

# 使用不符合FIPS的PBE演算法排除PKCS#12檔案安裝故障

## 目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[問題](#)

[解決方案](#)

[驗證](#)

## 簡介

本檔案介紹如何透過Cisco Firepower管理中心(FMC)使用非聯邦資訊處理標準(FIPS)相容的密碼型加密(PBE)演算法，對公鑰加密標準(PKCS)#12檔的安裝失敗進行疑難排解。其中說明了一個識別該來源及使用OpenSSL建立新相容套件組合的程式。

## 背景資訊

在受管裝置上啟用通用標準(CC)或統一功能批准產品清單(UCAP)模式時，Cisco Firepower威脅防禦(FTD)支援符合FIPS 140。此配置是FMC平台設定策略的一部分。應用後，**fips enable**命令會顯示在FTD的**show running-config**輸出中。

PKCS#12定義用於捆綁私鑰和相應身份證書的檔案格式。也可以選擇包括屬於驗證鏈的任何根或中間證書。PBE演算法可保護PKCS#12檔案的證書和私鑰部分。由於消息驗證方案(MD2/MD5/SHA1)和加密方案(RC2/RC4/DES)的組合，存在多個PBE演算法，但唯一一個符合FIPS的演算法是PBE-SHA1-3DES。

附註：要瞭解有關思科產品中FIPS的更多資訊，請導航至[FIPS 140](#)。

附註：要瞭解可用於FTD和FMC的安全認證標準的更多資訊，請導航至[FMC配置指南](#)的安全認證[合規性一章](#)。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 公開金鑰基礎架構 (PKI)

- OpenSSL

## 採用元件

本檔案中的資訊是根據以下軟體版本：

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

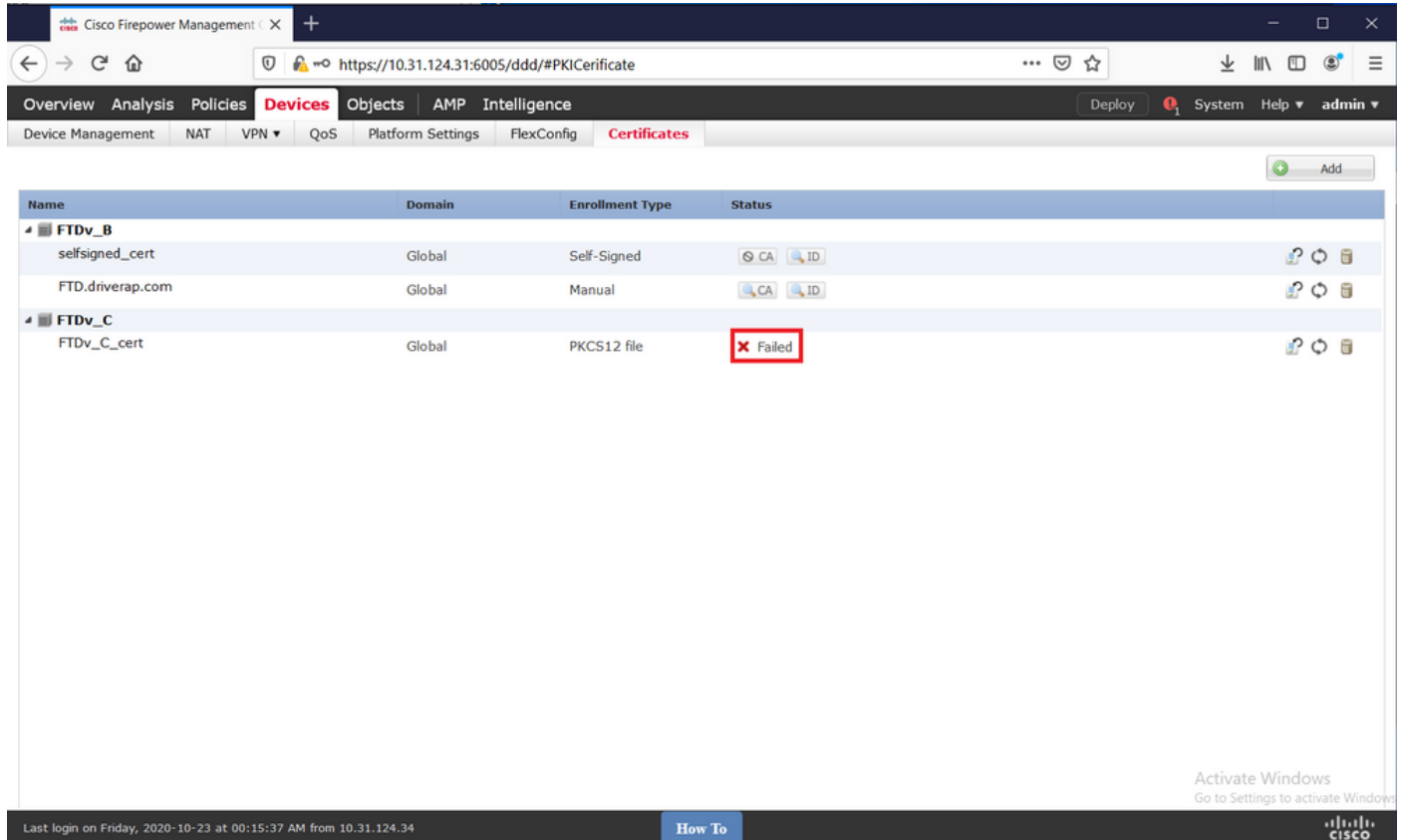
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

**附註：**本文檔中描述的方法可以實施到存在類似問題的任何其他平台，例如，思科自適應安全裝置(ASA)，因為問題在於證書不符合FIPS。

**附註：**本文檔未說明PKCS#12元件本身因任何其他原因(如Rivest、Shamir、Adleman(RSA)金鑰長度或用於簽署身份證書的簽名演算法)而不符合的條件。在這種情況下，需要重新頒發證書以符合FIPS。

## 問題

在FTD中啟用FIPS模式時，如果用於保護PKCS#12檔案的PBE演算法不符合FIPS，則證書安裝可能會失敗。



The screenshot shows the Cisco Firepower Management Center (FMC) interface. The browser address bar displays <https://10.31.124.31:6005/ddd/#PKICertificate>. The navigation menu includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The 'Certificates' tab is active, showing a table of certificates. The table has columns for Name, Domain, Enrollment Type, and Status. One certificate, 'FTDv\_C\_cert', is highlighted in red and has a 'Failed' status.

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_cert	Global	PKCS12 file	Failed

**附註：**有關如何使用FMC在FMC管理的FTD上證書安裝和續訂的PKCS12註冊一節中的FMC來安裝PKCS#12檔案的逐步程式。

如果由於此原因證書安裝失敗，PKI調試將列印以下錯誤：

```
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_oss1_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_oss1_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_oss1_set_cert_store_dirty, pki_oss1_certstore.c:38
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.c:41
PKI[13]: label: FTDv_C_cert
PKI[13]: TP list label: FTDv_C_cert
```

您還可以使用OpenSSL確認手頭的PKCS#12包含不符合的FIPS PBE演算法。

```
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
```

在前面的輸出中有兩個PBE演算法，pbeWithSHA1和40BitRC2-CBC和pbeWithSHA1And3-KeyTripleDES-CBC，分別保護證書和私鑰。第一個不符合FIPS。

## 解決方案

解決方案是為證書和私鑰保護配置PBE-SHA1-3DES演算法。在上方範例中，僅需變更憑證演算法。首先，您需要使用OpenSSL取得原始PKCS#12檔案的Privacy-Enhanced Mail(PEM)版本。

```
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:
```

最後，您需要使用以下命令以及符合FIPS的PBE演算法（使用在上一步中獲取的PEM檔案）來生成全新的PKCS#12檔案：

```
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'
```

**附註：**如果保護私鑰的演算法也需要更改，您可以在同一命令中附加-keypbe關鍵字，後跟 PBE-SHA1-3DES:pkcs12 -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -export -in -out -out <PKCS12 cert file>。

## 驗證

使用相同的OpenSSL命令獲取有關PKCS#12檔案結構的資訊，以確認正在使用FIPS演算法：

```
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
```

現在，當證書安裝成功時，PKI調試顯示下面的輸出。

```
PKI[13]: crypto_parsepkcs12, pki_oss1_pkcs12.c:1484
PKI[13]: pki_unpack_p12, pki_oss1_pkcs12.c:1414
PKI[13]: pki_unpack_bags, pki_oss1_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_oss1_pkcs12.c:1313
PKI[13]: add_cert, pki_oss1_pkcs12.c:1284
PKI[13]: add_cert_node, pki_oss1_pkcs12.c:1187
PKI[13]: pki_unpack_bag, pki_oss1_pkcs12.c:1313
PKI[13]: add_cert, pki_oss1_pkcs12.c:1284
PKI[13]: add_cert_node, pki_oss1_pkcs12.c:1187
PKI[13]: pki_unpack_bags, pki_oss1_pkcs12.c:1383
PKI[13]: pki_unpack_bag, pki_oss1_pkcs12.c:1313
PKI[13]: add_key, pki_oss1_pkcs12.c:1252
PKI[13]: add_cert_node, pki_oss1_pkcs12.c:1187
PKI[14]: compare_key_ids, pki_oss1_pkcs12.c:1150
PKI[12]: transfer_p12_contents_to_asa, pki_oss1_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_oss1_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\_oss1\_set\_cert\_store\_dirty,  
pki\_oss1\_certstore.c:38

PKI[13]: crypto\_pki\_get\_oss1\_env, pki\_oss1.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\_oss1\_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\_oss1\_set\_cert\_store\_dirty,  
pki\_oss1\_certstore.c:38

PKI[13]: crypto\_pki\_get\_oss1\_env, pki\_oss1.c:41

PKI[9]: Cleaned PKI cache successfully

PKI[9]: Starting to build the PKI cache

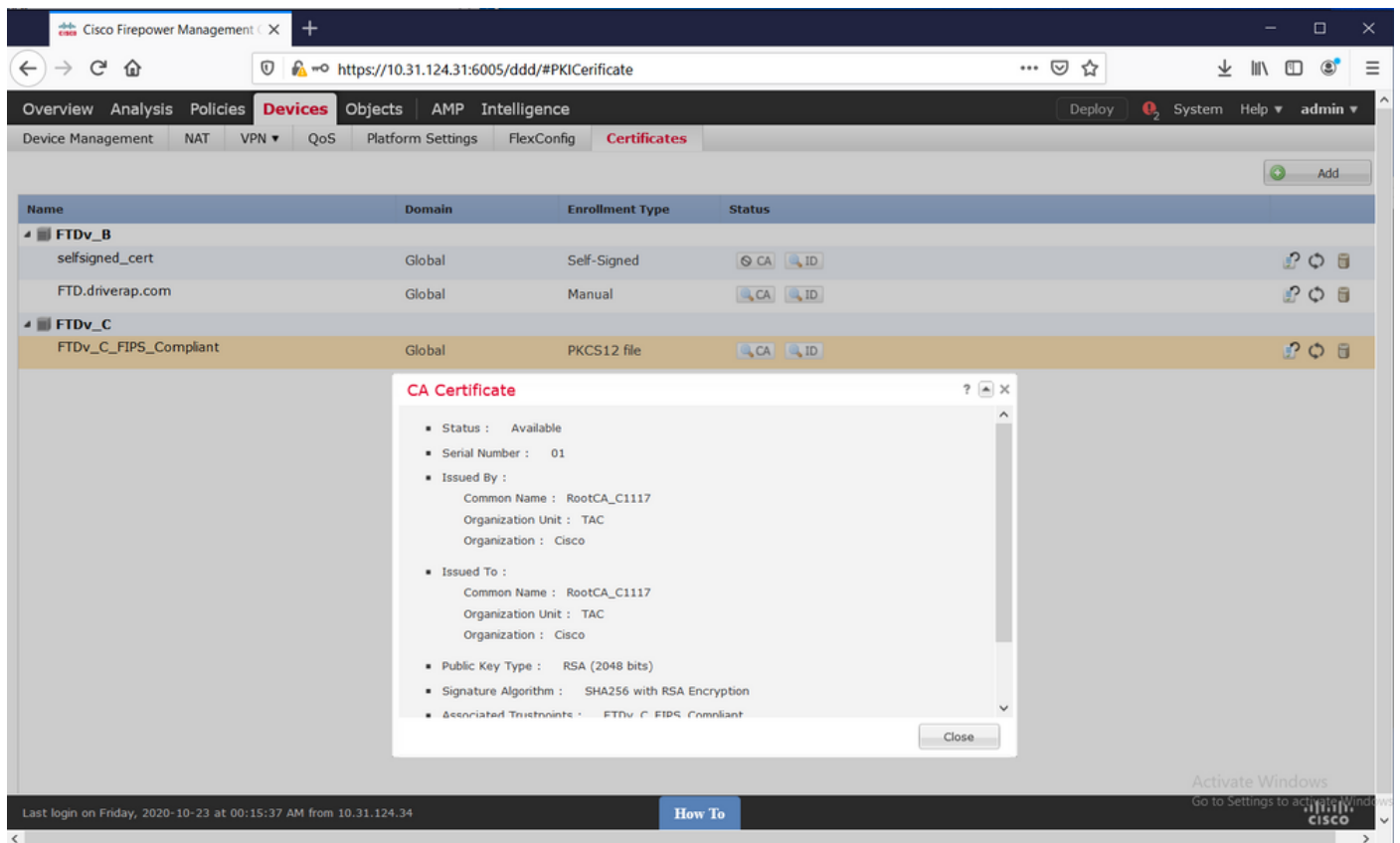
CRYPTO\_PKI(Cert Lookup) issuer="cn=RootCA\_C1117,ou=TAC,o=Cisco" serial number=16 | .

```
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_oss1_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_oss1_set_cert_store_dirty, pki_oss1_certstore.c:38
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.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

最後，FMC顯示CA和身份證書均可用：



Cisco Firepower Management | X +

https://10.31.124.31:6005/ddd/#PKICertificate

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  
Go to Settings to activate Windows

Last login on Friday, 2020-10-23 at 00:15:37 AM from 10.31.124.34

How To

CISCO