

# Install a Trusted Certificate for FXOS Chassis Manager

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Generate a CSR](#)

[Import the Certificate Authority Certificate Chain](#)

[Import the Signed Identity Certificate for the Server](#)

[Configure Chassis Manager to Use the New Certificate](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes how to generate a Certificate Signing Request (CSR) and install the identity certificate that is the result for use with the Chassis Manager for Firepower eXtensible Operating System (FXOS) on the Firepower 4100 and 9300 series devices.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Configure FXOS from the Command Line
- Use CSR
- Private Key Infrastructure (PKI) Concepts

### Components Used

The information in this document is based on these software and hardware versions:

- Firepower 4100 and 9300 Series Hardware
- FXOS Versions 1.1 and 2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Background Information

After initial configuration, a self-signed SSL certificate is generated for use with the Chassis Manager web application. Since that certificate is self-signed, it will not be automatically trusted by client browsers. The first time that a new client browser accesses the Chassis Manager web interface for the first time, the browser throws an SSL warning similar to your connection, it is not private and requires the user to accept the certificate before you access the Chassis Manager. This process allows a certificate signed by a trusted certificate authority to be installed which can allow a client browser to trust the connection, and bring up the web interface with no warnings.

## Configure

**Note:** There is currently no way to generate a CSR in the Chassis Manager GUI. It must be done via command line.

### Generate a CSR

Perform these steps in order to obtain a certificate that contains the IP address or Fully Qualified Domain Name (FQDN) of the device (which allows a client browser to identify the server properly):

- Create a keyring and select the modulus size of private key.

**Note:** The keyring name can be any input. In these examples, **firepower\_cert** is used.

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

- Configure the CSR fields. The CSR can be generated with just basic options like a subject-name. This prompts for a certificate request password as well.

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

- The CSR can also be generated with more advanced options that allow information like locale and organization to be embedded in the certificate.

```
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
```

- Export the CSR to provide to your certificate authority. Copy the output that starts with (and

includes) -----BEGIN CERTIFICATE REQUEST----- ends with (and includes) -----END CERTIFICATE REQUEST-----.

```
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-----
MIIC6zCCAdMCAQAwZzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCKNhbgGlm3JuaWEEx
ETAPBgNVBACMCFNhb3NlMRYwFAyDVQKDA1DaXNjbyBTexNOZWlzMQwwCgYD
VQQLDANUQUMxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmXvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSL0ShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHAKV9bttYg3kf/UEUUGk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABOC8wLQYJ
KoZIHvCNAQkOMSAwHjAcBgNVHREEFtATghFmcDQxMjAudGVzdC5sb2NhbdANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVdCL+tATu5xFE3LA310ck6Gj1Nv6W/6r
jBNLxusYilrZZcW+CgnvNs4ArqYGYNVBySOavJO/VvQ1KfyxxJ1OIkyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNTHWTvcQy55+/hDPD2Bv8pQOC2Zng3I
kLFG1dxWf1xAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJmVaqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjyQ21DXyDjEXp7rCx9
+6bvD1ln70JCegHdCWtP75SaNyaBEPk00365rTckbw==
-----END CERTIFICATE REQUEST-----
```

## Import the Certificate Authority Certificate Chain

**Note:** All certificates must be in Base64 format to be imported into FXOS. If the certificate or chain received from the Certificate Authority is in a different format, you must first convert it with an SSL tool such as OpenSSL.

- Create a new trustpoint to hold the certificate chain.

**Note:** The trustpoint name can be any input. In the examples firepower\_chain is used.

```
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-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOP3uKNgJHZDAKBggqhkJOPQDAjBTMRUw
>EwYKCZImiZPyLQGByfBg9jYWwwGDAWBgOJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbWfhZDN0aW4tTtFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
```



```
>IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
fp4120 /security/keyring* # commit-buffer
```

## Configure Chassis Manager to Use the New Certificate

The certificate has now been installed, but the web service is not yet configured to use it.

```
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
```

## Verify

Use this section in order to confirm that your configuration works properly.

- **show https** - Output displays the keyring associated with the HTTPS server. It should reflect the name created in the steps mentioned before. If it still shows default then it has not been updated to use the new certificate.

```
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
```

- **show keyring <keyring\_name> detail** - Output displays the contents of the certificate that is imported and show if it is valid or not.

```
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-----

MIIe8DCBjAgAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkJOPQQDAjBT
MRUwEwYKCZImiZPyLQGByfBg9jYwWxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmfhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMjYwNDI0MTMw
OTU0WbcNMjYwNDI0MTMwOTU0WjB3MQswCQYDVQGEwJVUzETMBEGA1UECBMKQ2F5
aWZvcmluZTERMA8GA1UEBxMIU2FuIEpvc2UxZjAUBGNVBAoTDUNpc2NvIFN5c3Rl
bXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMjYwNDI0MTMwOTU0WjB3MQswCQYDVQGE
wJVUzETMBEGA1UECBMKQ2F5aWZvcmluZTERMA8GA1UEBxMIU2FuIEpvc2UxZjAUBGNV
BAoTDUNpc2NvIFN5c3RlbnR8xKfKo4vvnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gzczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopXlu21iDeR/9QRRSCT8TKtWrcH67Y0yig9WrvqZOwbHBg
yodskS/g+a5GNyTzzIS9XAfslMSKP06/Ftq2MONVIkdKFRG0Jqe/IG8a4s/9D82a

```
/cu jcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2H109XR2FagMB
AAGjggJYMIICVDACBgNVHREEFtATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8D1ZWcuHZwPtU5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBY6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMETtleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydG1maWNhdGVsZXZvY2F0aW9uTG1z
dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50IHMBGgrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVE1OLVBDLUNBLENOPUFJQSxDTj1QdWJsaWM1mJBLZXklmJBTZXXJ2aWN1cyxD
Tj1TZXJ2aWN1cyxDTj1Db25maWdlcmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydG1maWNhdGU/YmFzZT9vYmplY3RDbGFzc21jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBggjCUAgQUHhIAVwB1AGIAUwB1AHIAAgB1AHIAwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOtvUdUd9b6K1Uw=
-----END CERTIFICATE-----
```

Zeroized: No

- Enter **https://<FQDN\_or\_IP>/** in the address bar of a web browser and browse to the Firepower Chassis Manager and verify that the new trusted certificate is presented.

**Warning:** Browsers also verify the subject-name of a certificate against the input in the address bar, so if the certificate is issued to the fully qualified domain name, it must be accessed that way in the browser. If it is accessed via IP address, a different SSL error is thrown (Common Name Invalid) even if the trusted certificate is used.

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## Related Information

- [Accessing the FXOS CLI](#)
- [Technical Support & Documentation - Cisco Systems](#)