Solución de problemas de falla de instalación de archivos PKCS#12 con algoritmos PBE que no cumplen con FIPS

Contenido

Introducción

Este documento describe cómo resolver el problema de la falla de instalación de un archivo PKCS (Public Key Cryptography Standards)#12 con algoritmos de cifrado basado en contraseña (PBE) no conformes con el estándar de procesamiento de información (FIPS) a través de Cisco Firepower Management Center (FMC). Explica un procedimiento para identificarlo y crear un nuevo paquete compatible con OpenSSL.

Antecedentes

Cisco Firepower Threat Defense (FTD) admite el cumplimiento de FIPS 140 cuando se activa el modo Common Criteria (CC) o Unified Capabilities Aprobated Products List (UCAP) en un dispositivo administrado. Esta configuración forma parte de una política de configuración de plataforma FMC. Después de aplicar, el comando **fips enable** aparece en el resultado **show running-config** de FTD.

PKCS#12 define un formato de archivo utilizado para agrupar una clave privada y el certificado de identidad correspondiente. Existe la opción de incluir cualquier certificado raíz o intermedio que también pertenezca a la cadena de validación. Los algoritmos PBE protegen los certificados y las partes de clave privada del archivo PKCS#12. Como resultado de la combinación del esquema de autenticación de mensajes (MD2/MD5/SHA1) y el esquema de cifrado (RC2/RC4/DES), hay varios algoritmos PBE, pero el único que cumple con FIPS es PBE-SHA1-3DES.

> **Nota:** Para obtener más información sobre FIPS en los productos de Cisco, navegue hasta FIPS 140.

> **Nota:** Para obtener más información sobre los estándares de certificaciones de seguridad disponibles para FTD y FMC, vaya al capítulo **Cumplimiento de Certificaciones de Seguridad** de la Guía de Configuración de FMC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Public Key Infrastructure (PKI)
- OpenSSL

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

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

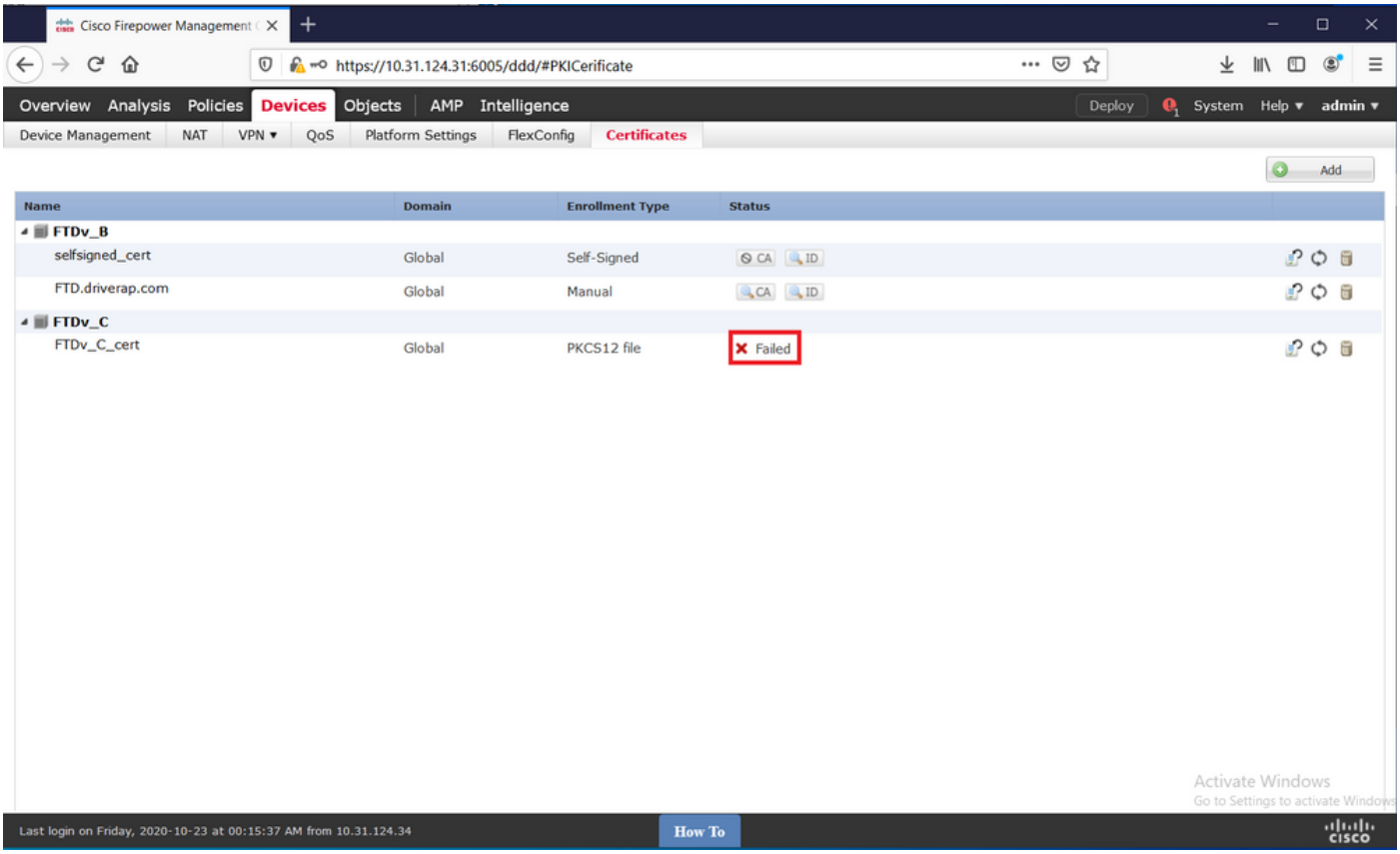
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

> **Nota:** El enfoque descrito en este documento se puede implementar en cualquier otra plataforma con un problema similar, por ejemplo, un Cisco Adaptive Security Appliance (ASA), ya que el problema es que el certificado no cumple con FIPS.

> **Nota:** Este documento no aborda la condición en la que los propios componentes PKCS#12 no cumplen con ninguna otra razón como la longitud de la clave Rivest, Shamir, Adleman (RSA) o el algoritmo de firma utilizado para firmar el certificado de identidad. En tales casos, es necesario volver a expedir los certificados para que cumplan con los requisitos de FIPS.

Problema

Cuando se habilita el modo FIPS en FTD, la instalación del certificado podría fallar si los algoritmos PBE utilizados para proteger el archivo PKCS#12 no cumplen con FIPS.



Nota: Busque un procedimiento paso a paso sobre cómo instalar un archivo PKCS#12 mediante la sección **Inscripción** en **PKCS12 de** Instalación y Renovación de Certificados en FTD administrado por FMC.

Si la instalación del certificado falla por esta razón, las depuraciones de PKI imprimen el siguiente error:

```
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
```

También puede confirmar con OpenSSL que PKCS#12 incluye algoritmos PBE de FIPS no conformes.

```
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
```

En la salida anterior hay dos algoritmos PBE, pbeWithSHA1And40BitRC2-CBC y pbeWithSHA1And3-KeyTripleDES-CBC, que protegen los certificados y la clave privada respectivamente. El primero no cumple con FIPS.

Solución

La solución es configurar el algoritmo PBE-SHA1-3DES para la protección de certificado y de clave privada. En el ejemplo anterior, sólo es necesario cambiar el algoritmo del certificado. En primer lugar, debe obtener la versión de Correo Mejorado en Privacidad (PEM) del archivo PKCS#12 original que utiliza 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:
```

Por último, debe utilizar el siguiente comando con el algoritmo PBE compatible con FIPS utilizando el archivo PEM obtenido en el paso anterior para generar un nuevo archivo PKCS#12:

```
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'
```

> **Nota:** Si el algoritmo para proteger la clave privada también necesita ser cambiado, puede anexar la palabra clave **-keypbe** seguida de **PBE-SHA1-3DES** al mismo comando: **pkcs12 -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -export -in -out -out *<PKCS12 cert file>*** .

Verificación

Utilice el mismo comando OpenSSL para obtener información sobre la estructura de archivos PKCS#12 para confirmar que los algoritmos FIPS están en uso:

```
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
```

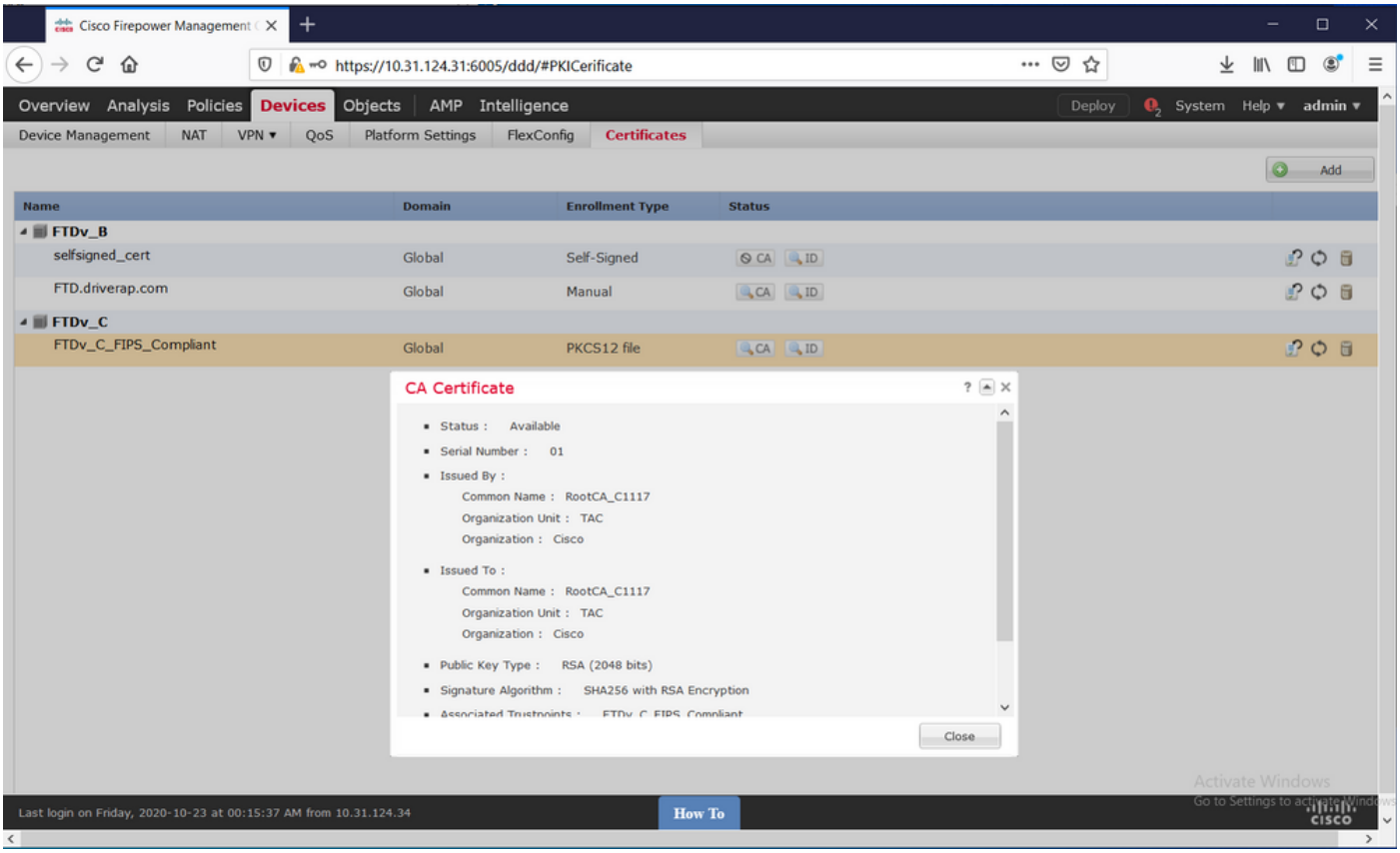
Ahora, las depuraciones PKI muestran el resultado siguiente cuando la instalación del certificado se realiza correctamente.

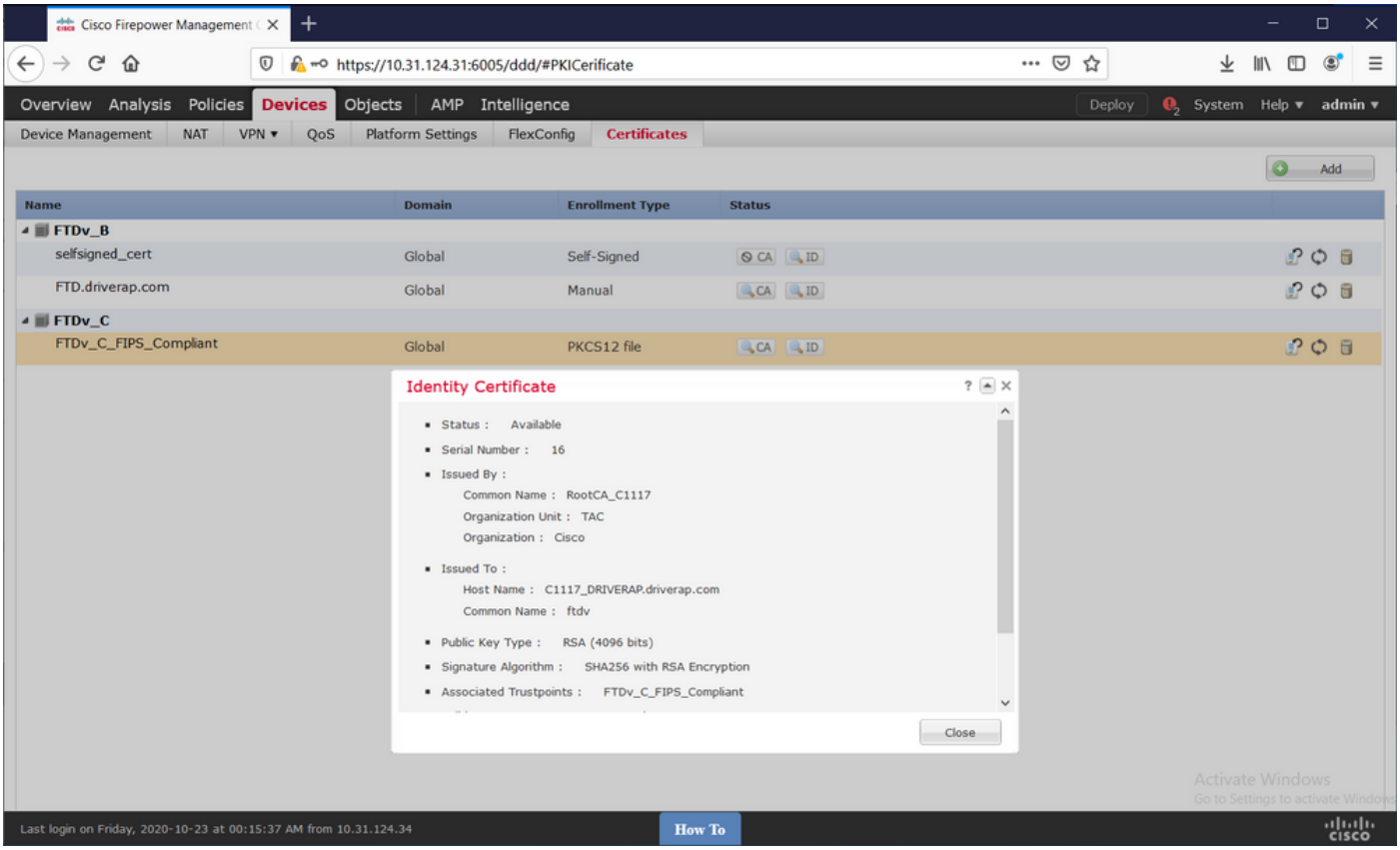
```
PKI[13]: crypto_parsepkcs12, pki_ossl_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_ossl_pkcs12.c:1414
PKI[13]: pki_unpack_bags, pki_ossl_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_cert, pki_ossl_pkcs12.c:1284
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[13]: pki_unpack_bag, 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
```

Por último, FMC muestra los certificados de CA e identidad como disponibles:




Cisco Firepower Management
https://10.31.124.31:6005/ddd/#PKICerificate
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
FTDv_B
selfsigned_cert Global Self-Signed CA ID
FTD.driverap.com Global Manual CA ID
FTDv_C
FTDv_C_FIPS_Compliant Global PKCS12 file CA ID
Identity Certificate
Status : Available
Serial Number : 16
Issued By :
Common Name : RootCA_C1117
Organization Unit : TAC
Organization : Cisco
Issued To :
Host Name : C1117_DRIVERAP.driverap.com
Common Name : ftdv
Public Key Type : RSA (4096 bits)
Signature Algorithm : SHA256 with RSA Encryption
Associated Trustpoints : FTDv_C_FIPS_Compliant
Close
Activate Windows
Last login on Friday, 2020-10-23 at 00:15:37 AM from 10.31.124.34
How To