Troubleshoot PKCS#12 File Installation Failure with Non-FIPS Compliant PBE Algorithms

Contents

[Introduction](#)
[Background Information](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Problem](#)
[Solution](#)
[Verification](#)

Introduction

This document describes how to troubleshoot the installation failure of a Public Key Cryptography Standards (PKCS)#12 file with non-Federal Information Processing Standard (FIPS) compliant Password-Based Encryption (PBE) algorithms via Cisco Firepower Management Center (FMC). It explains a procedure to identify it and to create a new compliant bundle with OpenSSL.

Background Information

The Cisco Firepower Threat Defense (FTD) supports compliance with FIPS 140 when you enable Common Criteria (CC) or Unified Capabilities Approved Products List (UCAP) mode on a managed device. This configuration is part of a FMC Platform Settings policy. After applied, the **fips enable** command appears in the **show running-config** output of FTD.

PKCS#12 defines a file format used to bundle a private key and the respective identity certificate. There is the option to include any root or intermediate certificate that belongs to the validation chain as well. PBE algorithms protect the certificates and private key portions of the PKCS#12 file. As a result of the combination of the Message Authentication Scheme (MD2/MD5/SHA1) and the Encryption scheme (RC2/RC4/DES), there are multiple PBE algorithms but the only one that is FIPS compliant is PBE-SHA1-3DES.

> **Note**: To learn more about FIPS in Cisco products navigate to FIPS 140.

> **Note**: To learn more about the security certifications standards available for FTD and FMC navigate to the **Security Certifications Compliance** chapter of the FMC Configuration Guide.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Public Key Infrastructure (PKI)
- OpenSSL

Components Used

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

- FMCv - 6.5.0.4 (build 57)
- FTDv - 6.5.0 (build 115)

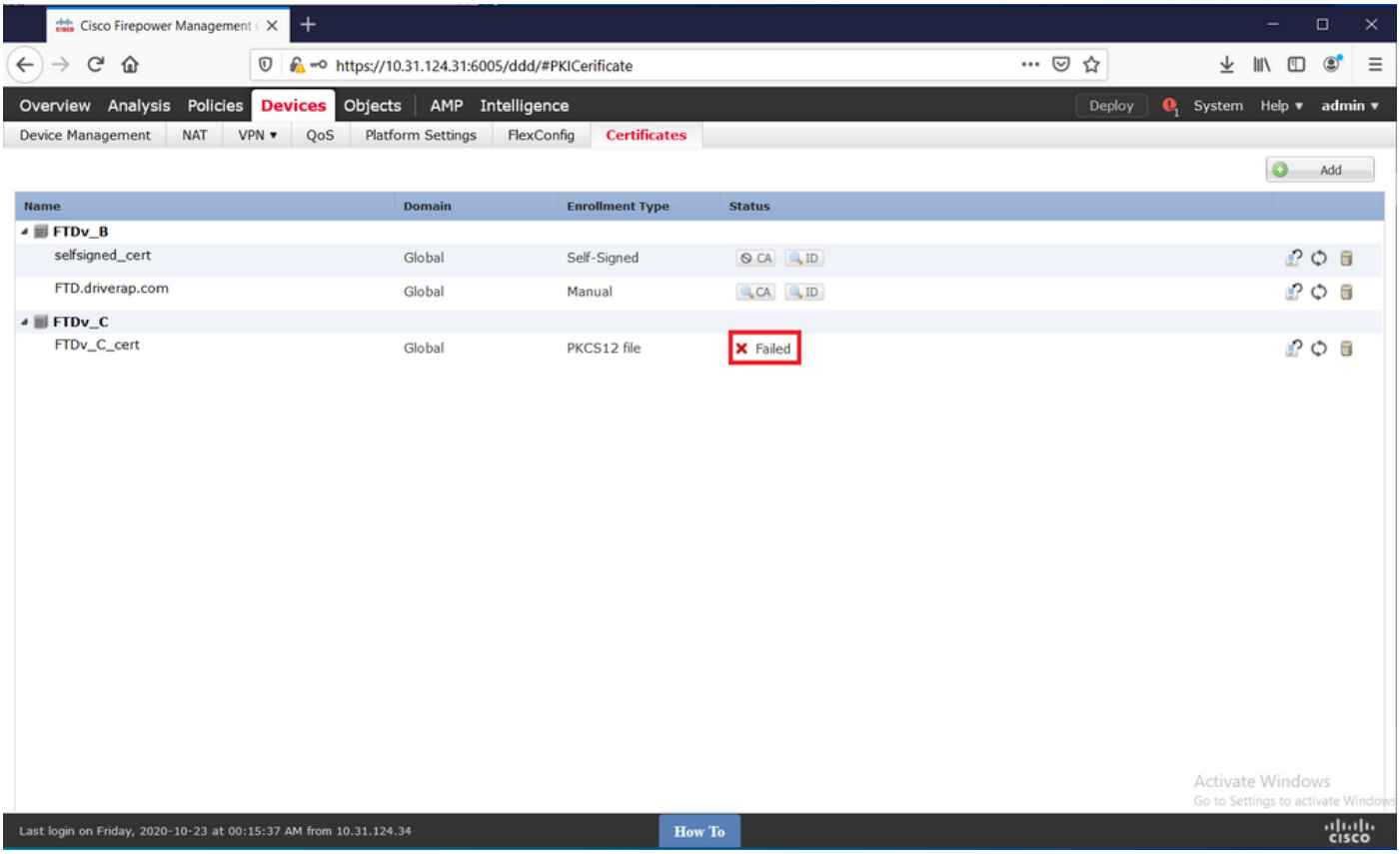
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

> **Note**: The approach described in this document can be implemented to any other platform with a similar issue, for instance, a Cisco Adaptive Security Appliance (ASA), since the issue is with the certificate being non-FIPS compliant.

> **Note**: This document does not address the condition where the PKCS#12 components themselves are not compliant by any other reason like the Rivest, Shamir, Adleman (RSA) key length or the Signature algorithm used to sign the identity certificate. In such cases, certificates need to be re-issued to be FIPS compliant.

Problem

When FIPS mode is enabled in FTD, certificate installation might fail if the PBE algorithms used to protect the PKCS#12 file are not FIPS compliant.



Note: Find a step-by-step procedure on how to install a PKCS#12 file using the FMC in **PKCS12 Enrollment** section of Certificate Installation and Renewal on FTD managed by FMC.

If certificate installation fails for this reason, PKI debugs prints error below:

```
firepower# debug crypto ca 14
firepower# show debug
debug crypto ca enabled at level 14
Conditional debug filters:
Conditional debug features:

firepower# PKI[13]: crypto_parsepkcs12, pki_ossl_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_ossl_pkcs12.c:1414
PKI[4]: Error unpacking pkcs7 encrypted data
PKI[1]: error:060A60A3:digital envelope routines:FIPS_CIPHERINIT:disabled for fips in fips_enc.c
line 143.
PKI[1]: error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen failure in evp_pbe.c
line 203.
PKI[1]: error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit error in
p12_decr.c line 93.
PKI[1]: error:2306A075:PKCS12 routines:PKCS12_item_decrypt_d2i:pkcs12 pbe crypt error in
p12_decr.c line 145.
PKI[4]: pkcs7 encryption algorithm may not be fips compliant
PKI[4]: Error unpacking pkcs12 struct to extract keys and certs
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list is NULL
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list label: FTDv_C_cert
PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list label: FTDv_C_cert
```

You can also confirm with OpenSSL that the PKCS#12 at hand includes non-compliant FIPS PBE algorithms.

```
OpenSSL> pkcs12 -info -in ftdv_C_.p12 -noout
Enter Import Password:
MAC Iteration 2048
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Certificate bag
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
```

In previous output there are two PBE algorithms, pbeWithSHA1And40BitRC2-CBC and pbeWithSHA1And3-KeyTripleDES-CBC, which protect the certificates and private key respectively. The first one is not FIPS compliant.

Solution

The solution is to configure PBE-SHA1-3DES algorithm for both certificate and private key protection. In the above example, only the certificate algorithm needs to be changed. First, you need to get the Privacy-Enhanced Mail (PEM) version of the original PKCS#12 file leveraging OpenSSL.

```
OpenSSL> pkcs12 -in ftdv_C_.p12 -out ftdv_C_.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Last, you need to use below command with the FIPS compliant PBE algorithm using the PEM file obtained in the previous step to generate a brand new PKCS#12 file:

```
OpenSSL> pkcs12 -certpbe PBE-SHA1-3DES -export -in ftdv_C_.pem -out ftdv_C_FIPS_compliant.p12
Enter pass phrase for ftdv_C_.pem:
Enter Export Password:
Verifying - Enter Export Password:
unable to write 'random state'
```

> **Note**: If the algorithm to protect the private key needs to be changed as well, you can append the **-keypbe** keyword followed by **PBE-SHA1-3DES** to the same command: **pkcs12 -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -export -in -out -out *<PKCS12 cert file>*.**

Verification

Use the same OpenSSL command to obtain information about the PKCS#12 file structure to confirm FIPS algorithms are in use:

```
OpenSSL> pkcs12 -info -in ftdv_C_FIPS_compliant.p12 -noout
Enter Import Password:
MAC Iteration 2048
```

```
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Certificate bag
Certificate bag
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
```

Now PKI debugs shows output below when certificate installation succeeds.

```
PKI[13]: crypto_parsepkcs12, pki_ossl_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_ossl_pkcs12.c:1414
PKI[13]: pki_unpack_bags, pki_ossl_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_cert, pki_ossl_pkcs12.c:1284
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_cert, pki_ossl_pkcs12.c:1284
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[13]: pki_unpack_bags, pki_ossl_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_key, pki_ossl_pkcs12.c:1252
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[14]: compare_key_ids, pki_ossl_pkcs12.c:1150
PKI[12]: transfer_p12_contents_to_asa, pki_ossl_pkcs12.c:375
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list is NULL

CRYPTO_PKI: examining router cert:
CRYPTO_PKI: issuerName=/O=Cisco/OU=TAC/CN=RootCA_C1117
CRYPTO_PKI: subjectname=/CN=ftdv/unstructuredName=C1117_DRIVERAP.driverap.com
CRYPTO_PKI: key type is RSAPKI[13]: GetKeyUsage, pki_ossl_pkcs12.c:278

CRYPTO_PKI: bitValue of ET_KEY_USAGE = a0
CRYPTO_PKI: Certificate Key Usage = GENERAL_PURPOSE
CRYPTO_PKI: adding RSA Keypair
CRYPTO_PKI: adding as a router certificate.
CRYPTO_PKI: InsertCertData: subject name =

30 3b 31 0d 30 0b 06 03 55 04 03 13 04 66 74 64 76 31 2a 30
28 06 09 2a 86 48 86 f7 0d 01 09 02 16 1b 43 31 31 31 37 5f
44 52 49 56 45 52 41 50 2e 64 72 69 76 65 72 61 70 2e 63 6f
6d
CRYPTO_PKI: InsertCertData: issuer name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
CRYPTO_PKI: InsertCertData: serial number = 16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Inserted cert into list.PKI[14]: pki_ossl_set_cert_store_dirty,
pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[9]: Cleaned PKI cache successfully
PKI[9]: Starting to build the PKI cache
PKI[4]: No identity cert found for TP: FTDv_C_FIPS_Compliant
PKI[4]: Failed to cache certificate chain for the trustpoint FTDv_C_FIPS_Compliant or none
available
```

```
PKI[13]: CERT_GetTrustedIssuerNames, vpn3k_cert_api.c:1760
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[4]: Failed to retrieve trusted issuers list or no trustpoint configured
PKI[13]: CERT_FreeTrustedIssuerNames, vpn3k_cert_api.c:1782
PKI[13]: crypto_pkcs12_add_sync_record, pki_ossl_pkcs12.c:144
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant

CRYPTO_PKI(Cert Lookup) issuer="cn=RootCA_C1117,ou=TAC,o=Cisco" serial number=16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.

CRYPTO_PKI: ID cert in trustpoint FTDv_C_FIPS_Compliant successfully validated with CA cert.

CRYPTO_PKI: crypto_pki_authenticate_tp_cert()

CRYPTO_PKI: trustpoint FTDv_C_FIPS_Compliant authentication status = 0

CRYPTO_PKI: InsertCertData: subject name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
CRYPTO_PKI: InsertCertData: issuer name =

30 35 31 0e 30 0c 06 03 55 04 0a 13 05 43 69 73 63 6f 31 0c
30 0a 06 03 55 04 0b 13 03 54 41 43 31 15 30 13 06 03 55 04
03 0c 0c 52 6f 6f 74 43 41 5f 43 31 31 31 37
CRYPTO_PKI: InsertCertData: serial number = 01 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
17 9d 0e b0 15 9d cd a2 5a 01 95 bf c6 8c 4f 2e | ........Z.....O.

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Inserted cert into list.PKI[14]: pki_ossl_set_cert_store_dirty,
pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[9]: Cleaned PKI cache successfully
PKI[9]: Starting to build the PKI cache

CRYPTO_PKI(Cert Lookup) issuer="cn=RootCA_C1117,ou=TAC,o=Cisco" serial number=16 | .

CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.
PKI[7]: Get Certificate Chain: number of certs returned=2
PKI[13]: CERT_GetDNbyBuffer, vpn3k_cert_api.c:993
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[7]: Built trustpoint cache for FTDv_C_FIPS_Compliant
PKI[13]: CERT_GetTrustedIssuerNames, vpn3k_cert_api.c:1760
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[9]: Added 1 issuer hashes to cache.
PKI[13]: CERT_FreeTrustedIssuerNames, vpn3k_cert_api.c:1782
PKI[13]: crypto_pkcs12_free_sync_record, pki_ossl_pkcs12.c:113
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
PKI[14]: pki_ossl_set_cert_store_dirty, pki_ossl_certstore.c:38
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:41
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant

CRYPTO_PKI: certificate data
```

```
<omitted output>
CRYPTO_PKI: status = 0: failed to get extension from cert

CRYPTO_PKI: certificate data
<omitted output>
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
```

Finally, the FMC shows both CA and Identity certificates as available: