# Certificaten installeren en verlengen op door het VCC beheerde FTD

## Inhoud



## Inleiding

Dit document beschrijft hoe u zelfondertekende certificaten en certificaten kunt installeren, vertrouwen en vernieuwen die zijn ondertekend door een certificeringsinstantie van een derde partij (CA) of een interne CA op een Firepower Threat Defence (FTD) die wordt beheerd door Firepower Management Center (FMC).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Handmatige certificaatinschrijving vereist toegang tot een vertrouwde CA van derden.
- Voorbeelden van CA-leveranciers van derden zijn onder meer Entrust, Geotrust, GoDaddy, Thawte en VeriSign.
- Controleer of de FTD de juiste kloktijd, datum en tijdzone heeft. Met certificaatverificatie wordt aanbevolen een NTP-server (Network Time Protocol) te gebruiken om de tijd op de FTD te

synchroniseren.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FMCv actief 6.5
- FTDv met 6.5
- Voor het maken van de PKCS12 wordt OpenSSL gebruikt

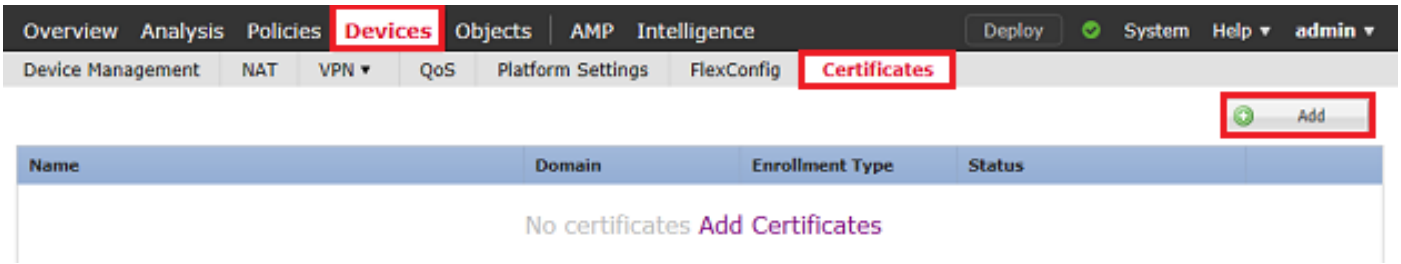
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Configureren

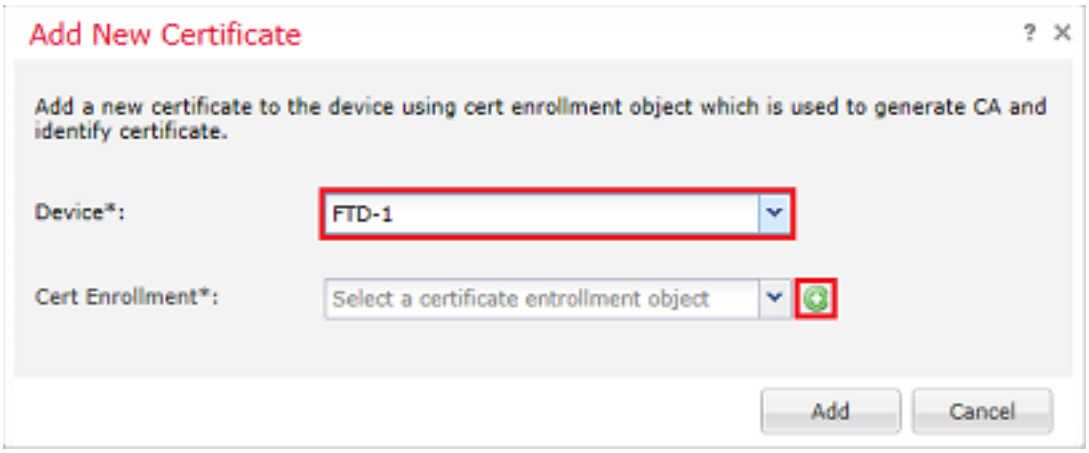
## Certificaatinstallatie

### Zelfondertekende inschrijving

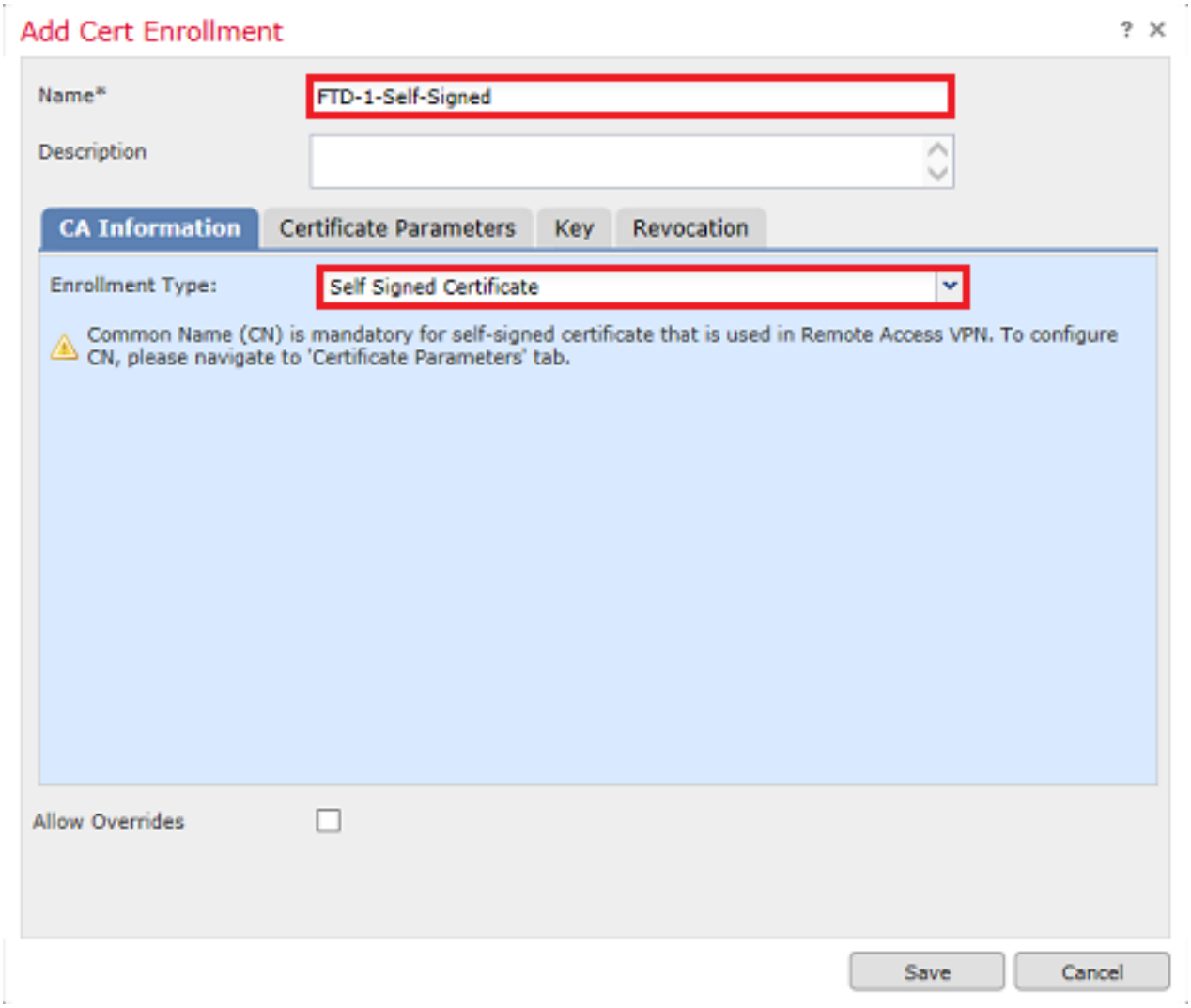
1. Navigeer naar **Apparaten > Certificaten** en klik vervolgens op **Toevoegen** zoals in de afbeelding.



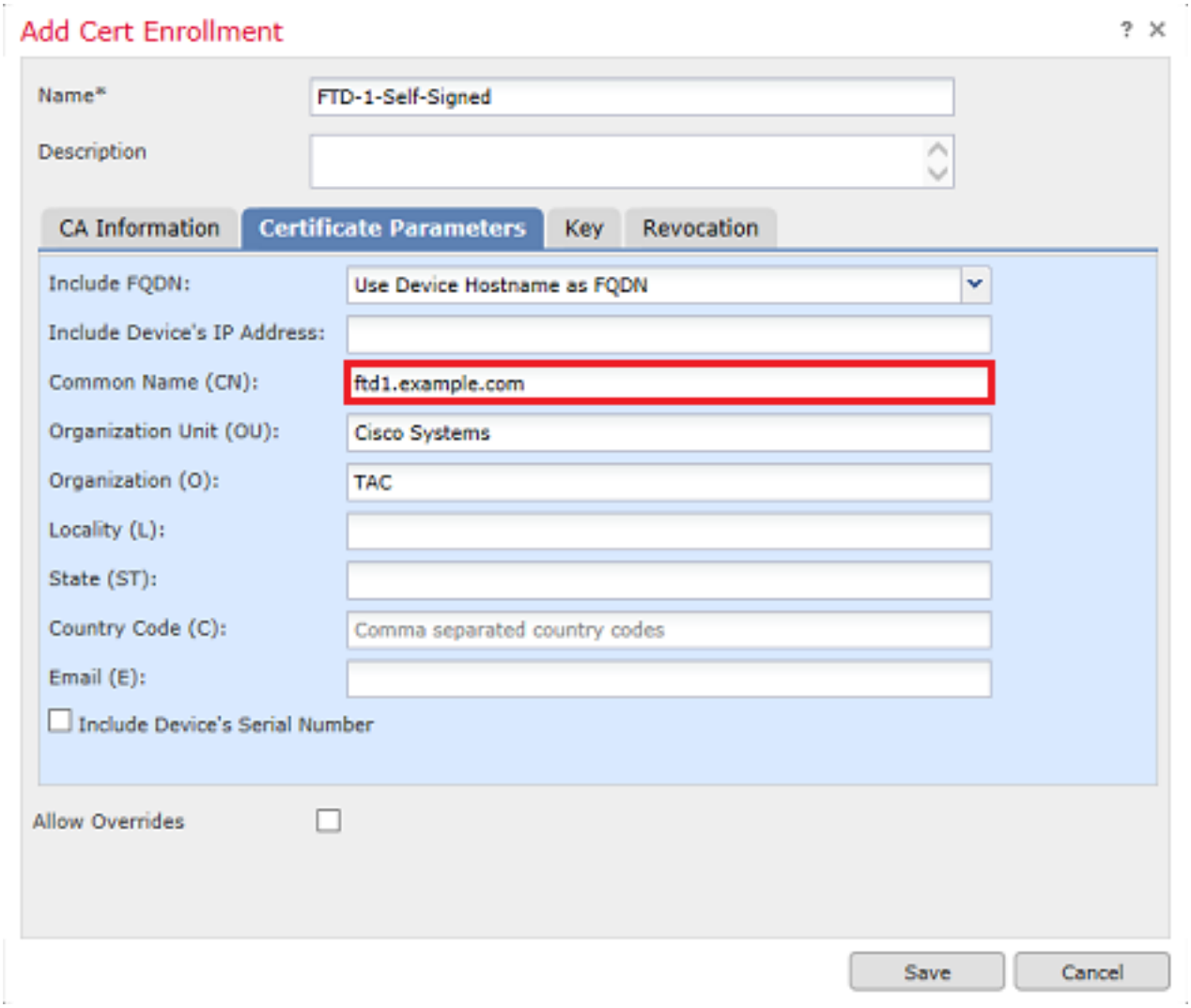

2. Selecteer het apparaat en het certificaat wordt toegevoegd aan in de vervolgkeuzelijst **Apparaat***. Klik vervolgens op het groene **+** symbool zoals in de afbeelding.



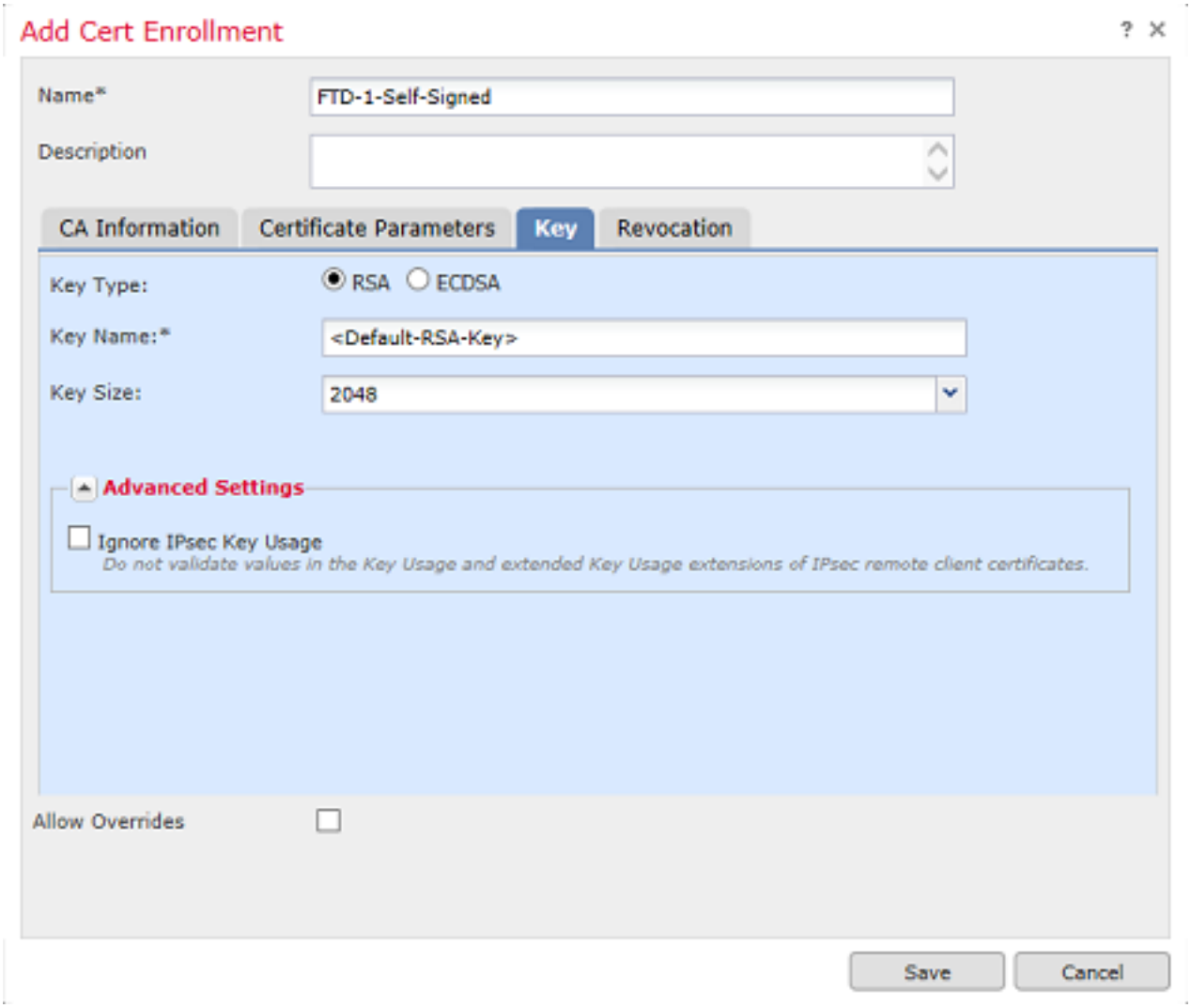

3. Geef een **naam op** voor het trustpoint en selecteer onder het tabblad **CA Information** de optie Inschrijftype: **Zelfondertekend Certificaat** zoals weergegeven in de afbeelding.



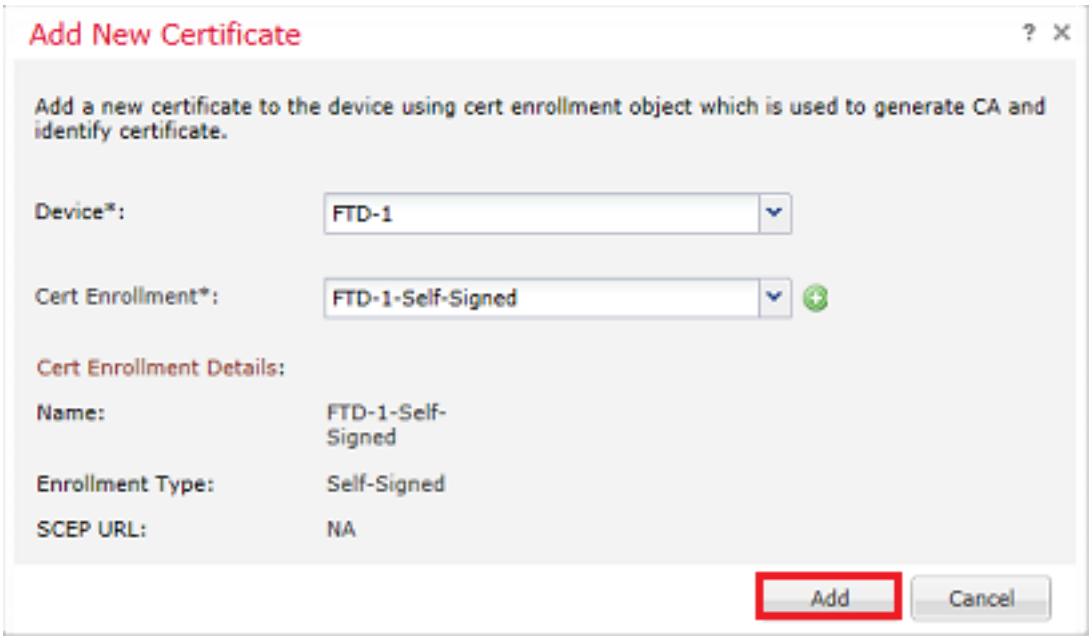

4. Voer in het tabblad **Certificaatparameters** een algemene naam in voor het certificaat. Dit moet overeenkomen met het fqdn- of IP-adres van de service waarvoor het certificaat wordt gebruikt, zoals in de afbeelding.



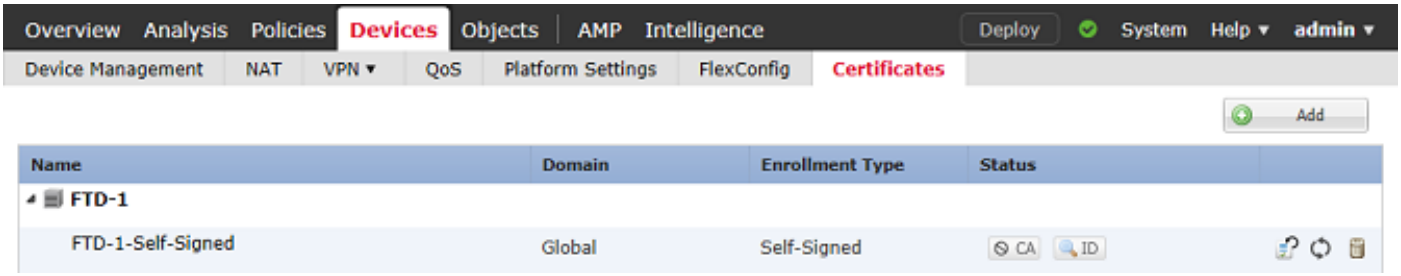

5. (Optioneel) Onder het tabblad **Key** kunnen het type, de naam en de grootte van de private sleutel die voor het certificaat wordt gebruikt, worden gespecificeerd. Standaard gebruikt de toets een RSA-toets met de naam **<Default-RSA-Key>** en een grootte van 2048; het verdient echter aanbeveling voor elk certificaat een unieke naam te gebruiken, zodat niet hetzelfde particuliere/openbare sleutelpaar wordt gebruikt als in de afbeelding.




6. Klik op **Opslaan** en vervolgens op **Toevoegen** zoals in de afbeelding.

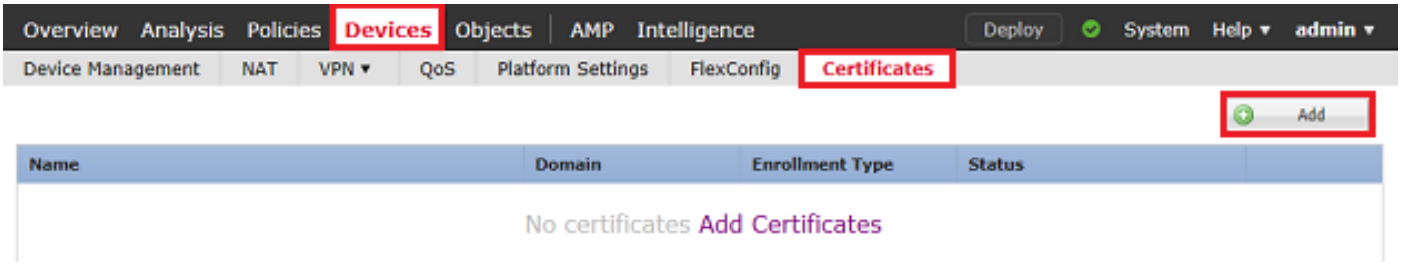



7. Zodra het certificaat is voltooid, wordt het zelfondertekende certificaat in de afbeelding weergegeven.

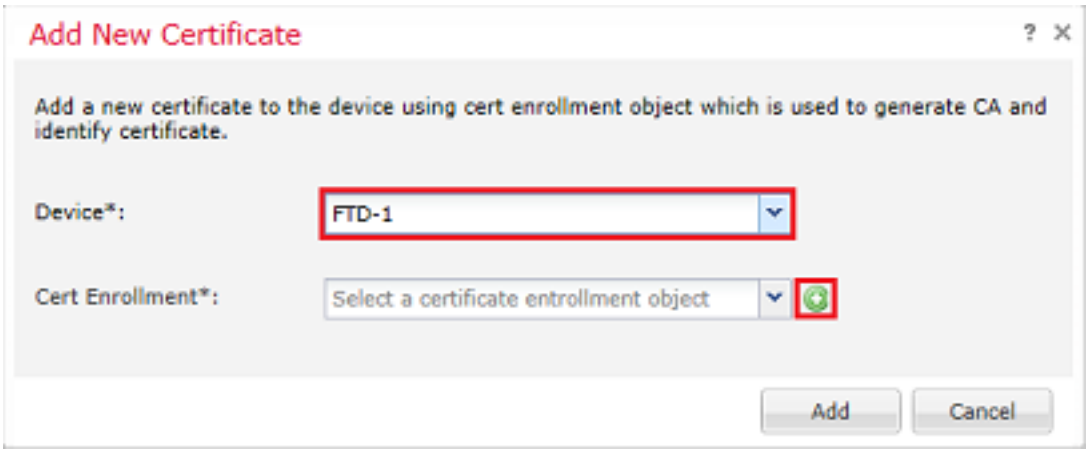



## Handmatige inschrijving

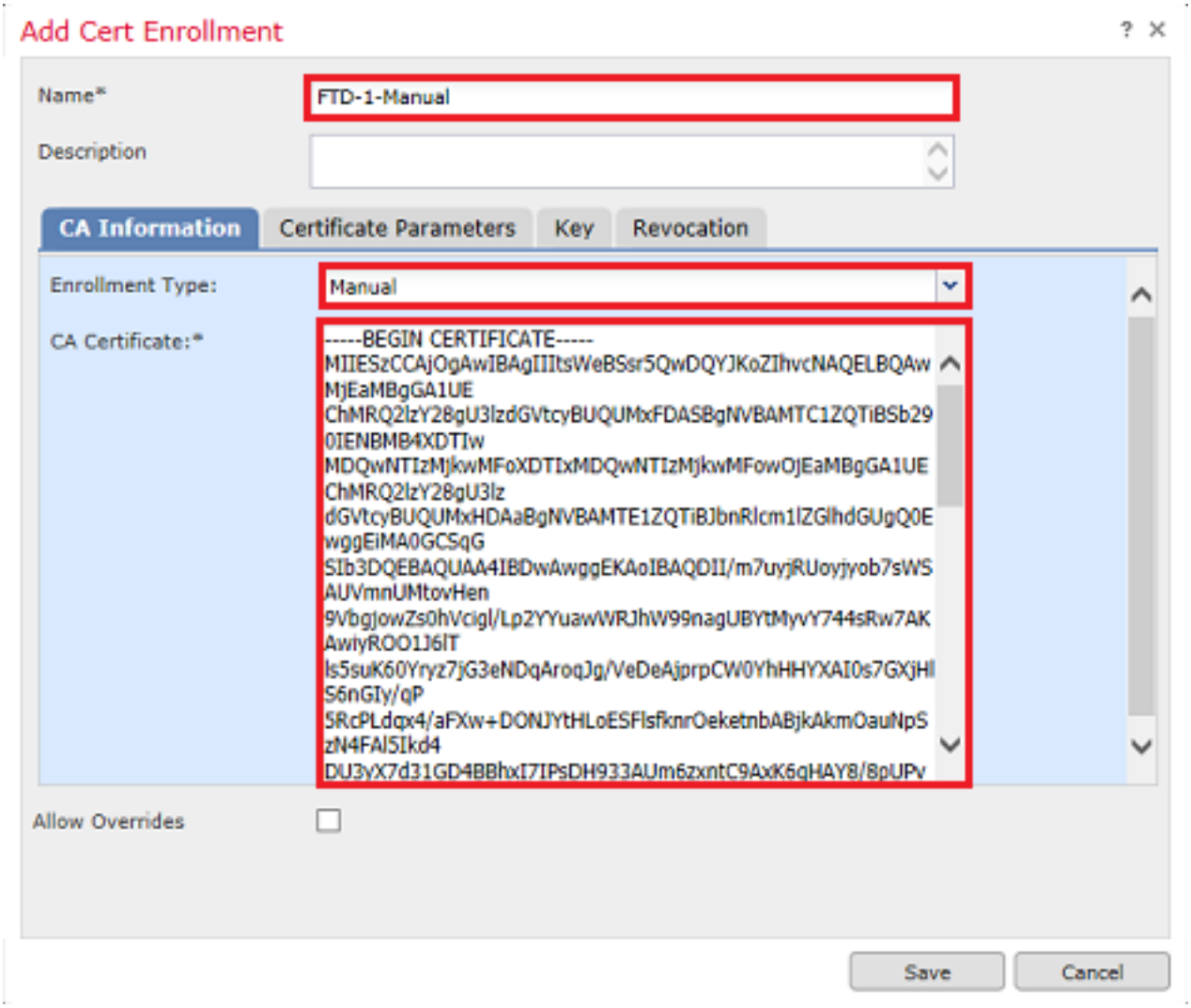
1. Navigeer naar **Apparaten > Certificaten** en klik vervolgens op **Toevoegen** zoals in de afbeelding.



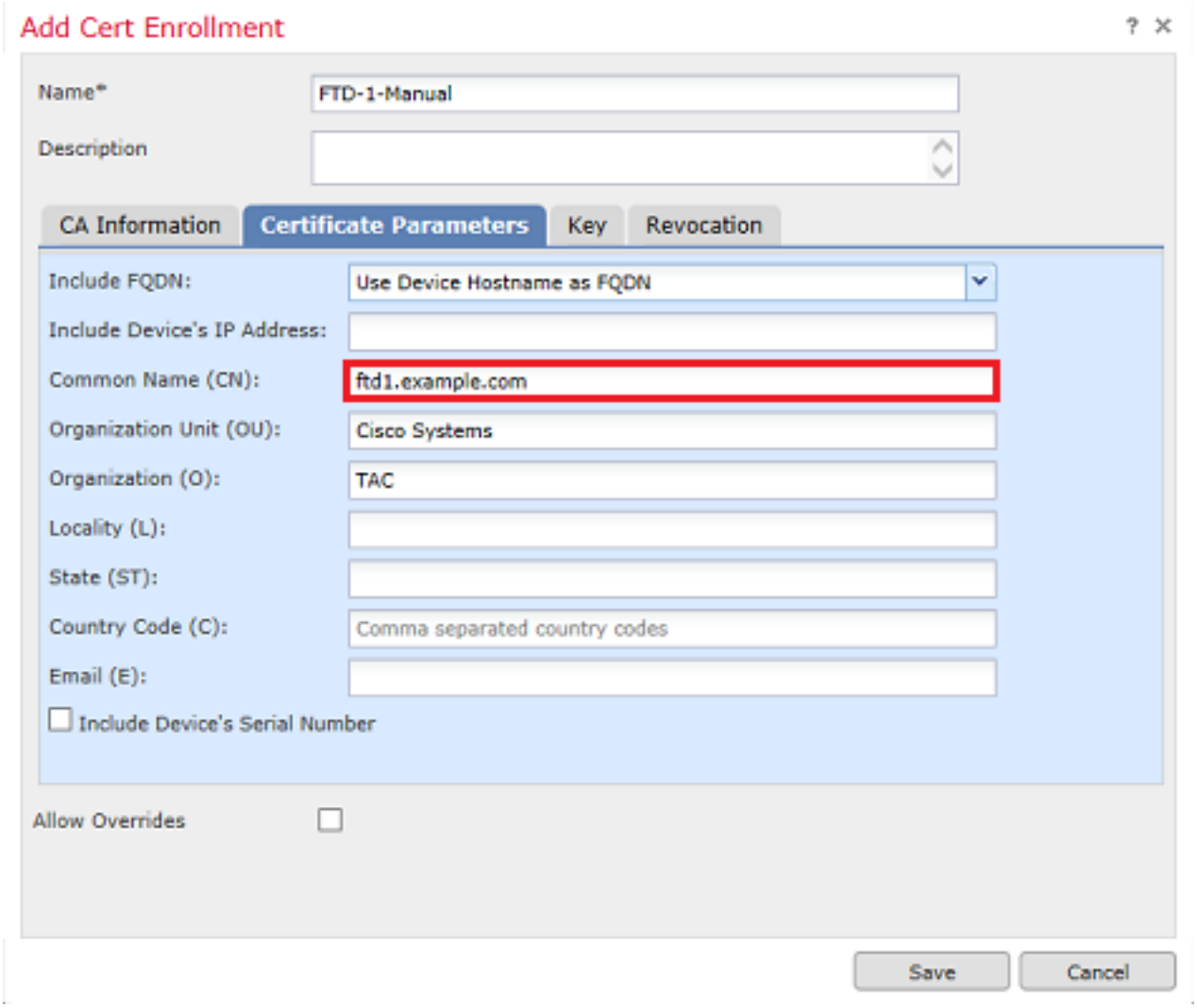

2. Selecteer het apparaat waaraan het certificaat is toegevoegd in de vervolgkeuzelijst **Apparaat*** en klik vervolgens op het groene **+** symbool zoals in de afbeelding.



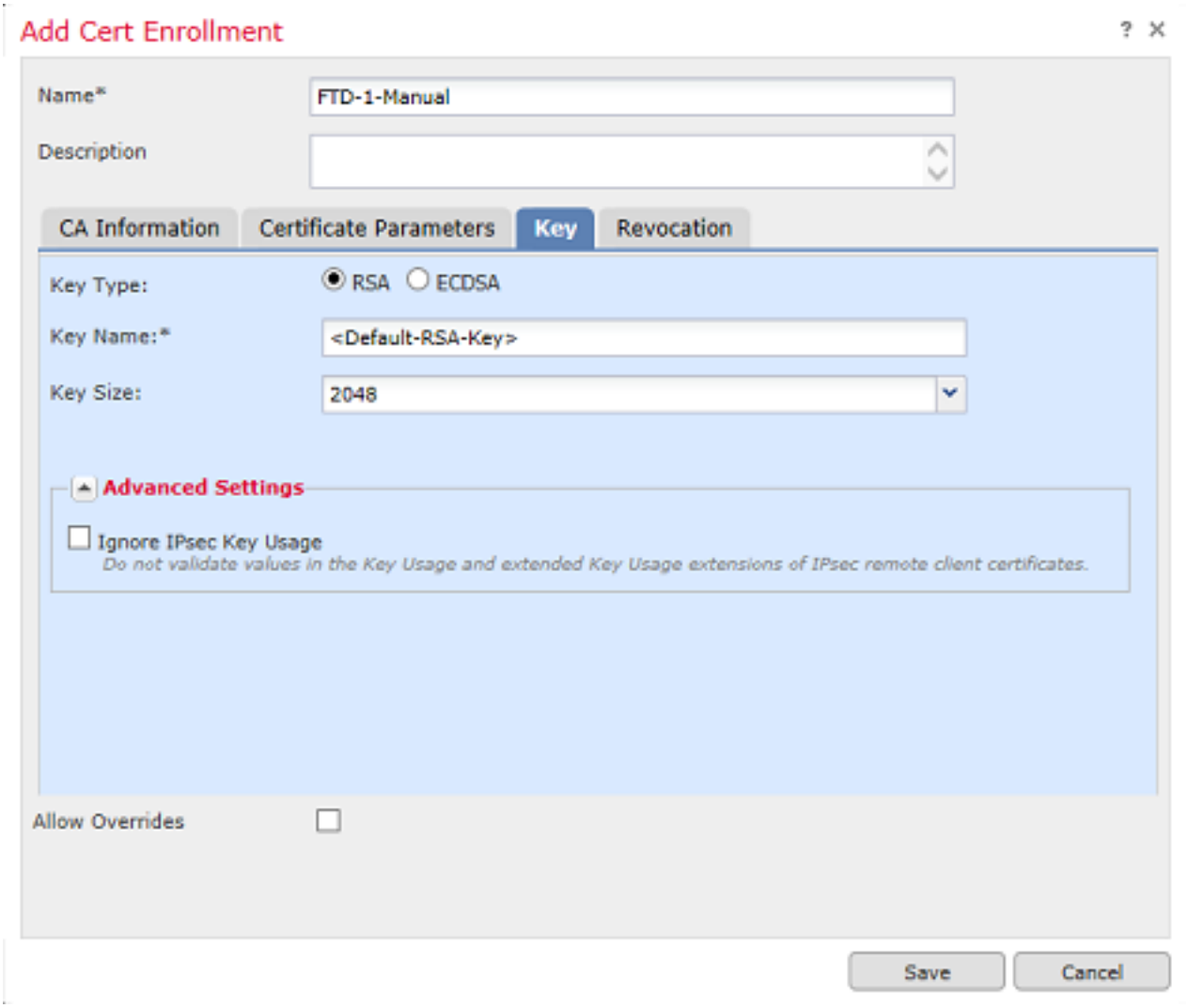

3. Geef een **naam op** voor het trustpoint en selecteer onder het tabblad **CA Information** de optie Inschrijftype: **Handmatig**. Voer het pem-certificaat in van de CA die wordt gebruikt om het identiteitscertificaat te ondertekenen. Als dit certificaat op dit moment niet beschikbaar of bekend is, voeg dan een CA-certificaat als plaatsaanduiding toe en herhaal deze stap zodra het identiteitscertificaat is afgegeven om de werkelijke CA van afgifte toe te voegen zoals in de afbeelding.



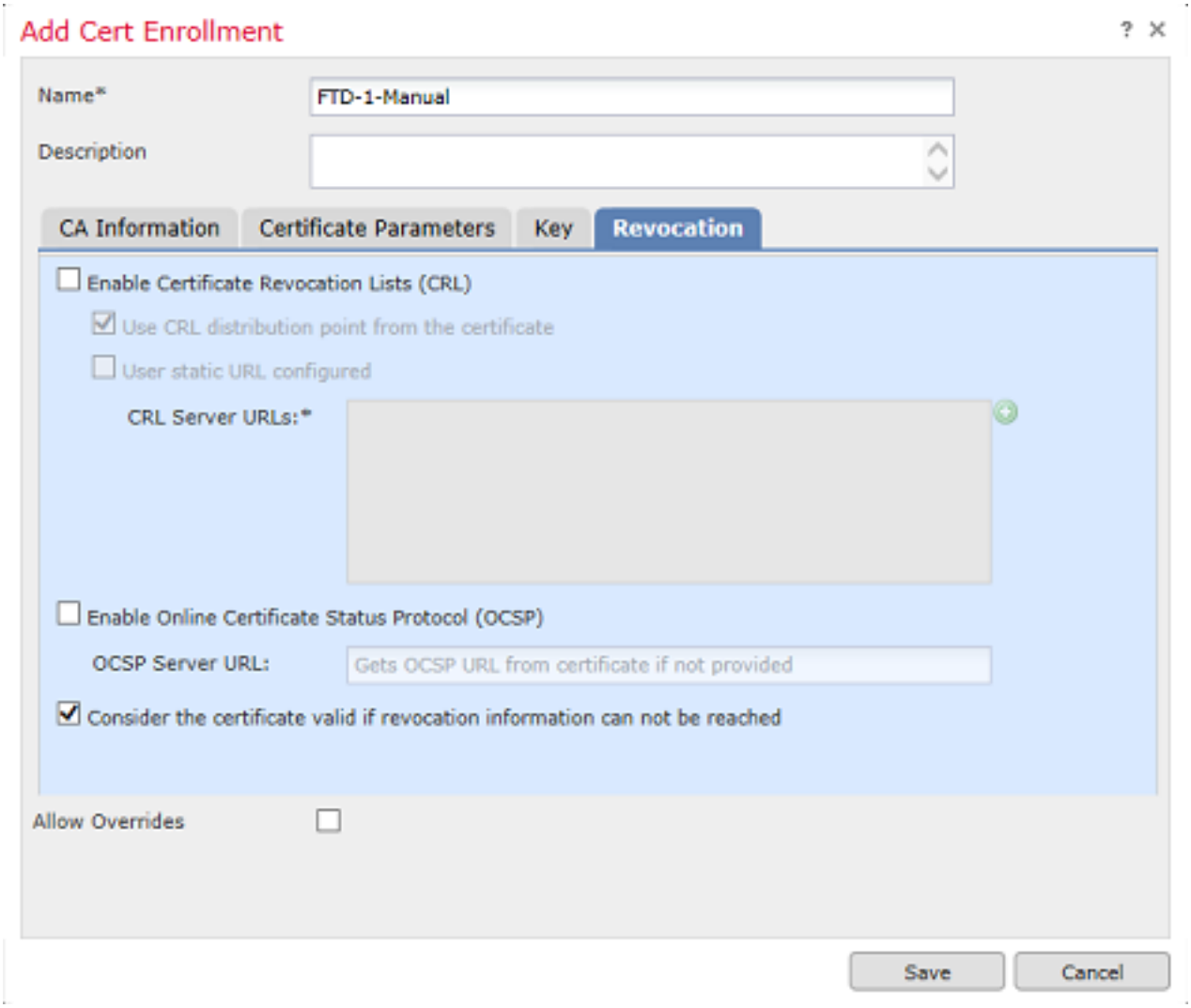

4. Voer in het tabblad **Certificaatparameters** een algemene naam in voor het certificaat. Dit moet overeenkomen met het fqdn- of IP-adres van de service waarvoor het certificaat wordt gebruikt, zoals in de afbeelding.



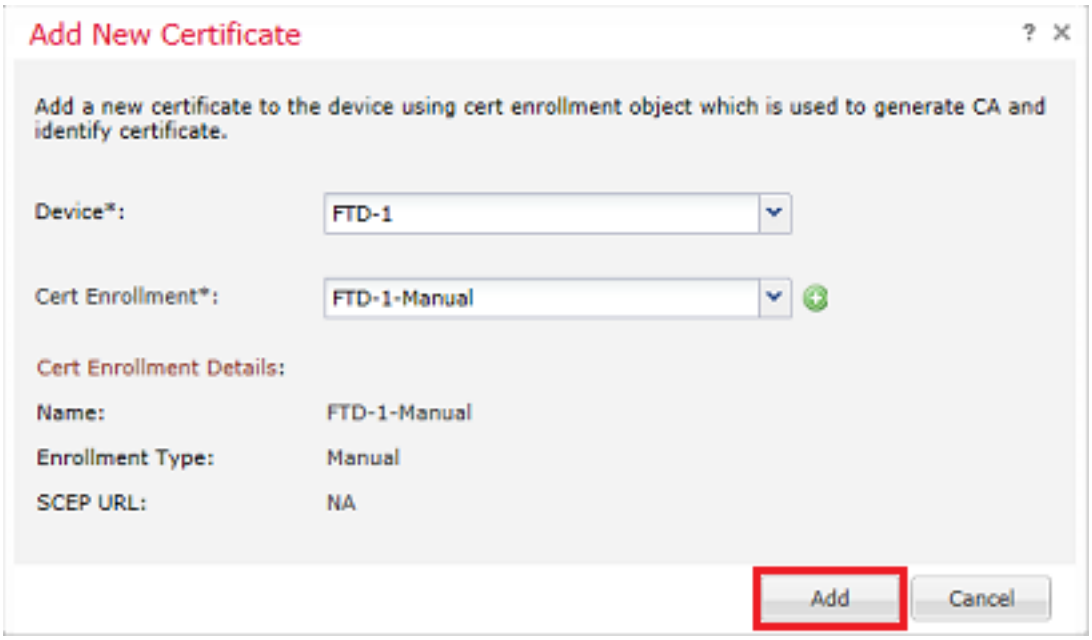

5. (Optioneel) Onder het tabblad **Key** kunnen het type, de naam en de grootte van de private sleutel die voor het certificaat wordt gebruikt, optioneel worden gespecificeerd. Standaard gebruikt de toets een RSA-toets met de naam **<Default-RSA-Key>** en een grootte van 2048; het verdient echter aanbeveling voor elk certificaat een unieke naam te gebruiken, zodat niet hetzelfde particuliere/openbare sleutelpaar wordt gebruikt als in de afbeelding.



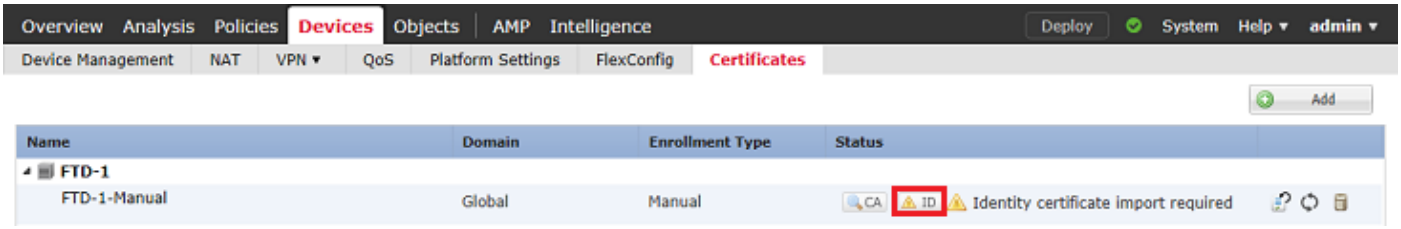

6. (Optioneel) Onder het tabblad **Herroeping** wordt de herroeping van de certificaatlijst (CRL) of het Online Certificate Status Protocol (OCSP) gecontroleerd en kan deze worden geconfigureerd. Standaard is geen van beide ingeschakeld zoals in de afbeelding.




7. Klik op **Opslaan** en vervolgens op **Toevoegen** zoals in de afbeelding.

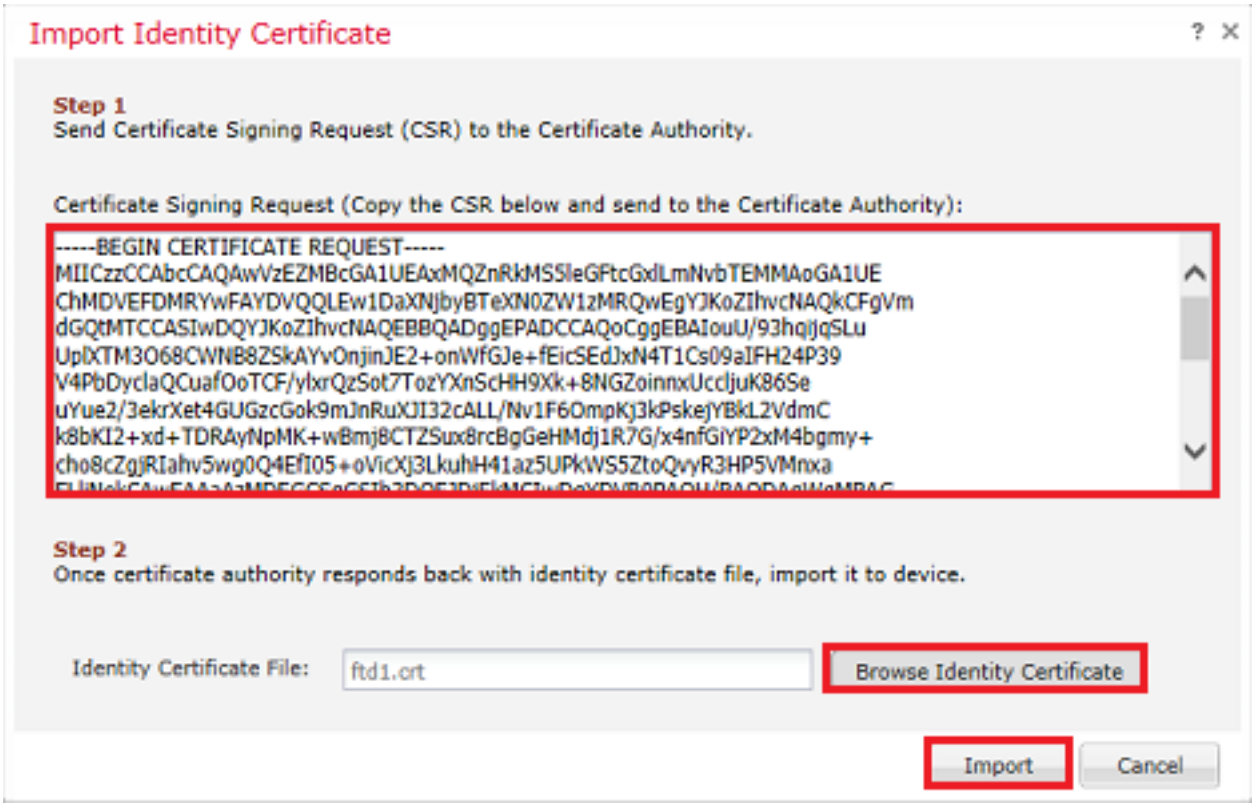



8. Nadat u het verzoek hebt verwerkt, stelt FMC de optie voor om een identiteitsbewijs toe te voegen. Klik op de knop **ID** zoals in de afbeelding.

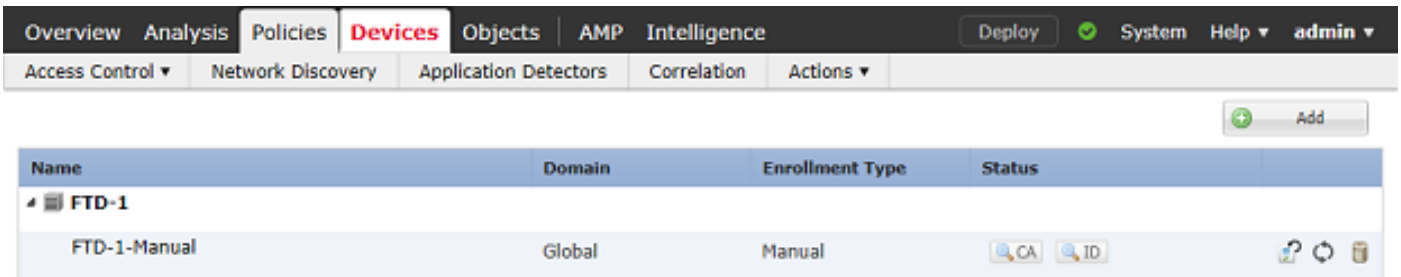



9. Er verschijnt een venster dat aangeeft dat een MVO is gegenereerd. Klik op **Ja** zoals in de afbeelding.


10. Vervolgens wordt een MVO gegenereerd die kan worden gekopieerd en verzonden naar een CA. Na ondertekening van de MVO wordt een identiteitsbewijs verstrekt. Blader naar het meegeleverde identiteitscertificaat en selecteer het en klik vervolgens op **Importeren** zoals in de afbeelding.

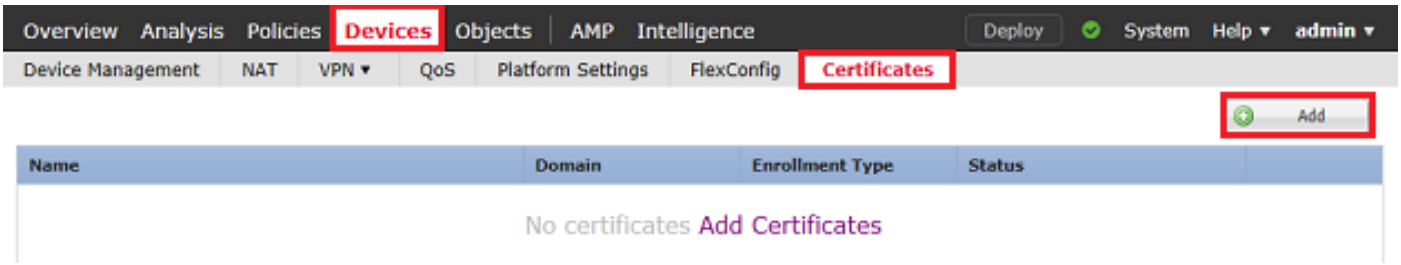



11. Zodra het handmatige certificaat is ingevuld, wordt dit op de afbeelding weergegeven.

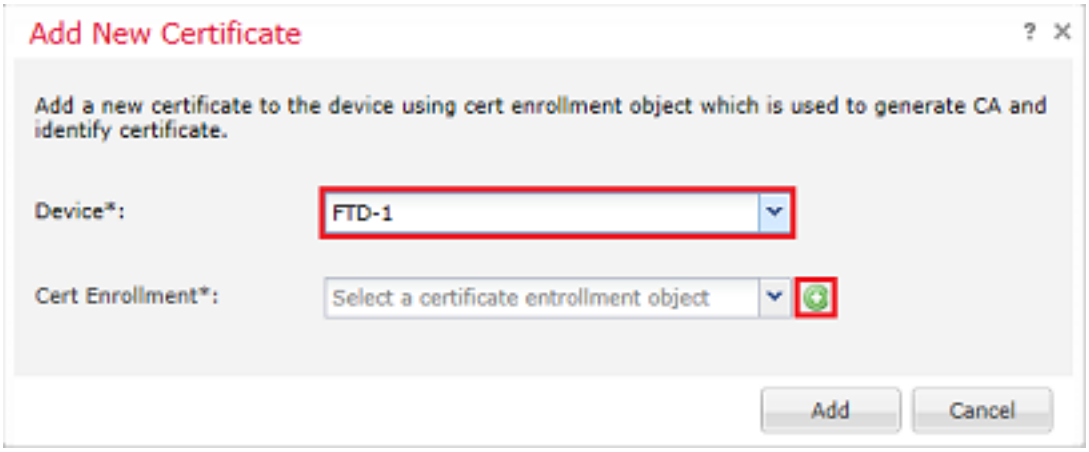


## PKCS C12-inschrijving

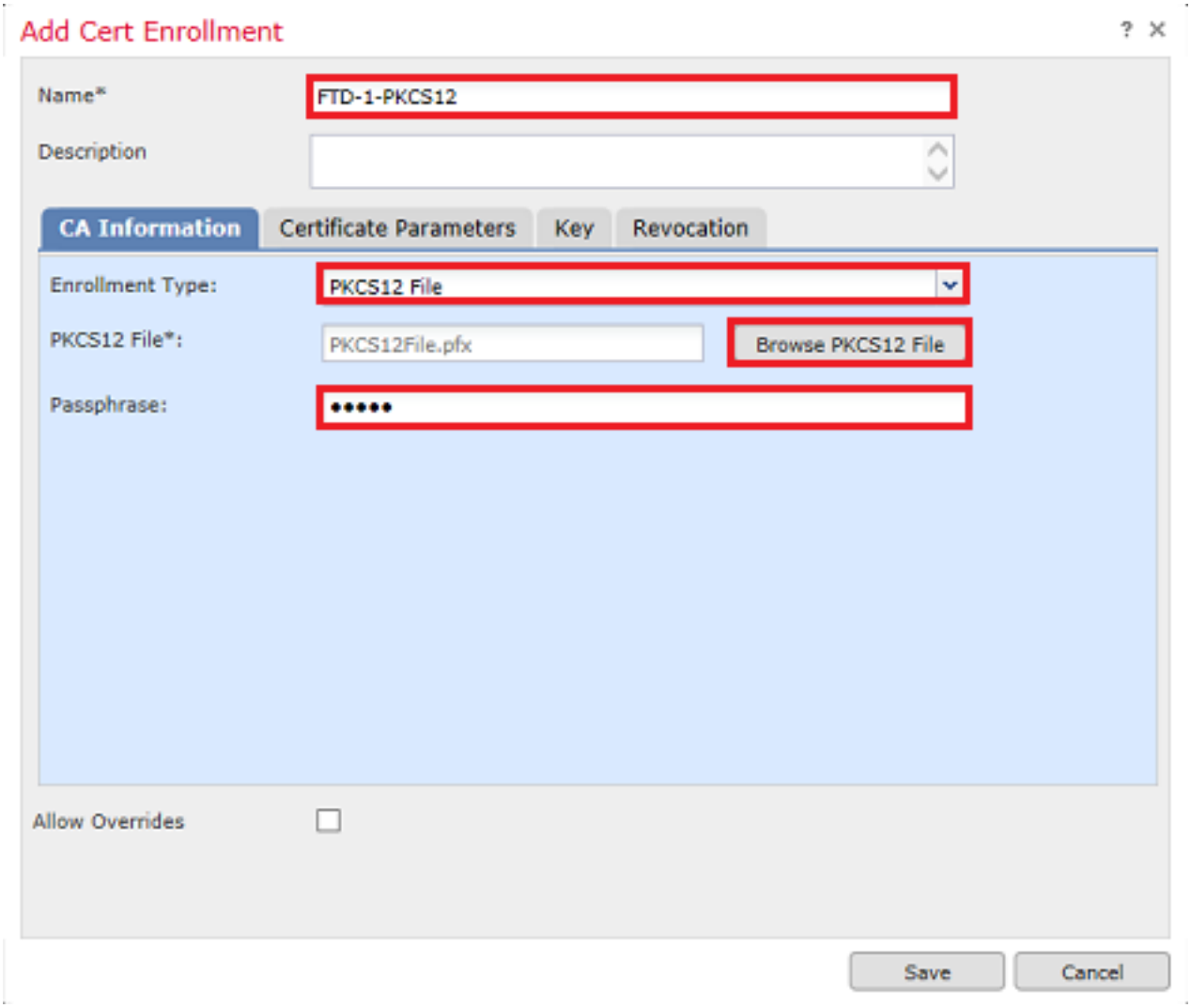
1. Om een ontvangen of gemaakt PKCS12-bestand te installeren, navigeer naar **Apparaten > Certificaten** en klik vervolgens op **Toevoegen** zoals in de afbeelding.



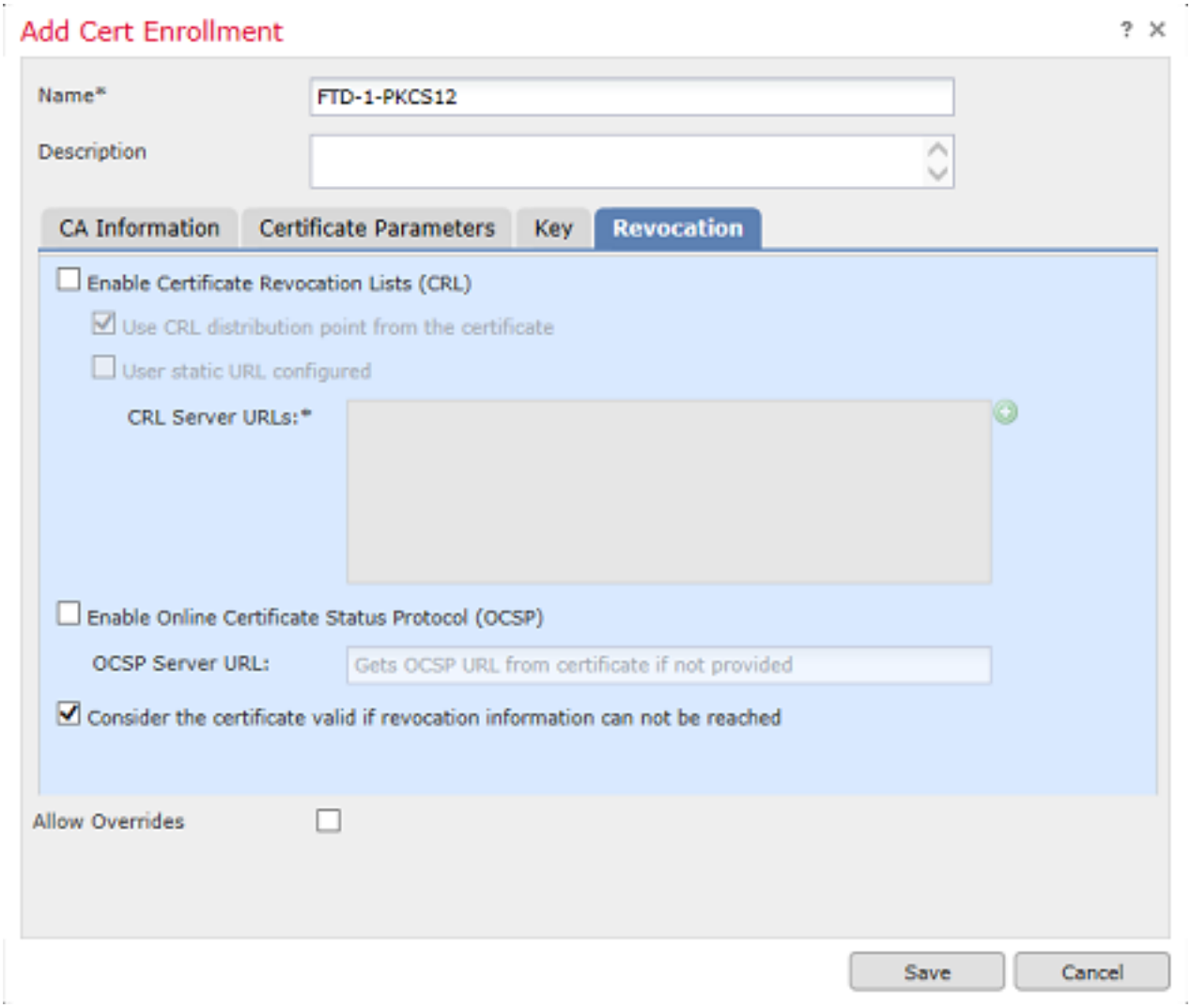

2. Selecteer het apparaat waaraan het certificaat is toegevoegd in de vervolgkeuzelijst **Apparaat*** en klik vervolgens op het groene **+** symbool zoals in de afbeelding.



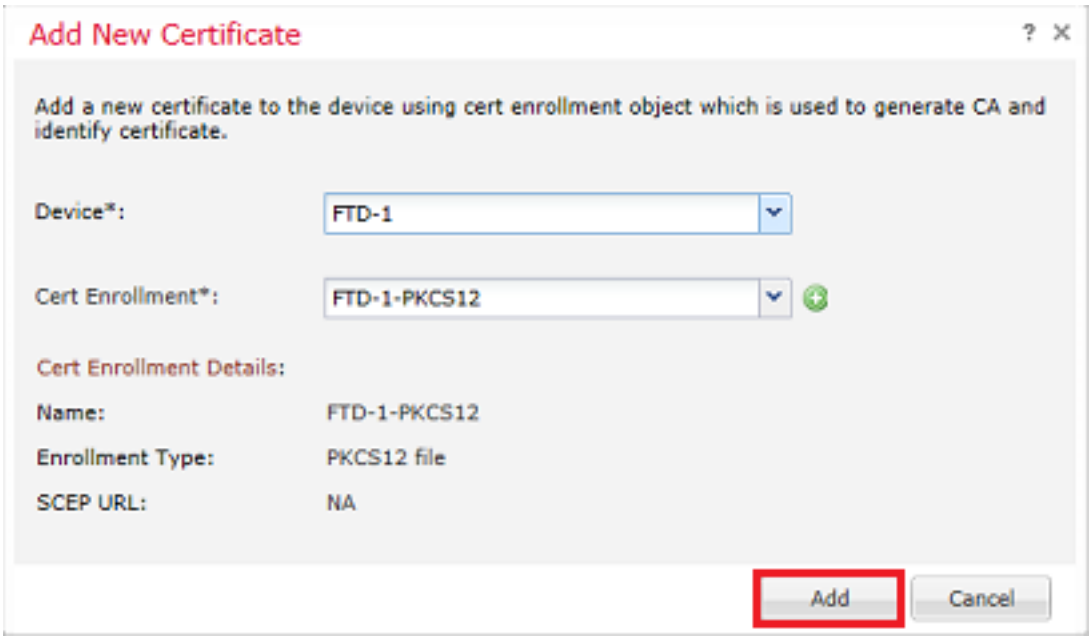

3. Geef een **naam op** voor het trustpoint en selecteer onder het tabblad **CA Information** de optie Inschrijftype: **PKCS 12-bestand**. Blader naar het gemaakte PKCS12-bestand en selecteer het. Voer de gebruikte wachtcode in wanneer u de PKCS12 maakt zoals in de afbeelding.



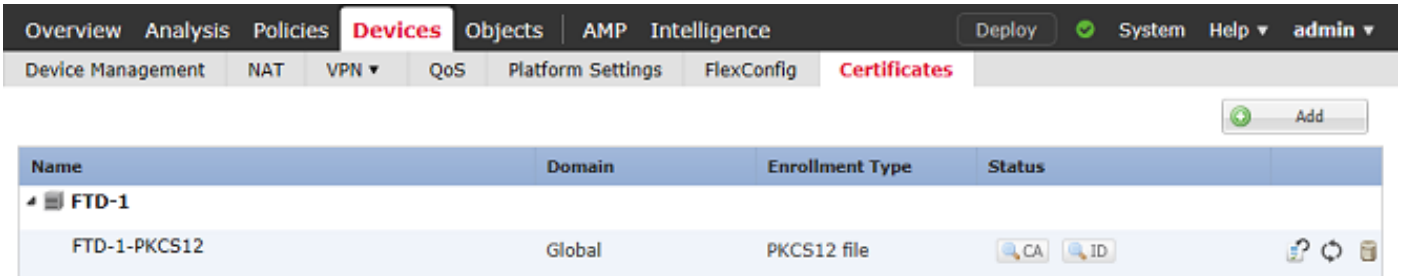

4. (Optioneel) De tabbladen **Certificaatparameters** en **Sleutel** zijn grijs omdat deze al met de PKCS12 zijn gemaakt. Het tabblad **Herroeping** om CRL en/of OCSP herroepingscontrole in te schakelen kan echter worden gewijzigd. Standaard worden beide geselecteerd zoals in de afbeelding.




5. Klik op **Opslaan** en vervolgens op **Toevoegen** in dit venster zoals in de afbeelding.



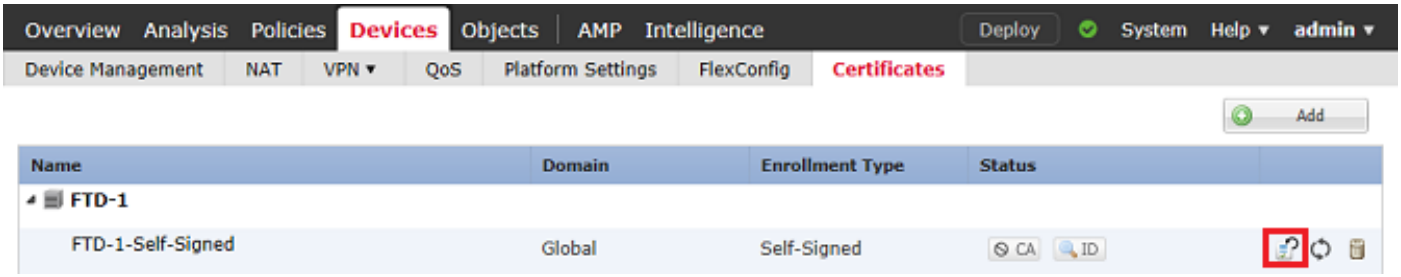

6. Wanneer het certificaat is ingevuld, ziet het PKCS12-certificaat eruit zoals in de afbeelding.



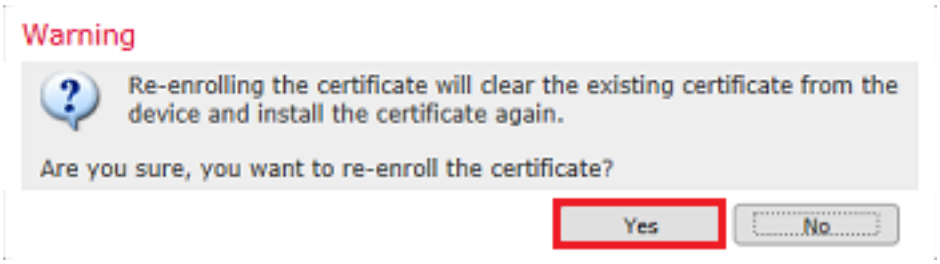

## Certificaatverlenging

### Verlenging van het zelfondertekende certificaat

1. Druk op de knop Certificaat opnieuw inschrijven zoals in de afbeelding.



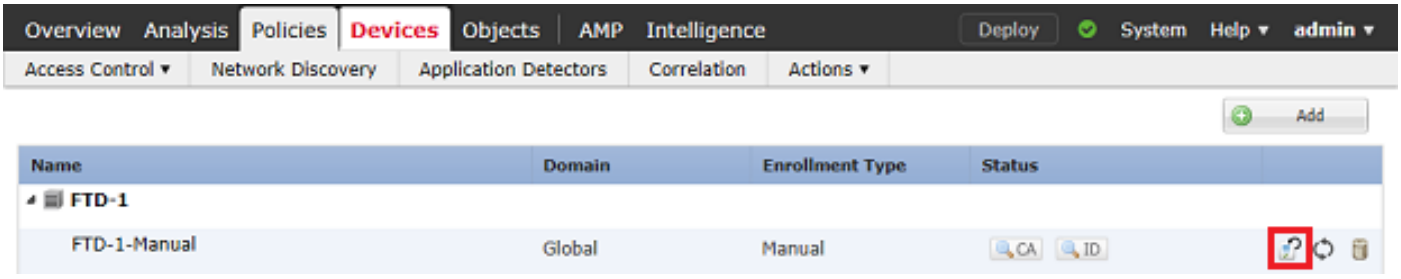

2. Een venster toont aan dat het zelfondertekende certificaat wordt verwijderd en vervangen. Klik op **Ja** zoals in de afbeelding.




3. Een hernieuwd zelfondertekend wordt naar het FTD gedrukt. Dit kan worden geverifieerd wanneer u op de knop ID klikt en de Geldige tijd controleert.

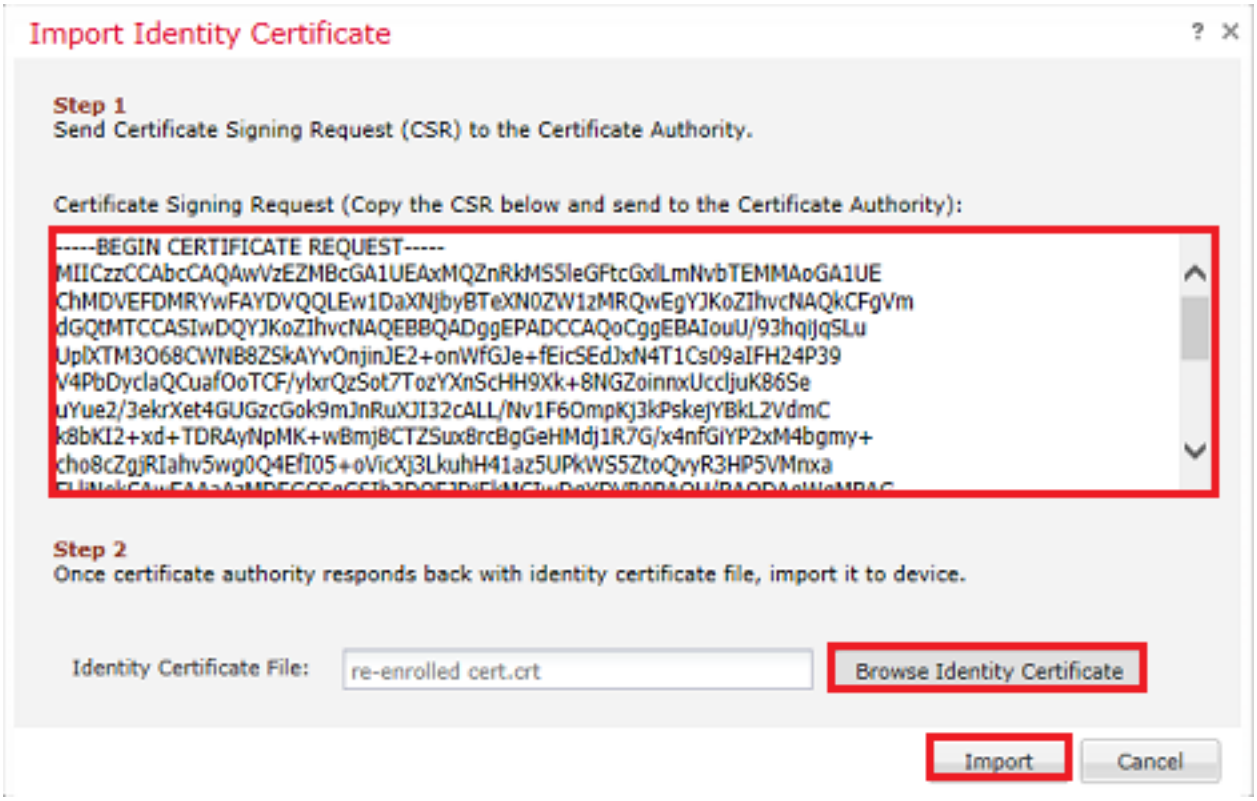
### Handmatige certificaatverlenging

1. Druk op de knop Certificaat opnieuw inschrijven zoals in de afbeelding.




2. Een venster toont aan dat een verzoek voor het ondertekenen van een certificaat wordt gegenereerd. Klik op **Ja** zoals in de afbeelding.


3. In dit venster wordt een MVO gegenereerd die kan worden gekopieerd en verzonden naar dezelfde CA die het identiteitsbewijs eerder heeft ondertekend. Zodra de MVO is ondertekend, wordt het nieuwe identiteitsbewijs verstrekt. Blader naar het meegeleverde identiteitscertificaat en selecteer het en klik vervolgens op **Importeren** zoals in de afbeelding.




4. Het FTD wordt voorzien van een nieuw handboek. Dit kan worden geverifieerd wanneer u op de knop ID klikt en de Geldige tijd controleert.

### PKCS C12-verlenging

Als u op de knop Certificaat opnieuw inschrijven klikt, wordt het certificaat niet verlengd. Om een PKCS12 te vernieuwen moet er een nieuw PKCS12-bestand gemaakt en geüpload worden met gebruik van de eerder genoemde methoden.

## PKCS E12-conversie met OpenSSL

1. Met het gebruik van OpenSSL of een soortgelijke toepassing, genereert u een privé-sleutel en een verzoek om certificaatondertekening (CSR). Dit voorbeeld toont een 2048-bits RSA-sleutel met de naam **private.key** en een CSR met de naam **ftd1.csr** die in OpenSSL is gemaakt:

```
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. Kopieer de gegenereerde CSR en verstuur deze naar een CA. Na ondertekening van de MVO wordt een identiteitsbewijs verstrekt. Meestal worden ook de CA-certificaten geleverd. Als u een PKCS12 wilt maken, voert u een van deze opdrachten uit in OpenSSL:

Gebruik deze opdracht om alleen het CA-certificaat op te nemen dat is afgegeven in de PKCS12:

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

- **ftd.pfx** is de naam van het pkcs12 bestand (in der formaat) dat wordt geëxporteerd door openssl.
- **ftd.crt** is de naam van het ondertekende identiteitsbewijs dat door CA in pem-formaat is afgegeven.
- **private.key** is het sleutelpaar dat in Stap 1 is gemaakt.
- **ca.crt** is het certificaat van de certificeringsinstantie van afgifte in pem-formaat.

Als het certificaat deel uitmaakt van een keten met een wortel CA en 1 of meer tussenliggende CA's, kan deze opdracht worden gebruikt om de volledige keten in de PKCS12 toe te voegen:

```
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** is de naam van het pkcs12 bestand (in der formaat) dat wordt geëxporteerd door OpenSSL.
- **ftd.crt** is de naam van het ondertekende identiteitsbewijs dat door CA in pem-formaat is afgegeven.
- **private.key** is het sleutelpaar dat in Stap 1 is gemaakt.
- **cachain.pem** is een bestand dat de CA-certificaten bevat in de keten die beginnen met de uitgifte van tussenliggende CA en eindigt met de root CA in pem-formaat.

Als een PKCS7-bestand (.p7b, .p7c) wordt teruggegeven, kunnen deze opdrachten ook worden gebruikt om de PKCS12 te maken. Als de p7b in het gegevenstype der is, zorg er dan voor dat **der**

aan de argumenten wordt toegevoegd, anders niet inbegrepen:

```
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: *****
```

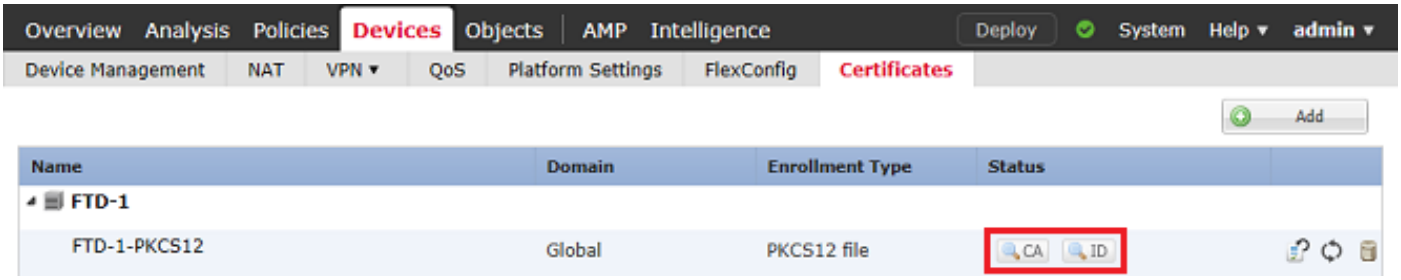
- **ftd.p7b** is de PKCS7 teruggestuurd door de CA met het ondertekende identiteitsbewijs en de CA-keten.
- **ftdpem.crt** is het geconverteerde p7b-bestand.
- **ftd.pfx** is de naam van het pkcs12 bestand (in der formaat) dat wordt geëxporteerd door OpenSSL.
- **private.key** is het sleutelpaar dat in Stap 1 is gemaakt.

# Verifiëren

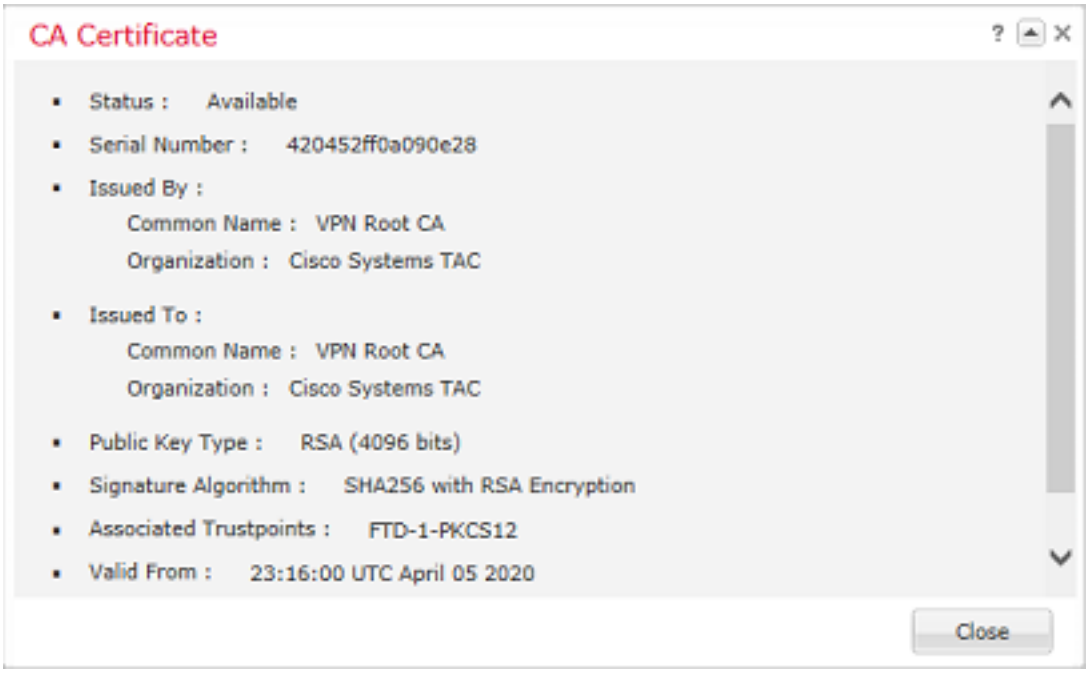
Gebruik deze sectie om te controleren of uw configuratie goed werkt.

## Geïnstalleerde certificaten bekijken in FMC

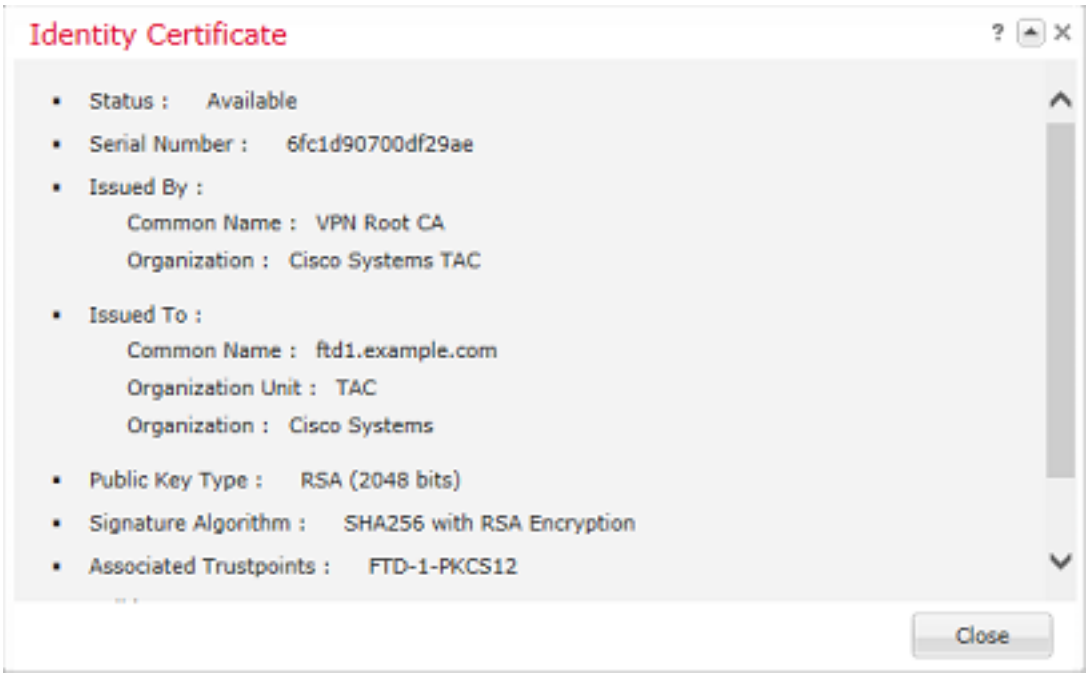
Ga in het VCC naar **Apparaten > Certificaten**. Voor de relevante trustpoint, klik op de **CA** of **ID** om meer details over het certificaat te bekijken zoals getoond in de afbeelding.




Controleer het CA-certificaat zoals in de afbeelding.




Controleer het identiteitscertificaat zoals aangegeven in de afbeelding.




## Geïnstalleerde certificaten bekijken in CLI

SSH naar de FTD en voer de opdracht **tonen crypto ca certificaat**.

```
> 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
```

# Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

## Debug opdrachten

Debugs kunnen worden uitgevoerd vanaf de diagnostische CLI nadat de FTD is verbonden via SSH in het geval van een fout in de installatie van een SSL-certificaat:

**debug crypto ca 14**

In oudere versies van FTD zijn deze debugs beschikbaar en aanbevolen voor probleemoplossing:

**debug crypto ca 255**

**debug crypto ca-bericht 255**

**debug crypto ca transactie 255**

## Veelvoorkomende problemen

Zie nog steeds het bericht "Identiteitscertificaat importeren vereist" nadat u een identiteitsbewijs hebt geïmporteerd.

Dit kan zich voordoen vanwege twee verschillende problemen:

1. Het CA-certificaat van afgifte is niet toegevoegd bij handmatige inschrijving

Wanneer het identiteitscertificaat wordt geïmporteerd, wordt het bij handmatige inschrijving gecontroleerd aan de hand van het CA-certificaat dat is toegevoegd onder het tabblad CA-informatie. Soms hebben netwerkbeheerders niet het CA-certificaat voor de CA die wordt gebruikt om hun identiteitscertificaat te ondertekenen. In deze situatie, is het noodzakelijk om een plaatsaanduiding CA certificaat toe te voegen wanneer u handmatige inschrijving doet. Zodra het Identiteitscertificaat is afgegeven en CA-certificaat is verstrekt, kan een nieuwe handmatige inschrijving worden gedaan met het juiste CA-certificaat. Wanneer u opnieuw door de handmatige inschrijvingswizard gaat, dient u dezelfde naam en grootte voor het sleutelpaar op te geven als bij de oorspronkelijke handmatige inschrijving. Als dit eenmaal is gedaan, kan in plaats van de MVO die opnieuw naar de CA wordt doorgestuurd, het eerder afgegeven identiteitsbewijs worden geïmporteerd in het nieuw gecreëerde trustpoint met het juiste CA-certificaat.

Om te controleren of hetzelfde CA-certificaat is toegepast bij handmatige inschrijving, klikt u op de CA-toets zoals opgegeven in het onderdeel Verifiëren of controleert u de uitvoer van **crypto CA-certificaten tonen**. Velden zoals het afgegeven nummer en het serienummer kunnen worden vergeleken met de velden in het CA-certificaat dat door de certificeringsinstantie wordt verstrekt.

2. Het sleutelpaar in het aangemaakte trustpoint is anders dan het sleutelpaar dat wordt gebruikt wanneer de MVO voor het afgegeven certificaat wordt aangemaakt.

Bij handmatige inschrijving, wanneer de sleutelpaar en MVO worden gegenereerd, wordt de openbare sleutel toegevoegd aan de MVO zodat deze kan worden opgenomen in het afgegeven identiteitsbewijs. Indien om de een of andere reden het sleutelpaar op het FTD wordt gewijzigd of het afgegeven identiteitsbewijs een andere openbare sleutel bevat, installeert het FTD het afgegeven identiteitsbewijs niet. Om te controleren of dit is gebeurd, zijn er twee verschillende tests:

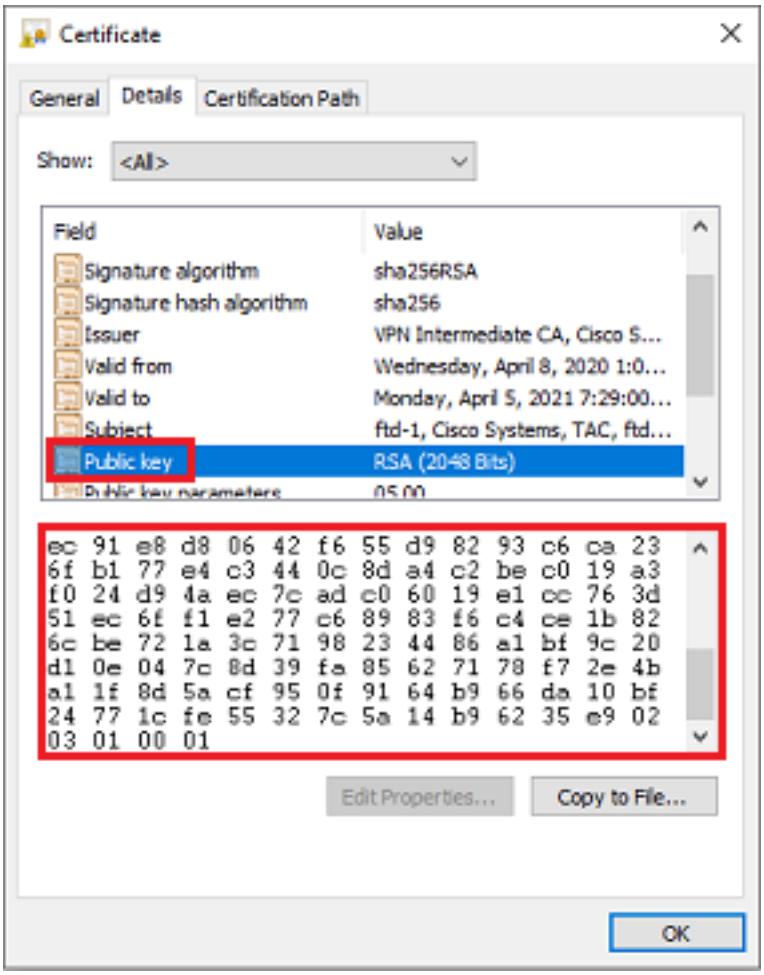
In OpenSSL kunnen deze opdrachten worden gegeven om de openbare sleutel in de CSR te vergelijken met de openbare sleutel in het afgegeven certificaat:

```
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** is de MVO die bij handmatige inschrijving uit het VCC wordt gekopieerd.
- **id.crt** is het identiteitsbewijs dat door CA is ondertekend.

De openbare sleutelwaarde van het FTD kan ook worden vergeleken met de openbare sleutel van het afgegeven identiteitsbewijs. Merk op dat de eerste tekens in het certificaat niet overeenstemmen met die in de FTD-uitvoer vanwege opvulling:

Afgegeven identiteitscertificaat geopend op Windows-pc:




Uitgetrokken publiek belangrijke output van identiteitsbewijs:

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

**Toon crypto key mypubkey rsa** uitvoer van FTD. Wanneer handmatige inschrijving is uitgevoerd, is de **<Default-RSA-Key>** gebruikt om de CSR te maken. De vetgedrukte sectie komt overeen met de geëxtraheerde openbare toetsuitvoer van het identiteitsbewijs.

```
> 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
```

Rood X naast CA in FMC

Dit kan gebeuren met PKCS12 inschrijving omdat het CA-certificaat niet is opgenomen in het PKCS12-pakket.


Om dit te verhelpen, heeft de PKCS12 het CA-certificaat nodig.

Geef deze opdrachten uit om het identiteitsbewijs en de persoonlijke sleutel te extraheren. Het wachtwoord dat wordt gebruikt bij het maken van PKCS12 en de beveiligde privé-sleutel zijn nodig:

```
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-----
```

Na voltooiing kunnen het identiteitscertificaat en de privésleutel in aparte bestanden worden geplaatst en kan het CA-certificaat worden geïmporteerd in een nieuw PKCS12-bestand met behulp van de stappen die worden genoemd in Stap 2. van de **PKCS12-creatie met OpenSSL**.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.