# Migrating Certificates from ASA to Firepower Threat Defense

September 3, 2019

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

# Table of Contents

# Introduction

This document describes the procedure to migrate Identity (ID) and Certificate Authority (CA) Certificates from Cisco Adaptive Security Appliance (ASA) to Firepower Threat Defense (FTD) device.

**Note**: This document does not cover migration of CA server feature of ASA.

**Note**: For more information on creating and applying certificates on FTD, see Managing FTD Certificates.

# Pre-Requisites

- Presence of Identity (ID) Certificate on Cisco ASA.

  **Note**: In this document, Cisco ASA means that the source ASA firewall which has the ID certificate that you want to migrate to your FTD device.
- When you migrate the ID certificate from source ASA to target FTD, the **PKCS#12** format of the certificate is migrated. This format has private and public RSA keys with certificate information.
- Migration of trustpoint which only contains a CA.

# Components Used

| Components | Version |
|---|---|
| Source ASA | Version 9.x |
| Target FMC | Version 6.2.3 or later |
| Target FTD | Version 6.2.3 or later |

# Prepare the ASA for Migration

Step 1 Identify the **trustpoint** that you want to migrate from the ASA device.

```
ASA# show crypto ca trustpoints

crypto ca trustpoint SSL-Trustpoint

enrollment terminal fqdn vpn.remoteasa.com

subject-name CN=vpn.remoteasa.com,O=Company Inc,C=US,St=California,L=San Jose

keypair SSL-Keypair
```

Step 2 Note down the name of the **trustpoint**.

The trustpoint name is highlighted in bold in the above configuration sample output.

# Export ID Certificates or Trustpoint(s) from Source ASA

## Using Command Line Interface

Use the following command to export your ID certificate along with CA certificate using the CLI:

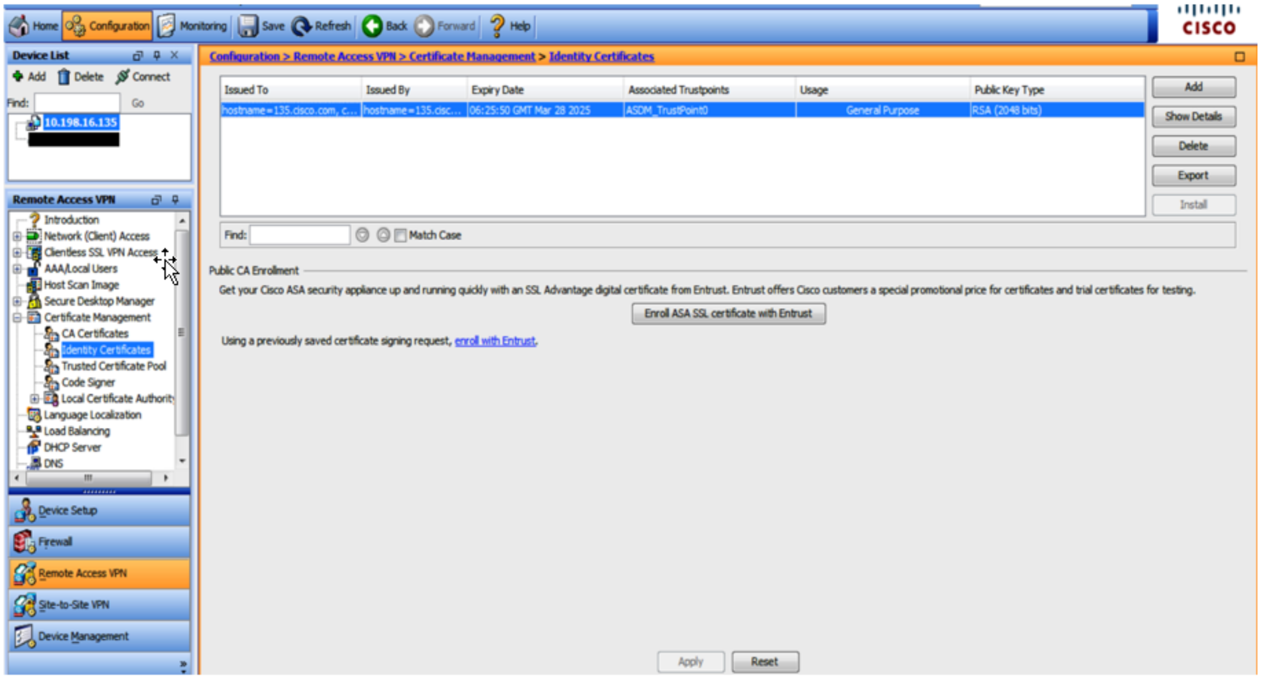
```
ASA(config)#crypto ca export <trustpoint-name> pkcs12 <passphrase>
```

**Note**: Passphrase protects the **PKSC#12** file and is required while importing the certificate in FTD.

## Using Adaptive Security Device Manager

Step 1 Navigate to **Configuration** > **Remote Access VPN** > **Certificate Management** > **Identity Certificates**.

**Figure 1 – Exporting trustpoint from ASDM**



Configuration > Remote Access VPN > Certificate Management > Identity Certificates

| Issued To | Issued By | Expiry Date | Associated Trustpoints | Usage | Public Key Type |
|---|---|---|---|---|---|
| hostname=135.cisco.com, c... | hostname=135.cisc... | 06:25:50 GMT Mar 28 2025 | ASDM_TrustPoint0 | General Purpose | RSA (2048 bits) |

Public CA Enrollment

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

Using a previously saved certificate signing request, enroll with Entrust.

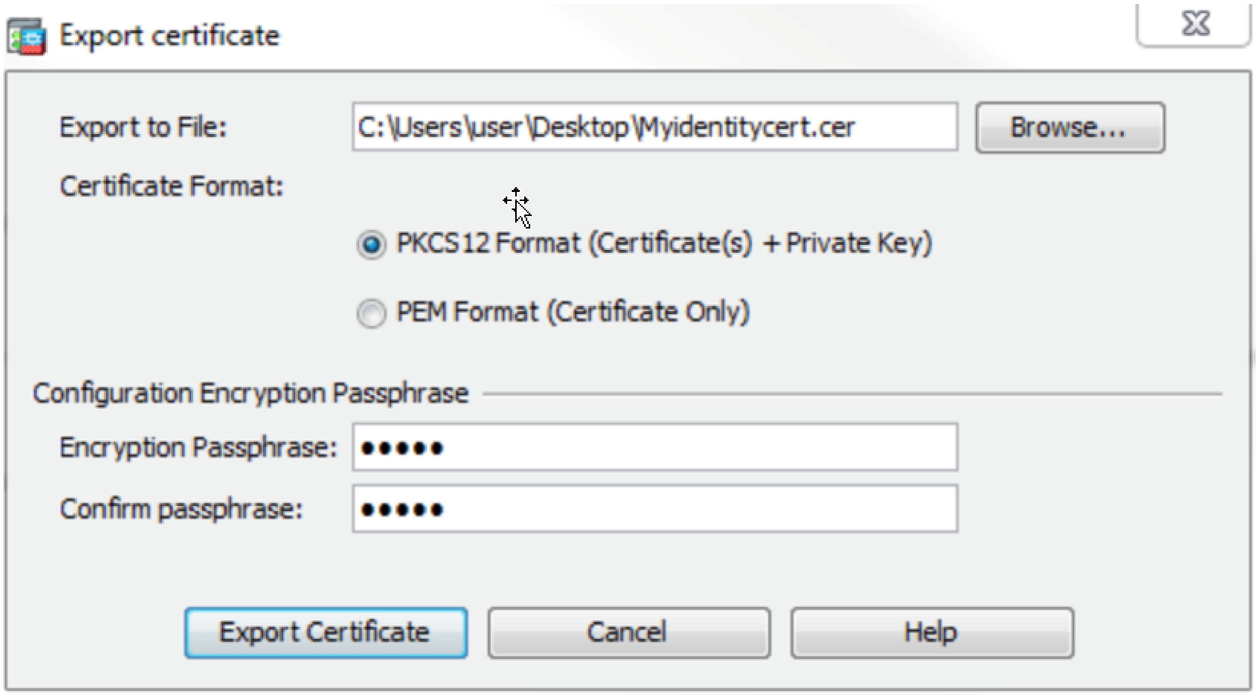
Step 2 In the **Destination** screen, you can choose the certificate that you want to migrate, and click **Export**.

Step 3 Browse the location where you want to save the certificate and perform the following:

a. Choose **PKCS#12 Format (Certificate(s) + Private Key)** option.

b. Enter the passphrase for the file as shown in Figure 2.

**Figure 2 - Export trustpoint in PKCS#12 format from ASDM**



Export certificate

Export to File: C:\Users\user\Desktop\Myidentitycert.cer

Certificate Format:

● PKCS12 Format (Certificate(s) + Private Key)

○ PEM Format (Certificate Only)

Configuration Encryption Passphrase

Encryption Passphrase: ●●●●●

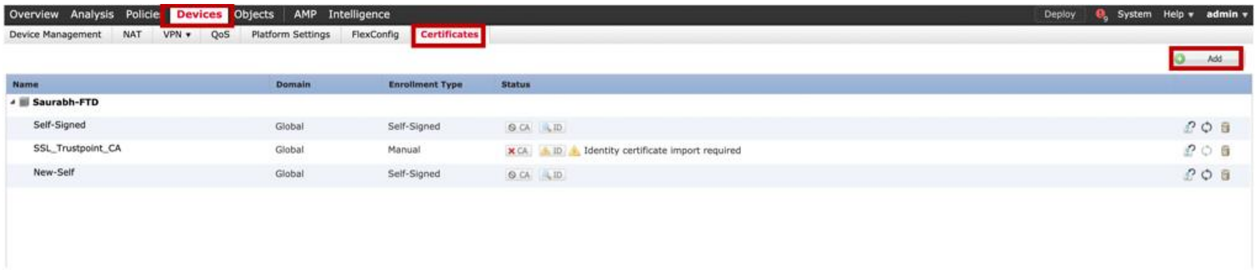
Confirm passphrase: ●●●●●

## Import Exported Certificate(s) to Target FTD

You must now have a **.p12** file in your possession. This is the certificate bundle with all its associated keys that allows you to import to the FMC by performing the following steps:

Step 1 Navigate to **Devices** > **Certificates**, and click **Add** to open a **New Certificate** dialog box.

**Figure 3 - Add Certificate Object on FMC**



| Name | Domain | Enrollment Type | Status |
|---|---|---|---|
| Saurabh-FTD | | | |
| Self-Signed | Global | Self-Signed | CA ID |
| SSL_Trustpoint_CA | Global | Manual | CA ID Identity certificate import required |
| New-Self | Global | Self-Signed | CA ID |

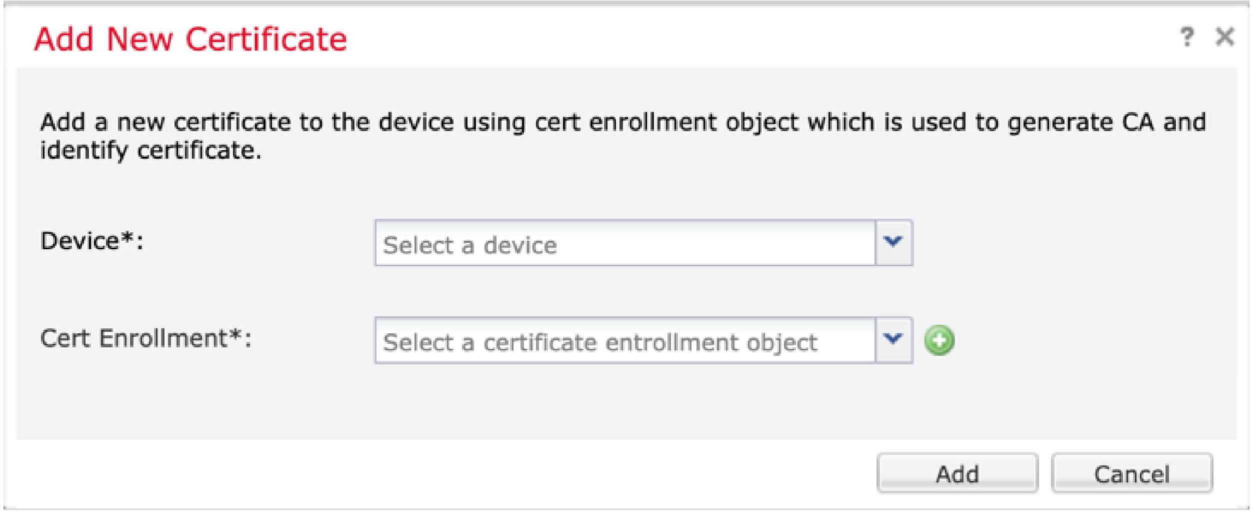
Step 2 Choose the appropriate Target FTD device from the **Device** drop-down list, and in the **Add New Certificate** screen, perform the following:

a. Choose the appropriate **Target FTD device** from the **Device** drop-down list.

b. Click the **Plus (+)** symbol to add the certificate enrollment object.

c. Click **Add** to add the object or click **Cancel** to cancel the operation.

**Figure 4 - Cert Enrollment Object on FMC**



Add New Certificate

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

Device*: Select a device

Cert Enrollment*: Select a certificate entrollment object

Step 3 In the **Add Cert Enrollment** screen, perform the following:

a. Enter the **trustpoint** name.

b. (Optional) Enter the **trustpoint** description.

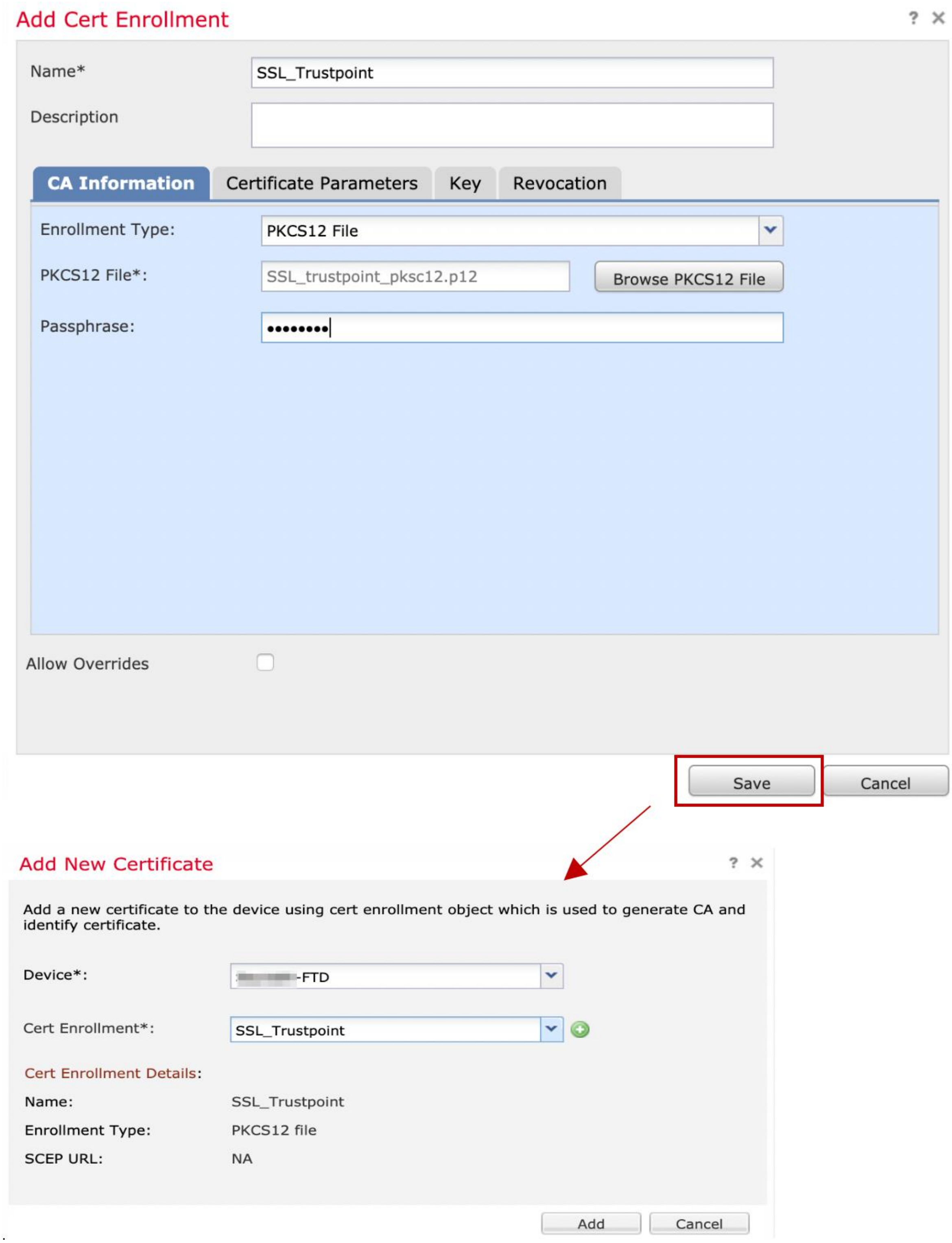
c. In the **CA Information** tab, associate a certificate enrollment object with target FTD by selecting **PKCS#12** format from the **Enrollment Type** drop-down list.

d. Browse the **.p12** file.

e. Enter the **Passphrase key**.

f. Click **Save**.

**Figure 5 – PKCS#12 File Selection**



Add Cert Enrollment

Name*: SSL_Trustpoint

Description:

Enrollment Type: PKCS12 File

PKCS12 File*: SSL_trustpoint_pksc12.p12

Passphrase: ••••••••

Allow Overrides □

Add New Certificate

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

Device*: [redacted]-FTD

Cert Enrollment*: SSL_Trustpoint

Cert Enrollment Details:

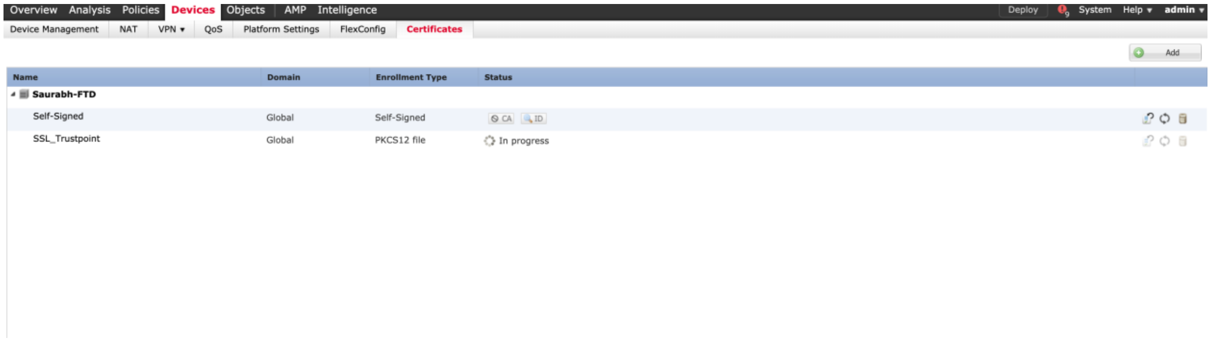
Name: SSL_Trustpoint

Enrollment Type: PKCS12 file

SCEP URL: NA

To add a new certificate, click **Add**. The **CA certificate and Identity certificate** status changes from **In Progress** to **Available** as it installs the **PKSC#12** file on the device.

**Figure 6 – Certificate Installation on FMC**

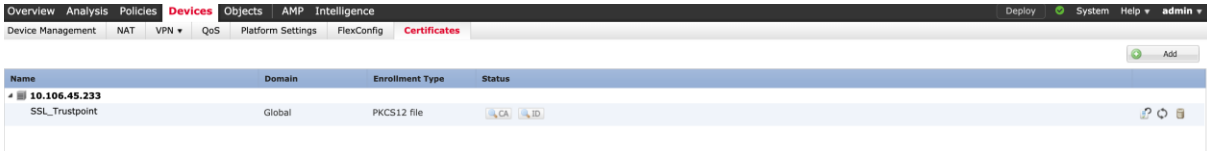


| Name | Domain | Enrollment Type | Status |
|---|---|---|---|
| Saurabh-FTD | | | |
| Self-Signed | Global | Self-Signed | CA ID |
| SSL_Trustpoint | Global | PKCS12 file | In progress |

## Verify the Identity and CA Certificate

Once the certificate status turns to **Available**, click the magnifying glass to view the Identity and CA certificate for the target FTD.

**Figure 7 - Verify Certificate Installation**



| Name | Domain | Enrollment Type | Status |
|---|---|---|---|
| 10.106.45.233 | | | |
| SSL_Trustpoint | Global | PKCS12 file | CA ID |

# Export Trustpoint which have Only CA Certificate from the Source ASA

Step 1 Execute the **show run** command to copy the **hexdump** of the certificate of the source ASA.

```
ciscoasa# sh run

: Saved

:

: Serial Number: FCH1549777C

: Hardware:         ASA5512, 4096 MB RAM, CPU Clarkdale 2792 MHz, 1 CPU (2 cores)

:

------------ omitted output ------------------ crypto ca certificate chain SSL_Trustpoint_CA certificate ca 00e54fa390fac4d43e

30820595 3082037d a0030201 02020900 e54fa390 fac4d43e 300d0609 2a864886 f70d0101 0b050030 61310b30 09060355
04061302 494e310b 30090603 5504080c 024b4131 0c300a06 03550407 0c034247 4c311030 0e060355 040a0c07 4a756e69

70657231 0d300b06 0355040b 0c045443 4f4e3116 30140603 5504030c 0d6b616e

61762e6a 756e6970 6572301e 170d3139 30343039 30393238 35355a17 0d323430

34303830 39323835 355a3061 310b3009 06035504 06130249 4e310b30 09060355

------------ omitted output ------------------
```

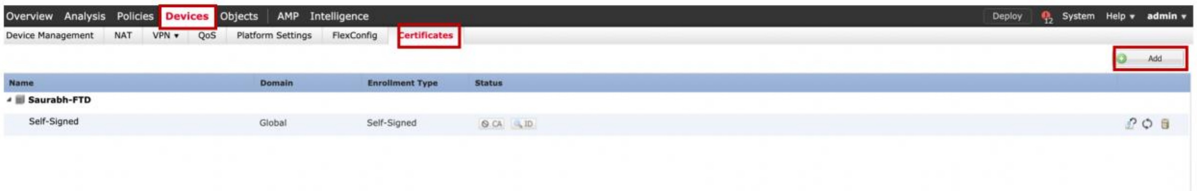
```
8919f0da c967f291 81f293d5 d9ea8d6a 4a993d59 4f0e82bb 22d6f865 06bdcc78 231060c5 46d5ea92 856851cb cee44ff9
771a1859 bcdb3710 6abbb3c7 de976d72 64d45c4e 5374f2c7 cf8aaf3b d32a0c6f 26234ce9 1347f4cf 6db5751a df892b6a
1fbe00e9 2102b038 4c8ebcca 84f85f39 f4ca59aa 4e402ff4 3a
quit
```

Step 2 Convert the **hexdump** to **base64** format.

**Note**: You can use the readily available online conversion tools.

Step 3 Navigate to **Devices** > **Certificates**, and click **Add** to open the **New Certificate** dialog box.

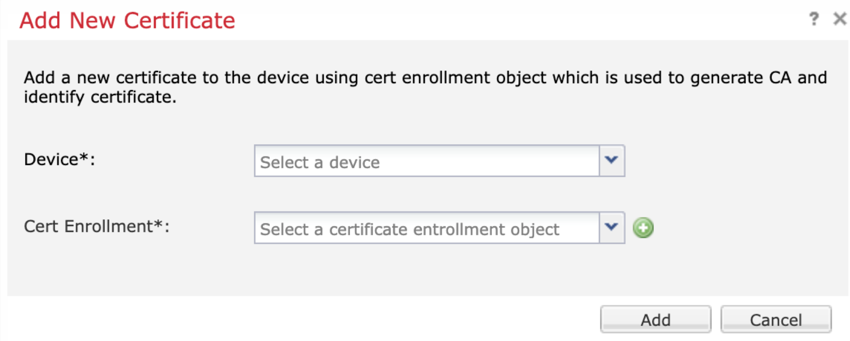
**Figure 8 – Add Certificate Object on FMC**



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

Step 4 Choose the appropriate Target FTD device from the **Device** drop-down list and click the **Plus (+)** symbol, to add the certificate enrollment object.

**Figure 9 - Cert Enrollment Object on FMC**



Add New Certificate

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

Device*: Select a device

Cert Enrollment*: Select a certificate entrollment object

Step 5 In the **Cert Enrollment** screen, perform the following:

a. Enter the **trustpoint** name.

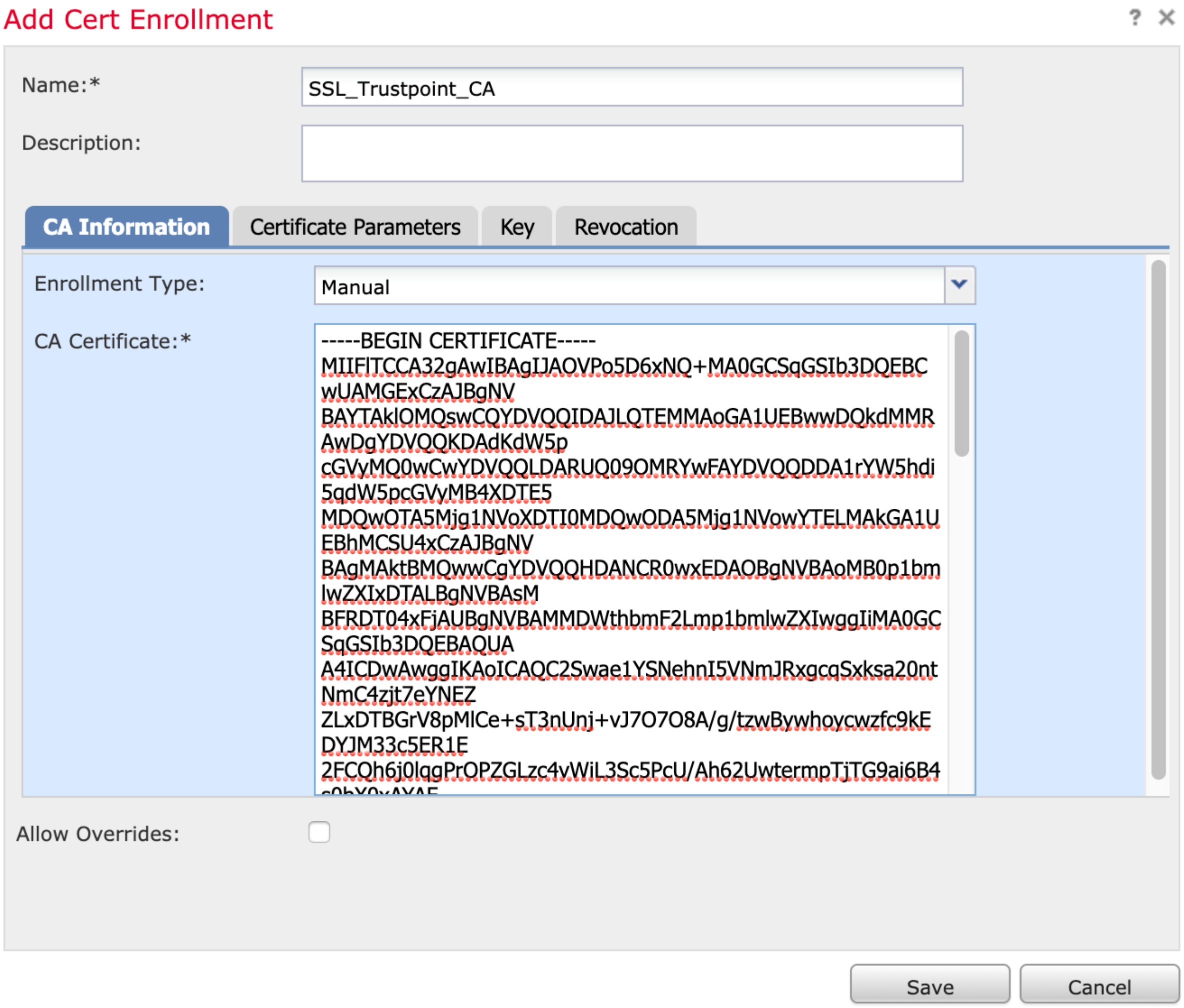
b. (Optional) Enter the **trustpoint** description.

c. In the **CA Information** tab, associate a certificate enrollment object with target FTD by selecting **Manual** from the **Enrollment** Type drop-down list.

d. Enter the **base64** format of the CA certificate in the **CA certificate** field.

e. Click **Save**.

**Figure 10 - Manual Enrollment Selection**



Add Cert Enrollment

Name:* SSL_Trustpoint_CA

Description:

Enrollment Type: Manual

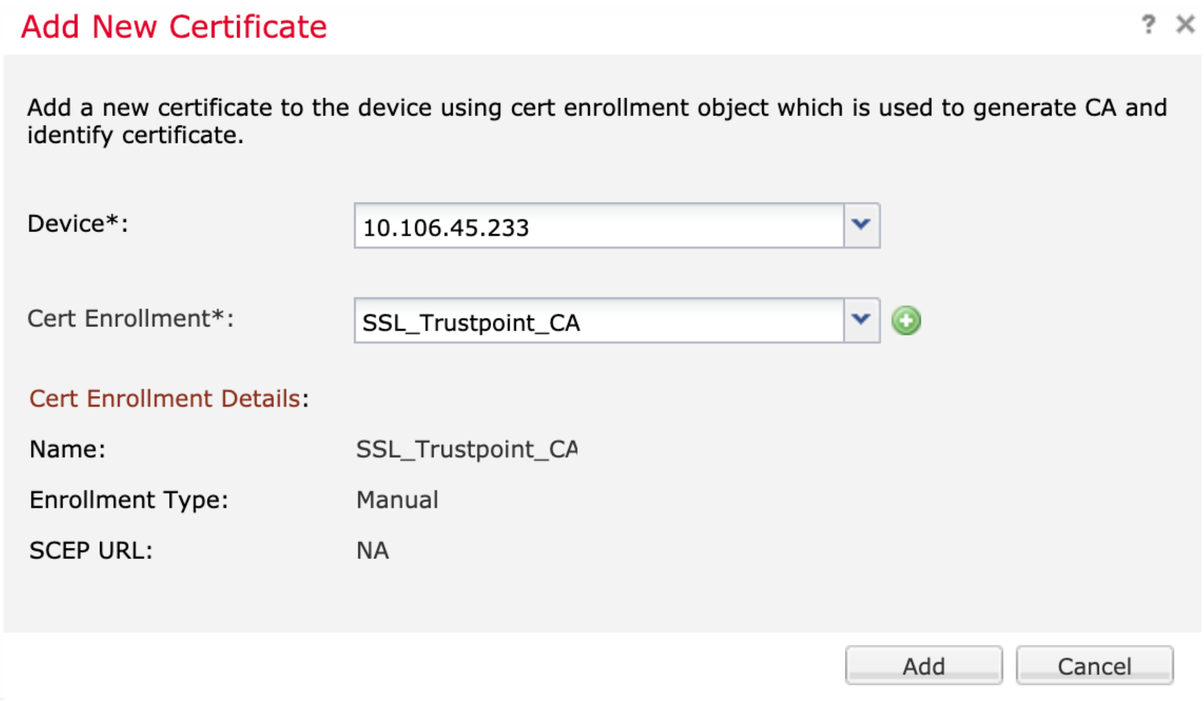
CA Certificate:*

```
-----BEGIN CERTIFICATE-----
MIIFlTCCA32gAwIBAgIJAOVPo5D6xNQ+MA0GCSqGSIb3DQEBC
wUAMGExCzAJBgNV
BAYTAklOMQswCQYDVQQIDAJLQTEMMAoGA1UEBwwDQkdMMR
AwDgYDVQQKDAdKdW5p
cGVyMQ0wCwYDVQQLDARUQ09OMRYwFAYDVQQDDA1rYW5hdi
5qdW5pcGVyMB4XDTE5
MDQwOTA5Mjg1NVoXDTI0MDQwODA5Mjg1NVowYTELMAkGA1U
EBhMCSU4xCzAJBgNV
BAgMAktBMQwwCgYDVQQHDANCR0wxEDAOBgNVBAoMB0p1bm
lwZXIxDTALBgNVBAsM
BFRDT04xFjAUBgNVBAMMDWthbmF2Lmp1bmlwZXIwggIiMA0GC
SqGSIb3DQEBAQUA
A4ICDwAwggIKAoICAQC2Swae1YSNehnI5VNmJRxgcqSxksa20nt
NmC4zjt7eYNEZ
ZLxDTBGrV8pMlCe+sT3nUnj+vJ7O7O8A/g/tzwBywhoycwzfc9kE
DYJM33c5ER1E
2FCQh6j0lqgPrOPZGLzc4vWiL3Sc5PcU/Ah62UwtermpTjTG9ai6B4
c0hY0xAYAE
```

Allow Overrides: □

Step 6 Click **Save**. Click **Add** to add the certificate enrollment object.

**Figure 11 - Add Certificate on FMC**



Add New Certificate

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

Device*: 10.106.45.233

Cert Enrollment*: SSL_Trustpoint_CA

Cert Enrollment Details:

Name: SSL_Trustpoint_CA

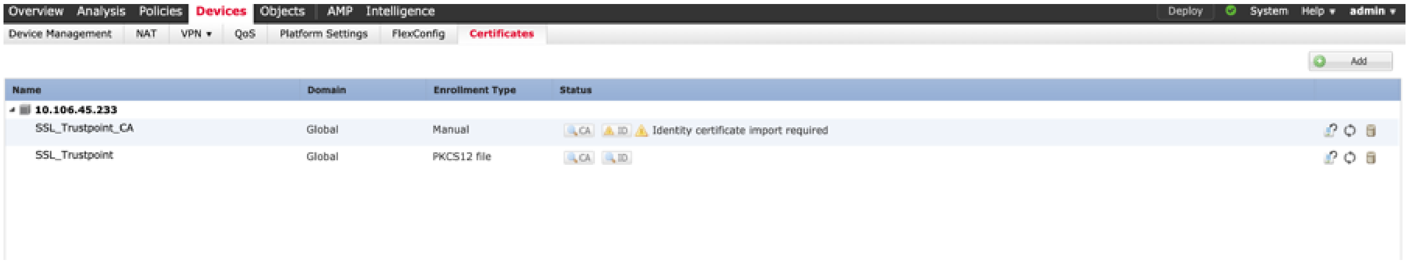
Enrollment Type: Manual

SCEP URL: NA

## Verify Certificate Object Status

You can see the status when the certificate object is complete. The trustpoint with the CA certificate is now complete.

**Figure 12 - Verify Certificate on FMC**



| Name | Domain | Enrollment Type | Status |
|---|---|---|---|
| 10.106.45.233 | | | |
| SSL_Trustpoint_CA | Global | Manual | CA ID ⚠ Identity certificate import required |
| SSL_Trustpoint | Global | PKCS12 file | CA ID |