Solucionar error de certificado "Se requiere importación de certificado de identidad" en FMC

Contenido

Introducción

Este documento describe cómo resolver problemas y corregir el error "Se requiere importación de certificado de identidad" en los dispositivos Firepower Threat Defense (FTD) administrados por Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

La información utilizada en el documento se basa en estas versiones de software:

- MacOS x 10.14.6
- CSP 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.

Antecedentes

> **Nota:** En los dispositivos FTD, se necesita el certificado de la autoridad certificadora (CA) antes de generar la solicitud de firma de certificado (CSR).

- Si el CSR se genera en un servidor externo (como Windows Server o OpenSSL), el **método de inscripción manual** está destinado a fallar, ya que FTD no admite la inscripción manual de claves. Se debe utilizar un método diferente, como PKCS12.

Problema

Se importa un certificado en el FMC y se recibe un error que indica que se requiere un certificado de identidad para continuar con la inscripción del certificado.

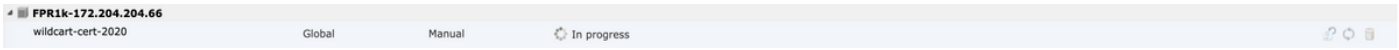
Escenario 1

- La inscripción manual está seleccionada
- CSR se genera externamente (Windows Server, OpenSSL, etc.) y no se dispone de la información de clave privada (o esta no la conoce)
- Se utiliza un certificado de CA anterior para rellenar la información del certificado de CA, pero se desconoce si este certificado es responsable del signo del certificado

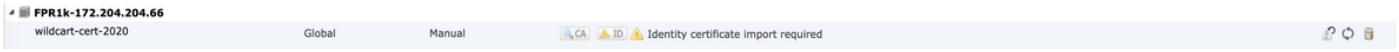
Escenario 2

- La inscripción manual está seleccionada
- CSR se genera externamente (Windows Server, OpenSSL)
- Tiene el archivo de certificado de la CA que firma nuestra CSR

Para ambos procedimientos, se carga el certificado y se muestra una indicación de progreso como se muestra en la imagen.



Tras un par de segundos, el CSP sigue indicando que se requiere un certificado de identificación:



El error anterior indica que el certificado de la CA no coincide con la información del emisor en el certificado de ID o que la clave privada no coincide con la generada de forma predeterminada en el FTD.

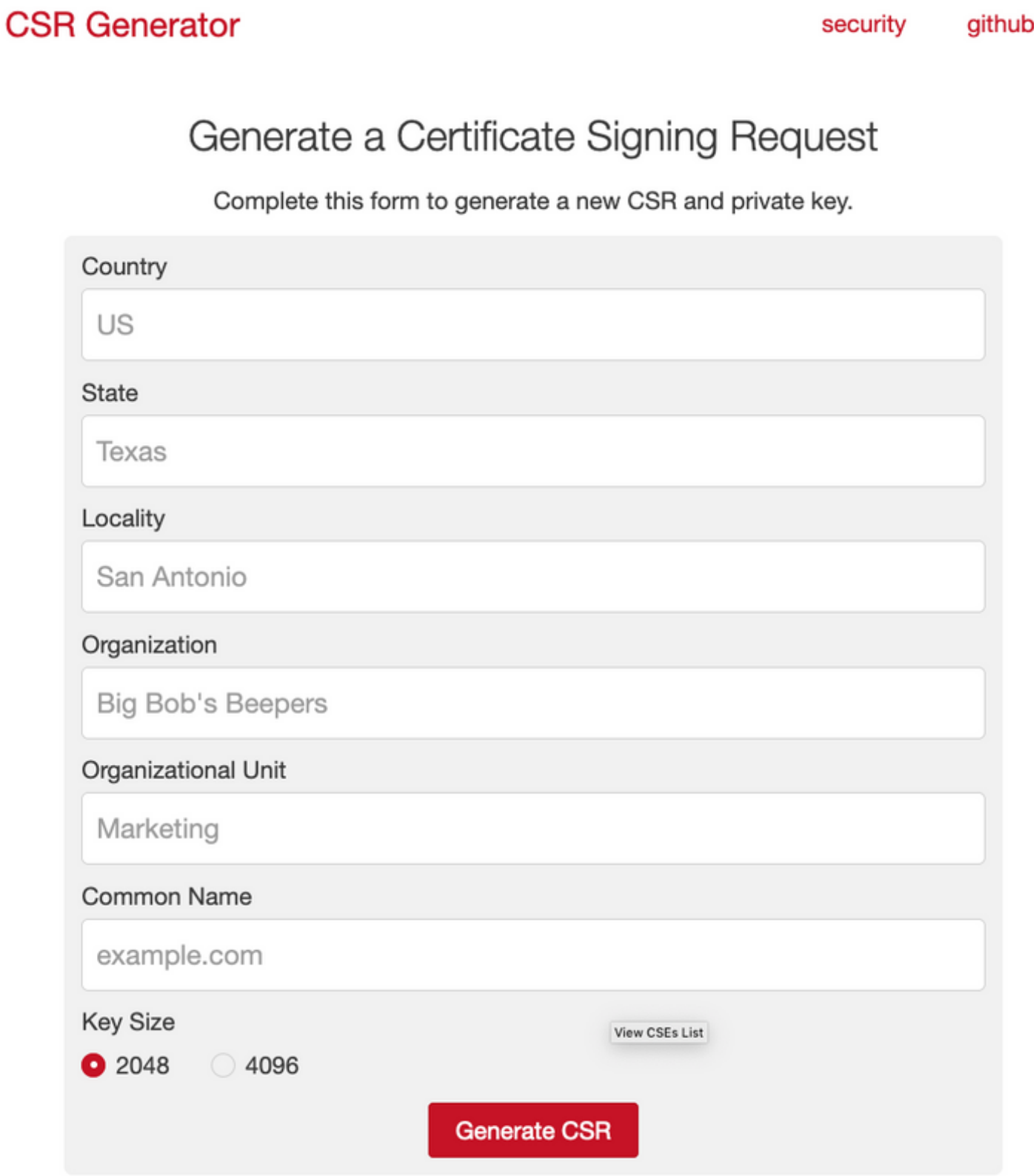
Solución

Para que esta inscripción de certificados funcione, debe tener las claves correspondientes para el certificado de ID. Con el uso de OpenSSL se genera un archivo PKCS12.

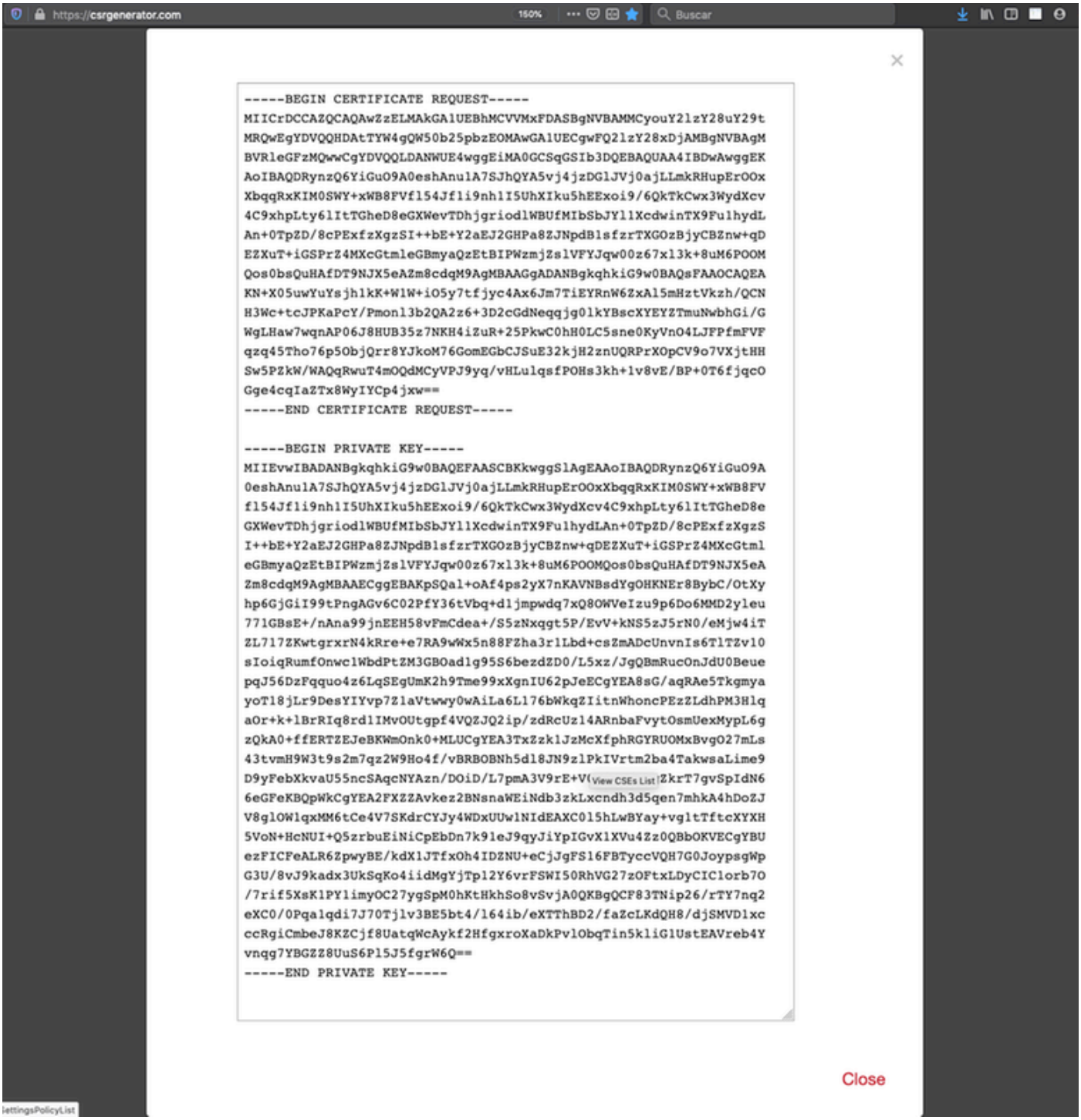
Paso 1. Generar una CSR (opcional)

Puede obtener una CSR junto con su clave privada con el uso de una herramienta de terceros llamada **generador CSR** (csrgenerator.com).

Una vez que la información del certificado se haya rellenado en consecuencia, seleccione la opción para **Generar CSR**.



Esto proporciona la CSR + clave privada para que la enviemos a una autoridad de certificación:



Paso 2. Firme el CSR

El CSR debe estar firmado por una CA de terceros (GoDaddy, DigiCert). Una vez firmado el CSR, se proporciona un archivo zip que contiene, entre otras cosas:

- Certificado de identidad
- Paquete de CA (certificado intermedio + certificado raíz)

Paso 3. Verificar y separar los certificados

Verifique y separe los archivos con el uso de un editor de texto (por ejemplo, un bloc de notas). Cree los archivos con nombres fácilmente identificables para la clave privada (**key.pem**), el certificado de identidad (**ID.pem**), el certificado de CA (**CA.pem**).

En el caso de que el archivo de agrupamiento de CA tenga más de 2 certificados (1 CA raíz, 1 CA secundaria), debe eliminarse la CA raíz, el emisor del certificado de ID es la CA secundaria, por lo tanto, no es relevante tener la CA raíz en este escenario.

Contenido del archivo denominado **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-----
```

Contenido del archivo denominado **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-----
```

Contenido del archivo denominado **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-----
```

Paso 4. Fusionar los certificados en un PKCS12

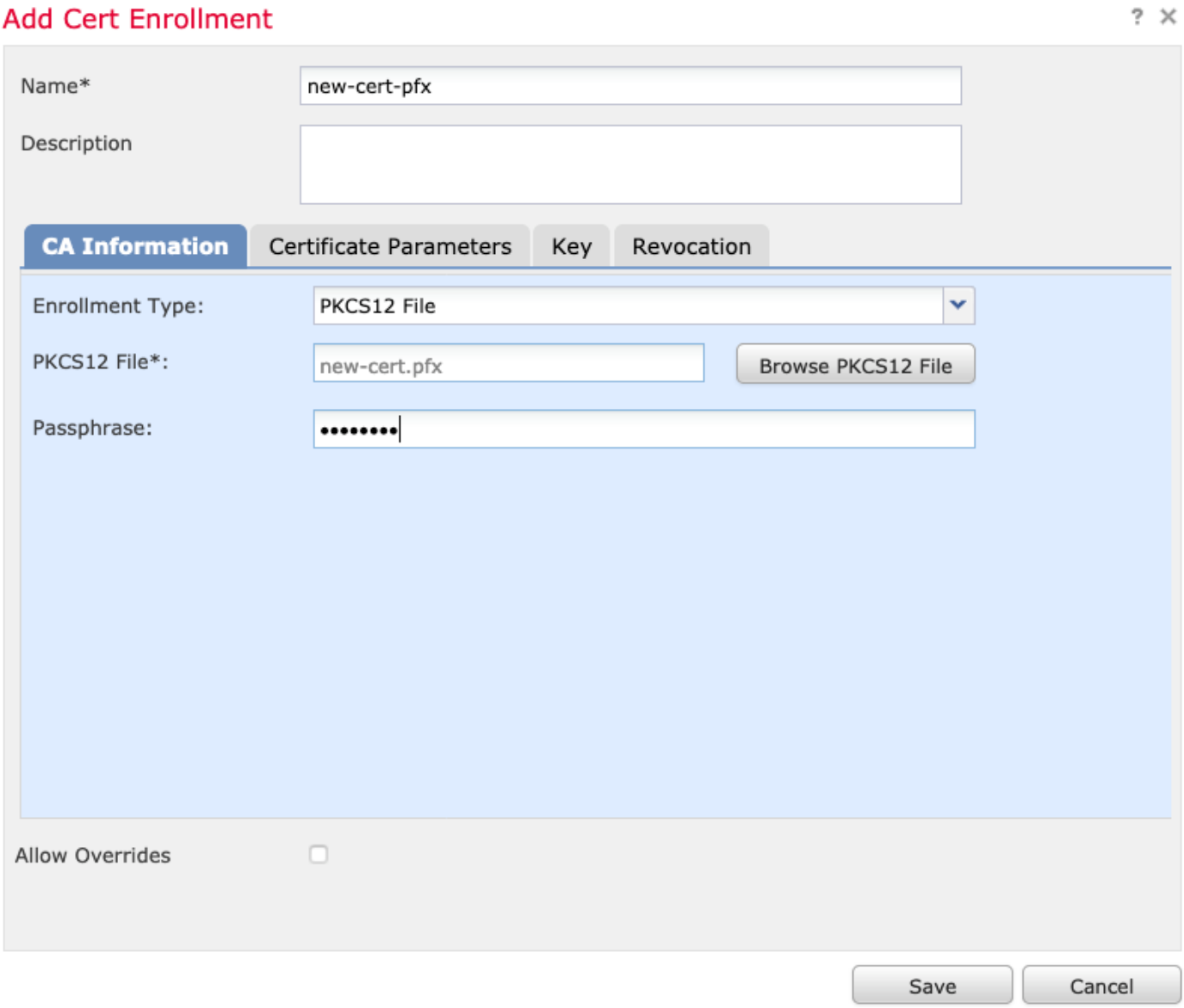
Combine el certificado de CA con el certificado de ID y la clave privada en un archivo **.pfx**. Debe proteger este archivo con una frase de contraseña.

```
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$
```

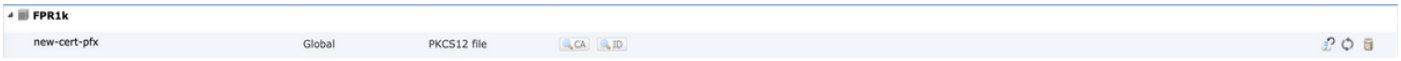
Paso 5. Importar el certificado PKCS12 en el FMC

En el FMC, navegue hasta **Device > Certificates** e importe el certificado al firewall deseado:



Verificación

Para verificar el estado del certificado junto con la información de **CA** e **ID**, puede seleccionar los iconos y confirmar que se importó correctamente:



Seleccione el icono **ID**:

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).