

Risoluzione dei problemi relativi a "Certificate Error "Fail to Configure CA Certificate" on FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Soluzione](#)

[Passaggio 1. Individuare il certificato con estensione pfx](#)

[Passaggio 2. Estrarre i certificati e la chiave dal file con estensione pfx](#)

[Passaggio 3. Verificare i certificati in un editor di testo](#)

[Passaggio 4. Verificare la chiave privata in un Blocco note](#)

[Passaggio 5. Dividere i certificati CA](#)

[Passaggio 6. Unire i certificati in un file PKCS12](#)

[Passaggio 7. Importare il file PKCS12 nel FMC](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come risolvere i problemi relativi all'errore di importazione CA (Certification Authority) nei dispositivi Firepower Threat Defense gestiti da FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Mac OS x 10.14.6
- CCP 6.4
- OpenSSL

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

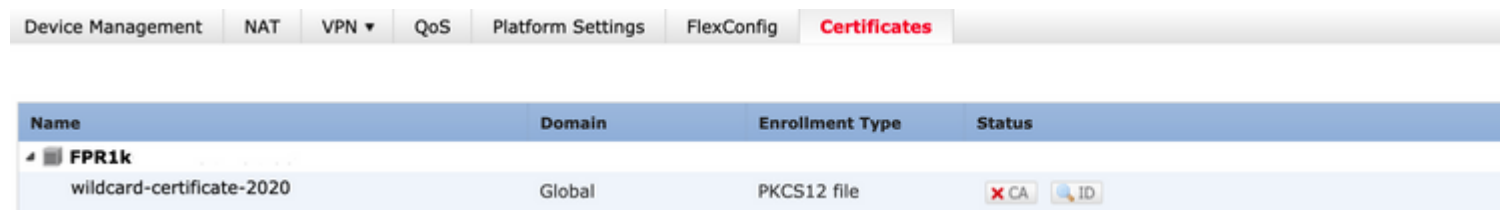
Premesse

Nota: nei dispositivi FTD, il certificato CA è necessario prima della generazione della richiesta di firma del certificato (CSR).



- Se il CSR viene generato in un server esterno (ad esempio Windows Server o OpenSSL), il metodo di registrazione manuale potrebbe non riuscire, in quanto FTD non supporta la registrazione manuale delle chiavi. Utilizzare un metodo diverso, ad esempio PKCS12.

Problema

In questo particolare scenario, il CCP visualizza una croce rossa nello stato del certificato CA (come illustrato nell'immagine), che indica che la registrazione del certificato non è riuscita a installare il certificato CA. Questo errore si verifica in genere quando il certificato non è stato inserito correttamente nel pacchetto o il file PKCS12 non contiene il certificato dell'autorità di certificazione corretto, come mostrato nell'immagine.



The screenshot shows the 'Certificates' tab in the FTD management interface. A table lists certificates with columns for Name, Domain, Enrollment Type, and Status. One certificate, 'wildcard-certificate-2020', is shown 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 

Nota: nelle versioni più recenti di FMC, il problema è stato risolto in modo da corrispondere al comportamento ASA che crea un trust point aggiuntivo con la CA radice inclusa nella catena di trust del certificato con estensione pfx.

Soluzione

Passaggio 1. Individuare il certificato con estensione pfx

Ottenere il certificato pfx registrato nell'interfaccia utente grafica di FMC, **salvarlo** e individuare il file nel terminale Mac (CLI).

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

sl

Passaggio 2. Estrarre i certificati e la chiave dal file con estensione pfx

Estrarre il certificato client (non i certificati CA) dal file pfx (è necessaria la passphrase utilizzata per generare il file con estensione pfx).

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

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

esportazione identità

Estrarre i certificati CA (non i certificati client).

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

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

esportazione cacerts

Estrarre la chiave privata dal file pfx (è necessaria la stessa passphrase del passaggio 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:
```

esportazione chiave

A questo punto esistono quattro file: cert.pfx (il bundle pfx originale), certs.pem (i certificati CA), id.pem (c

```
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
```

controllo soggetto

Il file cacert che corrisponde all'oggetto con l'autorità emittente del file id.pem (come mostrato nelle immagini precedenti), è la CA secondaria utilizzata successivamente per creare il certificato PFX.

Eliminare il file cacert senza oggetto corrispondente. In questo caso, il certificato era cacert-aa.pem.

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

Passaggio 6. Unire i certificati in un file PKCS12

Unire il certificato della CA secondaria (in questo caso, il nome era cacert-ab.pem) con il certificato ID (id.pem) e la chiave privata (key.pem) in un nuovo file PFX. È necessario proteggere il file con una passphrase. Se necessario, modificare il nome del file cacert-ab.pem in modo che corrisponda al file.

```
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:
```

creazione pfx

Passaggio 7. Importare il file PKCS12 nel FMC

Nel FMC, selezionare **Periferica > Certificati** e importare il certificato nel firewall desiderato, come mostrato nell'immagine.

The screenshot shows the Fortinet FMC interface with the 'Add New Certificate' dialog box open. The dialog is titled 'Add New Certificate' and contains the following fields:

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

At the bottom of the dialog, there are 'Add' and 'Cancel' buttons.

In Windows, è possibile riscontrare un problema in cui il sistema operativo visualizza l'intera catena per il certificato anche se il file .pfx contiene solo il certificato ID, nel caso in cui abbia la catena SubCA, CA nel suo archivio.

Per controllare l'elenco dei certificati in un file PFX, è possibile utilizzare strumenti quali certutil o openssl.

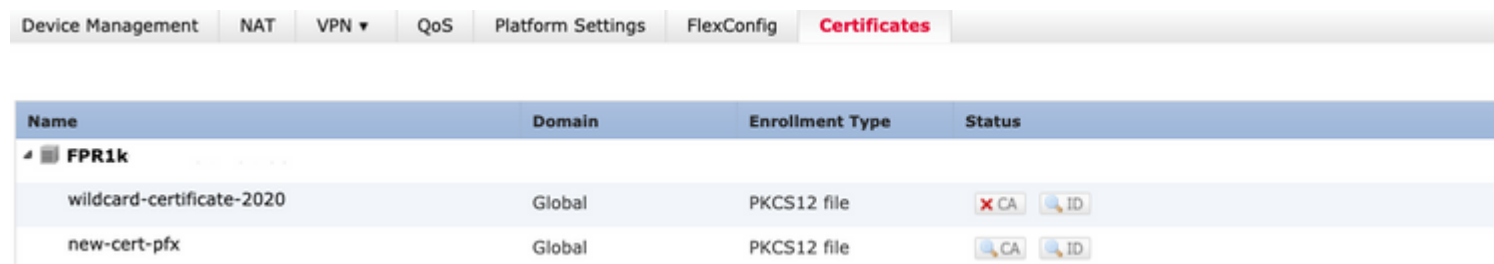
```
certutil -dump cert.pfx
```

Il certutil è un'utilità della riga di comando che fornisce l'elenco dei certificati in un file con estensione pfx. È necessario visualizzare l'intera catena con ID, SubCA, CA incluso (se presente).





In alternativa, è possibile utilizzare un comando openssl, come mostrato nel comando seguente.

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

Per verificare lo stato del certificato insieme alle informazioni sull'ID e sulla CA, è possibile selezionare le icone e confermare l'importazione:



The screenshot shows a web interface for managing certificates. At the top, there is a navigation bar with tabs: Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig, and Certificates (which is highlighted in red). Below the navigation bar is a table with the following columns: Name, Domain, Enrollment Type, and Status. The table contains two rows of certificate information.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).