

Fehlerbehebung bei Zertifikatfehler "Fehler beim Konfigurieren des Zertifizierungsstellenzertifikats" auf FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Problem](#)

[Lösung](#)

[Schritt 1: Suchen Sie das PFX-Zertifikat.](#)

[Schritt 2: Extrahieren der Zertifikate und Schlüssel aus der PFX-Datei](#)

[Schritt 3: Überprüfen der Zertifikate in einem Text-Editor](#)

[Schritt 4: Überprüfen des privaten Schlüssels in einem Editor](#)

[Schritt 5: CA-Zertifikate aufteilen](#)

[Schritt 6: Zusammenführen der Zertifikate in einer PKCS12-Datei](#)

[Schritt 7. PKCS12-Datei in FMC importieren](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie Fehler beim Importieren der Zertifizierungsstelle (Certificate Authority, CA) auf FirePOWER Threat Defense-Geräten, die von FMC verwaltet werden, beheben.

Voraussetzungen

Anforderungen

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

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

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- MacOS x 10.14.6
- FMC 6.4
- OpenSSL

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 Netz Live ist, überprüfen Sie, ob Sie die

mögliche Auswirkung jedes möglichen Befehls verstehen.

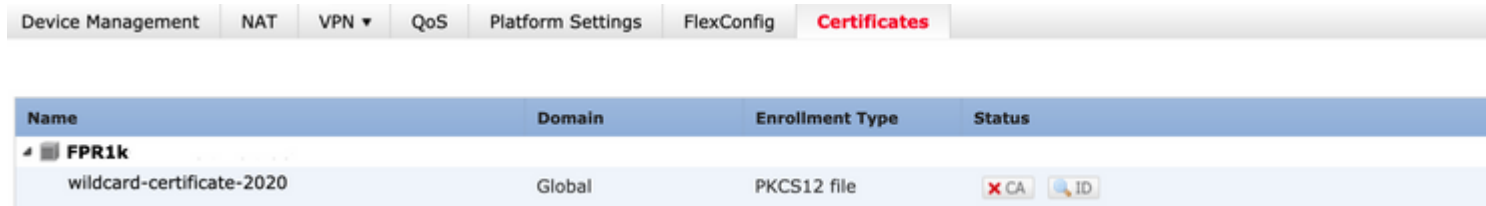
Hintergrundinformationen

Hinweis: Auf FTD-Geräten wird das Zertifizierungsstellenzertifikat benötigt, bevor die CSR (Certificate Signing Request) generiert wird.



- Wenn der CSR auf einem externen Server (wie Windows Server oder OpenSSL) generiert wird, ist die manuelle Registrierungsmethode als fehlerhaft gedacht, da FTD die manuelle Registrierung von Schlüsseln nicht unterstützt. Es muss eine andere Methode wie PKCS12 verwendet werden.

Problem

In diesem speziellen Szenario zeigt das FMC ein rotes Kreuz im Zertifizierungsstellen-Zertifikatstatus an (wie im Bild gezeigt), das besagt, dass die Zertifikatregistrierung das Zertifizierungsstellen-Zertifikat nicht installieren konnte. Dieser Fehler tritt häufig auf, wenn das Zertifikat nicht ordnungsgemäß gepackt wurde oder die PKCS12-Datei nicht das richtige Ausstellerzertifikat enthält, wie im Bild gezeigt.



The screenshot shows the 'Certificates' tab in the FMC interface. The table below lists a certificate with a red 'X' icon in the status column, indicating an error.

Name	Domain	Enrollment Type	Status
FPR1k wildcard-certificate-2020	Global	PKCS12 file	 CA 

Hinweis: Bei neueren FMC-Versionen wurde dieses Problem so behoben, dass es mit dem ASA-Verhalten übereinstimmt, das einen zusätzlichen Vertrauenspunkt mit der Stamm-CA erstellt, die in der Vertrauenskette des PFX-Zertifikats enthalten ist.

Lösung

Schritt 1: Suchen Sie das PFX-Zertifikat.

Rufen Sie das PFX-Zertifikat ab, das in der FMC-GUI registriert war, **speichern Sie** es, und suchen Sie die Datei im Mac Terminal (CLI).

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

LS

Schritt 2: Extrahieren der Zertifikate und Schlüssel aus der PFX-Datei

Extrahieren Sie das Client-Zertifikat (nicht die CA-Zertifikate) aus der PFX-Datei (die Passphrase, die zum Generieren der PFX-Datei verwendet wurde, ist erforderlich).

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

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

Identitätsexport

Extrahieren Sie die Zertifizierungsstellenzertifikate (nicht die Clientzertifikate).

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

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

Ausfuhr von Kakteen

Extrahieren Sie den privaten Schlüssel aus der PFX-Datei (die gleiche Passphrase aus Schritt 2 ist erforderlich).

```
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:
```

Schlüsselexport

Vier Dateien existieren jetzt: cert.pfx (das ursprüngliche pfx-Paket), certs.pem (die CA-Zertifikate), id.pem (

```
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
```

Sachkontrolle

Die Zertifikatsdatei, die den Betreff mit dem Aussteller der Datei id.pem vergleicht (wie in den vorherigen Bildern gezeigt), ist die Sub-Zertifizierungsstelle, die später zum Erstellen des PFX-Zertifikats verwendet wird.

Löschen Sie die Zertifikatsdatei, die nicht über den entsprechenden Betreff verfügt. In diesem Fall war das Zertifikat cacert-aa.pem.

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

Schritt 6: Zusammenführen der Zertifikate in einer PKCS12-Datei

Führen Sie das Sub-CA-Zertifikat (in diesem Fall cacert-ab.pem) zusammen mit dem ID-Zertifikat (id.pem) und dem privaten Schlüssel (key.pem) in einer neuen pfx-Datei. Sie müssen diese Datei mit einer Passphrase schützen. Ändern Sie ggf. den Dateinamen cacert-ab.pem so, dass er Ihrer Datei entspricht.

```
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:
```

Präfix

Schritt 7. PKCS12-Datei in FMC importieren

Navigieren Sie im FMC zu **Device > Certificates** (Gerät > Zertifikate), und importieren Sie das Zertifikat in die gewünschte Firewall, wie im Bild dargestellt.

The screenshot shows the Fortinet FMC interface with the 'Devices' tab selected. The 'Certificates' sub-tab is active. A modal dialog titled 'Add New Certificate' is open. The dialog contains the following fields:

- Device*:** A dropdown menu with 'FTDv-' selected. A red arrow points to this dropdown with the number '2' next to it.
- Cert Enrollment*:** A dropdown menu with 'Select a certificate enrollment object' selected. A red circle highlights the dropdown arrow, and a red arrow points to it.

The dialog also includes a description: 'Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.'

In Windows können Sie auf ein Problem stoßen, bei dem das Betriebssystem die gesamte Kette für das Zertifikat anzeigt, obwohl die PFX-Datei nur das ID-Zertifikat enthält. Falls die Unterzertifizierungsstelle, die Zertifizierungsstellenkette in ihrem Speicher vorhanden ist.

Um die Liste der Zertifikate in einer PFX-Datei zu überprüfen, können Tools wie certutil oder openssl verwendet werden.

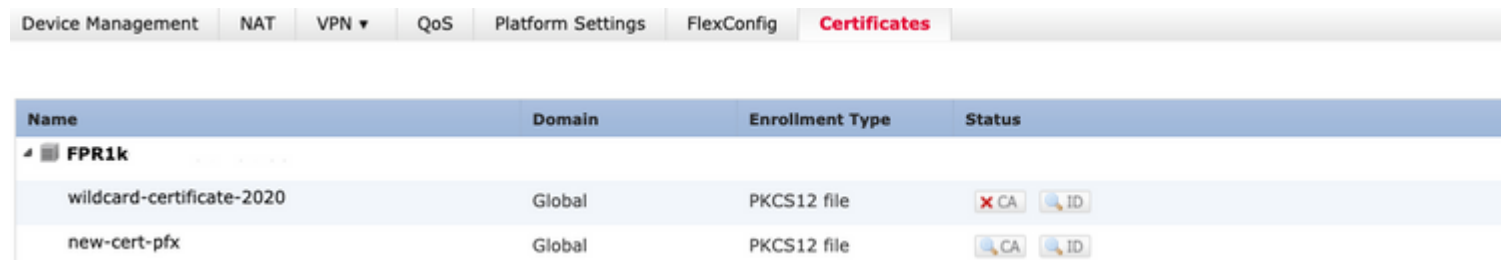
```
certutil -dump cert.pfx
```





certutil ist ein Befehlszeilendienstprogramm, das die Liste der Zertifikate in einer PFX-Datei bereitstellt. Sie müssen die gesamte Kette mit ID, SubCA, CA (falls vorhanden) sehen.

Alternativ können Sie den Befehl openssl verwenden, wie im folgenden Befehl gezeigt.

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

Um den Zertifikatsstatus zusammen mit den CA- und ID-Informationen zu überprüfen, können Sie die Symbole auswählen und bestätigen, dass das Zertifikat erfolgreich importiert wurde:



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

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.