Risolvere i problemi relativi agli errori dei certificati in FMC

Sommario

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.

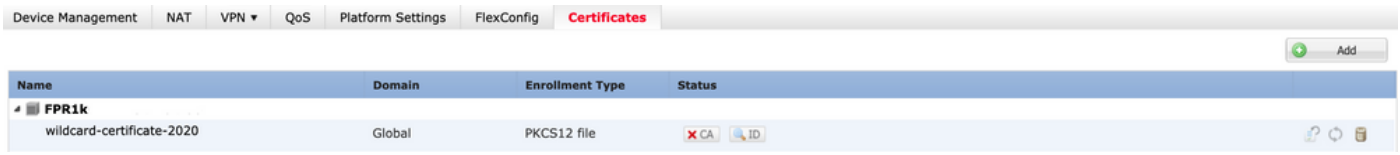
Premesse

Nota: nei dispositivi gestiti con 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 FMC visualizza una croce rossa nello stato del certificato CA (come mostrato nell'immagine), che indica che la registrazione del certificato non è riuscita a installare il certificato CA con il messaggio "Impossibile configurare 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.



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 cert.pfx
```

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 -nokeys -out id.pem
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 -nokeys -out certs.pem
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 key.pem
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 (certificato client) e key.pem (la chiave privata).

```
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#
```

ls dopo l'esportazione

Passaggio 3. Verificare i certificati in un editor di testo

Verificare i certificati utilizzando un editor di testo, ad esempio nano certs.pem.

Per questo particolare scenario, certs.pem conteneva solo la CA secondaria (CA emittente).

A partire dal passaggio 5, in questo articolo viene illustrata la procedura per lo scenario in cui il file certs.pem contiene 2 certificati (una CA radice e una CA secondaria).

```
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-----
```

visualizzazione certificati

Passaggio 4. Verificare la chiave privata in un Blocco note

Verificare il contenuto del file key.pem utilizzando un editor di testo (ad esempio: nano certs.pem).

```
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-----
```

Passaggio 5. Dividere i certificati CA

Nel caso in cui il file certs.pem disponga di 2 certificati (1 CA radice e 1 CA secondaria), la CA radice deve essere rimossa dalla catena di certificati per poter importare il certificato in formato pfx nel FMC, lasciando solo la CA secondaria nella catena ai fini della convalida.

Dividendo il file certs.pem in più file, il comando successivo rinomina i certificati come cacert-XX.

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

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

```
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#
```

splitter dopo la divisione

Aggiungere l'estensione .pem a questi nuovi file con il comando descritto di seguito.

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

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

rinomina script

Esaminare i due nuovi file e determinare quale contiene la CA radice e quale contiene la CA secondaria con i comandi descritti.

Individuare innanzitutto l'autorità emittente del file id.pem, ovvero il certificato di identità.

```
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
```

visualizzazione emittente

Trovare ora l'oggetto dei due file cacert- (certificati CA).

```
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
```

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.

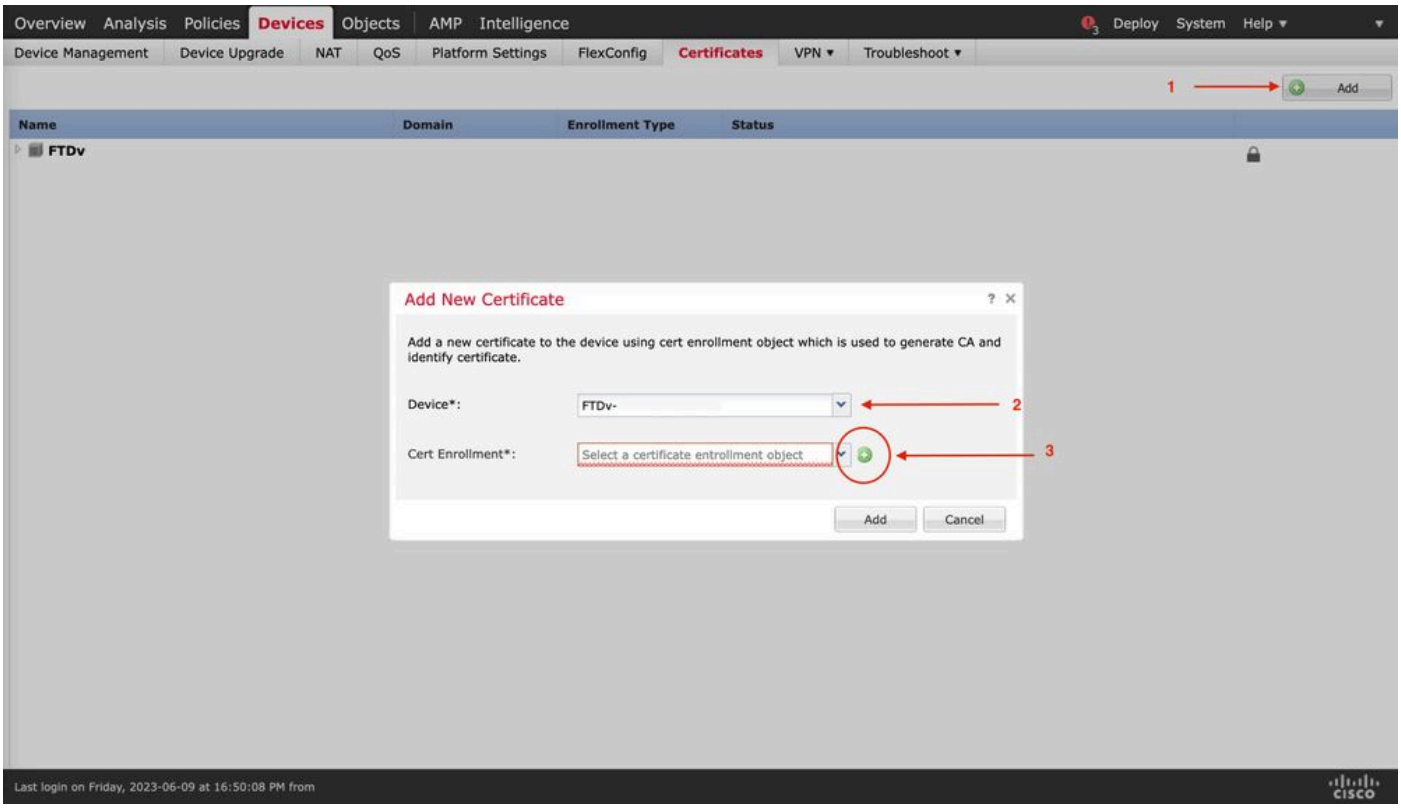
```
openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
```

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

creazione pfx

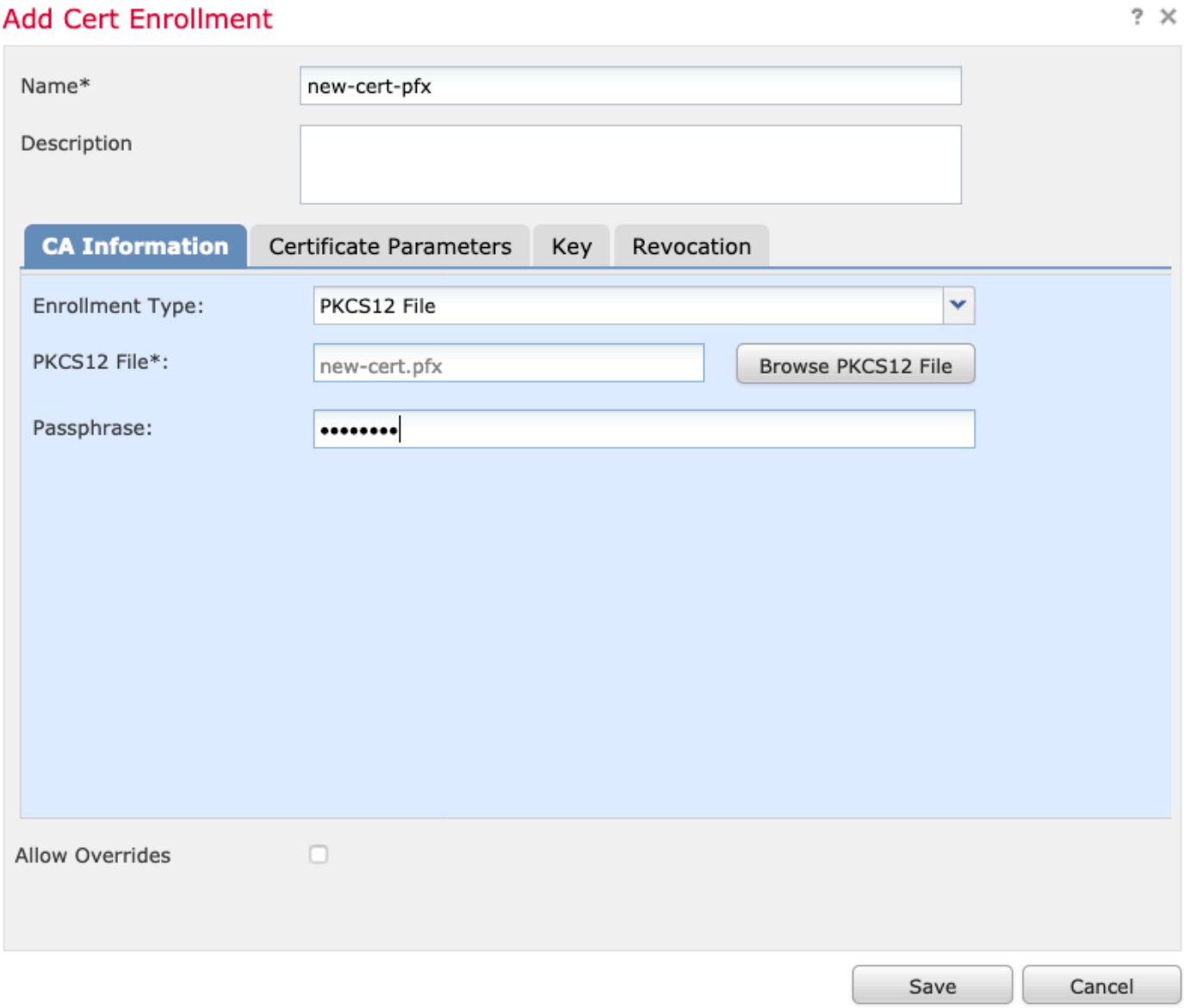
Passaggio 7. Importare il file PKCS12 nel FMC

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



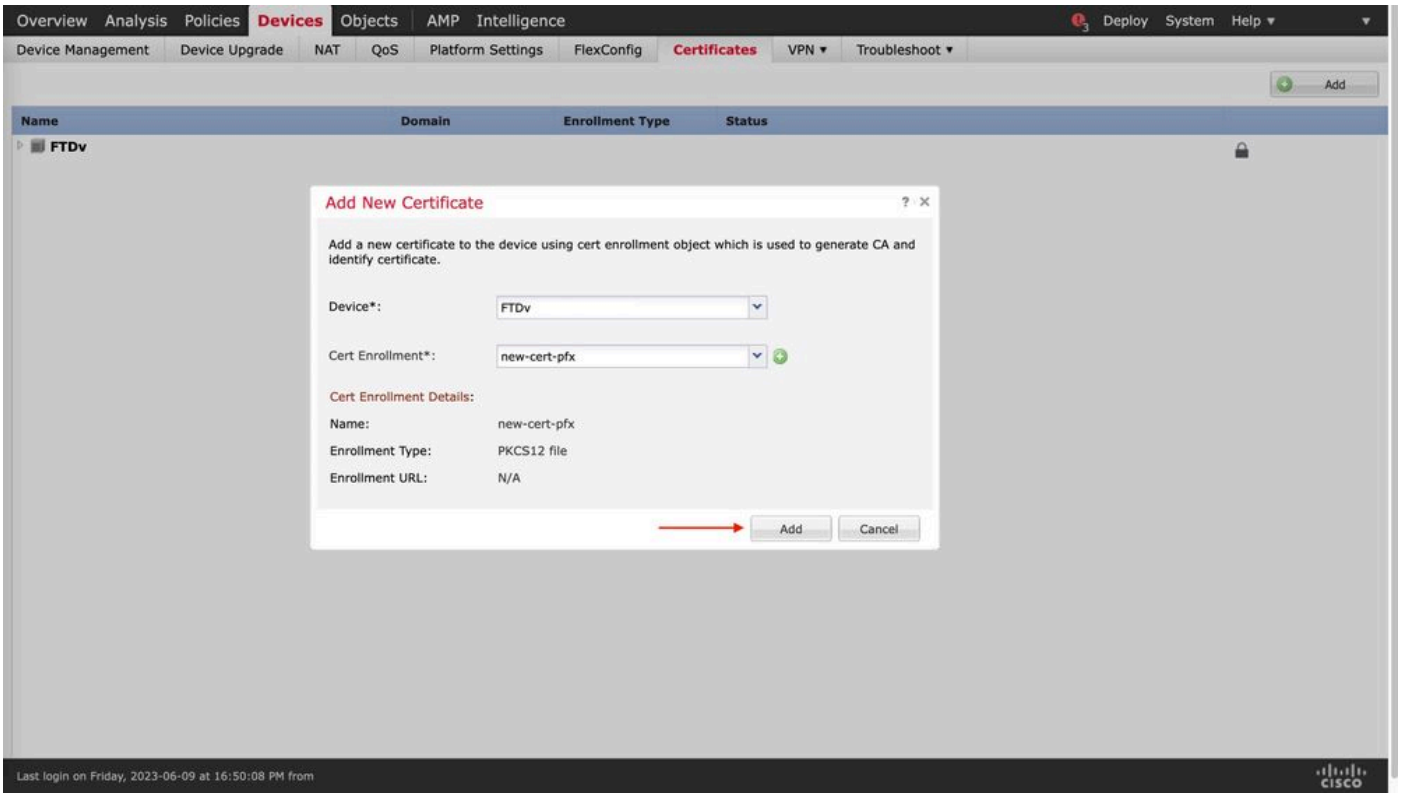
registrazione certificato

Inserire un nome per il nuovo certificato.



Iscrizione

Aggiungere il nuovo certificato e attendere che il processo di registrazione distribuisca il nuovo certificato nell'FTD.



nuovo certificato

Il nuovo certificato deve essere visibile senza una croce rossa nel campo CA.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

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.

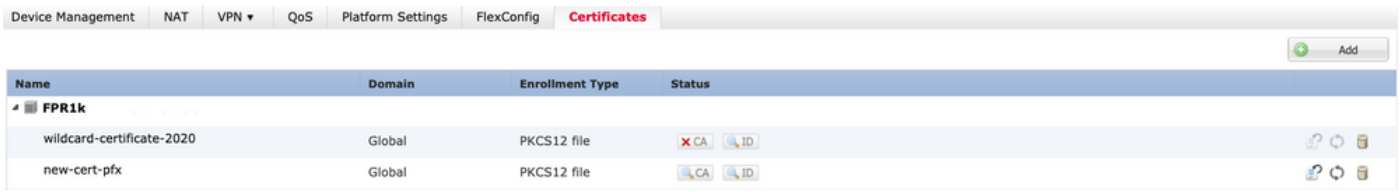
```
certutil -dump cert.pfx
```

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:



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).