

نم ةرادم ال FTD ىلع تاداهش ال دي دجت و تي ب ث ت FMC لبق

تايوت حمل ال

[ةمدقم ال](#)

[ةيس اساس ال تابل طت ال](#)

[تابل طت ال](#)

[ةمدختت سمل تانوك ال](#)

[ةي فلخ ال](#)

[نيوك ال](#)

[ةداهش ال تي ب ث ت](#)

[ايتاذ عوقوم ال لي ج س ال](#)

[يودي ال لي ج س ال](#)

[PKCS12 لي ج س ت](#)

[ةداهش ال دي دجت](#)

[ايتاذ عوقوم ال ةداهش ال دي دجت](#)

[ةداهش ال ليودي ال دي دجت ال](#)

[PKCS12 دي دجت](#)

[OpenSSL مادختت ساب PKCS12 عاش ال](#)

[ةحص ال نم ق قحت ال](#)

[FMC يف ةت ب ث ت ال تاداهش ال ضرع](#)

[CLI يف ةت ب ث ت ال تاداهش ال ضرع](#)

[اهج الص او اعاطخ ال فاشك ت سا](#)

[جي حص ال بماو](#)

[ةعئ اش ال تالك شم ال](#)

ةمدقم ال

هتراد ا م ت فTD ىلع اه دي دجت و اه ق ي ث و تاداهش ال تي ب ث ت ةي ف ي ك دن ت س م ال اذه حض و ي
FMC ةط س ا و ب .

ةيس اساس ال تابل طت ال

تابل طت ال

ةي ل ال اع ي ض ا و م ل اب ة فر ع م ك ي دل ن و ك ت ن اب Cisco ي ص و ت :

- ةي ج ر ا خ ة ه ج ن م ة ق ت ق د ص م ع ج ر م ال ل و ص و ل ا ي و د ي ال ة د ا ه ش ال ل ي ج س ت ب ل ط ت ي .
- ر ص ح ال ال ل ا ث م ال ل ي ب س ى ل ع ، ةي ج ر ا خ ة ه ج ل ن ي ع ب ا ت ال CA ع ي ئ ا ب ة ل ث م ا ل م ش ت و Entrust ، ر ص ح ال ال ل ا ث م ال ل ي ب س ى ل ع ، ةي ج ر ا خ ة ه ج ل ن ي ع ب ا ت ال CA ع ي ئ ا ب ة ل ث م ا ل م ش ت و Geotrust و GoDaddy و Thawte و VeriSign .
- ةع اس ل ل ة ح ي ح ص ل ا ةي ن م ز ل ا ة ق ط ن م ل ا و خ ي ر ا ت ال و ت ق و ل ا ى ل ع ي و ت ح ي فTD ن ا ن م ق ق ح ت .

(NTP) ةكبشلا تقو لوكوتورب مداخ مادختساب ىصوي ،ةداهشلا ةقداصم مادختساب
FTD. ىلع تقولا ةنامل

ةمدختسمل تانوكمل

ةيلال ةيدامل تانوكمل او جماربل تارادصا ىل دننستسمل اذف ةدراول تامولعمل دننست

- FMCv 6.5 لىغشت
- FTDv 6.5 لىغشت
- OpenSSL مادختسا متي ، PKCS12 ءاشنال

ةصاخ ةيلمعم ةئيب يف ةدوجومل ةزهجال نم دننستسمل اذف ةدراول تامولعمل ءاشنال مت
تناك اذف. (يضارتفا) حوسمم نيوكتب دننستسمل اذف ةمدختسمل ةزهجال ءيمج تادب
رما ىل لمحتحمل ريثاتلل كمهف نم دكاتف ، لىغشتلا دي قكتكبش

ةيفلخال

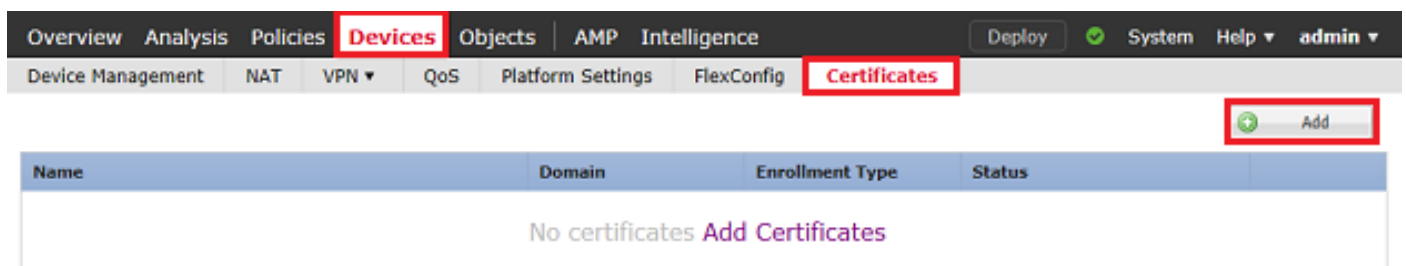
تاداهشلا و (CA) ايتاذ ةعقومل تاداهشلا و تاداهشلا تيبتت ةيفي دننستسمل اذف حضوي
ديدهت دض ةيامح" ىلع (CA) ىلخاد قدصم ءجرم و (CA) ىجراخ قدصم ءجرم لبق نم ةعقومل
FirePOWER (FMC) ةرادا زكرم اهردي ىتل " (FTD) ةيرانلا ةقاول

نيوكتل

ةداهشلا تيبتت

ايتاذ ةقومل لىجستلا

1. ةروصل يف حضوم وه امك ةفاضل قوف رقنا م ، تاداهشلا > ةزهجال ىل لقتنا .



2. رضال زمرلا رقنا م . *زاهجال ةلدسنملا ةمئاقلا يف هىل ةداهشلا ةفاضل متتوزاهجال دح .
+ ةروصل يف حضوم وه امك

Add New Certificate

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

Device*:

Cert Enrollment*:

3. داهش :ليجستلا عون دح ، CA تامولعم بيوبتلا عمال ع تحت و لاصلتالا ةطقنل مسا دح . ةروصلال يف حضورم وه امك ايتاذا ةعقوم .


Add Cert Enrollment

Name*:

Description:

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type:

 Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.

Allow Overrides

4. عم اذه قباطتي نا بجي . داهشلل اماع امسا لخدأ ، داهشلا تامولعم بيوبتلا عمال ع تحت .

يفترضون وه امك اهلجأ نم ةداهشلا مادختسا متي يتلا ةمدخلاب صاخلا IP ناونع وأ FQDN ةروصل.

Add Cert Enrollment



Name*	FTD-1-Self-Signed
Description	
CA Information Certificate Parameters Key Revocation	
Include FQDN:	Use Device Hostname as FQDN
Include Device's IP Address:	
Common Name (CN):	ftd1.example.com
Organization Unit (OU):	Cisco Systems
Organization (O):	TAC
Locality (L):	
State (ST):	
Country Code (C):	Comma separated country codes
Email (E):	
<input type="checkbox"/> Include Device's Serial Number	
Allow Overrides	<input type="checkbox"/>
Save Cancel	

مدختسما صاخلا حاتفملا عون ديدحت نكمي، حاتفملا بيوبتلا ةمالع تحت (يراي تخا). 5. RSA حاتفم حاتفملا مدختسي، يضارتفا لكش ب. همجحو همساو ةداهشلا نومدختسي ال شيحب، ةداهش لك ديفر مسا مادختساب يصوي، كلذ عمو؛ 2048 مجحو <Default-RSA-Key> ةروصل يف حضورم وه امك ماعلا/صاخلا حاتفملا جوز سفن.

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters **Key** Revocation

Key Type: RSA ECDSA

Key Name:*

Key Size:

Advanced Settings

Ignore IPsec Key Usage
Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.

Allow Overrides

Save Cancel

6. ةروصل ايف حضورم وه امك ةفاض ا قوف رقنا م طفح قوف رقنا ،ءاهت اال درجم ب.

Add New Certificate

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

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: FTD-1-Self-Signed

Enrollment Type: Self-Signed

SCEP URL: NA

7. ةروصلال ي ف ايتاذ ةعقومال ةداهشال ضرع م تي ،اهلامتك ا درجم ب .

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA ID

يوديال ليحستال

1. ةروصلال ي ف حضوم وه امك ةفاضل قوف رقنا م ت اداهشال > ةزهأل ال ل قتنا .

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

2. قوف رقنا م ت *زاهال ةلدسنمال ةمئالال ي ف هيال ةداهشال ةفاضل م تي ذل زاهال دح .
 ةروصلال ي ف حضوم وه امك رضأل + زمرال

Add New Certificate



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

Device*:

FTD-1

Cert Enrollment*:

Select a certificate enrollment object

Add

Cancel

3. ليلدلا: ليجستلا عون دح، CA تامولعم بيوبتلا عمال ع تحت و لاصلتالا ةطقنل مسادح. مل اذا. ةيوهلا ةداهش عيقوتل اهمادختسا متي يتلا CA ب ةصاخلا PEM قيسنت ةداهش لخدأ عضومك CA ةداهش يا ةفاضاب مقف، تقولا اذه يف ةفورعم وأ ةرفوتم ةداهشلا هذه نكت وه امك يلصلأا قدصملا عجرملا ةفاضال ةوطخال هذه ررك، ةيوهلا ةداهش رادصا درجمبو، تقوم ةروصلال يف حضورم.

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*
-----BEGIN CERTIFICATE-----
MIIESzCCAjOgAwIBAgIIItsWeBSsr5QwDQYJKoZIhvcNAQELBQAw
MjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUxkFDASBgNVBAMTC1ZQTiBSb29
OIEBMB4XDTEw
MDQwNTIzMjkwMFoXDTEwMDQwNTIzMjkwMFowOjEaMBgGA1UE
ChMRQ2lzY28gU3lz
dGVtcyBUQUxkHDAaBgNVBAMTE1ZQTiBjb3Rlcm1lZGhhdGUgQ0E
wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDII/m7uyjRUoyjyob7sWS
AUVmnUMtovHen
9VbgjowZs0hVcig/Lp2YYuawWRJhW99nagUBYtMyvY744sRw7AK
AwlyROO1J6IT
Is5suK60Yryz7JG3eNDqAroqJg/VeDeAjprpCW0YhHHYXAI0s7GXjHI
S6nGIy/qP
SRcPLdqx4/aFXw+DONJYHLoE5FlsfknrOeketnbABjkAkmOauNpS
zN4FAISIk4
DU3yX7d31GD4BBhxI7IPsDH933AUm6zxntC9AxK6gHAY8/8pUPv

Allow Overrides

Save Cancel

4. عم اذه قباطتي نأ بجي .ةداهشلل اماع امسا لخدا ،ةداهشلا تاملعم بيوبتلا ةمالع تحت
في حضورم وه امك اهلجأ نم ةداهشلا مادختسا متي يتلا ةمدخلاب صاخلا IP ناوع وأ FQDN
ةروصلا.

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

Save Cancel

5. مدختسملا صاخلا حاتفملا عون ديدحت نكمي، حاتفم بيوبتلا عمال ع تحت (يرايتخا) مساب RSA حاتفم حاتفملا مدختسي، يضارتفا لكش ب. ايرايتخا همجحو همساو عدهشلل ال يتح عدهاش لكل ديرف مسا مادختساب ي صوي، كلذ عمو؛ 2048 مچحو <Default-RSA-Key> عروصلال يف حضورم وه امك ماعلا/صاخلا حاتفم جوز سفن مدختست.

Add Cert Enrollment

? X

Name*

Description

CA Information Certificate Parameters **Key** Revocation

Key Type: RSA ECDSA

Key Name:*

Key Size:

Advanced Settings

Ignore IPsec Key Usage
Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.

Allow Overrides

Save Cancel

6. (CRL) ةداهشلا اءاغلا ةمئاق لاطبإ نم ققحتلا متي، لاطبإلا بيوبتلا ةمالع تحت (يراي تخإ).
يضارتفا لكشب .هنيوكت نكميو (OCSP) تنرتنإلا ربع ةداهشلا ةلاح لوكوتورب لاطبإ وأ
ةروصلال يف حضوم وه امك امهنم يا ريشأت متي ال

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key **Revocation**

Enable Certificate Revocation Lists (CRL)

Use CRL distribution point from the certificate

User static URL configured

CRL Server URLs:*

Enable Online Certificate Status Protocol (OCSP)

OCSP Server URL:

Consider the certificate valid if revocation information can not be reached

Allow Overrides

Save Cancel

7. ةروصلال ي ف حضورم وه امك ةفاضل قوف رقنا م ث ظفح قوف رقنا ،ءاهتالال درجم ب .

Add New Certificate

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

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: FTD-1-Manual

Enrollment Type: Manual

SCEP URL: NA

8. في حضوره وه امك ةي وه ل رز رقنا .ةي وه ةداهش ةفاضل را يخ FMC مدقت ،ب لطلال ةجل ام دع ب .ةروصل

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Manual	Global	Manual	CA ID Identity certificate import required

9. ةروصل في حضوره وه امك معن ل ع رقنا .تقلخ CSR نأ ملعي راطل رهظي .

Warning



This operation will generate Certificate Signing Request do you want to continue?

Yes

No

10. م تي ، CSR عي قوت درجم ب . CA ل اهل اسرا و اخ سن نكمي ي تال CSR ءاشن م تي ، كلذ دع ب . وه امك داريتس ل ع رقنا م ث ، اهدحو ةرفوت مل ةي وه ل ةداهش ل حفصت . ةي وه ةداهش ريفوت

ةروصلال ي ف حضوم.

Import Identity Certificate

Step 1
Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICzzCCAbcCAQAwVzEZMBcGA1UEAxMQZnRkMSSleGFtcGxlMnVbTEMMAoGA1UE  
ChMDVEFDMRyYwFAYDVQQLEw1DaXNjbyBTeXN0ZW1zMRRQwEgYjKoZihvcNAQkCFgVm  
dGQMTCCASlWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAlouU/93hqjgSLu  
UpXTM3O68CWNB8ZSkAYvOnjinJE2+onWfGJe+fEicSEdJxN4T1Cs09aIFH24P39  
V4PbDyclaQCuafOoTCF/ylxrQzSot7TozYXnSCHH9Xk+8NGZoinnxUcdljuK86Se  
uYue2/3ekrXet4GUGzcGok9mJnRuXJI32cALL/Nv1F6OmpKj3kPskejYBkL2VdmC  
k8bKI2+xd+TDRAyNpMK+wBmj8CTZSux8rcBgGeHMDj1R7G/x4nfGIYP2xM4bgmy+  
cho8cZgjRIahv5wg0Q4Eft05+oVicXj3LkuhH41az5UPkWS5ZtoQvyR3HP5VMmxa  
FUIJwKCaYFAA+4MBECCeCFtk3DGF3pck1MCTyDexYUg994QUUBAQAQoUwMBAQ
```

Step 2
Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:

ةروصلال ي ف امك رهظت، ةيوديلا ةداهشلال امكك ا درجم 11.

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

Access Control Network Discovery Application Detectors Correlation Actions

+ Add

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Manual	Global	Manual	CA ID

كجست PKCS12 لي

1. رقنا م تاداهشلال > ةزهجال ا ل لقتنا، أشنم واملتسم PKCS12 فلم تيبت ل ج أ نم ةروصلال ي ف حضوم وه امك ةفاضل.

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

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

+ Add

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

2. قوف رقنا م * زاهجال ةلدسنملا ةمئاقلا ي ف هيلا ةداهشلال ةفاضل م ت ي ذلا زاهجال دح ةروصلال ي ف حضوم وه امك رضخال + زمرلا.

Add New Certificate



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

Device*:

FTD-1

Cert Enrollment*:

Select a certificate enrollment object

Add

Cancel

3. فلم: ليجستال عون، CA تامولعم بيوبتال عمال ع تحت و لاصلتال اطقنل مسادح. دن ع مدختسمل رورملا زمر لخدأ. هددحو هؤاشنإ مت يذلا PKCS12 فلم ىلإ حفصت. ةروصلال ي ف حضوم وه امك PKCS12 ءاشنإ

Add Cert Enrollment



Name*

FTD-1-PKCS12

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

PKCS12 File

PKCS12 File*:

PKCS12File.pfx

Browse PKCS12 File

Passphrase:

Allow Overrides

Save

Cancel

4. هذه إضافة جراح لـ في حيث أفعل أو أدهش لـ تام لعم بيوبت تام ال ع عضو متي (يراي تخا).
ة مال ع ليدت نكمي، كلذ عم و، PKCS12 مادختساب ل ع فلأب اهؤاشنإ مت بيوبت تام ال ع
متي ال، يضارتفا لكش ب. OCSP لاطبإ نم ققحتلأ وأ/و CRL نيكمتل لاطبإ بيوبت لـ
ة روصلأ في حضورم وه امك امه نم يا ريشأت.

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key **Revocation**

Enable Certificate Revocation Lists (CRL)

Use CRL distribution point from the certificate

User static URL configured

CRL Server URLs:*

Enable Online Certificate Status Protocol (OCSP)

OCSP Server URL:

Consider the certificate valid if revocation information can not be reached

Allow Overrides

Save Cancel

5. في حضورم وه امك راطلأ اذه ل ع فاضا قوف رقنا م ث ظفح قوف رقنا، اءاتنالا درجم ب.
ة روصلأ.

Add New Certificate

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

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: FTD-1-PKCS12

Enrollment Type: PKCS12 file

SCEP URL: NA

Add **Cancel**

6. ةروصلال ي ف حضورم وه امك رهظت ، PKCS12 ةداهشلال لامتك درجم ب .

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID

ةداهشلال دي دجت

ايتاذ عقوملال ةداهشلال دي دجت

1. ةروصلال ي ف حضورم وه امك ةداهشلال ليجست ةداع رز طغضا .

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Self-Signed	Global	Self-Signed	CA ID

2. ي ف حضورم وه امك معن ىل ع رقنا . اهلادبتساوا ايتاذ عقوملال ةداهشلال ةلازاب ةذفان كبلاطت . ةروصلال .

Warning



Re-enrolling the certificate will clear the existing certificate from the device and install the certificate again.

Are you sure, you want to re-enroll the certificate?

Yes

No

3. قوف رقننلا دنع ءارجإلا اذه نم ققحتللا نكمي. FTD ىلإ ددجتمللا يتاذللا عيقوتلا عفدم تي.
ححصلا تقولا ديدحتو فرعم رزلا

ةداهشلل يوديلا ديدجتلا

1. ةروصللا يف حضورم وه امك ةداهشلا ليجست ةداعإ رز طغضا.

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-Manual	Global	Manual	CA ID

2. ةروصللا يف حضورم وه امك معن ىلع رقنا. ةداهش عيقوت بلط ءاشنإب ةذفان كبلاطت.

Warning

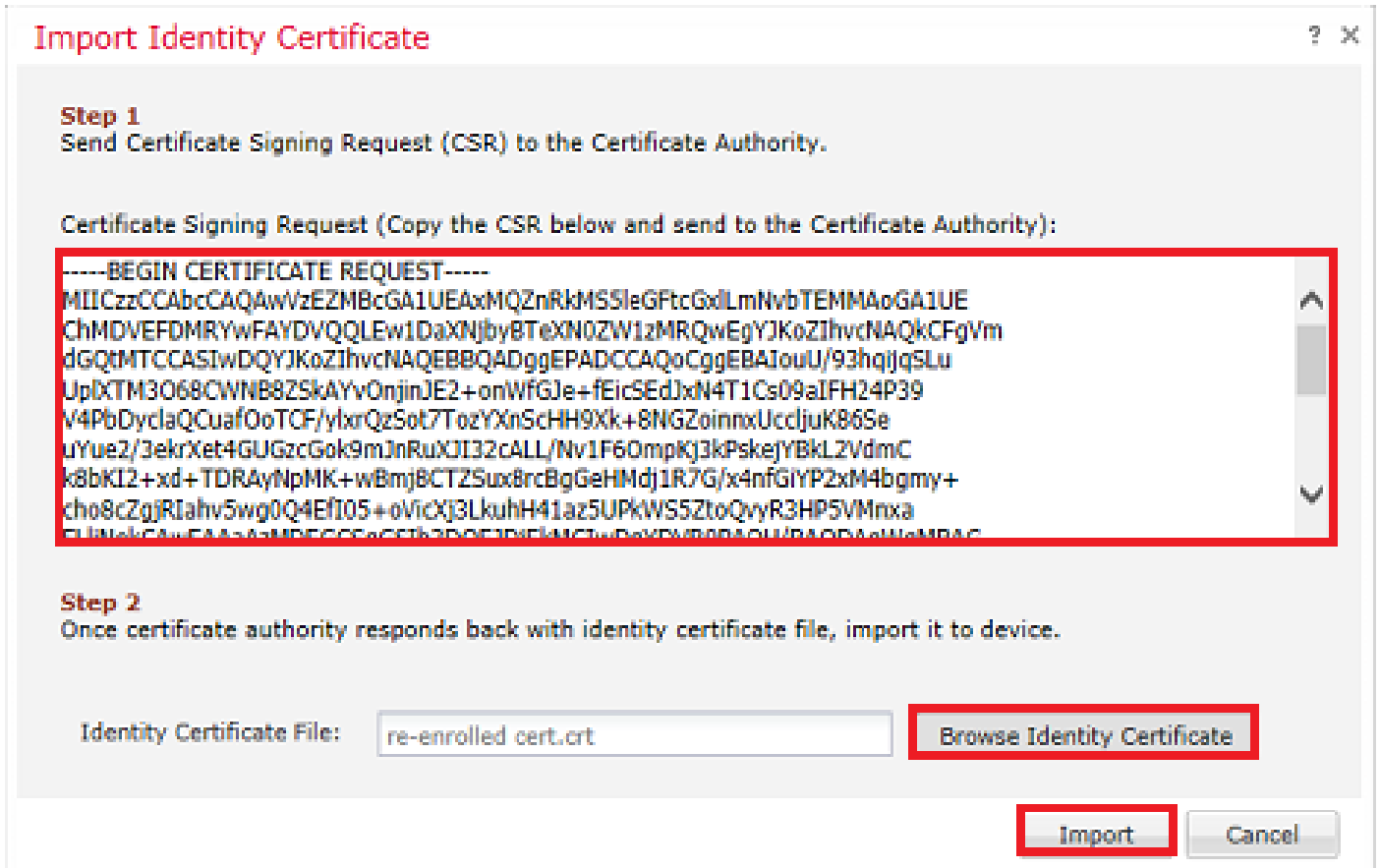


This operation will generate Certificate Signing Request do you want to continue?

Yes

No

3. ةداهش عيقوتلا ذللا CA هسفنلا ىلإ هلاسراو هخسن نكمي CSR ءاشنإم تي، راطإلا اذه يف.
ةداهش ىلإ حفصت. ةددجتمللا ةداهش ريفوتم تي، CSR عيقوت درجمب. اقباس ةيوهلا
ةروصللا يف حضورم وه امك داريستسا ىلع رقنا م، اهدحو ةرفوتمللا ةيوهلا



4. زللا قوف رقلل دنع ءارجلال اذه نم ققحتللا نكمي. FTD ىلإ ةددم ةيودي ةداهش عفد متي .
 جححصلا تقوللا ديدحتو فرعم

ديجت PKCS12

مزللي، PKCS12 ديدجتل . ةداهشلا دجت ال اهنإف ، ةداهشلا ليجست ةداعل رز قوف ترقلن اذإ
 اقباس ةروكذملل بيلالسال مادختساب هلي محتو ديدج PKCS12 فلم عاشنإ

OpenSSL مادختساب PKCS12 عاشنإ

ةداهشلا عي قوت بلطو صاخ حاتفم عاشنإب مق ، لثامم قيبطت وأ OpenSSL مادختساب .
 (CSR) ftd1.csr م سباب و private.key م سباب تب 2048 رادصل RSA حاتفم لاثملا اذه حضوي .
 OpenSSL ي هؤاشنإ متي يذلا :

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd1.csr
Generating a 2048 bit RSA private key
.....+++
.....+++
written to a new private key to 'private.key'
-----
You are about to be asked to enter information that is incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', the field is left blank.
-----
```

Country Name (2 letter code) [AU]:.
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd1.example.com
Email Address []:.

Please enter these 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

2. ةيوه ةداهش ريفوت م تي، CSR عيقوت درجمب CA. لىل هل اسراو هؤاشن| مت يذلا CSR خسنا. رماً اذه نم دحاو، PKCS12 تقلخ in order to تلخد. كلكذك CA (تاداهش) ةداهش ريفوت م تي ام ةداعو يف OpenSSL:

رماً اذه مدختساً، طقف PKCS12 نمض ةرداصلال CA ةداهش ني مضت ل

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -certfile ca.crt  
Enter Export Password: *****  
Verifying - Enter Export Password: *****
```

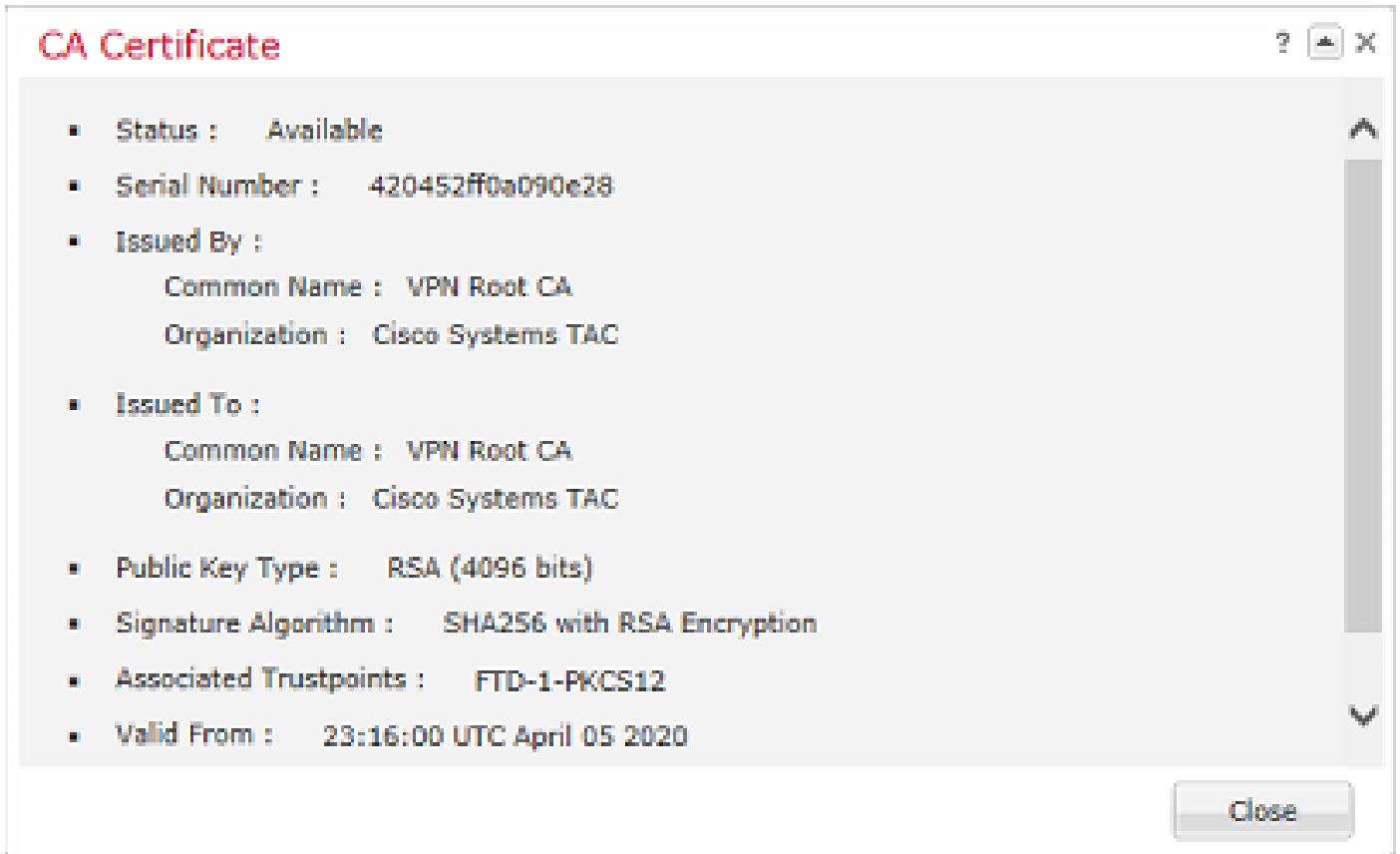
- ftd.pfx وه م سا و OpenSSL ةطساوب هري دصت م تي يذلا (der قي سنن ت ب) PKCS12 فلم م سا وه
- ftd.crt وه م سا و PEM قي سنن ت ب قدصم ل ا عجرم ل ا هردصي ي ت ل ا ةعقوم ل ا ةي وه ل ا ةداهش م سا وه
- private.key وه م سا و 1. ةوطخلال ي ف هؤاشن| مت يذلا حيتافم ل ا جوز وه
- CA.CRT وه م سا و PEM قي سنن ت ب ةردصم ل ا قدصم ل ا عجرم ل ا ةداهش وه

، ةطيسو ةقدصم عجارم نم رثكاً و 1 و ي رذج قدصم عجرم تا ذة لس لس نم اعزج ةداهش ل ا تناك اذا PKCS12: ي ف ةلمالكال ةلس لس ل ا ةفاضل رماً اذه مادختس| نكم ي

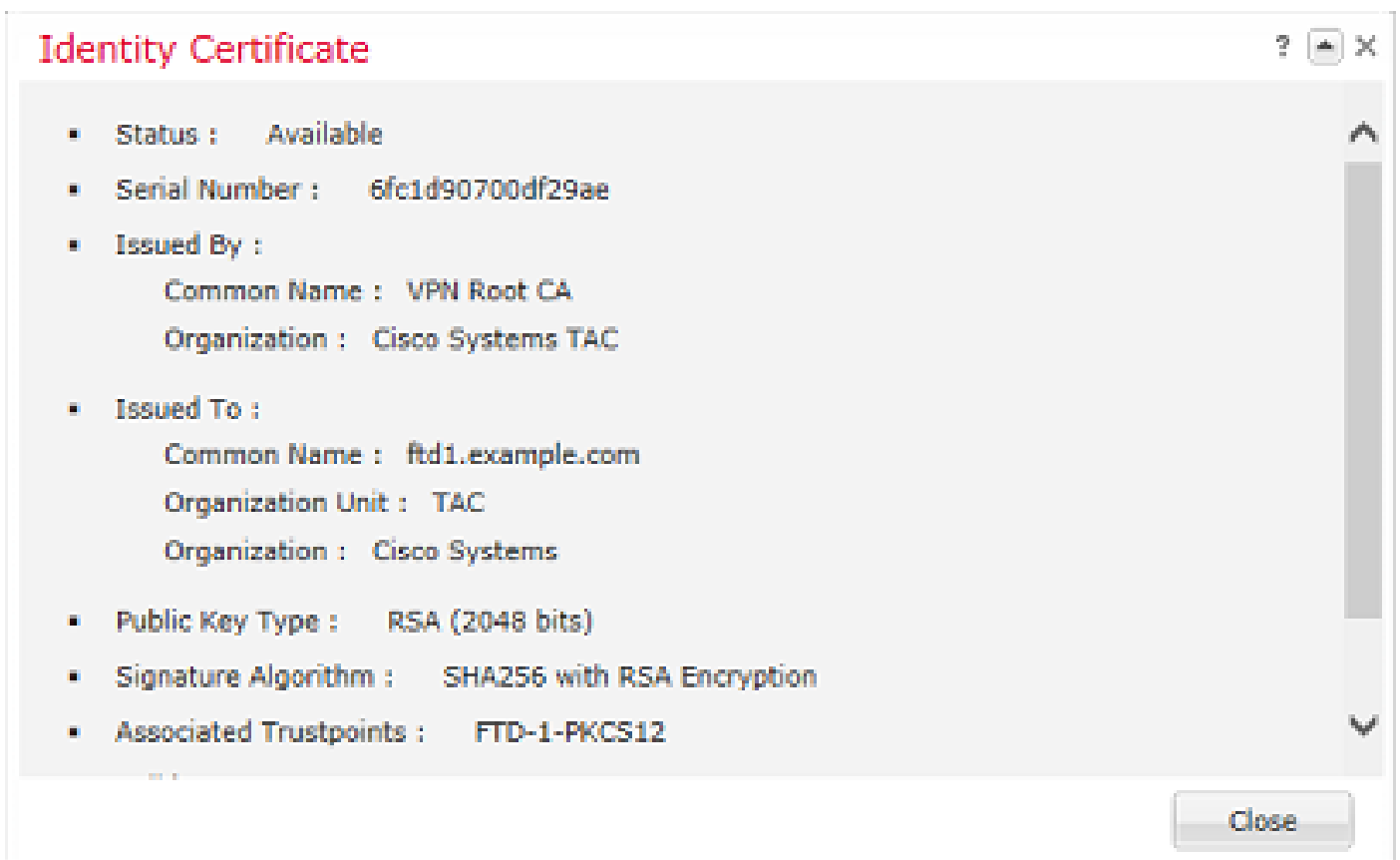
```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -chain -CAfile cachain.pem  
Enter Export Password: *****  
Verifying - Enter Export Password: *****
```

- ftd.pfx وه م سا و OpenSSL ةطساوب هري دصت م تي يذلا (der قي سنن ت ب) PKCS12 فلم م سا وه
- ftd.crt وه م سا و PEM قي سنن ت ب قدصم ل ا عجرم ل ا هردصي ي ت ل ا ةعقوم ل ا ةي وه ل ا ةداهش م سا وه
- private.key وه م سا و 1. ةوطخلال ي ف هؤاشن| مت يذلا حيتافم ل ا جوز وه
- cachain.pem وه م سا و CA رادصلاب أدبت ي ت ل ا ةلس لس ل ا ي ف CA تاداهش ل ا ع يوتحي فلم وه PEM قي سنن ت ب ي ف CA رذل ل ا ب ي هتنت و طيسول

PKCS12 ل ا قلخي نأ تلمعتسا تنك اضيأ عي طتسي رماً اذه، (p7b، p7c). دربم PKCS7 تعجرن| موقت ال ال او، تا طيسول ل ا تامول عم ردصم ةفاضل نم دكأتف، der قي سنن ت ي ف p7b ناك اذا: اهني مضت ب



قروصلال ي ف حضوم وه امك ةي وهلا ةداهش نم ققحت



CLL ف ةت بثلما تاداهشلا ضرع

SSH لى FTD اؤ لخد اؤ show crypto ca certificate.

```
> show crypto ca certificates
```

Certificate

```
Status: Available
Certificate Serial Number: 6fc1d90700df29ae
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
  cn=VPN Root CA
  o=Cisco Systems TAC
Subject Name:
  cn=ftd1.example.com
  ou=TAC
  o=Cisco Systems
Validity Date:
  start date: 15:47:00 UTC Apr 8 2020
  end date: 15:47:00 UTC Apr 8 2021
Storage: config
Associated Trustpoints: FTD-1-PKCS12
```

CA Certificate

```
Status: Available
Certificate Serial Number: 420452ff0a090e28
Certificate Usage: General Purpose
Public Key Type: RSA (4096 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
  cn=VPN Root CA
  o=Cisco Systems TAC
Subject Name:
  cn=VPN Root CA
  o=Cisco Systems TAC
Validity Date:
  start date: 23:16:00 UTC Apr 5 2020
  end date: 23:16:00 UTC Apr 5 2030
Storage: config
Associated Trustpoints: FTD-1-PKCS12
```

اه حال ص اؤ اءاط خ اؤ فاش ك ت سا

اه حال ص اؤ نيوك ت ل اءاط خ اؤ فاش ك ت سا ال اهم اد خ ت سا كن كم ي تام ول عم م س ق ل ا ذه رفوي

ح ي ح ص ت ل ا رم اؤ اؤ

رب ع FTD ل ي ص و ت د ع ب ة ي ص ي خ ش ت ل ا رم اؤ اؤ ر ط س ة ه ج اؤ ن م اءاط خ اؤ ح ي ح ص ت ل ي غ ش ت ن كم ي SSL: ة داه ش ت ي ب ت ل ش ف ة ل ا ح ي ف SSH

```
debug crypto ca 14
```

فاش ك ت سا ال ا ه ب ي ص و ي و ه ذه اءاط خ اؤ ح ي ح ص ت ت ا ي ل م ع رف و ت ت ، FTD ن م م د ق اؤ ا ت ا ر ا د ص اؤ ا ي ف ا ه حال ص اؤ اءاط خ اؤ ا

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 255

ةعئاشللال تالكلشمل

ةداهش داريتسإ دعب "بولطم ةيوهال ةداهش داريتسإ" ةلاسرللا ةداهشم لكانكمإب لازي ال ةرداصلال ةيوهال.

نيتلصفنم نيتلكشم ببسب اذه ثدحي دق:

1. يوديلا ليجستللا دنع ةرداصلال قدصملا عجرملا ةداهش ةفاضللا متت مل

اهتفاضللا تمت يتللا قدصملا عجرملا ةداهش لباقم اهصحف متي، ةيوهال ةداهش داريتسإ دنع ال نايحلأا ضعب في. يوديلا ليجستللا في قدصملا عجرملا تامولعم بيوبتللا ةمالع نمض ةيوهال ةداهش عيقوتل مدختست يتللا CA ل قدصملا عجرملا ةداهش ةكبشللا ولوؤسم كلمي كمايق دنع تقوؤمللا عضوملل CA ةداهش ةفاضللا يرورضلل نم، ةلالللا هذه في. مهب ةصاخلل ءارجلانكمي، قدصملا عجرملا ةداهش ريفوتو ةيوهال ةداهش رادصللا درجمبو. يوديلا ليجستللاب جلاعم لالخنم للاقتناللا دنع. ةححصلا قدصملا عجرملا ةداهشب ديدج يودي ليجستللا في متامك حيتافملا جوزل مجحللاو مساللا سفن ديدحت نم دكأت، يرخأ ةرم يوديلا ليجستللا نكمي، يرخأ ةرم CA ل CSR هيحوت ةداعل نم ال دب، ءاهتناللا درجمبو. يلصلأا يوديلا ليجستللا اثيدح ءاؤشنللا مت يتللا ةقثللا ةطقنللا اقبسمل اهرادصللا مت يتللا ةيوهال ةداهش داريتسإ ةححصلا CA ةداهش مادختساب.

نأ امإف، يوديلا ليجستللا دنع اهقبيبطت مت دق اهسفن CA ةداهش تنانك اذا ام نم ققحتلل نكمي. show crypto ca تاداهش جارخل نم ققحت وأ ققحتللا مسق في ددحم وه امك CA رزرقنت ةداهش" في ةدوجوملا لوقحلاب "يلسلستللا مقرلا"و "للا اهرادصللا مت" لثم لوقحلا ةنراقم قدصملا عجرملا نم ةمدقملا "قدصملا عجرملا

2. دنع مدختستسمللا حيتافملا جوز نع ءاؤشنللا مت يذل TrustPoint في حيتافملا جوز فلتيخي. ةرداصلال ةداهشلل CSR ءاشنللا

(CSR)، دعب نع لوصوللا في مكحتللا ليعفتو حيتافملا جوز ءاشنللا دنع، يوديلا ليجستللا عم ناك اذا. ةرداصلال ةيوهال ةداهش في هنيمضت نكمي يتح CSR للا ماعللا حاتفملا ةفاضللا متت مت يتللا ةيوهال ةداهش تنانك وأ ام ببسل هليدعت مت دق FTD للا ةدوجوملا حيتافملا جوز ةرداصلال ةيوهال ةداهش تيبتت موقيل ال FTD نإف، فلتيخم ماع حاتفم للا ةدوجوملا حيتافملا جوز نالفتللا نارايتخل دجوي، اذه ثودح نم ققحتلل

في ماعللا حاتفملا ل CSR في ماعللا حاتفملا ةنراقم لراماوالا هذه رادصللا نكمي، OpenSSL في ةرداصلال ةداهشللا

```
openssl req -noout -modulus -in ftd.csr
```

```
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB981941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B966DA10BF24771CFE55327C5A14B96235E9
```

```
openssl x509 -noout -modulus -in id.crt
```

```
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE  
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9  
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C  
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B  
B966DA10BF24771CFE55327C5A14B96235E9
```

- ftd.csr لاي جاستال في FMC نم خسن ي CSR ل او وه
- ID.CRT وه ع ق و م ل ا ي وه ل ا ع د ا ه ش وه

نمض ماعل اجات فم ل ل باقم FTD في ماعل اجات فم ل ا عميق نراقم اضي انكم ي، كلذ نم ال دب في ةدوجوم ل كلت عم قباطت ال ةداهش ل ا في لوال فورحل ن ا ظ حال. ةرداصل ا ي وه ل ا ع د ا ه ش ة: فاض ا ل ا ب س ب FTD ج ر خ م

Windows رتوي بم كل ل ا ل ع ةرداصل ا ي وه ل ا ع د ا ه ش حت ف م ت

Certificate [X]

General Details Certification Path

Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	VPN Intermediate CA, Cisco S...
Valid from	Wednesday, April 8, 2020 1:0...
Valid to	Monday, April 5, 2021 7:29:00...
Subject	ftd-1, Cisco Systems, TAC, ftd...
Public key	RSA (2048 Bits)
Public key parameters	05 00

```

ec 91 e8 d8 06 42 f6 55 d9 82 93 c6 ca 23
6f b1 77 e4 c3 44 0c 8d a4 c2 be c0 19 a3
f0 24 d9 4a ec 7c ad c0 60 19 e1 cc 76 3d
51 ec 6f f1 e2 77 c6 89 83 f6 c4 ce 1b 82
6c be 72 1a 3c 71 98 23 44 86 a1 bf 9c 20
d1 0e 04 7c 8d 39 fa 85 62 71 78 f7 2e 4b
a1 1f 8d 5a cf 95 0f 91 64 b9 66 da 10 bf
24 77 1c fe 55 32 7c 5a 14 b9 62 35 e9 02
03 01 00 01

```

Edit Properties... Copy to File...

OK

دەواى دەستسەلمەنە مەنەلەتەنە جەنە:

```
f6e0fdfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b8af3a491b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8da4c2bec0e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f8d5acf955327c5a14b96235e90203010001
```

مادختسا مت، يوديلا ليچستلا عارجا دنع FTD. نم جتانلا RSA mypubkey key crypto show
جرتستسما ماعلا حاتفملا عارجا عم فرخزما مسقلا قباطتي CSR. `<default-rsa-key>` عاشنلا
ةوهلا ةداهش نم.

```
> show crypto key mypubkey rsa
Key pair was generated at: 16:58:44 UTC Jan 25 2019
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 2048
Storage: config
Key Data:

30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
008a2e53 ff7786a8 a3a922ee 5299574c cdceebc0 96341f19 4a4018bc e9e38a72
44dbea27 59f1897b e7c489c4 84749c4d e13d42b3 4f5a2051 f6e0fdfd 5783db0f
27256900 ae69f3a8 4c217fca 5c6b4334 a8b7b4e8 cd85e749 c1c7f579 3ef0d199
a229e7c5 471c963b 8af3a49e b98b9edb fdde92b5 deb78194 1b3706a2 4f662674
6e5c9237 d9c00b2f f36fd45e 8e9a92a3 de43ec91 e8d80642 f655d982 93c6ca23
6fb177e4 c3440c8d a4c2bec0 19a3f024 d94aec7c adc06019 e1cc763d 51ec6ff1
e277c689 83f6c4ce 1b826cbe 721a3c71 98234486 a1bf9c20 d10e047c 8d39fa85
627178f7 2e4ba11f 8d5acf95 0f9164b9 66da10bf 24771cfe 55327c5a 14b96235
e9020301 0001
```

FMC ي CA بنجاب رمح X

PKCS12 ةمزح ي ةنمضتم ريغ CA ةداهش نأل PKCS12 ليچست عم كلذ ثدحي نأ نكمي.



اهتفاضلا تمت يتلا CA ةداهش PKCS12 جاتحي، كلذ حالصال.

م تي يتلا رورملا ةملك. صاخ حاتفمو ةداهش ةيوهلا تجرتسا in order to رم اذه تردصأ
ةبولطم نمألا صاخلا حاتفملاو PKCS12 عاشنلا تقو اهمادختسا:

```
openssl pkcs12 -info -in test.p12
Enter Import Password: [pkcs12 pass phrase here]
MAC Iteration 1
MAC verified OK
PKCS7 Encrypted data: pbewithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
  friendlyName: Test
  localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
subject=/CN=ftd1.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Intermediate CA
```

-----BEGIN CERTIFICATE-----

MIIC+TCCAeGgAwIBAgIIAUIM3+3IMhIwDQYJKoZIhvcNAQELBQAwOjEaMBgGA1UEChMRQ2l2Yz8gU3lzdGVtcyBUQUUMxHDAaBgNVBAMTE1ZQTiBJbnR1cm1lZG1hdGUgQ0EwHhcNMjAwNDA0MTY1ODAwWhcNMjEwNDA1MjMyOTAwWjAbMRkwFwYDVQQDExBm dGQxLmV4Yw1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA 043eLVP18K0jnYfHCBZuFUyRXTTB28Z1ouIJ5yyrDzCN781GFrHb/wCczRx/jW4n pF9q2z7FHr5bQCI4oSUSX40UQfr0/u0K5riI1uZumPUx1Vp1zVkyuqDd/i1r0+0j PyS7BmyGfV7aebYWZnr8R9ebDsnC2U3nKjP5RaE/wNdVGTs/180H1rIjMpcFMXps LwxdxiEz0hCMnDm9RC+7uWZQd1wZ9oNANCBQC0px/Zikj9Dz70RhhbzBTeUNKD3p sN3VqdDPvGZHFGLPCnhKYyZ79+6p+CHC8X8BFjuTJYoo116uGgiB4Jz2Y9ZeFSQz Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBg1ghkgBhvCAQOEERYPeGNhIGN1 cnRpZm1jYXR1MA0GCsQGSiB3DQEBcWUAA4IBAQCv/MgshWxXtwpwmMF/6KqEj8nB S1jbfz1zNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRY54taRI27W+gLneCbQAux 9amxXuhpxP5E0hnc+tsYS9eriAKpHuS1Y/2uwn92FHIb3HEXPO1HBJueI8PH3ZK 41rPKA9oIQPUW/uueHEF+xCbG4xCLi5H0GeHX+FTigGNqazaX5GM4RBUa4bk8jks Ig53twvop71wE53COTH0EkSRCsVcW5mdJsd9BUZHjguhpw8Giv7Z36qWv18I/Owf RhLhtsgenc25udglv9Sy5xK53a5Ieg8biRpWL9tIjguGjxYZwtyVeHi32S7

-----END CERTIFICATE-----

PKCS7 Data

Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048

Bag Attributes

friendlyName: Test

localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2

Key Attributes: <No Attributes>

Enter PEM pass phrase: [private-key pass phrase here]

Verifying - Enter PEM pass phrase: [private-key pass phrase here]

-----BEGIN ENCRYPTED PRIVATE KEY-----

MIIFDjBAbGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI1KyWxk8cgTMCaggA MBQGccqGSiB3DQMHBAGcm0qRxx/dcwSCBmiF7BpgJNIPhdU5Zorn1jm3pmsI/XkJ MRHc1Ree10ziSLCZOSTr84JFQxNpbThXLhsHC9WhpPy5sNXIvXS7Gu+U10/V1NSA rW1X6SPftAYiFq5QxyEutSHdZZwgQIqpj97seu3Px0agvI0bw1Lo8or51SydnMjp Ptv50Ko95BSHwWycqkTAia4ZKxytyIc/mIu5m72LucOFmoRB05JZu1avWXjbCAA+ k2ebkb1FT0YRQT1Z4tZHSqX1LFPZe170NZEUG7rIcWak1Yw7XNUPh0n6FHL/ieIZ IhvIfj+IqQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E Gnh8r31903A1kPMBkMdx0q1pzo2naIy2KGrUn0SHajVwclR9dTPWIDyjd95YoeS IUE7Ma00pjJc02FNbWyxRrYt+4hp3aJt0ZW83FHiS1B5UIzGrBMAgKJc2Hb2RTV 9gxZGve1cRco1LeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShn0wHzridF8Zn F06XvBDSyXVSpkxwAd1Twxq62tUnLIkyRXo2CSz8z8W29UXmF04o3G67n28//LJ Ku8wj1jeq1vFgXSQiWLADNH772RNwzCMeobfxG1BprF9DPT8yvyBdQviUIuFpJ nNs5FYbLTv9ygZ1S9xwQpTcqEu+y4F5BJuYLMHqcZ+VpFA4nM0YHhZ5M3sccRSR4 1L+a3BPJJsh1TIJQg0TixDaveCfpDcpS+ydUgS6YwY8xw17v0+1f7y5z1t4TkZrt ItBHHA6yDzR0Cn0/ZH3y88a/asDcuKw6bsRaY5iT8nAWGTQVed3xXj+EgeRs25HB dIBBX5gTvqN7qDanhkaPUcEawj1/38M0pAYULei3e1fKKrhwaYsBFaV/BeUMWuNW BmKprkKKQv/JdWnoJ149KcS4bfa3GHG9Xnyvbg8HxopcYFMTEjao+wLZH9agqKe Y0jyoHFN6ccBBC7vn7u12tmXOM5RcnPLmaDaBFDsBBFS8Y8VkeHn3P0q7+sEQ26d vL807WdgLH/wKqovoJRYxwzz+TryRq9cd5BNyyLaABESa1sWRhk81C2P+B+Jdg9w d6RsvJ2dt3pd1/+pUR3CdC0b8qRZOoL03+onUIUoEsCCndp0x8Yj/mvc6ReXtOKB 2qVmhVMYseiU1r0AQgt7XMe1UuiJ+dRnqcfAfbDGeOp+6epm1TK1BJL2mA1QWx51 73Qo4M7rR71aeq/dqob3o1PhcoMLa5z/Lo5vDe7S+LZMuAwjRkSfso0KQOY3kAP1 eZ2Eh2go4eJ7hHf5VFqBLL8Ci3rd3EOijRkNm3fAQmFJ1aFmooBM3Y2Ba+U8cMTH 1gjSfK11FAWpfxw9aSEECNCvEMm1Ghm6/tJDLV1jyTqWajHnWIZCc+P2AXgn1LzG HVVfxs0c8FGUJJPQHAtXYd7worWCxszaufJ99E4PaoZnAOYUFW2jaZEwo0NBpbd1 AjQ8aciuosv0FKpp/jXDI78/aYAEk662tPsfGmxvAWB+UMFarA9ZTiihK3x/tDPy GZ6ByGWJYp/0tNNmJRCFhcAYY83EtzHK9h+8LatFA6WrJ4j3dhceUPzrPXjMffNN 0Yg=

-----END ENCRYPTED PRIVATE KEY-----

نكومي و قلم فنم تافل م يف صاخلا حات فلم او ةيوهلا ةداهش عضو نكمي ،اهلامتكا درجم بو يف ةروكذملا تاوطلخال مادختساب ديدج PKCS12 فلم ىلى قىدصملا عجرملا ةداهش داريتسا

OpenSSL ماديختساب PKCS12 ءاشنإ نم 2. ةوطخلا

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا