

在FDM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](#)

[配置](#)

[证书安装](#)

[自签名注册](#)

[手动注册](#)

[受信任CA证书安装](#)

[证书续订](#)

[常用OpenSSL操作](#)

[从PKCS12文件提取身份证书和私钥](#)

[验证](#)

[查看FDM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](#)

[导入ASA导出的PKCS12](#)

简介

本文档介绍如何在FTD上安装、信任和续订由第三方CA或内部CA签名的自签名证书和证书。

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证书颁发机构(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Firepower威胁防御(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FTDv。

- 对于密钥对和证书签名请求(CSR)的创建，使用OpenSSL。

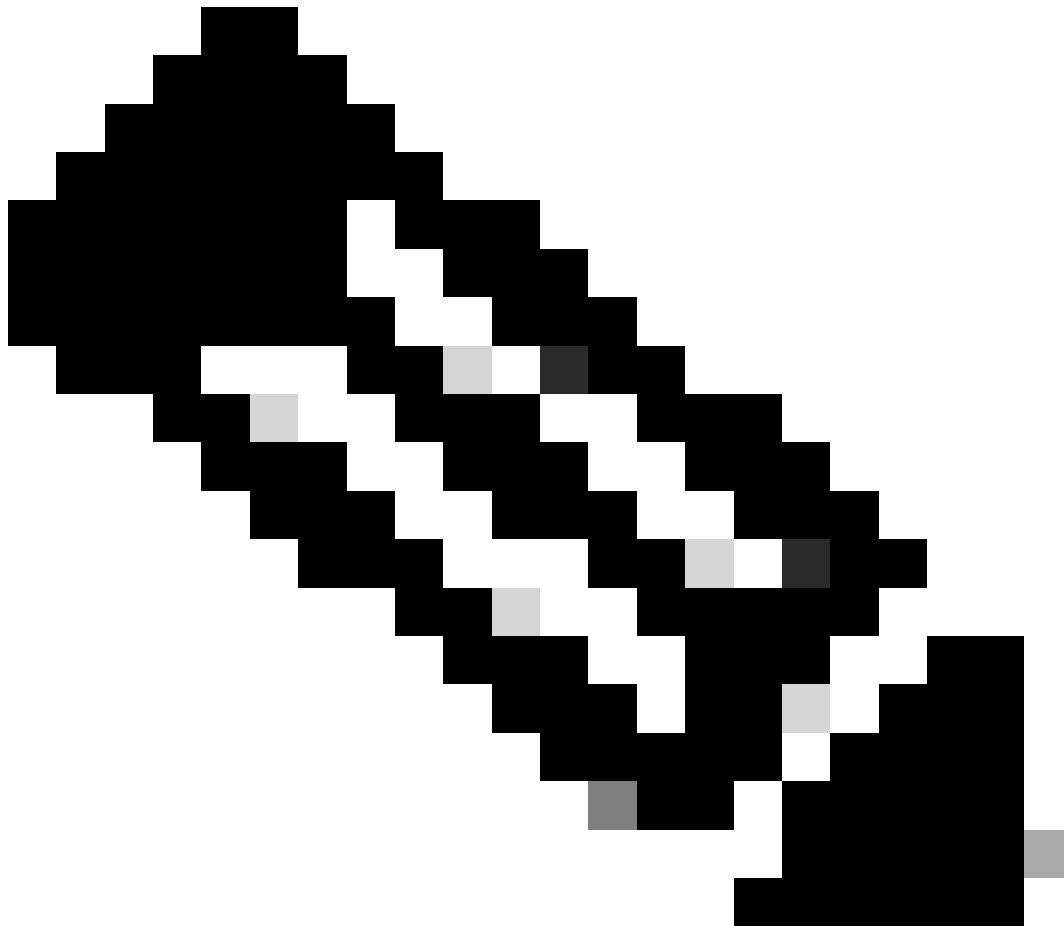
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

证书安装

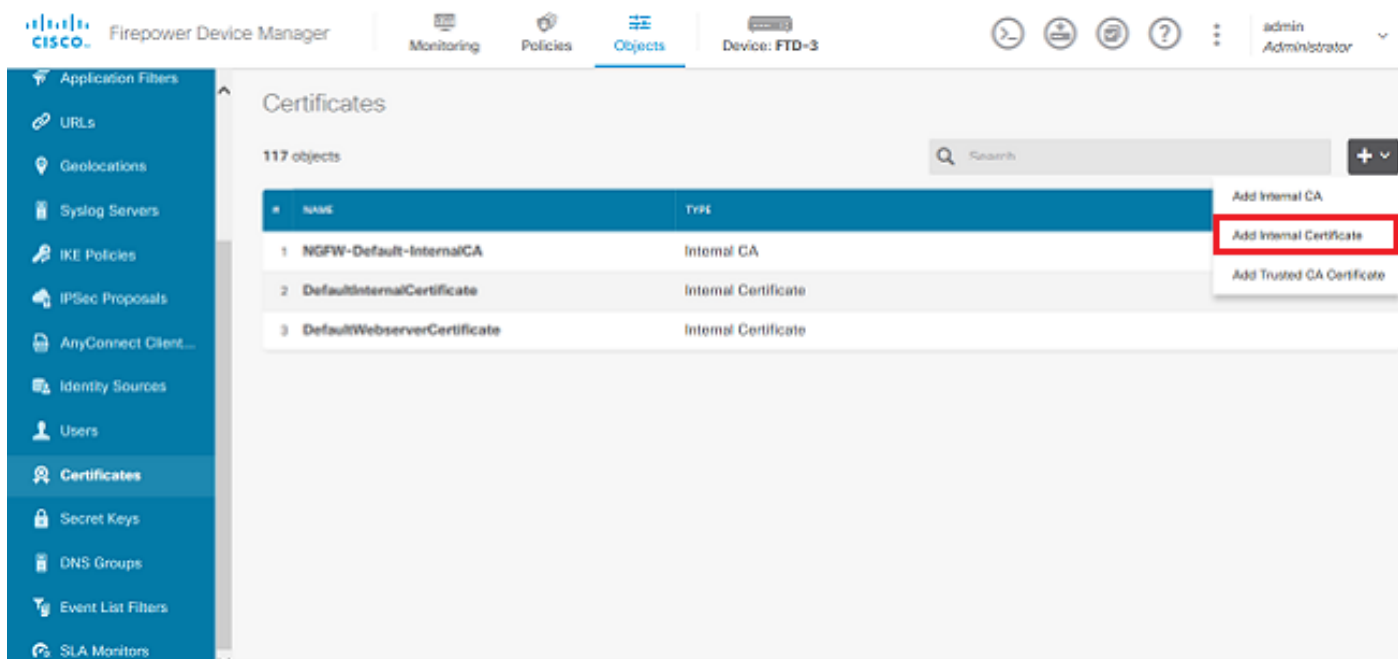
自签名注册

自签名证书是向FTD设备添加相应字段的证书的简单方法。虽然在大多数位置无法信任它们，但它们仍可提供与第三方签名证书类似的加密优势。尽管如此，仍建议使用受信任CA签名的证书，以便用户和其他设备能够信任FTD提供的证书。

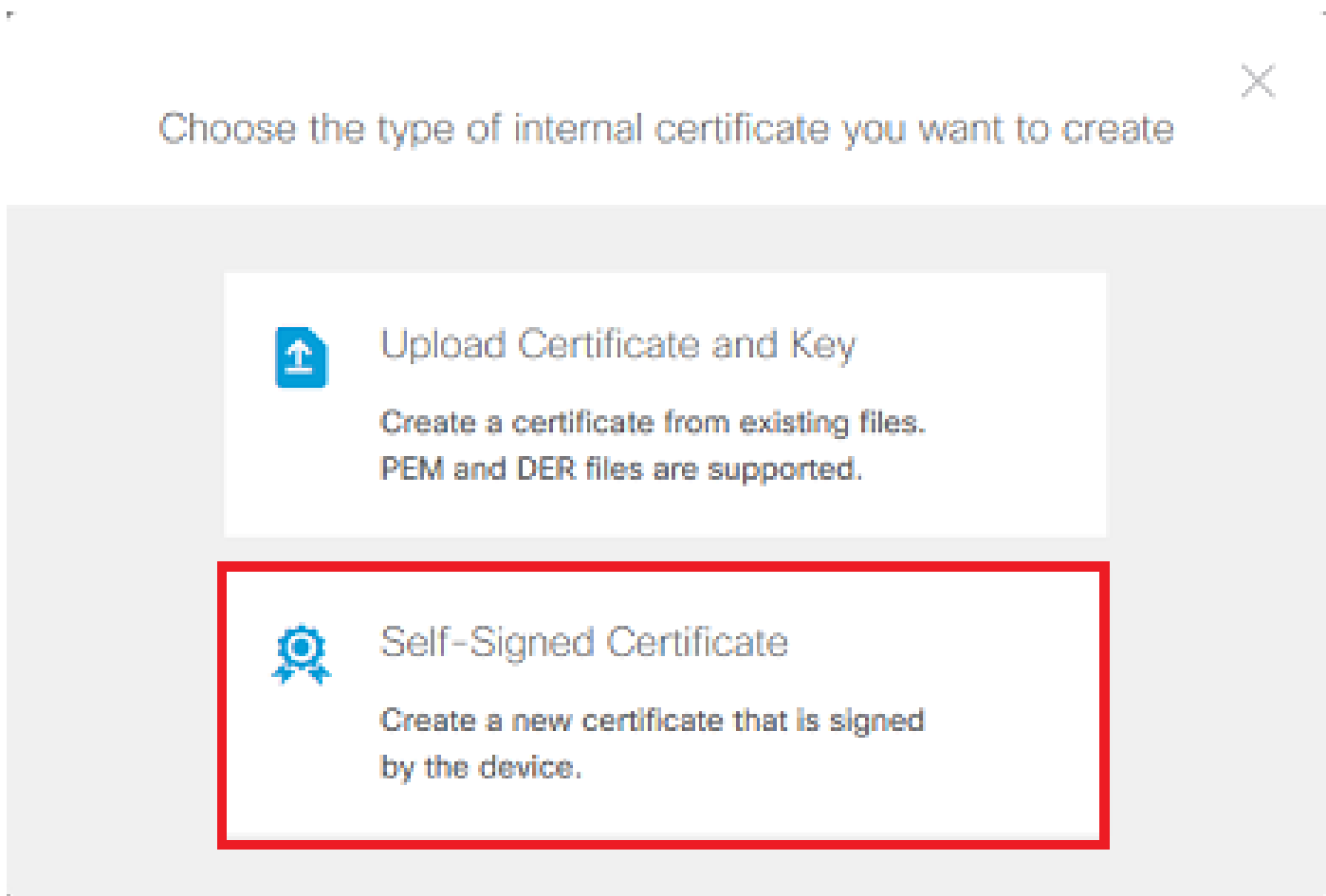


注意：Firepower设备管理(FDM)具有名为DefaultInternalCertificate的默认自签名证书，可用于类似用途。

1. 导航到对象>证书。单击+符号，然后选择添加内部证书（如图所示）。



2. 在弹出窗口中选择自签名证书（如图所示）。



3. 为信任点指定Name，然后填写主题可分辨名称字段。至少可以添加Common Name字段。这可以与使用证书的服务的完全限定域名(FQDN)或IP地址匹配。完成后，请单击Save（如图所示）。

Add Internal Certificate



Name

FTD-3-Self-Signed

Country

State or Province

Locality or City

Organization

Cisco Systems

Organizational Unit (Department)

TAC

Common Name

ftd3.example.com

You must specify a Common Name to use the certificate with remote access VPN.

CANCEL

SAVE

4. 单击屏幕右上方的待定更改按钮（如图所示）。

Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

admin Administrator

Application Filters

- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- AnyConnect Client...
- Identity Sources
- Users
- Certificates**
- Secret Keys
- DNS Groups
- Event List Filters
- SLA Monitors

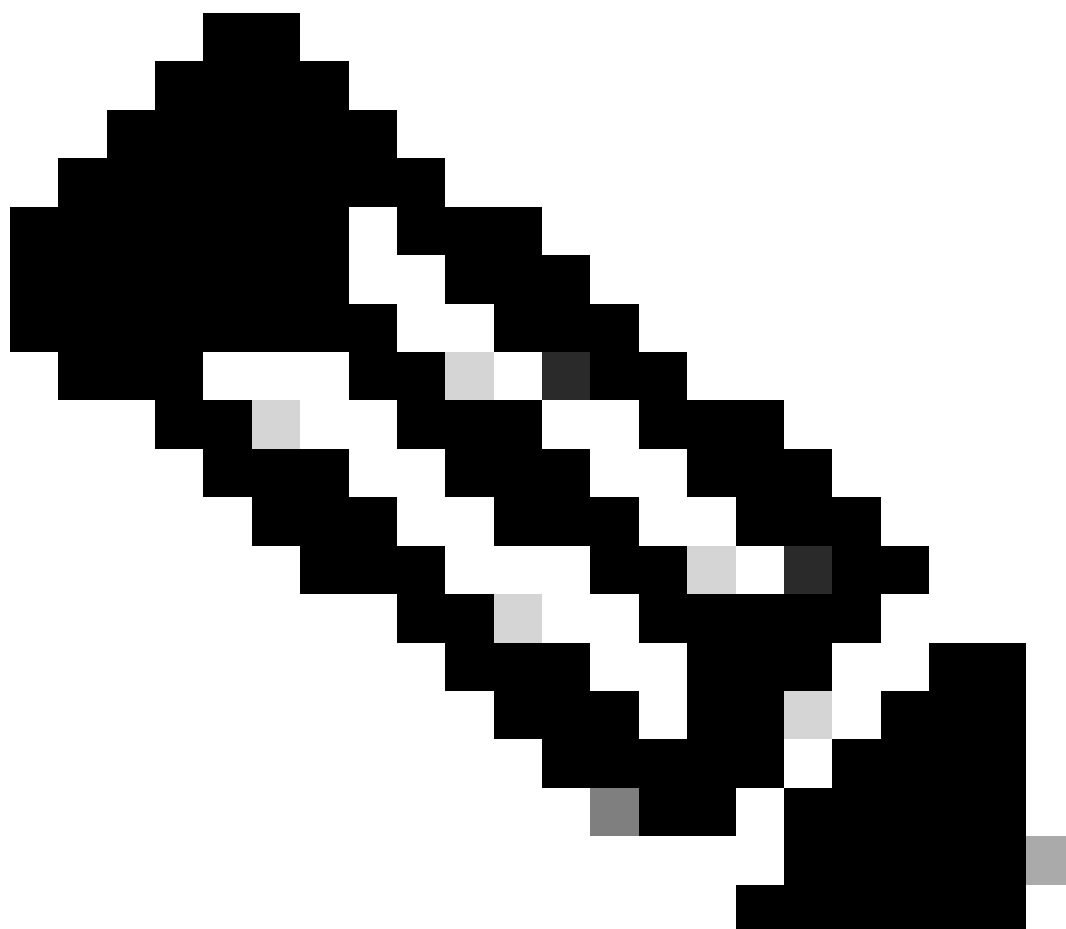
Certificates

118 objects

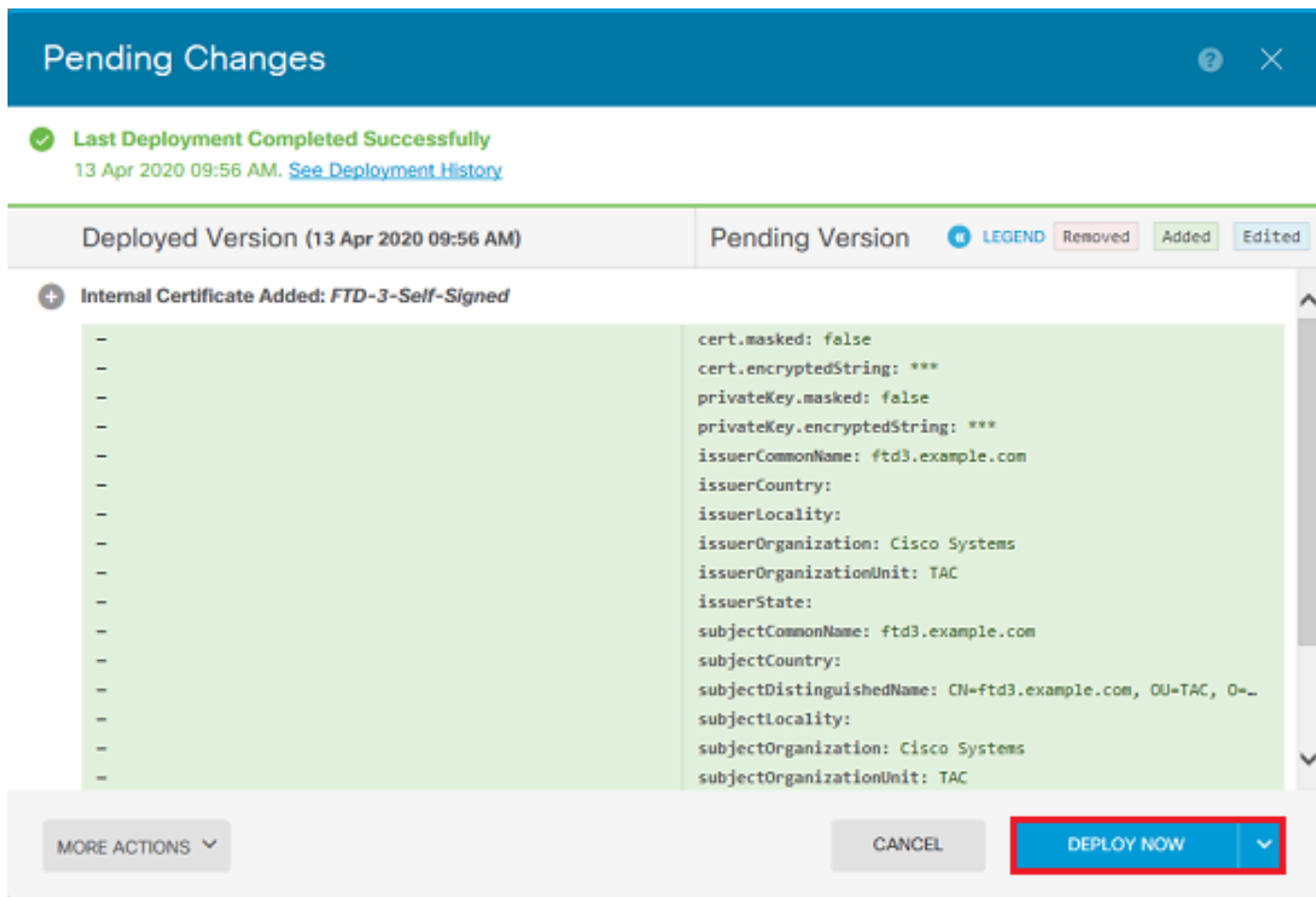
Search

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Self-Signed	Internal Certificate	

5. 单击Deploy Now按钮。



注意：部署完成后，只有在有使用证书的服务（如AnyConnect）后，才能在CLI中看到证书，如图所示。



手动注册

手动注册可用于安装受信任CA颁发的证书。OpenSSL或类似工具可用于生成接收CA签名证书所需的私钥和CSR。这些步骤涵盖用于生成私钥和CSR的常见OpenSSL命令，以及获取证书和私钥后安装证书和私钥的步骤。

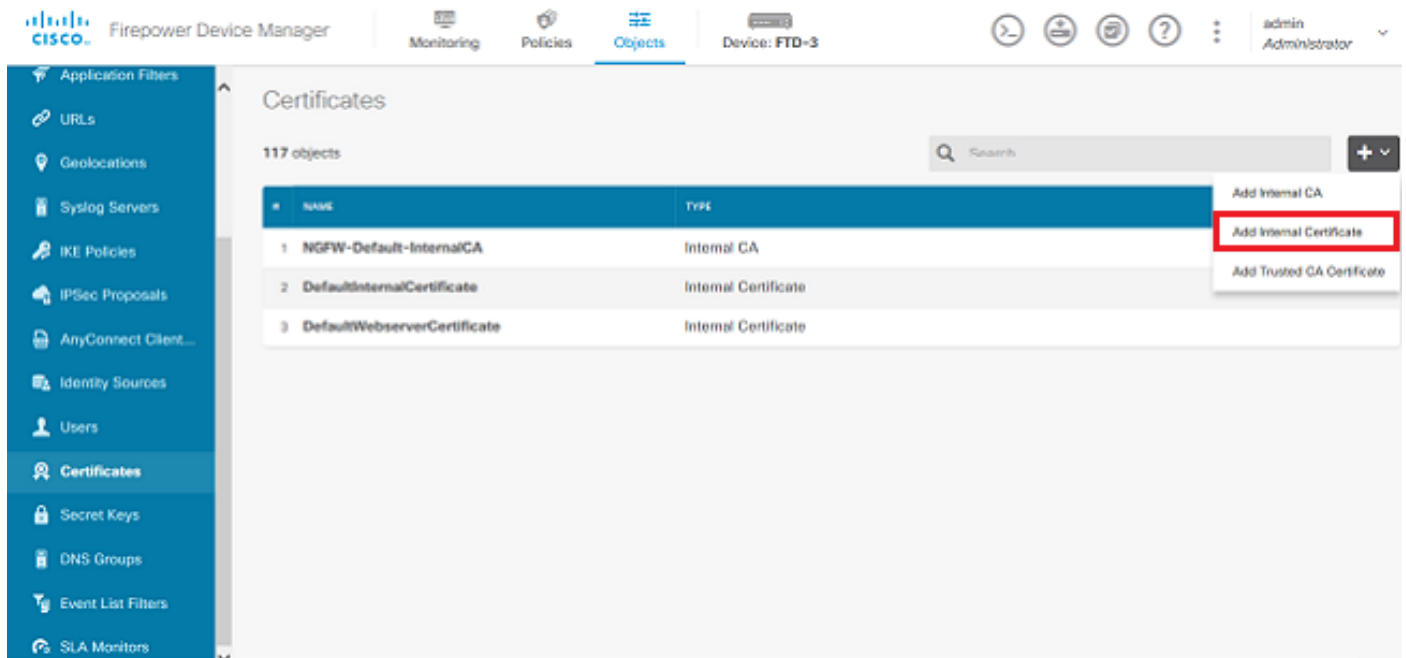
1. 使用OpenSSL或类似应用，生成私钥和证书签名请求(CSR)。本示例显示一个名为private.key的2048位RSA密钥和一个在OpenSSL中创建的名为ftd3.csr的CSR。

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
.....+++
.....+++
writing 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 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) []:ftd3.example.com
Email Address []:.

Please enter the following '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，系统会提供身份证书。
3. 导航到对象>证书。单击+符号，然后选择Add Internal Certificate (如图所示)。



4. 在弹出窗口中选择上传证书和密钥 (如图所示)。



Choose the type of internal certificate you want to create



Upload Certificate and Key

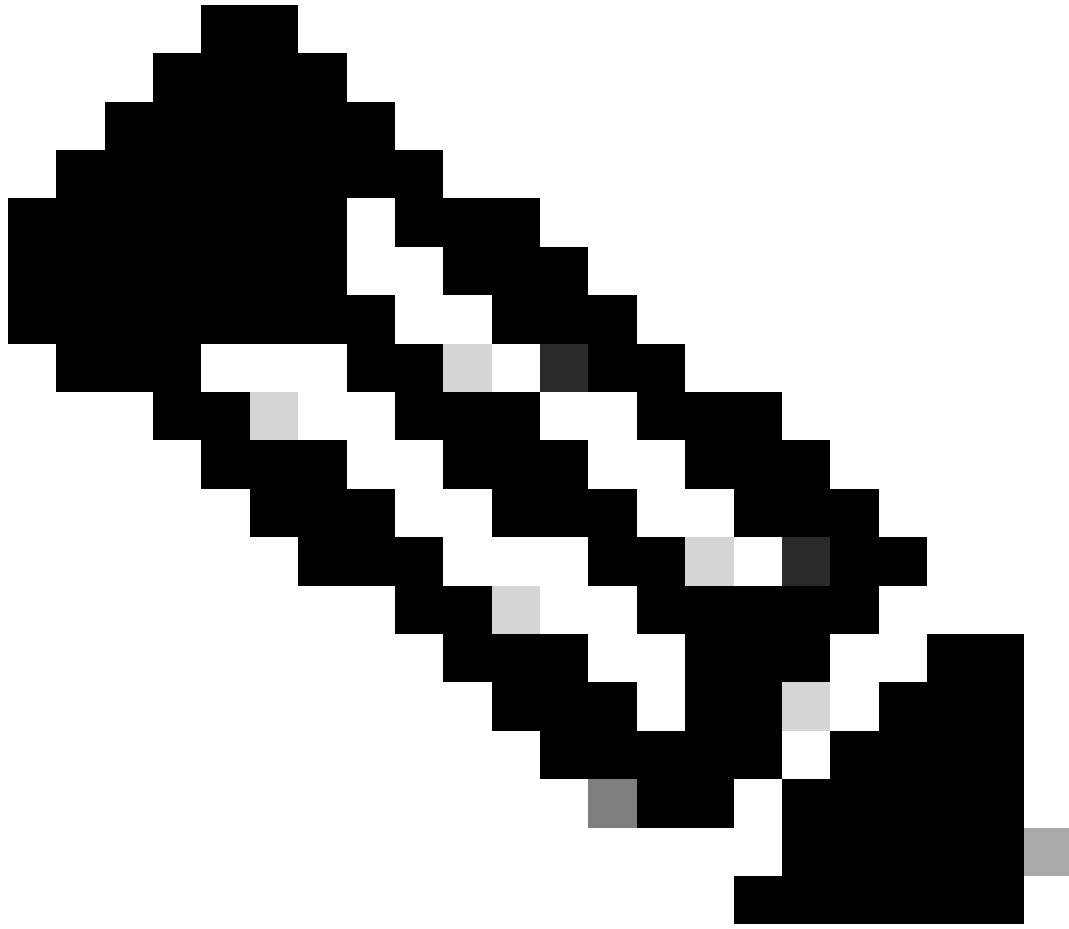
Create a certificate from existing files.
PEM and DER files are supported.



Self-Signed Certificate

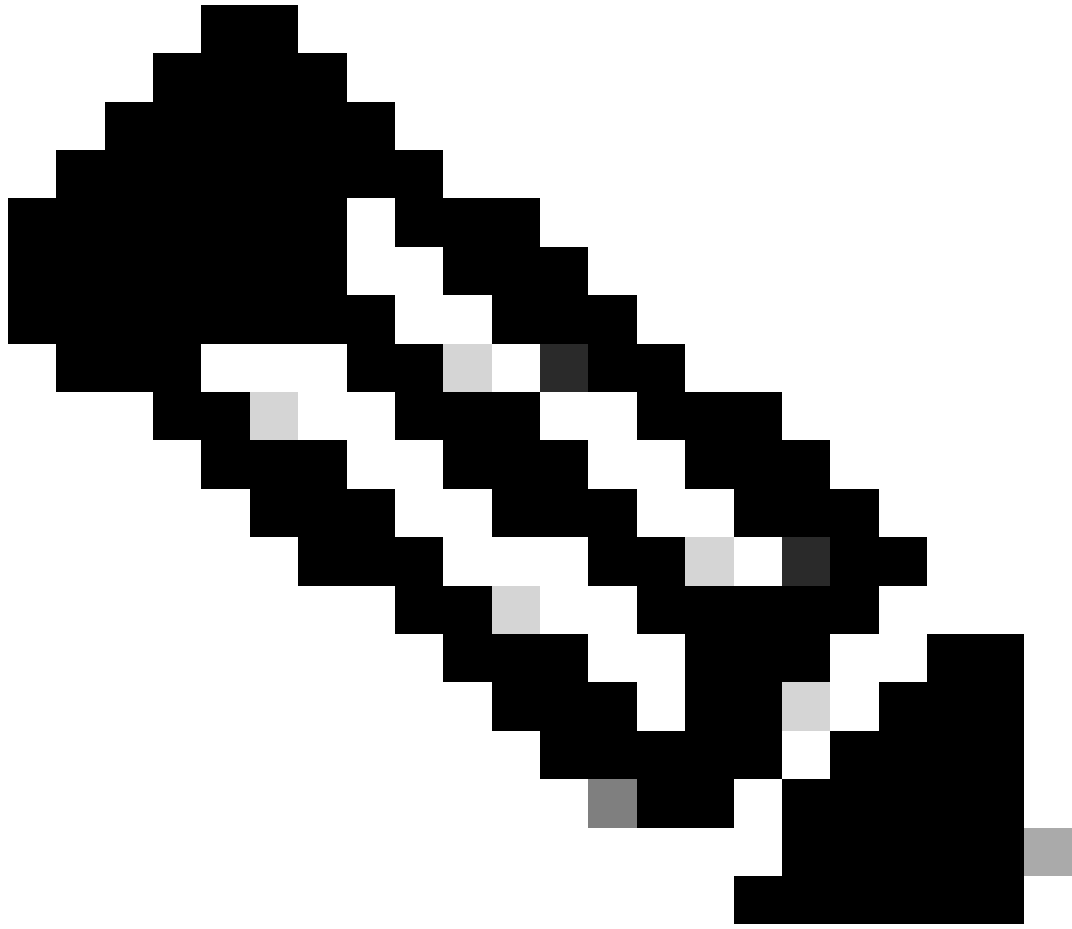
Create a new certificate that is signed
by the device.

5. 为信任点指定名称，然后上传或复制并粘贴身份证书和私有密钥，采用隐私增强型邮件(PEM)格式。如果CA在一个PKCS12中同时提供了证书和密钥，请导航到本文档后面的从PKCS12文件中提取身份证书和私钥部分以将它们分开。



注意：文件名不能有任何空格，或者FDM不接受它们。此外，不得对私钥进行加密。

完成后单击OK (如图所示)。



注意：部署完成后，只有在有使用证书的服务（如AnyConnect）后，才能在CLI中看到证书，如图所示。

Pending Changes ? X

✓ **Last Deployment Completed Successfully**
13 Apr 2020 09:56 AM. [See Deployment History](#)

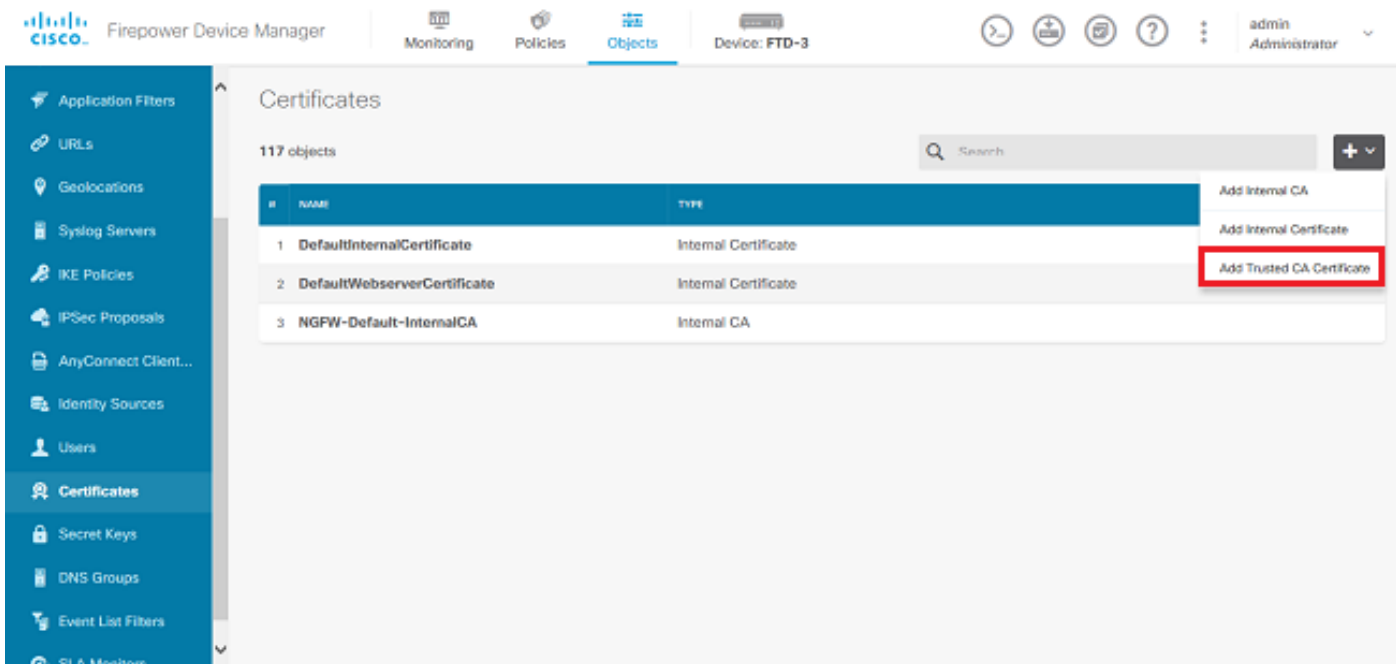
Deployed Version (13 Apr 2020 09:56 AM)	Pending Version
+ Internal Certificate Added: <i>FTD-3-Manual</i>	
<pre>cert.masked: false cert.encryptedString: *** privateKey.masked: false privateKey.encryptedString: *** issuerCommonName: VPN Root CA issuerCountry: issuerLocality: issuerOrganization: Cisco Systems TAC issuerOrganizationUnit: issuerState: subjectCommonName: ftd3.example.com subjectCountry: subjectDistinguishedName: CN=VPN Root CA, O=Cisco Systems.. subjectLocality: subjectOrganization: Cisco Systems subjectOrganizationUnit: TAC</pre>	

MORE ACTIONS ▾ CANCEL **DEPLOY NOW** ▾

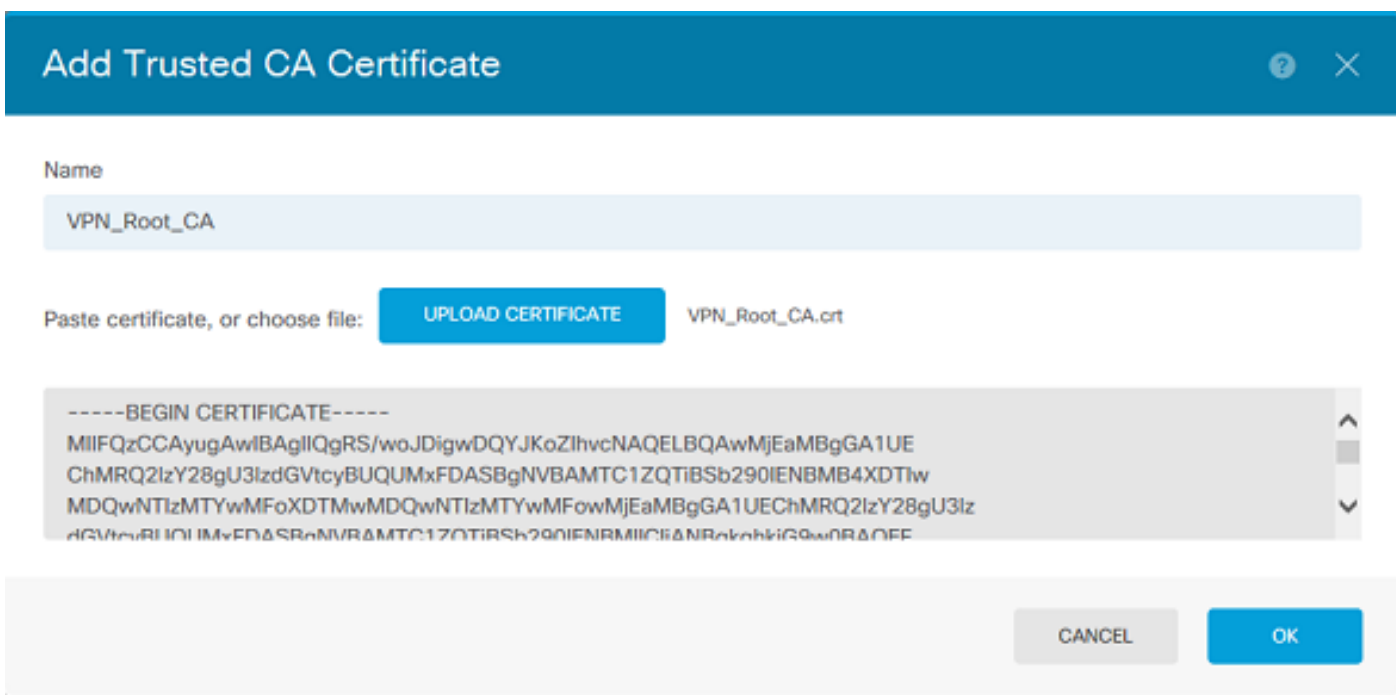
受信任CA证书安装

安装受信任CA证书时，必须成功对向FTD提供身份证书的用户或设备进行身份验证。常见示例包括AnyConnect证书身份验证和S2S VPN证书身份验证。这些步骤介绍如何信任CA证书，以便该CA颁发的证书也受信任。

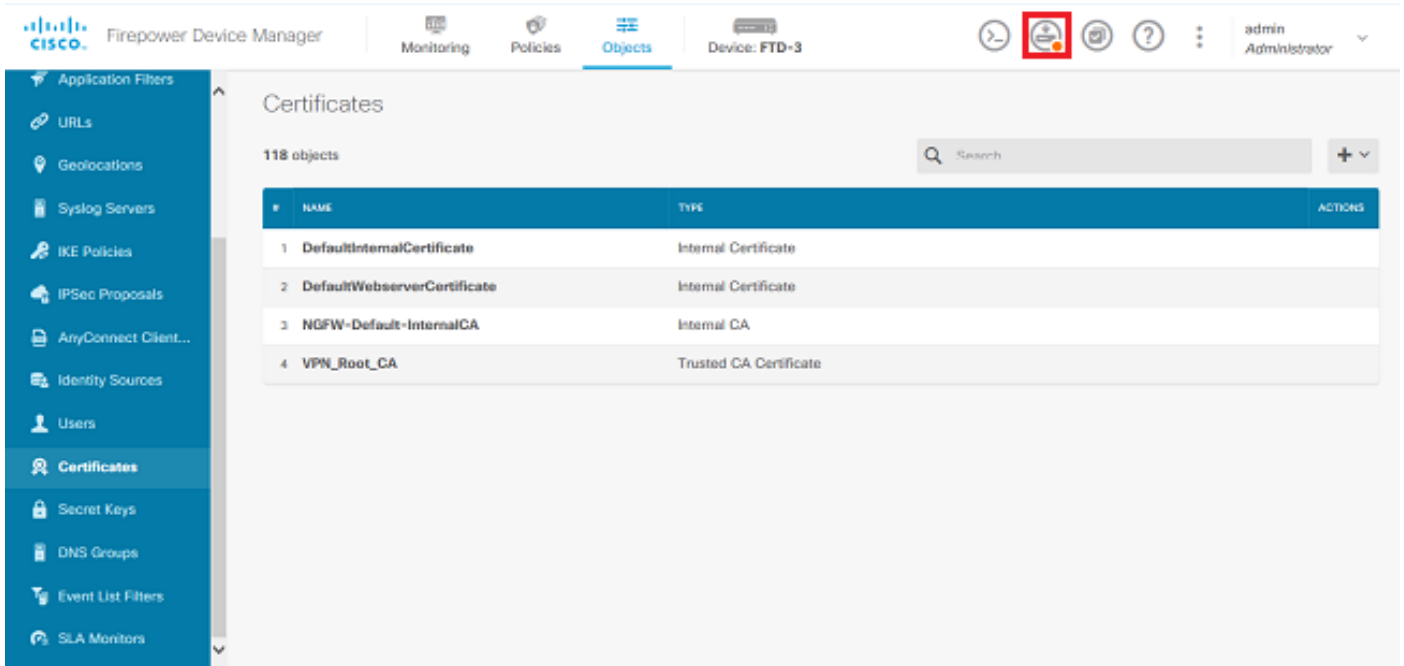
1. 导航到对象>证书。单击+符号，然后选择添加受信任CA证书（如图所示）。



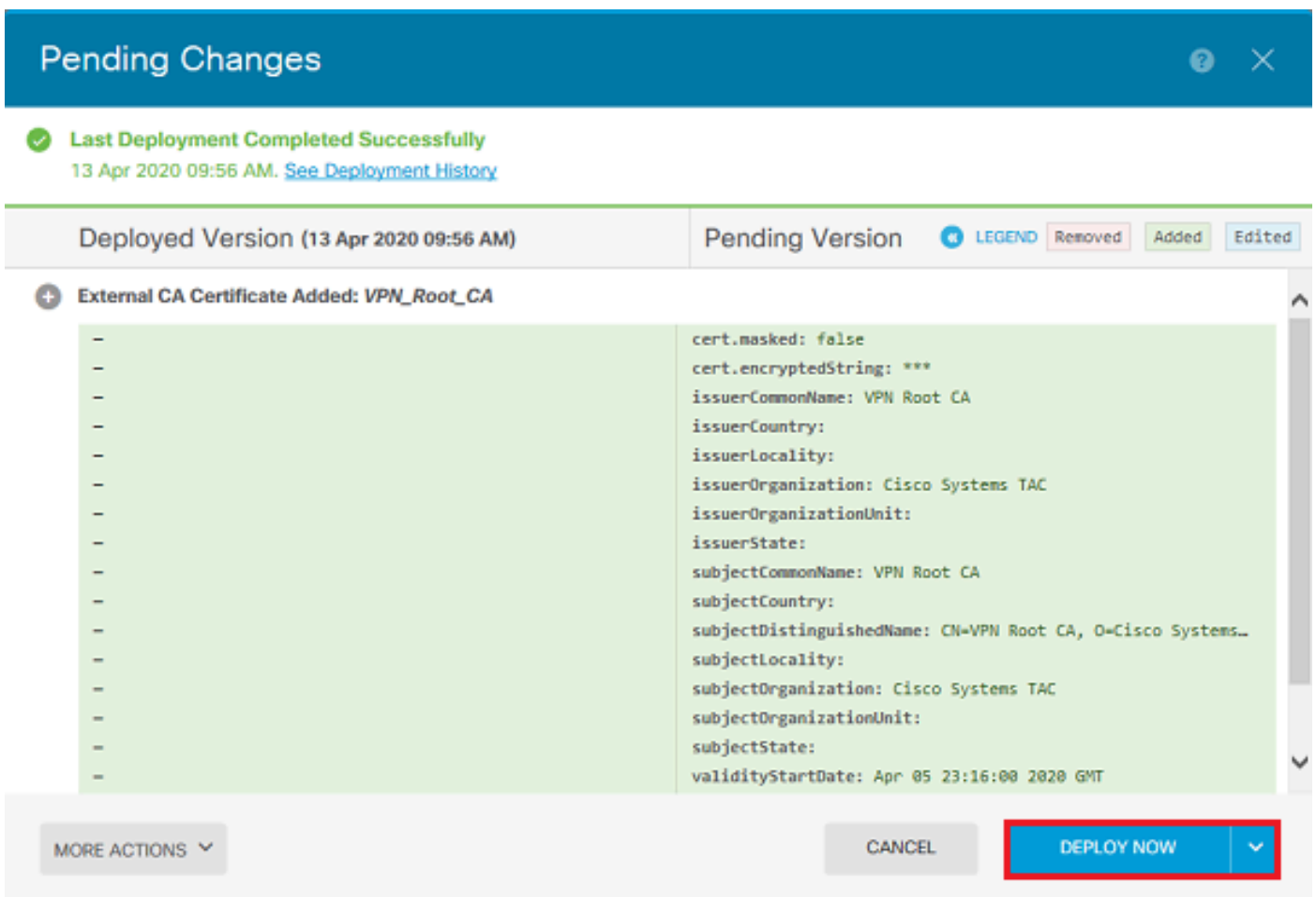
2. 指定信任点的名称。然后，上传或复制并粘贴PEM格式的CA证书。完成后单击OK（如图所示）。



3. 单击屏幕右上方的待定更改按钮（如图所示）。



4. 单击Deploy Now按钮（如图所示）。



证书续订

在FDM管理的FTD上续订证书涉及替换以前的证书，可能还包括私钥。如果您没有用于创建原始证书的原始CSR和私钥，则需要创建新的CSR和私钥。

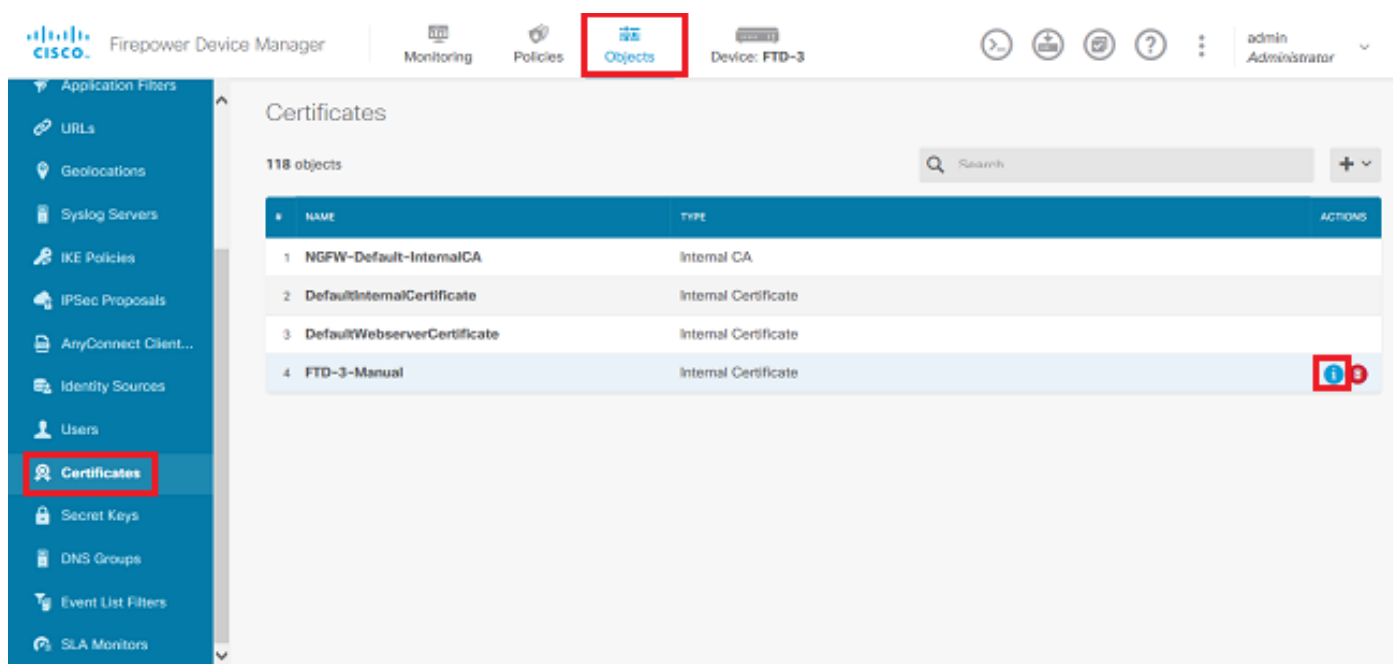
1. 如果您具有原始CSR和私钥，则可以忽略此步骤。否则，需要创建新的私钥和CSR。使用 OpenSSL或类似应用程序生成私钥和CSR。本示例显示一个名为private.key的2048位RSA密钥和一个在OpenSSL中创建的名为ftd3.csr的CSR。

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
.....+++
.....+++
writing 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 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) []:ftd3.example.com
Email Address []:.

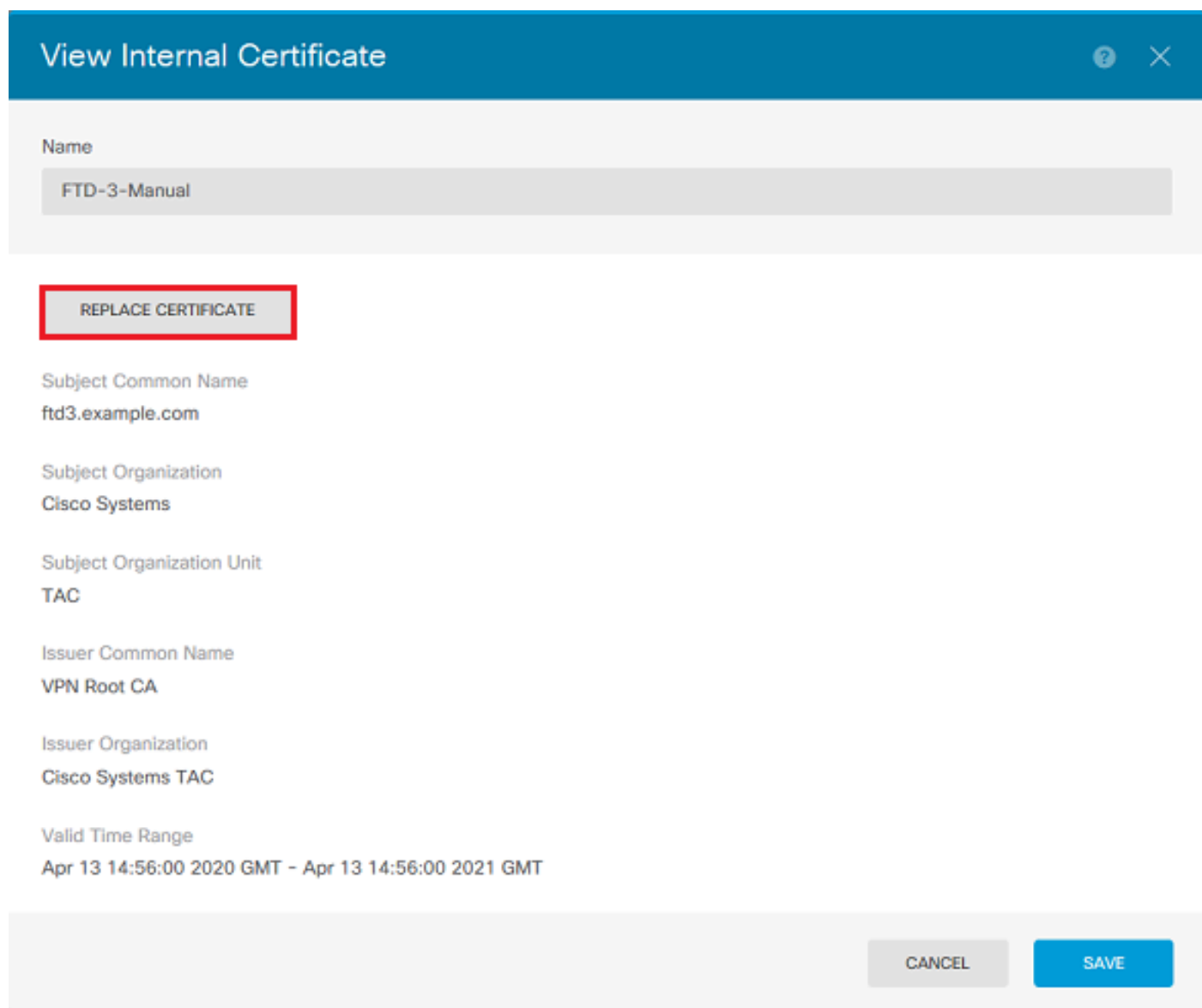
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

2. 将生成的CSR或原始CSR发送到证书颁发机构。签署CSR后，提供续订的身份证书。

3. 导航到对象>证书。将鼠标悬停在要续订的证书上，然后单击View按钮（如图所示）。



4. 在弹出窗口中，单击Replace Certificate，如图所示。



5. 上传，或者复制并粘贴PEM格式的身份证书和私钥。完成后单击OK（如图所示）。

Edit Internal Certificate ? X

Name
FTD-3-Manual

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file: REPLACE CERTIFICATE ftd3-renewed.crt

```
-----BEGIN CERTIFICATE-----
MIIErTCCApWgAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEUMC8w
ChMRQ2IzY28gU3lzdGVtcyBUQUVxMjEUMC8wDQYJKoZIhvcNAQELBQAw
-----
```

CERTIFICATE KEY

Paste key, or choose file: REPLACE KEY private.key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAAnGpzMjuf+HtRG5ZYf80V6V1sSyF7XhRxiRi80wUih5wBz6qN
ntQkd0JPog+CFqEXswTpel7ibPMtaTEVUEzcBpGbmyNz+A6jgNqAkTvaFMZV/RrW
-----
```

CANCEL OK

6. 单击屏幕右上方的待定更改按钮（如图所示）。

The screenshot shows the Cisco Firepower Device Manager interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: FTD-3'. The 'Objects' tab is active. On the right side of the top bar, there is a 'Deploy Now' button (a gear icon with a plus sign) highlighted with a red box. Below the navigation bar, the 'Certificates' page is displayed, showing a list of 118 objects. The list includes:

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Manual	Internal Certificate	

7. 单击Deploy Now按钮（如图所示）。

CSqGSIB3DQEBcWUAA4ICAQCjJrMjruGH5fpcFND8qfuVU0hkszcWq201oMqMrvXn
gENKcXxT27z6AHnQXeX3vhDcY3zs+FzFSOP5tRRPmy/413HAN+QEP2L9MQVD9PH
f50rQ/Ke5c16hMOJ08daR7wNzvFkcbicKCLRH0EvEoI0SPKsLyGSSxGmh6QXfZcM
GX3jG9Krglupg2UEqOug9HPTpgsbuNcHw8xXgFp6IA10LrytwrLeMIh5V+Vh5p11
yTl9wo5VADoYKgn408D21TeJIj6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwFMXM4T1
Rk3E0dSTENqzq2ZwnqJ4HCoqar7AS1Q5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBU1badlnEfi5J18G+/vZ16ykcmXe9hokKYxY8cg/U7170n/FbAmdYwRYgMAE4
RWFbP0voNzn97cG+qzogo7j/0kTFYu309DzdU3uy+R8JJkBrerkrZR7w70fP610
IAS86N5Zb18U14Gfc9m0eXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2Px0yam/bR0n0FoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJF0iV0GV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfPmWtiT47I
ng==

-----END CERTIFICATE-----

Certificate bag

Bag Attributes: <No Attributes>

subject=/O=Cisco Systems TAC/CN=VPN Root CA

issuer=/O=Cisco Systems TAC/CN=VPN Root CA

-----BEGIN CERTIFICATE-----

MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBGGA1UE
ChMRQ21zY28gU31zdGVtcyBUQUUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQwNTIzMTYwMFoXDTMwMDQwNTIzMTYwMFowMjEaMBGGA1UEChMRQ21zY28gU31z
dGVtcyBUQUUMxFDASBgNVBAMTC1ZQTiBSb290IENBMTIiIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCGKCAgEAXhTBKiB1xzLg2Jr48h/2u84RcWah0TmPYCNGYZg0PvSf
J0pKvAu5tz4z625Yx1nBtjSsEgzF+qETpSp1EhjW2NxIc1xuNirfrnSJQfIw51yT
PaFv7u+VhgyYbYsSxGAB/m6RWwpiNbg8SDoUACU7R/bvp1Rb8W6tXk/rsT1jc7L2
c/G5MeDLNmc/i/M1zuMjhj0tCphsJPhvNII71cNj6K0pvg2yB/Md7PX0ZnLaz9pf
Ggpjph0zzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXm1HQcgp
g5BgZMGqro015rcq0PjtK9Tqg7q013Vf0kM1sofMp+Bu1CiFDpawF/j8uSPuswEs
rzvJ+8Gb0Y1WEHtohgNGjP00q8wnKQu0C47Ft1UMpdSwUsMMze0X43dyp/WoZtLW
4v/Pn/NibE3aoP0aMhIo4CdwSBHZ0gVag4INqVsuFX1uPKD25Whr109LQ93P/sN3
FhoAh98HK0cuQ64Ua3AaShdzornD+G2J2pd1Nf1Dah1z1skIMt1URSwDLjsHLKft
JqS0oLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/1yNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cx11jIN0LdB+/jQqkfzmx9ziB1PXnIshNRbf1LLrNfdD09agqQsvsC
AwEAAaNdMfswDAYDVR0TBAAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDKc4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDKc4wCwYDVR0PBAQD
AgEGMAOGCSqGSIB3DQEBcWUAA4ICAQC6B+Y3obatEZqv0RQz1MS6o0umCgNWGi8d
kcRDxkY2F+zw3pBFa54Sin10FRPjvZvLNJV50dXmvH51uh6KJDMVrLMWniSgI7Tn
0ipqKraokS20o0STwQ7Q9Wk1xCrxwMfTuDJFMe80qabFAU55705PDXPtFEutn0xz
Ou8VMLBRY+gDc+0WARsjFj+0gU0c2Wj3gQ81G1yoPYgufWRnztn5rQxwzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AysGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p702FZ1y51xuzuA/wPnR89HiIkSF130MTpn0I13d6d07s3bwyNja8JikYTCf11e5
2CSsz4Cn/B1wfWyAcLN3HxUjG4Ev2818fWwPkYmuxujpKDFfzF0skpKAK53tNKPF
pn4+w5FyLo18o0AydtpoKjYkDqbgV/SRPbt92mdTIF7E6J+o8J60V3YL+IyrZ+u0
MYqPd450i4cgHdMFICandN3PYSrCrGYHawfVxp+R+G4dTJWdMvthh3ftS0mkiKJ8
m1NH7WYST1kYcTbcokZi0IcZa+VvV5UOLIt/hD0VG7xqZ01pMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpTIsmDv9rQzxBjuCyKn+23FkkUhfJt0D989UUyp08H9vDoJr
yzm9J0pMrg==

-----END CERTIFICATE-----

PKCS7 Data

Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048

Bag Attributes

localKeyID: 28 20 C1 B4 08 1E 65 2E 4D 1D F9 F3 25 07 62 F7 D9 96 A7 F4

friendlyName: ftd3.example.com

Key Attributes: <No Attributes>

Enter PEM pass phrase: [private-key-passcode]

Verifying - Enter PEM pass phrase: [private-key-passcode]

-----BEGIN ENCRYPTED PRIVATE KEY-----

MIIFDjBABgkqhkiG9w0BBQowMzAbBgkqhkiG9w0BBQwwDgQIScA8T0ogup4CAggA
MBQGcCqGSIB3DQMHBAGkQoTuZzoXsASCBMg0TEb24ENJ14/qh3GpsE2C20CnJeid
ptDDIFdy0V4A+su30JWz1nHrCuIhjR8+/p/N0W1A73x47R4T6+u4w4/ctHkveBQj
gZJZzFWTed9HqidhcKxx0oM/w6/uDv/opc6/r1IZiaKp6F09h0ibq1GI9kjkWQC
EQR8cM1U2yi0vagL8p0YdeujCrzBtorRp9BMJe1CP1Mw9t0EbAC4mmuedzs+86r1

```
xadK7qHBuWUJc03SLXLCmX5yLSGteWcoaPZnIK09UhLxpUSJTkwLHr2VtE1ACMRc
R1PBXMLb70nMtPTqct158+Q/axtQCWUs8caHs3LvVf0nRG+War49/F8Ii8mqnNnb
M6ZTWt0Z1sn0f4ohVePrW/kkd1QavJbPa+0dzjZvs88C1EXAJ/XIEgfSWifJAXqP
3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jj1KgfoxubtnuFq
un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZH0BuF1s+wZEmzYqw+cuc+I8XEFVOM18
P3ah28Nno0jXmk4MpFfJ1YmCmMq66xj5gZtcVZxOGC0sw0CKU0JiFFQTEmmVf9/C
65a96np7YCI8s6UuWi5Zp/NrbN31HkP0wt7+1DFGFit1pTTGv0FchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG115NsS1wKbTGiiwCYw0N8c09TXQb04rMomFDAv8
aef1aBsJMqEUkz0ZK0U2ZgTxM1ine8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubp0
qtmFX/DtSu9J2yevfv+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc40
w94fQH/DJ/1KsmSVwBLQLEKR1/nIDz36kmA27+1nVtX42PbEaIaFgucU4xHKx3zN
mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaQ8
fN17vEB+aret+PmqCiQY1Hqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUR0TuBHQhRK
3XpHfGxpe/00GdW3LeiFNlvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP
VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzd0cJ3aGCeA184XuPRfQhHe/Aj7q616uqB
W3Kt+kMj9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/
QCyhIRk3mx+8a1YLqk+h0MjWwBDEHX2mvbdKicK/jhwRdR/WmFOALq51phgtZ1z
Zed15UbPqWahJsjo09N5pp7Uq5iV0/xq4M1+/xQIYo2GIrQyat4AdB2B6K8K3xQd
Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTFzH5zgneUwLwnuBAbGT3oMSQ/
OKXnhcmUGu8XvLEfU/PITvGzKr06o12/hHJtzXQ8eNPDJbvcd/okRRKZpmjH+ijp
FPD/WgQ/vm09HdCwW3f1hqceqfHff8C1CJYFLxsgZp4M3G+WyQTKy4J8+6uTn/mj
yyZ5JCZd1t42haSNqu/ynioCjh5XY4m8WMZs0JBNPjKZiUX/vqVcc+/nod17VRZy
ELk=
-----END ENCRYPTED PRIVATE KEY-----
```

pkcs12file.pfx是需要解包的PKCS12文件。

在本示例中，将创建三个单独的文件：

一个用于身份证书。您可以断定，这是subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com的身份证书。

```
subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIErTCCApGwAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ21zY28gU31zdGVtcyBUQUUMxZDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTEw
MDQxMzE2NDQwMFoXDTEwMDQxMzE2NDQwMFowQTEwMBQGA1UEChMNQ21zY28gU31z
dGVtczEMMAoGA1UECXMDFEFDMDRkZmVhY2V0Y2V0Y2V0Y2V0Y2V0Y2V0Y2V0Y2V0
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAnGpzMjuf+HtRG5ZYf80V6V1s
SyF7XhRxxjR180wUih5wBz6qNntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZ0IcpzVqL6h0ziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50
QpQDTgviD1bYpPiWkP50g1PZDnX8b740s0pVKVXTsuJqSqH1va9BB6hK1JCoZa
HrP9Y0x09+MpVMH33R9vR13S0EF6kpZ6VEdGI4s6/IRvaM1z1BcK10N/N2+mjwID
AQABo4G3MIGOMAKGA1UdEwQCAAwHQYDVR0OBBYEFMcvjL0XiSTzNADJ/ptNb/cd
zB8wMB8GA1UdIwQYMBaAFHekzDnhI40727mjLXuwCRVfgyguMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwGwYDVRORBBQwEoIQZnRk
My51teGFtcGx1LmNvbTAeBg1ghkgBhvCAQ0EERYPEGNhIGN1cnRpZm1jYXR1MAOG
CSqGSIb3DQEBCwUAA4ICAQCjJrMjruGH5fpcFND8qfVU0hkszcwq201oMqMrvXn
gENKcXxt27z6AHnQXeX3vhDcY3zs+FzFSop5tRRPmy/413HAN+QEP2L9MQVD9PH
f50rQ/Ke5c16hMOJ08daR7wNzvFkcbicKCLRHOEvEoI0SPKsLyGSSxGmh6QXfZcM
GX3jG9Krg1ugp2UEqOug9HPTpgsbuNcHw8xXgFp6IA10LrytwrLeMIh5V+Vh5p11
yT19wo5VADoYKgn408D21TeJiJ6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwFMXMT1
Rk3E0dSTENqzq2ZwnqJ4HCoqar7AS1Q5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBU1bad1nEfi5J18G+/vZ16yckmXe9hokKYxY8cg/U7170n/FbAmdYwRYgMAE4
RwFBp0voNzn97cG+qzogo7j/okTfyu309DzdU3uy+R8JJKBrerkrZR7w70fP610
```

IAs86N5Zb18U14Gfc9m0eXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxpHn4zmkjI2Px0yam/bR0n0FoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJFOiV0GV+UBRi g p j X E a U f J j 4 y M w a M Y e r Z c Z Q V J f Z 7 5 + 8 S S 5 r f G f p M w T i T 4 7 I
ng==
-----END CERTIFICATE-----

一个用于颁发CA证书。您可以断定，这是subject=/O=Cisco Systems TAC/CN=VPN Root CA的身份证书。此值与先前看到的身份证书中的颁发者相同：

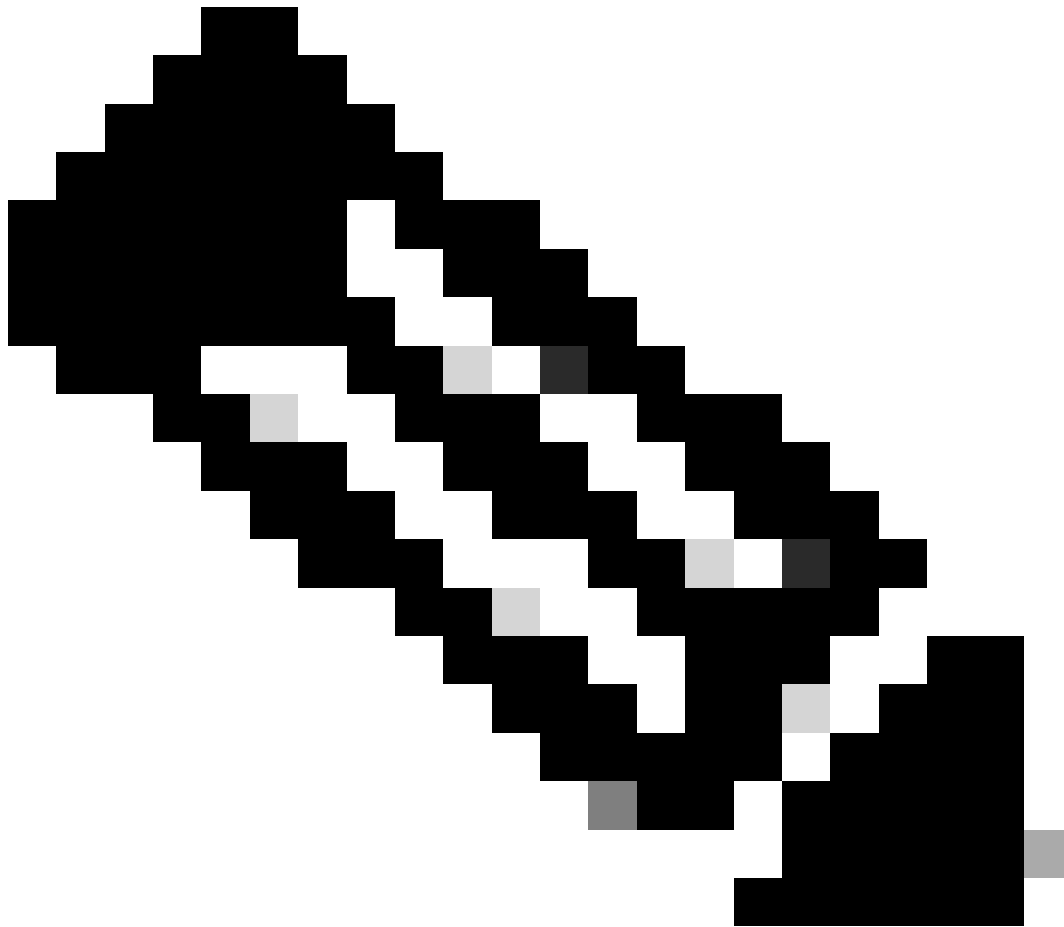
```
subject=/O=Cisco Systems TAC/CN=VPN Root CA
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBGGA1UE
ChMRQ2l2Y28gU3lzdGVtcyBUQUxhZDAsbG9uZS90IENBMjE2Y28gU3lzdGVt
cyBUQUxhZDAsbG9uZS90IENBMjE2Y28gU3lzdGVtcyBUQUxhZDAsbG9uZS90
AAOCAg8AMIICGKCAgEAXhTBKiB1xzLg2Jr48h/2u84RcWah0TmPVCNGYZg0PvSf
J0pKvAu5tz4z625Yx1nBtjSsEgzF+qETpSp1EhjW2NxIc1xuNirfrmSJQfIw51yT
PaFv7u+VhgyYbYsSxGAB/m6RWwpiNbg8SDoUACU7R/bvp1Rb8W6tXk/rsT1jc7L2
c/G5MeDLNmc/i/M1zuMjhj0tCphsJPhvNII71cNj6K0pvg2yB/Md7PX0ZnLaz9pf
Ggpjph0zzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXm1HQcgp
g5BgZMGqro015rcq0PjtK9Tqg7q013Vf0kM1sofMp+Bu1CiFDpawF/j8uSPuswEs
rzvJ+8Gb0Y1WEHtohgNGjP00q8wnKQu0C47Ft1UMpdSwUsMMzeOX43dyp/WoZtLW
4v/Pn/NibE3aoP0aMhIo4CdwSBHZ0gVag4INqVsuFX1uPKD25Whr109LQ93P/sN3
FhoAh98HK0cuQ64Ua3AaShdzornD+G2J2pd1Nf1Dahlz1skIMt1URSwDLjsHLKft
JqS0oLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/1yNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cx11jINOLdB+/jQqkfzmx9ziB1PXnIshNRbf1LLrNfdD09agqQsvsC
AwEAAaNDMfswDAYDVR0TBAAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDK4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDK4wCwYDVR0PBAQD
AgEGMAOGCSqGSIb3DQEBwUAA4ICAQC6B+Y3obatEZqv0RQz1MS6o0umCgNWGi8d
kcRDxkY2F+zw3pBfa54Sin10fRPJvZvLNJV50dXmvH51uh6KJDMVrLMWniSgI7Tn
0ipqKraokS20o0STwQ7Q9Wk1xCrwxMfTuDJFMe80qabFAU55705PDXPtFEutn0xz
Ou8VMLBry+gDc+0WARsjFj+0gU0c2Wj3gQ81G1yoPYgufWRnztn5rQxWzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AysGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p702FZ1y51xuzuA/wPnR89HiIkSF130MTpnOI13d6d07s3bwyNja8JikYTCf11e5
2CSsz4Cn/B1wfwyAcLN3HxUjG4Ev2818fWwPkYmuxujpKDFfzF0skpKAK53tNKPf
pn4+w5FyLo18o0AydtpokjYkdqbgV/SRPbt92mdTIF7E6J+o8J60V3YL+IyrZ+u0
MYqPd450i4cgHdMFICandN3PYSrCrGYHawfVxp+R+G4dTJWdMvthh3ftS0mkiKJ8
m1NH7WYST1kYcTbcokziOicZa+Vv5UOLIt/hD0VG7xqZ01pMQKkYUBzg5LbGINm
8ypfhQ1faI5fQRxpxTismDv9rQzxBjuCyKn+23FkkuHFjt0D989UUyp08H9vDoJr
yzm9J0pMrg==
-----END CERTIFICATE-----
```

一个用于私钥：

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBAGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIScA8T0ogup4CAggA
MBQGCGcGSiB3DQMHBAGkqoTuZzoXsASCBMg0TEb24ENJ14/qh3GpsE2C20CnJeid
ptDDIFdy0V4A+su30JWz1nHrCuIhjR8+/p/N0W1A73x47R4T6+u4w4/ctHkvEbQj
gZJZzFWTed9HqidhcKxx0oM/w6/udv/opc6/r1ZiaKp6F09h0ibq1GI9kjkWQC
EQR8cM1U2yi0vagL8pOYdeujCrzBtorRp9BMJe1CP1Mw9t0EbAC4mmuedzs+86r1
xadK7qhBUUJc03SLXLcmX5yLSGteWcoaPZnIK09UhlxpUSJTKwLHr2VtE1ACMRc
R1PBXMLb70nMtPTqct158+Q/axtQCWUs8caHs3LvVf0nRG+War49/F8Ii8mqnNnb
```

M6ZTwTOZ1sn0f4ohVePrW/kkd1QavJbPa+0dzjZvs88C1EXAJ/XIEgfSwifJAXqP
3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jj1KgfoxubtnuFq
un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZH0BuF1s+wZEmzYqw+cuc+I8XEFVOM18
P3ah28Nno0jXMk4MpfFJ1YMcMmq66xj5gZtcVZxOGC0sw0CKU0JiFFQTEmmVf9/C
65a96np7YCI8s6UnUWi5Zp/NrbN31HkP0wt7+1DFGFit1pTTGv0FchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG115NSs1wkBTGiiwCYw0N8c09TXQb04rMomFDAv8
aef1aBsJMqEUkz0ZK0U2ZgTxM1ine8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubp0
qtmFX/DtSu9J2yevfV+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc40
w94fQH/DJ/1KsmSVwBLQLEKR1/nIDz36kmA27+1nVtX42PbEaIaFgucU4xHKx3zN
mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaq8
fN17vEB+aret+PmqCiQY1Hqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUR0TuBHQhRK
3XpHFGXpe/00GdW3LeifNLvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP
VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzd0cJ3aGCeA184XuPRfQhHe/Aj7q616uqB
W3Kt+kMJ9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/
QCyhIRK3mx+8a1YLqK+h0MjWBDEHX2mvbdKicK/jhwRdR/WmFOALq51phgtZ1z
Zed15UbPqWahJsjo09N5pp7Uq5iV0/xq4M1+/xQIYo2GIrQyat4AdB2B6K8K3xQd
Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTFzH5zgneUwLwnuBAbGT3oMSQ/
OKXnhcmUGu8XvLEfU/PITvGzKr06o12/hHJtzXQ8eNPDJbvcd/okRRKZpmjH+ijp
FPD/WgQ/vm09HdCwW3f1hqceqfHff8C1CJYFLxsgZp4M3G+WyQTKy4J8+6uTn/mj
yyZ5JCZd1t42haSNqu/ynioCjh5XY4m8WMZs0JBNPjKZiUX/vqVcc+/nod17VRZy
ELk=

-----END ENCRYPTED PRIVATE KEY-----



注意：私钥已加密，FDM不接受加密的私钥。

要将私钥解密，请将加密的私钥复制到文件中，然后运行此openssl 命令：

```
openssl rsa -in encrypted.key -out unencrypted.key
Enter pass phrase for encrypted.key: [private-key passphrase]
writing RSA key
```

- encrypted.key是保存加密私钥的文件的名称。
- unencrypted.key是包含未加密密钥的文件的名称。

未加密的私钥可以显示-----BEGIN RSA PRIVATE KEY-----而不是-----BEGIN ENCRYPTED PRIVATE KEY-----，如以下示例所示：

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAAnGpzMjuF+HtRG5ZYf80V6V1sSyF7XhRxjRl80wUih5wBz6qN
ntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGbmYnz+A6jgNqAkTvaFMZV/RrW
qCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqNBqotoz3/8CrZOIcpzVqL6hOz
iJFBgdiWJEYBoFuE1jmmSJi3qd39ib9+t6LhkS50QpQDTgvIiD1bYpPiWKpS0g1P
ZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZaHrP9Y0x09+MpVMH33R9vRl3S
OEF6kpZ6VEdGI4s6/IRvaM1z1BcK10N/N2+mjwIDAQABAoIBAEQzCd1KMBrosdmk
eRvoMPiAemBbze2cXlJWXZ2orICSXhvM0okBGJFDQXN47ZCuVqYAq0ecjU9RzGgE
NbXYfUsD6+P91k+/Gj1RiCNLBHBwdgewzw1quTxP54zSpAVlIXyQ+Fo1TzjH1yfw
7iHhuSujYsAYLWPY4Yg3NpU2IdzeQoK5ViuSTTNx8LHYBKw1Qf7HVaQTfmsW0Ayg
/vjZqjRkukqKM41srgk0/HjPnEBDuUWVTehzMCk1etijENC7ttISzYIEMNPthe60
NpidXAHoJ11JM6HB9ZraBH5fu7MJZJZ00n6YVKQuCdW0WfnKiNQCDsXq7X5Ewsaj3
cgyjw1kCgYEAy33k1wXp7WEqg1zEwq0Vq7AtoL6i4V9QCenMThQAHwNAAUGGOSIF
JhpKyApm/BUogSIOMzIPse+NgAA66TRn4qfkbpvTI98CeCuxiUPcbRmqZnYxC0fp
Pzosv50nBl1toIoprI02S5a261w6JGNAFD95tCjCYrB8Cw/HbZOLPUCgYEAxMbZ
KVyosBxaAIFQinHaff3fVSTsEOZFPcBbLybgLcP8LsLdahBsJ6HK/hAffKX0dvm
35CAM7ZL/WCI1Jb+dx4YcD9q81bVMu4HTvS12deTZoZrBG2iFX60Ssn2rLKAH+cH
uLSHCNAj9cj9syldZErGLZtBQpJtpLRd6iy0vMCGYBP/zoLYJHOBBLWeY3QioLO
cABABTG7L+EjRIpQ14QErR5oX/4IT9t+Uy+63HwH9b1qqpye6e359jUzUJbk4KT
1DU1VoT2wSETYmvK7qa1LUXT6fr12FtVw+T7m2w5azwxshDuBQmRRbq7ZBJnY61i
KwIJVUy1U/tSE9LsN1McUQKBgQC1c4ykeoRbj3sdcZ2GyrQru4pMzP6wNu3Xy5EH
HI6ja0i74ImCJDcY5/o/vjx7qb39qBJa5+Tj1iP0p5x1I5BSF7v0pV4G5Xvd1sY0
XSYWRGxriBnzXzspV3/M4oPGMVAJgve7Fg90GY4i2xx1yBH+geCf+CqnDt53Zhs7
YVz6gQKBgQDG42tZZ1kNAn0x/k11U1ZrEeF8iqdsyVcRf4fAvqsPbY3+kdae+80r
+cQpVoeWzOQLUkA6eMsiTLmcWYb62qMgdpluyKo0ciPG9+2AGNTvQp/ig34pF2F/
90GuVY1A1p7mkP8Vb1Mo1ugV0zUqAIjHKiGUzBWVsx0ZsGa+SY47uw==
-----END RSA PRIVATE KEY-----
```

一旦私钥未加密，可以上传身份和私钥文件，或者复制并粘贴到FDM中，使用前面提到的手动注册部分中的步骤3。可以使用前面提到的受信任CA证书安装步骤来安装颁发CA。

验证

使用本部分可确认配置能否正常运行。

查看FDM中安装的证书

1. 导航到对象>证书。将鼠标悬停在要验证的证书上，并单击view按钮（如图所示）。

Firepower Device Manager

Monitoring Policies **Objects** Device: FTD-3

admin Administrator

Application Filters

- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- AnyConnect Client...
- Identity Sources
- Users
- Certificates**
- Secret Keys
- DNS Groups
- Event List Filters
- SLA Monitors

Certificates

118 objects

Search

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Manual	Internal Certificate	

2. 弹出窗口提供有关证书的其他详细信息，如图所示。

View Internal Certificate

Name

FTD-3-Manual

REPLACE CERTIFICATE

Subject Common Name
ftd3.example.com

Subject Organization
Cisco Systems

Subject Organization Unit
TAC

Issuer Common Name
VPN Root CA

Issuer Organization
Cisco Systems TAC

Valid Time Range
Apr 13 16:44:00 2020 GMT - Apr 13 16:44:00 2021 GMT

CANCEL SAVE

在CLI中查看已安装的证书

可以使用FDM中的CLI控制台或SSH进入FTD，然后运行命令show crypto ca certificates以验证证书是否已应用到设备，如图所示。

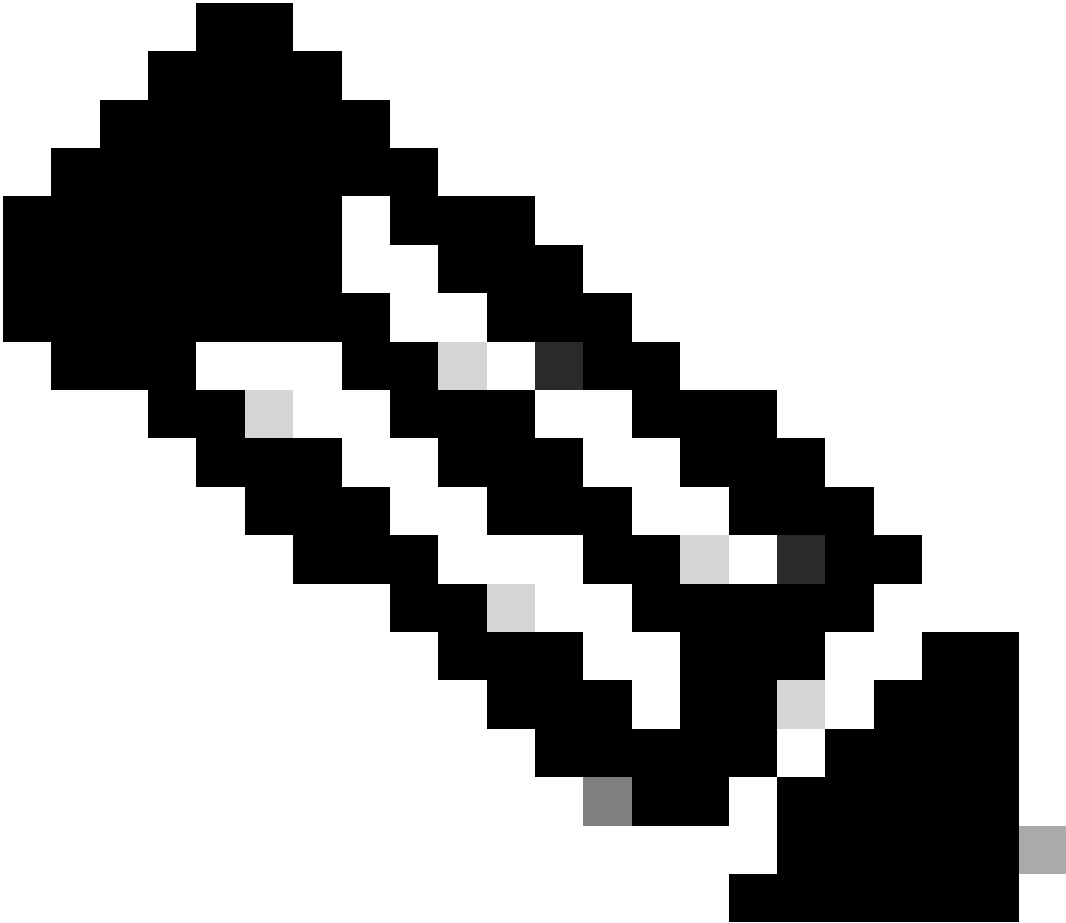


示例输出：

```
> show crypto ca certificates
```

Certificate

```
Status: Available
Certificate Serial Number: 6b93e68471084505
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=ftd3.example.com
  ou=TAC
  o=Cisco Systems
Validity Date:
  start date: 16:44:00 UTC Apr 13 2020
  end date: 16:44:00 UTC Apr 13 2021
Storage: config
Associated Trustpoints: FTD-3-Manual
```



注意：身份证书仅在与服务（例如AnyConnect）一起使用时在CLI中显示。受信任的CA证书在部署后即会出现。

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

如果安装SSL证书失败，可在通过SSH连接FTD后从诊断CLI运行调试：`debug crypto ca 14`

在FTD的较早版本中，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ASA导出的PKCS12

当您尝试从OpenSSL中导出的ASA PKCS12中提取身份证书和私钥时，您会收到类似以下内容的错误：

```
openssl pkcs12 -info -in asaexportedpkcs12.p12
6870300:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1220:
6870300:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:386:Type=PK
```

要解决此问题，必须首先将pkcs12文件转换为DER格式：

```
openssl enc -base64 -d -in asaexportedpkcs12.p12 -out converted.pfx
```

完成后，可按照本文档前面部分的“从PKCS12文件提取身份证书和私钥”部分中的步骤导入身份证书和私钥。

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）。