FMC에서 CA 인증서 구성 실패 " 인증서 오류 트러블슈팅

목차

소개

이 문서에서는 FMC에서 관리하는 Firepower Threat Defense 장치에서 CA(Certificate Authority) 가져오기 오류를 해결하고 수정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- MacOS x 10.14.6

- FMC 6.4
- OpenSSL

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

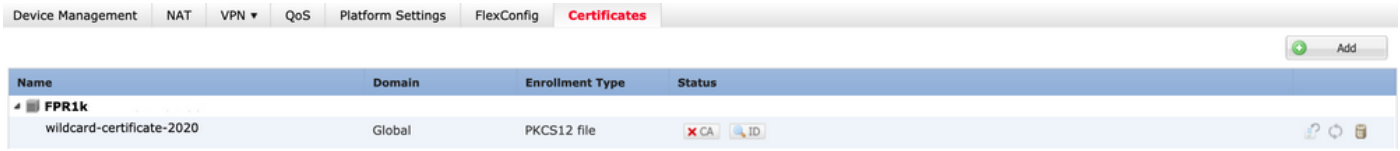
배경 정보

참고: FTD 디바이스에서는 CSR(Certificate Signing Request)이 생성되기 전에 CA 인증서가 필요합니다.

- CSR이 외부 서버(예: Windows Server 또는 OpenSSL)에서 생성되는 경우, FTD는 수동 키 등록을 지원하지 않으므로 수동 등록 방법은 실패할 수 있습니다. 다른 메서드(예: PKCS12)를 사용해야 합니다.

문제

이 특정 시나리오에서 FMC는 CA 인증서 상태(그림과 같이)에 빨간색 십자선을 표시하며, 이는 인증서 등록이 CA 인증서를 설치하지 못했다는 것을 나타냅니다. 이 오류는 일반적으로 이미지에 표시된 것처럼 인증서가 제대로 패키지되지 않았거나 PKCS12 파일에 올바른 발급자 인증서가 없을 때 나타납니다.



참고: 최신 FMC 버전에서는 .pfx cert의 신뢰 체인에 포함된 루트 CA를 사용하여 추가 신뢰 지점을 생성하는 ASA 동작과 일치하도록 이 문제가 해결되었습니다.

솔루션

1단계. .pfx 인증서 찾기

FMC GUI에 등록된 pfx 인증서를 가져와 저장하고 Mac Terminal(CLI)에서 파일을 찾습니다.

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

ls

2단계. .pfx 파일에서 인증서 및 키 추출

pfx 파일에서 클라이언트 인증서(CA 인증서가 아님)를 추출합니다. .pfx 파일을 생성하는 데 사용한

패스프레이즈가 필요합니다.

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

```
docs# openssl pkcs12 -in cert.pfx -clcerts -nokeys -out id.pem
Enter Import Password:
MAC verified OK
```

id 내보내기

CA 인증서를 추출합니다(클라이언트 인증서가 아님).

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

```
docs# openssl pkcs12 -in cert.pfx -cacerts -nokeys -out certs.pem
Enter Import Password:
MAC verified OK
```

cacerts 내보내기

pfx 파일에서 개인 키를 추출합니다(2단계와 동일한 패스프레이즈가 필요함).

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

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

키 내보내기

이제 cert.pfx(원본 pfx 번들), certs.pem(CA 인증서), id.pem(클라이언트 인증서) 및 key.pem(개인 키)의 네 가지 파일이 있습니다.

```
docs# ls -l
total 40
-rw-r--r--  1 holguins  staff  4701 May 23 15:11 cert.pfx
-rw-r--r--  1 holguins  staff  2301 Jun 10 01:34 certs.pem
-rw-r--r--  1 holguins  staff  2410 Jun 10 01:34 id.pem
-rw-r--r--  1 holguins  staff  1958 Jun 10 01:34 key.pem
docs#
```

내보내기 후 ls

3단계. 텍스트 편집기에서 인증서 확인

텍스트 편집기(예: nano certs.pem)를 사용하여 인증서를 확인합니다.

이 특정 시나리오에서는 certs.pem에 하위 CA(발급 CA)만 포함되었습니다.

5단계부터 이 문서에서는 certs.pem 파일에 2개의 인증서(하나의 루트 CA와 하나의 하위 CA)가 포함된 시나리오를 다룹니다.

```
Bag Attributes: <No Attributes>
subject=/C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Intermediate CA
issuer=/C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Root CA
-----BEGIN CERTIFICATE-----
MIIF0zCCA7ugAwIBAgICEAUwDQYJKoZIhvcNAQELBQAwdjELMAkGA1UEBhMCTVgx
DTALBgNVBAgMBENETVgxEjAQBgNVBAoMCVVuZ3UgQ29ycDEoMCYGA1UECwwfVW5n
dSBDb3JwIENlcnRpZmljYXRlIEF1dGhvcml0eTEaMBgGA1UEAwwRVW5ndSBDb3Jw
IFJvb3QgQ0EwHhcNMjIwMjAyMDc1MDQ4WhcNMzIwMTMxMDc1MDQ4WjB+MQswCQYD
VQQGEwJNWDENMAsGA1UECAwEQ0RNWDESMBAGA1UECgwJVW5ndSBDb3JwMSgwJgYD
VQQLDB9Vbmd1IENvcnAgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSIwIAYDVQQDDBlV
bmd1IENvcnAgSW50ZXJtZWRpYXRlIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICCgKCAgEAt9zB5lbrhMTEEyGmRVRnuQ+mt86axF3QZEeSYCfV5gZs9R25cw+N
L7U9agbL/bNfvR0ON8I8ywVahiTWJP9kuzGksEDaUzyHXybDslYpHUNt0fYn5zFi
GGa8lr9OKmxSpsXeQB+GB0D8wezA1bAAGSKDiQymtBdQQMpnKTCmCRCjcPD1rBq1
EwiO/7ePWhHK4KhtBBfSmjqxZYb1QIG5DBWCKA4q2DlME9/o+pL944Utw+HMLrAH
4bT86kT7cYQVbeVSmoCastuN+1jux2aJ+4jT0GJM44yn0KzVANolgEjw/DPhW460
u9I1oJGMCh4j7EfL8bYvHTd+8yEejmHR+ASycsy+8qoymWq3wIPiWJA0r160Hn2c
JOZpu2oQQs+9O+wBrzn/yV7aZmVDdbEJSXKHJkIGA7k5VWe/CvXbfExHSCfdZ5EV
uIx4AixdgwEddOrgpHvYOGS1IHBmXNKoPp6s41oLMsmSr8lgZqm5mgdDlUKNA8tG
OjVrURiHLalHhyynoYHHVihEjhPRjNL9T26Dq9iAhX6yMClIXB1QG/QUxef7ALO7
nzIBA5rYnAEv+TvgYkRE4Z9gVKxYhNLpxnVgOycHiZbco2IcQzqIWdQAqQS2LRWP
8eNuPd9l+5BgsSYgK3NxQPzMXZwmMXgnGye3lueBUL9DSkuknxOaFVMCAwEAAaNj
MGEwHQYDVR0OBBYEFE/DAVTSyUoHThBtxlvip1L0TEQoMB8GA1UdIwQYMBaAFJMO
DF6TWo6EkboLkLC0t59zO1QwMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQD
AgGGMA0GCSqGSIb3DQEBCwUAA4ICAQBUNUuk9jMTGmcP6j/tqBFM3Inhj/84ABMY
T4RBdtxi1v5HPjtknyEIp1B31QxrWi4pLiyh0ILb181mNxnawZDOMvzv7BsxepvX
xHrGhGac2y4yT72vGcIp/++8H2LatFaGAGePIssCjzTcLG9bruPB/MXYJ3MrlGXl
FbqvTdDJS5qBO+jRnMbACbV/nTUVXl6f6vb3AW2ZyO/u0+S6VoiB5Uk4xLZuhrwl
IXxSTghQWLqK4FBLj+XxyK2u+10iR3+6JGkkaIbb62zJsklnSJ+gVHgsMhEjATto
HOZw5+uoJQyl/pa4ukOUaRPksIcH82p+4gPeCg5cEQAcI4niqJgIH0oPYJQszRwD
IB2w3nTAaNMTDyH6Ih/N/MvPiBhaYI3jynGEmJmansw8zcBPoeak4bTsEx3hu7a/
kWddLmv2TscsfkGCL0XLOfcJLcW4R6QvsZaj3Ia0AsX/Lm0eYb7RnXfjPHenp3rA
a9IOLNe9/AyQrAqp3hQ4XSNs3zgScCja40ZcXiSgJcf1XIs8Ml2phT4bob89vY+u
xIawv6bXItQE7P2RBUeJWPMFcJ75JMplRYsj2xogkneMiPpc9w5moZLxZpvznqgy
aCi37m1d+CT6hYTWxe3HztS03VJ+24IqEr+wmi+FB04VHZtqc/BpajbOTpGBUGex
wxMFkoFWSA==
-----END CERTIFICATE-----
```

certs 보기

4단계. 메모장에서 개인 키 확인

텍스트 편집기(예: nano certs.pem)를 사용하여 key.pem 파일의 내용을 확인합니다.

```
Bag Attributes
    localKeyID: 4B ED BA 56 76 3A C9 22 C3 75 54 A7 0A 1A F1 7D 3B 5E B0 D8
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI9vQUkrEl0MMCAggA
MBQGCCqGSIb3DQMHBAjnRV9YTIYsSwSCBMjqflLhs3v0RL0DHkvi7yvWSd3xWLMn
jt1hgOLsU1TDmBAWp/LXpqSP27c4XCQiZcOeiFDqm8aKw9xTDjgkEUBVactZs+Sz
yCE1gcG6NRH9lZFiwOYy+MCR4EPYh06DJPQ+MxLvtjjHrErruyXlAlywfAtrAcQk
E5tJniCaNTppwfVOfLpd/oHa2tFOkBMVVjS3HyxAXEfNThmzMwKRygsLPUKShtfb
iv0bu8zI6fVfB4db3J/FjqikoiCHKXbWetm/GewZO71H3DW0HamtPw3InUuvYuzv
SM08x+NJi6uo7gtrQ6Rld2z5fN6vTtAw3xlOAHjxm+vfOxt95zXhABYkMg2zHaQg
0djTHYFWdHwpdmSSNWM8hWnY8AvFxdjXURp/5MNP+v6ty5W/ETVe6o+Dh1sa9i7v
PzUwIDWs6kt0rxp0v82O0lmqSKD6C4UnDlVf2hH7AyMuwRpYamOEIuPtg8GgeiHJ
6vxpIJ3dY9/s0eyElkvKimZgiXpexBV/nDnksCLJTGyR08AE56iq2+XiBkwIoUai
QTZNi3S+PmPf8glHFtVKR8V6Zk4u8xov3reNTTmKXxXcH3mHPaMU/Nhdldn8fpx+
phTzULmdtIpD3rlHknh0uMvjrw0RYTLp1WGiEo5DU1SyI5jrMCYa0mhufOI7vtPp
rQqXNo6JleXuBteWSIHDqFynrtIdLyUVhK5QwF4Om9+OvGkXNuqMDv4fH4+7nv9l
KqK2NS4yUXW1KjbAFe+Cxz9E7stt4Nyvwx56l/FpYLHymYDjQA3kFrC3tPHeULjT
fp95fJ+6g2ROnr4yKerHbV5BAaiOV3rRVpBWhgzBK5o3w4+C+QIH6tgD1f2Jp9YA
TZLj/BDxIc4OQ6AORATjWcbE1fvuNmNvMEQpDFMOgP8mlqnnBGzc5mwxC1xTNcQD
nmaFYykWVxYCzsvQAgwkvyzzZw2mPNQpj3lVIOVRdZy8NWVkKCBLpq2XTSA6AQIK
mnJLY+rSAEi6miVnHeUW683un8KND9+HQlYZbpKDK+JGcwkP/KhEHKmipEoHS8b5
MLby4tL7qrA3sfddMooJJYsCC372WYrd8xPrDZ9kYJ0N64ks9sYhvRUxRMJaxqaY
Int7b6p9Oi1r0LpielhUUrEvbuOCudM4sLDyXq8Fqf9G5u8dMuchCjXrEPGhmf4Y
ZhTfQF3xxQYtLBbLfWeQUFt6GBsJMLGZFTFPM06/e3vToRu/Opw4Z9hrA6zBfQWa
bcT868DNME+UQxoT825SLwsFFPcjOpixn21FSm6baiq6QWvTV9+5797+AEPnG23i
1x/KKsvTEuwyHGgAX6p9Z0bfPOVcikMZkO9MvMDU5MOUm0lbnb0zINrrblG0qmRX
SYNNoL7lJ3joAKzv056KURWAMk9tQE8hAefWAZHSlPacwgUIWxOSAszRMkneptiR
VCm5UvzbYiMIAOrJjx6PTakuPIhdfokLyWfMI74ETao0Hl7KdDD1i/w11fAWFqtN
2gzfPw7QO2F7iZiYtxV9ryVBnH4wqut9pFjPYGu2oXC5q4Y7lJ1DrMzc879vAchM
C1dBcaJLWdpdTmrg2WNiao/rv3A20JjPOzAOeUwRo9r5OS0oF9ez1ghBpAAtehyi
FGY=
-----END ENCRYPTED PRIVATE KEY-----
```

5단계. CA 인증서 분할

certs.pem 파일에 2개의 인증서(1개의 루트 CA와 1개의 하위 CA)가 있는 경우, FMC에서 pfx 형식의 인증서를 가져오려면 신뢰 체인에서 루트 CA를 제거해야 하며, 검증을 위해 체인에 하위 CA만 남겨둡니다.

certs.pem을 여러 파일로 분할한 다음 명령은 certs의 이름을 cacert-XX로 바꿉니다.

```
split -p "-----BEGIN CERTIFICATE-----" certs.pem cacert-
```

```
docs# split -p "-----BEGIN CERTIFICATE-----" certs.pem cacert-
docs#
```

분할

```
docs# ls -l
total 56
-rw-r--r--  1 holguins  staff   219 Jun 10 01:46 cacert-aa
-rw-r--r--  1 holguins  staff  2082 Jun 10 01:46 cacert-ab
-rw-r--r--  1 holguins  staff  4701 May 23 15:11 cert.pfx
-rw-r--r--  1 holguins  staff  2301 Jun 10 01:34 certs.pem
-rw-r--r--  1 holguins  staff  2410 Jun 10 01:34 id.pem
-rw-r--r--  1 holguins  staff  1958 Jun 10 01:34 key.pem
docs#
```

분할 후 ls

아래에 설명된 명령을 사용하여 이러한 새 파일에 .pem 확장명을 추가합니다.

```
for i in cacert-*;do mv "$i" "$i.pem";done
```

```
docs# for i in cacert-*;do mv "$i" "$i.pem";done
docs#
```

스크립트 이름 바꾸기

두 개의 새 파일을 검토하고 어떤 파일에 루트 CA가 포함되어 있는지, 어떤 파일에 하위 CA가 포함되어 있는지 설명한 명령을 통해 확인합니다.

먼저 id.pem 파일(ID 인증서)의 발급자를 찾습니다.

```
openssl x509 -in id.pem -issuer -noout
```

```
docs# openssl x509 -in id.pem -issuer -noout
issuer= /C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Intermediate CA
```

발급자 보기

이제 두 개의 accert 파일(CA 인증서)의 제목을 찾습니다.

```
openssl x509 -in cacert-aa.pem -subject -noout
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=Ungu Corp Intermediate CA
```

주체 수표

Subject와 id.pem 파일의 Issuer를 매칭하는 cacert 파일은(이전 그림에 나와 있듯이) 나중에 PFX 인증서를 만드는 데 사용되는 Sub CA입니다.

일치하는 제목이 없는 cacert 파일을 삭제합니다. 이 경우 해당 인증서는 cacert-aa.pem입니다.

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

6단계. PKCS12 파일에서 인증서 병합

새 pfx 파일에서 ID 인증서(id.pem) 및 개인 키(key.pem)와 함께 하위 CA 인증서(이 경우 이름은 cacert-ab.pem임)를 병합합니다. 암호를 사용하여 이 파일을 보호해야 합니다. 필요한 경우 cacert-ab.pem 파일 이름을 파일과 일치하도록 변경합니다.

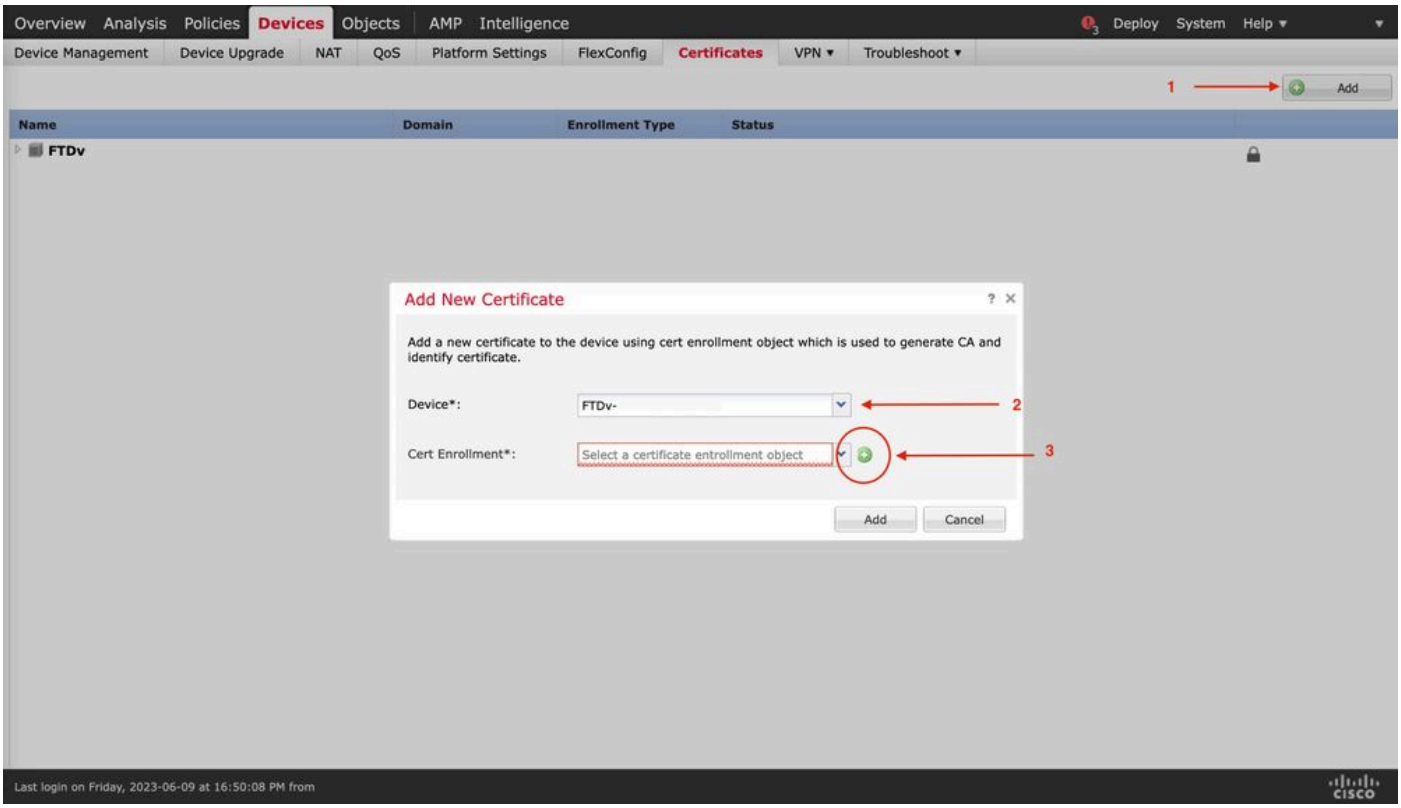
```
openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
```

```
docs# openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
Enter Export Password:
Verifying - Enter Export Password:
```

pfx 생성

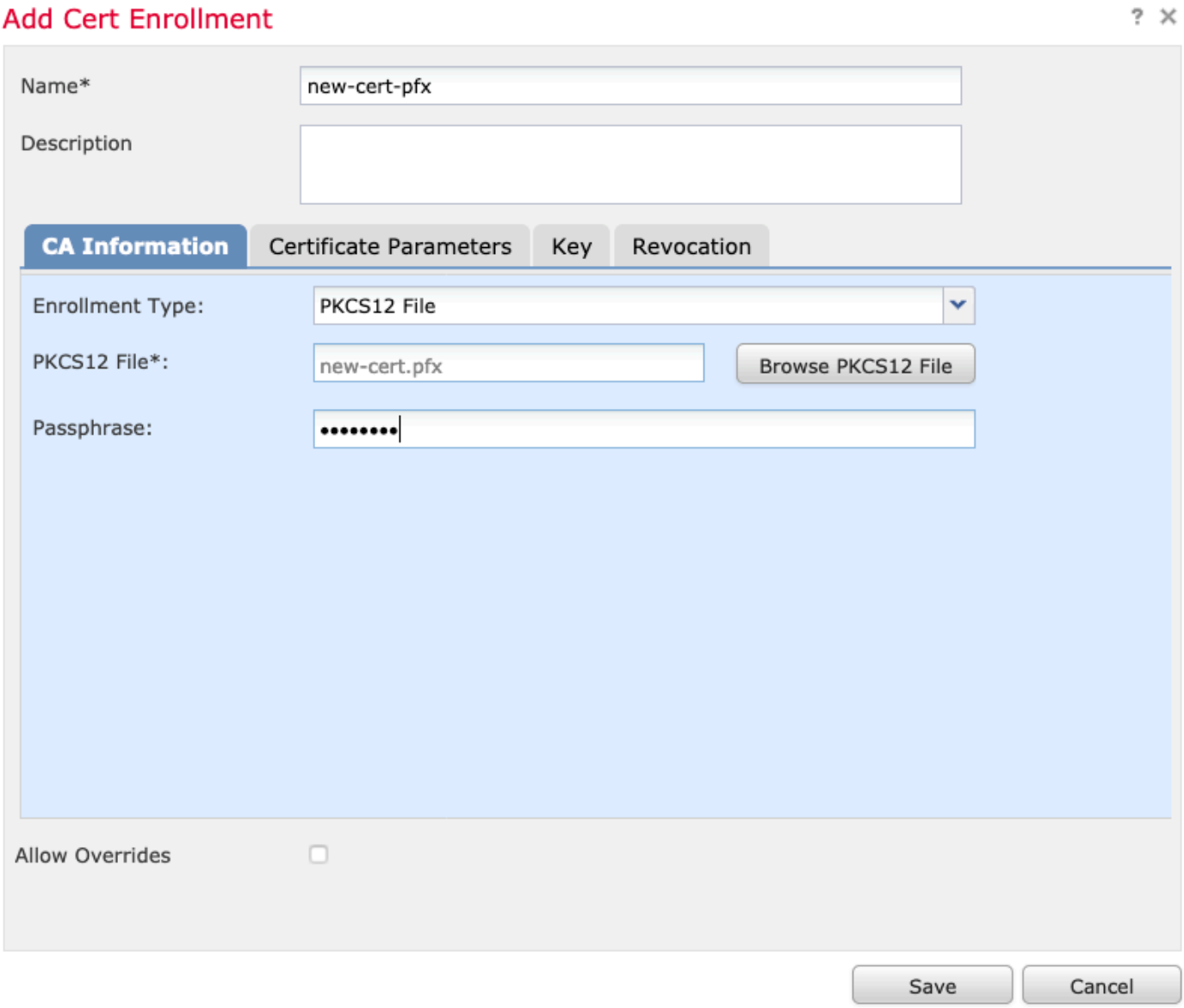
7단계. FMC에서 PKCS12 파일 가져오기

FMC에서 Device(디바이스) > Certificates(인증서)로 이동하고 이미지에 표시된 대로 인증서를 원하는 방화벽으로 가져옵니다.



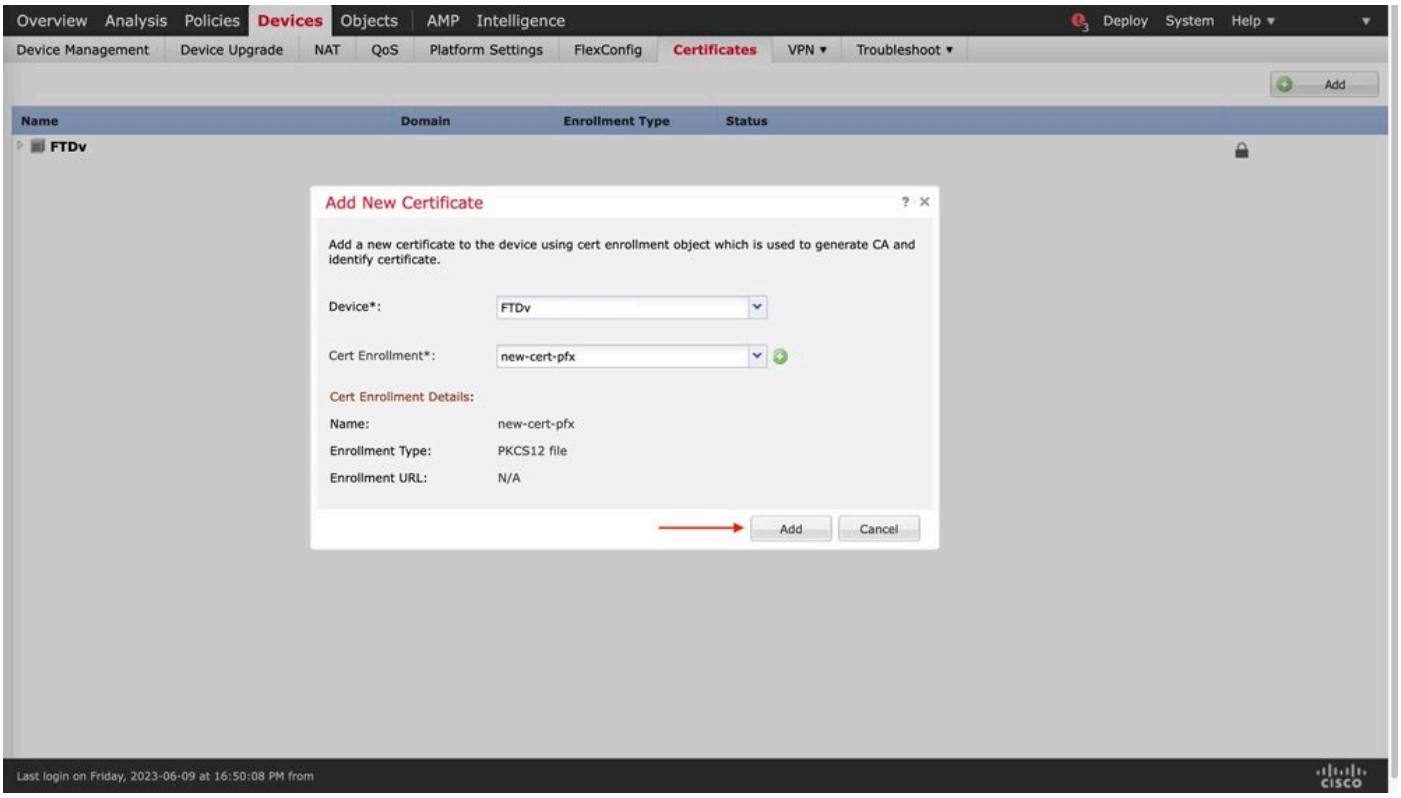
인증서 등록

새 인증서의 이름을 삽입합니다.



등록

새 인증서를 추가하고 등록 프로세스가 FTD에 새 인증서를 구축할 때까지 기다립니다.



새 인증서

새 인증서는 CA 필드에 빨간색 십자가 없이 표시되어야 합니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

Windows에서는 .pfx 파일에 ID 인증서만 포함되어 있지만 저장소에 하위 CA, CA 체인이 있는 경우 OS에서 인증서의 전체 체인을 표시하는 문제가 발생할 수 있습니다.

.pfx 파일에서 인증서 목록을 확인하려면 certutil 또는 openssl과 같은 도구를 사용할 수 있습니다.

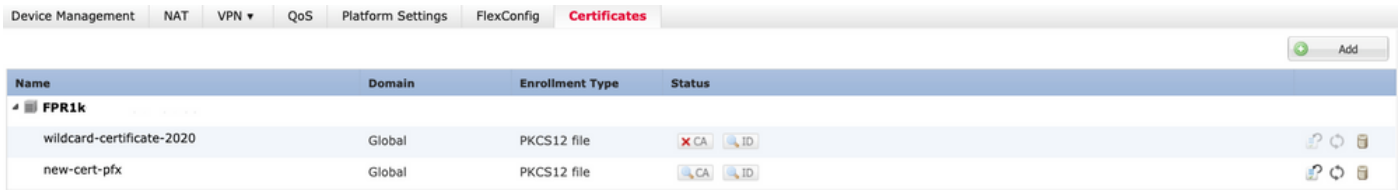
```
certutil -dump cert.pfx
```

certutil은 .pfx 파일의 인증서 목록을 제공하는 명령줄 유틸리티입니다. ID, SubCA, CA가 포함된 전체 체인(있는 경우)을 확인해야 합니다.

또는 아래 명령과 같이 openssl 명령을 사용할 수 있습니다.

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

CA 및 ID 정보와 함께 인증서 상태를 확인하려면 아이콘을 선택하여 성공적으로 가져왔는지 확인할 수 있습니다.



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.