

對FMC上的證書錯誤「需要匯入身份證書」進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[問題](#)

[解決方案](#)

[步驟1. 產生CSR \(可選\)](#)

[步驟2. 簽署CSR](#)

[步驟3. 驗證並分離憑證](#)

[步驟4. 合併PKCS12中的證書](#)

[步驟5. 匯入FMC中的PKCS12證書](#)

[驗證](#)

簡介

本文說明如何排解和修正由Firepower管理中心(FMC)管理的Firepower威脅防禦(FTD)裝置上的「需要身份證書匯入」錯誤。

必要條件

需求

思科建議您瞭解以下主題：

- 公開金鑰基礎架構 (PKI)
- FMC
- FTD
- OpenSSL

採用元件

文中使用的資訊是根據以下軟體版本：

- MacOS x 10.14.6
- FMC 6.4
- OpenSSL

背景資訊

附註：在FTD裝置上，需要先取得憑證授權單位(CA)憑證，才能產生憑證簽署請求(CSR)。

- 如果在外部伺服器 (例如Windows Server或OpenSSL) 中產生CSR，則**手動註冊方法**會失敗，因為FTD不支援手動金鑰註冊。必須使用其他方法，例如PKCS12。

問題

在FMC中匯入證書並收到一個錯誤，說明需要身份證書才能繼續進行證書註冊。

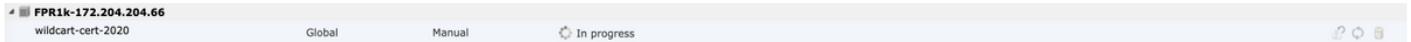
案例 1

- 已選擇手動註冊
- CSR是從外部生成的 (Windows Server、OpenSSL等)，您沒有 (或知道) 私鑰資訊
- 以前的CA證書用於填充CA證書資訊，但不知道此證書是否負責證書簽名

案例 2

- 已選擇手動註冊
- CSR是從外部生成的(Windows Server、OpenSSL)
- 您有來自CA的憑證檔案，用於簽署我們的CSR

兩個程式都會上傳憑證，並顯示進度指示，如下圖所示。



幾秒鐘後，FMC仍宣告需要ID證書：



上一個錯誤指出CA憑證與ID憑證中的頒發者資訊不相符，或是私鑰與FTD中預設產生的私鑰不相符。

解決方案

要使此證書註冊生效，您必須具有ID證書的相應金鑰。使用OpenSSL可產生PKCS12檔案。

步驟1。產生CSR (可選)

您可以使用稱為**CSR generator**(csrgenerator.com)的第三方工具取得CSR及其私密金鑰。

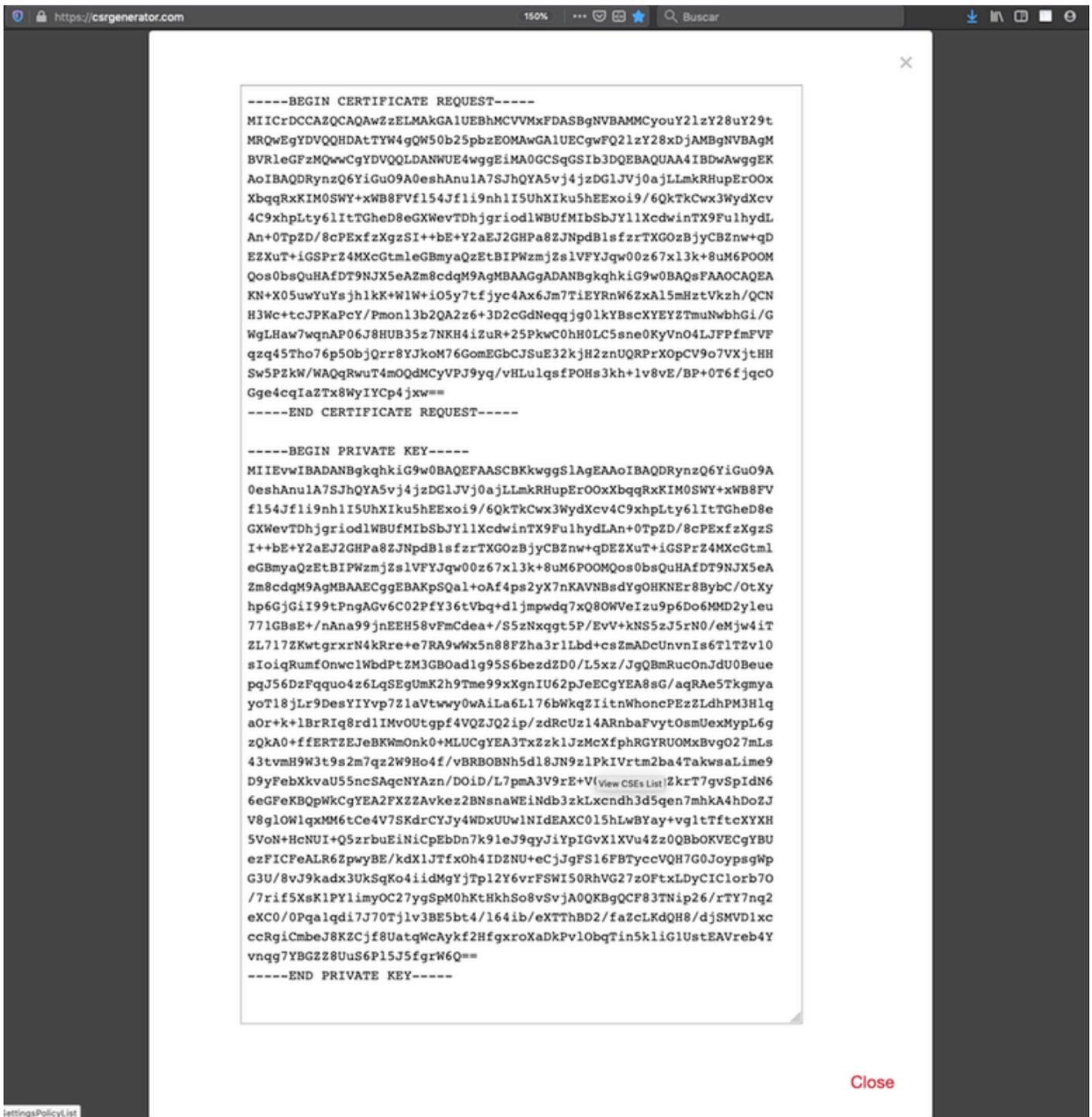
在相應填寫證書資訊後，選擇**生成CSR**選項。

Generate a Certificate Signing Request

Complete this form to generate a new CSR and private key.

Country	<input type="text" value="US"/>
State	<input type="text" value="Texas"/>
Locality	<input type="text" value="San Antonio"/>
Organization	<input type="text" value="Big Bob's Beepers"/>
Organizational Unit	<input type="text" value="Marketing"/>
Common Name	<input type="text" value="example.com"/>
Key Size	<input checked="" type="radio"/> 2048 <input type="radio"/> 4096 View CSEs List
<input type="button" value="Generate CSR"/>	

這提供了CSR +私鑰以便我們傳送到證書頒發機構：



步驟2. 簽署CSR

CSR需要由第三方CA(GoDaddy、DigiCert)簽署，一旦簽署CSR，便會提供一個zip檔案，其中包括：

- 身份證書
- CA套件組合（中間憑證+根憑證）

步驟3. 驗證並分離憑證

使用文字編輯器（例如記事本）驗證和分隔檔案。為私密金鑰(key.pem)、身分識別憑證(ID.pem)和CA憑證(CA.pem)建立具有可輕易識別名稱的檔案。

如果CA套件組合檔案具有超過2個憑證（1個根CA、1個子CA），則需要移除根CA，ID憑證發出者是子CA，因此，在此案例中與具有根CA無關。

名為CA.pem的檔案的內容：

```
-----BEGIN CERTIFICATE-----
MIIFojCCA4qgAwIBAgICEBQwDQYJKoZIhvcNAQELBQAwfjELMAkGA1UEBhMCTVgx
DTALBgNVBAGMBENETVgxEjAQBgNVBAoMCMVVuZ3UgQ29ycDEoMCMYGA1UECwwfVW5n
dSBDb3JwIENlcnRpbWljYXRlIEF1dGhvcml0eTEiMCAGA1UEAwwZVW5ndSBDb3Jw
IEludGVybWVkaWZ0ZSBDbQAEFw0yMDAyMjcwNjE1MjRaFw0yMTAzMDgwNjE1MjRa
MGcxZzAJBgNVBAYTA1VTMQ4wDAYDQQIDAVUZXRhczEUMBIGA1UEBwwLU2FuIEFu
dG9uaW8xZjAMBgNVBAoMBUNpc2NvMQwwCgYDQQQLDANWUE4xFDASBgNVBAMMCyou
Y2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsrPghHA3
7r/ShqU7Hj016muESBwmeDYTb0SBDz6T30E95T67Ey0ra8/sxyorCMzTHSPr6adF
o7xbrjm1onhneeJv+6sUbF1FnZnyNjrjAd/6u8BCJcXPdHESp4kvFGv8fuNAE01s
gjfuJ+Ap1iPbWUjsxs1CD1q208H/NyPn+mvu2Kvo1sJZ1s5VAak6D2FxSpwos4tV
sXUn71lymyArhDMQ0sGib8s8oOPqnBYPhy12+AWECqHTccMbsVxC3S11hHQMPci
LAEC/ijQeISM0xdR/p4CpjbunJTIQQw8CRqjSvkY2DGZs3s1Lo56RrHpRjdcukD5
zKGRlRkCt0jvyQIDAQABo4IBPzCCATswCQYDVR0TBAIwADARBg1ghkgBhvhCAQEE
BAMCBkAwMwYJYIZIAyB4QgENBCYWJE9wZW5TU0wgR2VuZXJhdGVkIFNlcnZ1ciBD
ZXJ0aWZ0Z2F0ZTAdBgNVHQ4EFgQUzED6CQ5u/wcK7y+GYz9ccDkrUigwgaEGA1Ud
IwSBMTCB1oAUT8MBVNLJSgdOEG3Gw+KnUvRMRCiheqR4MHYxCzAJBgNVBAYTAk1Y
MQ0wCwYDQQQIDARDRE1YMRiEAYDQQKDA1Vbmd1IENvcnAxKDAwBgNVBAsMH1VU
Z3UgQ29ycCBZDZXJ0aWZ0ZSBDbDxRob3JpdHkxGjAYBgNVBAMMEVVuZ3UgQ29y
cCBSb290IENBggIQADA0BgNVHQ8BAf8EBAMCBaAwEwYDVR01BAwwCgYIKwYBBQUH
AwEwDQYJKoZIhvcNAQELBQADggIBAJuAihWxJ44ug/vEhZaUapUtYSqKwzMLZbBr
un1IMsL8I8AhuWM93PPmHX2Tm2XwQ1o9PBN3aNacUz/FneZ/NNfQwC1GfJCTHJVE
K4+GWDNIeVznY7hbMppt5iJNuBMR/EoYoQ0xdqPtnLEqt92WgGjn6kvjVLw6eJKB
Ph75RDyr5DQz86Agnl/JzjvpeLR10eqMTCxgQJbY0eUrZCRNDwaV/ahpvmZ9xPV6
MB11a6GipT5EcFe16WPniqQa+3f+y8nsnsMDNE8UXW8nSqZwdTdA8THxkpogcPTb
isw8a9CkindzZhI6rtoCI0QXmqkw6uXPwCW5PnTT08TnSQoMjnc/Hvaa/tiiFA3F
dkaPLepgDScFZED2nPIFsXfb2zFRCN2YLirose/k9wc8rX1Z639uVCXN4yYmx9b
ADrqqQdkUXCGCGrQjXzWRNCORZihfTKg+ANoEaWgBsgInqtV5R/nsSkeibva9rBG
yHPukZB70Xz2AuINod70aPdIQCabEpVTcV5dr8+r9L1h5UQCIm+wPgBAQzG9Bz9
JM5RHriNhdmKQkvjDbqcKx8V3tjYpDNHgwAlwnaoICEoDKbSoildWgaPt4F1kipW
2RImd7X9wPetswGeOpI3q39mBtgQ1eAARXVB373il2WvxEwnjfBa9V4GAZcoMjpx
92xpoxS1
-----END CERTIFICATE-----
```

名為key.pem的檔案的內容：

```
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
MBQGCCqGSIB3DQMHBajnRV9YTIYsSwSCBMjqf1Lhs3v0RL0DHkvi7yvWSd3xWLMn
jt1hgOLsU1TDmBAWp/LXpqSP27c4XCQiZc0eiFDqm8aKw9xTDjgkEUBVactZs+Sz
yCE1gcG6NRH9lZFiwOYy+MCR4EPYh06DJPQ+MxLvtjjHrErruyXlAlywfAtrAcQk
E5tJniCaNTppwfVOfLpd/oHa2tF0kBMVVjS3HyxAXEfNThmzMwKRYgsLPUKShTfb
iv0bu8zI6fVfB4db3J/FjqikoiCHKXbWetm/GewZ071H3DW0HamtPw3InUuvYuzv
SM08x+Nji6uo7gtrQ6Rld2z5fN6vTtAw3x10AHjxm+vf0xt95zXhABYkMg2zHaQg
0djTHYFwdHwPdmSSNWM8hWnY8AvFxdjXURp/5MNP+v6ty5W/ETVe6o+Dh1sa9i7v
PzUwIDWs6kt0rxp0v8200lmqSKD6C4UnD1Vf2hH7AyMuwRpYamOEIuPtg8GgeiHJ
6vxpIJ3dY9/s0eyElkvKimZgiXpexBV/nDnksCLJTgyR08AE56iq2+XiBkwIoUai
QTZNi3S+PmPf8glHFtVKR8V6Zk4u8xov3reNTTmKXXcH3mHPaMU/Nhdldn8fpx+
phTzULmdtIpD3r1Hknh0uMvjrw0RYTLp1WGiEo5DU1SyI5jrMcyA0mhufOI7vtPp
rQqXNo6JleXuBteWSIHdqFynrtIdLyUVhK5QwF40m9+OvGkXNuqMDv4fH4+7nv9l
KqK2NS4yUXW1KjbaFe+Cxz9E7stt4Nyvwx56l/FpYlHymYDjQA3kFrC3tPHeULjT
fp95fJ+6g2R0nr4yKerHbV5BAai0V3rRVpBWhgzBK5o3w4+C+QIH6tgD1f2Jp9YA
TZLj/BDxIc40Q6AORATjWcbE1fvuNmNvMEQpDFM0gP8mlqnnBGzc5mwxC1xTNcQD
nmaFYykvWxYCzsvQAgwkvzyzzZw2mPNQpj3lVIOVRdZy8NWVkkCBLpq2XTSA6AQIK
mnJLY+rSAEi6miVnHeUW683un8KND9+HQ1YZbpKDK+JGcwkP/KhEHKmipEoHS8b5
MLby4tL7qrA3sfddMooJJYsCC372WYrd8xPrDZ9kYJ0N64ks9sYhvRUxRMJaxqaY
Int7b6p90i1r0LpielhUUrEvbuOCudM4sLDyXq8Fqf9G5u8dMuchCjXrEPGhmf4Y
ZhTfQF3xxQYtLBbLfwEQUft6GBsJMLGZFTFPM06/e3vToRu/Opw4Z9hrA6zBfQWa
bcT868DNME+UQxoT825SLwsFFPcjOpixn21FSm6baiq6QWvTV9+5797+AEPnG23i
1x/KKsvTEuwyHGgAX6p9Z0bfP0VcikMZk09MvMDU5MOUm01bnb0zINrrblG0qmRX
SYNNOL7lJ3joAKzv056KURWAMk9tQE8hAefWAZHS1PacwgUIWxOSAszRMkneptiR
VCm5UvzbYiMIA0rJjx6PTakuPIhdfokLyWfMI74ETao0Hl7KdDD1i/w11fAWFqtN
2gzfPw7Q02F7iZiYtxV9ryVBnH4wqut9pFjPYGu2oXC5q4Y7lJ1DrMzc879vAchM
C1dBcaJLWdpdTmrg2WNiao/rv3A20JjP0zA0eUwRo9r50S0oF9ez1ghBpAAtehyi
FGY=
-----END ENCRYPTED PRIVATE KEY-----
```

名為ID.pem的檔案的內容：

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

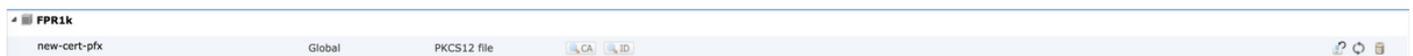
PKCS12 File*:

Passphrase:

Allow Overrides

驗證

若要確認憑證狀態以及CA和ID資訊，您可以選擇圖示並確認其已成功匯入：



選擇ID圖標：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。