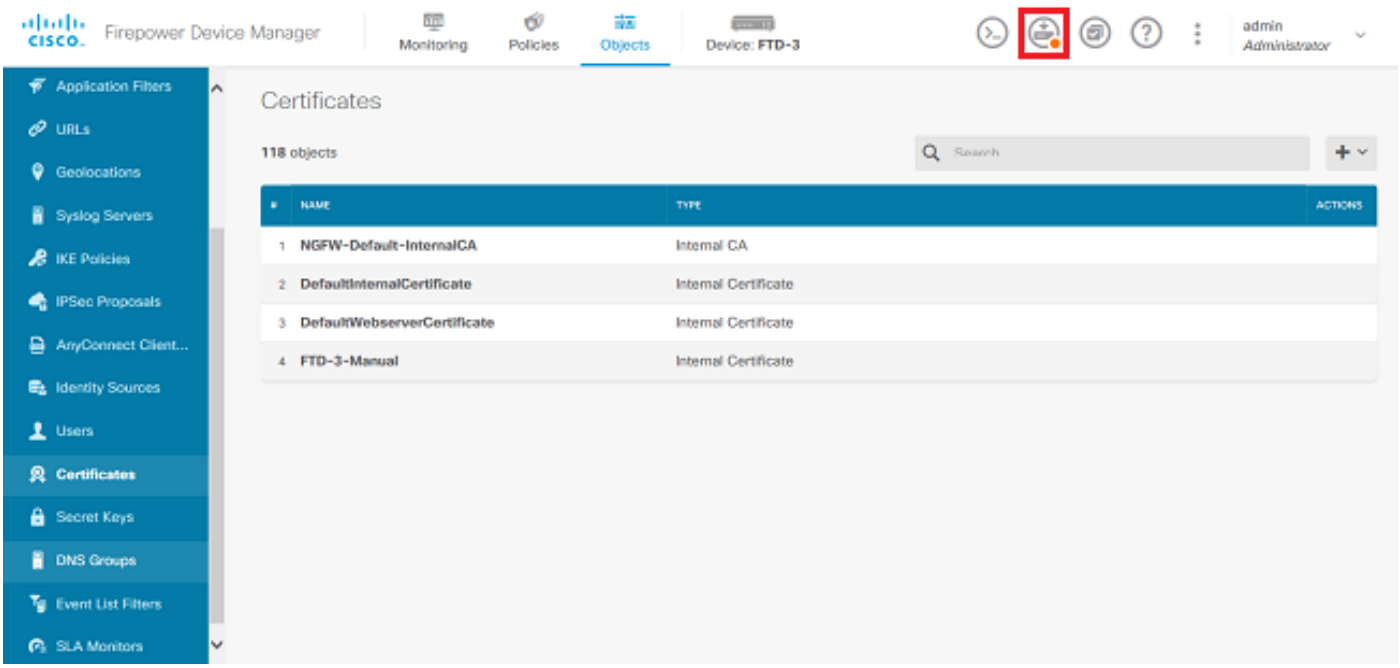
4. Klicken Sie im Popup-Fenster auf Zertifikat ersetzen, wie im Bild dargestellt.



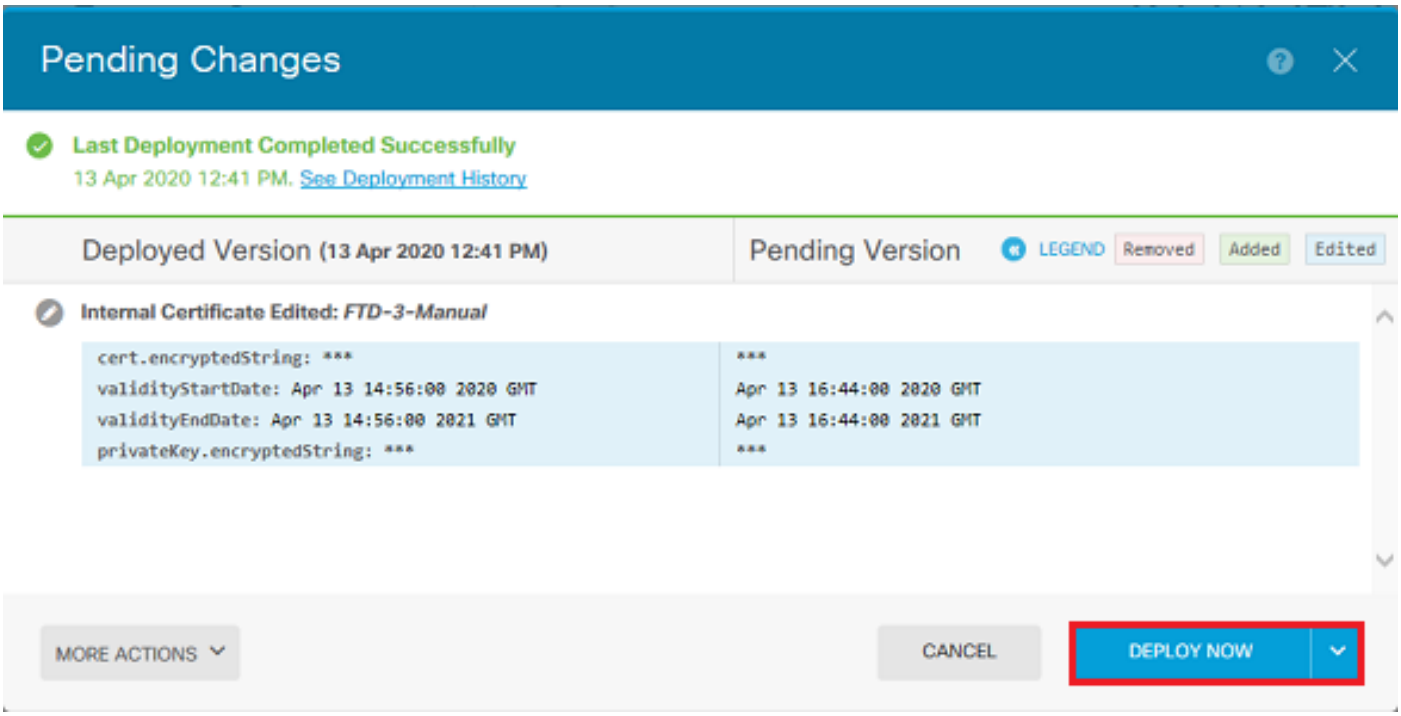
5. Laden Sie das Identitätszertifikat und den privaten Schlüssel im PEM-Format hoch, oder kopieren Sie sie, und fügen Sie sie ein. Klicken Sie auf OK, wenn Sie wie im Bild dargestellt fertig sind.



6. Klicken Sie auf die Schaltfläche Ausstehende Änderungen oben rechts auf dem Bildschirm, wie in der Abbildung dargestellt.



7. Klicken Sie auf die Schaltfläche Jetzt bereitstellen, wie in der Abbildung dargestellt.



Allgemeine OpenSSL-Vorgänge

Identitätszertifikat und privaten Schlüssel aus PKCS12-Datei extrahieren

Ein Administrator kann eine PKCS12-Datei erhalten, die in das FTD importiert werden muss. FDM unterstützt derzeit nicht den Import von PKCS12-Dateien. Um die in der PKCS12-Datei enthaltenen Zertifikate und privaten Schlüssel zu importieren, müssen die einzelnen Dateien mithilfe eines Tools wie OpenSSL aus der PKCS12 extrahiert werden. Sie benötigen den Passcode zur Verschlüsselung des 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+HtRG5ZYf80V6V1s
SyF7XhRxjRl8OwUih5wBz6qNntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZOIcpzVqL6hOziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS5O
QpQDTgvIiD1bYpPiWKpSOg1PZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZa
```

```
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
YRQ1ft1FxHpn4zMkjI2PxOyam/bROnOFoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
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+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-----
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/N0WlA73x47R4T6+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/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 ist eine PKCS12-Datei, die entpackt werden muss.

In diesem Beispiel werden drei separate Dateien erstellt:

Einen für das Identitätszertifikat. Sie können feststellen, dass es sich um das Identitätszertifikat gemäß dem Betreff=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com handelt.

```
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+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/U7170n/FbAmdYwRYgMAE4
RWfBpOvoNzn97cG+qzogo7j/OkTfYu3O9DzdU3uy+R8JJkBrerktrZR7w7OfP61O
IAs86N5Zb18U14Gfc9mOeXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2PxOyam/bROnOFoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJFOiVOGV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfpMwTiT47I
ng==
-----END CERTIFICATE-----
```

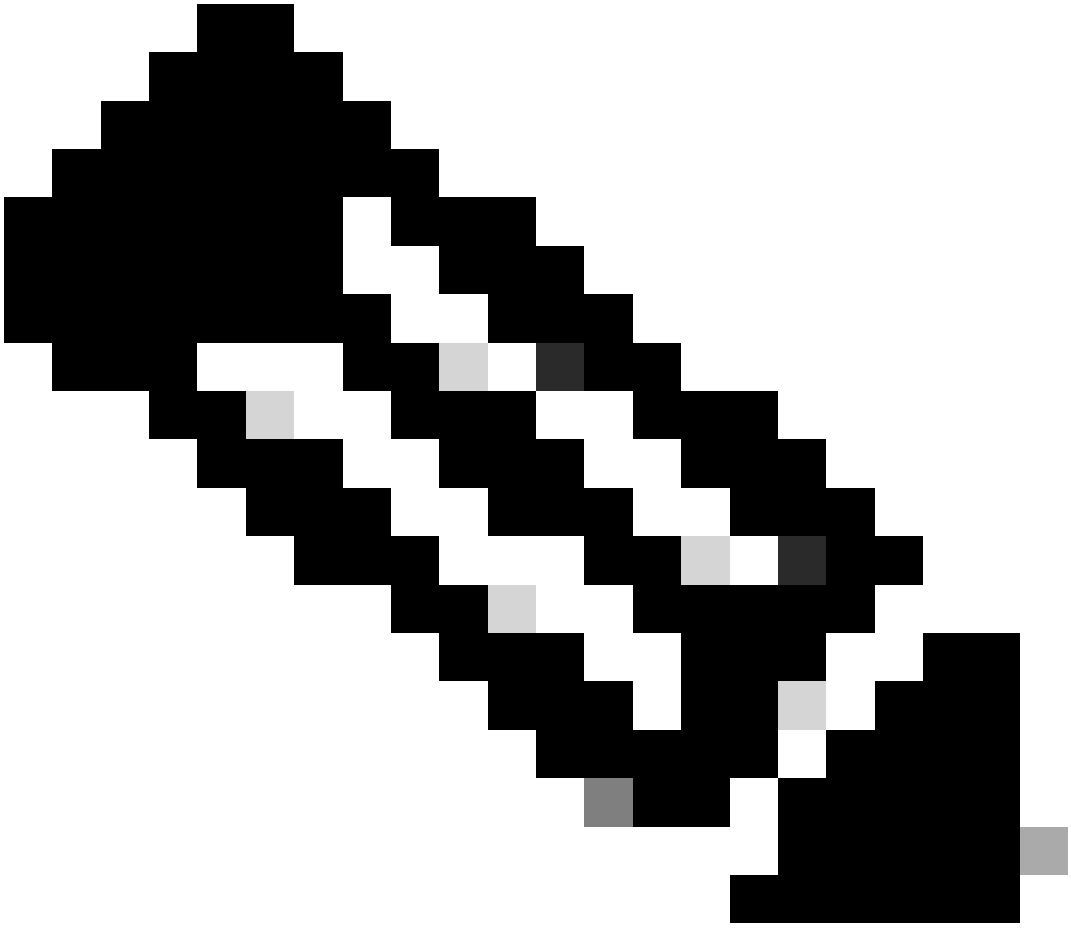
Eine für das ausstellende Zertifizierungsstellenzertifikat. Sie erkennen, dass es sich um das Identitätszertifikat handelt, das der Betreffzeile entspricht=/O=Cisco Systems TAC/CN=VPN Root CA. Dies ist derselbe Wert wie der Aussteller im Identitätszertifikat, der zuvor angezeigt wurde:

```
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+8GbOY1WEHtohgNGjPOOq8wnKQuOC47Ft1UMpdSwUsMMze0X43dyp/WoZtLW
4v/Pn/NibE3aoPOaMhIo4CdwSBHZOgVag4INqVsuFX1uPKD25WhrlO9LQ93P/sN3
FhoAh98HKOcuQ64Ua3AaShdzornD+G2J2pd1Nf1DahlzlskIMtlURSWdLjsHLKft
JqSOoLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/lyNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cxl1jINOLdB+/jQqkfzmx9ziB1PXnIshNRbflLLrNfdDO9agqQsvsC
AwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDKC4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDKC4wCwYDVR0PBAQD
AgEGMA0GCSqGSIb3DQEBCwUAA4ICAQC6B+Y3obatEZqv0RQz1MS6oOumCgNWGi8d
kcRDxkY2F+zw3pBFa54Sin1OfRPJvZvLNJV5OdXmvH5luh6KJDMVrLMWNiSgI7Tn
OipqKraokS2Oo0STwQ7Q9Wk1xCrwxMfTuDJFMe8OqabFAU557O5PDXPtFEutn0xz
Ou8VMLBRy+gDc+0WARsjFj+0gUOc2Wj3gQ81GlyoPYgufWRnztN5rQxWzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AydsGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p7O2FZly5lxuzuA/wPnR89HiIkSF13OMTpnOIl3d6dO7s3bwyNja8JikYTCflle5
2CSsz4Cn/BlwfWyAcLN3HxUjG4Ev2818fWWpkYmuxujpKDFFzFOskpKAK53tNKPf
pn4+w5FyLo18oOAydtPoKjYkDqbvG/SRPbt92mdTIF7E6J+o8J6OV3YL+IyrZ+u0
MYqPd45Oi4cgHdMFICAndN3PYScrrGYHawfVxp+R+G4dTJWdMvthh3ftSOmkiKJ8
m1NH7WYST1kYcTbcokZiOIcZa+VVv5UOLIt/hDOVG7xqZOlpMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpxTIsmDv9rQzxBjuCyKn+23FkkUhFJtOD989UUypO8H9vDoJr
yzm9JOpMrg==
-----END CERTIFICATE-----
```

Und eine für den privaten Schlüssel:

```
-----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/NrbN31HkP0wt7+1DFGFit1pTTGvOFchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG1l5NSslwKbTGiiwCYw0N8c09TXQbO4rMomFDAv8
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/PITvGzKr06o12/hHJtzXQ8eNPDJbvcD/okRRKZpmjH+ijp
FPD/WgQ/vmO9HdCWW3flhqceqfHff8ClCJYFLxsgZp4M3G+WyQTky4J8+6uTn/mj
yyZ5JCZdlt42haSNqU/ynioCjh5XY4m8WMZsOJBNPjKZiUX/vqVcc+/nodl7VRZy
ELk=
-----END ENCRYPTED PRIVATE KEY-----
```



Hinweis: Der private Schlüssel ist verschlüsselt, und FDM akzeptiert keine verschlüsselten privaten Schlüssel.

Um den privaten Schlüssel zu entschlüsseln, kopieren Sie den verschlüsselten privaten Schlüssel in eine Datei, und führen Sie dann den folgenden Befehl openssl aus:

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

- encrypted.key ist der Name der Datei, die den verschlüsselten privaten Schlüssel enthält.
- unencrypted.key ist der Name der Datei, die den unverschlüsselten Schlüssel hat.

Der unverschlüsselte private Schlüssel kann -----BEGIN RSA PRIVATE KEY----- anstelle von -----BEGIN ENCRYPTED PRIVATE KEY----- anzeigen, wie in diesem Beispiel gezeigt:

```
-----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+NgAA66TRn4qfkbpvTI98CeCUxiUPcbRmqZnYxCOfp
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-----
```

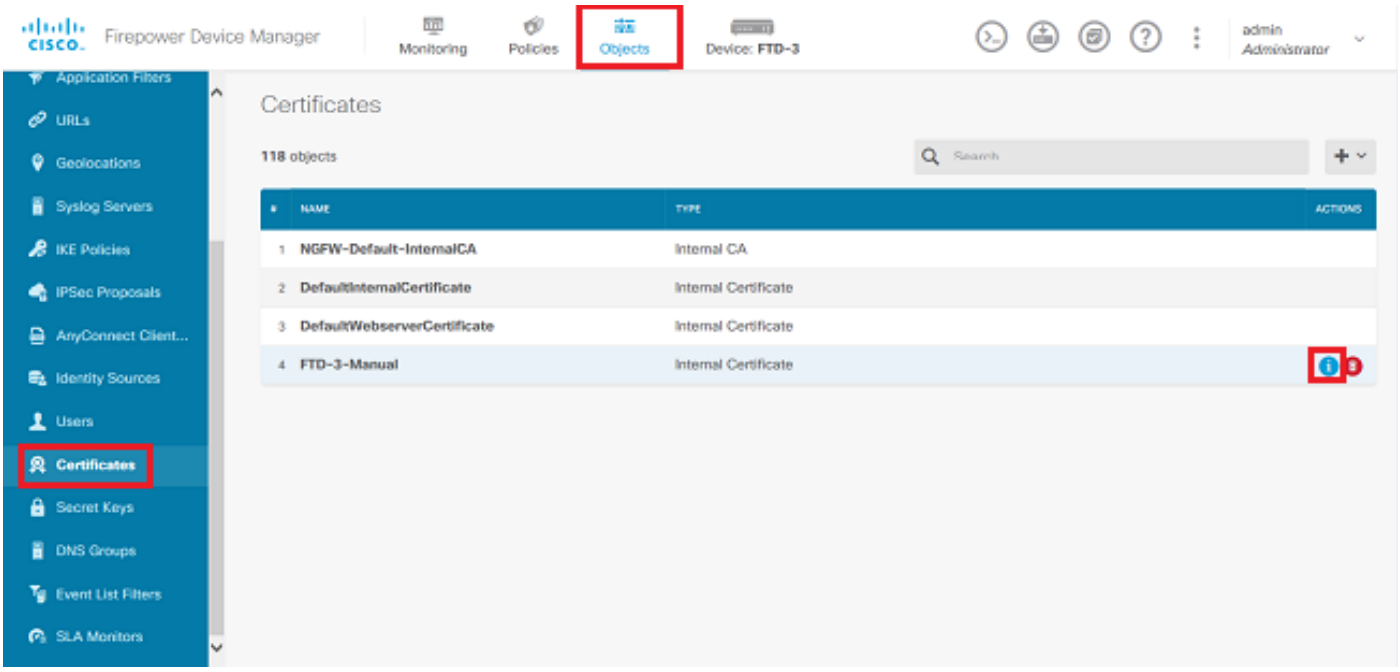
Nachdem der private Schlüssel unverschlüsselt wurde, können die Identitäts- und die private Schlüsseldatei hochgeladen, kopiert und mit Schritt 3 im zuvor erwähnten Abschnitt zur manuellen Registrierung in FDM eingefügt werden. Die ausstellende Zertifizierungsstelle kann mithilfe der zuvor erwähnten Schritte zur Installation des Zertifikats für vertrauenswürdige Zertifizierungsstellen installiert werden.

Überprüfung

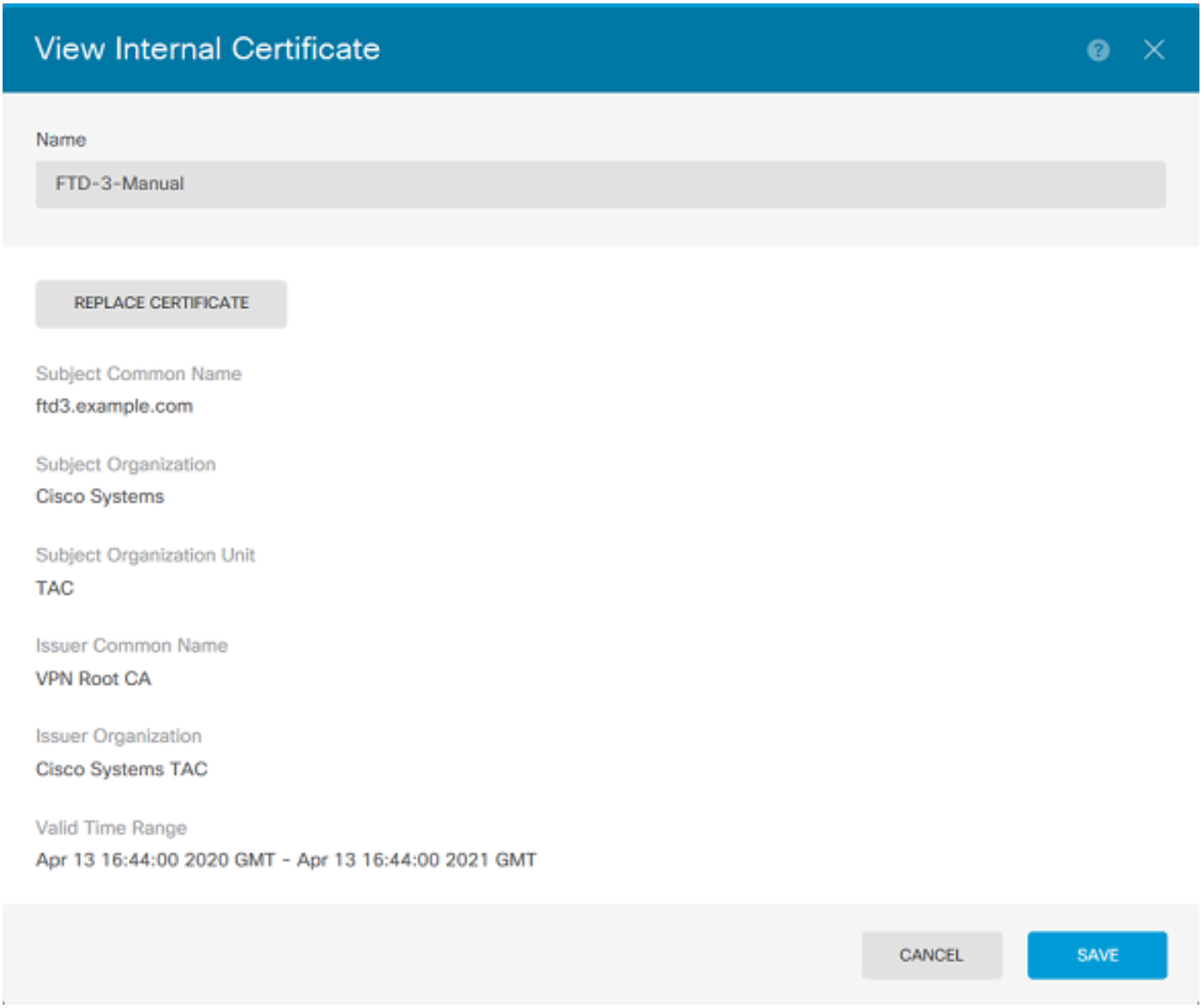
Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Installierte Zertifikate in FDM anzeigen

1. Navigieren Sie zu Objekte > Zertifikate. Bewegen Sie den Mauszeiger über das Zertifikat, das Sie überprüfen möchten, und klicken Sie auf die Schaltfläche Ansicht, wie im Bild dargestellt.



2. Das Popup-Fenster enthält zusätzliche Details zum Zertifikat, wie im Bild dargestellt.

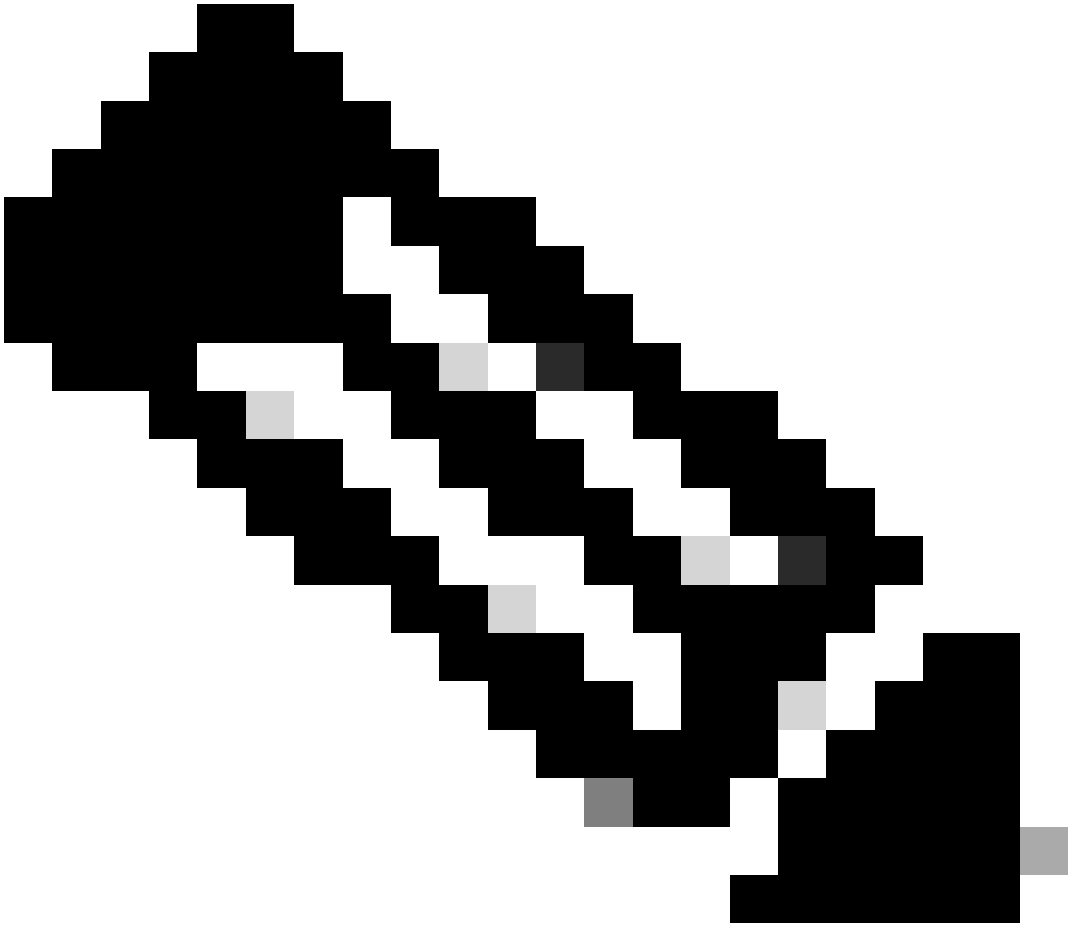


Installierte Zertifikate in CLI anzeigen

Sie können entweder die CLI-Konsole im FDM oder SSH im FTD verwenden und den Befehl show crypto ca-Zertifikate ausführen, um zu überprüfen, ob ein Zertifikat auf das Gerät angewendet wird, wie im Image gezeigt.

Beispiel:

```
> 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
```



Hinweis: Identitätszertifikate werden in der CLI nur angezeigt, wenn sie mit einem Dienst wie AnyConnect verwendet werden. Vertrauenswürdige Zertifizierungsstellenzertifikate werden angezeigt, sobald sie bereitgestellt wurden.

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Debug-Befehle

Im Falle eines Fehlers bei der SSL-Zertifikatsinstallation können nach dem Verbinden des FTD über SSH von der Diagnose-CLI aus Debugs ausgeführt werden: debug crypto ca 14

In älteren FTD-Versionen sind die folgenden Fehlerbehebungsschritte verfügbar und werden für die Fehlerbehebung empfohlen:

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 255

Häufige Probleme

ASA-exportierte PKCS12 importieren

Wenn Sie versuchen, das Identitätszertifikat und den privaten Schlüssel aus einer exportierten ASA PKCS12 in OpenSSL zu extrahieren, können Sie einen ähnlichen Fehler erhalten:

```
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
```

Um dies zu umgehen, muss die Datei pkcs12 zunächst in das DER-Format konvertiert werden:

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

Anschließend können die Schritte aus dem Abschnitt Extracting Identity certificate and private key from PKCS12 file weiter oben in diesem Dokument ausgeführt werden, um das Identitätszertifikat und den privaten Schlüssel zu importieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.