Install and Renew Certificate on FTD Managed by FDM

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Certificate Installation
Self-Signed Enrollment
Manual Enrollment
Trusted CA Certificate Installation
Certificate Renewal
Common OpenSSL Operations
Extract Identity Certificate and Private Key from PKCS12 File
Verify
View Installed Certificates in FDM
View Installed Certificates in CLI
Troubleshoot
Debug Commands
Common Issues
Import ASA Exported PKCS12

Introduction

This document describes how to install, trust, and renew self-signed certificates and certificates signed by a third party CA or internal CA on FTD.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Manual certificate enrollment requires access to a trusted third party Certificate Authority (CA). Examples of third party CA vendors include, but are not limited to, Entrust, Geotrust, GoDaddy, Thawte, and VeriSign.
- Verify that the Firepower Threat Defense (FTD) has the correct clock time, date, and time zone. With certificate authentication, it is recommended to use a Network Time Protocol (NTP) server to synchronize the time on the FTD.

Components Used

The information in this document is based on these software and hardware versions:

- FTDv that runs 6.5.
- For Keypair and Certificate Signing Request (CSR) creation, OpenSSL is used.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Certificate Installation

Self-Signed Enrollment

Self-Signed certificates are an easy way to get a certificate with the appropriate fields added to the FTD device. Although they cannot be trusted in most places, they can still provide similar encryption benefits as a third party signed certificate. Still, it is recommended to have a trusted CA-signed certificate so that users and other devices are able to trust the certificate presented by the FTD.



Note: Firepower Device Management (FDM) does have a default self-signed certificate named DefaultInternalCertificate that can be used for similar purposes.

1. Navigate to **Objects > Certificates**. Click the + symbol and then choose **Add Internal Certificate** as shown in the image.

- cis	Firepower De	evice Manager	Nonitoring	Policies	HE Objects	Device: FTD-3	(9 🖨 🙆	2:	admin Administrator
Ŧ	Application Filters	 Certificate 	es			-				
ø	URLs									
Ŷ	Geolocations	117 objects					Q Snar	h		+ ~
	Syslog Servers	* NAME				1996				Add Internal CA
ß	IKE Policies	1 NGFW-D	efault-InternalCA			Internal CA			- P	Add Internal Certificate
-	IPSec Proposals	2 Defaultin	ternalCertificate			Internal Certificate				Add Trusted CA Centricate
-	AnyConnect Client	3 DefaultV	/ebserverCertificate			Internal Certificate				
•	Identity Sources									
1	Users									
	Certificates									
8	Secret Keys									
ĩ	DNS Groups									
Tg	Event List Filters									
e.	SLA Monitors									

2. Choose Self-Signed Certificate in the popup window as shown in the image.



×

	Upload Certificate and Key Create a certificate from existing files. PEM and DER files are supported.
Q	Self-Signed Certificate Create a new certificate that is signed by the device.

3. Specify a **Name** for the trustpoint, then fill out the subject distinguished name fields. At a minimum, the **Common Name** field can be added. This can match the Fully Qualified Domain Name (FQDN) or IP address of the service for which the certificate is used. Click **Save** when done as shown in the image.

Add Internal Certificate	ø ×							
Name								
FTD-3-Self-Signed								
Country	State or Province							
×								
Locality or City								
Oroanization	Organizational Unit (Department)							
Cisco Systems	TAC							
Common Name								
You must specify a Common Name to use the certificate with remote access VPN								
	CANCEL SAVE							

4. Click the **Pending Changes** button from the top right of the screen as shown in the image.

cisco	Firepower De	avice N	Manager	四 Monitoring	Ø Policies	ika Objects	Device: FTD-3	()	2	?:	admin Administrator	×
🐨 App	dication Filters	^	Certificate	s								
Ø URI								0				1
🂡 Geo	olocations		118 objects					Q Search				ŦŤ
🖥 Sys	log Servers		* NAME				THE				ACT	TIONS
🔏 ike	Policies		1 NGFW-Def	ault-InternalCA			Internal CA					
🐴 iPS	ec Proposals		2 DefaultInte	emalCertificate			Internal Certificate					
🖨 Any	Connect Client		3 DefaultWe	bserverCertificat	•		Internal Certificate					
Et Ide	ntity Sources		4 FTD-3-Sel	f-Signed			Internal Certificate					
L Use												
요 Cer	tificates											
🔒 Sec	ret Keys											
🖥 DNS	S Groups											
Ty Eve	nt List Filters											
n su	Monitors	~										

5. Click the **Deploy Now** button.



Note: When the deploy is done, the certificate is not available to be seen in the CLI until there is a service that uses it such as AnyConnect as shown in the image.

Pending Changes	0 ×
Last Deployment Completed Successfully 13 Apr 2020 09:56 AM. See Deployment History	
Deployed Version (13 Apr 2020 09:56 AM)	Pending Version C LEGEND Removed Added Edited
Internal Certificate Added: FTD-3-Self-Signed	^
	<pre>cert.masked: false cert.encryptedString: *** privateKey.masked: false privateKey.encryptedString: *** issuerCommonName: ftd3.example.com issuerCountry: issuerCountry: issuerCoganization: Cisco Systems issuerOrganizationUnit: TAC issuerState: subjectCommonName: ftd3.example.com</pre>
- - - -	<pre>subjectCountry: subjectDistinguishedName: CN=ftd3.example.com, OU=TAC, O=_ subjectLocality: subjectOrganization: Cisco Systems subjectOrganizationUnit: TAC</pre>
MORE ACTIONS ~	CANCEL DEPLOY NOW

Manual Enrollment

Manual Enrollment can be used to install a certificate issued by a trusted CA. OpenSSL or a similar tool can be used to generate the private key and CSR required to receive a CA-signed certificate. These steps cover common OpenSSL commands in order to generate the private key and CSR as well as the steps to install the certificate and private key once obtained.

1. With OpenSSL or a similar application, generate a private key and Certificate Signing Request (CSR). This example shows a 2048 bit RSA key named private.key and a CSR named ftd3.csr that is created in OpenSSL.

```
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) []:ftd3.example.com
Email Address []:.
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

2. Copy the generated CSR and send it to a CA. Once the CSR has been signed, an identity certificate is provided.

3. Navigate to **Objects > Certificates**. Click the + symbol, then choose **Add Internal Certificate** as shown in the image.

cisco.	irepower Device Manager	Monitoring Policies	Device: FTD-3	> 🛎 🔊 ?	* admin Administrator
T Applicat	on Filters				
🖉 URLs	Certifica	ates			
💡 Geoloce	tions 117 objects			Q Snamh	+ -
📱 Syslog S	ervers • NAME		TYPE		Add Internal CA
🔎 IKE Polic	kos 1 NGFW	-Default-InternalCA	Internal CA		Add Internal Certificate
🐴 IPSec Pi	oposals 2 Defau	ItInternalCertificate	Internal Certificate		Add Trusted CA Certificate
AnyCon	a Defav	ltWebserverCertificate	Internal Certificate		
E Identity	Sources				
1 Users					
유 Certific	ites				
🔒 Secret K	eys				
📋 DNS Gro	ups				
😼 Event Li	it Filters				
🕫 SLA Mo	nitors				

4. Choose Upload Certificate and Key in the popup window as shown in the image.

Choose the type of internal certificate you want to create



5. Specify a **Name** for the trustpoint, then either upload, or copy and paste the identity certificate and private key in Privacy Enhanced Mail (PEM) format. If the CA provided the certificate and key together in a single PKCS12, navigate to the section titled **Extracting Identity certificate** and private key from **PKCS12** file later in this document in order to separate them.



Note: The file names cannot have any spaces or FDM does not accept them. Additionally, the private key must not be encrypted.

Click **OK** when done as shown in the image.

Add Internal Certificate

Name		
FTD-3-Manual		
SERVER CERTIFICATE (USER AGENT)		
Paste certificate, or choose file: UPLOAD CERTIFICATE ftd3.crt		
BEGIN CERTIFICATE MIIErTCCApWgAwIBAgIIc1J4vfTthUYwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE		^
ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTlw		~
CERTIFICATE KEY		
Paste key, or choose file: UPLOAD KEY private.key		
BEGIN RSA PRIVATE KEY		^
MIIEpAIBAAKCAQEAnGpzMjuf+HtRG5ZYf80V6V1sSyF7XhRxjRI80wUih5wBz6qN ntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGbmyNz+A6jgNqAkTvaFMZV/RrW		~
	CANCEL	ОК
	CANCEL	ОК

6. Click the **Pending Changes** button from the top right of the screen as shown in the image.

cisco. P	irepower Device	e Manager Monitoring	Policies Objects	Device: FTD-3	S 🚑 🛛 (?) : admin Administrator
🐬 Applicati	on Filters 🔺	Certificates				
Ø URLs					0	
Geolocal	ions	118 objects			Q Seawh	+ ~
🔋 Syslog S	ervers	# RAME		TYPE		ACTIONS
🔏 IKE Polic	es	1 NGFW-Default-InternalCA		Internal CA		
🐴 IPSec Pr	oposals	2 DefaultInternalCertificate		Internal Certificate		
AnyConr	ect Client	3 DefaultWebserverCertificate		Internal Certificate		
🛋 Identity S	Sources	4 FTD-3-Manual		Internal Certificate		
LUsers						
Cardifica	10.0					
A						
Secret K	179 -					
DNS Gro	aps					
Event Lis	t Filters					
C SLA Mor	itors 👻					

7. Click the **Deploy Now** button.

) ×



Note: When the deploy is done, the certificate is not available to be seen in the CLI until there is a service that uses it such as AnyConnect as shown in the image.

Pending Changes

Last Deployment Completed Successfully 13 Apr 2020 09:56 AM. See Deployment History

	Deployed Version (13 Apr 2020 09:56 AM)	Pending Version CLEGEND Removed Added Edited	ł
0	Internal Certificate Added: FTD-3-Manual		^
	- - - - - - - - -	<pre>cert.masked: false cert.encryptedString: *** privateKey.masked: false privateKey.encryptedString: *** issuerCommonName: VPN Root CA issuerCountry: issuerCountry: issuerLocality: issuerOrganization: Cisco Systems TAC issuerOrganizationUnit: issuerOrganizationUnit: issuerState: subjectCommonName: ftd3.example.com</pre>	
	- - - -	subjectCountry: subjectDistinguishedName: CN=VPN Root CA, O=Cisco Systems_ subjectLocality: subjectOrganization: Cisco Systems subjectOrganizationUnit: TAC	~
M	DRE ACTIONS V	CANCEL DEPLOY NOW -	

Trusted CA Certificate Installation

When you install a trusted CA certificate, it is necessary, in order to successfully authenticate users or devices which present identity certificates to the FTD. Common examples of this include AnyConnect certificate authentication and S2S VPN certificate authentication. These steps cover how to trust a CA certificate so that certificates issued by that CA are also trusted.

1. Navigate to **Objects > Certificates**. Click the + symbol, then choose **Add Trusted CA Certificate** as shown in the image.

CISCO. Firepower D	evice Manager	Monitoring	Policies 0	bjects Device:	m FTD-3	6	1	* admin * Administrator
🛷 Application Filters	^ Certificate	es						
🖉 URLs	117 objects				Q	Search		+ ~
Geolocations	a NAME			TIPE				Add Internal CA
Syslog Servers	1 Defaultin	ternalCertificate		Internal Certifi	icate			Add internal Certificate
🔏 IKE Policies	2 DefaultW	ebserverCertificate		Internal Certifi	icate			Add Trusted CA Certificate
🐴 IPSec Proposals	3 NGFW-D	afault-InternalCA		Internal CA				
AnyConnect Client								
Identity Sources								
1 Users								
A Certificates								
Secret Keys								
DNS Groups								
Y Event List Filters	~							
C SLA Monitors								

2. Specify a **Name** for the trustpoint. Then either upload, or copy and paste the CA certificate in PEM format. Click **OK** when done as shown in the image.

Add Trusted CA Certificate	0	×			
Name VPN_Root_CA					
Paste certificate, or choose file: UPLOAD CERTIFICATE VPN_Root_CA.crt					
BEGIN CERTIFICATE MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE ChMRQ2lzY28gU3lzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw MDQwNTlzMTYwMFoXDTMwMDQwNTlzMTYwMFowMjEaMBgGA1UEChMRQ2lzY28gU3lz dGVtcyRLIQLIMxEDASBaNI/BAMTC1ZQTiBSb290IENBMIICliANBakabkiG9w0BAQEE					
CANCEL	ОК				

3. Click the **Pending Changes** button from the top right of the screen as shown in the image.

cisco. Firepower De	avice Manager Monitoring Policies Objects	Device: FTD-3	stor ~
Application Filters	Certificates		
🖉 URLs	Certificates		
Geolocations	118 objects	Q. Search	+ ~
🚦 Syslog Servers	· HEAME	THE	ACTIONS
🔏 IKE Policies	1 DefaultInternalCertificate	Internal Certificate	
🐴 IPSec Proposals	2 DefaultWebserverCertificate	Internal Certificate	
AnyConnect Client	3 NGFW-Default-InternalCA	Internal CA	
📾 Identity Sources	4 VPN_Root_CA	Trusted CA Certificate	
1 Users			
與 Certificates			
🔒 Secret Keys			
DNS Groups			
😼 Event List Filters			
🕫 SLA Monitors	v		

4. Click the **Deploy Now** button as shown in the image.

Pe	ending Changes	@ ×
0	Last Deployment Completed Successfully 13 Apr 2020 09:56 AM. See Deployment History	
	Deployed Version (13 Apr 2020 09:56 AM)	Pending Version C LEGEND Removed Added Edited
0	External CA Certificate Added: VPN_Root_CA	^
	- - - - - - - - - - - - - - - - - - -	<pre>cert.masked: false cert.encryptedString: *** issuerCommonName: VPN Root CA issuerCountry: issuerOrganization: Cisco Systems TAC issuerOrganizationUnit: issuerState: subjectCommonName: VPN Root CA subjectCountry: subjectCountry: subjectDistinguishedName: CN=VPN Root CA, O=Cisco Systems subjectCorganization: Cisco Systems TAC subjectOrganizationUnit: subjectOrganizationUnit: subjectState: validityStartDate: Apr 05 23:16:00 2020 GMT</pre>
M	ORE ACTIONS Y	CANCEL DEPLOY NOW

Certificate Renewal

Certificate renewal on an FTD managed by FDM involves the replacement of the previous certificate and potentially the private key. If you do not have the original CSR and private key used to create the original certificate, then a new CSR and private key needs to be created.

1. If you have the original CSR and private key, this step can be ignored. Otherwise, a new private key and CSR need to be created. Use OpenSSL, or a similar application, to generate a private key and CSR. This example shows a 2048 bit RSA key named private.key and a CSR named ftd3.csr that is created in OpenSSL.

openss1 req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr Generating a 2048 bit RSA private key writing 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 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) []:ftd3.example.com Email Address []:. Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:

An optional company name []:

2. Send the generated CSR or the original CSR to a Certificate Authority. Once the CSR has been signed, a renewed identity certificate is provided.

3. Navigate to **Objects > Certificates**. Hover over the certificate you want to renew, and click the **View** button as shown in the image.

cisco. Firepower De	avice Manager 10 10 10 10 10 10 10 10 10 10 10 10 10	Device: FTD-3
 Application Filters 	^ Certificates	
🥔 URLs	Certificates	
Geolocations	118 objects	Q Search + ~
🖁 Syslog Servers	• NAME	TYPE ACTIONS
🔏 IKE Policies	1 NGFW-Default-InternalCA	Internal CA
🐴 IPSec Proposals	2 DefaultInternalCertificate	Internal Certificate
AnyConnect Client	3 DefaultWebserverCertificate	Internal Certificate
Identity Sources	4 FTD-3-Manual	Internal Certificate
👤 Users		
R Certificates		
🔒 Secret Keys		
DNS Groups		
y Event List Filters		
🕫 SLA Monitors	~	

4. In the pop-up window, click **Replace Certificate** as shown in the image.

View Internal Certificate	8	×
Name		
FTD-3-Manual		
REPLACE CERTIFICATE		
Subject Common Name		
ftd3.example.com		
Subject Organization		
Cisco Systems		
Subject Organization Unit		
TAC		
Issuer Common Name		
VPN Root CA		
Issuer Organization		
Cisco Systems TAC		
Valid Time Range		
Apr 13 14:56:00 2020 GMT - Apr 13 14:56:00 2021 GMT		
CANCEL	SAVE	

5. Either upload, or copy and paste the identity certificate and private key in PEM format. Click **OK** when done as shown in the image.

Edit Internal Certificate	0	×
Name		
FTD-3-Manual		
SERVER CERTIFICATE (USER AGENT)		
Paste certificate, or choose file: REPLACE CERTIFICATE ftd3-renewed.crt		
BEGIN CERTIFICATE MIIErTCCApWgAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE ChMRQ2IzY28gU3IzdGVtcyBUQUMxFDASBgNVBAMTC1ZQTIBSb290IENBMB4XDTIw		
CERTIFICATE KEY		
Paste key, or choose file: REPLACE KEY private.key		
BEGIN RSA PRIVATE KEY		^
MIIEpAIBAAKCAQEAnGpzMjuf+HtRG5ZYf80V6V1sSyF7XhRxjRl80wUih5wBz6qN ntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGbmyNz+A6jgNqAkTvaFMZV/RrW		
CANCEL	ОК	

6. Click the **Pending Changes** button from the top right of the screen as shown in the image.

cisco. Firepower Dev	rice Manager Monitoring Policies Objects	Device: FTD-3
🐬 Application Filters	Certificates	
Ø URLs		0
Geolocations	118 objects	Q Search + *
Syslog Servers	B NAME	TYPE AGTIONS
🔏 IKE Policies	1 NGFW-Default-InternalCA	Internal CA
🐴 IPSec Proposals	2 DefaultInternalCertificate	Internal Certificate
AnyConnect Client	3 DefaultWebserverCertificate	Internal Certificate
a Identity Sources	4 FTD-3-Manual	Internal Certificate
1 Users		
风 Certificates		
🔒 Secret Keys		
DNS Groups		
y Event List Filters		
🖓 SLA Monitors	,	

7. Click the **Deploy Now** button as shown in the image.

Ρ	ending Changes		0	×
0	Last Deployment Completed Successfully 13 Apr 2020 12:41 PM. See Deployment History			
	Deployed Version (13 Apr 2020 12:41 PM)	Pending Version C LEGEND Removed	Added	Edited
0	Internal Certificate Edited: FTD-3-Manual			~
	cert.encryptedString: *** validityStartDate: Apr 13 14:56:00 2020 GMT validityEndDate: Apr 13 14:56:00 2021 GMT privateKey.encryptedString: ***	Apr 13 16:44:00 2020 GMT Apr 13 16:44:00 2021 GMT		
				, ,
N	MORE ACTIONS Y	CANCEL DEPLOY N	IOW	~

Common OpenSSL Operations

Extract Identity Certificate and Private Key from PKCS12 File

An administrator can receive a PKCS12 file that needs to be imported on to the FTD. FDM does not currently support the import of PKCS12 files. In order to import the certificates and private key contained within the PKCS12 file, the individual files must be extracted from the PKCS12 with the use of a tool like OpenSSL. You need the passcode used to encrypt the PKCS12.

```
openssl pkcs12 -info -in pkcs12file.pfx
Enter Import Password: [PKCS12-passcode]
MAC Iteration 1
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    localKeyID: 28 20 C1 B4 08 1E 65 2E 4D 1D F9 F3 25 07 62 F7 D9 96 A7 F4
    friendlyName: ftd3.example.com
subject=/0=Cisco Systems/OU=TAC/CN=ftd3.example.com
issuer=/0=Cisco Systems TAC/CN=VPN Root CA
----BEGIN CERTIFICATE-----
MIIErTCCApWgAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ21zY28gU31zdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQxMzE2NDQwMFoXDTIxMDQxMzE2NDQwMFowQTEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEMMAoGA1UECxMDVEFDMRkwFwYDVQQDExBmdGQzLmV4YW1wbGUuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnGpzMjuf+HtRG5ZYf80V6V1s
SyF7XhRxjR180wUih5wBz6qNntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZOIcpzVqL6hOziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50
QpQDTgvIiD1bYpPiWKpS0g1PZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZa
HrP9Y0x09+MpVMH33R9vR13S0EF6kpZ6VEdGI4s6/IRvaM1z1BcK10N/N2+mjwID
AQABo4G3MIG0MAkGA1UdEwQCMAAwHQYDVR00BBYEFMcvjL0XiSTzNADJ/ptNb/cd
zB8wMB8GA1UdIwQYMBaAFHekzDnhi40727mjLXuwCRVFgyguMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwGwYDVR0RBBQwEoIQZnRk
My51eGFtcGx1LmNvbTAeBg1ghkgBhvhCAQ0EERYPeGNhIGN1cnRpZm1jYXR1MA0G
```

```
CSqGSIb3DQEBCwUAA4ICAQCjjrMjruGH5fpcFND8qfuVU0hkszCwq201oMqMrvXn
gENKcXxxT27z6AHnQXeX3vhDcY3zs+FzFSoP5tRRPmy/413HAN+QEP2L9MQVD9PH
f50rQ/Ke5c16hM0J08daR7wNzvFkcbicKCLRH0EvEoI0SPKsLyGSSxGmh6QXfZcM
GX3jG9Krg1ugp2UEqOug9HPTpgsbuNcHw8xXgFp6IA10LrytwrLeMIh5V+Vh5p11
yTl9wo5VADoYKgN408D21TeJIj6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwfMXM4Tl
Rk3EOdSTENqzq2ZwnqJ4HCoqar7AS1Q5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBUlbadlnEfi5Jl8G+/vZl6ykcmXe9hokKYxY8cg/U7170n/FbAmdYwRYgMAE4
RWfBp0voNzn97cG+qzogo7j/0kTfYu309DzdU3uy+R8JJkBrerktrZR7w70fP610
IAs86N5Zb18U14Gfc9m0eXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2Px0yam/bR0n0FoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJF0iV0GV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfpMwTiT47I
ng==
-----END CERTIFICATE-----
Certificate bag
Bag Attributes: <No Attributes>
subject=/0=Cisco Systems TAC/CN=VPN Root CA
issuer=/0=Cisco Systems TAC/CN=VPN Root CA
----BEGIN CERTIFICATE-----
MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ21zY28gU31zdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQwNTIzMTYwMFoXDTMwMDQwNTIzMTYwMFowMjEaMBgGA1UEChMRQ21zY28gU31z
dGVtcyBUQUMxFDASBqNVBAMTC1ZQTiBSb290IENBMIICIjANBqkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAxhTBKiB1xzLg2Jr48h/2u84RcWahOTmPYCNGYZg0PvSf
JOpKvAu5tz4z625Yx1nBtjSsEgzF+qETpSplEhjW2NxIclxuNirfrmSJQfIw51yT
PaFv7u+VhgyYbYsSxGAB/m6RWWpiNbg8SDoUACU7R/bvp1Rb8W6tXk/rsTljc7L2
c/G5MeDLNmc/i/M1zuMjhj0tCphsJPhvNII7lcNj6K0pvg2yB/Md7PX0ZnLaz9pf
GgpjpH0zzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXm1HQcgp
g5BgZMGqro015rcq0PjtK9Tqg7q013Vf0kMlsofMp+Bu1CiFDpawF/j8uSPuswEs
rzvJ+8GbOY1WEHtohgNGjPO0q8wnKQu0C47Ft1UMpdSwUsMMze0X43dyp/WoZtLW
4v/Pn/NibE3aoPOaMhIo4CdwSBHZOgVag4INqVsuFX1uPKD25Whr109LQ93P/sN3
FhoAh98HKOcuQ64Ua3AaShdzornD+G2J2pd1Nf1Dah1z1skIMt1URSWdLjsHLKft
JqSOoLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/lyNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cxl1jIN0LdB+/jQqkfzmx9ziB1PXnIshNRbflLLrNfdD09agqQsvsC
AwEAAaNdMFswDAYDVROTBAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDKC4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDKC4wCwYDVR0PBAQD
AgEGMA0GCSqGSIb3DQEBCwUAA4ICAQC6B+Y3obatEZqv0RQz1MS6o0umCgNWGi8d
kcRDxkY2F+zw3pBFa54Sin10fRPJvZvLNJV50dXmvH51uh6KJDMVrLMWNiSgI7Tn
0ipqKraokS20o0STwQ7Q9Wk1xCrwxMfTuDJFMe80qabFAU55705PDXPtFEutn0xz
Ou8VMLBRy+gDc+OWARsjFj+OgUOc2Wj3gQ81G1yoPYgufWRnztN5rQxWzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AydsGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p702FZ1y51xuzuA/wPnR89HiIkSF130MTpn0I13d6d07s3bwyNja8JikYTCf11e5
2CSsz4Cn/BlwfWyAcLN3HxUjG4Ev2818fWWpkYmuxujpKDFFzF0skpKAK53tNKPf
pn4+w5FyLo18o0AydtPoKjYkDqbvG/SRPbt92mdTIF7E6J+o8J60V3YL+IyrZ+u0
MYqPd450i4cqHdMFICAndN3PYScrrGYHawfVxp+R+G4dTJWdMvthh3ftS0mkiKJ8
m1NH7WYST1kYcTbcokZiOIcZa+VVv5UOLIt/hD0VG7xqZ01pMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpxTIsmDv9rQzxBjuCyKn+23FkkUhFJt0D989UUyp08H9vDoJr
yzm9J0pMrg==
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    localKeyID: 28 20 C1 B4 08 1E 65 2E 4D 1D F9 F3 25 07 62 F7 D9 96 A7 F4
    friendlyName: ftd3.example.com
Key Attributes: <No Attributes>
Enter PEM pass phrase: [private-key-passcode]
Verifying - Enter PEM pass phrase: [private-key-passcode]
----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIScA8TOogup4CAggA
MBQGCCqGSIb3DQMHBAgKqoTuZzoXsASCBMgOTEb24ENJ14/qh3GpsE2C20CnJeid
ptDDIFdyOV4A+su3OJWzlnHrCuIhjR8+/p/NOWlA73x47R4T6+u4w4/ctHkvEbQj
gZJZzFWTed9HqidhcKxxOoM/w6/uDv/opc6/r1IZiaKp6F09h0ibq1GI9kjxkWQC
EQR8cM1U2yi0vagL8pOYdeujCrzBtorRp9BMJe1CP1Mw9t0EbAC4mmuedzs+86r1
```

xadK7gHBuWUJcO3SLXLCmX5yLSGteWcoaPZnIKO9UhLxpUSJTkWLHr2VtE1ACMRc R1PBXMLb70nMtPTqct158+Q/axtQCWUs8caHs3LvVf0nRG+War49/F8Ii8mqnNnb M6ZTwT0Z1sn0f4ohVePrW/kkdlQavJbPa+0dzjZvs88ClEXAJ/XIegfSWifJAXqP 3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jj1KqfoxubtnuFq un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZHOBuF1s+wZEmzYqw+cuc+I8XEFVOM18 P3ah28Nno0jXMk4MpfFJ1YMCmMq66xj5gZtcVZxOGCOswOCKU0JiFFQTEmmVf9/C 65a96np7YCI8s6UnUWi5Zp/NrbN31HkP0wt7+1DFGFit1pTTGv0FchtLYWeB3Kj0 h/C/R7ciq6ZNCzwBrbztGV8jG115NSs1wKbTGiiwCYw0N8c09TXQb04rMomFDAv8 aef1aBsjMqEUkzOZKOU2ZgTxMline8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubpO qtmFX/DtSu9J2yevfV+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc40 w94f0H/DJ/1KsmSVwBLQLEKR1/nIDz36kmA27+1nVtX42PbEaIaFqucU4xHKx3zN mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaq8 fN17vEB+aret+PmqCiQY1Hqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUROTuBHQhRK 3XpHfGXpe/00GdW3LeifNLvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzd0cJ3aGCeA184XuPRfQhHe/Aj7q616uqB W3Kt+kMJ9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/ QCyhIRk3mx+8a1YLqK+hOMjWWBDEHX2mvbdKickK/jhwRdR/WmFOALq51phgtZlz Zed15UbPqWahJsjo09N5pp7Uq5iV0/xq4M1+/xQIYo2GIrqyat4AdB2B6K8K3xQd Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTfzH5zgneUwLwnuBAbGT3oMSQ/ OKXnhcmUGu8XvLEfU/PITvGzKr06o12/hHJtzXQ8eNPDJbvcD/okRRKZpmjH+ijp FPD/WgQ/vmO9HdCWW3f1hqceqfHff8C1CJYFLxsgZp4M3G+WyQTky4J8+6uTn/mj yyZ5JCZdlt42haSNqU/ynioCjh5XY4m8WMZsOJBNPjKZiUX/vqVcc+/nodl7VRZy FIk =

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

pkcs12file.pfx is aPKCS12 file that needs to be unpackaged.

In this example, three separate files are created:

One for the Identity Certificate. You can tell this is the identity certificate due to the subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com.

```
subject=/0=Cisco Systems/OU=TAC/CN=ftd3.example.com
issuer=/0=Cisco Systems TAC/CN=VPN Root CA
----BEGIN CERTIFICATE-----
MIIErTCCApWgAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ21zY28gU31zdGVtcyBUQUMxFDASBqNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQxMzE2NDQwMFoXDTIxMDQxMzE2NDQwMFowQTEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEMMAoGA1UECxMDVEFDMRkwFwYDVQQDExBmdGQzLmV4YW1wbGUuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnGpzMjuf+HtRG5ZYf80V6V1s
SyF7XhRxjR180wUih5wBz6qNntQkd0JPog+CFgEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bgotoz3/8CrZOIcpzVqL6hOziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50
QpQDTqvIiD1bYpPiWKpS0q1PZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZa
HrP9Y0x09+MpVMH33R9vR13S0EF6kpZ6VEdGI4s6/IRvaM1z1BcK10N/N2+mjwID
AQABo4G3MIG0MAkGA1UdEwQCMAAwHQYDVR00BBYEFMcvjL0XiSTzNADJ/ptNb/cd
zB8wMB8GA1UdIwQYMBaAFHekzDnhi40727mjLXuwCRVFgyguMAsGA1UdDwQEAwIF
oDAdBqNVHSUEFjAUBqqrBqEFBQcDAQYIKwYBBQUHAwIwGwYDVR0RBBQwEoIQZnRk
My5leGFtcGxlLmNvbTAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMA0G
CSqGSIb3DQEBCwUAA4ICAQCjjrMjruGH5fpcFND8qfuVU0hkszCwq201oMqMrvXn
gENKcXxxT27z6AHnQXeX3vhDcY3zs+FzFSoP5tRRPmy/413HAN+QEP2L9MQVD9PH
f50rQ/Ke5c16hM0J08daR7wNzvFkcbicKCLRH0EvEoI0SPKsLyGSSxGmh6QXfZcM
GX3jG9Krg1ugp2UEqOug9HPTpgsbuNcHw8xXgFp6IA10LrytwrLeMIh5V+Vh5p11
yT19wo5VADoYKqN408D21TeJIj6KB7YnYFB5wMqPGR5h5wx1qNq/MFixwfMXM4T1
Rk3EOdSTENgzg2ZwngJ4HCogar7AS1Q5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBUlbadlnEfi5Jl8G+/vZl6ykcmXe9hokKYxY8cg/U7170n/FbAmdYwRYgMAE4
RWfBp0voNzn97cG+qzogo7j/0kTfYu309DzdU3uy+R8JJkBrerktrZR7w70fP610
IAs86N5Zb18U14Gfc9m0eXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
```

```
YRQ1ft1FxHpn4zMkjI2PxOyam/bROn0FoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJF0iV0GV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfpMwTiT47I
ng==
-----END CERTIFICATE-----
```

One for the Issuing CA Certificate. You can tell this is the identity certificate due to the subject=/O=Cisco Systems TAC/CN=VPN Root CA. This is the same value as the issuer in the Identity Certificate that is seen previously:

```
subject=/0=Cisco Systems TAC/CN=VPN Root CA
issuer=/0=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MILEO=CCA.uugAutBAgIIOgBS (uugaDiguDO)/1/cgThuch
```

MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE ChMRQ21zY28gU31zdGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw MDQwNTIzMTYwMFoXDTMwMDQwNTIzMTYwMFowMjEaMBgGA1UEChMRQ21zY28gU31z dGVtcyBUQUMxFDASBgNVBAMTC1ZQTiBSb290IENBMIICIjANBgkqhkiG9w0BAQEF AAOCAg8AMIICCgKCAgEAxhTBKiB1xzLg2Jr48h/2u84RcWahOTmPYCNGYZg0PvSf JOpKvAu5tz4z625Yx1nBtjSsEgzF+qETpSplEhjW2NxIclxuNirfrmSJQfIw51yT PaFv7u+VhgyYbYsSxGAB/m6RWWpiNbg8SDoUACU7R/bvp1Rb8W6tXk/rsTljc7L2 c/G5MeDLNmc/i/M1zuMjhj0tCphsJPhvNII7lcNj6K0pvg2yB/Md7PX0ZnLaz9pf GgpjpH0zzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXm1HQcgp g5BgZMGqro0l5rcq0PjtK9Tqg7q013Vf0kMlsofMp+Bu1CiFDpawF/j8uSPuswEs rzvJ+8Gb0Y1WEHtohgNGjP00q8wnKQu0C47Ft1UMpdSwUsMMze0X43dyp/WoZtLW 4v/Pn/NibE3aoP0aMhIo4CdwSBHZ0gVag4INqVsuFX1uPKD25Whr109LQ93P/sN3 FhoAh98HKOcuQ64Ua3AaShdzornD+G2J2pd1Nf1Dah1z1skIMt1URSWdLjsHLKft JqSOoLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/lyNexDsd1m6PH7mQj+iL8/9 c2qDhuich3cxl1jIN0LdB+/jQqkfzmx9ziB1PXnIshNRbflLLrNfdD09agqQsvsC AwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUd6TM0eGLg7vbuaMte7AJ FUWDKC4wHwYDVR0jBBgwFoAUd6TM0eGLg7vbuaMte7AJFUWDKC4wCwYDVR0PBAQD AgEGMA0GCSqGSIb3DQEBCwUAA4ICAQC6B+Y3obatEZqv0RQz1MS6oOumCgNWGi8d kcRDxkY2F+zw3pBFa54Sin10fRPJvZvLNJV50dXmvH51uh6KJDMVrLMWNiSgI7Tn 0ipqKraokS20o0STwQ7Q9Wk1xCrwxMfTuDJFMe80qabFAU55705PDXPtFEutn0xz Ou8VMLBRy+gDc+OWARsjFj+OgUOc2Wj3gQ81G1yoPYgufWRnztN5rQxWzFLSsCNN jnIesjQv0vF3nY7SH5QasPN25AydsGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6 p702FZ1y51xuzuA/wPnR89HiIkSF130MTpnOI13d6d07s3bwyNja8JikYTCf1le5 2CSsz4Cn/BlwfWyAcLN3HxUiG4Ev2818fWWpkYmuxujpKDFFzF0skpKAK53tNKPf pn4+w5FyLo18o0AydtPoKjYkDqbvG/SRPbt92mdTIF7E6J+o8J60V3YL+IyrZ+u0 MYqPd450i4cgHdMFICAndN3PYScrrGYHawfVxp+R+G4dTJWdMvthh3ftS0mkiKJ8 m1NH7WYST1kYcTbcokZiOIcZa+VVv5U0LIt/hD0VG7xqZ01pMQKkYUBzg5LbGINm 8ypfhQ1faI5fQRxpxTIsmDv9rQzxBjuCyKn+23FkkUhFJt0D989UUyp08H9vDoJr yzm9J0pMrg==

----END CERTIFICATE----

And one for the private key:

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

MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIScA8TOogup4CAggA MBQGCCqGSIb3DQMHBAgKqoTuZzoXsASCBMgOTEb24ENJ14/qh3GpsE2C20CnJeid ptDDIFdy0V4A+su30JWz1nHrCuIhjR8+/p/N0WlA73x47R4T6+u4w4/ctHkvEbQj gZJZzFWTed9HqidhcKxx0oM/w6/uDv/opc6/r1IZiaKp6F09h0ibqlGI9kjxkWQC EQR8cM1U2yi0vagL8p0YdeujCrzBtorRp9BMJelCP1Mw9t0EbAC4mmuedzs+86r1 xadK7qHBuWUJc03SLXLCmX5yLSGteWcoaPZnIK09UhLxpUSJTkWLHr2VtE1ACMRc R1PBXMLb70nMtPTqct158+Q/axtQCWUs8caHs3LvVf0nRG+War49/F8Ii8mqnNnb M6ZTwT0Z1sn0f4ohVePrW/kkdlQavJbPa+0dzjZvs88C1EXAJ/XIeqfSWifJAXqP 3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jj1KgfoxubtnuFq un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZHOBuF1s+wZEmzYqw+cuc+I8XEFVOM18 P3ah28Nno0jXMk4MpfFJ1YMCmMq66xj5gZtcVZxOGCOswOCKU0JiFFQTEmmVf9/C 65a96np7YCI8s6UnUWi5Zp/NrbN31HkPOwt7+1DFGFit1pTTGvOFchtLYWeB3Kj0 h/C/R7ciq6ZNCzwBrbztGV8jG115NSs1wKbTGiiwCYw0N8c09TXQb04rMomFDAv8 aef1aBsjMqEUkzOZKOU2ZgTxMline8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubpO qtmFX/DtSu9J2yevfV+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc40 w94fQH/DJ/1KsmSVwBLQLEKR1/nIDz36kmA27+1nVtX42PbEaIaFgucU4xHKx3zN mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaq8 fN17vEB+aret+PmqCiQY1Hqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUROTuBHQhRK 3XpHfGXpe/00GdW3LeifNLvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzdOcJ3aGCeA184XuPRfQhHe/Aj7q616uqB W3Kt+kMJ9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/ QCyhIRk3mx+8a1YLqK+hOMjWWBDEHX2mvbdKickK/jhwRdR/WmFOALq51phgtZlz Zed15UbPqWahJsjo09N5pp7Uq5iV0/xq4M1+/xQIYo2GIrqyat4AdB2B6K8K3xQd Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTfzH5zgneUwLwnuBAbGT3oMSQ/ OKXnhcmUGu8XvLEfU/PITvGzKr06o12/hHJtzXQ8eNPDJbvcD/okRRKZpmjH+ijp FPD/WgQ/vm09HdCWW3flhqceqfHff8ClCJYFLxsgZp4M3G+WyQTky4J8+6uTn/mj yyZ5JCZdlt42haSNqU/ynioCjh5XY4m8WMZsOJBNPjKZiUX/vqVcc+/nodl7VRZy ELk=

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



Note: The private key is encrypted and FDM does not accept encrypted private keys.

In order to unencrypt the private key, copy the encrypted private key into a file then run this **openssl** command:

```
openssl rsa -in encrypted.key -out unencrypted.key
Enter pass phrase for encrypted.key: [private-key passphrase]
writing RSA key
```

- encrypted.key is the name of the file that holds the encrypted private key.
- unencrypted.key is the name of the file that has the unencrypted key.

The unencrypted private key can show -----BEGIN RSA PRIVATE KEY----- rather than -----BEGIN ENCRYPTED PRIVATE KEY----- as seen in this example:

```
----BEGIN RSA PRIVATE KEY-----
```

```
MIIEpAIBAAKCAQEAnGpzMjuf+HtRG5ZYf80V6V1sSyF7XhRxjR180wUih5wBz6qN
ntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGbmyNz+A6jgNqAkTvaFMZV/RrW
qCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqNBqotoz3/8CrZ0IcpzVqL6h0z
iJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50QpQDTgvIiD1bYpPiWKpS0g1P
ZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZaHrP9Y0x09+MpVMH33R9vR13S
OEF6kpZ6VEdGI4s6/IRvaM1z1BcK10N/N2+mjwIDAQABAoIBAEQzCd1KMBrosdmk
eRvoMPiaemBbze2cX1JWXZ2orICSXhvM0okBGJFD0XN47ZCuVqYAq0ecjU9RzGqE
NbXYfUsD6+P91k+/Gj1RiCNLBHBwdgewzw1quTxP54zSpAV1IXyQ+Fo1TzjH1yfW
7iHhuSujYsAYLWPy4Yg3NpU2IdzeQoK5ViuSTTNx8LHYBKw1Qf7HVaQTfmsWOAyg
/vjZqjRkukqKM41srgk0/HjPnEBDuUWVTehzMCk1etijENc7ttISzYIEMNPthe60
NpidXAHoJ11JM6HB9ZraBH5fu7MZJZOOn6YVKQuCdWOWfnKiNQCDsXq7X5EWsaj3
cgyjWlkCgYEAy33k1wxp7WEqg1zEwq0Vq7AtoL6i4V9QCenMThQAHwNAAUGGOSIF
JhpKyApm/BUogSIOMzIPse+NgAA66TRn4qfkbpvTI98CeCUxiUPcbRmqZnYxC0fp
Pzosv50nBL1toI0prI02S5a261w6JGNAfD95tCjCYYrB8Cw/HbZ0LPUCgYEAxMbZ
KVyosBxaAIFQinHaff3fVSTsE0ZFpLCBbLybgLcP8LsLdahBsj6HK/hAffKXOdvM
35CAM7ZL/WCI1Jb+dx4YcD9q81bVMu4HTvS12deTZoZrBG2iFX60Ssn2rLKAH+cH
uLSHCNAj9cj9sy1dZErGLZtBQpJPtpLRd6iy0vMCgYBP/zoLYJH0BBLWeY3QioL0
cABABTG7L+EjRIpQ14QErR5oX/4IT9t+Uy+63HwH9blqqpyye6e359jUzUJbk4KT
1DU1VoT2wSETYmvK7qa1LUXT6fr12FtVw+T7m2w5azwxshDuBQmRRbq7ZBJnY61i
KwIJVUy1U/tSE9LsN1McUQKBgQClc4ykeoRbj3sdcZ2GyrQru4pMzP6wNu3Xy5EH
HI6ja0i74ImCJDcY5/o/vjx7qb39qBJa5+TjliPOp5xlI5BSF7v0pV4G5XvdlsY0
XSYWRGxriBnzXzspV3/M4oPGMVAJgve7Fg90GY4i2xx1yBH+geCf+CqnDt53ZHs7
YVz6gQKBgQDG42tZZ1kNAn0x/k11U1ZrEeF8iqdsyVcRf4fAvqsPbY3+kdae+80r
+cQpVoeWzOQLUkA6eMsiTLmcWYb62qMgdpluyKoOciPG9+2AGNTvQp/ig34pF2F/
90GuVY1A1p7mkP8Vb1Mo1ugV0zUqAIjHKiGUzBWVsx0ZsGa+SY47uw==
----END RSA PRIVATE KEY-----
```

Once the private key has been unencrypted, the identity and private key file can be uploaded, or copied and pasted into FDM with Step 3 in the Manual Enrollment section mentioned previously. The Issuing CA can be installed with the use of the Trusted CA Certificate Installation steps mentioned previously.

Verify

Use this section to confirm that your configuration works properly.

View Installed Certificates in FDM

1. Navigate to **Objects** > **Certificates**. Hover over the certificate you want to verify, and click the **view** button as shown in the image.

cisco. Fire	power Devi	ce Manager 🕅 🐨 Monitoring Policies	Objects Device: FTD-3	> 🖆 🗐 ? :	admin Administrator
Application O URLs	Filters	Certificates			
Geolocation	e e	118 objects		Q Search	+ ~
🔋 Syslog Serv	ers	• NAME	TYPE		ACTIONS
🔏 IKE Policies		1 NGFW-Default-InternalCA	Internal CA		
🐴 IPSec Propo	sals	2 DefaultInternalCertificate	Internal Certificate		
AnyConnec	t Client	3 DefaultWebserverCertificate	Internal Certificate		
📾 Identity Sou	roes	4 FTD-3-Manual	Internal Certificate		0 3
👤 Users					
A Certificates					
🔒 Secret Keys					
DNS Groups					
📲 Event List F	Iters				
🖓 SLA Monito	• •				

2. The pop-up window provides additional details about the certificate as shown in the image.

View Internal Certificate

Name

FTD-3-Manual

REPLACE CERTIFICATE

Subject Common Name ftd3.example.com

Subject Organization Cisco Systems

Subject Organization Unit TAC

Issuer Common Name VPN Root CA

Issuer Organization Cisco Systems TAC

Valid Time Range Apr 13 16:44:00 2020 GMT - Apr 13 16:44:00 2021 GMT

CANCEL	SAVE	

View Installed Certificates in CLI

You can either use the CLI Console in FDM or SSH into the FTD and run the command **show crypto ca certificates** in order to verify that a certificate is applied to the device as shown in the image.



Example output:

> show crypto ca certificates

```
Certificate
Status: Available
Certificate Serial Number: 6b93e68471084505
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=ftd3.example.com ou=TAC o=Cisco Systems Validity Date: start date: 16:44:00 UTC Apr 13 2020 end date: 16:44:00 UTC Apr 13 2021 Storage: config Associated Trustpoints: FTD-3-Manual



Note: Identity Certificates only show in the CLI when they are used with a service such as AnyConnect. Trusted CA certificates appear once they have been deployed.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Debug Commands

Debugs can be run from the diagnostic CLI after you connect the FTD via SSH in the case of an SSL Certificate Installation failure: **debug crypto ca 14**

In older versions of FTD, these debugs are available and recommended for troubleshooting:

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 255

Common Issues

Import ASA Exported PKCS12

When you attempt to extract the identity certificate and private key from an exported ASA PKCS12 in OpenSSL, you can receive an error similar to this:

```
openssl pkcs12 -info -in asaexportedpkcs12.p12
6870300:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1220:
6870300:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:386:Type=PK
```

In order to work around this, the pkcs12 file must first be converted to DER format:

openssl enc -base64 -d -in asaexportedpkcs12.p12 -out converted.pfx

Once that is done, the steps from the section Extracting Identity certificate and private key from PKCS12 file earlier in this document can be followed in order to import the identity certificate and private key.