

Probleemoplossing Certificaatfout "CA-certificaat" niet configureren; op FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

[Stap 1. Zoek het .pfx certificaat](#)

[Stap 2. De certificaten en de sleutel uit het .pfx bestand halen](#)

[Stap 3. Controleer de certificaten in een Teksteditor](#)

[Stap 4. Verifieer de privé-sleutel in een Kladblok](#)

[Stap 5. De CA Certs splitsen](#)

[Stap 6. De certificaten samenvoegen in een PKCS12-bestand](#)

[Stap 7. Het PKCS12-bestand in het VCC importeren](#)

[Verifiëren](#)

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen en de importfout van de certificaatinstantie (CA) kunt verhelpen op Firepower Threat Defence devices die door FMC worden beheerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Public Key Infrastructure (PKI)
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- OpenSSL

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- MacOS x 10.14.6
- VCC 6.4
- OpenSSL

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 de potentiële impact van elke opdracht begrijpen.

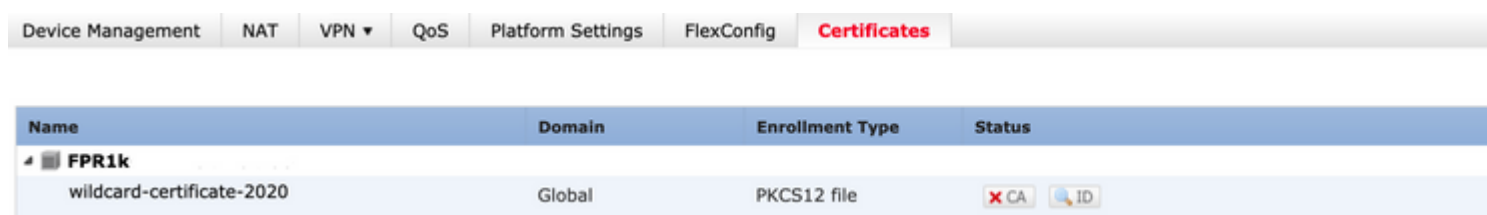
Achtergrondinformatie

Opmerking: op FTD-apparaten is het CA-certificaat nodig voordat het Certificate Signing Verzoek (CSR) wordt gegenereerd.



- Als de CSR wordt gegenereerd in een externe server (zoals Windows Server of OpenSSL), is de handmatige inschrijvingsmethode bedoeld te mislukken, aangezien FTD handmatige toeteninschrijving niet ondersteunt. Er moet een andere methode worden gebruikt, zoals PKCS12.

Probleem

In dit specifieke scenario toont het VCC een rood kruis in de CA-certificaatstatus (zoals weergegeven in de afbeelding), waarin staat dat de inschrijving van het certificaat het CA-certificaat niet heeft geïnstalleerd. Deze fout wordt vaak gezien wanneer het certificaat niet goed is verpakt of het PKCS12-bestand niet het juiste emittentencertificaat bevat zoals in de afbeelding.



The screenshot shows the 'Certificates' tab in the FMC GUI. The table below is a representation of the data shown in the image.

Name	Domain	Enrollment Type	Status
FP1k wildcard-certificate-2020	Global	PKCS12 file	 CA 

Opmerking: In nieuwere FMC versies is dit probleem aangepakt om het ASA gedrag dat een extra trustpoint creëert met de wortel CA opgenomen in de vertrouwensketen van de .pfx cert.

Oplossing

Stap 1. Zoek het .pfx certificaat

Ontvang het pfx-certificaat dat in de FMC GUI was ingeschreven, **sla** het op en zoek het bestand in de Mac Terminal (CLI).

```
docs# ls -l
total 16
-rw-r--r-- 1 holguins staff 4701 May 23 15:11 c
```

ls

Stap 2. De certificaten en de sleutel uit het .pfx bestand halen

Haal het clientcertificaat (niet CA-certificaten) uit het pfx-bestand (het wachtwoord dat is gebruikt om het .pfx-bestand te genereren is vereist).

```
openssl pkcs12 -in cert.pfx -clcerts -nokeys -out id.pem
```

```
docs# openssl pkcs12 -in cert.pfx -clcerts -nokey
[Enter Import Password:
MAC verified OK
```

identiteits-export

Haal de CA-certificaten uit (geen client-certificaten).

```
openssl pkcs12 -in cert.pfx -cacerts -nokeys -out certs.pem
```

```
docs# openssl pkcs12 -in cert.pfx -cacerts -nokey
[Enter Import Password:
MAC verified OK
```

cacerts exporteren

Haal de privé-toets uit het pfx-bestand (hetzelfde wachtwoord is vereist in stap 2).

```
openssl pkcs12 -in cert.pfx -nocerts -out key.pem
```

```
docs# openssl pkcs12 -in cert.pfx -nocerts -out ke
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

belangrijk exportproduct

Er bestaan nu vier bestanden: cert.pfx (de oorspronkelijke pfx-bundel), certs.pem (de CA-certificaten), id.pe

```
openssl x509 -in cacert-ab.pem -subject -noout
```

```
docs# openssl x509 -in cacert-ab.pem -subject -noout
subject= /C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=U
```

proefonderwerpregel

Het cacert-bestand dat het onderwerp aanpast met de uitgever van het id.pem-bestand (zoals getoond in de vorige afbeeldingen), is de sub-CA die later wordt gebruikt om de PFX-cert te maken.

Verwijdert het cacert-bestand zonder het bijbehorende onderwerp. In dit geval was dat cert cacert-aa.pem.

```
rm -f cacert-aa.pem
```

Stap 6. De certificaten samenvoegen in een PKCS12-bestand

Voeg het sub CA certificaat (in dit geval was de naam cacert-ab.pem) samen met het ID certificaat (id.pem) en privé sleutel (key.pem) in een nieuw pfx bestand. U moet dit bestand met een wachtwoord beveiligen. Indien nodig wijzigt u de bestandsnaam cacert-ab.pem in overeenstemming met uw bestand.

```
openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
```

```
docs# openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey ke
Enter Export Password:
Verifying - Enter Export Password:
```

PDF-bestanden maken

Stap 7. Het PKCS12-bestand in het VCC importeren

Navigeer in het VCC naar **Apparaat > Certificaten** en voer het certificaat in naar de gewenste firewall zoals aangegeven in de afbeelding.

The screenshot shows the VCC interface with the 'Certificates' tab selected. A dialog box titled 'Add New Certificate' is open. The 'Device*' dropdown is set to 'FTDv-'. The 'Cert Enrollment*' dropdown is set to 'Select a certificate enrollment object'. A red circle highlights the '+' icon in the 'Cert Enrollment*' dropdown, with a red arrow pointing to it from the right. Another red arrow points to the 'Device*' dropdown from the right. The background shows a table with columns 'Name', 'Domain', 'Enrollment Type', and 'Status', and a row for 'FTDv'.

In Windows, kunt u een probleem tegenkomen waar het OS de gehele keten voor het certificaat toont alhoewel het .pfx bestand alleen het ID-certificaat bevat, in het geval dat het de subCA, CA-keten in zijn winkel heeft.

Om de lijst van de certificaten in een .pfx bestand te controleren, kunnen tools zoals certutil of openssl worden gebruikt.

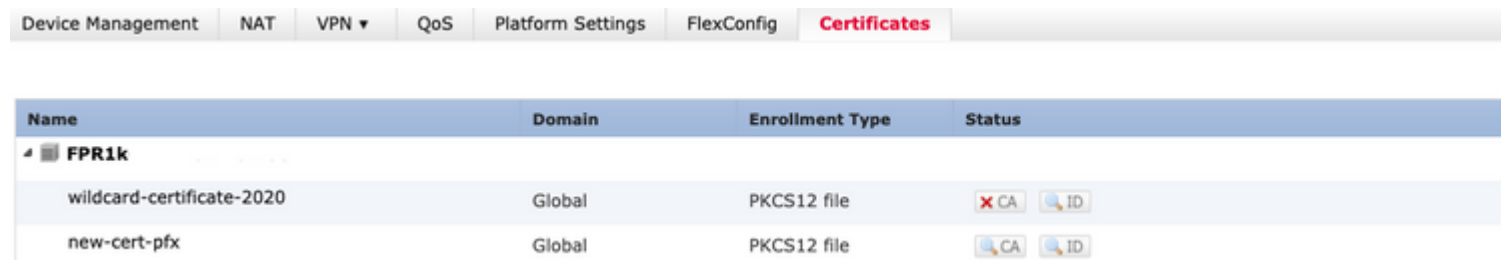
```
certutil -dump cert.pfx
```





De certutil is een opdrachtregel hulpprogramma dat de lijst van certificaten in een .pfx bestand biedt. U moet de hele keten met ID, SubCA, CA (indien aanwezig) zien.

U kunt ook een openssl-opdracht gebruiken, zoals in de opdracht hieronder wordt getoond.

```
openssl pkcs12 -info -in cert.pfx
```

Om de certificaatstatus en de CA- en ID-informatie te controleren, kunt u de pictogrammen selecteren en bevestigen dat de invoer is geslaagd:



Name	Domain	Enrollment Type	Status
FPR1k wildcard-certificate-2020	Global	PKCS12 file	 CA  ID
new-cert-pfx	Global	PKCS12 file	 CA  ID

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.