

لشف؛" اهحالصإو ةداهشللا ءاطخأ فاشكتسأ FMC ىلع ؛"CA ةداهش نيوكت

تايوتحمللا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ةلكشملا](#)

[لحللا](#)

[.pfx ةداهش ناكم ددح 1 ةوطخللا](#)

[.pfx فلم نمجاتفملا او تاداهشلا جارختسا 2 ةوطخللا](#)

[يصن برجم يف تاداهشلا نم ققحتلا 3 ةوطخللا](#)

[Notepad يف صاخلاجاتفملا ةحص نم ققحتلا 4 ةوطخللا](#)

[قدصملا عجرملا ةداهش ميسقت 5 ةوطخللا](#)

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

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

[ةحصلا نم ققحتلا](#)

ةمدقملا

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

ةيساسألا تابلطتملا

تابلطتملا

ةيالاتلا عيضاوملاب ةفرعم كيديل نوكت نأب Cisco يوصوت:

- (PKI) ماعلاجاتفملا ةيساسألا ةينبلا
- Firepower (FMC) ةرادا زكرم
- Firepower Threat Defense (FTD)
- OpenSSL

ةمدختسملا تانوكملا

ةيالاتلا جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- MacOS X 10.14.6

- FMC 6.4
- OpenSSL

نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال عيمج تادب. ةصاخ ةيلمعم ةئييب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراولا تامولعمل اءشن اذمت رمأ يال لمتمحمل ريتأتلل كعمف نم دكأنتف، قرشابم كفتكفبش تنك اذإ. (يضا ارتفا) حوسمم

ةيساسا تامولعم


 ةداهشلل عيقوت بلط ءاشن ا لبق CA ةداهش دوجو مزلي، FTD ةزهجال يف: ةظحالم

- ةقيرط نم دصقيف، (OpenSSL أو Windows Server لثم) يجرأ مءاخ يف CSR ءاشن ا مء اذإ بءي. يويءال ءاتفملا ليءست مءءي ال FTD نال ارطن، لشفلا ةيويءال ليءستلا لثم PKCS12 لثم فلءخم بولسا مءءءسا

ءلكشمل

يف ءضوم وه امك) CA ةداهش ءلاء يف رمءا ابيلص FMC ضرعت، دءملا ويءانيسلا اذه يف اءءال اذه رهظي. CA ةداهش ءيءء يف لشف ةداهشلل ليءست نال ريشي يءلاو، (ءروصلل لعل PKCS12 فلم يوءءي ال امءنء وأ ءيءص لكشب ةداهشلل مزء مءي ال امءنء ماع لكشب ةروصلل يف ءضوم وه امك ةءيءصلل رءصملا ةداهش

Name	Domain	Enrollment Type	Status
FPR1k wildcard-certificate-2020	Global	PKCS12 file	CA ID

 ASA كولس ءقباطملا ءلكشمل اذه ءءلام مء، FMC نم ءءءال ءاراءصلل يف: ةظحالم يف نمضملا يرءءال قءصملا ءءرملا عم ةيفاضا ءقء ءطقن ءاشن ا لعل يءوي يءلا قءصملا ءءرملا ءصءال ءقءال ءلسلس

لءل

.pfx ةداهش ناك مءء. 1 ءوطءال

FMC ل (GUI) ةيموسرلا مءءءسمل ا ءءاو يف اءل ليءست مء يءل PFX ةداهش لعل لصلءا، Mac Terminal (CLI) يف فلملا ءقوم دءو اءظفءاو

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

ls

.pfx فلم نم ءاتفملا وءاداهشلل ءارءءسا. 2 ءوطءال

مت يتي رورملا ةرابع) PFX فلم نم (CA تاداهش سي لو) لي معلقا ةداهش جارختساب مق (ةبولطم pfx. فلم ءاش نإل اهم ادختسا).

```
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
```

ةيوهلا ري دصت

(لي معلقا تاداهش سي لو) 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
```

cacerts ري دصت

(2 ةوطخلال نم رورملا ةرابع س فن بولطم) PFX فلم نم صاخالل حات فملا 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:
```

سي سي ئرلا ري دصتلا

ةداهش) id.pem، (CA تاداهش) certs.pem، (ةي لصلأل PFX ةمزح) cert.pfx: تافل م ةع برأ نأل دجوت (صاخالل حات فملا) key.pem و، (لي معلقا).

```
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#
```

رېډصت لال دعې ls

ي صرن ررحم ي ف تاداهش لال نم ققحت لال 3. ةوطخلال

(nano certs.pem، لال م لال لېس ىلع) ي صرن ررحم مادختساب تاداهش لال نم ققحت

ي عرف لال قدصم لال عجرم لال ىلع طوقف certs.pem ىوتح، صاخ لال ويرانېس لال اذهل ةبسن لال اب (رادص لال قدصم لال عجرم لال).

certs.pem ف ل م لال ه ي ف يوتحي ي ذل ويرانېس لال عارجا ةلاقم لال هذه لوانتت، 5 ةوطخلال نم ةي ادب (دحاو ي عرف قدصم عجرم دحاو ي رنج قدصم عجرم) ني تاداهش ىلع

```
Bag Attributes: <No Attributes>
subject=/C=MX/ST=CDMX/O=Ungu Corp Certificate Authority/CN=Ungu Corp Intermediate CA
issuer=/C=MX/ST=CDMX/O=Ungu Corp Certificate Authority/CN=Ungu Corp Root CA
-----BEGIN CERTIFICATE-----
MIIF0zCCA7ugAwIBAgICEAUwDQYJKoZIhvcNAQELBQAwdjELMAkGA1UEBhMCTVgx
DTALBgNVBAGMBENETVgxEjAQBgNVBAoMVCVvUzUgQ29ycDEoMCYGA1UECwwfVW5n
dSBDb3JwIENlcnRpZmljYXR1IEF1dGhvcml0eTEaMBGGA1UEAwwRVW5ndSBDb3Jw
IFJvb3QgQ0EwHhcNMjIwMDQ0WHcNMzIwMDQ0WjB+MQswCQYD
VQQGEWJNWDENMAsGA1UECAwEQ0RNdWESMBAGA1UECgwJVW5ndSBDb3JwMSgwJgYD
VQQGLDB9Vbmd1IENvcnAgQ2VydG1maWNhdGUgQXV0aG9yaXR5MSIwIAYDVQQDDb1V
bmd1IENvcnAgSW50ZXJtZWRRpYXR1IENBMTIICjANBgkqhkiG9w0BAQEFAAOCAg8A
MIICGKCAgEAt9zB5lbrhMTEEyGmRVRnuQ+mt86axF3QZEEsYCFv5gZs9R25cw+N
L7U9agbL/bNfvR00N8I8ywVahiTWJP9kuzGksEDaUzyHXybDs1YpHUNt0fYn5zFi
GGa81r90KmxSpsXeQB+GB0D8wezA1bAAGSKDiQymtBdQQMpnKTCmCRCjcPD1rBq1
Ewi0/7ePWhHK4KhtBBfSmjQxZyb1QIG5DBWCKA4q2D1ME9/o+pL944Utw+HMLrAH
4bT86kT7cYQVbeVSmoCastuN+1jux2aJ+4jT0GJM44yn0KzVANolGEjw/DPhW460
u9I1oJGMCh4j7Efl8bYvHTd+8yEejmHR+ASysy+8qoymWq3wIPiWJA0r160Hn2c
J0Zpu2oQQs+90+wBrzn/yV7aZmVdDbEJSXKHJkIGA7k5VWe/CvXbfExHSCfdZ5EV
uIx4AixdgwEdd0rgpHvYOGS1IHBmXNKoPp6s41oLmSmSr8lgZqm5mgdD1UKNA8tG
0jVrURiHLalHhyynoYHHVihEjhPrjNL9T26Dq9iAhX6yMCLIXB1QG/QUxef7AL07
nzIBASrYnAEv+TvgyKRE4Z9gVKxYhNLPxnVg0ycHiZbco2IcQzqIwDQAQs2LRWP
8eNuPd9l+5BgsSYgK3NxpZMXZwmMXgnGye3lueBUL9DSkuknx0aFVMCAwEAAAnj
MGEwHQYDVRO0BBYEFE/DAVTSyUoHThBtxlvip1L0TEQoMB8GA1UdIwQYMBaAFJMO
DF6TWO6EkboLkLC0t59z01QwMA8GA1UdEwEB/wQFMAMBAf8wDgYDVDR0PAQH/BAQD
AgGGA0GCSqGSIb3DQEBcWUAA4ICAQBUNUuk9jMTGmcP6j/tqBFM3Inhj/84ABMY
T4RBdtxi1v5HPjtknyEIP1B31QxrWi4pLiyh0ILb181mNxnawZD0Mvzv7Bsxepvx
xHrGhGac2y4yT72vGcIp/++8H2LatFaGAGePIssCjzTcLG9brubP/MXYJ3Mr1GXl
FbqvTdDJS5qB0+jRnMbACbv/nTUVXl6f6vb3AW2Zy0/u0+S6VoiB5Uk4xLZuhrwl
IXxSTghQWLqK4FBLj+XxyK2u+10iR3+6JGkkaIbb62zJsklnSJ+gVHgsMhEjATto
H0Zw5+uoJQy1/pa4uk0UaRPksIcH82p+4gPeCg5cEQAcI4niqJgIH0oPYJQszRwD
IB2w3nTAaNMtDyH6Ih/N/MvPiBhaYI3jynGEmJmansw8zcBPoek4bTsEx3hu7a/
kWddLmv2TscsfkGCL0XLOfcJLcW4R6QvsZaj3Ia0AsX/Lm0eYb7RnXfjPHenp3rA
a9IOLNe9/AyQrAqp3hQ4XSNs3zgScCja40ZcXiSgJcf1XIs8M12phT4bob89vY+u
xIawv6bXIteQ7P2RBUeJWPMFJC75JMp1RYsj2xogkneMiPpc9w5moZLxZpvznqgy
aCi37m1d+CT6hYTWxe3HztS03VJ+24IqEr+wmi+FB04VHZtqc/Bpajb0TpGBUGex
wxMFkoFWSA==
-----END CERTIFICATE-----
```

تاداهش لال ضرع ةقيرط


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

امت مصفون

```
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#
```

ماسقنالا دع ب ls

هاندأ حضومل رمال مادختساب ةديدل تافلما هذه لى 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#
```

يصنل جم انربلا ةيمست ةداع

يوتحي امهنم ي، رذل قدصملا عجرملا لىل ع يوتحي امهنم ي ددحو نيديدل ني فلما عجار
ةحضومل رمال مادختساب يعرفل قدصملا عجرملا لىل ع.

(ةيوهلا ةداهش وه) id.pem فلم رصم نع ثحبا، 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) ني لصفملا ني فلما عوضوم نع ثحبا، 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 روصولا يف حضورم وه امك) id.pem فلم ردصم عم عوضوملا قباطي يذلا cacert فلم
PFX ةداهش ءاشنإل اقحال همادختسا متي يذلا يعرفال قدصملا عجرملا وه

تناك ةلصلا كلت ،ةلاجل هذه يف .قباطملا عوضوملا هل سيل يذلا cacert فلم فذل
cacert-aa.pem.

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

PKCS12 فلم يف تاداهشلا جمد 6. ةوطخلال

(id.pem) فرعمل ةداهش عم (cacert-ab.pem مسالا ناك ،ةلاجل هذه) يعرفال CA ةداهش جمد
رورم ةرابع مادختساب فلملا اذه ةيامح بجي .ديج PFX فلم يف (key.pem) صاخال حاتفملاو
ك.فلم ةقباطملا رمألا مزلا اذإ cacert-ab.pem فلم مسار يفتب 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. ةوطخلال

حضورم وه امك بوغرملا ةيامحلا رادجلا صيخرتلا دروتساو تاداهش > ةادألا لقتنا ،FMC يف
ةوصولا 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 چاردا

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

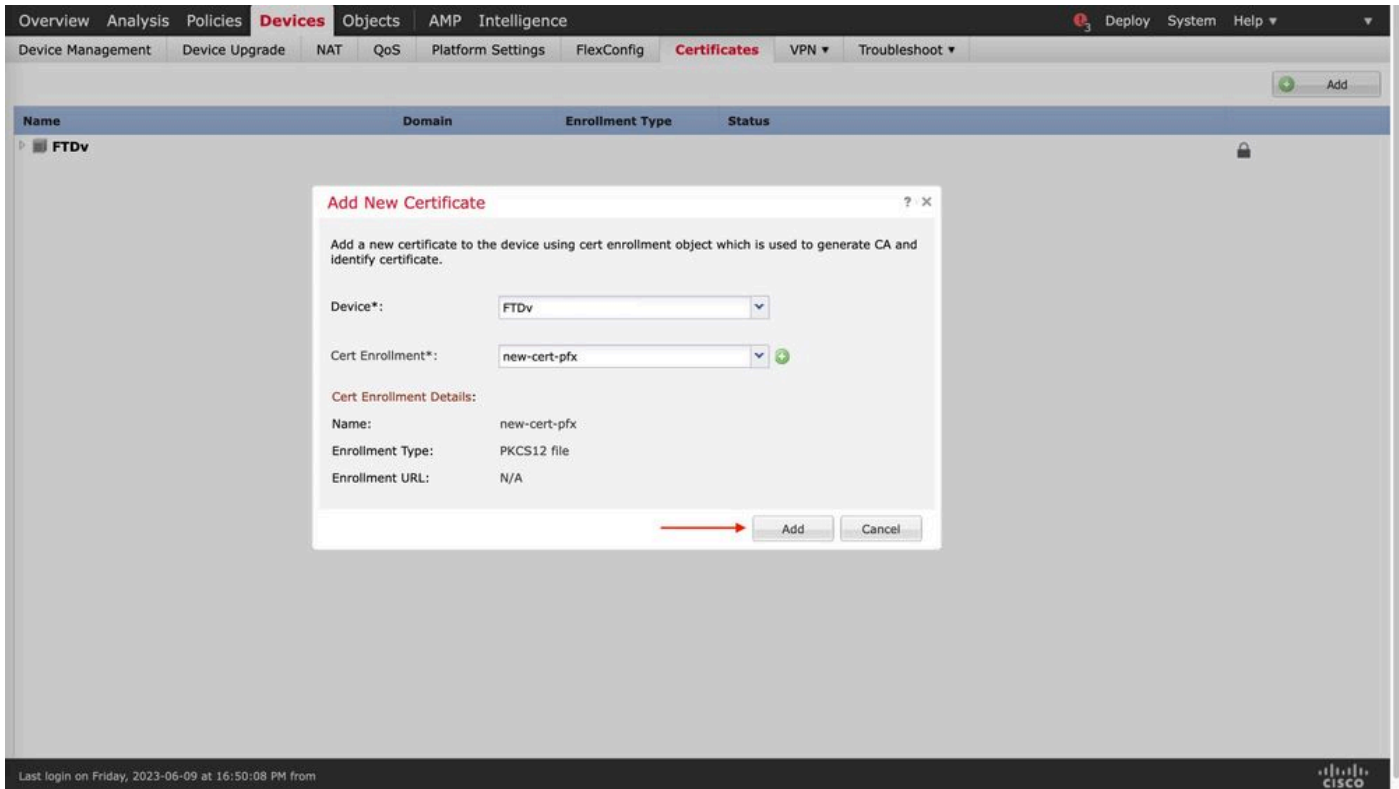
PKCS12 File*:

Passphrase:

Allow Overrides

ليجستال

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



ةديج ةداهش

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

ةحصلال نم ققحتلال

ححص لكش ب نيوكتل لمع ديكأتل مسقلا اذه مدختسا

ةلماكل ةلسلسلا ليغشتلا ماظن ضرعي شيح ةلكشم هجاوت نأ كنكمي في Windows، يوتحي يتلا ةلاحلا في ID ةداهش لىل طقف يوتحي pfx. فلم نأ نم مغرلا لىل ةداهشلل هـنـخـم في CA ةلسلس، subCA لىل اهيف

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







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

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

هاندا رمالا في حضورم وه امك، OpenSSL رما مادختسا كنكمي، كلذ نم الـب

```
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 ست امت انم دكأت ل او

Name	Domain	Enrollment Type	Status	
FPR1k				
wildcard-certificate-2020	Global	PKCS12 file	X 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 ةفارتحال ةمچرتل عم لاعل او
ىل إلمءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل ا دن تسمل