使用不符合FIPS的PBE算法排除PKCS#12文件安装故障

目录

[简介](#)

[背景信息](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[问题](#)

[解决方案](#)

[确认](#)

简介

本文档介绍如何通过Cisco Firepower管理中心(FMC)使用非联邦信息处理标准(FIPS)兼容的基于密码的加密(PBE)算法对公钥加密标准(PKCS)#12文件的安装故障进行故障排除。 本章介绍使用OpenSSL识别该捆绑包和创建新合规性捆绑包的过程。

背景信息

在受管设备上启用通用标准(CC)或统一功能批准产品列表(UCAP)模式时，Cisco Firepower威胁防御(FTD)支持符合FIPS 140。此配置是FMC平台设置策略的一部分。应用后，fips enable命令将显示在FTD的show running-config输出中。

PKCS#12定义用于捆绑私钥和相应身份证书的文件格式。也可以选择包括属于验证链的任何根证书或中间证书。PBE算法保护PKCS#12文件的证书和私钥部分。由于消息身份验证方案(MD2/MD5/SHA1)和加密方案(RC2/RC4/DES)的组合，存在多个PBE算法，但唯一一个符合FIPS的算法是PBE-SHA1-3DES。

注意：要了解有关思科产品中FIPS的更多信息，请导至FIPS 140。

注意：要了解可用于FTD和FMC的安全认证标准的详细信息，请导航至FMC配置指南的安全认证合规性一章。

先决条件

要求

Cisco 建议您了解以下主题：

- 公用密钥基础结构 (PKI)
- OpenSSL

使用的组件

本文档中的信息基于以下软件版本：

- FMCv - 6.5.0.4（内部版本57）
- FTDv - 6.5.0（内部版本115）

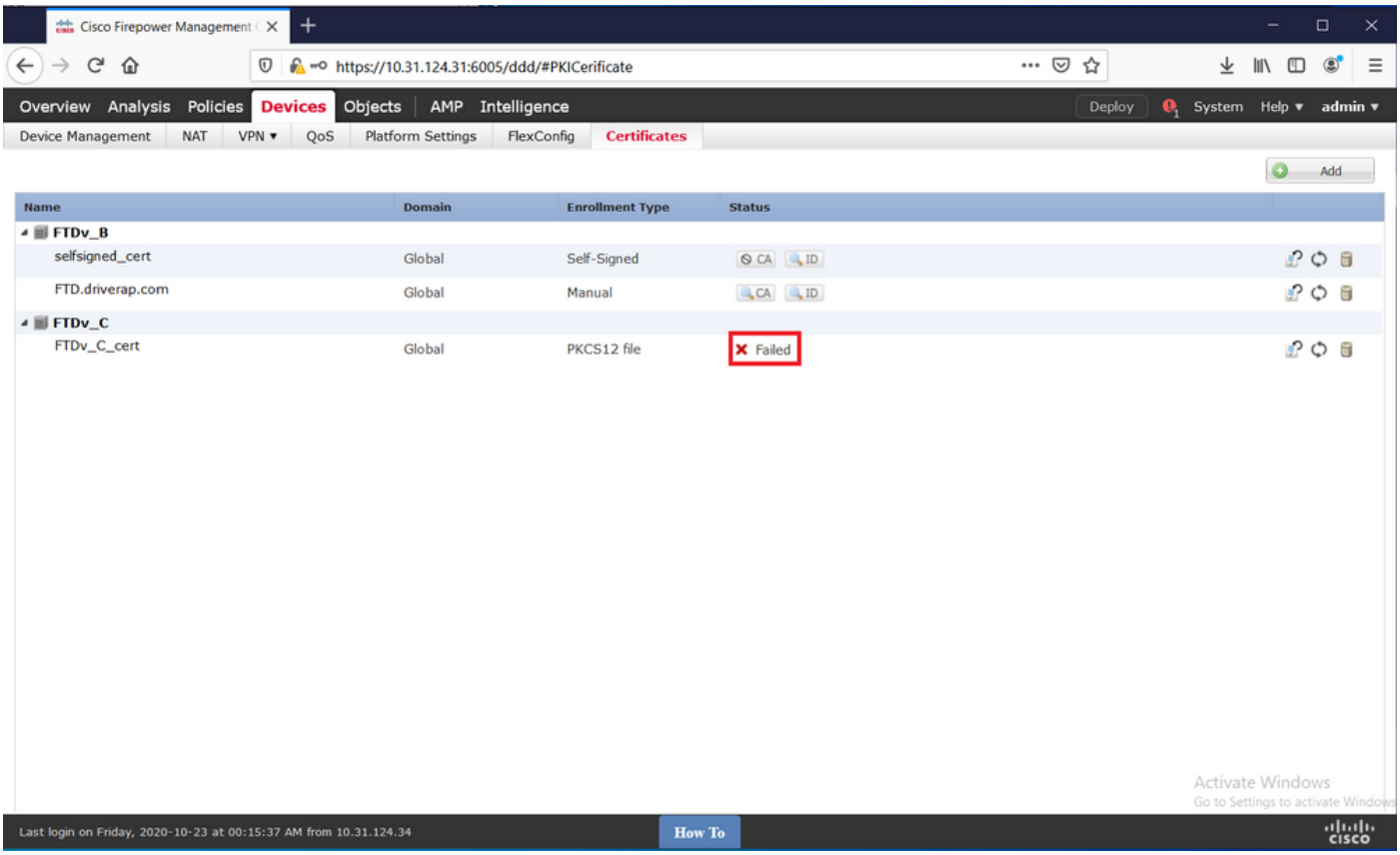
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

注意：本文档中描述的方法可以实施到存在类似问题的任何其他平台，例如，思科自适应安全设备(ASA)，因为问题在于证书不符合FIPS。

注意：本文档不讨论PKCS#12组件本身由于任何其他原因(如Rivest、Shamir、Adleman(RSA)密钥长度或用于签署身份证书的签名算法)而不符合的条件。在这种情况下，需要重新颁发证书以符合FIPS。

问题

在FTD中启用FIPS模式时，如果用于保护PKCS#12文件的PBE算法不符合FIPS，则证书安装可能会失败。



注意：在FMC管理的FTD上的证书安装和续订的PKCS12 Enrollment部分中，查找有关如何使用FMC安装PKCS#12文件的分步过程。

如果由于此原因导致证书安装失败，PKI调试会打印以下错误：

```
<#root>

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 1
PKI[1]: error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen failure in evp_pbe.c line 20
PKI[1]: error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit error in p12_decr.c lin
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
```

您还可以使用OpenSSL确认手头的PKCS#12包含不合规的FIPS PBE算法。

```
<#root>

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
```

在前面的输出中有两个PBE算法，pbeWithSHA1和40BitRC2-CBC和pbeWithSHA1And3-KeyTripleDES-CBC，分别保护证书和私钥。第一个不符合FIPS。

解决方案

解决方案是为证书和私钥保护配置PBE-SHA1-3DES算法。在上述示例中，仅需要更改证书算法。首先，您需要使用OpenSSL获取原始PKCS#12文件的Privacy-Enhanced Mail(PEM)版本。

```
<#root>

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:
```

最后，您需要使用上一步中获得的PEM文件，将以下命令与兼容FIPS的PBE算法配合使用，以生成全新的PKCS#12文件：

<#root>

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'
```

注意：如果保护私钥的算法也需要更改，您可以在同一命令中添加-keypbe关键字，后跟PBE-SHA1-3DES:pkcs12 -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -export -in -out -out <PKCS12证书文件>。

确认

使用相同的OpenSSL命令获取有关PKCS#12文件结构的信息，以确认正在使用FIPS算法：

<#root>

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
```

现在，当证书安装成功时，PKI调试将显示以下输出。

```
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 | .

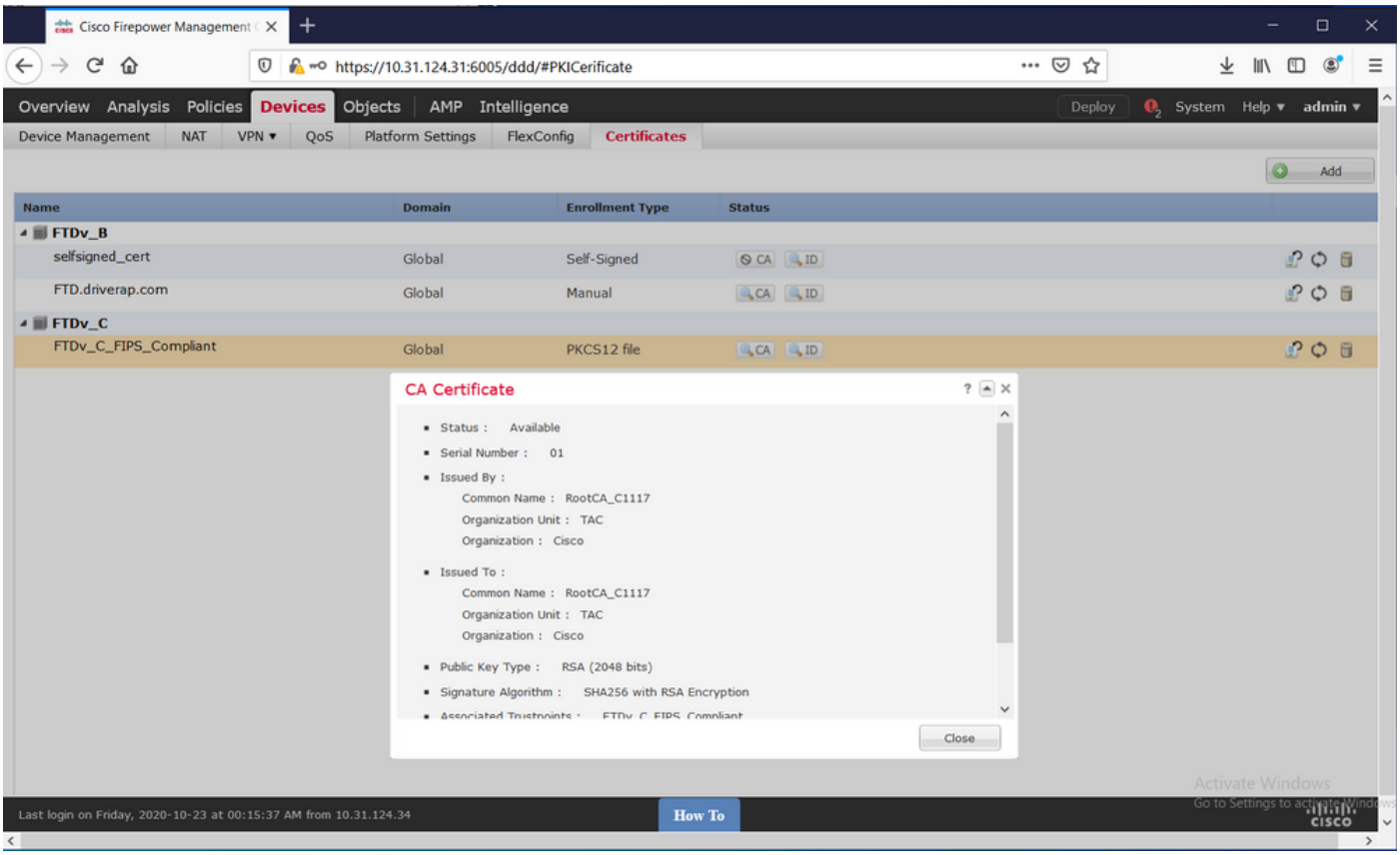
CRYPTO_PKI: looking for cert in handle=0x00002abdcb8cac50, digest=
aa 49 1e c2 c1 d5 30 60 4a 88 57 c8 3d 4e 3c 1c | .I....0`J.W.=N<.
PKI[7]: Get Certificate Chain: number of certs returned=2
PKI[13]: CERT_GetDNbyBuffer, vpn3k_cert_api.c:993
PKI[14]: map_status, vpn3k_cert_api.c:2229
PKI[7]: Built trustpoint 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

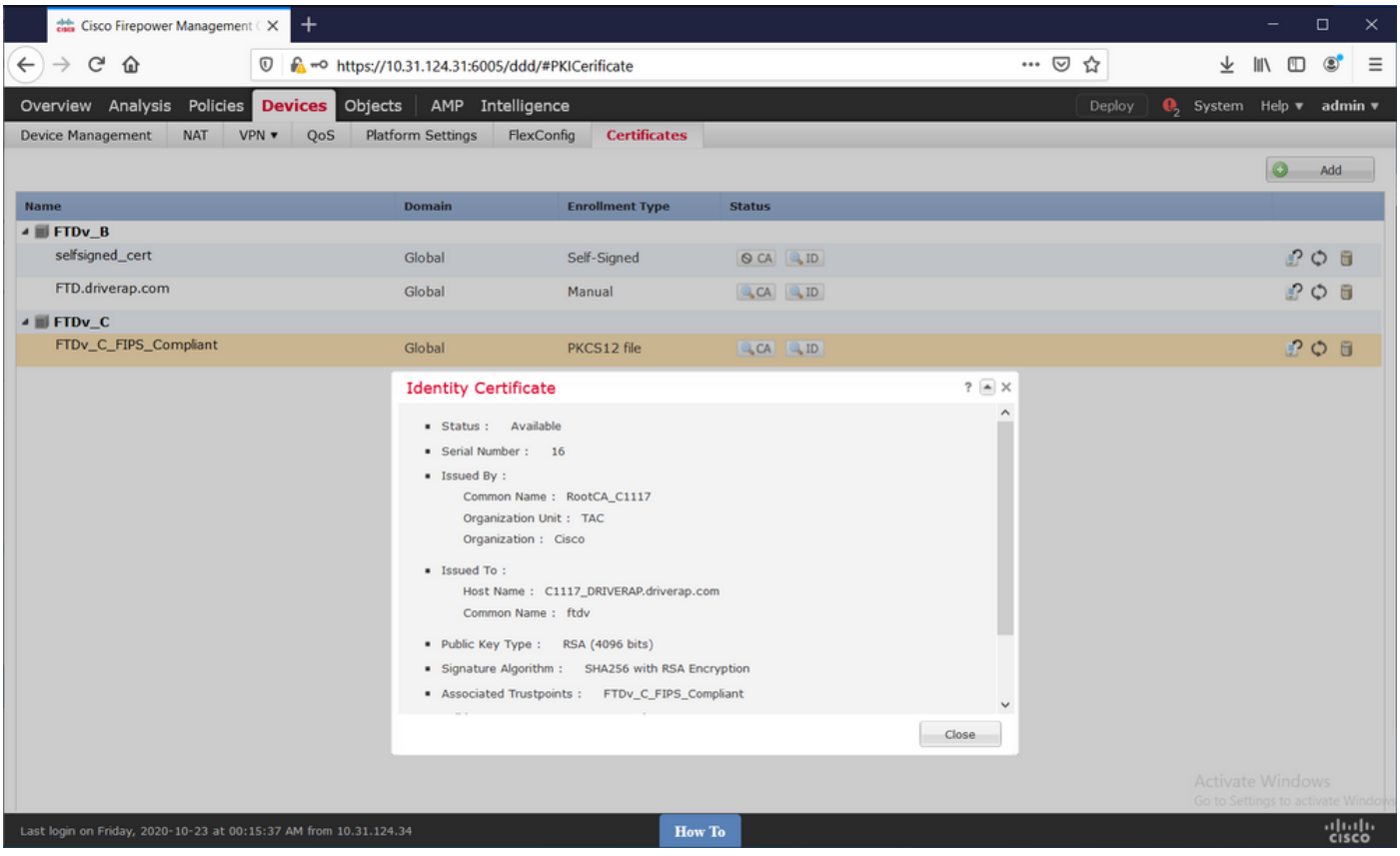
CRYPTO_PKI: certificate data
<omitted output>
CRYPTO_PKI: status = 0: failed to get extension from cert

CRYPTO_PKI: certificate data
<omitted output>
```

```
PKI[13]: label: FTDv_C_FIPS_Compliant
PKI[13]: TP list label: FTDv_C_FIPS_Compliant
```

最后，FMC显示CA和身份证书均可用：





关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。