Risoluzione dei problemi relativi all'errore del certificato "Importazione del certificato di identità obbligatoria" in FMC

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi all'errore "Importazione obbligatoria del certificato di identità" nei dispositivi Firepower Threat Defense (FTD) gestiti da Firepower Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni contenute nel 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:** Sui dispositivi FTD è necessario il certificato CA (Certification Authority) prima che venga generata la 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** non riuscirà, poiché FTD non supporta la registrazione manuale delle chiavi. È necessario utilizzare un metodo diverso, ad esempio PKCS12.

Problema

Nel CCP viene importato un certificato e viene visualizzato un errore che indica che per continuare la registrazione del certificato è necessario un certificato di identità.

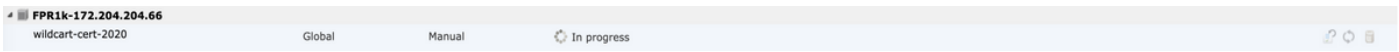
Scenario 1

- L'iscrizione manuale è selezionata
- CSR viene generato esternamente (Windows Server, OpenSSL e così via) e non si dispone (o si è a conoscenza) delle informazioni sulla chiave privata
- Per compilare le informazioni del certificato CA viene utilizzato un certificato CA precedente, ma non è noto se questo certificato è responsabile della firma del certificato

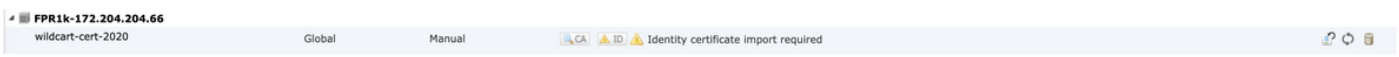
Scenario 2

- L'iscrizione manuale è selezionata
- CSR generato esternamente (Windows Server, OpenSSL)
- Si dispone del file di certificato della CA che firma il CSR

Per entrambe le procedure, il certificato viene caricato e viene visualizzata un'indicazione di avanzamento, come mostrato nell'immagine.



Dopo un paio di secondi, il CCP indica ancora che è necessario un certificato di identità:



L'errore precedente indica che il certificato CA non corrisponde alle informazioni sull'autorità emittente nel certificato ID oppure che la chiave privata non corrisponde a quella generata per impostazione predefinita nell'FTD.

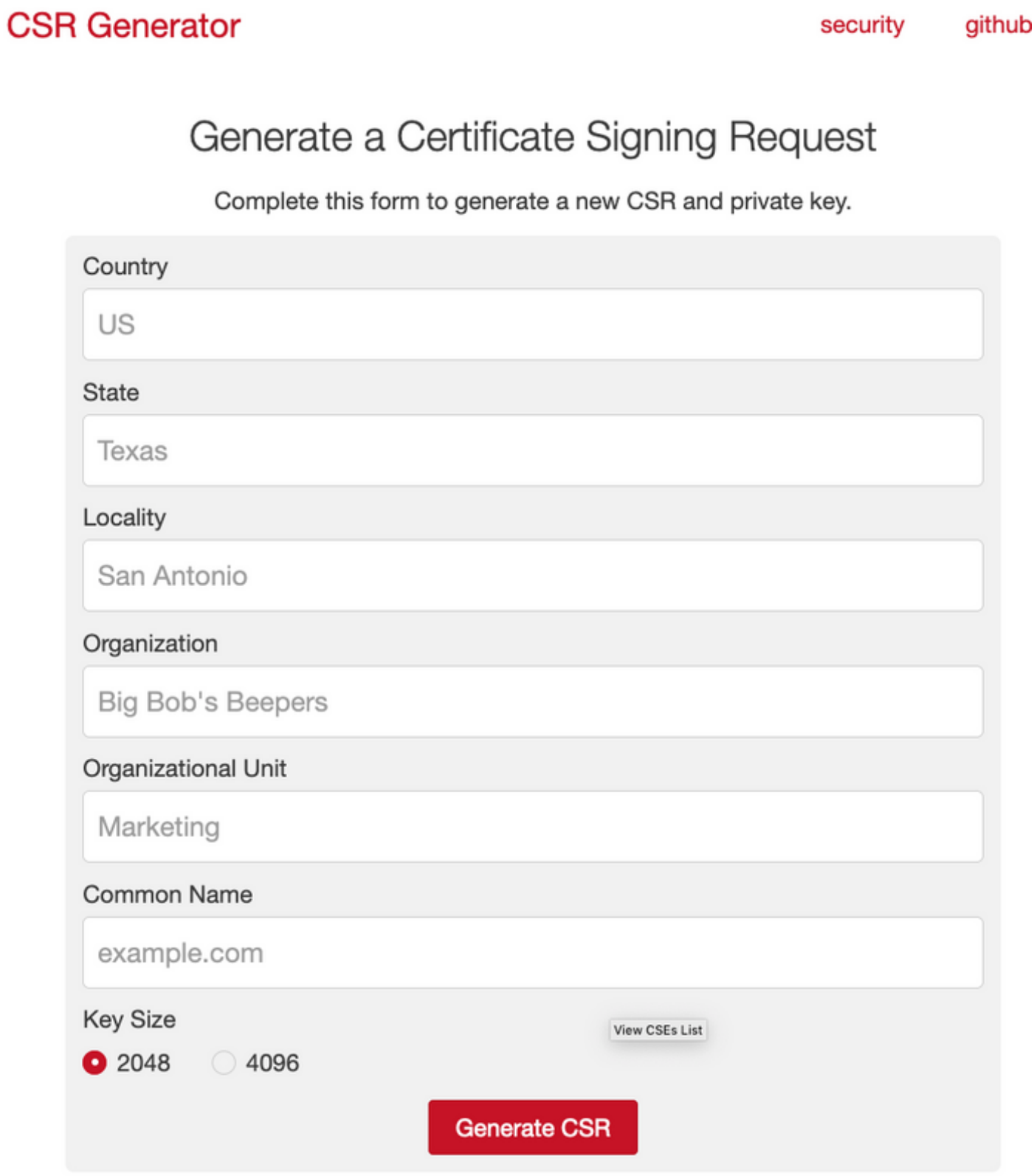
Soluzione

Affinché la registrazione del certificato funzioni, è necessario disporre delle chiavi corrispondenti per il certificato ID. Con OpenSSL viene generato un file PKCS12.

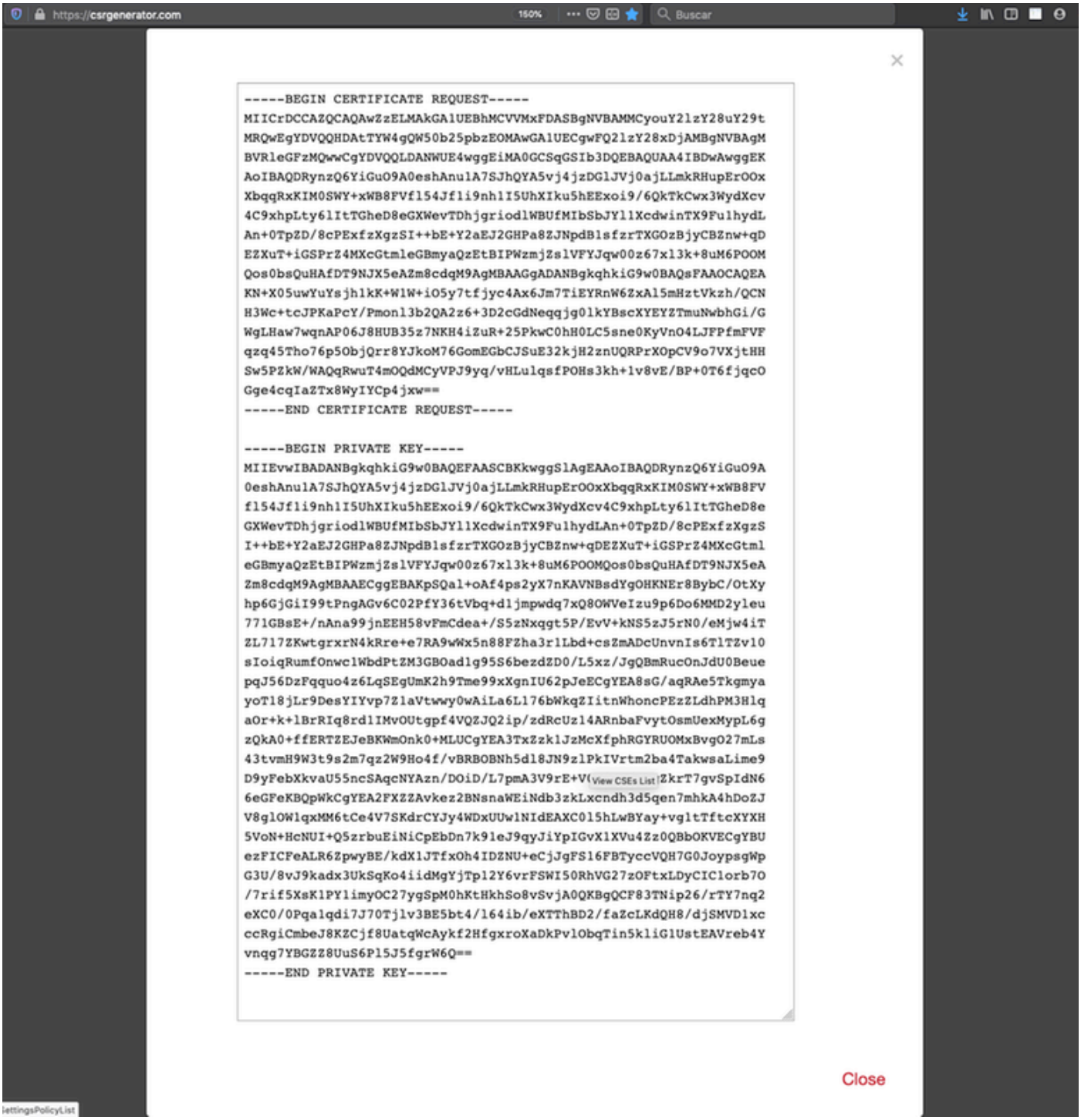
Passaggio 1. Generare un CSR (facoltativo)

Èpossibile ottenere un CSR insieme alla relativa chiave privata utilizzando uno strumento di terze parti denominato **CSR generator** (csrgenerator.com).

Una volta inserite le informazioni sul certificato, selezionare l'opzione **Genera CSR**.



In questo modo viene fornita la chiave CSR + Private da inviare a un'autorità di certificazione:



Passaggio 2. Firma CSR

Il CSR deve essere firmato da un'autorità di certificazione di terze parti (GoDaddy, DigiCert), dopo la firma del CSR viene fornito un file zip contenente, tra le altre cose:

- Certificato di identità
- Pacchetto CA (certificato intermedio + certificato radice)

Passaggio 3. Verificare e separare i certificati

Verificare e separare i file utilizzando un editor di testo, ad esempio il Blocco note. Creare i file con nomi facilmente identificabili per la chiave privata (**key.pem**), il certificato di identità (**ID.pem**), il certificato CA (**CA.pem**).

Nel caso in cui il file del bundle CA contenga più di 2 certificati (1 CA radice, 1 CA secondaria), la CA radice deve essere rimossa, l'autorità emittente del certificato ID è la CA secondaria, pertanto in questo scenario non è rilevante avere la CA radice.

Contenuto del file **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-----
```

Contenuto del file **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-----
```

Contenuto del file **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-----
```

Passaggio 4. Unire i certificati in un PKCS12

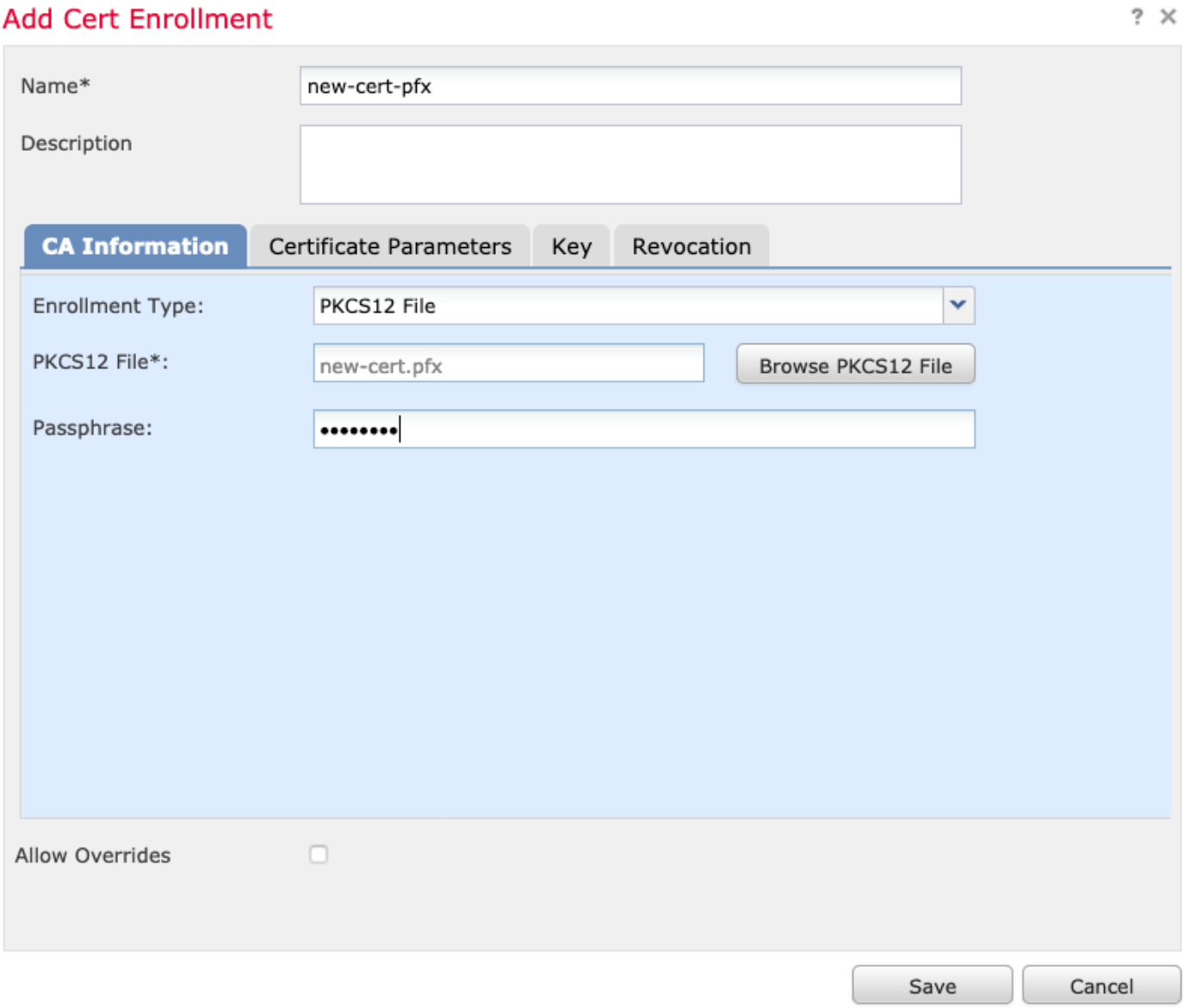
Unire il certificato CA con il certificato ID e la chiave privata in un file **pfx**. È necessario proteggere il file con una passphrase.

```
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$
```

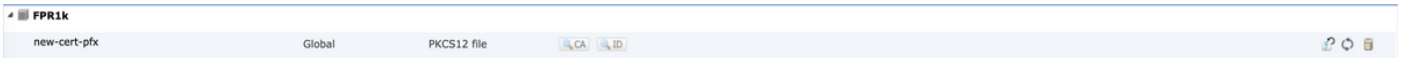
Passaggio 5. Importare il certificato PKCS12 nel CCP

Nel FMC, selezionare **Periferica > Certificati** e importare il certificato nel firewall desiderato:



Verifica

Per verificare lo stato del certificato insieme alle informazioni **CA** e **ID**, è possibile selezionare le icone e confermare l'importazione:



Selezionare l'icona **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

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).