

# 安装Firepower可扩展操作系统的机箱管理器的一个信任证书

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[生成证书签名请求](#)

[导入认证机关证书链](#)

[导入服务器的签名的身份证书](#)

[配置机箱管理器使用新证书](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文描述如何生成证书签名请求(CSR)和安装发生的身份证书为了用在Firepower可扩展操作系统的(FXO)机箱管理器上在Firepower 4100和9300系列设备。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 配置从line命令的FXO
- CSR使用情况
- 专用密钥基础设施(PKI)概念

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower 4100和9300系列硬件
- FXO版本1.1和2.0

## 背景信息

在初始配置以后，一自己签署的SSL证书生成为了用在机箱管理器Web应用程序上。因为该证书自

已签署的，不会由客户端浏览器自动信任。第一次那新的客户端浏览器第一次访问机箱管理器Web接口，浏览器将投掷警告的SSL类似于您的连接不私有，并且请要求用户在访问机箱管理器前接受证书。此进程将允许能允许客户端浏览器委托连接的委托签字的证书认证机关将安装，并且启动Web接口没有警告。

本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

**注意：**现在没有办法生成在机箱管理器GUI的CSR。必须通过line命令执行它。

### 生成证书签名请求

执行这些步骤获取包含设备(IP地址或完全合格的域名(FQDN)允许客户端浏览器适当地识别服务器)的证书：

- 创建钥匙圈并且选择模数大小专用密钥

**注意：**钥匙圈名称可以是所有输入。在示例中使用firepower\_cert

```
fp4120# scope security
fp4120 /security # create keyring firepower_cert
fp4120 /security/keyring* # set modulus <size>
fp4120 /security/keyring* # commit-buffer
```

- 配置CSR字段。CSR可以生成与基本选项类似a subject-name。这提示输入证书请求密码。

```
fp4120 /security/keyring # create certreq subject-name fp4120.test.local
Certificate request password:
Confirm certificate request password:
```

- CSR可能也生成与允许信息类似在证书和组织将嵌入的现场的高级选项。

```
fp4120 /security/keyring # create certreq
fp4120 /security/keyring/certreq* # set country US
fp4120 /security/keyring/certreq* # set state California
fp4120 /security/keyring/certreq* # set locality "San Jose"
fp4120 /security/keyring/certreq* # set org-name "Cisco Systems"
fp4120 /security/keyring/certreq* # set org-unit-name TAC
fp4120 /security/keyring/certreq* # set subject-name fp4120.test.local
fp4120 /security/keyring/certreq* # commit-buffer
```

- 导出CSR提供给您认证机关。复制输出开始与(和包括)“-----开始证书请求-----”结束与(和包括)“-----END证书请求-----”。

```
fp4120 /security/keyring/certreq # show certreq
Certificate request subject name: fp4120.test.local
Certificate request ip address: 0.0.0.0
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): California
Locality name (eg, city): San Jose
```

Organisation name (eg, company): Cisco Systems

Organisational Unit Name (eg, section): TAC

DNS name (subject alternative name):

Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAdMCAQAwZDZELMAkGA1UEBhMCVVMxExARBgNVBAGMCkNhbgG1mb3JuaWEx
ETAPBgNVBACMFNhb3N1MRYwFAyDVQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLDANUQUxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmXvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXm63FsrPcPmA7EwgqDSL0ShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHAKV9bttYg3kf/UEUUGk/EyrVq3B+u2DsooPVq76mTm8BwYmQHbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABOC8wLQYJ
KoZlIhvcNAQkOMSAwHjAcBgNVHREFTATghFmcDQxMjAudGVzdC5sb2NhbdANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVdL+Atu5xFE3LA310ck6Gj1Nv6W/6r
jBNLxusYi1rZZcW+CgnvNs4ArqYgYNVBySOavJO/VvQ1KfyxxJ10Ikyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNTHWTvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfg1dxWf1xAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJmVaqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ21DXyDjEXp7rCx9
+6bvD11n70JCegHdCWtP75SaNyaBEPk00365rTckbw==
-----END CERTIFICATE REQUEST-----
```

## 导入认证机关证书链

**注意：**所有证书必须在将导入的Base64格式到FXO。如果从或一系列接收的证书认证机关在一个不同的格式，您必须用一个SSL工具首先转换它例如Openssl。

- 创建一新的信任点拿着证书链

**注意：**信任点名称名称可以是所有输入。在示例firepower\_chain使用。

```
fp4120 /security/keyring/certreq # exit
fp4120 /security/keyring # exit
fp4120 /security # create trustpoint firepower_chain
fp4120 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOP3uKNgJHZDAKBggqhkiG9w0BAQDAjBTMRUw
>EwYKZCZImiZPyLQGBGRYFbG9jYWwzGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbWZhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMjUwNzI4MTc1NjU2
>WhcnMjAwNzI4MTc1NjU2WjBTMRUwEwYKZCZImiZPyLQGBGRYFbG9jYWwzGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbWZhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkiG9w0BAQIBBggqhkiG9w0BAQMBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKkneJUkmlxmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPPrFwEEBcbxGSgQW7pOVIkWEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAARQIhAP++QJTUmnIB/AxPDDN63Lqy
>18odMDofTtkG4p3Tb/2yMAiAtMYh1sv1gCxsQVOW0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
fp4120 /security/trustpoint* # commit-buffer
```

**注意：**对于认证机关该必须结合用途半成品证书、根和中间证书。在文本文件中，请在顶部粘贴根证明，跟随由一系列的每中间证书(包括所有开始证书和END证书标志)。然后请在ENDOFBUF描述前粘贴该整个文件。

## 导入服务器的签字的身份证书

- 连结在上一步创建的信任点与为CSR创建的钥匙圈。

```
fp4120 /security/trustpoint # exit
fp4120 /security # scope keyring firepower_cert
fp4120 /security/keyring # set trustpoint firepower_chain
```

- 粘贴提供的身份证书的內容认证机关

```
fp4120 /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkJOPQQAjBT
>MRUwEwYKZCImiZPyLGOBGRYFbG9jYWwxGDAWBoJkiaJk/IsZAEZFghuYWF1c3Rp
>bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
>OTU0WhcNMTYwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2F5
>aWZvcmlzPjYTERMA8GA1UEBxMIU2FuIEpvc2UxKjFjAUBGNVBAoTDUNpc2NvIFN5c3Rl
>bXNxDDAKBgNVBAsTA1RlbnQzEaMBGGA1UEAxMRZnA0MTIwLnRlc3QubG9jYVwwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLpv9rHtYY296D9c/7N3Tee3gzczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHvkDopX1u21iDeR/9QRRSCT8TKtWrch67YOyig9WrvqZOwbHBg
>yodskS/g+a5GNYTzzIS9Xafs1MSKP06/Ftq2MONVIkdKFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhhlVq1PGnodNR7Mfywgjm5q9Tp3W0H2ufLGAA2H109XR2FgMB
>AAGjggJYMIICVDACBgNVHREFTATghFmcDQxMjAudGVzdC5sb2NhbdAdBgNVHQ4E
>FgQU/1WpstiEYExs8D1ZwcuHwZPtU5QwHwYDVR0jBBgwFoAUyInbDHPFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBY6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0E049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMETtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmawNhdGVsZXZvY2F0aW9uTG1z
>dd9iYXNlP29iamVjdENSYXNzPWNSTERpc3RyaWJldG1vb1BvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVE1OLVBDLUNBLENOPUFJQSxDTj1QdWJsawW1MjBLZXk1MjBTZXJ2aWNlcyxD
>Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydGlmawNhdGU/YmFzZT9vYmplY3RDbGFzc3Z1ZjZjZj0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAQUHhIAVwBLAGIAUwBIAHIAHgBIAHIwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQMMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvxyjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
fp4120 /security/keyring* # commit-buffer
```

## 配置机箱管理器使用新证书

证书当前安装，但是网站服务没有配置使用它。

```
fp4120 /security/keyring # exit
fp4120 /security # exit
fp4120# scope system
fp4120 /system # scope services
fp4120 /system/services # set https keyring firepower_cert
Warning: When committed, this closes all the web sessions.
fp4120 /system/services* # commit-buffer
```

## 验证

使用本部分可确认配置能否正常运行。

- 显示https —输出显示用HTTPS服务器关联的钥匙圈。它应该反射在上面步骤创建的名称。它

, 如果仍然显示默认然后它未更新使用新证书。

```
fp4120 /system/services # show https
```

```
Name: https
```

```
Admin State: Enabled
```

```
Port: 443
```

```
Operational port: 443
```

```
Key Ring: firepower_cert
```

```
Cipher suite mode: Medium Strength
```

```
Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIU
```

```
M:+EXP:+eNULL
```

- **显示钥匙圈<keyring\_name>详细信息**—输出显示导入证书的内容并且显示，如果有效。

```
fp4120 /security # scope security
```

```
fp4120 /security # show keyring firepower_cert detail
```

```
Keyring firepower_cert:
```

```
RSA key modulus: Mod2048
```

```
Trustpoint CA: firepower_chain
```

```
Certificate status: Valid
```

```
Certificate:
```

```
Data:
```

```
Version: 3 (0x2)
```

```
Serial Number:
```

```
45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
```

```
Signature Algorithm: ecdsa-with-SHA256
```

```
Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
```

```
Validity
```

```
Not Before: Apr 28 13:09:54 2016 GMT
```

```
Not After : Apr 28 13:09:54 2018 GMT
```

```
Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC, CN=fp4120.test.local
```

```
Subject Public Key Info:
```

```
Public Key Algorithm: rsaEncryption
```

```
Public-Key: (2048 bit)
```

```
Modulus:
```

```
00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:  
0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:  
a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:  
50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:  
fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:  
d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:  
3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:  
a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:  
9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:  
20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:  
ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:  
87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:  
07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:  
47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:  
cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:  
5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:  
d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:  
1d:85
```

```
Exponent: 65537 (0x10001)
```

```
X509v3 extensions:
```

```
X509v3 Subject Alternative Name:
```

```
DNS:fp4120.test.local
```

```
X509v3 Subject Key Identifier:
```

```
FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
```

```
X509v3 Authority Key Identifier:
```

```
keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
```

```
X509v3 CRL Distribution Points:
```

```
Full Name:
```

```
URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-
pc,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,DC=local?certifica
teRevocationList?base?objectClass=cRLDistributionPoint
Authority Information Access:
CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,DC=local?cACertifi
cate?base?objectClass=certificationAuthority
1.3.6.1.4.1.311.20.2:
...W.e.b.S.e.r.v.e.r
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
Signature Algorithm: ecdsa-with-SHA256
30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIIe8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkJOPQQDAjBT
MRUwEwYKZCImiZPyLGQBGRYFbG9jYVwwGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMjYwNDI4MTMw
OTU0WhcNMjYwNDI4MTMwOTU0WjB3MQswCQYDVQGEwJVUzETMBEGA1UECBMKQ2F5
aWZvcml5TERMA8GA1UEBxMIU2FueEpvc2UxXjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxMDE0bG9uYVAsTA1RBQZzEaMBGGA1UEAxMRZnA0MTIwLnRlc3QubG9jYVwwggEi
MA0GCsGCSqIB3DQEBQUAA4IBDwAwgEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGCco48mMHCRQwIADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gzczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNyTzIs9XAfs1MSKP06/Ftq2MONVIkdKFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAGMB
AAGjggYMIICVDAcBgNVHREEFtATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZwcuHZwPtU5QwHwYDVR0jBBgwFoAUyInbDHPFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmXpYyUyMettleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYVww/Y2VydGlmawNhdGVsZXZvY2F0aW9uTG1z
dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBGgrBgEF
BQcBAQSBvzCBvDCBuYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVTE0LVBBDLUNBLENOPUFJQSxDTj1QdWJsaW1mJmJBLZk1mJmBTZk1mJmJmJmJmJm
Tj1TZk1mJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJm
Tj1TZk1mJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJm
P2NBQ2VydGlmawNhdGU/YmFzZT9vYmply3RDvGFzc1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBbjcUAQQUHhIAVwBlAGIAUwBlAHIAAgBlAHIAwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvYxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjot0TvUdUd9b6K1Uw=
-----END CERTIFICATE-----
```

Zeroized: No

- 浏览给Firepower机箱管理器通过输入在Web浏览器的地址栏的https:// <FQDN\_or\_IP>/并且验证提交新的信任证书。

**警告：**浏览器也验证subject-name证书在地址栏的输入，因此，如果证书发出对完全限定域名，必须访问在浏览器的方式。如果它通过IP地址访问，一个不同的SSL错误被投掷(无效的公用名称)，即使使用信任证书。

## 故障排除

目前没有针对此配置的故障排除信息。

## 相关信息

- [访问FXO CLI](#)
- [技术支持和文档 - Cisco Systems](#)