أستكشاف أخطاء تثبيت ملفات PKCS#12 وإصلاحها باستخدام خوارزميات PBE غير المتوافقة مع معايير FIPS

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء تثبيت ملف معايير تشفير المفاتيح العامة (PKCS)#12 وإصلاحها باستخدام خوارزميات التشفير القائمة على كلمة المرور (PBE) المتوافقة مع معايير معالجة المعلومات غير الفيدرالية (FIPS) عبر مركز إدارة الطاقة الناري (FMC) من Cisco. وهو يشرح إجراء لتعريف هذا الخيار وإنشاء حزمة متوافقة جديدة باستخدام OpenSSL.

معلومات أساسية

يدعم برنامج Cisco Firepower Threat Defense (المعروف إختصارا باسم FTD) التوافق مع معايير FIPS 140 عند تمكين وضع المعايير المشتركة (CC) أو وضع قائمة المنتجات المعتمدة للقدرات الموحدة (UCAP) على جهاز مدار. يعد هذا التكوين جزءا من نهج إعدادات النظام الأساسي ل FMC. بعد التطبيق، يظهر الأمر **fips enable** في إخراج **show running-config** من FTD.

يعرف PKCS#12 تنسيق ملف يستخدم لتجميع مفتاح خاص وشهادة الهوية ذات الصلة. هناك خيار لتضمين أي شهادة جذر أو متوسط تنتمي إلى سلسلة التحقق من الصحة أيضا. تحمي خوارزميات PBE الشهادات أو أجزاء المفاتيح الخاصة من ملف PKCS#12. نتيجة لمزيج من نظام مصادقة الرسائل (MD2/MD5/SHA1) ونظام التشفير (RC2/RC4/DES)، توجد عدة خوارزميات PBE ولكن الخوارزمية الوحيدة المتوافقة مع FIPS هي PBE-SHA1-3DES.

> **ملاحظة**: لمعرفة المزيد عن FIPS في منتجات Cisco، انتقل إلى FIPS 140.

> **ملاحظة**: لمعرفة المزيد حول معايير شهادات الأمان المتاحة ل FTD و FMC، انتقل إلى دليل تكوين FMC في فصل **توافق شهادات الأمان**.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- البنية الأساسية للمفتاح العام (PKI)
- OpenSSL

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

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

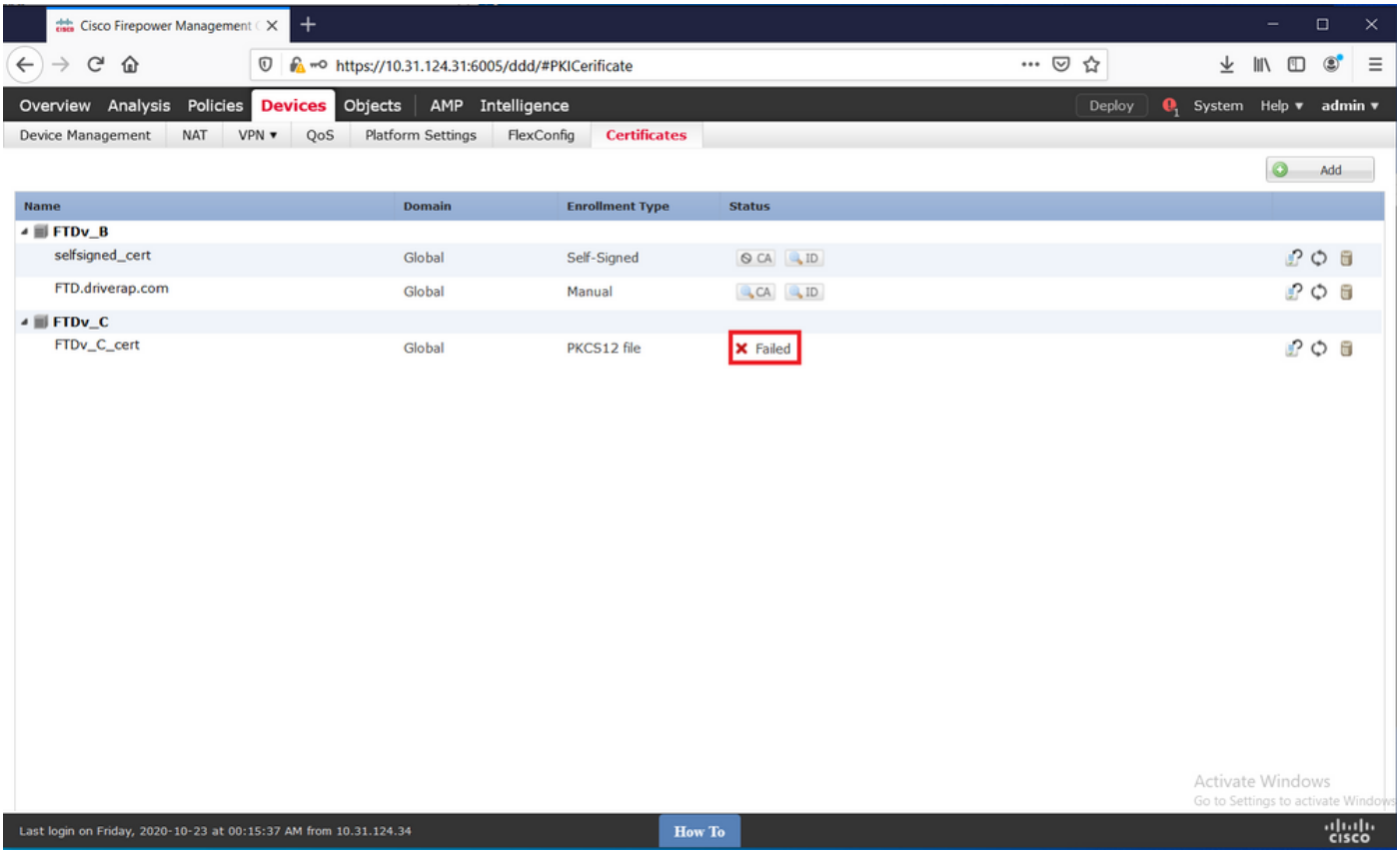
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

> **ملاحظة**: يمكن تنفيذ النهج الموضح في هذا المستند إلى أي منصة أخرى ذات مشكلة مماثلة، على سبيل المثال، جهاز الأمان القابل للتكيف (ASA) من Cisco، ظرا لأن المشكلة تتعلق بأن الشهادة غير متوافقة مع FIPS.

> **ملاحظة**: لا يتناول هذا المستند الحالة التي تكون فيها مكونات PKCS#12 نفسها غير متوافقة لأي سبب آخر مثل طول مفتاح Rivest أو Shamir أو Adleman (RSA) أو خوارزمية التوقيع المستخدمة لتوقيع شهادة الهوية. في تلك الحالات، يجب إعادة إصدار الشهادات لتكون متوافقة مع FIPS.

المشكلة

عند تمكين وضع FIPS في FTD، قد يفشل تثبيت الشهادة إذا لم تكن خوارزميات PBE المستخدمة لحماية ملف PKCS#12 متوافقة مع FIPS.



ملاحظة: يمكنك العثور على إجراء مفصل خطوة بخطوة حول كيفية تثبيت ملف PKCS#12 باستخدام قسم **تسجيل** FMC في **PKCS12** في [تثبيت وتجديد الشهادة في FTD الذي تتم ادارته من قبل FMC](#).

في حالة فشل تثبيت الشهادة لهذا السبب، فإن تصحيح أخطاء PKI يطبع الخطأ أدناه:

```
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
```

كما يمكن أيضا التأكيد من أن PKCS#12 الموجود يتضمن خوارزميات FIPS PBE غير المتوافقة.

```
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
```

في المخرجات السابقة، هناك خوارزميتان PBE، PBEwithSHA1و40BitRC2-CBC و PBEwithSHA1و3-KeyThreeDES-CBC، واللتين تحمي الشهادات والمفاتيح الخاص على التوالي. الأولى غير متوافقة مع FIPS.

الحل

الحل هو تكوين خوارزمية PBE-SHA1-3DES لكل من الشهادة وحماية المفاتيح الخاصة. في المثال أعلاه، يلزم تغيير خوارزمية الشهادة فقط. أولا، تحتاج إلى الحصول على إصدار البريد المحسن للخصوصية (PEM) من الملف PKCS#12 الأصلي الذي يستخدم 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:
```

أخيرا، تحتاج استخدام الأمر أدناه مع خوارزمية PBE المتوافقة مع FIPS باستخدام ملف PEM الذي تم الحصول عليه في الخطوة السابقة لإنشاء ملف PKCS#12 جديد:

```
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'
```

> **ملاحظة**: إذا كانت هناك حاجة إلى تغيير الخوارزمية لحماية المفاتيح الخاص أيضا، فيمكن إلحاق الكلمة الأساسية **keypbe** بالأمر السابق إلى **PBE-SHA1-3DES** متبوعة بـ **keypbe PBE-SHA1-3DES** على النحو التالي: **PKCS12 -certpbe-SHA1-3DES -keypbe PBE-SHA1-3DES -in-out*<PKCS12 Cert>***.

التحقق

استخدم الأمر OpenSSL نفسه للحصول على معلومات حول بنية ملف PKCS#12 لتأكيد استخدام خوارزميات FIPS:

```
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
```

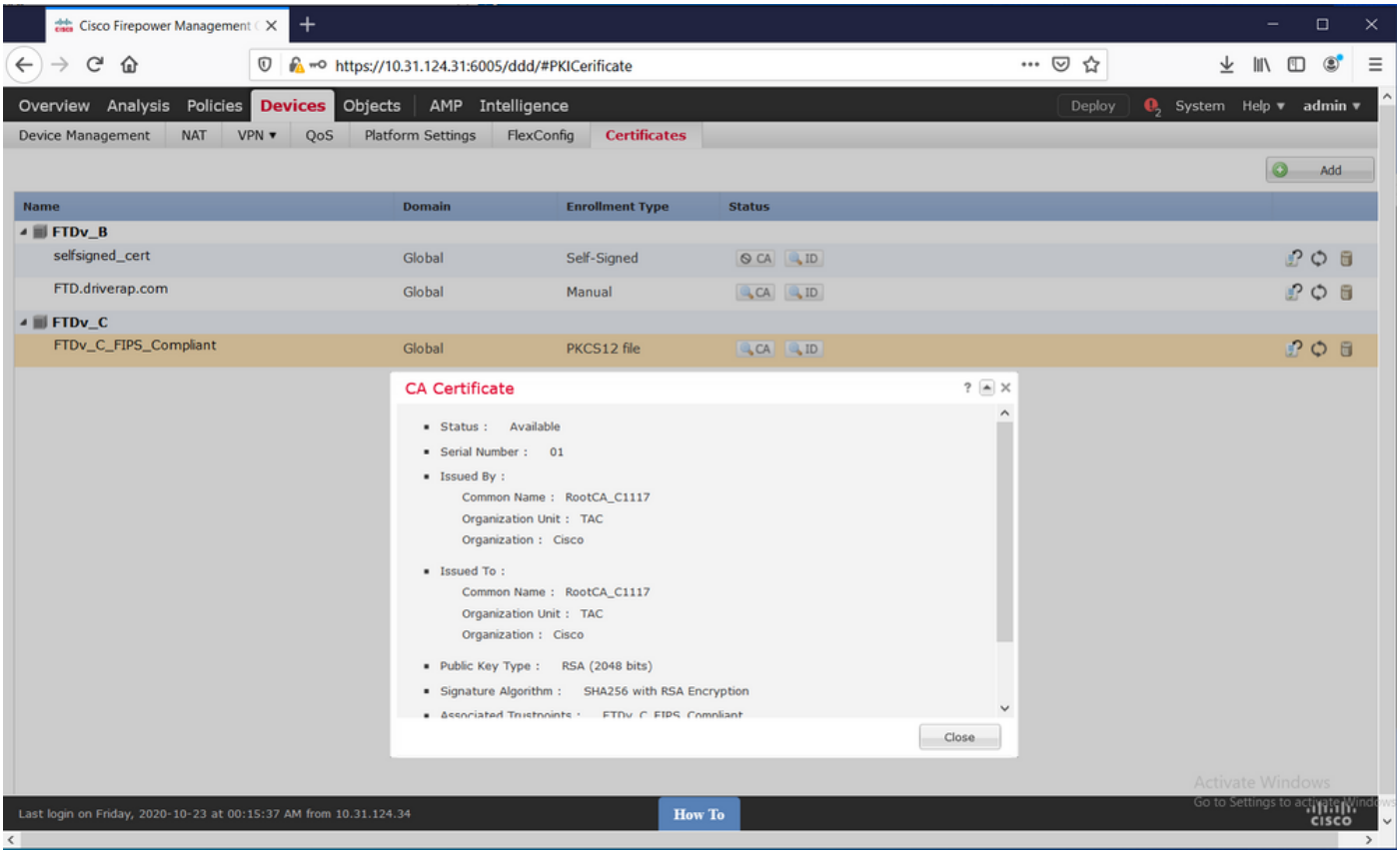
الآن تظهر تصحيح أخطاء PKI الإخراج أدناه عند نجاح تثبيت الشهادة.

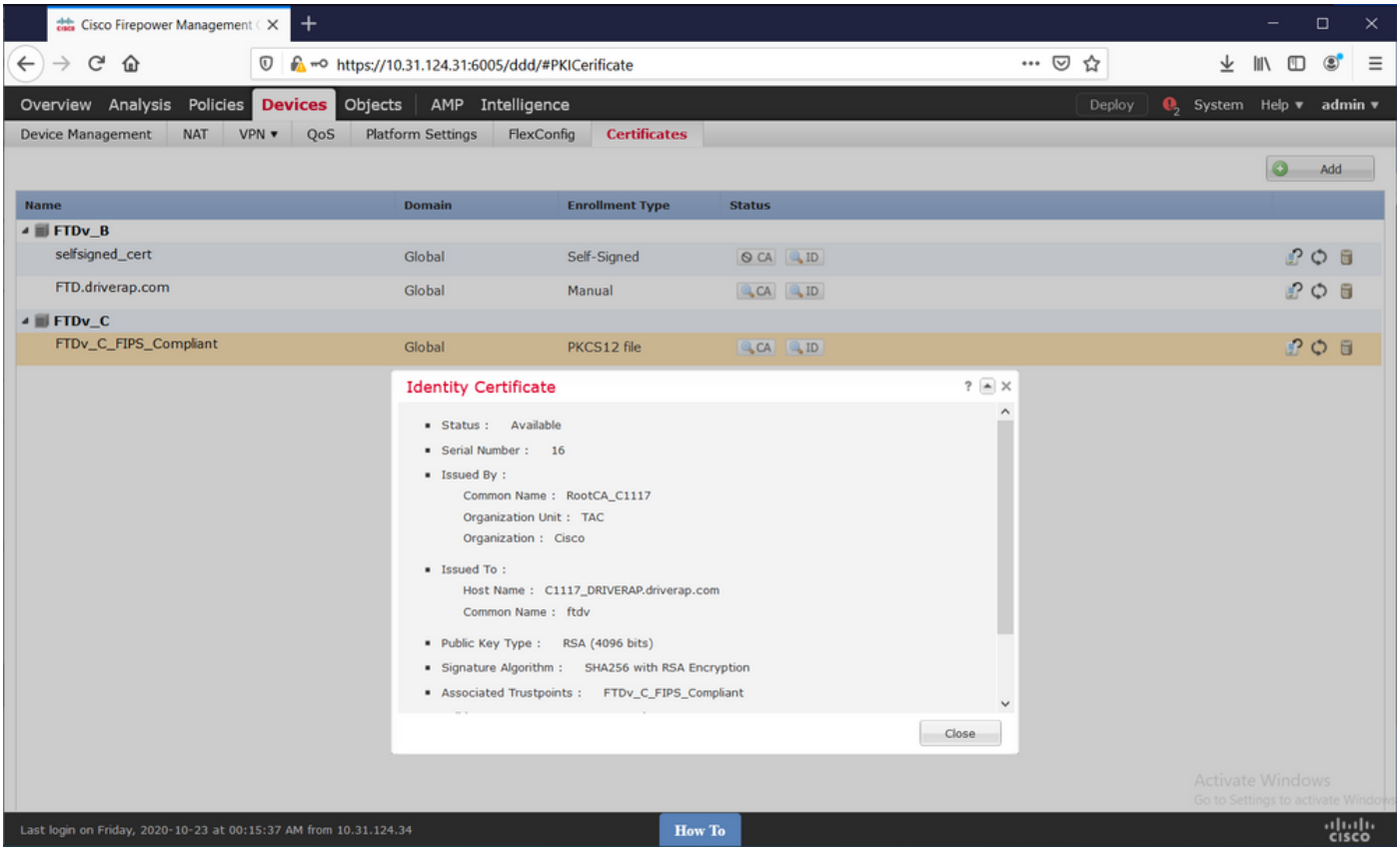
```
PKI[13]: crypto_parsepkcs12, pki_ossl_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_ossl_pkcs12.c:1414
PKI[13]: pki_unpack_bags, pki_ossl_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_cert, pki_ossl_pkcs12.c:1284
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[13]: pki_unpack_bag,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

وأخيرا، تعرض FMC كل من CA وشهادات الهوية حسب ما هو متاح:





حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).