

Troubleshooting de Erro de Certificado "Falha ao Configurar Certificado de CA" no FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Etapa 1. Localize o certificado .pfx](#)

[Etapa 2. Extraia os certificados e a chave do arquivo .pfx](#)

[Etapa 3. Verificar os certificados em um editor de texto](#)

[Etapa 4. Verifique a chave privada em um Bloco de notas](#)

[Etapa 5. Dividir os certificados CA](#)

[Etapa 6. Mesclar os certificados em um arquivo PKCS12](#)

[Passo 7. Importe o arquivo PKCS12 no FMC](#)

[Verificar](#)

Introdução

Este documento descreve como solucionar problemas e corrigir o erro de importação da autoridade de certificação (CA) em dispositivos Firepower Threat Defense gerenciados pelo FMC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- MacOS x 10.14.6
- CVP 6.4
- OpenSSL

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

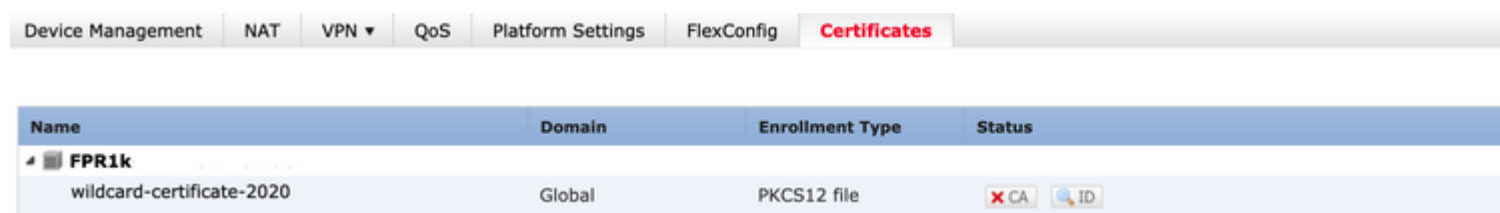
Informações de Apoio

Observação: em dispositivos FTD, o certificado CA é necessário antes que a CSR (Certificate Signing Request, Solicitação de assinatura de certificado) seja gerada.



- Se o CSR for gerado em um servidor externo (como o Windows Server ou o OpenSSL), o método de registro manual falhará, pois o FTD não oferece suporte ao registro manual de chave. Um método diferente deve ser usado, como PKCS12.

Problema

Neste cenário específico, o FMC exibe uma cruz vermelha no status do certificado da CA (como mostrado na imagem), que indica que a inscrição do certificado falhou ao instalar o certificado da CA. Esse erro é normalmente visto quando o certificado não foi empacotado corretamente ou o arquivo PKCS12 não contém o certificado do emissor correto, como mostrado na imagem.



The screenshot shows the 'Certificates' tab in the FMC GUI. 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 

Observação: nas versões mais recentes do FMC, esse problema foi resolvido para corresponder ao comportamento do ASA que cria um ponto de confiança adicional com a CA raiz incluída na cadeia de confiança do certificado .pfx.

Solução

Etapa 1. Localize o certificado .pfx

Obtenha o certificado pfx que foi registrado na GUI do FMC, **salve-o** e localize o arquivo no Mac Terminal (CLI).

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

ls

Etapa 2. Extraia os certificados e a chave do arquivo .pfx

Extraia o certificado do cliente (não certificados CA) do arquivo pfx (a senha usada para gerar o arquivo .pfx é necessária).

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

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

exportação de identidade

Extraia os certificados CA (não os certificados do cliente).

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

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

exportação de cacerts

Extraia a chave privada do arquivo pfx (a mesma senha da Etapa 2 é necessária).

```
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:
```

exportação de chave

Agora existem quatro arquivos: cert.pfx (o pacote pfx original), certs.pem (os certificados CA), id.pem (certi

```
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
```

verificação de assunto

O arquivo cacert que corresponde ao Assunto com o Emissor do arquivo id.pem (como mostrado nas imagens anteriores) é a Sub CA que é usada mais tarde para criar o certificado PFX.

Excluir o arquivo cacert que não tem o Assunto correspondente. Nesse caso, esse certificado era cacert-aa.pem.

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

Etapa 6. Mesclar os certificados em um arquivo PKCS12

Mescle o certificado da sub CA (nesse caso, o nome era cacert-ab.pem) com o certificado de ID (id.pem) e a chave privada (key.pem) em um novo arquivo pfx. Você deve proteger este arquivo com uma senha. Se necessário, altere o nome do arquivo cacert-ab.pem para corresponder ao seu arquivo.

```
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:
```

pfx-creation

Passo 7. Importe o arquivo PKCS12 no FMC

No FMC, navegue até **Device > Certificates** e importe o certificado para o firewall desejado conforme mostrado na imagem.

The screenshot shows the Fortinet FMC interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Below this, there are sub-tabs for 'Device Management', 'Device Upgrade', 'NAT', 'QoS', 'Platform Settings', 'FlexConfig', 'Certificates', 'VPN', and 'Troubleshoot'. The main content area shows a table with columns 'Name', 'Domain', 'Enrollment Type', and 'Status'. A single entry 'FTDv' is visible. A modal dialog titled 'Add New Certificate' is open, with the following fields: 'Device*' (set to 'FTDv-'), 'Cert Enrollment*' (set to 'Select a certificate enrollment object'), and a green plus icon in a circle next to the 'Cert Enrollment*' dropdown. Red arrows point to these elements, with a '2' next to the first arrow.

No Windows, você pode encontrar um problema em que o SO exibe a cadeia inteira para o certificado, mesmo que o arquivo .pfx contenha apenas o certificado de ID, caso ele tenha a cadeia subCA, CA em seu armazenamento.

Para verificar a lista de certificados em um arquivo .pfx, ferramentas como certutil ou openssl podem ser usadas.

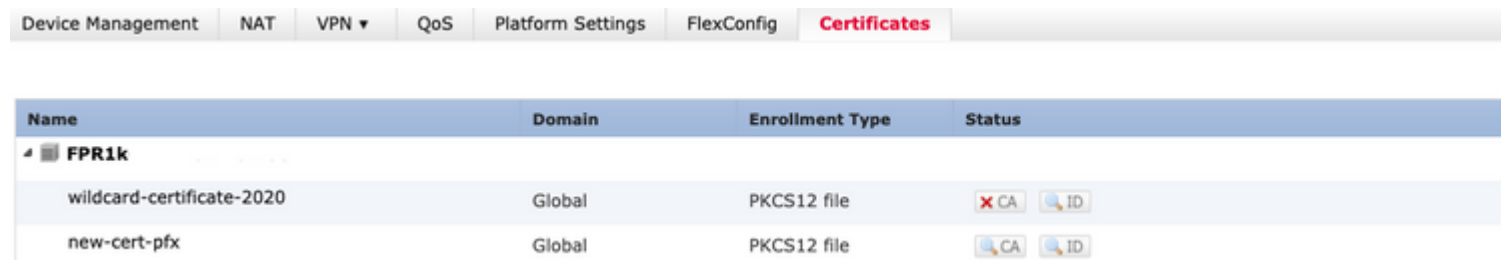
```
certutil -dump cert.pfx
```





O certutil é um utilitário de linha de comando que fornece a lista de certificados em um arquivo .pfx. Você deve ver toda a cadeia com ID, SubCA, CA incluídos (se houver).

Como alternativa, você pode usar um comando openssl, como mostrado no comando abaixo.

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

Para verificar o status do certificado junto com as informações de CA e ID, você pode selecionar os ícones e confirmar se ele foi importado com êxito:



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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.