Risoluzione dei problemi di installazione dei file PKCS#12 non riuscita con algoritmi PBE non conformi a FIPS

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di installazione di un file PKCS (Public Key Cryptography Standards)#12 con algoritmi PBE (Password-Based Encryption) non conformi allo standard FIPS (Federal Information Processing Standard) tramite Cisco Firepower Management Center (FMC). Illustra una procedura per identificarlo e creare un nuovo bundle conforme con OpenSSL.

Premesse

Cisco Firepower Threat Defense (FTD) supporta la conformità a FIPS 140 quando si abilita la modalità CC (Common Criteria) o UCAP (Unified Capabilities Approved Products List) su un dispositivo gestito. Questa configurazione fa parte di un criterio di Impostazioni piattaforma FMC. Dopo l'applicazione, il comando **fips enable** viene visualizzato nell'output **show running-config** di FTD.

PKCS#12 definisce un formato di file utilizzato per includere una chiave privata e il relativo certificato di identità. È possibile includere anche qualsiasi certificato radice o intermedio appartenente alla catena di convalida. Gli algoritmi PBE proteggono i certificati e le parti della chiave privata del file PKCS#12. Grazie alla combinazione dello schema di autenticazione dei messaggi (MD2/MD5/SHA1) e dello schema di crittografia (RC2/RC4/DES), sono disponibili più algoritmi PBE, ma l'unico compatibile con FIPS è PBE-SHA1-3DES.

> **Nota:** Per ulteriori informazioni su FIPS nei prodotti Cisco, passare a FIPS 140.

> **Nota:** Per ulteriori informazioni sugli standard di certificazione di sicurezza disponibili per FTD e FMC, vedere il capitolo **Certificazioni di sicurezza e conformità** della Guida alla configurazione di FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PKI (Public Key Infrastructure)
- OpenSSL

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

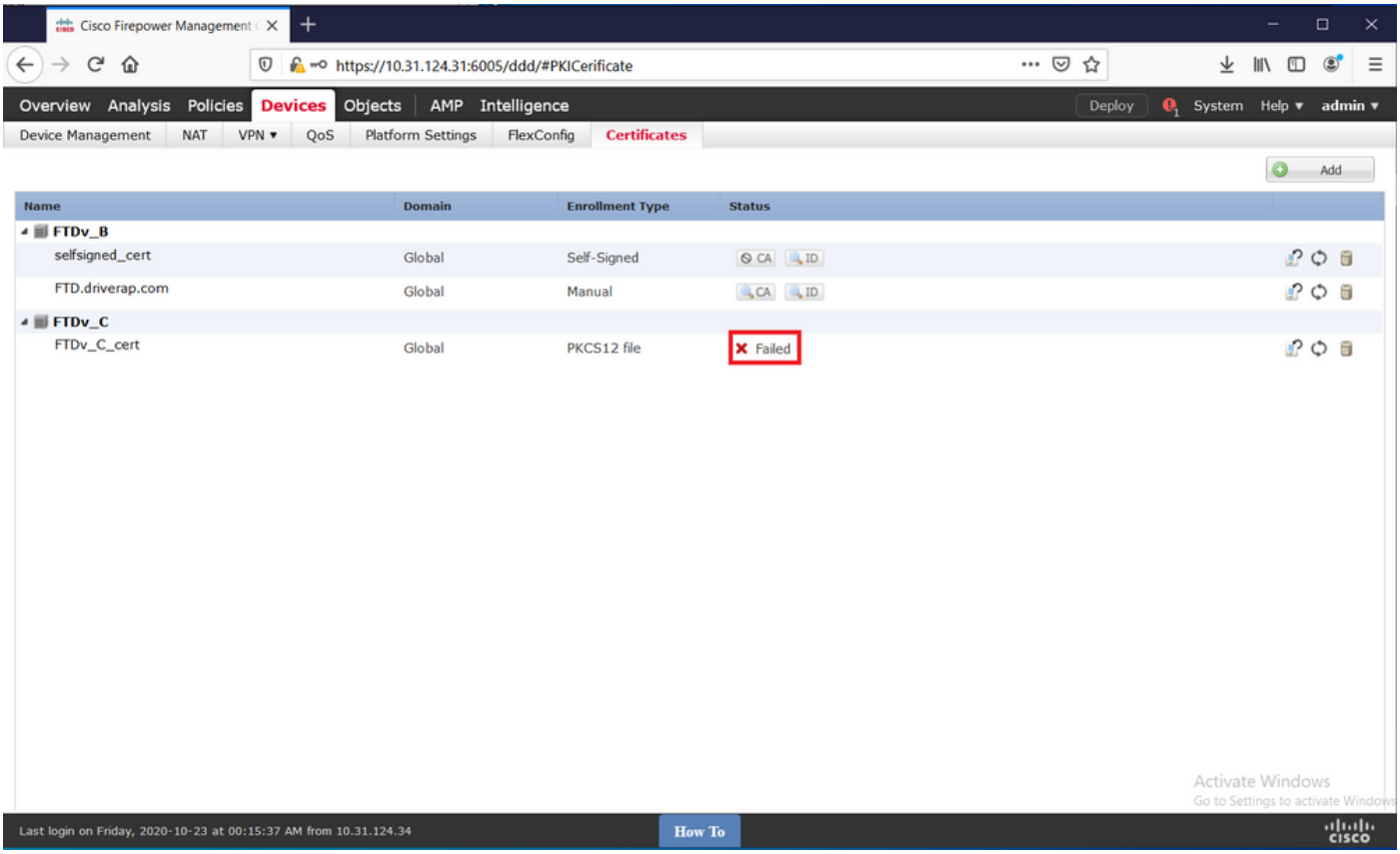
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

> **Nota:** L'approccio descritto in questo documento può essere implementato su qualsiasi altra piattaforma con un problema simile, ad esempio una Cisco Adaptive Security Appliance (ASA), poiché il problema si verifica quando il certificato non è conforme allo standard FIPS.

> **Nota:** Questo documento non risolve il problema della mancata conformità dei componenti PKCS#12 per qualsiasi altro motivo, ad esempio per la lunghezza della chiave Rivest, Shamir, Adleman (RSA) o per l'algoritmo Signature usato per firmare il certificato di identità. In questi casi, è necessario riemettere i certificati per garantire la conformità FIPS.

Problema

Quando la modalità FIPS è attivata in FTD, l'installazione dei certificati potrebbe non riuscire se gli algoritmi PBE utilizzati per proteggere il file PKCS#12 non sono conformi a FIPS.



Nota: Trovare una procedura dettagliata su come installare un file PKCS#12 utilizzando il FMC nella sezione **Iscrizione PKCS12** di Installazione e rinnovo certificati su FTD gestito da FMC.

Se l'installazione del certificato non riesce per questo motivo, il debug PKI visualizza l'errore riportato di seguito:

```
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
```

Èinoltre possibile verificare con OpenSSL che PKCS#12 includa algoritmi PBE FIPS non conformi.

```
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
```

Nell'output precedente sono disponibili due algoritmi PBE, pbeWithSHA1And40BitRC2-CBC e pbeWithSHA1And3-KeyTripleDES-CBC, che proteggono rispettivamente i certificati e la chiave privata. Il primo non è conforme allo standard FIPS.

Soluzione

La soluzione consiste nel configurare l'algoritmo PBE-SHA1-3DES per la protezione del certificato e della chiave privata. Nell'esempio precedente è necessario modificare solo l'algoritmo del certificato. Innanzitutto, è necessario ottenere la versione Privacy-Enhanced Mail (PEM) del file PKCS#12 originale utilizzando 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:
```

Infine, per generare un nuovo file PKCS#12, è necessario utilizzare il comando riportato di seguito con l'algoritmo PBE conforme a FIPS utilizzando il file PEM ottenuto nel passaggio precedente:

```
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:** Se è necessario modificare anche l'algoritmo per la protezione della chiave privata, è possibile aggiungere la parola chiave **-keypbe** seguita da **PBE-SHA1-3DES** allo stesso comando: **pkcs12 -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -export -in -out -out *<file certificato PKCS12>***.

Verifica

Utilizzare lo stesso comando OpenSSL per ottenere informazioni sulla struttura di file PKCS#12 e verificare che gli algoritmi FIPS siano in 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
```

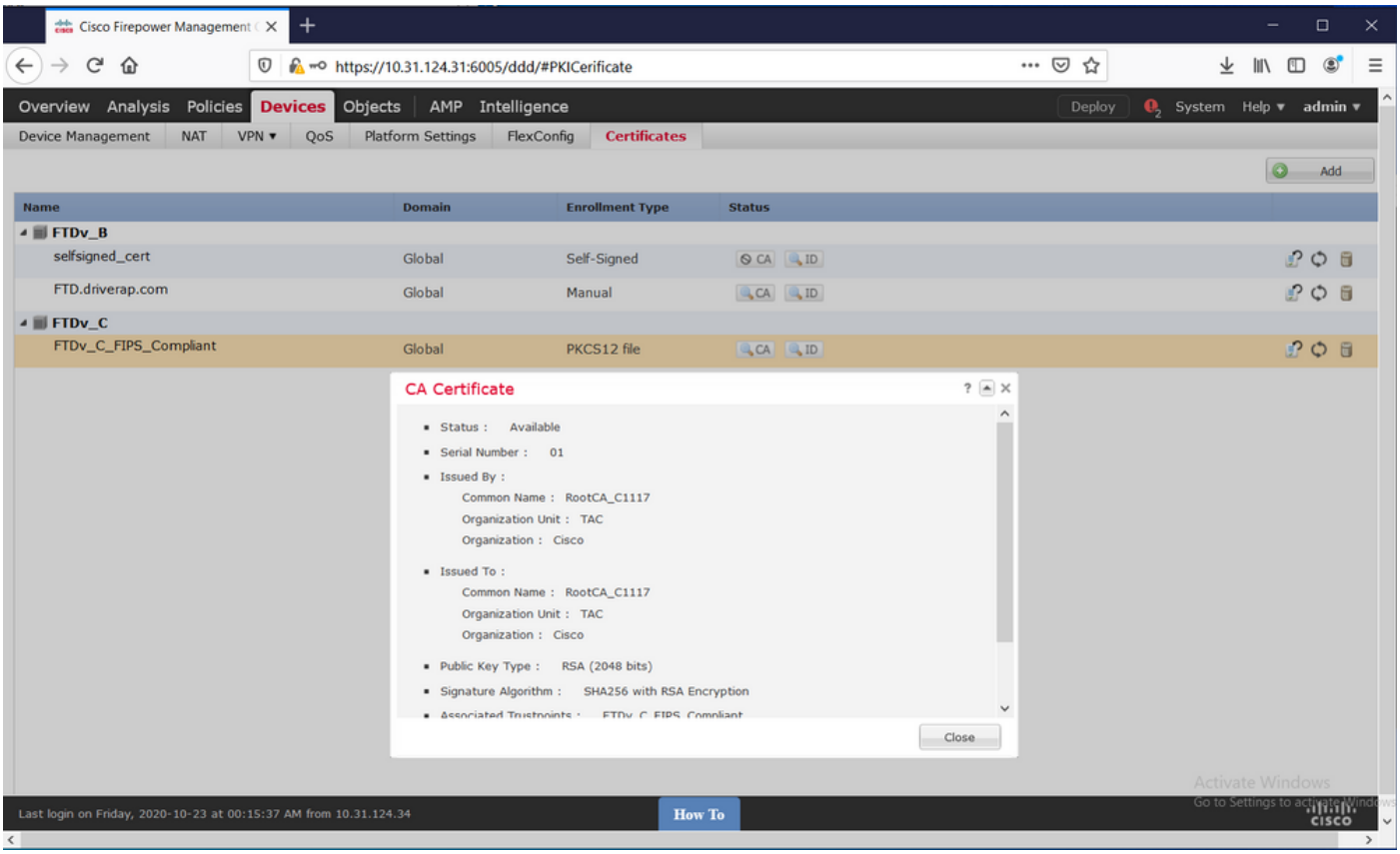
Ora i debug PKI mostrano di seguito l'output al completamento dell'installazione del certificato.

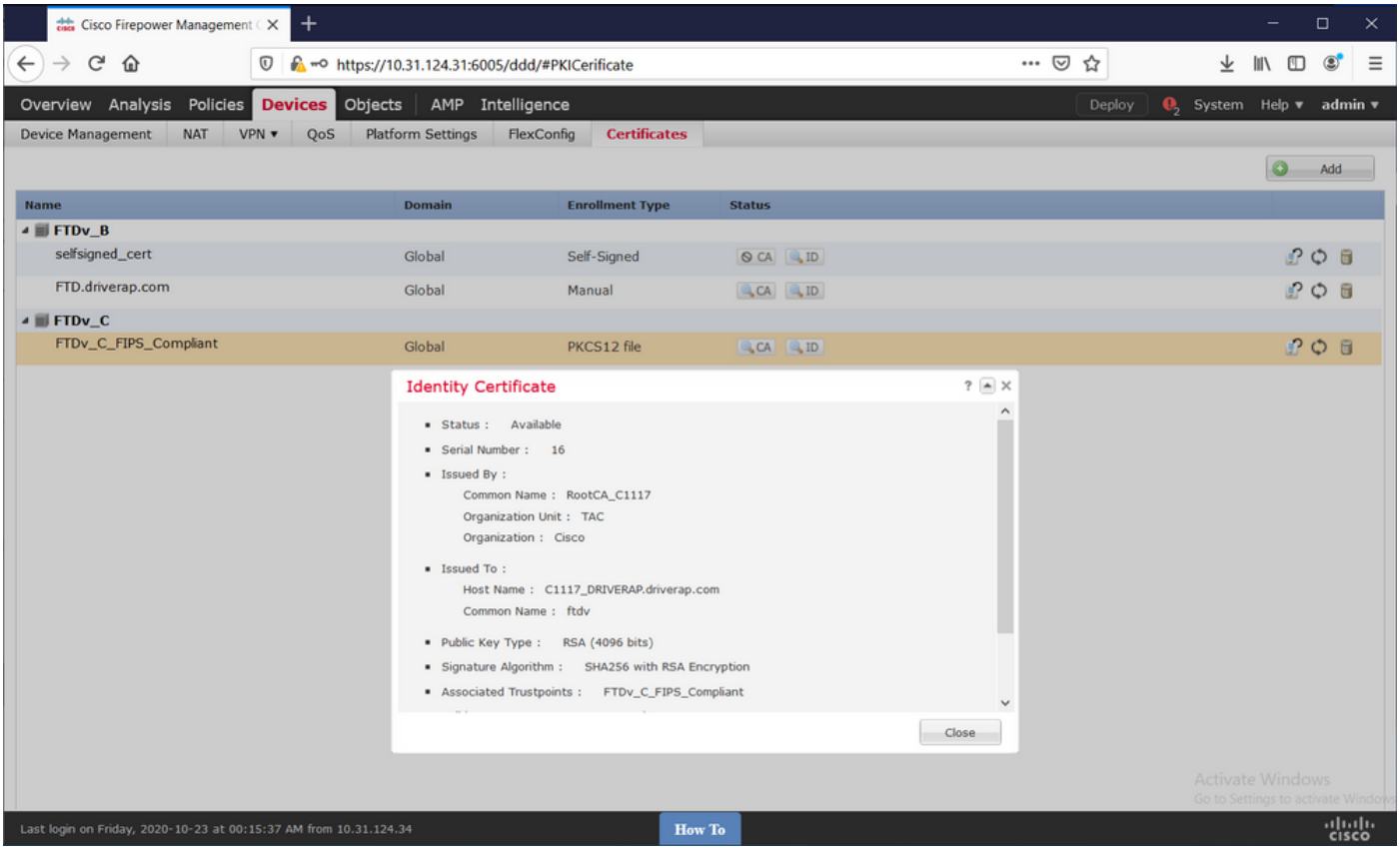
```
PKI[13]: crypto_parsepkcs12, pki_ossl_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_ossl_pkcs12.c:1414
PKI[13]: pki_unpack_bags, pki_ossl_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_ossl_pkcs12.c:1313
PKI[13]: add_cert, pki_ossl_pkcs12.c:1284
PKI[13]: add_cert_node, pki_ossl_pkcs12.c:1187
PKI[13]: pki_unpack_bag,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

Infine, il CCP mostra i certificati di identità e CA come disponibili:




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