FMC上的证书错误“需要身份证书导入”故障排除

目录

简介

本文档介绍如何排除和修复由Firepower管理中心(FMC)管理的Firepower威胁防御(FTD)设备上的“需要身份证书导入”错误。

先决条件

要求

Cisco 建议您了解以下主题：

- 公用密钥基础结构 (PKI)
- FMC
- FTD
- OpenSSL

使用的组件

本文档中使用的信息基于以下软件版本：

- MacOS x 10.14.6
- FMC 6.4
- OpenSSL

背景信息

注意：在FTD设备上，生成证书签名请求(CSR)之前需要证书颁发机构(CA)证书。

- 如果在外部服务器（例如Windows Server或OpenSSL）中生成CSR，**manual enrollment method**将会失败，因为FTD不支持手动密钥注册。必须使用其他方法，例如PKCS12。

问题

在FMC中导入证书并收到错误，表明需要身份证书才能继续进行证书注册。

场景 1

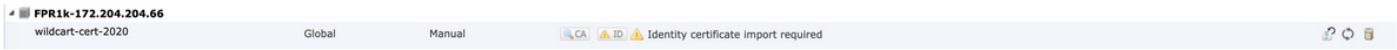
- 已选择手动注册
- CSR在外部生成（Windows Server、OpenSSL等），并且您没有（或知道）私钥信息
- 以前的CA证书用于填充CA证书信息，但是如果此证书负责证书签名，则此证书未知

场景 2

- 已选择手动注册
- CSR在外部生成(Windows Server、OpenSSL)
- 您拥有来自CA的证书文件，用于签署我们的CSR

对于这两个过程，都会上传证书并显示进度指示，如图所示。

几秒钟后，FMC仍声明需要ID证书：



上一个错误表示CA证书与ID证书中的颁发者信息不匹配，或者私钥与FTD中默认生成的密钥不匹配。

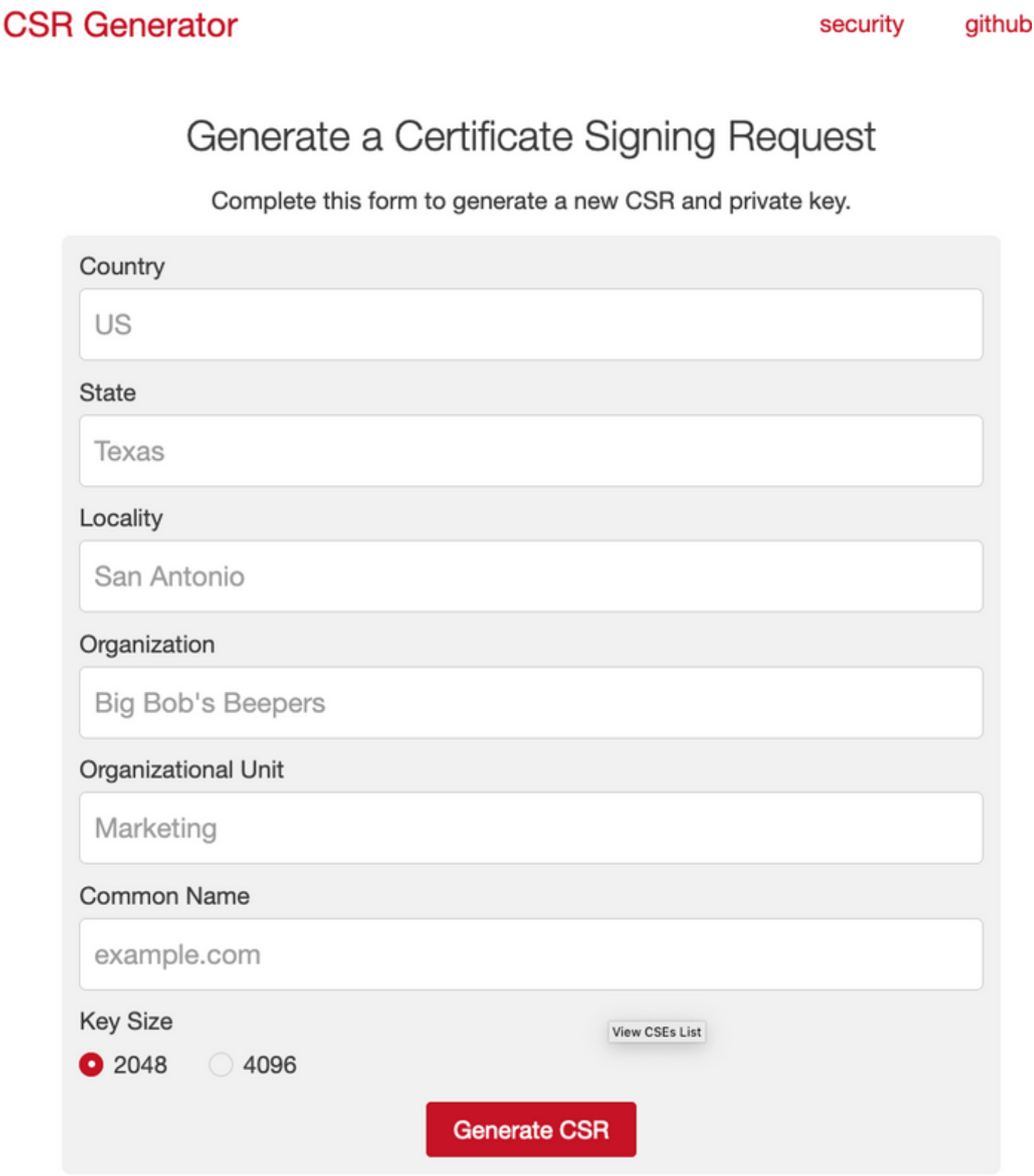
解决方案

要使此证书注册生效，您必须具有ID证书的相应密钥。使用OpenSSL可生成PKCS12文件。

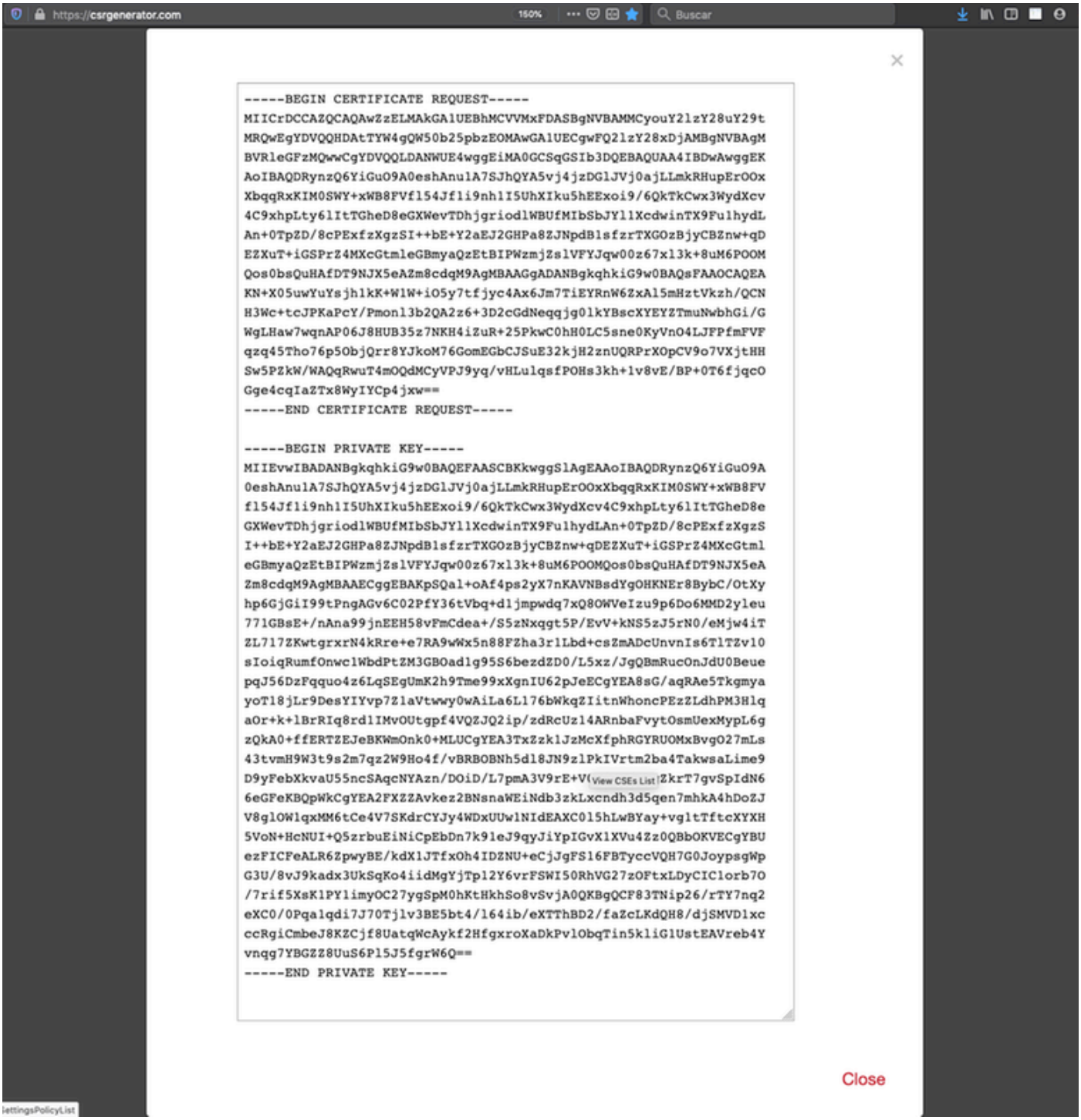
步骤1.生成CSR（可选）

您可以使用称为CSR生成器的第三方工具(csrgenerator.com)获取CSR**及其私**钥。

在相应填写证书信息后，选择**生成CSR**选项。



这为我们提供了要发送到证书颁发机构的CSR +私钥：



步骤2.签署CSR

CSR需要由第三方CA(GoDaddy、DigiCert)签署，签署CSR后，将提供一个压缩文件，其中包含：

- 身份证书
- CA捆绑包（中间证书+根证书）

步骤3.检验并分离证书

使用文本编辑器（例如，记事本）验证和分隔文件。 使用私钥(**key.pem**)、身份证书(**ID.pem**)和CA证书(**CA.pem**)的易识别名称创建文件。

对于CA捆绑文件具有超过2个证书（1个根CA，1个子CA）的情况，需要删除根CA，ID证书颁发机

构是子CA，因此，在此场景中拥有根CA不相关。

CA.pem文件的内容：

```
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-----
```

名为key.pem的文件的内容：

```
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-----
```

名为ID.pem的文件的内容：

```
-----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-----
```

步骤4.合并PKCS12中的证书

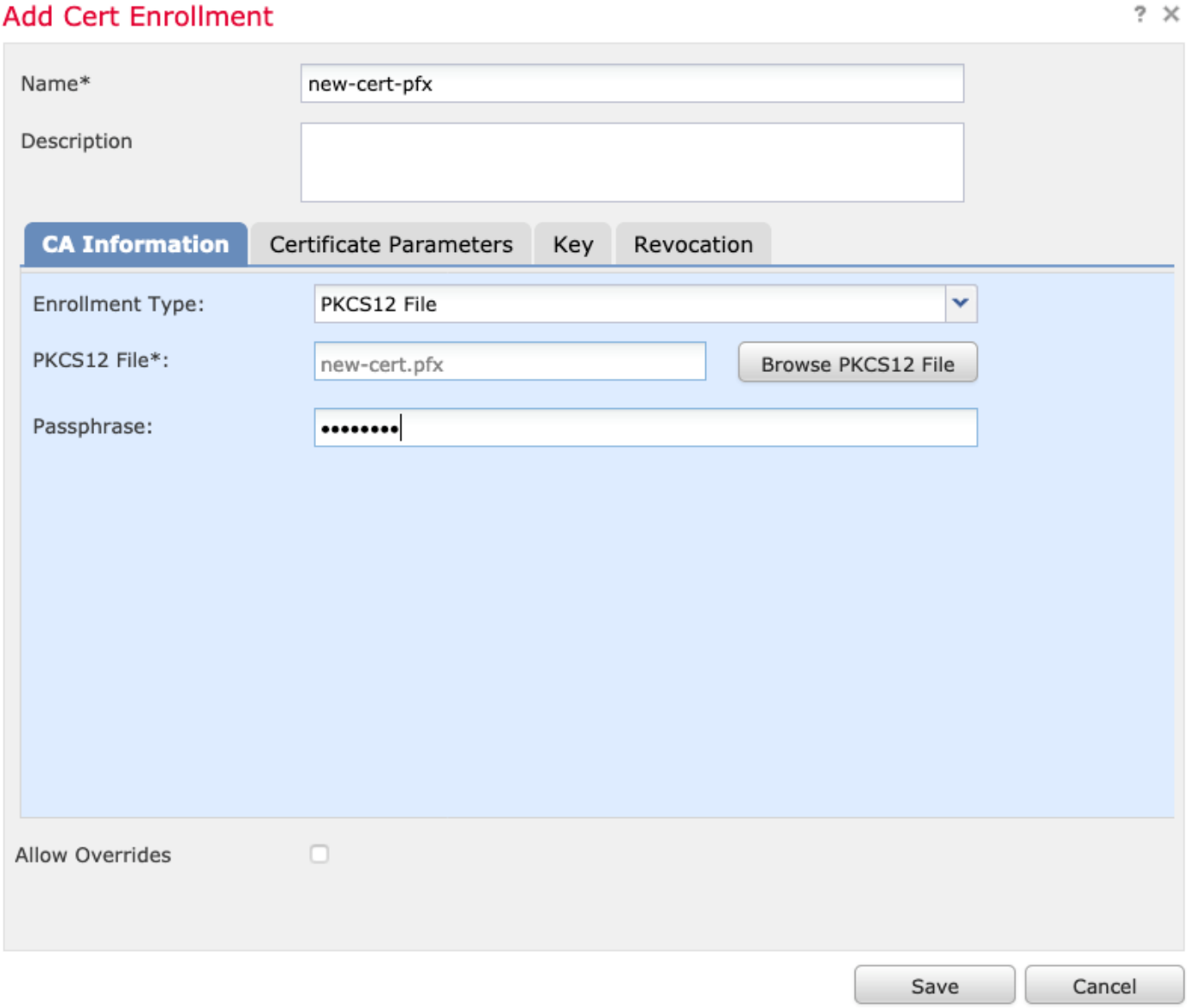
将CA证书与ID证书和私钥合并到.pfx**文件**中。您必须使用密码保护此文件。

```
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$
```

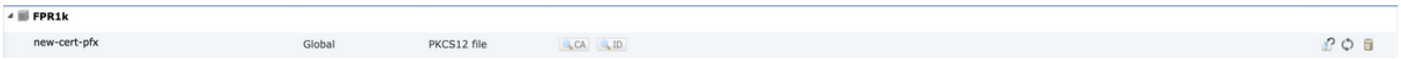
步骤5.在FMC中导入PKCS12证书

在FMC中，导航到**Device > Certificates**并将证书导入所需的防火墙：



验证

要验证证书状态以及CA和ID信息，您可以选择图标并确认其已成功导入：



选择ID图标：

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。