Troubleshoot Certificate Error "Identity certificate import required" on FMC

Contents

Introduction

This document describes how to troubleshoot and fix the "Identity certificate import required" error on Firepower Threat Defense (FTD) devices managed by Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Public Key Infrastructure (PKI)
- FMC
- FTD
- OpenSSL

Components Used

The information used in the document is based on these software versions:

- MacOS x 10.14.6
- FMC 6.4
- OpenSSL

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact

of any command.

Background information

> **Note**: On FTD devices, the Certificate Authority (CA) certificate is needed before the Certificate Signing Request (CSR) is generated.

- If the CSR is generated in an external server (such as Windows Server or OpenSSL), the **manual enrollment method** is intended to fail, since FTD does not support manual key enrollment. A different method must be used such as PKCS12.

Problem

A certificate is imported in the FMC and an error is received which states that an identity certificate is required to proceed with the certificate enrollment.

Scenario 1

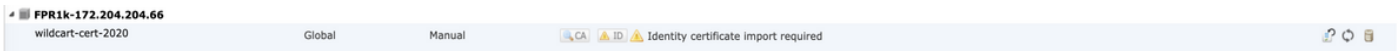
- Manual enrollment is selected
- CSR is generated externally (Windows Server, OpenSSL, etc) and you don't have (or know) the private key information
- A previous CA cert is used to fill the CA cert information, but it is unknown if this cert is responsible for the certificate sign

Scenario 2

- Manual enrollment is selected
- CSR is generated externally (Windows Server, OpenSSL)
- You have the certificate file from the CA that signs our CSR

For both procedures, the certificate is uploaded and a progress indication is displayed as shown in the image.

After a couple of seconds, the FMC still states that an ID cert is required:



The previous error indicates that either the CA certificate does not match with the issuer information in the ID certificate or, the private key does not match with the one generated by default in the FTD.

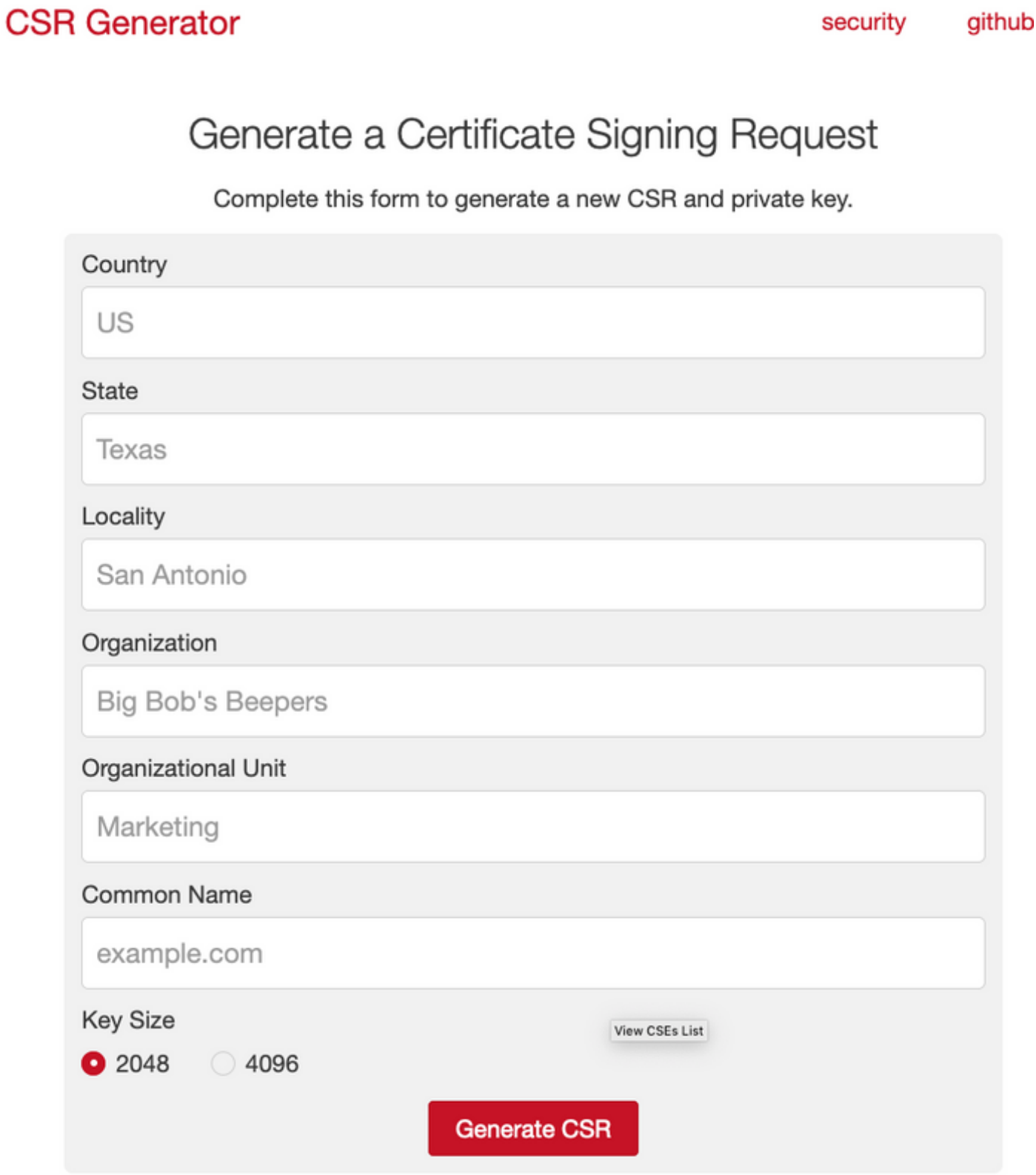
Solution

In order to make this certificate enrollment to work, you must have the correspondent keys for the ID certificate. With the use of OpenSSL a PKCS12 file is generated.

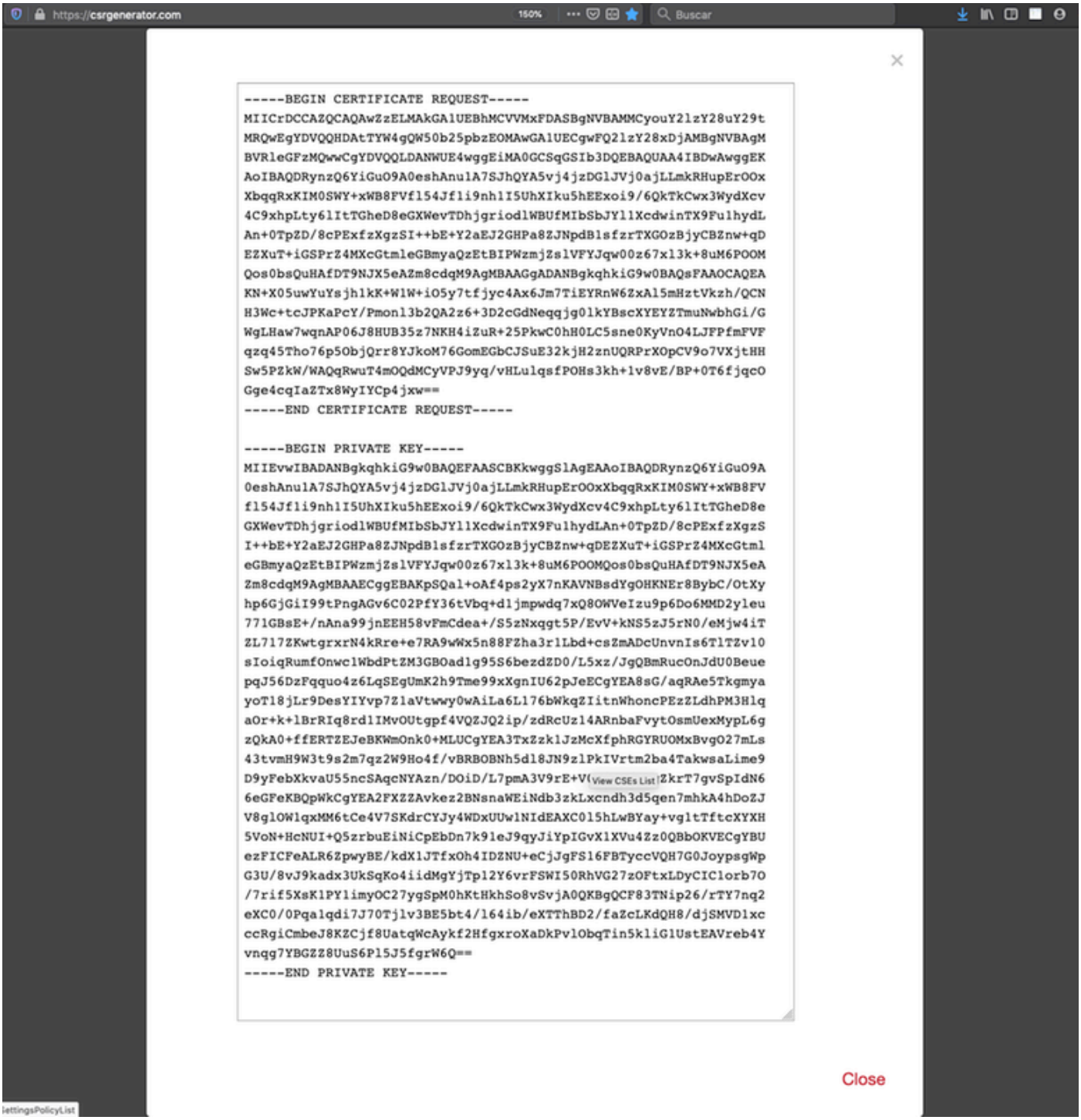
Step 1. Generate a CSR (Optional)

You can get a CSR along with its private key with the use of a third-party tool called **CSR generator** (csrgenerator.com).

Once the certificate information is filled accordingly, select the option to **Generate CSR**.



This provides the CSR + Private key for us to send to a Certificate Authority:



Step 2. Sign the CSR

The CSR needs to be signed by a third-party CA (GoDaddy, DigiCert), once the CSR is signed, a zip file is provided, which contains among other things:

- Identity Certificate
- CA bundle (Intermediate certificate + root certificate)

Step 3. Verify and Separate the Certificates

Verify and separate the files with the use of a text editor (for example, notepad). Create the files with easily identifiable names for the private key (**key.pem**), identity certificate (**ID.pem**), CA certificate (**CA.pem**).

For the case in which the CA bundle file has more than 2 certificates (1 root CA, 1 sub-CA), the root CA needs to be removed, the ID certificate issuer is the sub-CA, therefore, it is not relevant to have the root CA in this scenario.

Content of the file named **CA.pem:**

```
Bag Attributes
    localKeyID: 4B ED BA 56 76 3A C9 22 C3 75 54 A7 0A 1A F1 7D 3B 5E B0 D8
subject=/C=US/ST=Texas/L=San Antonio/O=Cisco/OU=VPN/CN=*.cisco.com
issuer=/C=MX/ST=CDMX/O=Ungu Corp/OU= Corp Certificate Authority/CN=Corp Intermediate CA
-----BEGIN CERTIFICATE-----
MIIFojCCA4qgAwIBAgICEBowDQYJKoZIhvcNAQELBQAwfjELMAkGA1UEBhMCTVgx
DTALBgNVBAgMBENETVgxEjAQBgNVBAoMCVVuZ3UgQ29ycDEoMCYGA1UECwwfVW5n
dSBDb3JwIENlcnRpZmljYXRlIEF1dGhvcml0eTEiMCAGA1UEAwwZVW5ndSBDb3Jw
IEludGVybWVkaWF0ZSBDQTAeFw0yMDAyMjcwNjE1MjRaFw0yMTAzMDgwNjE1MjRa
MGcxCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczEUMBIGA1UEBwwLU2FuIEFu
dG9uaW8xDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANWUE4xFDASBgNVBAMMCyou
Y2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsrPghHA3
7r/ShqU7HjOl6muESBwmeDYTbOSBDz6T3OE95T67Ey0ra8/sxyorCMzTHSPr6adF
o7xbrjm1onhneeJv+6sUbF1FnZnyNjrjAd/6u8BCJcXPdHESp4kvFGv8fuNAE01s
gjfuj+Ap1iPbWUjsxs1CDlq2O8H/NyPn+mvu2Kvo1sJZls5VAAk6D2FxSpwos4tV
sXUn71lymzyArhDMQ0sGib8s8oOPqnBYPhy12+AWECqHTccMbsVxC3S11hHQMPCi
LAEC/ijQeISMOxdR/p4CpjbuNJTIQQw8CRqjSvkY2DGZs3slLo56RrHpRJdcukD5
zKGRLrKCtOjvyQIDAQABo4IBPzCCATswCQYDVR0TBAIwADARBglghkgBhvhCAQEE
BAMCBkAwMwYJYIZIAYb4QgENBCYWJE9wZW5TU0wgR2VuZXJhdGVkIFNlcnZlciBD
ZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUzED6CQ5u/wcK7y+GYz9ccDkrUigwgaEGA1Ud
IwSBmTCBloAUT8MBVNLJSgdOEG3GW+KnUvRMRCiheqR4MHYxCzAJBgNVBAYTAk1Y
MQ0wCwYDVQQIDARDRE1YMRIwEAYDVQQKDAlVbmd1IENvcnAxKDAmBgNVBAsMH1Vu
Z3UgQ29ycCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkxGjAYBgNVBAMMEVVuZ3UgQ29y
cCBSb290IENBggIQADAOBgNVHQ8BAf8EBAMCBaAwEwYDVR0lBAwwCgYIKwYBBQUH
AwEwDQYJKoZIhvcNAQELBQADggIBAJuAihWxJ44ug/vEhZaUapUtYSqKWzMLZbBr
un1IMsL8I8AhuWM93PPmHX2Tm2XwQlo9PBN3aNacUz/FneZ/NNfQwC1GfJCTHJVE
K4+GWDNIeVznY7hbMppt5iJNuBMR/EoYoQ0xdqPtnLEqt92WgGjn6kvjVLw6eJKB
Ph75RDyr5DQz86Agnl/JzjvpeLRl0eqMTCxgQJbYOeUrZCRNDWaV/ahpvmZ9xPV6
MB1la6GipT5EcFe16WPNiqQa+3f+y8nsnsMDNE8UXW8nSqZwdTdA8THxkpogcPTb
isw8a9CkindzZhI6rtoCI0QXmqkw6uXPWcw5PnTTO8TnSQoMJnC/Hvaa/tiiFA3F
dkaPLePgDScFZED2nPIFsbXfb2zFRCN2YLirose/k9wc8rXlZ639uVCXN4yYmx9b
ADrqqQdkUXCGCGrQjXzWRNCORZihfTKg+ANoEaWgBsgInqtV5R/nsSkeibva9rBG
yHPUkZB70Xz2AuINod70aPDiQCabEpVTcV5dr8+r9L1h5UQCIim+wPgBAQzG9Bz9
JM5RHriNhdmKQkvjDbqcKx8V3tjYpDNHgWAlwnaoICEoDKbSoiLdWgaPt4F1kipW
2RImd7X9wPetswGeOpI3q39mBtgQ1eAARXVB373il2WvxEWnjfBa9V4GAZcoMjpx
92xpoxSl
-----END CERTIFICATE-----
```

Content of the file named **key.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-----
```

Content of the file named **ID.pem**:

```
-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICEAEwDQYJKoZIhvcNAQELBQAwgZIxCzAJBgNVBAYTAk1Y
MQ0wCwYDVQQIDARDRE1YMRIwEAYDVQQKDAlVbmd1IENvcnAxMjAwBgNVBAsMKUFu
eWNvbm5lY3QgaG9sZ3VpbnMgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSwwKgYDVQQD
DCNBbnljb25uZWN0IGhvbGd1aW5zIEludGVybWVkaWF0ZSBDQTAeFw0yMDA0MDUy
MjI3NDhaFw0yMDA0MjUyMjI3NDhaMGcxCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVU
ZXhhczEUMBIGA1UEBwwLU2FuIEFudG9uaW8xDjAMBgNVBAoMBUNpc2NvMQwwCgYD
VQQLDANWUE4xFDASBgNVBAMMCyouY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAxcrtoc7qbNIqPD5jwxTZRZPTQJbDE9y/WIySZWQ0CEL9
AwFSziHOsuXpivM4Q5Lx1TOPhHaPS7lligmIfca4m2/5E6n4kMqUMnlPTR+7QGT7
j+0872AA0Rr0tag7XmdBSw7V66aTodkYhrJoUxHsCdey5D1xdapyvzl2hHcYqemi
HZtXthVq1XTfeC2LGESvz1cb0++MKcraeZgykM6Ho3aaOG52w1xzFlFGUe2nkKaT
I6WcuD4dnQLXFiWDGmh7foQ30biFyJ4MjT4QZBCQdW080axeYCQbR38Qn28tFzuU
/xj33kUKyExuJeSFuZoKcuwhrPgwekcvYxw4NzMOuQIDAQABo4IBPzCCATswCQYD
VR0TBAIwADARBglghkgBhvhCAQEEBAMCBkAwMwYJYIZIAYb4QgENBCYWJE9wZW5T
U0wgR2VuZXJhdGVkIFNlcnZlciBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQURWLK5NOS
KlNN/LPU6E0Q/SVp/K0wgaEGA1UdIwSBmTCBloAUzMVIA+G1XbnwtEZX0syJQGUq
jeaheqR4MHYxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRIwEAYDVQQKDAlV
bmd1IENvcnAxKDAmBgNVBAsMH1VuZ3UgQ29ycCBDZXJ0aWZpY2F0ZSBBdXRob3Jp
dHkxGjAYBgNVBAMMEVVuZ3UgQ29ycCBSb290IENBggIQAjAOBgNVHQ8BAf8EBAMC
BaAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQADggIBAJtmMncK
3iF+q31fE8/m3gghNjfkqrvyCkILnwuw2vx2CHCMgGzU4MT5AodGJfJJZNq2Cbhy
VaPGm7/X010gW5dfbeHPLvyWqdK4nQLtw2krlpRznoeEk16qumPBrHVmWUZQoWpV
elDzSiqzhbv+vFMP4OFOlbMYHDSAcolLedCS7KuQ/c0soGNR1oGSA2hUYM60MEiW
ezBgT7R/XK+Rh5zwlok4mje8R1rY7qUIn/hrKUDf/JNiBNFUvD6vDYLHJA3W2slO
ou3vdLy7z57Lj4WbtheHXQsmD6n9N+ANxmHpqpWPPD94YRalvpDbefU2hYrHx7fn
1jSdpzyOmw6JluxWbWOkp+BER+5Ya3rqIpBtljfbhZ18C17Hhb5oixSqBwL6oGa9
vOu6mhVHQBrPLeg+A/Pfkmpwq/wr19iUOLW+tJ8Lc7/Qlst7kCEjncub4SNvb6cx
RRzi53fE3MVVqL6pBpBm4Pgt552ku7Lr3254haAmIczQ6Lxhq28Wo/Sq6bNDlXBh
Wg8ZfjpwraAloKStUPYPQyHuz6POuPGybaBjyjChkTooO3CkBpl1YIZdttZMtFHC
bmKJMQ45LsaF5aGcuL0sr4YB2EyJBVU4vAWnVJ7j1SZOnntPFNebfRKV/hjZ4k+g
ViWh5GmceXBbcTQ7wbVxpbYFnXtYge78OzUz
-----END CERTIFICATE-----
```

Step 4. Merge the Certificates in a PKCS12

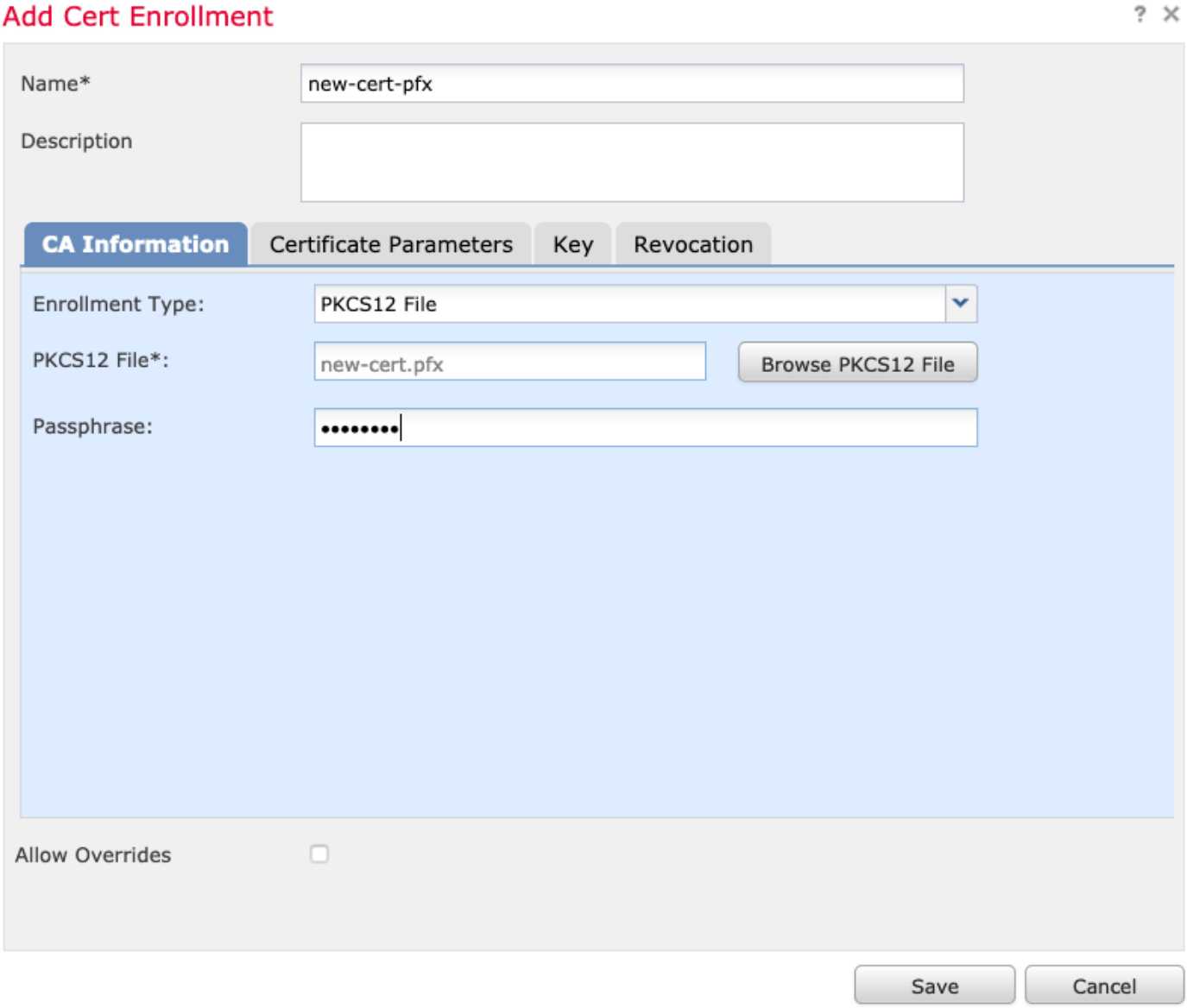
Merge the CA certificate along with the ID Certificate and private key in a **.pfx** file. You must protect this file with a passphrase.

```
openssl pkcs12 -export -in ID.pem -certfile ca.pem -inkey key.pem -out new-cert.pfx
```

```
HOLGUINS-M-Q3UV:tshoot hugoolguin$ openssl pkcs12 -export -in ID.pem -certfile ca.pem -inkey key.pem -out new-cert.pfx
Enter pass phrase for key.pem:
Enter Export Password:
Verifying - Enter Export Password:
HOLGUINS-M-Q3UV:tshoot hugoolguin$
```

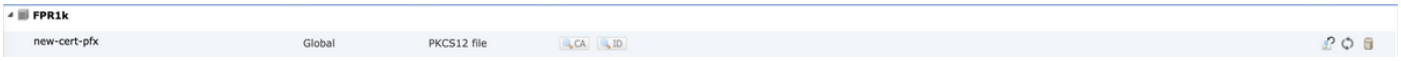
Step 5. Import the PKCS12 Certificate in the FMC

In the FMC, navigate to **Device > Certificates** and import the certificate to the desired firewall:



Verify

In order to verify the certificate status along with the **CA** and **ID** information, you can select the icons and confirm that it was successfully imported:



Select the **ID** icon:

Identity Certificate

- Serial Number : 101a
- Issued By :
  - Common Name : Ungu Corp Intermediate CA
  - Organization Unit : Ungu Corp Certificate Authority
  - Organization : Ungu Corp
  - State : CDMX
  - Country Code : MX
- Issued To :
  - Common Name : *.cisco.com
  - Organization Unit : VPN
  - Organization : Cisco
  - Locality : San Antonio
  - State : Texas

Close