

# FMC ىلع اهحالصإو ةداهشلا ءاطخأ فاشكتسأ

## تايوتحمل

[قمدملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ةلكشملا](#)

[لحلما](#)

[.pfx ةداهش ناكم ددح 1 ةوطخلما](#)

[.pfx فلم نم حاتفملا او تاداهشلا جارختسا 2 ةوطخلما](#)

[يصن برخم يف تاداهشلا نم ققحتلا 3 ةوطخلما](#)

[Notepad يف صاخال حاتفملا ةحص نم ققحتلا 4 ةوطخلما](#)

[قدصملا عجرملا ةداهش ميسقت 5 ةوطخلما](#)

[PKCS12 فلم يف تاداهشلا جمد 6 ةوطخلما](#)

[FMC يف PKCS12 فلم دروتسا 7 ةوطخلما](#)

[ةحصلما نم ققحتلا](#)

## ةمدقملا

ىلع اهحالصإو (CA) تاداهشلا عجرم داريئتسا ءاطخأ فاشكتسأ ةيفيكن دنتسملا اذه حضوي FMC اهريدت يتلا FirePOWER ديدهت نع عافدلا ةزهجأ.

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلتال عيضاوملاب ةفرعم كيذل نوكت نأب Cisco ي صوت:

- (PKI) ماعلا حاتفملا ةيساسألا ةينبلا
- Firepower (FMC) ةرادإ زكرم
- Firepower Threat Defense (FTD)
- OpenSSL

### ةمدختسملا تانوكملا

ةيلتال جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- MacOS X 10.14.6
- FMC 6.4
- OpenSSL

نيوكتب دنتسمل اذه يف تمذختسمل ازه جال اعيمج تادب. عصاخ ةيلمعم ةئيب يف ةدوجوملا ازه جال نم دنتسمل اذه يف ةدراولا تامولعمل اءاشن اذ مت رم أ يال لمدتعمل ريثأتلل كمهف نم دكأف، ةرشابم كفتكفبش تنك اذ. (يضارتفا) حوسمم

## ةيساسأ تامولعم

ءاشن اذ لبق CA ةداهش رفوت مزلي، FTD ةطساوب اهتراد اذ مت يتلا ازه جال يف: ةظالم (CSR) ةداهشل اعيقوت بلط

- ةقيرط نم دصقيف، (OpenSSL أو Windows Server لثم) يجراخ مداخل يف CSR ءاشن اذ مت اذ اذ بجي. يوديلا حاتفملا ليجست معددي ال FTD نال ارطن، لشفلا ةيوديلا ليجستلا لثم PKCS12 لثم فلتم بولسا مادختسا.

## ةلكشملا

يف حضورم وه امك CA ةداهش ةلاح يف رمحا ابلص FMC ضرعت، اديحت ويرانيسلا اذه يف ةلاسرع CA ةداهش تيبتت يف لشف ةداهشل ليجست نال اذ ريشي يذلاو، (ةروصل) لكشب ةداهشل مزح متي ال امدنع ماع لكشب أطخل اذه رهظي "CA ةداهش نيوكت يف لشف" يف حضورم وه امك ةححصلا ردصملا ةداهش لعل PKCS12 فلم يوتحي ال امدنع وأ ححص ةروصل.



Name	Domain	Enrollment Type	Status
wildcard-certificate-2020	Global	PKCS12 file	CA

ASA كولس ةقباطملا ةلكشملا هذه ةجلام مت، FMC نم ثدخال تارادصل يف: ةظالم يف نمضملا يرذجال قدصملا عجرملا عم ةيفاضا ةقت ةطقن ءاشن اذ اذ ريشي يذلاو، (ةروصل) ق. قدصملا عجرملا ةصاخلا ةقتلا ةلسلس

## لحل

1. ةوطخل .pfx ةداهش ناكم ددح.

FMC ل (GUI) ةيموسرلا مدختسمل ازه جال يف اهليلجست مت يتلا PFX ةداهش لعل لصح، Mac Terminal (CLI) يف فلملا عقوم ددحو اهظفحو

```
docs# ls -l
total 16
-rw-r--r-- 1 holguins staff 4701 May 23 15:11 cert.pfx
```

ls

2. ةوطخل .pfx فلم نم حاتفملاو تاداهشل جارختسا.

مت يتلا رورملا ةرابع) PFX فلم نم (CA تاداهش سيولو) ليمعلا ةداهش جارختساب مق (ةبولطم .pfx فلم ءاشن اذ اهمادختسا).

```
openssl pkcs12 -in cert.pfx -clcerts -nokeys -out id.pem
```

```
docs# openssl pkcs12 -in cert.pfx -clcerts -nokeys -out id.pem
Enter Import Password:
MAC verified OK
```

ةيوهال ري دصت

(لوميال تاداهش سيلو) CA تاداهش جارختسا

```
openssl pkcs12 -in cert.pfx -cacerts -nokeys -out certs.pem
```

```
docs# openssl pkcs12 -in cert.pfx -cacerts -nokeys -out certs.pem
Enter Import Password:
MAC verified OK
```

ت cacerts ري دصت

(2 ةوطخال نم رورملا ةرابع سفن بولطم) PFX فلم نم صخال حااتفملا جارختسا

```
openssl pkcs12 -in cert.pfx -nocerts -out key.pem
```

```
docs# openssl pkcs12 -in cert.pfx -nocerts -out key.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

يسيسئرلا ري دصتلا

ةداهش) id.pem، (CA تاداهش) certs.pem، (ةيلصلال PFX ةمزح) cert.pfx: تا فلم ةعبرأ نال دجوت  
(صخال حااتفملا) key.pem و، (لومي)

```
docs# ls -l
total 40
-rw-r--r-- 1 holguins staff 4701 May 23 15:11 cert.pfx
-rw-r--r-- 1 holguins staff 2301 Jun 10 01:34 certs.pem
-rw-r--r-- 1 holguins staff 2410 Jun 10 01:34 id.pem
-rw-r--r-- 1 holguins staff 1958 Jun 10 01:34 key.pem
docs#
```

ري دصتلا دع ب ls

يصن ررحم يف تاداهشلا نم ققحتلا 3 ةوطخال



```
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+6g2R0nr4yKerHbV5BAaiOV3rRVpBWhgzBK5o3w4+C+QIH6tgD1f2Jp9YA
TZLj/BDxIc40Q6AORATjWcbE1fvuNmNvMEQpDFM0gP8mlqnnBGzc5mwxC1xTNcQD
nmaFYykwVxYcZsvQAgwkvzyzZw2mPNQpj3lVIOVRdZy8NWVkkCBLpq2XTSA6AQIK
mnJLY+rSAEi6miVnHeUW683un8KND9+HQ1YZbpKDK+JGcwKp/KhEHKmiPEoHS8b5
MLby4tL7qrA3sfddMooJJYsCC372WYrd8xPrDZ9kYJ0N64ks9sYhvRUxRMJaxqaY
Int7b6p90i1r0LpielhUUrEvbu0CudM4sLDyXq8Fqf9G5u8dMuchCjXrEPGhmf4Y
ZhTfQF3xxQYtLBbLfWeQUft6GBsJMLGZFTFPM06/e3vToRu/Opw4Z9hrA6zBfQWa
bcT868DNME+UQxoT825SLwsFFPcj0pixn21FSm6baiq6QWvTV9+5797+AEPnG23i
1x/KKsvTEuwyHGgAX6p9Z0bfP0VcikMzk09MvMDU5MOUm01bnb0zINrrblG0qmRX
SYNNOL7lJ3joAKzv056KURWAMk9tQE8hAefWAZHS1PacwgUIWxOSAszRMkneptiR
VCm5UvzbYiMIA0rJjx6PTakuPIhdfokLyWfMI74ETao0H17KdDD1i/w11fAWFqtN
2gzfPw7Q02F7iZiYtxV9ryVBnH4wqut9pFjPYGu2oXC5q4Y7lJ1DrMzc879vAchM
C1dBcaJLWdpdTmrg2WNiao/rv3A20JjP0zAOeUwRo9r50S0oF9ez1ghBpAAtehyi
FGY=
-----END ENCRYPTED PRIVATE KEY-----
```

## قصدصم لاجرم لاداهش ميسقت 5. ةوطخلال

(يعرف قصدصم عجرم 1 و يرذج قصدصم عجرم 1) ني تاداهش يلع يوتحي certs.pem فلم ناك لاج ي ف، تاداهش لاداري تسا نم نكمتي يكل ةقثلا ةلسلس نم رذجال قصدصم لاجرم لادالا مزلي ضارغال ةلسلس لاي ف طقف يعرف لاداهش لاجرم لاداهش الكرات، FMC ي ف PFX قيسنتب ةحصلال نم ققحتلال.

جئاتن لاداهش ةداعاب يلات لاداهش موقيس، ةددعت مافلم ي ف certs.pem ميسقتب مق cacert-xx انا يلع

```
split -p "-----BEGIN CERTIFICATE-----" certs.pem cacert-
```

```
docs# split -p "-----BEGIN CERTIFICATE-----" certs.pem cacert-
docs#
```

```
docs# ls -l
total 56
-rw-r--r-- 1 holguins staff 219 Jun 10 01:46 cacert-aa
-rw-r--r-- 1 holguins staff 2082 Jun 10 01:46 cacert-ab
-rw-r--r-- 1 holguins staff 4701 May 23 15:11 cert.pfx
-rw-r--r-- 1 holguins staff 2301 Jun 10 01:34 certs.pem
-rw-r--r-- 1 holguins staff 2410 Jun 10 01:34 id.pem
-rw-r--r-- 1 holguins staff 1958 Jun 10 01:34 key.pem
docs#
```

ماسقنا دعب لصاوف

هاندأ حضوملا رمأل مادختساب ةديدل تافللملا هذه لىل pem. قحلم فضا

```
for i in cacert-*;do mv "$i" "$i.pem";done
```

```
docs# for i in cacert-*;do mv "$i" "$i.pem";done
docs#
```

يصلنل جم انربلا ةيمست ةداعل

يوتحي امهنم ياو، رذل قدصملا عجرملا لىل ع يوتحي امهنم يا دحو نيديدل ني فللملا عجار  
ع حضوملا رمأل مادختساب يعرفل قدصملا عجرملا لىل

(ةوهلا ةداهش وهو) id.pem فلم رصم نع شحبا، الوأ

```
openssl x509 -in id.pem -issuer -noout
```

```
docs# openssl x509 -in id.pem -issuer -noout
issuer= /C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Intermediate CA
```

ردصملا ضرع ةقيرط

(CA تاداهش) نيلصملا ني فللملا عوضوم نع شحبا، نأل

```
openssl x509 -in cacert-aa.pem -subject -noout
openssl x509 -in cacert-ab.pem -subject -noout
```

```
docs# openssl x509 -in cacert-ab.pem -subject -noout
subject= /C=MX/ST=CDMX/O=Ungu Corp/OU=Ungu Corp Certificate Authority/CN=Ungu Corp Intermediate CA
```

عوضوملا صحف

(ةقباسلا روصلال يف حضوم وه امك) id.pem فلم رصم عم عوضوملا قباطي يذل cacert فلم

PFX. ةداهش ءاشنإل اقحال همادختسإ متي يذلا يعرفلا قءصملا عجرملا وه

تناك ةلصحلا كلت ،ةلاحلا هذه يف .قباطملا عوضوملا هل سيل يذلا cacert فلم فذح  
cacert-aa.pem.

```
rm -f cacert-aa.pem
```

## PKCS12 فلم يف تاداهشلا جم د 6. ةوطخلا

(id.pem) فرعملا ةداهش عم (cacert-ab.pem مسالناك ،ةلاحلا هذهل) ةيعرفلا CA ةداهش جمدا  
رورم ةرابع مادختساب فلملا اذه ةيامح بجي .ديج PFX فلم يف (key.pem) صاخلا حاتفملاو  
كفلم ةقباطملا رمألا مزلا اذإ cacert-ab.pem فلم مساري يغتب مق

```
openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx
```

```
docs# openssl pkcs12 -export -in id.pem -certfile cacert-ab.pem -inkey key.pem -out new-cert.pfx  
Enter Export Password:  
Verifying - Enter Export Password:
```

PFX ءاشنإ

## FMC يف PKCS12 فلم دروتسا 7. ةوطخلا

حضوم وه امك بوغرملا ةيامحلا راجلإ صيخرتلا دروتساو تاداهش > ةادأىلإ لقتنا ،FMC يف  
ةروصلال يف .

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help

Device Management Device Upgrade NAT QoS Platform Settings FlexConfig **Certificates** VPN Troubleshoot 1 → Add

Name	Domain	Enrollment Type	Status
FTDv			🔒

**Add New Certificate** ? X

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:  ← 2

Cert Enrollment\*:  ← 3

Last login on Friday, 2023-06-09 at 16:50:08 PM from

ةداهشلا ليجست

ةديجال ةدحولل مسا چاردإ

## Add Cert Enrollment



Name\*

Description

**CA Information** Certificate Parameters Key Revocation

Enrollment Type:

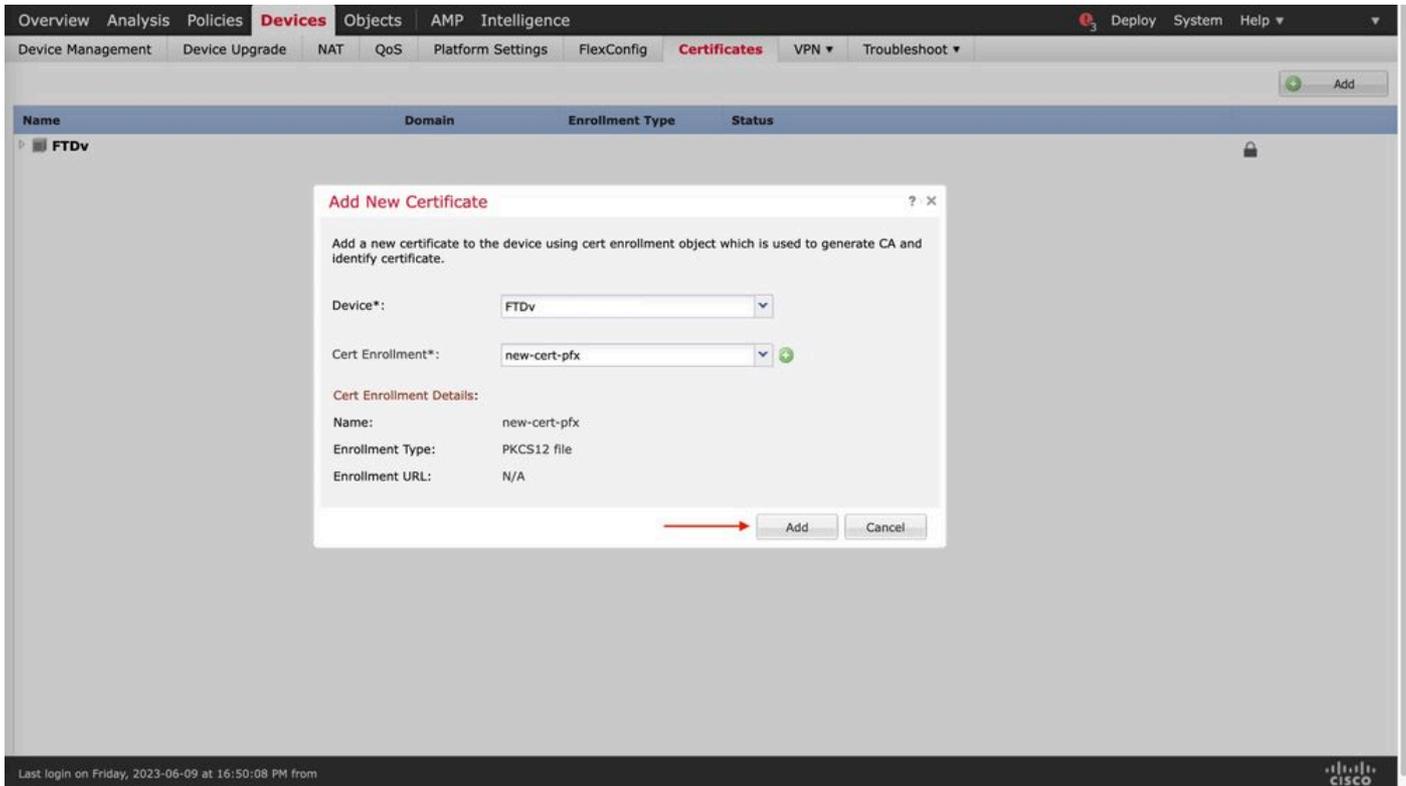
PKCS12 File\*:

Passphrase:

Allow Overrides

ليجستال

FTD. في ةديجال ةداهشال رشنل ليجستال ةيلمع رظتناو، ةديجال ةداهشال ةفاضاب مق



ةديج ةداهش

CA ل قح يف رمحأ بيلص ةمالع نودب ةيئرمة ةديجال ةداهشلا نوكت نأ بجي.

## ةحصلال نم ققحتلال

ححص لكش ب نيوكتلال لمع ديكأتل مسقلا اذه مدختسا

ةلماكلال ةلسلسلال ليغشتلال ماظن ضرعي شيح ةلكشم هجاوت نأ كنكمي في Windows، يوتحي يتلال ةلالال في ID ةداهش لىل طقف يوتحي pfx. فلم نأ نم مغرلا لىل ةداهشلل هنزخم في CA ةلسلسل subCA لىل اهيف.

وأ certutil لثم تاودأ مادختسا نكمي pfx. فلم في ةدوجوملا تاداهشلا ةمئاق نم ققحتلال openssl.

```
certutil -dump cert.pfx
```

اهلمكأب ةلسلسلال ىرت نأ بجي pfx. فلم في تاداهشلا ةمئاق رفوت رماوأ رطس ةادأ وه عجرملا (دجو نأ) نم ضم CA، SubCA، فرعمب.

هاندا رمالا في حضوم وه امك، OpenSSL رما مادختسا كنكمي، كلذ نم ال دب.

```
openssl pkcs12 -info -in cert.pfx
```

تانونقي ألادي دحت كنكمي، فرعمل او قدصم لاجرم ل تامول عم عم ةداهش ل ةلاح نم ققحت ل  
حاجنب اهداري ستا مت اهنأ نم دكأت ل او

Name	Domain	Enrollment Type	Status	
FPR1k				
wildcard-certificate-2020	Global	PKCS12 file	<span style="color: red;">X</span> CA   ID	  
new-cert-pfx	Global	PKCS12 file	CA   ID	  

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل