在FMC管理的FTD上安装并续订证书

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 证书安装
  - 自签名注册
  - 手动注册
  - PKCS12注册
- 证书续订
  - 自签名证书续订
  - 手动证书续订
  - PKCS12续订
- 使用OpenSSL创建PKCS12

验证

- 查看FMC中安装的证书
- 在CLI中查看已安装的证书

故障排除

- 调试命令
- 常见问题

简介

本文档介绍如何在FMC管理的FTD上安装、信任和续订证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 手动证书注册需要访问受信任的第三方CA。
- 第三方CA供应商的示例包括（但不限于）Entrust、Geotrust、GoDaddy、Thawte和

VeriSign。
- 验证FTD具有正确的时钟时间、日期和时区。对于证书身份验证，建议使用网络时间协议(NTP)服务器同步FTD上的时间。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行6.5的FMCv
- 运行6.5的FTDv
- 创建PKCS12时，使用OpenSSL

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。

背景信息

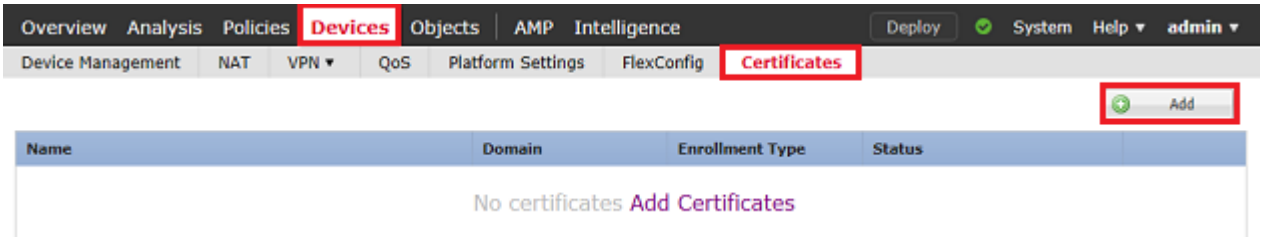
本文档介绍如何在Firepower管理中心(FMC)管理的Firepower威胁防御(FTD)上安装、信任和续订由第三方证书颁发机构(CA)或内部CA签名的自签名证书和证书。

配置

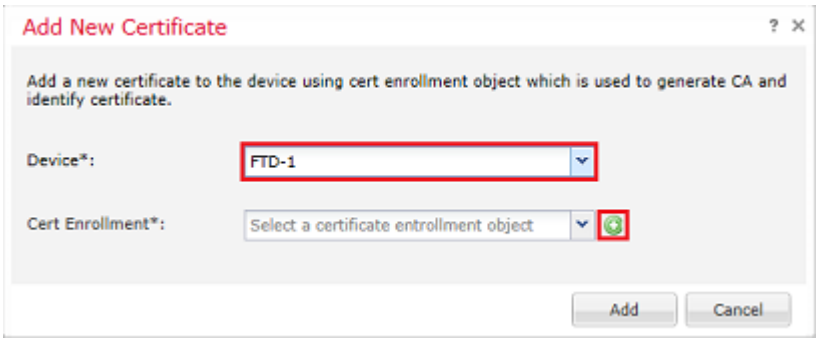
证书安装

自签名注册

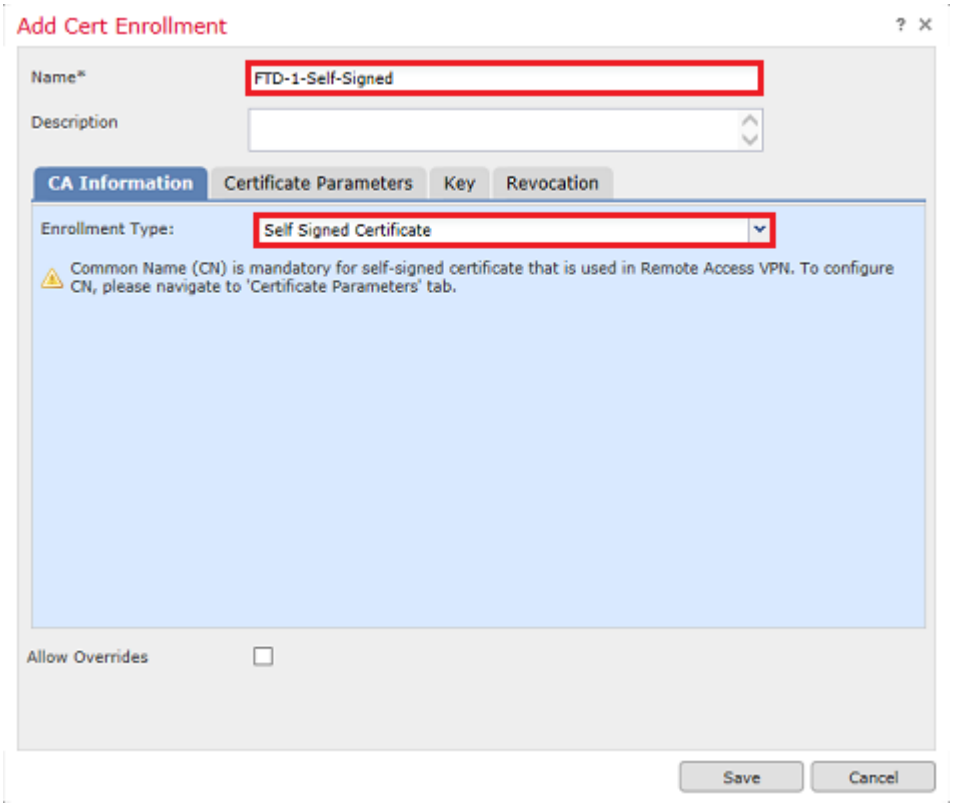
1.导航到设备>证书，然后单击添加，如图所示。



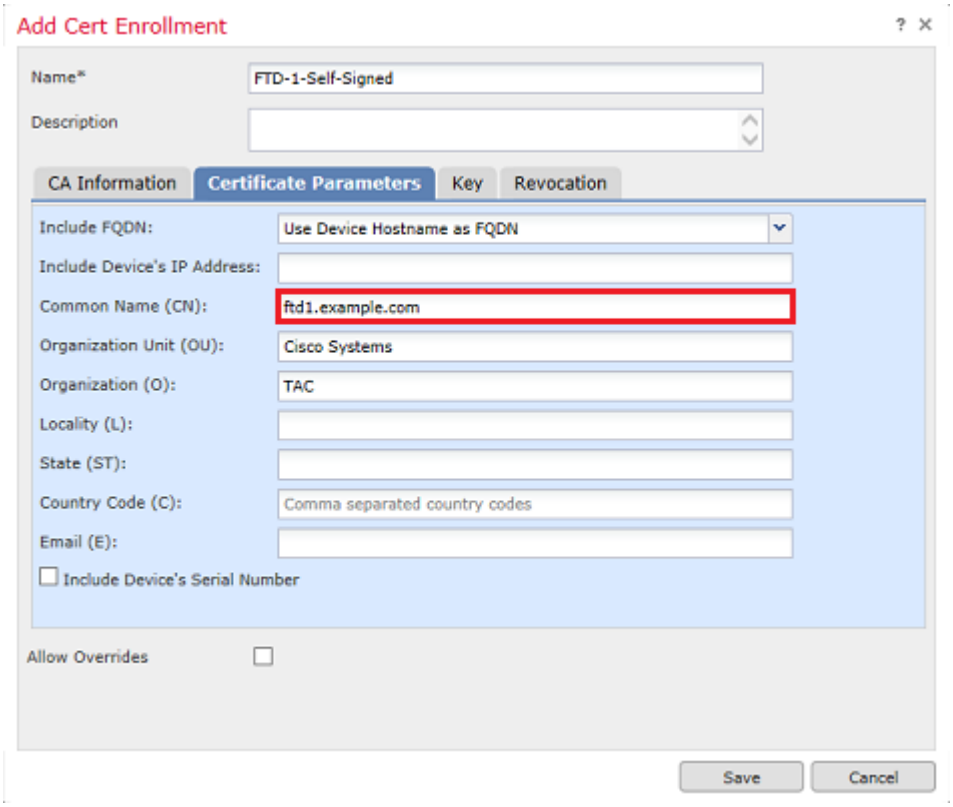
2.选择设备，证书将添加到Device*下拉列表中。然后单击绿色+符号，如图所示。



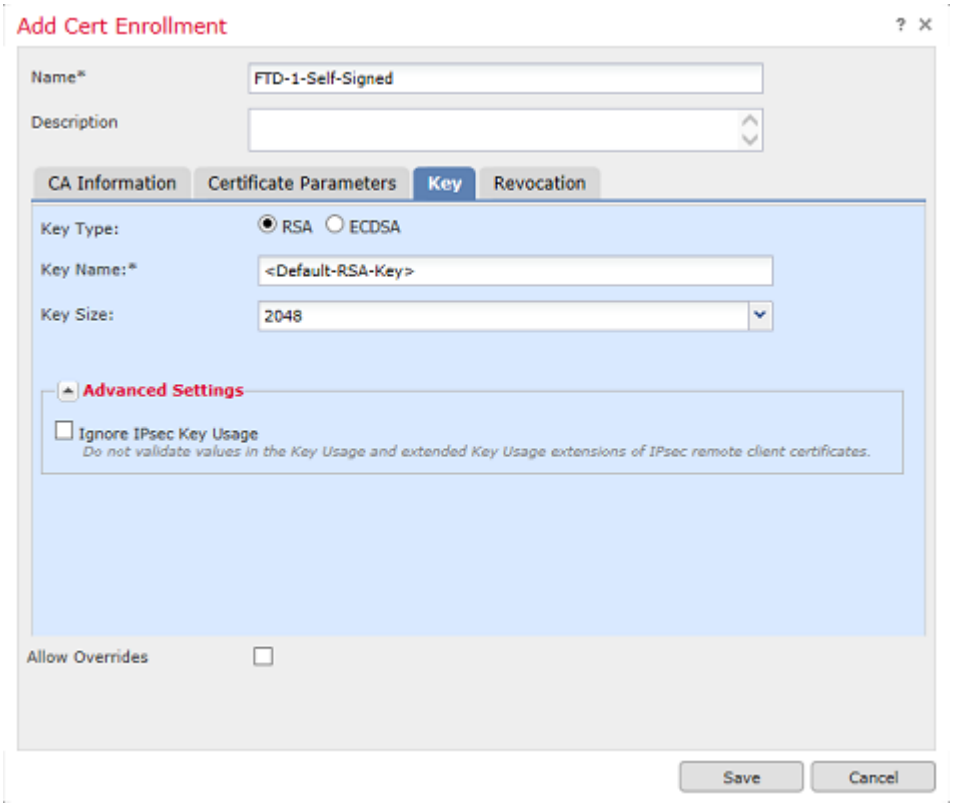
3.指定信任点的名称，然后在“CA信息”选项卡下，选择“注册类型”：自签名证书，如图所示。



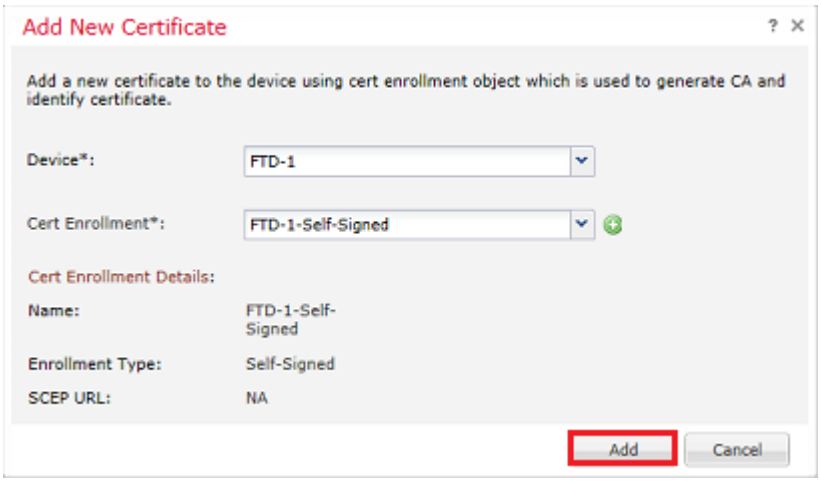
4.在Certificate Parameters选项卡下，输入证书的Common名称。这必须与使用证书的服务（如图所示）的FQDN或IP地址匹配。



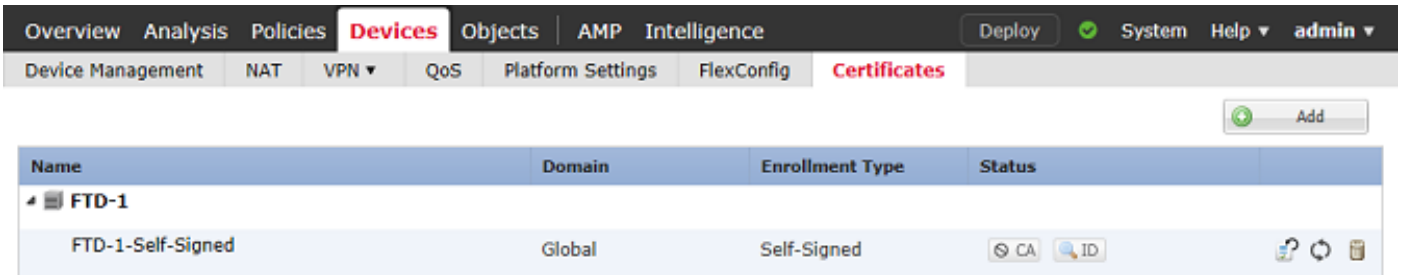
5.（可选）在密钥选项卡下，可以指定用于证书的私钥的类型、名称和大小。默认情况下，密钥使用名称为<Default-RSA-Key>、大小为2048的RSA密钥；但是，建议为每个证书使用唯一的名称，以便它们不使用如图所示的相同私有/公共密钥对。



6.完成后，单击Save，然后单击Add，如图所示。

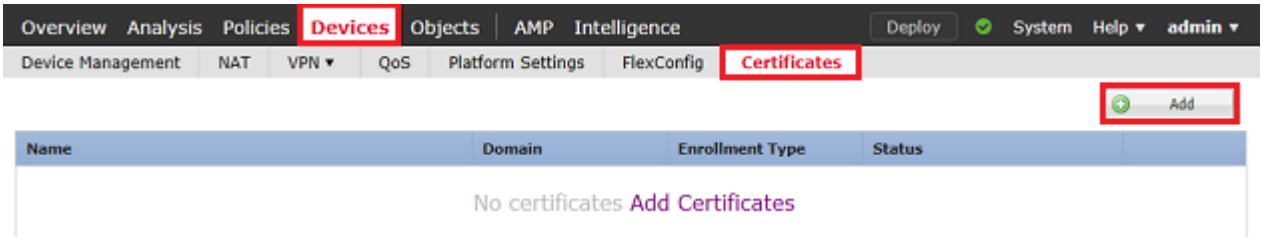


7.完成之后，自签名证书将显示在图像中。

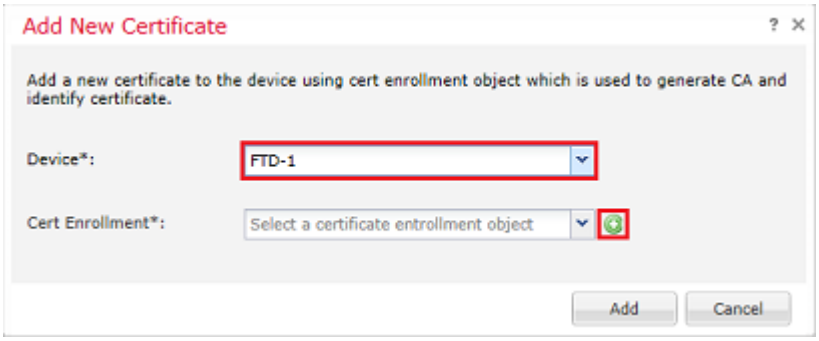


手动注册

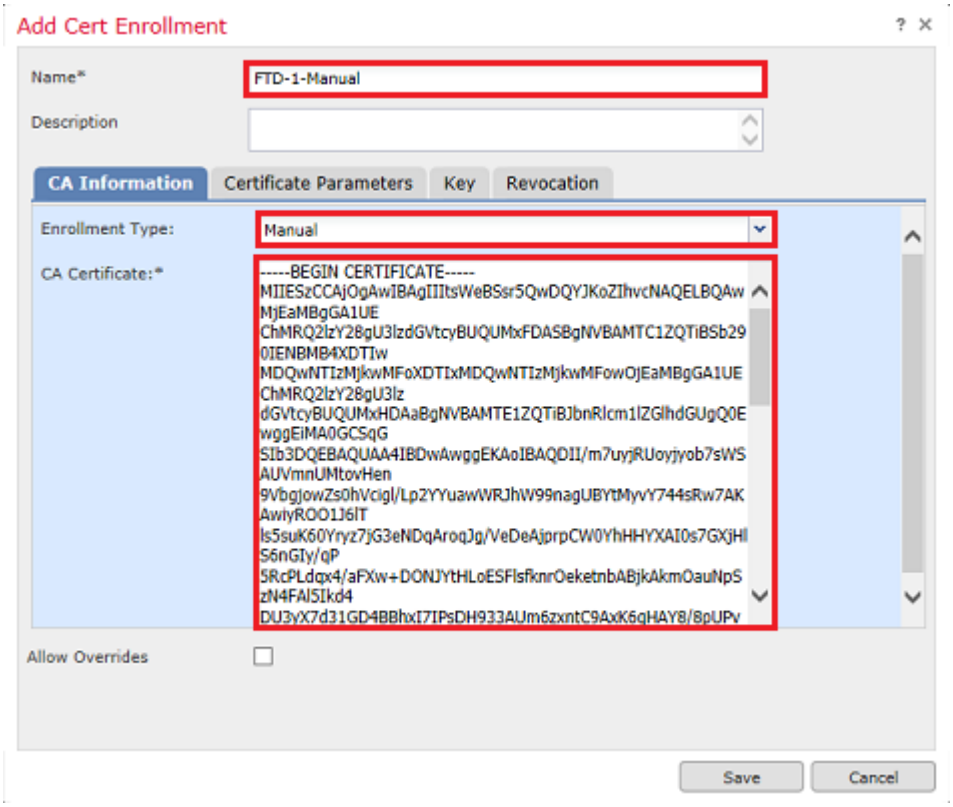
1.导航到设备>证书，然后单击添加，如图所示。



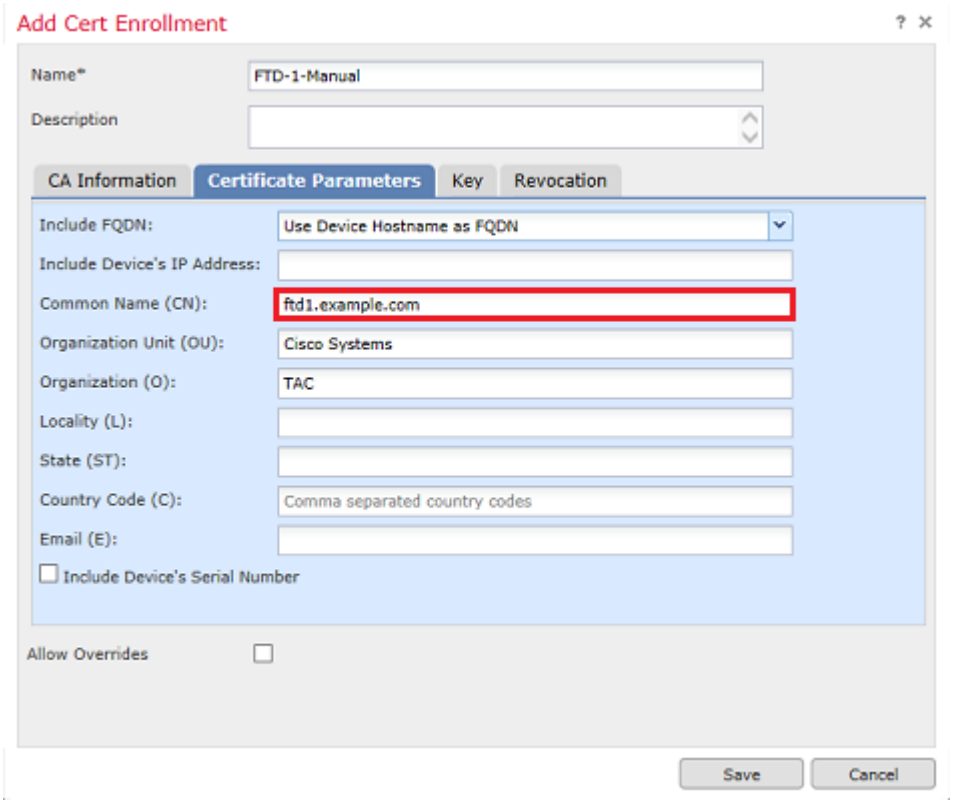
2.在Device*下拉菜单中选择证书添加到的设备，然后单击绿色+符号，如图所示。



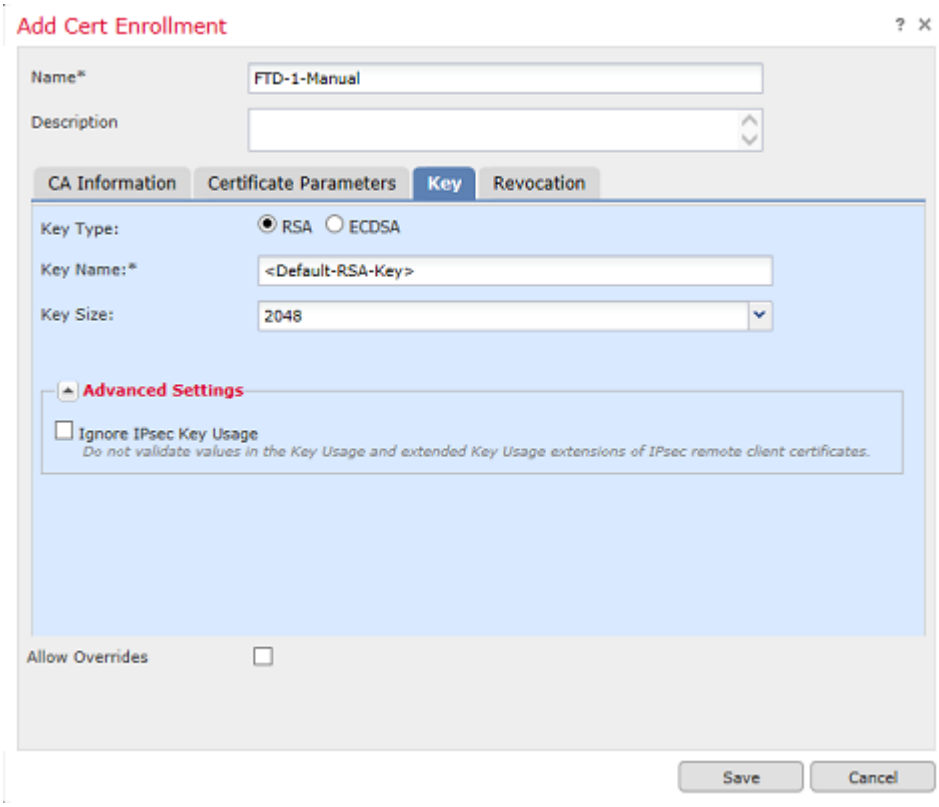
3.指定信任点的名称，然后在“CA信息”选项卡下，选择“注册类型”：手动。输入用于签署身份证书的CA的PEM格式证书。如果此证书当前不可用或未知，请添加任何CA证书作为占位符，在颁发身份证书后，重复此步骤以添加实际颁发CA，如图所示。



4.在Certificate Parameters选项卡下，输入证书的Common名称。这必须与使用证书的服务的fqdn或IP地址匹配，如图所示。

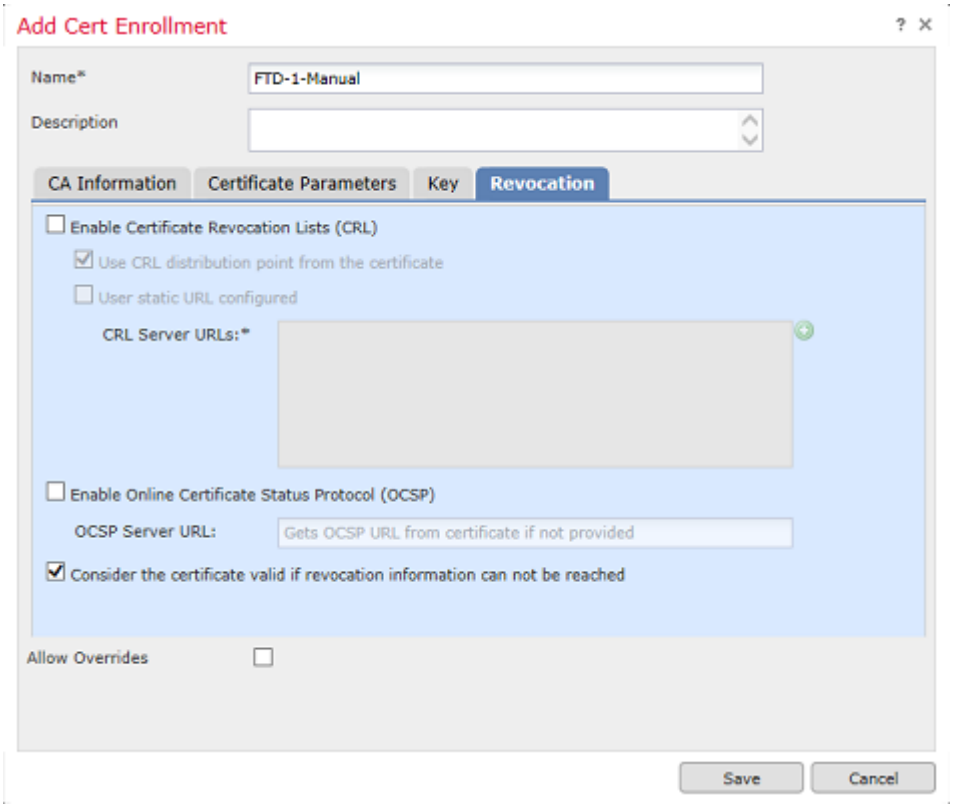


5.（可选）在Key选项卡下，可以选择指定用于证书的私钥的类型、名称和大小。默认情况下，密钥使用名称为<Default-RSA-Key>、大小为2048的RSA密钥；但是，建议为每个证书使用唯一的名称，以便它们不使用如图所示的相同私有/公共密钥对。

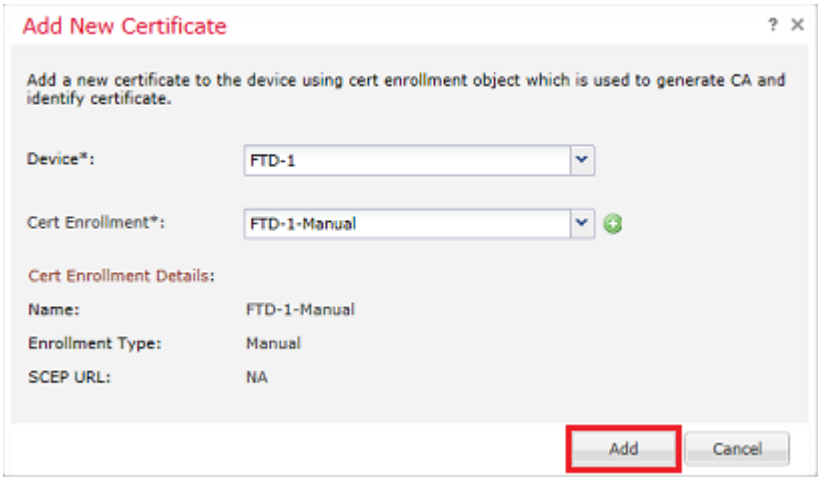


6.（可选）在Revocation选项卡下，Certificate Revocation List(CRL)或Online Certificate Status

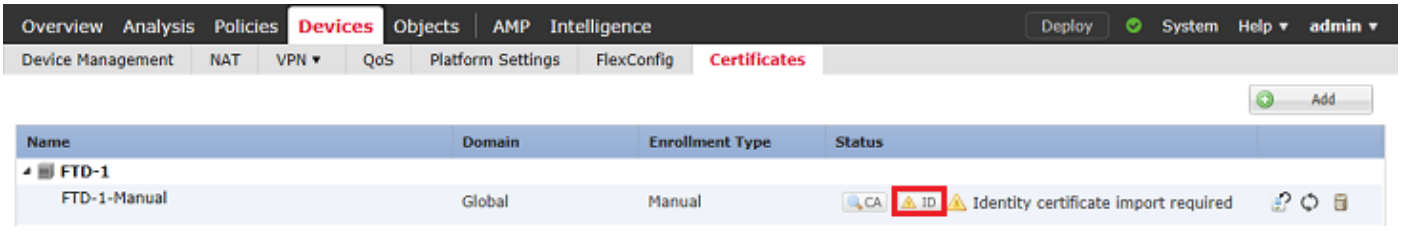
Protocol(OCSP)revocation已选中并可进行配置。默认情况下，两者均未选中，如图所示。



7.完成后，单击Save，然后单击Add，如图所示。



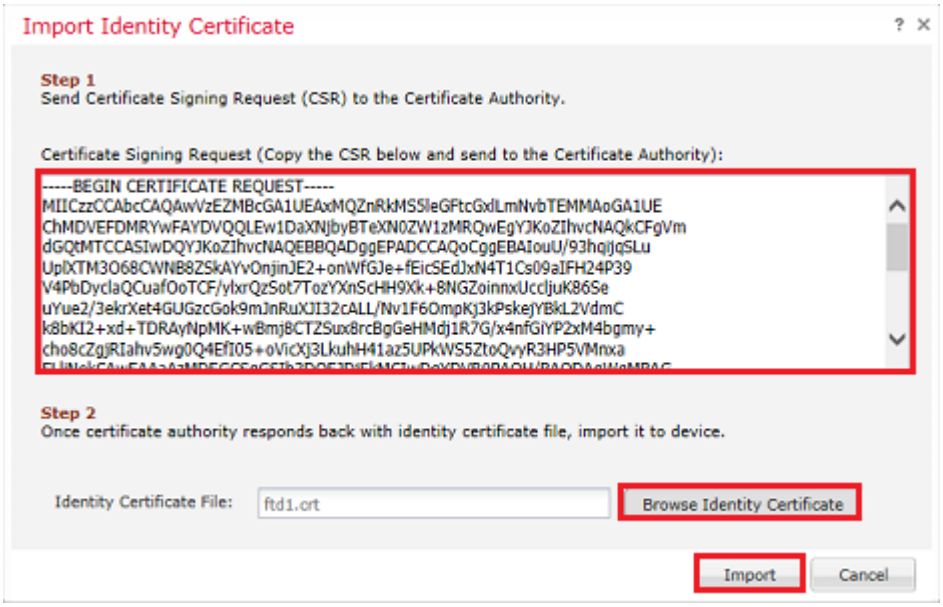
8.处理请求后，FMC提供添加身份证书的选项。单击ID按钮，如图所示。



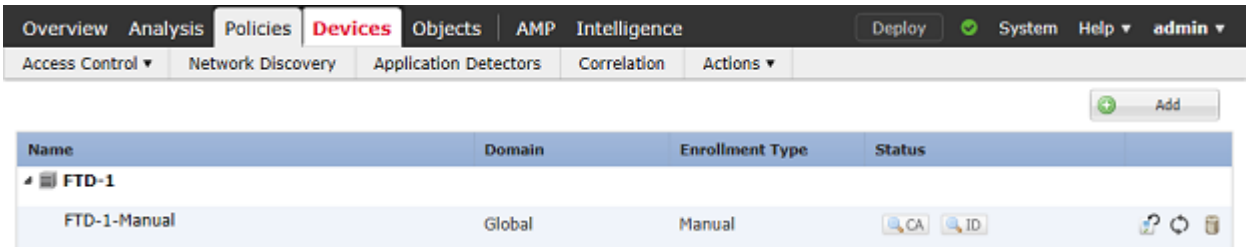
9.弹出一个窗口，通知生成CSR。单击Yes，如图所示。



10.接下来，生成可以复制并发送到CA的CSR。签署CSR后，提供身份证书。浏览到提供的身份证书并选择它，然后单击Import，如图所示。

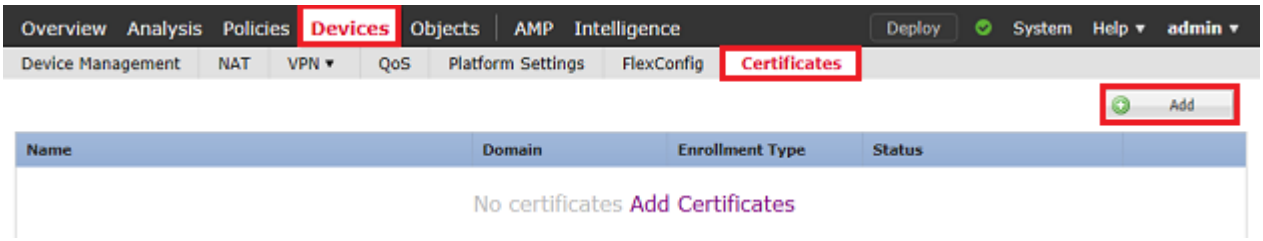


11.完成之后，手动证书如图所示。

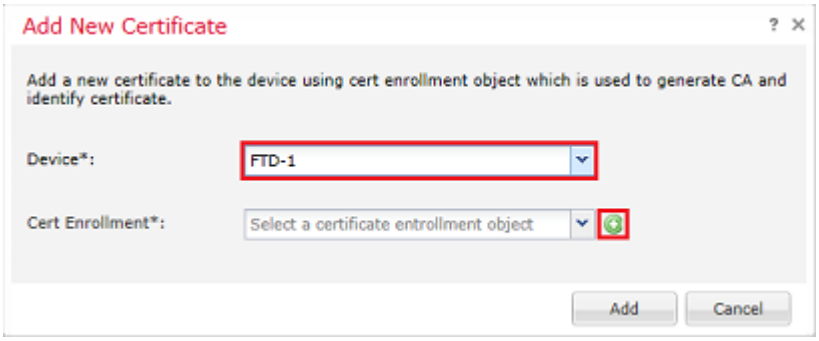


PKCS12注册

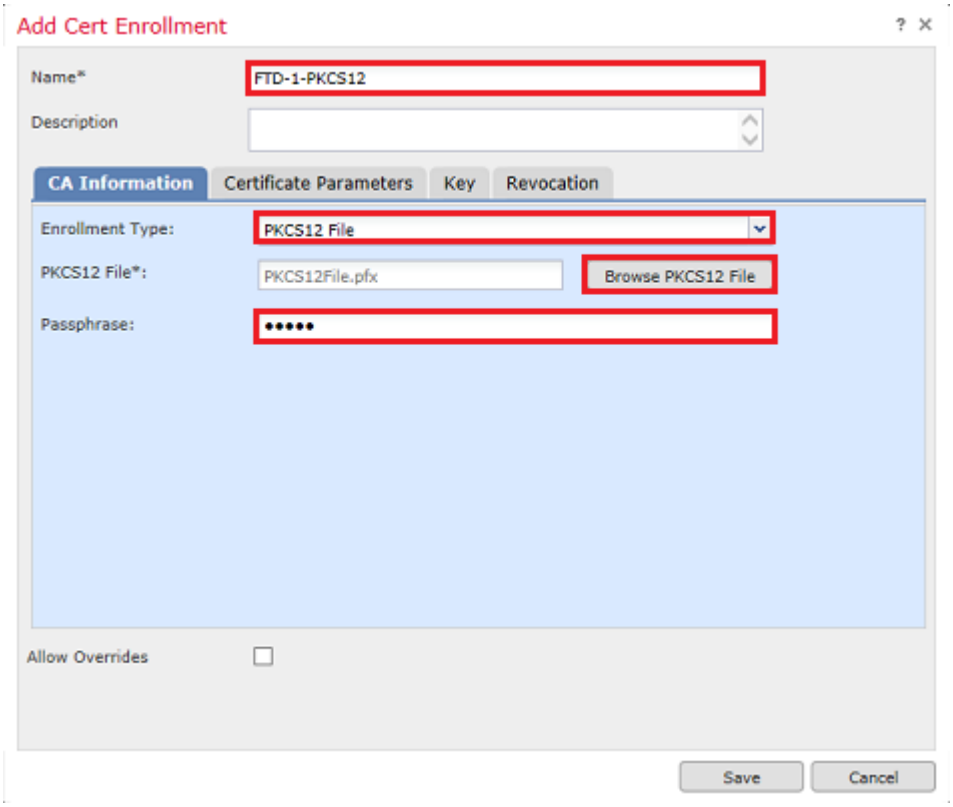
1.要安装已接收或已创建的PKCS12文件，请导航到设备>证书，然后单击添加（如图所示）。



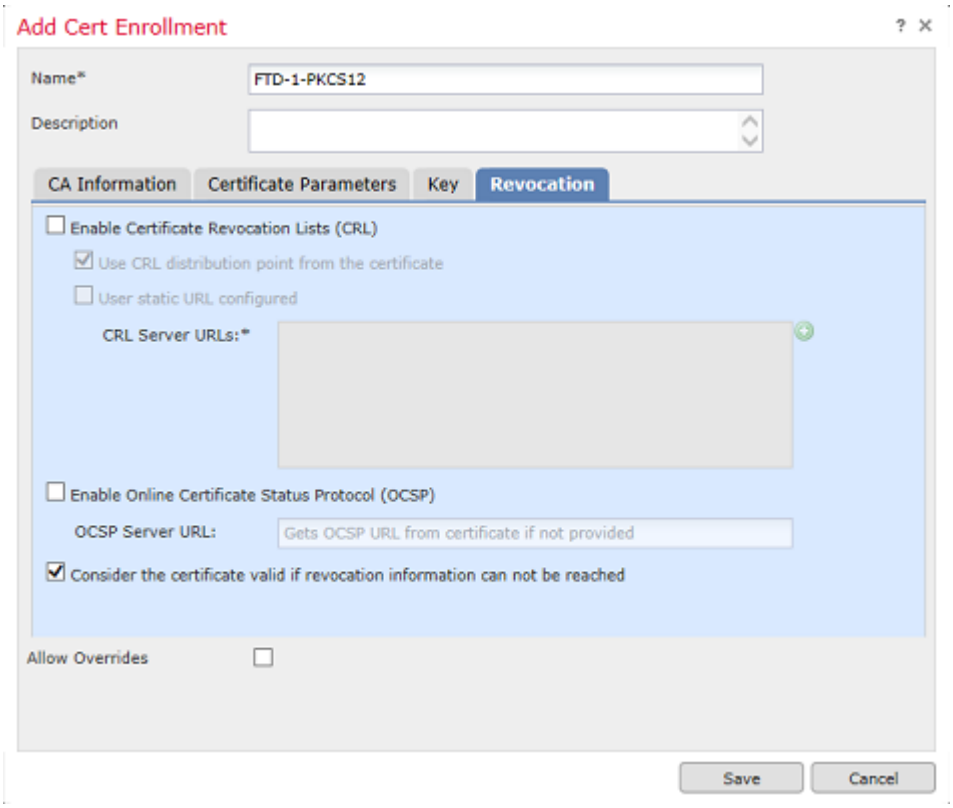
2.在Device*下拉菜单中选择证书添加到的设备，然后单击绿色+符号，如图所示。



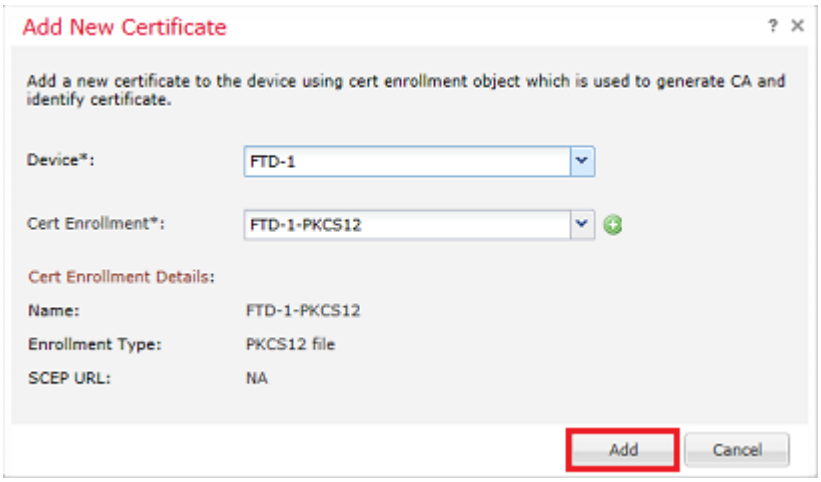
3.指定信任点的名称，然后在“CA信息”选项卡下，选择“注册类型”：PKCS12文件。浏览到创建的PKCS12文件并选择该文件。输入创建PKCS12时使用的密码，如图所示。



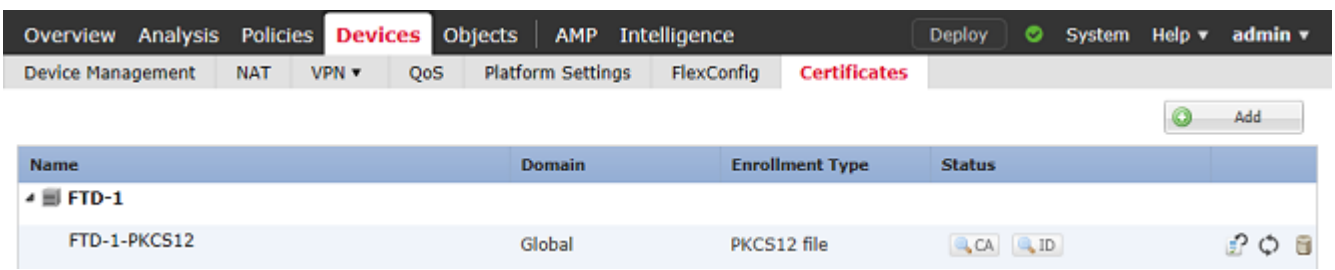
4.（可选）Certificate Parameters和Key选项卡显示为灰色，因为它们是使用PKCS12创建的，但是，可以修改启用CRL和/或OCSP撤销检查的Revocation选项卡。默认情况下，两者均未按照映像中所示进行检查。



5.完成后，单击保存，然后单击添加（如图所示）。



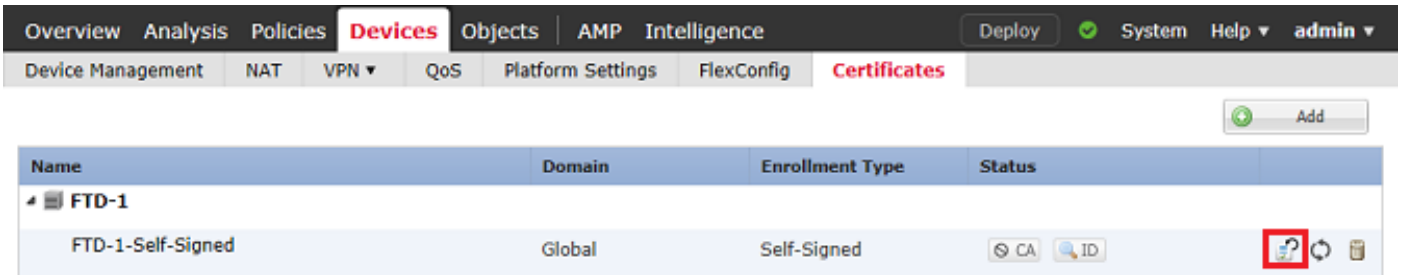
6.完成后，PKCS12证书如图所示。



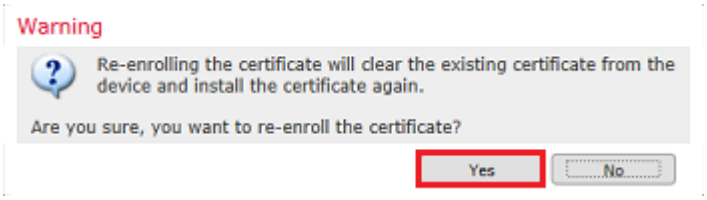
证书续订

自签名证书续订

1.按Re-enroll certificate按钮，如图所示。



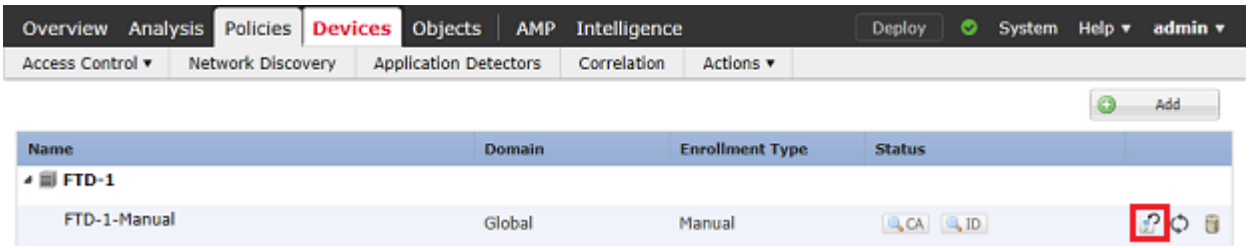
2.系统将显示一个窗口，提示已移除并替换自签名证书。单击Yes，如图所示。



3.续签自签名将被推送至金融交易税办公室。单击ID按钮并选中Valid time（有效时间）可以验证这一点。

手动证书续订

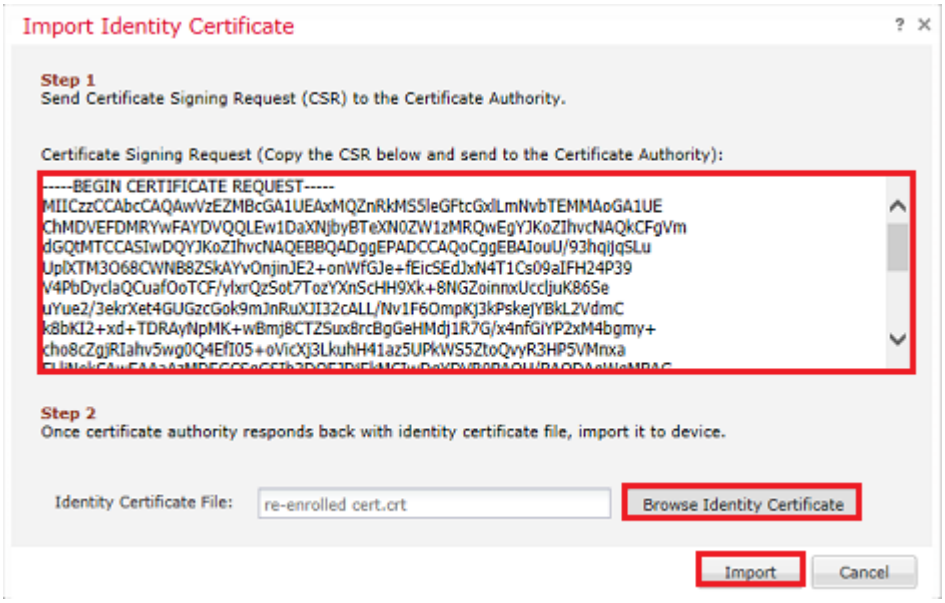
1.按Re-enroll certificate按钮，如图所示。



2.窗口将提示生成证书签名请求。单击Yes，如图所示。



3.在此窗口中，生成CSR，可以将其复制并发送到之前签署身份证书的同一CA。CSR签名后，提供续订的身份证书。浏览到提供的身份证书并选择它，然后单击Import，如图所示。



4.更新后的手动证书将推送到FTD。单击ID按钮并选中Valid time（有效时间）可以验证这一点。

PKCS12续订

如果点击re-enroll certificate按钮，则不会续订证书。要更新PKCS12，需要使用前面提到的方法创建和上传新的PKCS12文件。

使用OpenSSL创建PKCS12

1.使用OpenSSL或类似应用程序生成私钥和证书签名请求(CSR)。 此示例显示一个名为private.key的2048位RSA密钥和一个在OpenSSL中创建的ftd1.csr:

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd1.csr
Generating a 2048 bit RSA private key
.....................................+++
.....................................................................................+++
written to a new private key to 'private.key'
-----
You are about to be asked to enter information that is incorporated
```

```
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', the field is left blank.
-----
Country Name (2 letter code) [AU]:.
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd1.example.com
Email Address []:.

Please enter these'extra'attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

2.复制生成的CSR并将其发送到CA。签署CSR后，提供身份证书。通常还会提供CA证书。要创建PKCS12，请在OpenSSL中运行以下命令之一：

要仅包括在PKCS12中颁发的CA证书，请使用以下命令：

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -certfile ca.crt
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

- ftd.pfx是由openssl导出的pkcs12文件的名称（采用der格式）。
- ftd.crt是CA以pem格式颁发的签名身份证书的名称。
- private.key是在步骤1中创建的密钥对。
- ca.crt是以pem格式颁发的证书颁发机构的证书。

如果证书是带根CA和1个或多个中间CA的链的一部分，则此命令可用于在PKCS12中添加完整的链：

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -chain -CAfile cachain.pem
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

- ftd.pfx是由OpenSSL导出的pkcs12文件的名称（格式为der）。
- ftd.crt是CA以pem格式颁发的签名身份证书的名称。
- private.key是在步骤1中创建的密钥对。
- cachain.pem是一个文件，它包含链中的CA证书，以发出中间CA开头，以pem格式的根CA结尾。

如果返回PKCS7文件(.p7b， .p7c)，这些命令也可用于创建PKCS12。如果p7b格式为der，请确保将add-inform der添加到参数中，否则不要包含它：

```
openssl pkcs7 -in ftd.p7b -inform der -print_certs -out ftdpem.crt

openssl pkcs12 -export -in ftdpem.crt -inkey private.key -out ftd.pfx
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

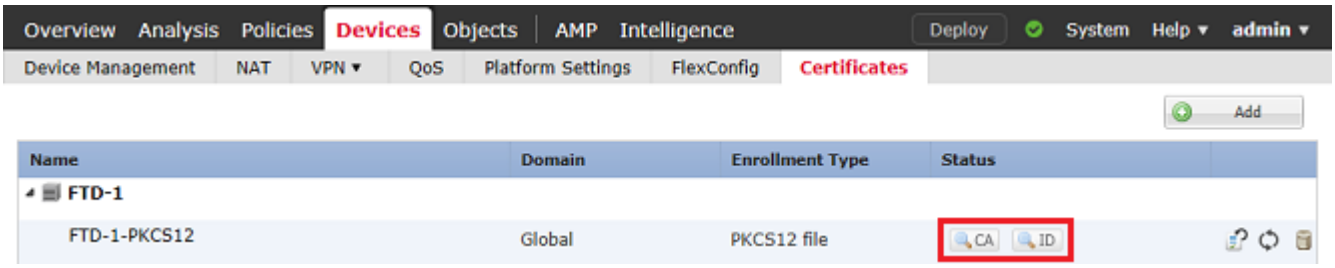
- ftd.p7b是CA返回的PKCS7，其中包含已签名的身份证书和CA链。
- ftdpem.crt是转换后的p7b文件。
- ftd.pfx是由OpenSSL导出的pkcs12文件的名称（格式为der）。
- private.key是在步骤1中创建的密钥对。

验证

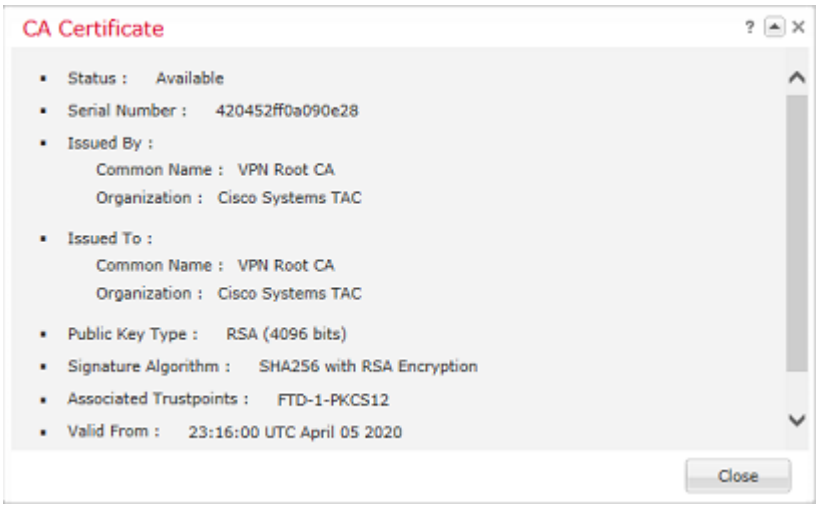
使用本部分可确认配置能否正常运行。

查看FMC中安装的证书

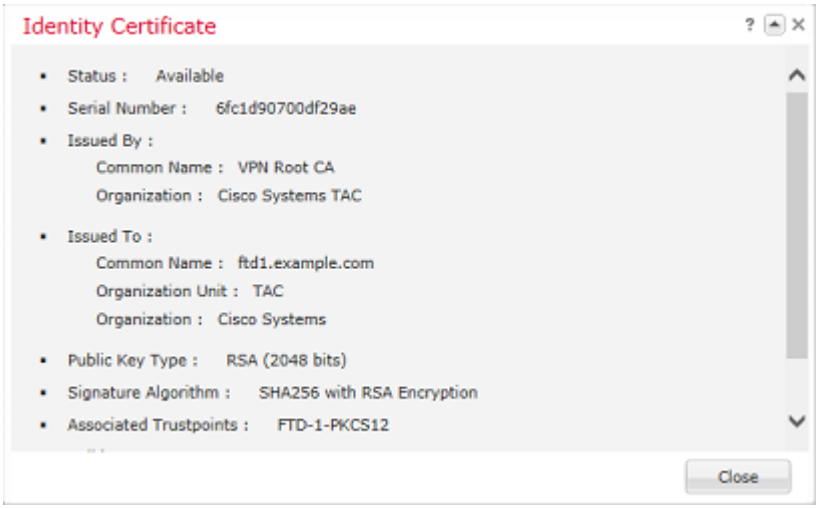
在FMC中，导航到设备>证书。对于相关信任点，请点击CA或ID以查看有关证书的详细信息，如图所示。



如图所示验证CA证书。



如图所示验证身份证书。



在CLI中查看已安装的证书

通过SSH连接到FTD，然后输入命令show crypto ca certificate。

```
> show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 6fc1d90700df29ae
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Subject Name:
    cn=ftd1.example.com
    ou=TAC
    o=Cisco Systems
  Validity Date:
```

```
    start date: 15:47:00 UTC Apr 8 2020
    end   date: 15:47:00 UTC Apr 8 2021
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12

CA Certificate
  Status: Available
  Certificate Serial Number: 420452ff0a090e28
  Certificate Usage: General Purpose
  Public Key Type: RSA (4096 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Subject Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Validity Date:
    start date: 23:16:00 UTC Apr 5 2020
    end   date: 23:16:00 UTC Apr 5 2030
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

调试命令

在SSL证书安装失败的情况下，FTD通过SSH连接后，可以从诊断CLI运行调试：

debug crypto ca 14

在FTD的早期版本中，以下调试可用且建议用于故障排除：

debug crypto ca 255

debug crypto ca message 255

debug crypto ca transaction 255

常见问题

导入已颁发的身份证书后，仍会看到消息“需要导入身份证书”。

出现这种情况可能是因为两个单独的问题：

1.手动注册时未添加颁发的CA证书

导入身份证书后，系统会根据手动注册时在CA Information选项卡下添加的CA证书检查身份证书。有时，网络管理员没有用于签署其身份证书的CA的CA证书。在这种情况下，当您执行手动注册时，必须添加占位符CA证书。在颁发身份证书并提供CA证书后，可以使用正确的CA证书完成新的手动注册。再次完成手动注册向导时，请确保为密钥对指定与原始手动注册中相同的名称和大小。完成后，不再使用CSR再次转发到CA，之前颁发的身份证书可以使用正确的CA证书导入到新创建的信任点。

要检查在手动注册时是否应用了相同的CA证书，请点击Verify部分中指定的CA按钮，或检查show crypto ca certificates的输出。“颁发给”和“序列号”等字段可与证书颁发机构提供的CA证书中的字段进行比较。

2.创建的信任点中的密钥对不同于为已颁发的证书创建CSR时使用的密钥对。

通过手动注册，当生成密钥对和CSR时，公共密钥会添加到CSR，以便可以包含在颁发的身份证书中。如果由于某种原因，修改了FTD上的密钥对，或者颁发的身份证书包含其他公钥，则FTD不会安装颁发的身份证书。要检查是否发生这种情况，有两种不同的测试：

在OpenSSL中，可以发出以下命令来将CSR中的公钥与已颁发证书中的公钥进行比较：

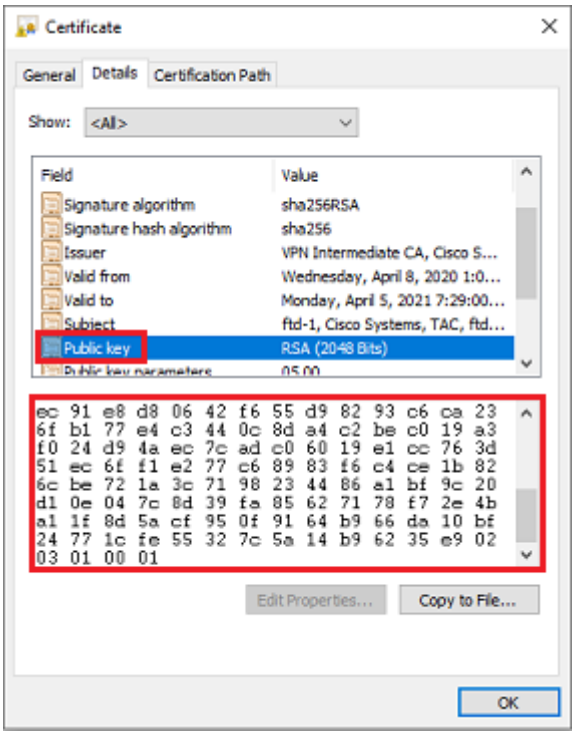
```
openssl req -noout -modulus -in ftd.csr
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B
B966DA10BF24771CFE55327C5A14B96235E9

openssl x509 -noout -modulus -in id.crt
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B
B966DA10BF24771CFE55327C5A14B96235E9
```

- ftd.csr是手动注册时从FMC复制的CSR。
- id.crt是CA签名的身份证书。

或者，也可以将FTD上的公钥值与颁发的身份证书中的公钥进行比较。由于填充，证书中的前几个字符与FTD输出中的字符不匹配：

已在Windows PC上打开颁发的身份证书：



从身份证书提取的公钥输出：

```
3082010a02820101008a2e53ff7786a8a3a922ee5299574ccdceebc096341f194a4018bce9e38a7244dbea2759f1897be7c489c
f6e0fdfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b8af3a49
1b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8da4c2bec
e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f8d5acf9
55327c5a14b96235e90203010001
```

Show crypto key mypubkey rsa从FTD的输出。完成手动注册后，<Default-RSA-Key>用于创建CSR。加粗部分匹配从身份证书提取的公钥输出。

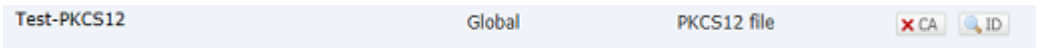
```
> show crypto key mypubkey rsa
Key pair was generated at: 16:58:44 UTC Jan 25 2019
 Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Storage: config
 Key Data:

  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
  008a2e53 ff7786a8 a3a922ee 5299574c cdceebc0 96341f19 4a4018bc e9e38a72
  44dbea27 59f1897b e7c489c4 84749c4d e13d42b3 4f5a2051 f6e0fdfd 5783db0f
  27256900 ae69f3a8 4c217fca 5c6b4334 a8b7b4e8 cd85e749 c1c7f579 3ef0d199
  a229e7c5 471c963b 8af3a49e b98b9edb fdde92b5 deb78194 1b3706a2 4f662674
  6e5c9237 d9c00b2f f36fd45e 8e9a92a3 de43ec91 e8d80642 f655d982 93c6ca23
  6fb177e4 c3440c8d a4c2bec0 19a3f024 d94aec7c adc06019 e1cc763d 51ec6ff1
  e277c689 83f6c4ce 1b826cbe 721a3c71 98234486 a1bf9c20 d10e047c 8d39fa85
```

```
  627178f7 2e4ba11f 8d5acf95 0f9164b9 66da10bf 24771cfe 55327c5a 14b96235
  e9020301 0001
```

FMC中CA旁边的红色X。

PKCS12注册时可能会出现这种情况，因为CA证书不包含PKCS12软件包中。



要解决此问题，PKCS12需要添加CA证书。

发出这些命令以提取身份证书和私钥。需要创建PKCS12时使用的密码和安全私钥：

```
openssl pkcs12 -info -in test.p12
Enter Import Password: [pkcs12 pass phrase here]
MAC Iteration 1
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    friendlyName: Test
    localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
subject=/CN=ftd1.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Intermediate CA
-----BEGIN CERTIFICATE-----
MIIC+TCCAeGgAwIBAgIIAUIM3+3IMhIwDQYJKoZIhvcNAQELBQAwOjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxHDAaBgNVBAMTE1ZQTiBJbnRlcm1lZGlhdGUg
Q0EwHhcNMjAwNDA4MTY1ODAwWhcNMjEwNDA1MjMyOTAwWjAbMRkwFwYDVQQDExBm
dGQxLmV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
043eLVPl8K0jnYfHCBZuFUYrXTTB28Z1ouIJ5yyrDzCN781GFrHb/wCczRx/jW4n
pF9q2z7FHr5bQCI4oSUSX40UQfr0/u0K5riI1uZumPUx1Vp1zVkYuqDd/i1r0+0j
PyS7BmyGfV7aebYWZnr8R9ebDsnC2U3nKjP5RaE/wNdVGTS/180HlrIjMpcFMXps
LwxdxiEz0hCMnDm9RC+7uWZQdlwZ9oNANCbQC0px/Zikj9Dz7ORhhbzBTeUNKD3p
sN3VqdDPvGZHFGlPCnhKYyZ79+6p+CHC8X8BFjuTJYoo1l6uGgiB4Jz2Y9ZeFSQz
Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBglghkgBhvhCAQ0EERYPeGNhIGNl
cnRpZmljYXRlMA0GCSqGSIb3DQEBCwUAA4IBAQCV/MgshWxXtwpwmMF/6KqEj8nB
Sljbfzl zNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRyY54taRI27W+gLneCbQAux
9amxXuhpxP5EOhnk+tsYS9eriAKpHuS1Y/2uwN92fHIbh3HEXPO1HBJueI8PH3ZK
4lrPKA9oIQPUW/uueHEF+xCbG4xCLi5HOGeHX+FTigGNqazaX5GM4RBUa4bk8jks
Ig53twvop71wE53COTHOEkSRCsVCw5mdJsd9BUZHjguhpw8Giv7Z36qWv18I/Owf
RhLhtsgenc25udglvv9Sy5xK53a5Ieg8biRpWL9tIjgUgjxYZwtyVeHi32S7
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    friendlyName: Test
    localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
Key Attributes: <No Attributes>
Enter PEM pass phrase: [private-key pass phrase here]
Verifying - Enter PEM pass phrase: [private-key pass phrase here]
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIlKyWXk8cgTMCAggA
```

MBQGCCqGSIb3DQMHBAgGmOqRXh/dcwSCBMiF7BpgJNIpHdU5Zorn1jm3pmsI/XkJ
MRHc1Reel0ziSLCZ0STr84JFQxNpbThXLhsHC9WhpPy5sNXIvXS7Gu+U10/VlNSA
rWlX6SPftAYiFq5QXyEutSHdZZwgQIqpj97seu3Px0agvIObW1Lo8or5lSydnMjp
Ptv5OKo95BShWWYcqkTAia4ZKxytyIc/mIu5m72LucOFmoRBO5JZu1avWXjbCAA+
k2ebkblFT0YRQT1Z4tZHSqX1LFPZe17ONZEUg7rIcWAk1Yw7XNUPhOn6FHL/ieIZ
IhvIfj+1gQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E
Gnh8r3l9O3AlkPMBkMdxOqlpzo2naIy2KGrUnOSHajVWcLr9dTPWIDyjdn95YoeS
IUE7MaOOpjJcO2FNBwyNxRrYt+4hp3aJt0ZW83FHiSlB5UIzGrBMAgKJc2Hb2RTV
9gxZGve1cRcolLeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShnOwHzridF8Zn
FO6XvBDSyuXVSpkxwAdlTwxq62tUnLIkyRXo2CSz8z8W29UXmFO4o3G67n28//LJ
Ku8wj1jeqlvFgXSQiWLADNhIY772RNwzCMeobfxGlBprF9DPT8yvyBdQviUIuFpJ
nNs5FYbLTv9ygZ1S9xwQpTcqEu+y4F5BJuYLmHqcZ+VpFA4nMOYHhZ5M3sceRSR4
1L+a3BPJJshlTIJQgOTIxDaveCfpDcpS+ydUgS6YWY8xW17vO+1f7y5zlt4TkZRt
ItBHHA6yDzROCnO/ZH3y88a/asDcukw6bsRaY5iT8nAWgTQVed3xXj+EgeRs25HB
dIBBX5gTvqN7qDanhkaPUcEawj1/38MOpAYULei3elfKKrhwAySBFaV/BeUMWuNW
BmKprkKKQv/JdWnoJl49KcS4bfa3GHG9XXnyvbg8HxopcYFMTEjao+wLZH9agqKe
YOjyoHFN6ccBBC7vn7u12tmXOM5RcnPLmaDaBFDSBBFS8Y8VkeHn3POq7+sEQ26d
vL8O7WdgLH/wKqovoJRyxwzz+TryRq9cd5BNyyLaABESalsWRhk81C2P+B+Jdg9w
d6RsvJ2dt3pdl/+pUR3CdC0b8qRZOoLO3+onUIUoEsCCNdpOx8Yj/mvc6ReXtOKB
2qVmhVMYseiUlrOAQGt7XMe1UuiJ+dRnqcfAfbdGeOp+6epm1TK1BJL2mAlQWx5l
73Qo4M7rR7laeq/dqob3olPhcoMLa5z/Lo5vDe7S+LZMuAWjRkSfsoOKQOY3kAP1
eZ2Eh2go4eJ7hHf5VFqBLL8Ci3rd3EOijRkNm3fAQmFJlaFmooBM3Y2Ba+U8cMTH
lgjSFkl1FAWpfwx9aSEECNCvEMm1Ghm6/tJDLV1jyTqwajHnWIZCc+P2AXgnlLzG
HVVfxsOc8FGUJPQHatXYd7worWCxszauhfJ99E4PaoZnAOYUFw2jaZEwoONBPbD1
AjQ8aciuosv0FKpp/jXDI78/aYAEk662tPsfGmxvAWB+UMFarA9ZTiihK3x/tDPy
GZ6ByGWJYp/0tNNmJRCFhcAYY83EtzHK9h+8LatFA6WrJ4j3dhceUPzrPXjMffNN
0Yg=
-----END ENCRYPTED PRIVATE KEY-----

完成后，可以使用使用OpenSSL创建PKCS12的步骤2.中提到的步骤，将身份证书和私钥放入单独的文件中，并将CA证书导入到新的PKCS12文件中。

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）。