

Installez un certificat de confiance pour le gestionnaire de châssis FXOS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Générez un CSR](#)

[Importez la chaîne de certificat d'autorité de certification](#)

[Importez le certificat d'identité signé pour le serveur](#)

[Configurez le gestionnaire de châssis pour utiliser le nouveau certificat](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment générer une demande de signature de certificat (CSR) et installer le certificat d'identité qui est le résultat pour l'usage avec le gestionnaire de châssis pour le système d'exploitation extensible de FirePOWER (FXOS) sur les périphériques de gammes 4100 et 9300 de FirePOWER.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configurez FXOS de la ligne de commande
- CSR d'utilisation
- Concepts d'infrastructure de clé privée (PKI)

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Matériel de gammes 4100 et 9300 de FirePOWER
- Versions 1.1 et 2.0 FXOS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

Après configuration initiale, un certificat ssl auto-signé est généré pour l'usage avec l'application Web de gestionnaire de châssis. Puisque ce certificat auto-est signé, il ne sera pas automatiquement fait confiance par des navigateurs de client. La première fois que cela un nouveau navigateur de client accède à l'interface web de gestionnaire de châssis pour la première fois, le navigateur jette un avertissement SSL semblable à votre connexion, elle n'est pas privée et exige de l'utilisateur de recevoir le certificat avant que vous accédiez au gestionnaire de châssis. Ce processus permet un certificat signé par une autorité de certification de confiance à installer qui peut permettre à un navigateur de client pour faire confiance à la connexion, et évoque l'interface web sans des avertissements.

Configurez

Note: Il n'y a actuellement aucune manière de générer un CSR dans le GUI de gestionnaire de châssis. Il doit être fait par l'intermédiaire de la ligne de commande.

Générez un CSR

Exécutez ces étapes afin d'obtenir un certificat qui contient l'adresse IP ou le nom de domaine complet (FQDN) du périphérique (qui permet à un navigateur de client pour identifier le serveur correctement) :

- Créez un keyring et sélectionnez la taille de module de la clé privée.

Note: Le nom de keyring peut être n'importe quelle entrée. Dans ces exemples, le **firepower_cert** est utilisé.

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

- Configurez les champs CSR. Le CSR peut être généré avec juste des options de base comme un subject-name. Ceci incite pour un mot de passe de demande de certificat aussi bien.

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

- Le CSR peut également être généré avec des options plus avancées qui permettent les informations comme le paramètre régional et l'organisation à encastrent dans le certificat.

```

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

```

- Exportez le CSR pour fournir à votre autorité de certification. Copiez la sortie par laquelle commence (et inclut) -----COMMENCEZ LA DEMANDE DE CERTIFICAT----- extrémités avec (et inclut) -----DEMANDE DE CERTIFICAT D'EXTRÉMITÉ-----.

```

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-----
MIIC6zCCAAdMCAQAwZELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbG1mb3JuaWEx
ETAPBgNVBACMFNhb3NlMRYwFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLDANUQUxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmV2Y2F5MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDLSLoShtBEV10hhf4+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-----

```

Importez la chaîne de certificat d'autorité de certification

Note: Tous les Certificats doivent être dans le format Base64 à importer dans FXOS. Si le certificat ou la chaîne reçue de l'autorité de certification est dans un format différent, vous devez d'abord le convertir avec un outil SSL tel qu'OpenSSL.

- Créez un nouveau point de confiance pour tenir la chaîne de certificat.

Note: Le nom de nom de point de confiance peut être n'importe quelle entrée. Dans des exemples le firepower_chain est utilisé.

```

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-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6B0p3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKcZImiZPyLQBGryFbG9jYwWxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKcZImiZPyLQBGryFbG9jYwWxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgqhkhjOPQIBBggqhkjOPQMBBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQROqZKnkeJUkmlxmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFQQUyInbDHPFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAARQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDOFTkG4p3Tb/2yMAiAtMYh1sv1gCxsQVow0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
fp4120 /security/trustpoint* # commit-buffer

```

Note: Pour une autorité de certification qui l'utilise des Certificats intermédiaires, la racine et des Certificats d'intermédiaire doivent être combinés. Dans le fichier texte, collez le certificat racine au dessus, suivi de chaque certificat intermédiaire dans la chaîne (qui inclut toute **COMMENCENT LE CERTIFICAT** et **CERTIFICAT D'EXTRÉMITÉ** signale). Collez alors ce fichier complet avant la délimitation ENDOFBUF.

Importez le certificat d'identité signé pour le serveur

- Associez le point de confiance créé dans l'étape précédente avec le keyring qui a été créé pour le CSR.

```

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

```

- Collez le contenu du certificat d'identité fourni par l'autorité de certification.

```

fp4120 /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkjOPQQDAjBT
>MRUwEwYKcZImiZPyLQBGryFbG9jYwWxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>bJEGMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2F5
>aWZvcmluZS5yTERMA8GA1UEBxMIU2FuIEpvc2UxZjAUBGNVBAOTDUNpc2NvIFN5c3Rl
>bXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2WjBTMRUwEwYKcZImiZPy
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGo48mMHCQRwLADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopXlu2liDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZOwbHBg
>yodskS/g+a5GNYTzzIS9XafslMSKP06/Ftq2MONVikdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhh1Vq1PGnodNR7mfYwgjm5q9Tp3W0H2ufLGAA2H109XR2FAGMB

```

```

>AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/1WpstiEYExs8DlZWCuHZwPtU5QwHwYDVR0jBBgwFoAUyInbDHPPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBY6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMETleSUyMFNlcnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGhmaWNhdGVsZXZvY2F0aW9uTG1z
>dD9iYXNlP29iamVjdENSYXNzPWNSTERpc3RyaWJldGlvb1BvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDCCBuQYIKWyBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVE10LVBDLUNBLENOPUFJQSxDTj1QdWJsaWMLMjBLZXk1MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydGhmaWNhdGU/YmFzZT9vYmplY3RDdGFzZcz1jZkxJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAUgQUHhIAVwBLAGIAUwBIAHIAHgBIAHIwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvYxjkQ4/dVo2oI6CRB308WQbYHNuU/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF

```

```
fp4120 /security/keyring* # commit-buffer
```

Configurez le gestionnaire de châssis pour utiliser le nouveau certificat

Le certificat a été maintenant installé, mais le service Web n'est pas encore configuré pour l'utiliser.

```

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

```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- **https d'exposition** - La sortie affiche le keyring associé avec le serveur HTTPS. Il devrait refléter le nom créé dans les étapes mentionnées avant. Il si les expositions le transfèrent toujours alors n'a pas été mis à jour pour utiliser le nouveau certificat.

```

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

```

- **affichez le détail de <keyring_name> de keyring** - La sortie affiche le contenu du certificat qui est importé et exposition si elle est valide ou pas.

```
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:

