Installieren und Erneuern von Zertifikaten auf FTD, das von FMC verwaltet wird

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie selbstsignierte Zertifikate und Zertifikate, die von einer Zertifizierungsstelle eines Drittanbieters (Certificate Authority, CA) oder einer internen Zertifizierungsstelle signiert wurden, auf einem vom FirePOWER Management Center (FMC) verwalteten FirePOWER Threat Defense (FTD) installiert, vertrauen 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 Drittanbieter-Zertifizierungsstelle erforderlich.
- Beispiele für Drittanbieter von Zertifizierungsstellen sind Entrust, Geotrust, GoDaddy, Thawte und VeriSign.
- Vergewissern Sie sich, dass das 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:

- FMCv mit 6.5
- FTDv mit 6.5
- Für die Erstellung von PKCS12 wird OpenSSL verwendet

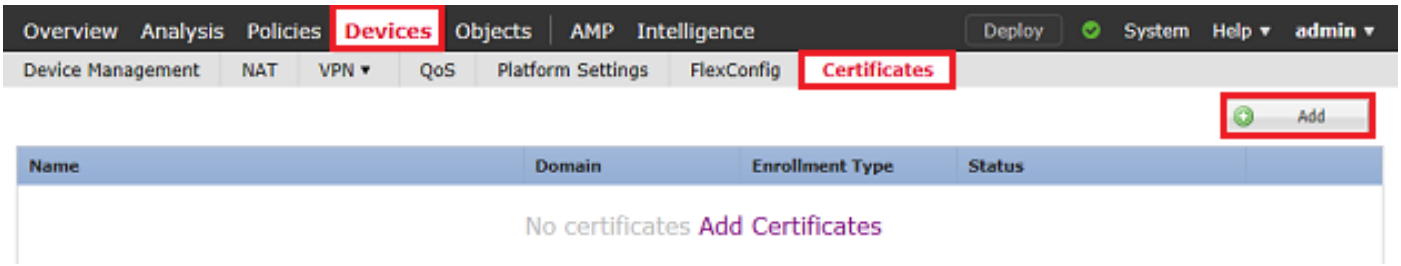
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfigurieren

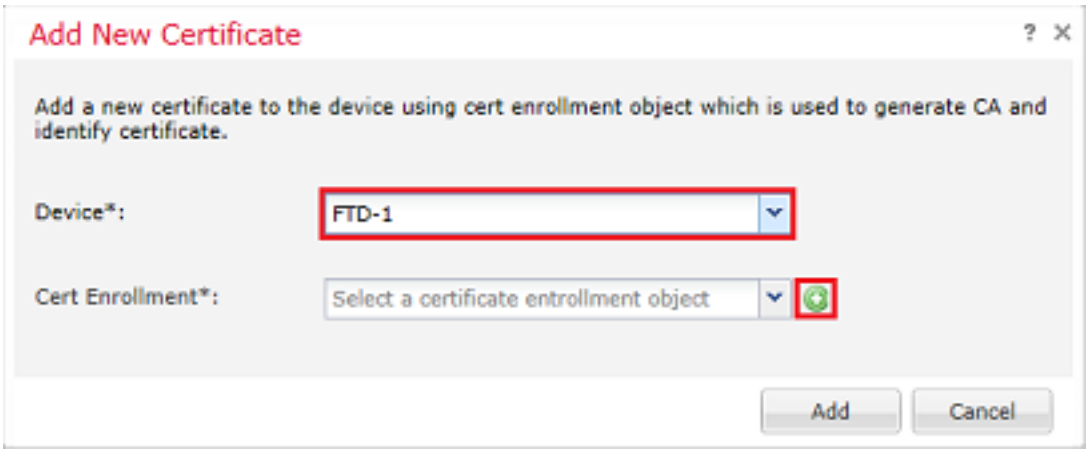
Installation des Zertifikats

Selbstsignierte Registrierung

1. Navigieren Sie zu **Geräte > Zertifikate**, und klicken Sie dann auf **Hinzufügen**, wie im Bild dargestellt.

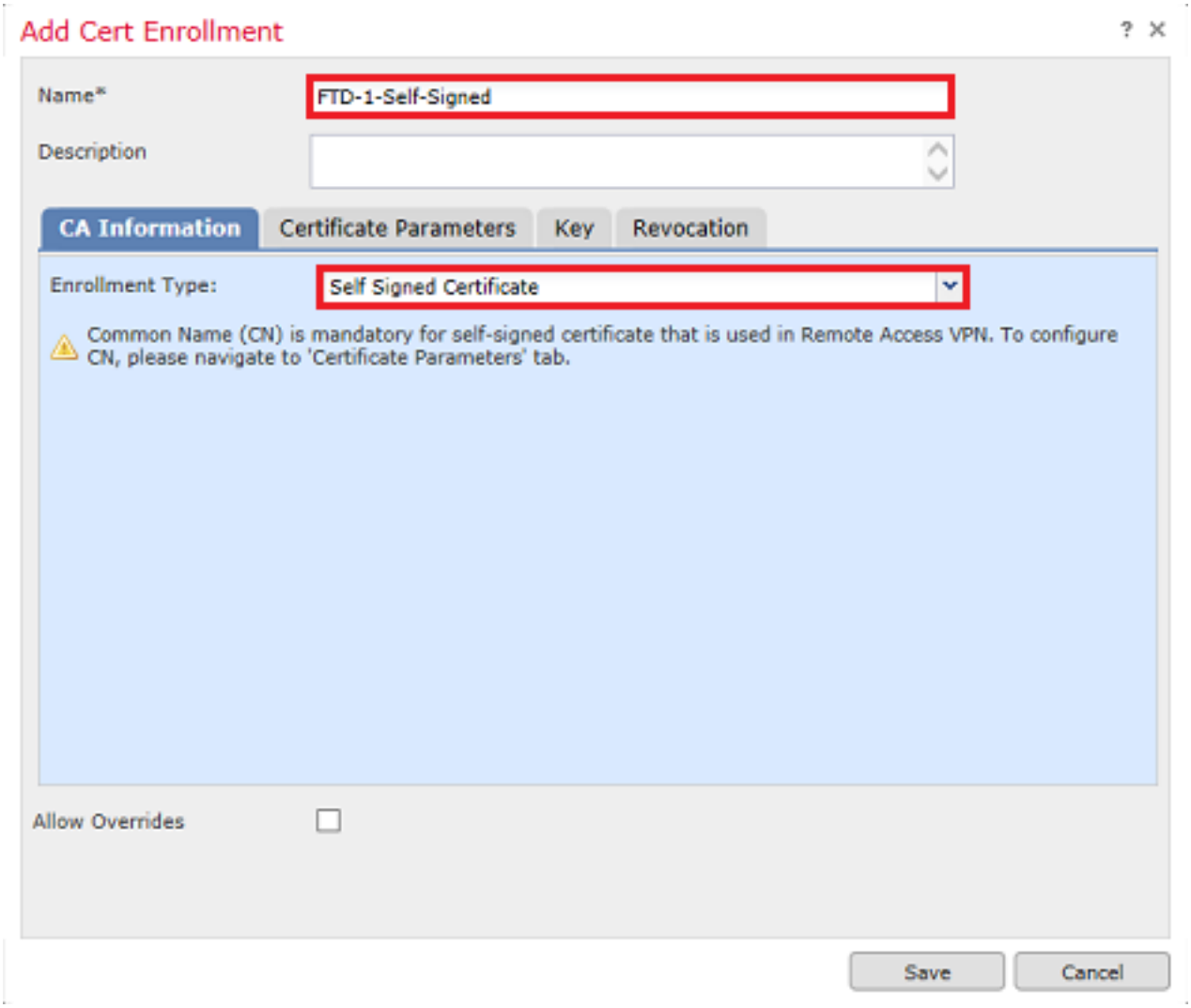


2. Wählen Sie das Gerät, und das Zertifikat wird in der **Geräte***-Dropdown hinzugefügt. Klicken Sie dann auf das grüne **+** Symbol, wie im Bild dargestellt.

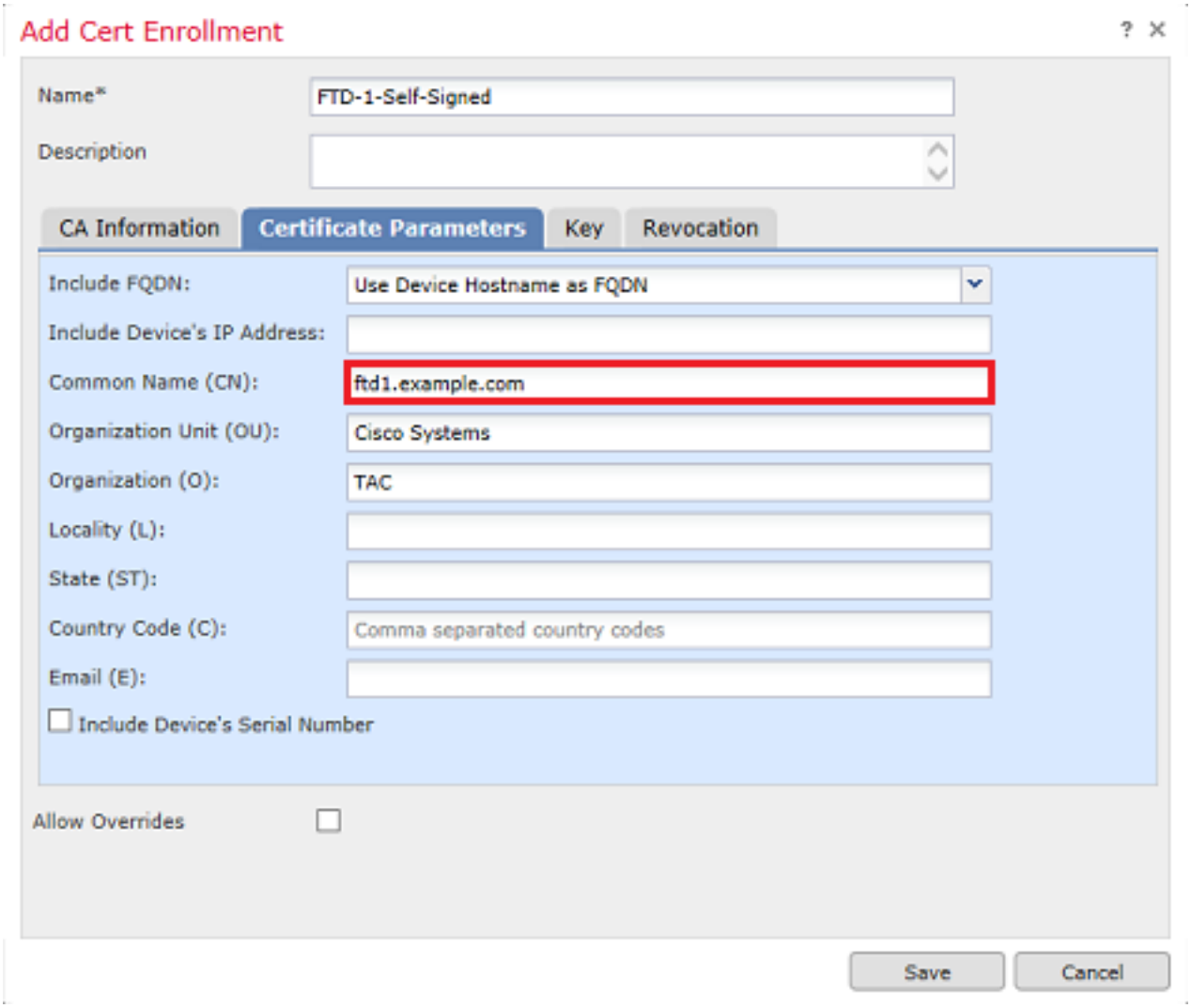


3. Geben Sie einen **Namen** für den Vertrauenspunkt an, und wählen Sie auf der Registerkarte **CA Information (Zertifizierungsstelleninformationen)** die Option Enrollment Type (Anmeldungstyp) aus:

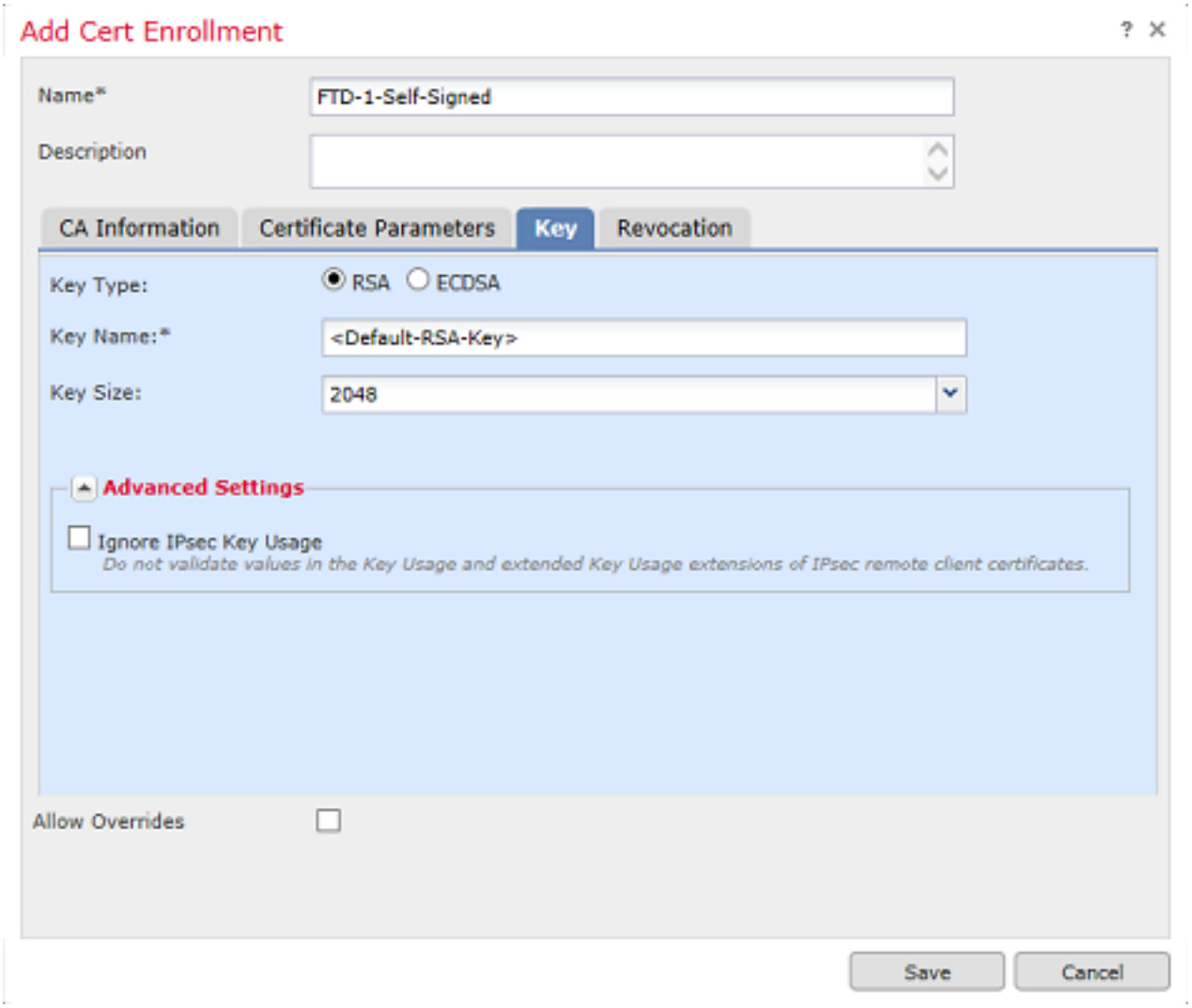
Selbstsigniertes Zertifikat wie im Bild dargestellt.



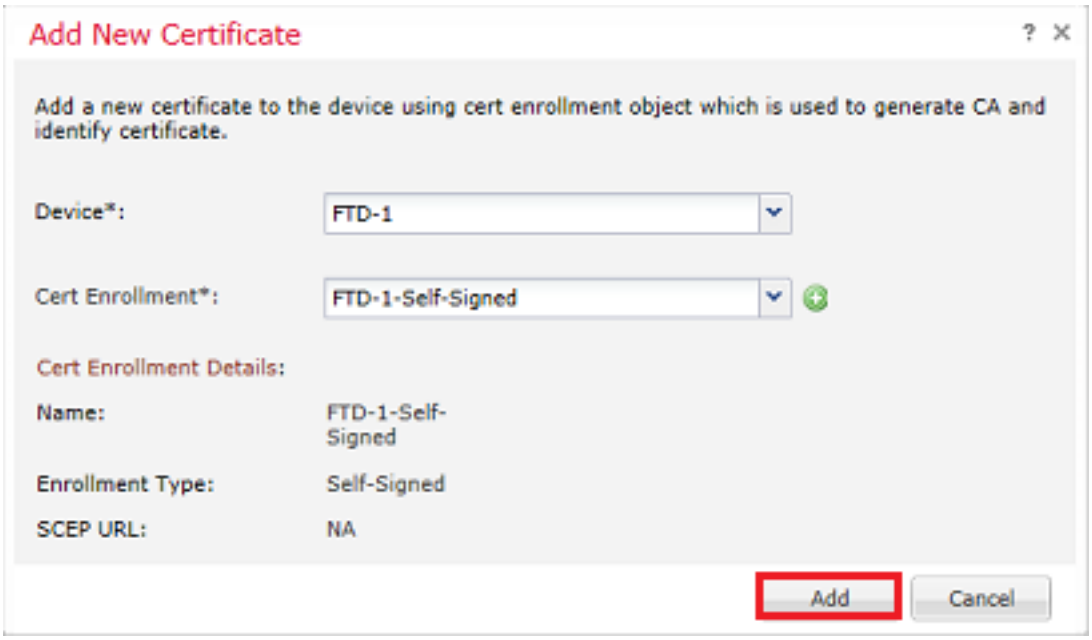
4. Geben Sie auf der Registerkarte **Zertifikatparameter** einen gemeinsamen Namen für das Zertifikat ein. Dies muss mit der fqdn- oder IP-Adresse des Dienstes übereinstimmen, für den das Zertifikat verwendet wird, wie im Bild gezeigt.



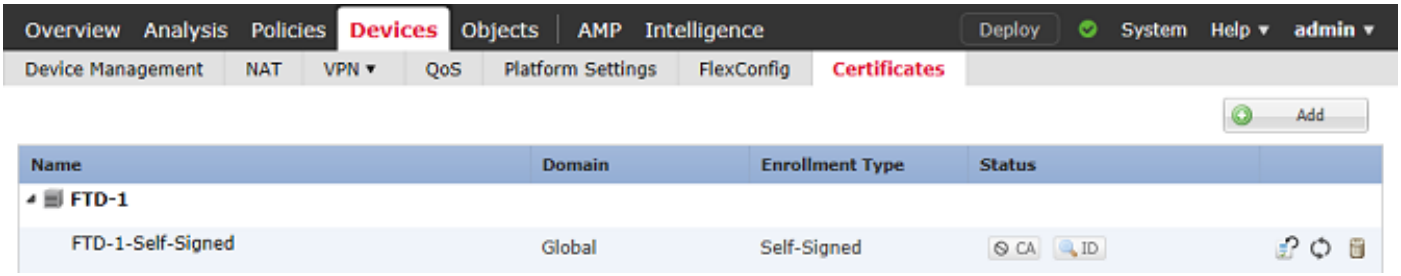
5. (Optional) Auf der Registerkarte **Key (Schlüssel)** können Typ, Name und Größe des für das Zertifikat verwendeten privaten Schlüssels angegeben werden. Standardmäßig verwendet der Schlüssel einen RSA-Schlüssel mit dem Namen **<Default-RSA-Key>** und der Größe 2048. Es wird jedoch empfohlen, für jedes Zertifikat einen eindeutigen Namen zu verwenden, damit nicht dieselbe private/öffentliche Tastatur wie im Bild gezeigt verwendet wird.



6. Klicken Sie abschließend auf **Speichern** und dann auf **Hinzufügen**, wie im Bild dargestellt.

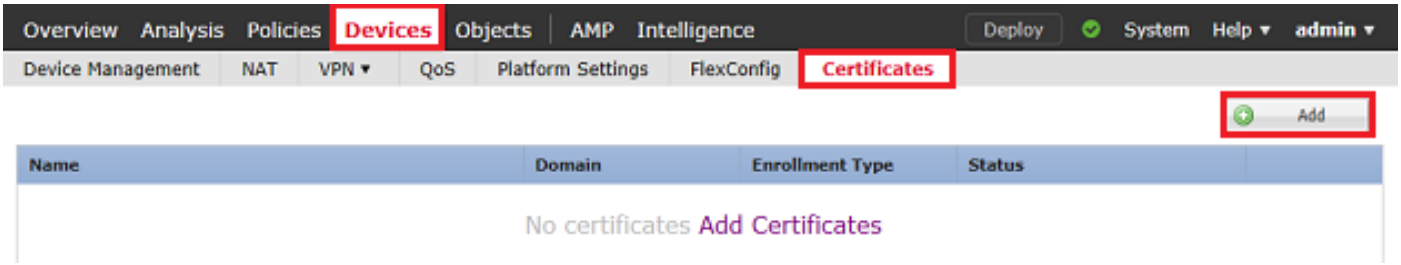


7. Nach Abschluss wird das selbstsignierte Zertifikat im Bild angezeigt.

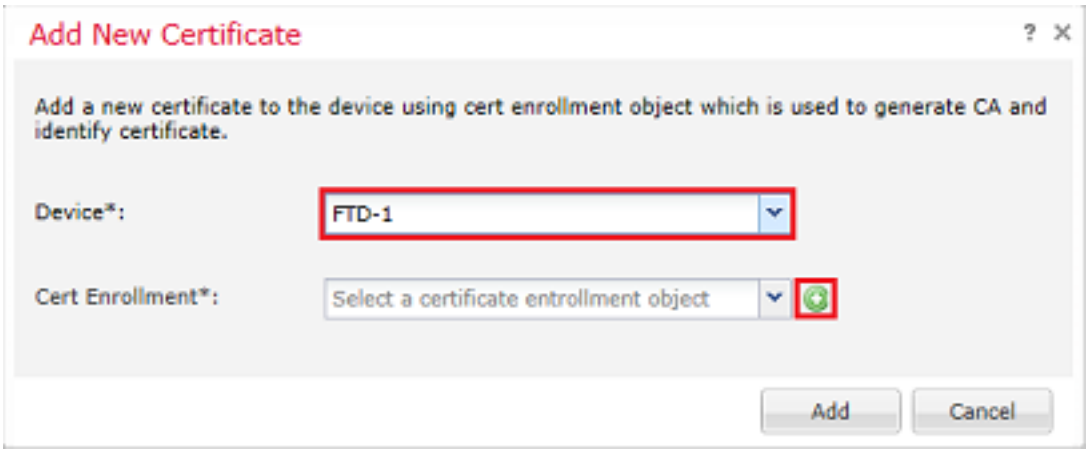


Manuelle Registrierung

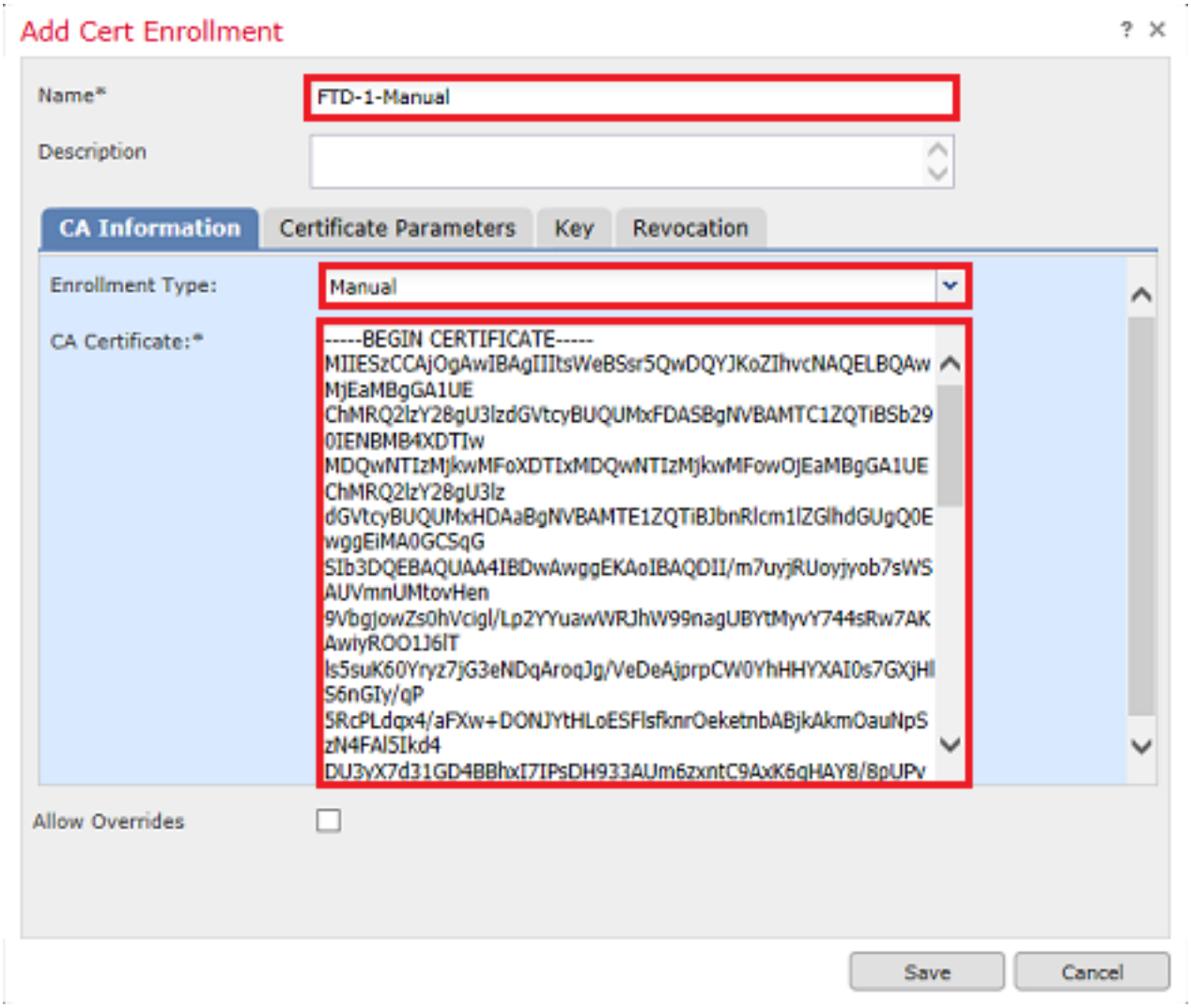
1. Navigieren Sie zu **Geräte > Zertifikate,** und klicken Sie dann auf **Hinzufügen**, wie im Bild dargestellt.



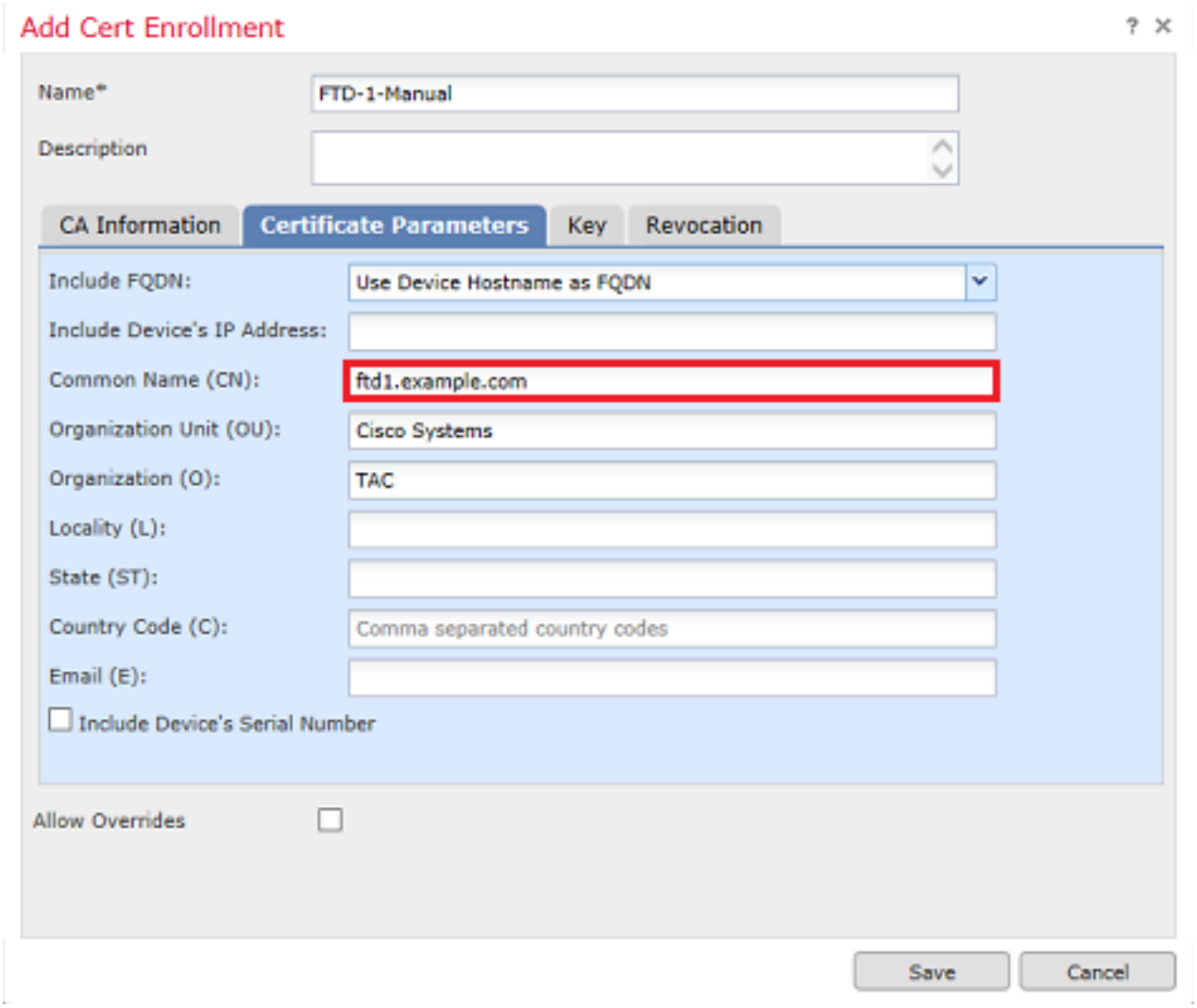
2. Wählen Sie das Gerät, dem das Zertifikat hinzugefügt wird, in der **Geräte*-**Dropdown-Liste und klicken Sie dann auf das grüne **+** Symbol, wie im Bild gezeigt.



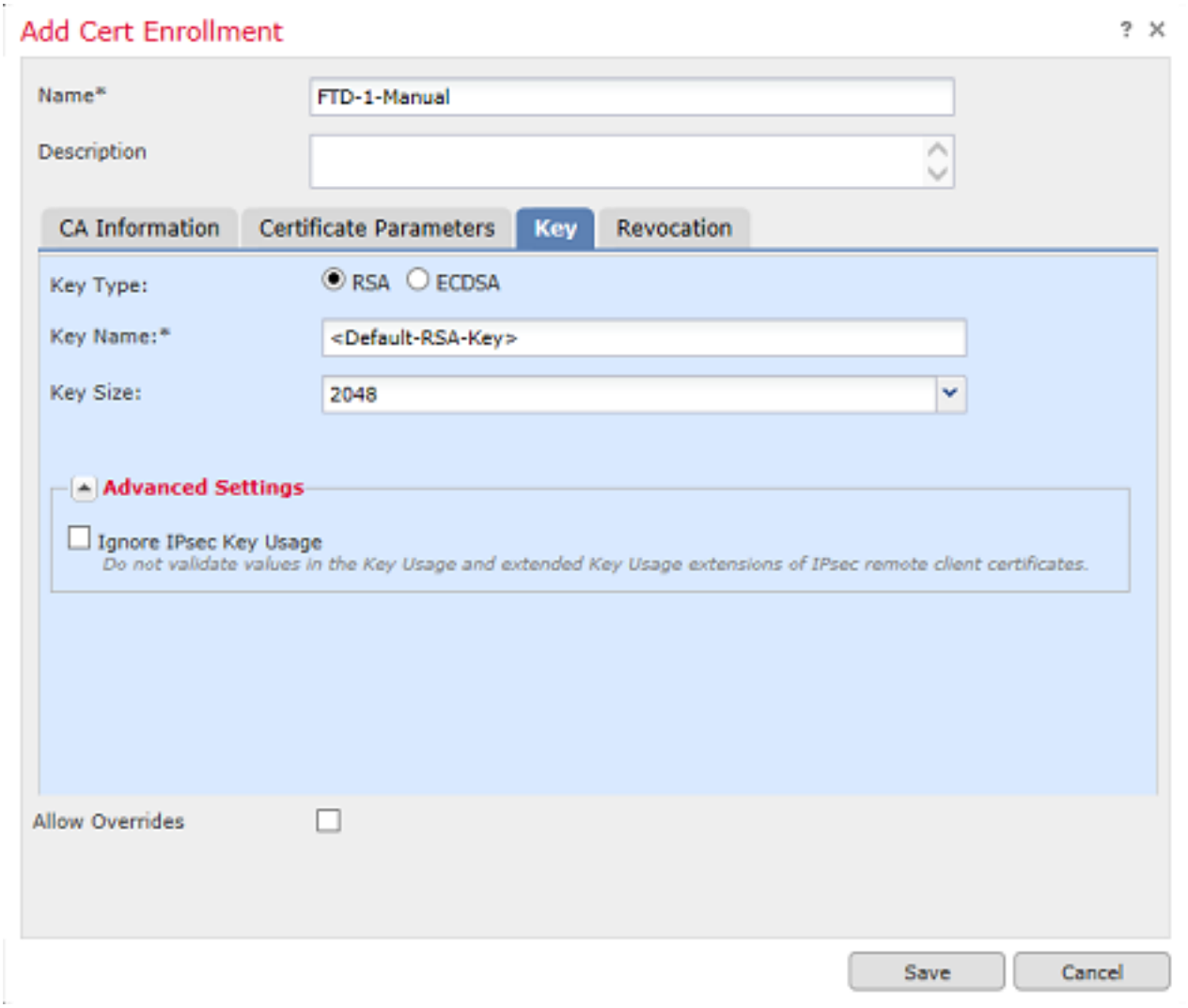
3. Geben Sie einen **Namen** für den Vertrauenspunkt an, und wählen Sie auf der Registerkarte **CA Information (Zertifizierungsstelleninformationen)** die Option Enrollment Type (Anmeldungstyp) aus: **Manuell**. Geben Sie das Zertifikat im PEM-Format der Zertifizierungsstelle ein, die zum Signieren des Identitätszertifikats verwendet wird. Wenn dieses Zertifikat zu diesem Zeitpunkt nicht verfügbar oder bekannt ist, fügen Sie ein Zertifizierungsstellenzertifikat als Platzhalter hinzu. Wiederholen Sie diesen Schritt, sobald das Identitätszertifikat ausgestellt wurde, und fügen Sie die echte ausstellende Zertifizierungsstelle wie im Bild dargestellt hinzu.



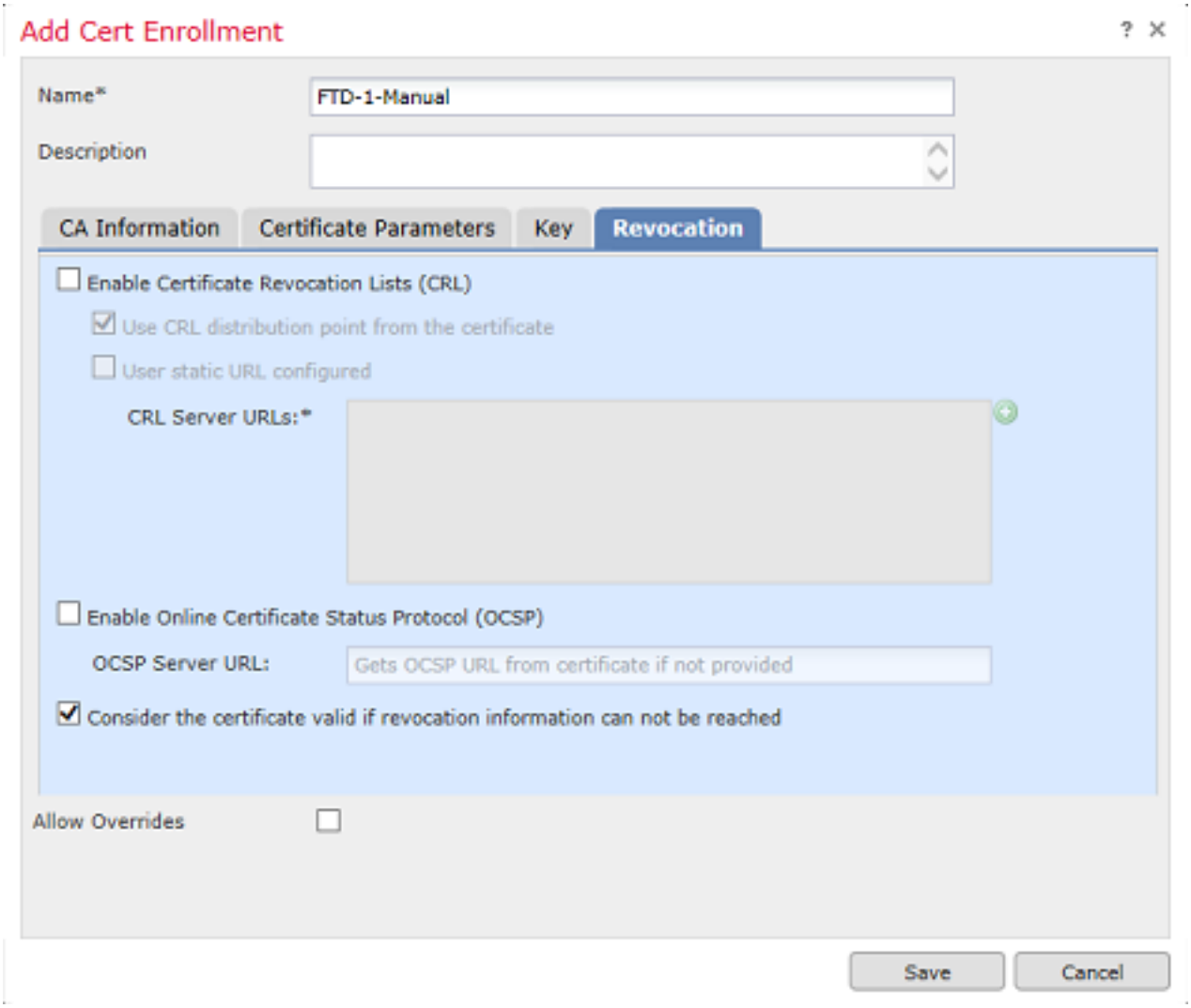
4. Geben Sie auf der Registerkarte **Zertifikatparameter** einen gemeinsamen Namen für das Zertifikat ein. Dies muss mit der fqdn- oder IP-Adresse des Dienstes übereinstimmen, für den das Zertifikat verwendet wird, wie im Bild gezeigt.



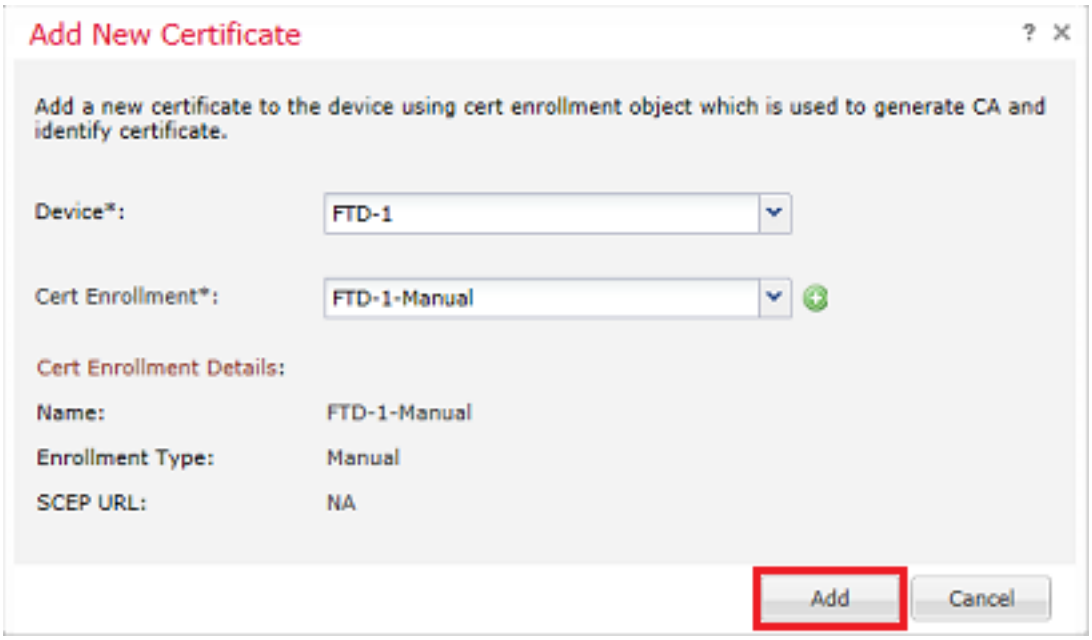
5. (Optional) Auf der Registerkarte **Schlüssel** können Sie optional den Typ, den Namen und die Größe des für das Zertifikat verwendeten privaten Schlüssels angeben. Standardmäßig verwendet der Schlüssel einen RSA-Schlüssel mit dem Namen **<Default-RSA-Key>** und der Größe 2048. Es wird jedoch empfohlen, für jedes Zertifikat einen eindeutigen Namen zu verwenden, damit nicht dieselbe private/öffentliche Tastatur wie im Bild gezeigt verwendet wird.



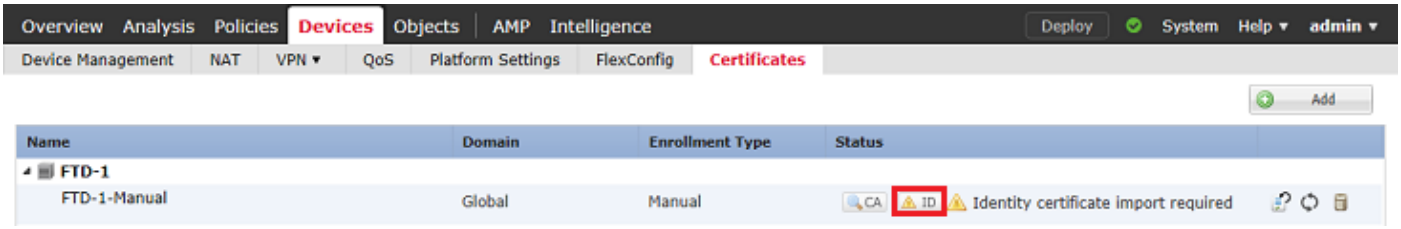
6. (Optional) Auf der Registerkarte **Widerruf** wird die Widerrufung der Zertifikatsperrliste (Certificate Revocation List, CRL) oder des Online Certificate Status Protocol (OCSP) überprüft und kann konfiguriert werden. Standardmäßig ist keines von beiden aktiviert, wie im Bild gezeigt.



7. Klicken Sie abschließend auf **Speichern** und dann auf **Hinzufügen**, wie im Bild dargestellt.

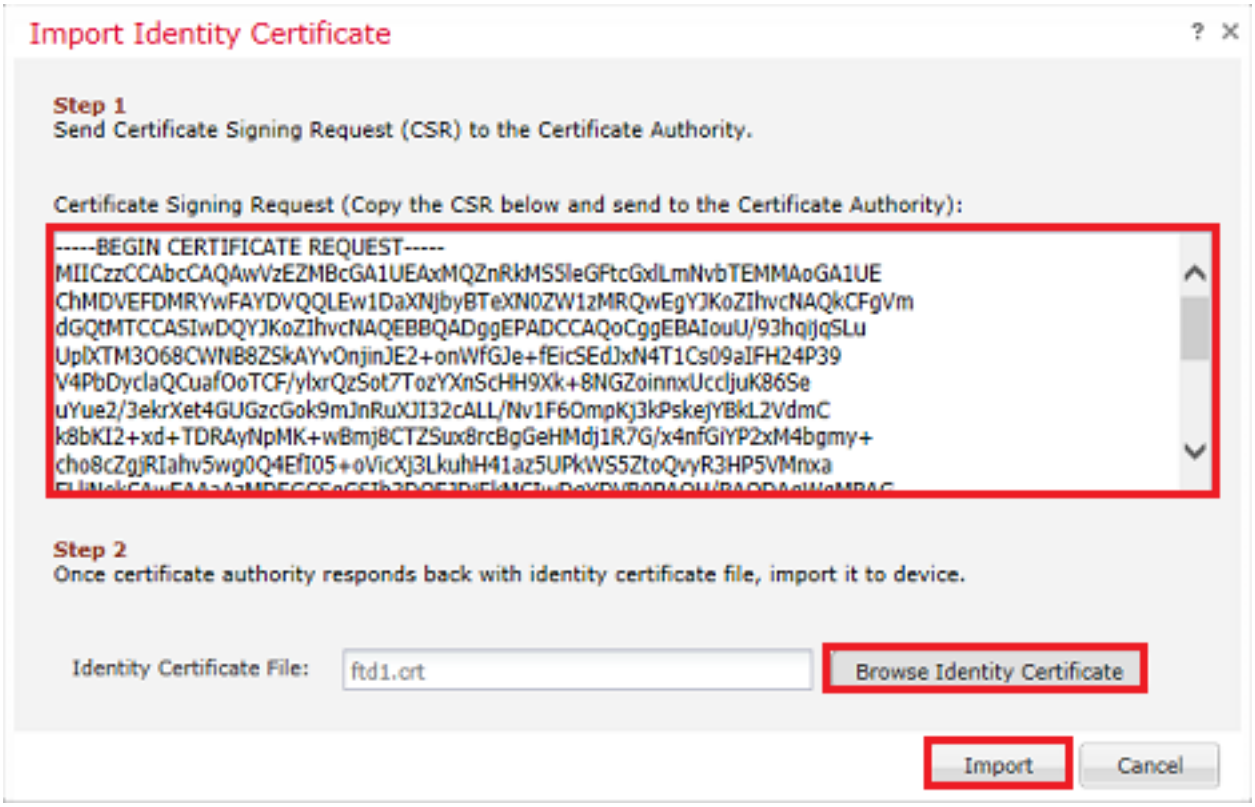


8. Nachdem Sie die Anforderung bearbeitet haben, bietet FMC die Option, ein Identitätszertifikat hinzuzufügen. Klicken Sie auf die Schaltfläche **ID**, wie im Bild dargestellt.

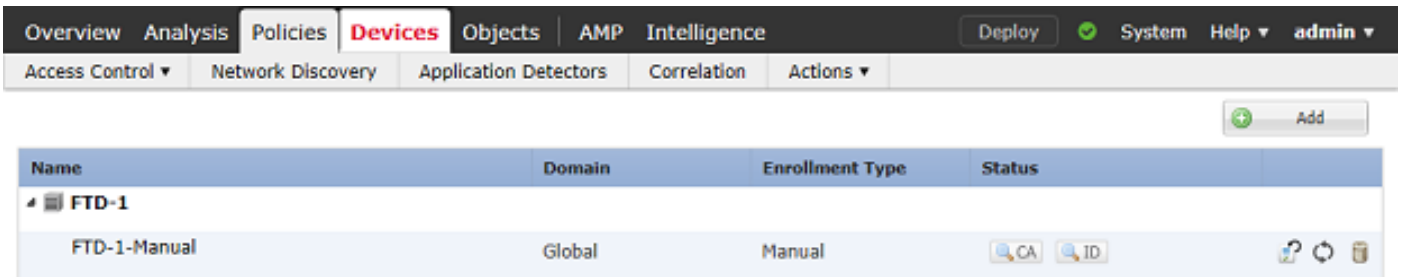


9. Es erscheint ein Fenster, das anzeigt, dass eine CSR-Anfrage generiert wird. Klicken Sie wie in der Abbildung dargestellt auf **Ja**.

10. Als Nächstes wird ein CSR generiert, der kopiert und an eine CA gesendet werden kann. Nach dem Signieren des CSR wird ein Identitätszertifikat bereitgestellt. Navigieren Sie zum bereitgestellten Identitätszertifikat, und wählen Sie es aus. Klicken Sie dann auf **Importieren**, wie im Bild dargestellt.

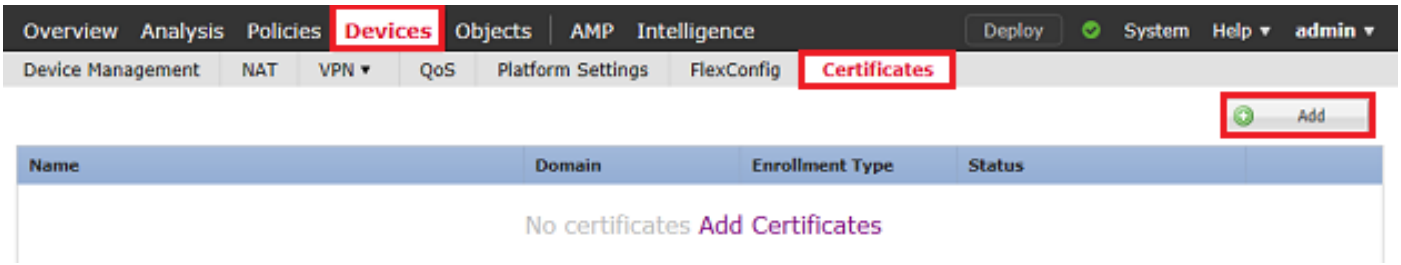


11. Nach Abschluss wird das manuelle Zertifikat wie im Bild angezeigt.

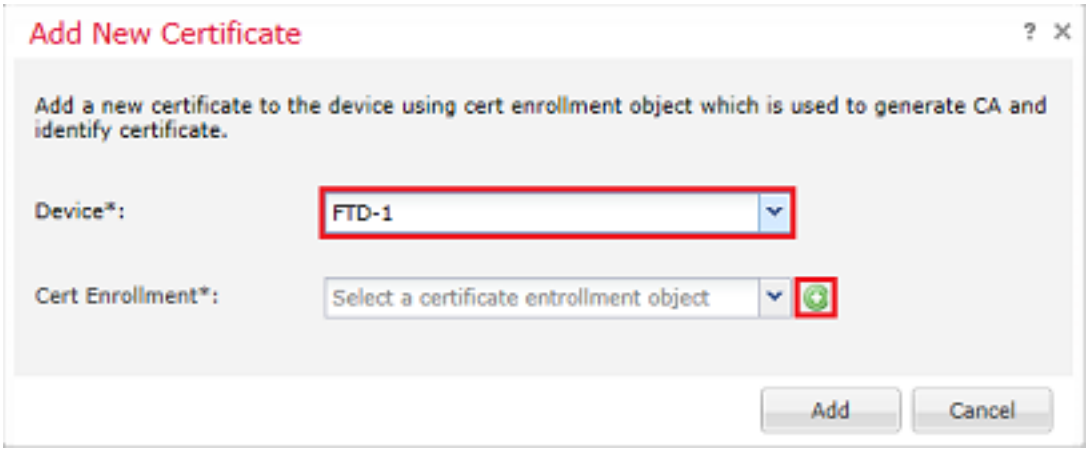


PKCS12-Registrierung

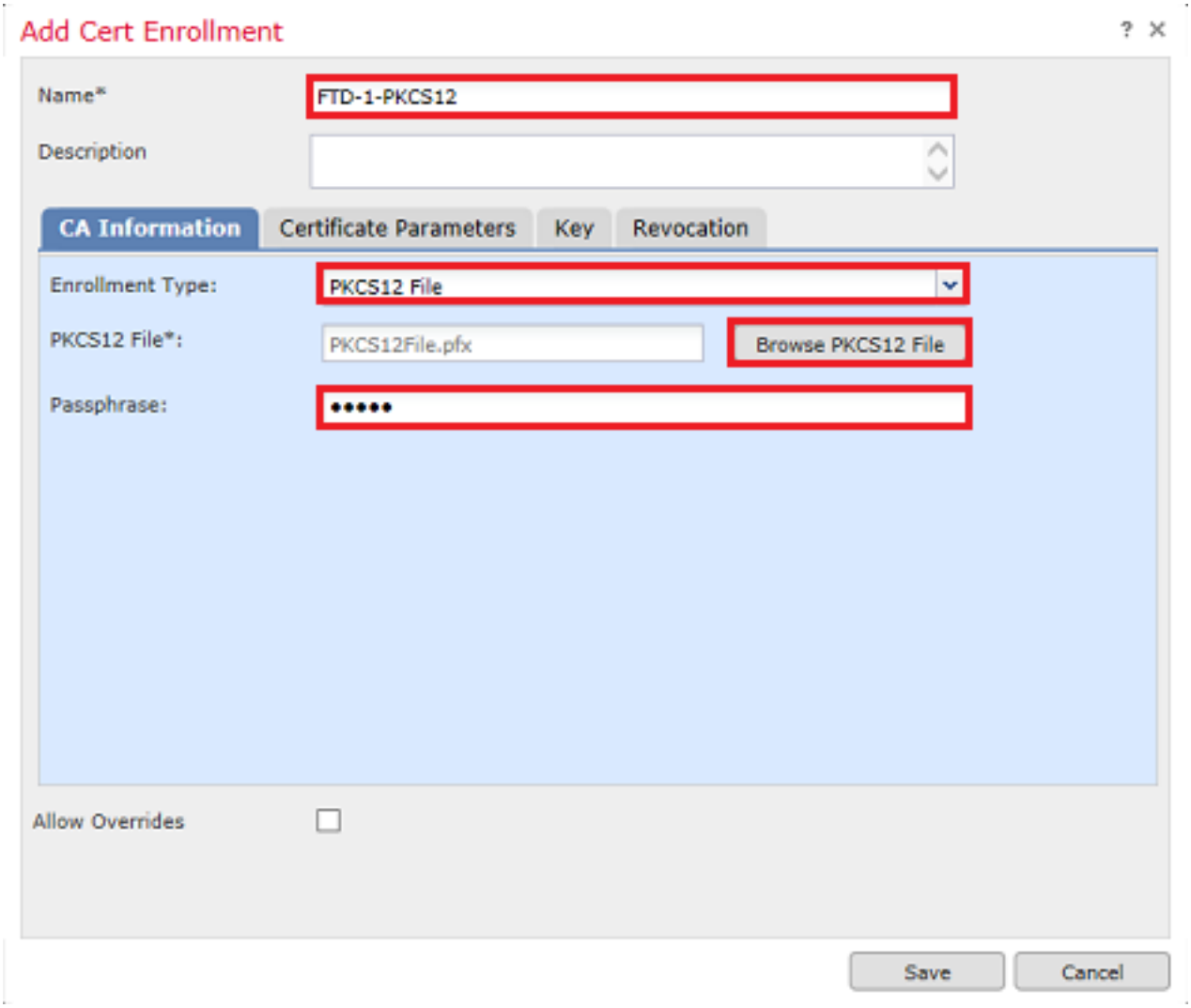
1. Um eine empfangene oder erstellte PKCS12-Datei zu installieren, navigieren Sie zu **Geräte > Zertifikate,** und klicken Sie dann auf **Hinzufügen,** wie im Bild dargestellt.



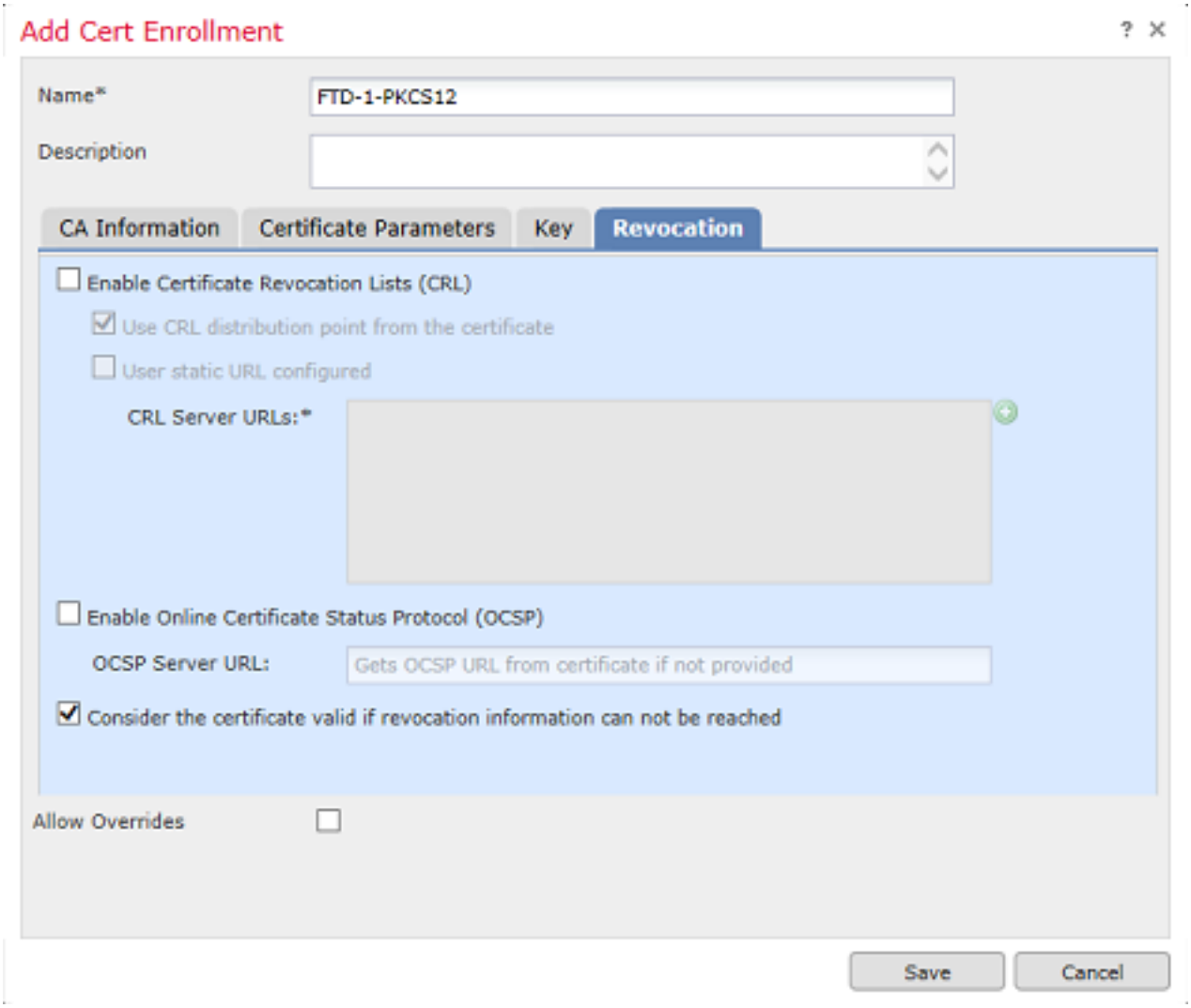
2. Wählen Sie das Gerät, dem das Zertifikat hinzugefügt wird, in der **Geräte*-**Dropdown-Liste und klicken Sie dann auf das grüne **+** Symbol, wie im Bild gezeigt.



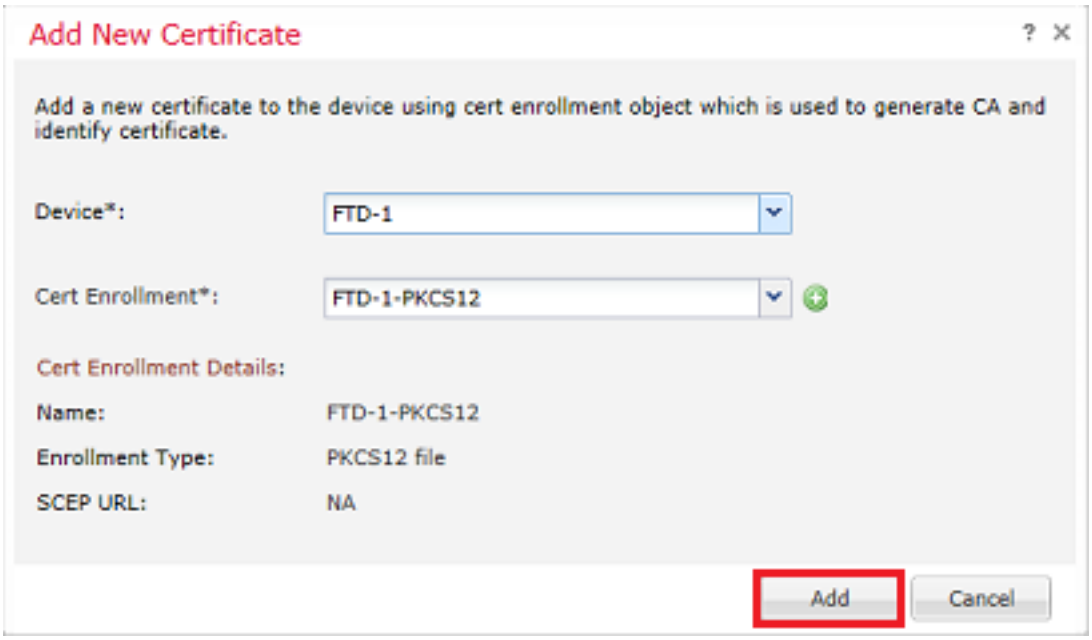
3. Geben Sie einen **Namen** für den Vertrauenspunkt an, und wählen Sie auf der Registerkarte **CA Information (Zertifizierungsstelleninformationen**) die Option Enrollment Type (Anmeldungstyp) aus: **PKCS12-Datei**. Navigieren Sie zur erstellten PKCS12-Datei, und wählen Sie sie aus. Geben Sie den Passcode ein, den Sie beim Erstellen des PKCS12 verwenden, wie im Bild dargestellt.



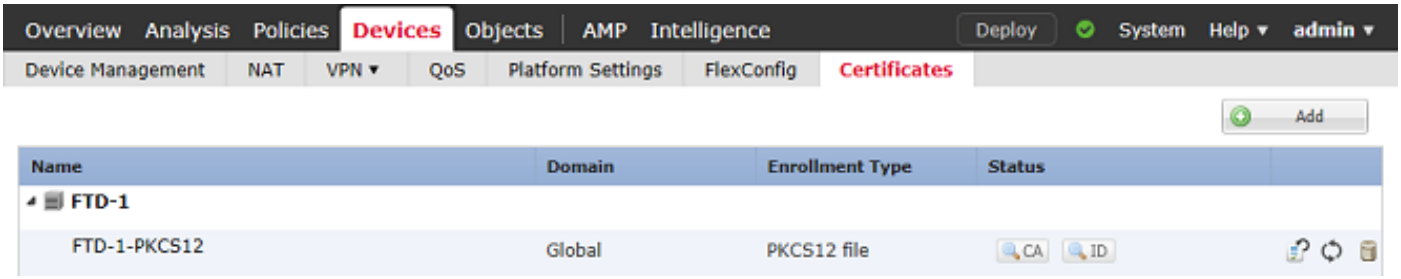
4. (Optional) Die Registerkarten **Zertifikatparameter** und **Schlüssel** sind abgeblendet, da diese bereits mit PKCS12 erstellt wurden. Die Registerkarte **Sperrung zur** Aktivierung der Sperrlisten- und/oder OCSP-Sperrprüfung kann jedoch geändert werden. Standardmäßig sind keine der Registerkarten wie im Bild dargestellt aktiviert.



5. Klicken Sie abschließend auf **Speichern** und dann auf **Hinzufügen**, wie im Bild dargestellt.



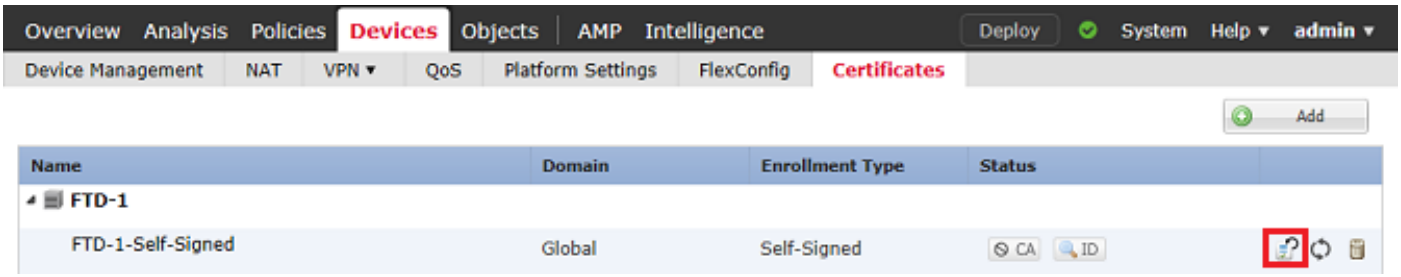
6. Nach Abschluss des Vorgangs sieht das PKCS12-Zertifikat wie im Bild dargestellt aus.



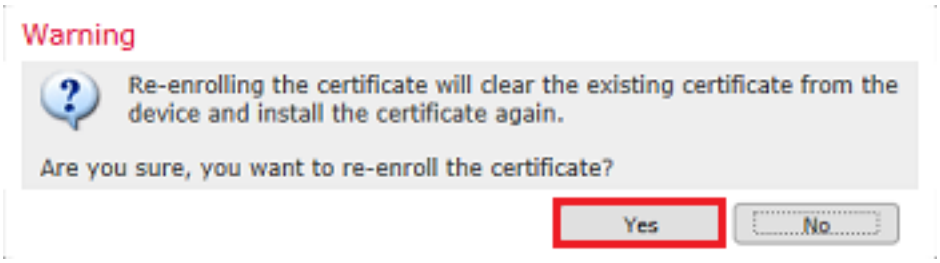
Erneuerung des Zertifikats

Selbstsignierte Zertifikatverlängerung

1. Drücken Sie die Taste Re-enroll certificate (Zertifikat erneut einschreiben), wie im Bild dargestellt.



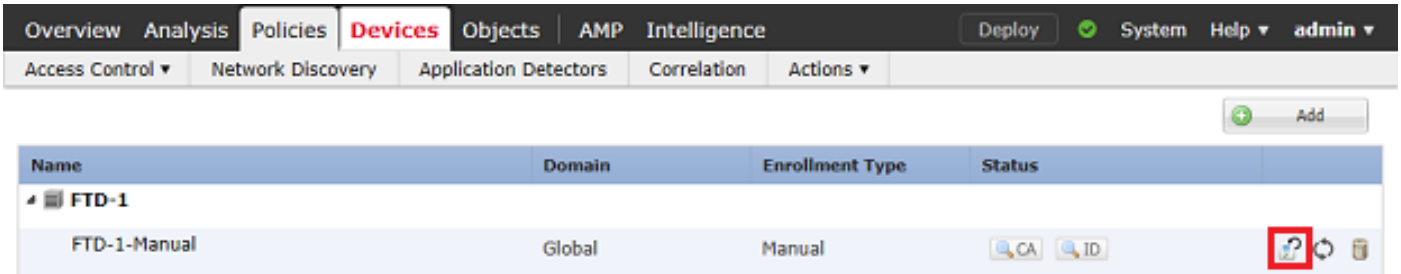
2. Ein Fenster fordert Sie auf, das selbstsignierte Zertifikat zu entfernen und zu ersetzen. Klicken Sie wie in der Abbildung dargestellt auf **Ja**.



3. Eine erneuerte Selbstsignatur wird an die FTD weitergeleitet. Dies kann überprüft werden, wenn Sie auf die Schaltfläche ID klicken und die Gültige Zeit überprüfen.

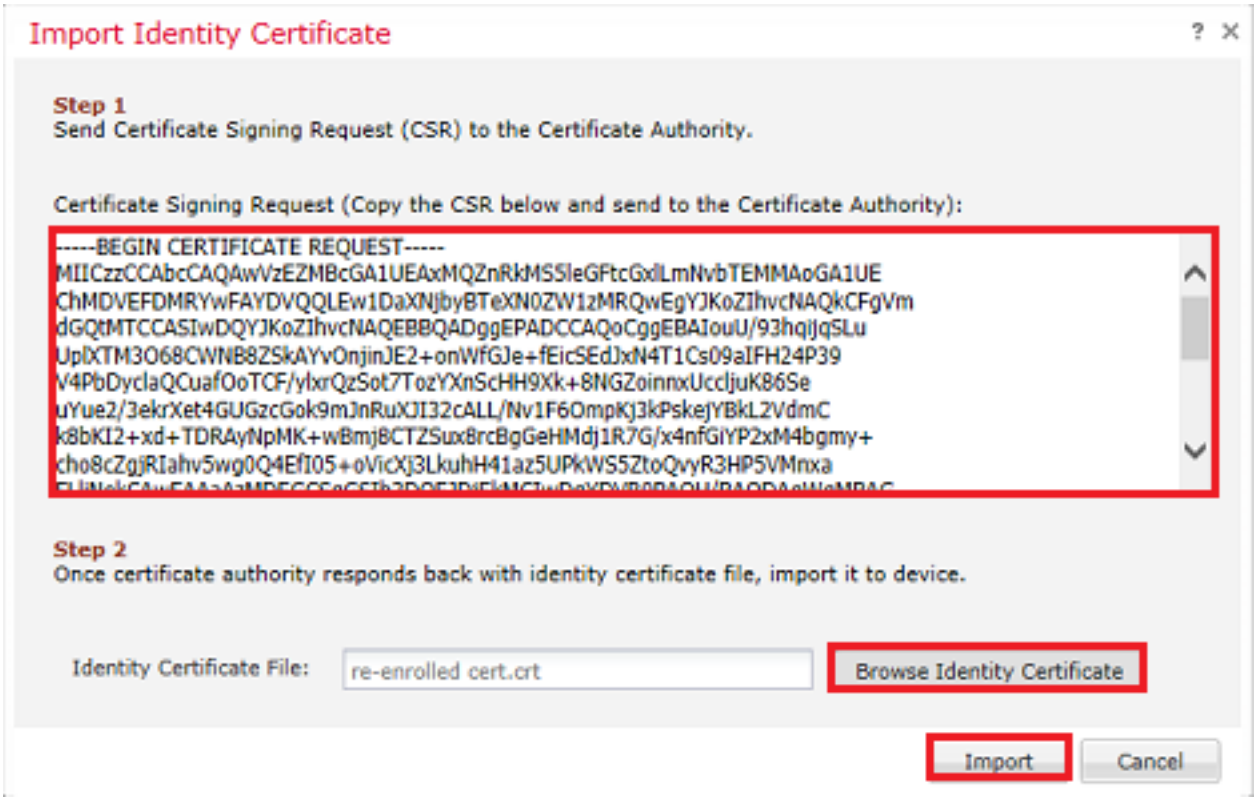
Manuelle Erneuerung des Zertifikats

1. Drücken Sie die Taste Re-enroll certificate (Zertifikat erneut einschreiben), wie im Bild dargestellt.



2. Ein Fenster fordert Sie auf, eine Anforderung zum Signieren des Zertifikats zu generieren. Klicken Sie wie in der Abbildung dargestellt auf **Ja**.

3. In diesem Fenster wird ein CSR generiert, der kopiert und an dieselbe Zertifizierungsstelle gesendet werden kann, die das Identitätszertifikat zuvor signiert hat. Sobald der CSR signiert wurde, wird das erneuerte Identitätszertifikat bereitgestellt. Navigieren Sie zum bereitgestellten Identitätszertifikat, und wählen Sie es aus. Klicken Sie dann auf **Importieren**, wie im Bild dargestellt.



4. Ein erneutes manuelles Zertifikat wird an die FTD weitergeleitet. Dies kann überprüft werden, wenn Sie auf die Schaltfläche ID klicken und die Gültige Zeit überprüfen.

PKCS12-Verlängerung

Wenn Sie auf die Schaltfläche "Re-enroll certificate" (Zertifikat erneut registrieren) klicken, wird das Zertifikat nicht erneuert. Um eine PKCS12 zu erneuern, muss eine neue PKCS12-Datei erstellt und mithilfe der zuvor genannten Methoden hochgeladen werden.

PKCS12-Erstellung mit OpenSSL

1. Generieren Sie unter Verwendung von OpenSSL oder einer ähnlichen Anwendung einen privaten Schlüssel und eine Zertifikatsanforderung (Certificate Signing Request, CSR). Dieses Beispiel zeigt einen 2048-Bit-RSA-Schlüssel mit dem Namen **private.key** und einen CSR mit dem Namen **ftd1.csr,** der in OpenSSL erstellt wird:

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd1.csr
```

```
Generating a 2048 bit RSA private key
.....................................+++
.....................................................................+++
written to a new private key to 'private.key'
-----
You are about to be asked to enter information that is incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', the field is left blank.
-----
Country Name (2 letter code) [AU]:.
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd1.example.com
Email Address []:.

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

2. Kopieren Sie den erstellten CSR, und senden Sie ihn an eine Zertifizierungsstelle. Nach dem Signieren des CSR wird ein Identitätszertifikat bereitgestellt. In der Regel werden auch die Zertifizierungsstellenzertifikate bereitgestellt. Um ein PKCS12 zu erstellen, führen Sie einen der folgenden Befehle in OpenSSL aus:

Verwenden Sie den folgenden Befehl, um nur das in PKCS12 ausgestellte Zertifizierungsstellenzertifikat einzuschließen:

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -certfile ca.crt
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

- **ftd.pfx** ist der Name der pkcs12-Datei (im Format), die von openssl exportiert wird.
- **ftd.crt** ist der Name des signierten Identitätszertifikats, das von der Zertifizierungsstelle im PEM-Format ausgegeben wird.
- **private.key** ist das in Schritt 1 erstellte Schlüsselpaar.
- **ca.crt** ist das Zertifikat der ausstellenden Zertifizierungsstelle im PEM-Format.

Wenn das Zertifikat Teil einer Kette mit einer Stammzertifizierungsstelle und mindestens einer zwischengeschalteten Zertifizierungsstelle ist, kann der folgende Befehl verwendet werden, um die gesamte Kette in PKCS12 hinzuzufügen:

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -chain -CAfile cachain.pem
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

- **ftd.pfx** ist der Name der pkcs12-Datei (im Format), die von OpenSSL exportiert wird.
- **ftd.crt** ist der Name des signierten Identitätszertifikats, das von der Zertifizierungsstelle im PEM-Format ausgegeben wird.
- **private.key** ist das in Schritt 1 erstellte Schlüsselpaar.
- **cachain.pem** ist eine Datei, die die Zertifizierungsstellenzertifikate in der Kette enthält, die mit

der ausstellenden Zwischen-Zertifizierungsstelle beginnen und mit der Stammzertifizierungsstelle im PEM-Format enden.

Wenn eine PKCS7-Datei (.p7b, .p7c) zurückgegeben wird, können diese Befehle auch verwendet werden, um die PKCS12 zu erstellen. Wenn die Datei p7b das Format "der" hat, stellen Sie sicher, dass **-notify der** zu den Argumenten hinzugefügt wird, andernfalls schließen Sie sie nicht ein:

```
openssl pkcs7 -in ftd.p7b -inform der -print_certs -out ftdpem.crt

openssl pkcs12 -export -in ftdpem.crt -inkey private.key -out ftd.pfx
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

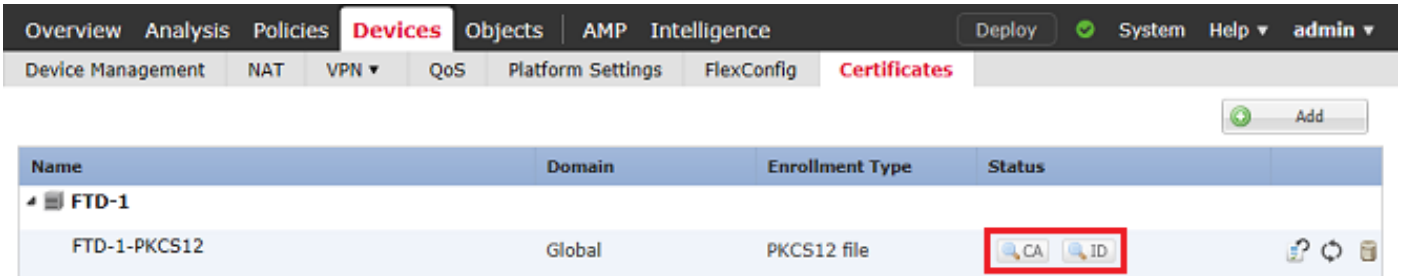
- **ftd.p7b** ist das PKCS7, das von der Zertifizierungsstelle zurückgegeben wird, die das signierte Identitätszertifikat und die Zertifizierungsstellenkette enthält.
- **ftdpem.crt** ist die konvertierte Datei p7b.
- **ftd.pfx** ist der Name der pkcs12-Datei (im Format), die von OpenSSL exportiert wird.
- **private.key** ist das in Schritt 1 erstellte Schlüsselpaar.

Überprüfung

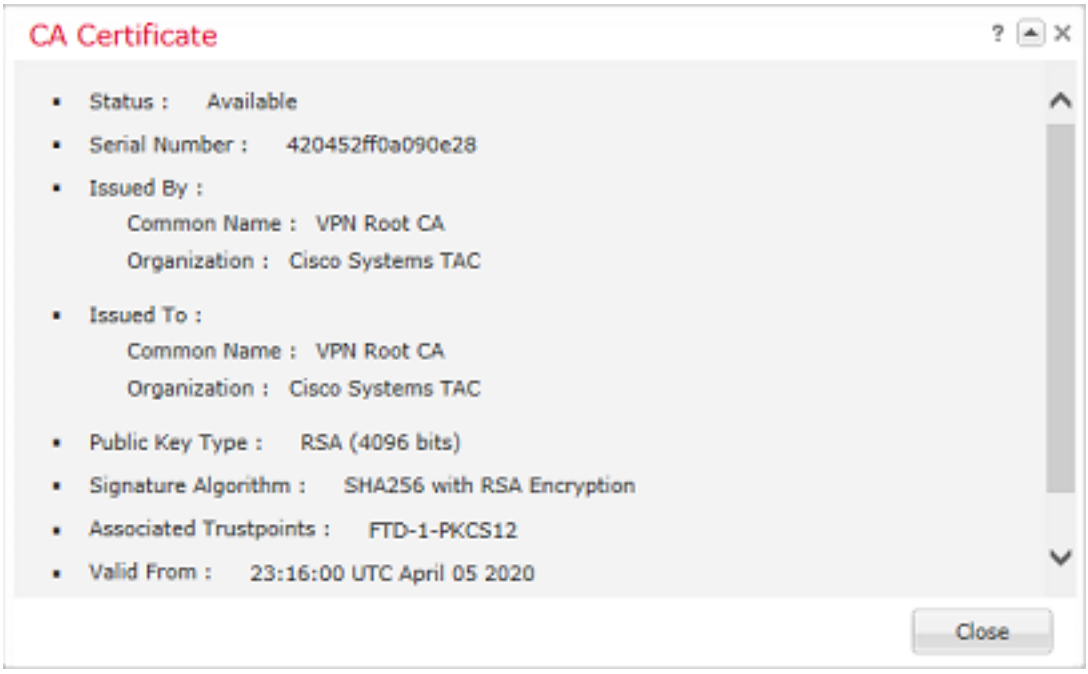
Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Installierte Zertifikate in FMC anzeigen

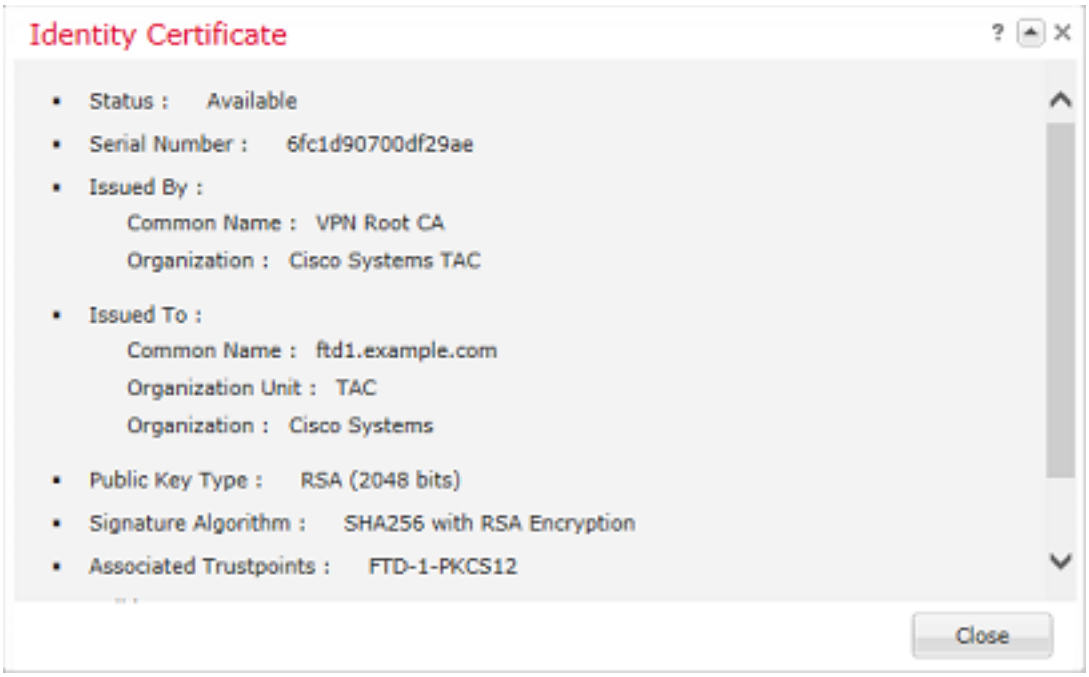
Navigieren Sie in FMC zu **Geräte > Zertifikate**. Klicken Sie für den entsprechenden Vertrauenspunkt auf die **Zertifizierungsstelle** oder **ID,** um weitere Details zum Zertifikat anzuzeigen, wie im Bild gezeigt.



Überprüfen Sie das Zertifizierungsstellenzertifikat wie im Bild gezeigt.



Überprüfen Sie das Identitätszertifikat wie im Bild gezeigt.



Installierte Zertifikate in CLI anzeigen

SSH zum FTD und geben Sie den Befehl **show crypto ca certificate ein**.

```
> show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 6fc1d90700df29ae
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Subject Name:
```

```
    cn=ftd1.example.com
    ou=TAC
    o=Cisco Systems
  Validity Date:
    start date: 15:47:00 UTC Apr 8 2020
    end   date: 15:47:00 UTC Apr 8 2021
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12

CA Certificate
  Status: Available
  Certificate Serial Number: 420452ff0a090e28
  Certificate Usage: General Purpose
  Public Key Type: RSA (4096 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Subject Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Validity Date:
    start date: 23:16:00 UTC Apr 5 2020
    end   date: 23:16:00 UTC Apr 5 2030
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12
```

Fehlerbehebung

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

Debugbefehle

Im Fall eines Fehlers bei der Installation des SSL-Zertifikats können Fehlerbehebungen über die Diagnose-CLI ausgeführt werden, nachdem die FTD über SSH verbunden ist:

debug crypto ca 14

In älteren FTD-Versionen sind diese Fehlerbehebungsschritte verfügbar und werden zur Fehlerbehebung empfohlen:

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 255

Häufige Probleme

Beachten Sie auch nach dem Import des ausgestellten Identitätszertifikats die Meldung "Import des Identitätszertifikats erforderlich".

Dies kann aufgrund von zwei verschiedenen Problemen auftreten:

1. Das ausstellende Zertifizierungsstellenzertifikat wurde bei der manuellen Registrierung nicht

hinzugefügt.

Wenn das Identitätszertifikat importiert wird, wird es bei der manuellen Registrierung mit dem auf der Registerkarte "CA Information" (CA-Informationen) hinzugefügten Zertifizierungsstellenzertifikat abgeglichen. In manchen Fällen verfügen Netzwerkadministratoren nicht über das Zertifizierungsstellenzertifikat für die Zertifizierungsstelle, mit dem ihr Identitätszertifikat signiert wird. In diesem Fall muss bei der manuellen Registrierung ein Platzhalter-Zertifizierungsstellenzertifikat hinzugefügt werden. Sobald das Identitätszertifikat ausgestellt und das Zertifizierungsstellenzertifikat bereitgestellt wurde, kann mit dem richtigen Zertifizierungsstellenzertifikat eine neue manuelle Registrierung durchgeführt werden. Wenn Sie den Assistenten für die manuelle Registrierung erneut durchlaufen, stellen Sie sicher, dass Sie für das Tastenpaar denselben Namen und dieselbe Größe wie bei der ursprünglichen manuellen Registrierung angeben. Anschließend kann das zuvor ausgestellte Identitätszertifikat anstelle des erneut an die Zertifizierungsstelle weitergeleiteten CSR in den neu erstellten Vertrauenspunkt mit dem richtigen Zertifizierungsstellenzertifikat importiert werden.

Um zu überprüfen, ob dasselbe CA-Zertifikat bei der manuellen Registrierung angewendet wurde, klicken Sie entweder auf die CA-Schaltfläche, wie im Abschnitt Überprüfen angegeben, oder überprüfen Sie die Ausgabe von **show crypto ca-Zertifikaten**. Felder wie "Ausgestellt an" und "Seriennummer" können mit den Feldern im Zertifizierungsstellenzertifikat verglichen werden, das von der Zertifizierungsstelle bereitgestellt wird.

2. Das Tastenpaar im erstellten Vertrauenspunkt unterscheidet sich vom Tastenpaar, das beim Erstellen des CSR für das ausgestellte Zertifikat verwendet wird.

Bei der manuellen Registrierung wird der öffentliche Schlüssel dem CSR hinzugefügt, sodass er in das ausgestellte Identitätszertifikat aufgenommen werden kann, wenn das Schlüsselpaar und die CSR generiert werden. Wenn aus irgendeinem Grund das Schlüsselpaar auf dem FTD geändert wird oder das ausgestellte Identitätszertifikat einen anderen öffentlichen Schlüssel enthält, installiert das FTD das ausgestellte Identitätszertifikat nicht. Um zu überprüfen, ob dies geschehen ist, gibt es zwei verschiedene Tests:

In OpenSSL können diese Befehle ausgegeben werden, um den öffentlichen Schlüssel im CSR mit dem öffentlichen Schlüssel im ausgestellten Zertifikat zu vergleichen:

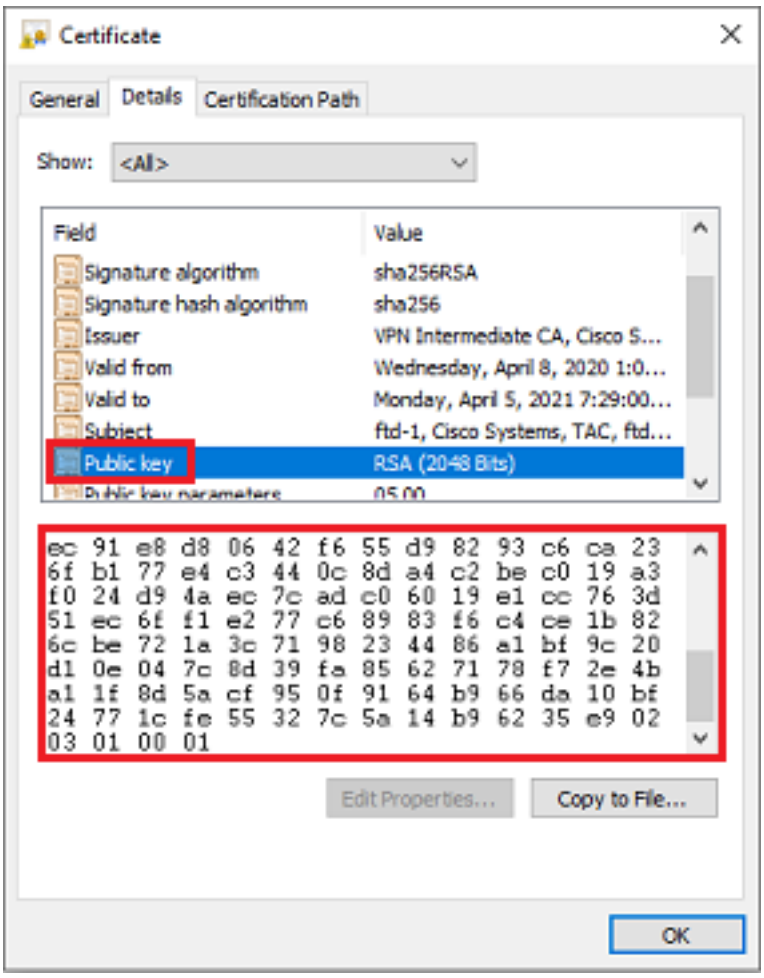
```
openssl req -noout -modulus -in ftd.csr
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484
749C4DE13D42B34F5A2051F6E
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF
3A49EB98B9EDBFDDE92B5DEB7
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C344
0C8DA4C2BEC019A3F024D94AE
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA8562717
8F72E4BA11F8D5ACF950F9164
B966DA10BF24771CFE55327C5A14B96235E9 openssl x509 -noout -modulus -in id.crt
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484
749C4DE13D42B34F5A2051F6E
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF
3A49EB98B9EDBFDDE92B5DEB7
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C344
0C8DA4C2BEC019A3F024D94AE
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA8562717
8F72E4BA11F8D5ACF950F9164
B966DA10BF24771CFE55327C5A14B96235E9
```

- **ftd.csr** ist der CSR, der bei der manuellen Registrierung von FMC kopiert wird.

- **id.crt** ist das von der Zertifizierungsstelle signierte Identitätszertifikat.

Alternativ kann der Wert des öffentlichen Schlüssels auf dem FTD auch mit dem öffentlichen Schlüssel im ausgestellten Identitätszertifikat verglichen werden. Beachten Sie, dass die ersten Zeichen im Zertifikat nicht mit denen in der FTD-Ausgabe übereinstimmen, die aufgrund der Füllung ausgegeben werden:

Ausgestelltes Identitätszertifikat, das auf dem Windows-PC geöffnet wurde:



Ausgabe des öffentlichen Schlüssels aus dem Identitätszertifikat wurde extrahiert:

```
3082010a02820101008a2e53ff7786a8a3a922ee5299574ccdceebc096341f194a4018bce9e38a7244dbea2759f1897b
e7c489c484749c4de13d42b34f5a2051
f6e0fdfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b
8af3a49eb98b9edbfdde92b5deb78194
1b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8d
a4c2bec019a3f024d94aec7cadc06019
e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f
8d5acf950f9164b966da10bf24771cfe
55327c5a14b96235e90203010001
```

Kryptografieschlüssel mypubkey rsa Ausgabe von FTD **anzeigen**. Nach der manuellen Registrierung wurde der **<Default-RSA-Key>** zum Erstellen des CSR verwendet. Der fett formatierte Abschnitt entspricht der extrahierten Ausgabe des öffentlichen Schlüssels aus dem Identitätszertifikat.

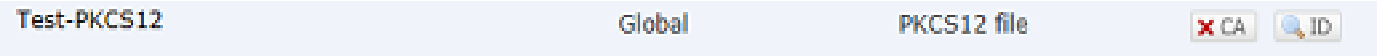
```
> show crypto key mypubkey rsa
Key pair was generated at: 16:58:44 UTC Jan 25 2019
 Key name: <Default-RSA-Key>
```

```
Usage: General Purpose Key
Modulus Size (bits): 2048
Storage: config
Key Data:

 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
 008a2e53 ff7786a8 a3a922ee 5299574c cdceebc0 96341f19 4a4018bc e9e38a72
 44dbea27 59f1897b e7c489c4 84749c4d e13d42b3 4f5a2051 f6e0fdfd 5783db0f
 27256900 ae69f3a8 4c217fca 5c6b4334 a8b7b4e8 cd85e749 c1c7f579 3ef0d199
 a229e7c5 471c963b 8af3a49e b98b9edb fdde92b5 deb78194 1b3706a2 4f662674
 6e5c9237 d9c00b2f f36fd45e 8e9a92a3 de43ec91 e8d80642 f655d982 93c6ca23
 6fb177e4 c3440c8d a4c2bec0 19a3f024 d94aec7c adc06019 e1cc763d 51ec6ff1
 e277c689 83f6c4ce 1b826cbe 721a3c71 98234486 a1bf9c20 d10e047c 8d39fa85
 627178f7 2e4ba11f 8d5acf95 0f9164b9 66da10bf 24771cfe 55327c5a 14b96235
 e9020301 0001
```

Rotes X neben CA in FMC

Dies kann bei der PKCS12-Registrierung auftreten, da das Zertifizierungsstellenzertifikat nicht im PKCS12-Paket enthalten ist.



Um dies zu beheben, muss das Zertifizierungsstellenzertifikat für PKCS12 hinzugefügt werden.

Führen Sie diese Befehle aus, um das Identitätszertifikat und den privaten Schlüssel zu extrahieren. Das Kennwort, das bei der Erstellung von PKCS12 verwendet wird, und der sichere private Schlüssel werden benötigt:

```
openssl pkcs12 -info -in test.p12
Enter Import Password: [pkcs12 pass phrase here]
MAC Iteration 1
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    friendlyName: Test
    localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
subject=/CN=ftd1.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Intermediate CA
-----BEGIN CERTIFICATE-----
MIIC+TCCAeGgAwIBAgIIAUIM3+3IMhIwDQYJKoZIhvcNAQELBQAwOjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxHDAaBgNVBAMTE1ZQTiBJbnRlcm1lZGlhdGUg
Q0EwHhcNMjAwNDA4MTY1ODAwWhcNMjEwNDA1MjMyOTAwWjAbMRkwFwYDVQQDExBm
dGQxLmV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
043eLVPl8K0jnYfHCBZuFUYrXTTB28Z1ouIJ5yyrDzCN781GFrHb/wCczRx/jW4n
pF9q2z7FHr5bQCI4oSUSX40UQfr0/u0K5riI1uZumPUx1Vp1zVkYuqDd/i1r0+0j
PyS7BmyGfV7aebYWZnr8R9ebDsnC2U3nKjP5RaE/wNdVGTS/180HlrIjMpcFMXps
LwxdxiEz0hCMnDm9RC+7uWZQdlwZ9oNANCbQC0px/Zikj9Dz7ORhhbzBTeUNKD3p
sN3VqdDPvGZHFGlPCnhKYyZ79+6p+CHC8X8BFjuTJYoo1l6uGgiB4Jz2Y9ZeFSQz
Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBglghkgBhvhCAQ0EERYPeGNhIGNl
cnRpZmljYXRlMA0GCSqGSIb3DQEBCwUAA4IBAQCV/MgshWxXtwpwmMF/6KqEj8nB
SljbfzlzNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRyY54taRI27W+gLneCbQAux
9amxXuhpxP5EOhnk+tsYS9eriAKpHuS1Y/2uwN92fHIbh3HEXPO1HBJueI8PH3ZK
4lrPKA9oIQPUW/uueHEF+xCbG4xCLi5HOGeHX+FTigGNqazaX5GM4RBUa4bk8jks
Ig53twvop71wE53COTH0EkSRCsVCw5mdJsd9BUZHjguhpw8Giv7Z36qWv18I/Owf
RhLhtsgenc25udglvv9Sy5xK53a5Ieg8biRpWL9tIjgUgjxYZwtyVeHi32S7
-----END CERTIFICATE-----
PKCS7 Data
```

```
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    friendlyName: Test
    localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
Key Attributes: <No Attributes>
Enter PEM pass phrase: [private-key pass phrase here]
Verifying - Enter PEM pass phrase: [private-key pass phrase here]
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIlKyWXk8cgTMCAggA
MBQGCCqGSIb3DQMHBAgGmOqRXh/dcwSCBMiF7BpgJNIpHdU5Zorn1jm3pmsI/XkJ
MRHc1Reel0ziSLCZ0STr84JFQxNpbThXLhsHC9WhpPy5sNXIvXS7Gu+U10/VlNSA
rWlX6SPftAYiFq5QXyEutSHdZZwgQIqpj97seu3Px0agvIObW1Lo8or5lSydnMjp
Ptv5OKo95BShWWYcqkTAia4ZKxytyIc/mIu5m72LucOFmoRBO5JZu1avWXjbCAA+
k2ebkblFT0YRQT1Z4tZHSqX1LFPZe170NZEUg7rIcWAk1Yw7XNUPhOn6FHL/ieIZ
IhvIfj+1gQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E
Gnh8r3l903AlkPMBkMdxOqlpzo2naIy2KGrUnOSHajVWcLr9dTPWIDyjdn95YoeS
IUE7Ma00pjJcO2FNBwyNxRrYt+4hp3aJt0ZW83FHiSlB5UIzGrBMAgKJc2Hb2RTV
9gxZGve1cRcolLeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShn0wHzridF8Zn
FO6XvBDSyuXVSpkxwAdlTwxq62tUnLIkyRXo2CSz8z8W29UXmFO4o3G67n28//LJ
Ku8wj1jeqlvFgXSQiWLADNhIY772RNwzCMeobfxGlBprF9DPT8yvyBdQviUIuFpJ
nNs5FYbLTv9ygZ1S9xwQpTcqEu+y4F5BJuYLmHqcZ+VpFA4nM0YHhZ5M3sceRSR4
1L+a3BPJJshlTIJQg0TIxDaveCfpDcpS+ydUgS6YWY8xW17v0+1f7y5zlt4TkZRt
ItBHHA6yDzR0Cn0/ZH3y88a/asDcukw6bsRaY5iT8nAWgTQVed3xXj+EgeRs25HB
dIBBX5gTvqN7qDanhkaPUcEawj1/38M0pAYULei3elfKKrhwAySBFaV/BeUMWuNW
BmKprkKKQv/JdWnoJl49KcS4bfa3GHG9XXnyvbg8HxopcYFMTEjao+wLZH9agqKe
YOjyoHFN6ccBBC7vn7u12tmXOM5RcnPLmaDaBFDSBBFS8Y8VkeHn3P0q7+sEQ26d
vL8O7WdgLH/wKqovoJRyxwzz+TryRq9cd5BNyyLaABESalsWRhk81C2P+B+Jdg9w
d6RsvJ2dt3pdl/+pUR3CdC0b8qRZOoLO3+onUIUoEsCCNdp0x8Yj/mvc6ReXtOKB
2qVmhVMYseiUlrOAQGt7XMe1UuiJ+dRnqcfAfbdGeOp+6epm1TK1BJL2mAlQWx5l
73Qo4M7rR7laeq/dqob3olPhcoMLa5z/Lo5vDe7S+LZMuAWjRkSfsoOKQOY3kAP1
eZ2Eh2go4eJ7hHf5VFqBLL8Ci3rd3EOijRkNm3fAQmFJlaFmooBM3Y2Ba+U8cMTH
lgjSFkl1FAWpfwx9aSEECNCvEMm1Ghm6/tJDLV1jyTqwajHnWIZCc+P2AXgnlLzG
HVVfxsOc8FGUJPQHatXYd7worWCxszauhfJ99E4PaoZnAOYUFw2jaZEwo0NBPbD1
AjQ8aciuosv0FKpp/jXDI78/aYAEk662tPsfGmxvAWB+UMFarA9ZTiihK3x/tDPy
GZ6ByGWJYp/0tNNmJRCFhcAYY83EtzHK9h+8LatFA6WrJ4j3dhceUPzrPXjMffNN
0Yg=
-----END ENCRYPTED PRIVATE KEY-----
```

Nach Abschluss des Vorgangs können das Identitätszertifikat und der private Schlüssel in separate Dateien eingefügt werden. Das CA-Zertifikat kann mithilfe der in Schritt 2. der **PKCS12-Erstellung mit OpenSSL** beschriebenen Schritte in eine neue PKCS12-Datei importiert werden.

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.