

# FXOS シャーシ マネージャのための信頼できる 証明書をインストールして下さい

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[CSR の生成](#)

[認証局証明書 チェーンをインポートして下さい](#)

[サーバのための署名された ID証明をインポートして下さい](#)

[シャーシ マネージャを新しい証明書を使用するために設定して下さい](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

この文書に証明書署名要求 ( CSR ) を生成し Firepower 4100 および 9300 シリーズ デバイスの Firepower 拡張可能なオペレーティング システム ( FXOS ) のためのシャーシ マネージャと併用するための結果である ID証明をインストールする方法を記述されています。

## 前提条件

### 要件

次の項目に関する知識が推奨されます。

- コマンド・ラインからの FXOS を設定して下さい
- CSR を使用して下さい
- プライベートキー インフラストラクチャ ( PKI ) 概念

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Firepower 4100 および 9300 シリーズ ハードウェア
- FXOS バージョン 1.1 および 2.0

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響につい

て確実に理解しておく必要があります。

## 背景説明

初期設定の後で、自己署名 SSL 証明書はシャーシ マネージャ Webアプリケーションと併用するための生成されます。その証明書は自己署名であるので、クライアント ブラウザによって自動的に承認されません。それが新しいクライアント ブラウザ シャーシ マネージャ Webインターフェイスにはじめてアクセスする時最初に、ブラウザは接続と同じような SSL 警告を投げます。シャーシ マネージャにアクセスする前に私用でし、ユーザを証明書を受け入れるように要求します。このプロセスはインストールされるべき警告無しでクライアント ブラウザが接続を信頼するように許すことができるおよび始動署名する証明書を Webインターフェイス可能にします信頼された認証局によって。

## 設定

注: 現在シャーシ マネージャ GUI の CSR を生成する方法がありません。それはコマンド・ラインによってする必要があります。

### CSR の生成

( クライアント ブラウザがサーバをきちんと識別するようにする含まれている ) の IP アドレスか完全修飾ドメイン名 ( FQDN ) がデバイス証明書を得るためにこれらのステップを実行して下さい:

- キーホルダーを作成し、プライベートキーの剰余サイズを選択して下さい。

注: キーホルダー名前はどの入力である場合もあります。これらの例では、`firepower_cert` は使用されます。

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

- CSR フィールドを設定して下さい。CSR は subject-name のようなちようど基本的なオプションと生成することができます。これは Certificate 要求パスワードのためにまたプロンプト表示します。

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

- CSR はまた証明書で組み込まれるべき場所および組織のような情報を可能にする高度オプションと生成することができます。

```
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
```

- 認証局に提供するために CSR をエクスポートして下さい。開始する出力をコピーすれば (含んでいます) -----BEGIN CERTIFICATE REQUEST----- 端との (および含んでいます) -----END CERTIFICATE REQUEST-----を探します。

```
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-----
MIIC6zCCAAdCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAGMCkNhbG1mb3JuaWEX
ETAPBgNVBACMCFNhb3N1MRYwFAyDVQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLDANUQUxGjAyaBjNVBAMMEWZwNDEyMC50ZXN0LmxvY2FsmIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDLSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHAKV9bttYg3kf/UEUUGk/EyrVq3B+u2DsooPVq76mTm8BwYmGhbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjdjVVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABOC8wLQYJ
KoZIHvcNAQkOMSAwHjAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVdCL+tATu5xFE3LA310ck6Gj1Nv6W/6r
jBNLxusYilrZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ1OIkyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNTHWTvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfg1dxWf1xAxLzF5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjyQ21DXyDjExp7rCx9
+6bvD1ln70JCegHdCwtP75SaNyaBEPk00365rTckbw==
-----END CERTIFICATE REQUEST-----
```

## 認証局証明書 チェーンをインポートして下さい

注: すべての証明書はインポートされるべき FXOS Base64 フォーマットににある必要があります。認証局から届く証明書がチェーンが別のフォーマットにある場合、OpenSSL のような SSL ツールによって最初にそれを変換して下さい。

- 証明書 チェーンを保持するために新しいトラストポイントを作成して下さい。

注: トラストポイント名前名前はどの入力である場合もあります。例で firepower\_chain は使用されます。

```
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 END_OFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOP3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKZCZImiZPyLQGQBGryFbG9jYwWxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKZCZImiZPyLQGQBGryFbG9jYwWxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgckhkJOPQIBBggqhkjOPQMBBwNCAASvEA27V1EnqlgMtLkvJ6rx
>GXRpXWIEyuiBM4eQroqZKnkeJUkmlxmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAyYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTuMniB/AxPDDN63Lqy
>18odMDofTkg4p3Tb/2yMAiAtMYhlsvlgCxsQVow0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>END_OFBUF
fp4120 /security/trustpoint* # commit-buffer

```

注: 使用する認証局に関しては中間証明書、ルートおよび中間物証明書は結合する必要があります。テキストファイルでは、(上にルート証明を先行しているすべてを始める証明書および END Certificate フラグを含む)の各々の中間証明書にチェーン貼り付けて下さい。それから END\_OFBUF 描写の前にその全体のファイルを貼り付けて下さい。

## サーバのための署名された ID証明をインポートして下さい

- 前の手順で作成される CSR のために作成されたキーホルダーとトラストポイントを関連付けて下さい。

```

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

```

- 認証局によって提供される ID証明の内容を貼り付けて下さい。

```

fp4120 /security/keyring* # set cert
Enter lines one at a time. Enter END_OFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkjOPQQDAjBT
>MRUwEwYKZCZImiZPyLQGQBGryFbG9jYwWxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>bJEGMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>OTU0WhcNMTgwNDI4MTgwOTU0WjBTMRUwEwYKZCZImiZPyLQGQBGryFbG9jYwWxGDAWBgoJ
>aWZvcms5YTERMA8GA1UEBxMIU2FuIEpvc2UxZjAUBGNVBAoTDUNpc2NvIFN5c3Rl
>bXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2WjBTMRUwEwYKZCZImiZPyL
>MA0GCsQsIb3DQEBAAQAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGo48mMHCRCQw1ADWZCxFANxsnbfb+wrR8xKfKo4vvnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67Y0yig9WrvqZObwHBg
>yodsks/g+a5GNYTzzIS9XafslMSKP06/Ftq2MONVIkdKFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhh1Vq1PGnodNR7mfYwgjM5q9Tp3W0H2ufLGAA2H109XR2FAGMB
>AAGjggJYMIICVDAcBgNVHREEFtATghFmcDQxMjAudGVzdC5sb2NhbdAdBgNVHQ4E
>FgQU/1WpstiEYExs8D1ZwcuHwZPtU5QwHwYDVR0jBBgwFoAUyInbDHPPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2WjBTMRUwEwYKZCZImiZPyL
>YmXpYyUyMETlesUyMFNlcnZpY2VzLENOPVnlcnZpY2VzLENOPUNvbmZpZ3VyYXRp

```

```
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGhmaWNhdGVsZXZvY2F0aW9uTG1z
>dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDcBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVE10LVBDLUNBLENOPUFJQSxDTj1QdWJsaWMLMjBLZXk1MjBTZXJ2aWNlcyxD
>Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydGhmaWNhdGU/YmFzZT9vYmplY3RDdGFzZcz1jZlZlJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAUQUHhIAVwBLAGIAUwBIAHIAHgBIAHIwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvYxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
fp4120 /security/keyring* # commit-buffer
```

## シャーシマネージャを新しい証明書を使用するために設定して下さい

証明書は今インストールされてしまいましたが、それを使用するために Web サービスはまだ設定されていません。

```
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
```

## 確認

このセクションでは、設定が正常に機能していることを確認します。

- 示して下さい **https** -出力は HTTPS サーバによって関連付けられるキーホルダーを表示したものです。それは前に述べられるステップで作成される名前を反映する必要があります。それでもデフォルトにそしてそれを示せば新しい証明書を使用することをアップデートしませんでした。

```
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
```

- 示して下さいキーホルダー **<keyring\_name>** 細部-出力はインポートされる表示し、有効であるかどうか示したものです証明書の内容を。

```
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

MRUwEwYKcZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp  
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw  
OTU0WhcNMtgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMQ2Fs  
aWZvcn5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFljAUBgNVBAoTDUNpc2NvIFN5c3Rl  
bXMxDDAKBgNVBAsTAR1RBQzEaMBGGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi  
MA0GCsqGSIB3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga  
BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vvnMLuK3F5U  
RlHLPv9rHtYY296D9c/7N3Tee3gzczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D  
ikoJn55JKRImRMHVkdopXlu21iDeR/9QRRSCT8TKtWrcH67Y0yig9WrvqZOwbHBg  
yodskS/g+a5GNyTzzIS9XAFslMSKP06/Ftq2MONVIkdKFRG0Jqe/IG8a4s/9D82a  
/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2H109XR2FagMB  
AAGjggJYMIICVDAcBgNVHREEFtAtghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E  
FgQU/1WpstiEYExs8DlZWcuHZwPtU5QwHwYDVR0jBBgwFoAUyInbDHPFwEEBcbx  
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh  
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1  
YmXpYyUyMettleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp  
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydG1maWNhdGV5ZXZvY2F0aW9uTG1z  
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50MIHMBGgrBgEF  
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B  
QVVTVE10LVBDLUNBLENOPUFJQSxDTj1QdWJsaW1mJmJBLZkxkMjBTZXXJ2aWNlcYxDTj1  
Tj1TZXJ2aWNlcYxDTj1Db25maWdlcmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs  
P2NBQ2VydG1maWNhdGU/YmFzZT9vYmplY3RDbGFzc21jZXJ0aWZpY2F0aW9uQXV0  
aG9yaXR5MCEGCSsGAQQBjcUAgQUHhIAVwBlAGIAUwBlAHIAAgBlAHIdGyDVR0P  
AQH/BAQDAgWgMBMGA1UdJQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC  
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm  
sgoIK60akbjot0TvUdUd9b6K1Uw=

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

Zeroized: No

- [https:// <FQDN\\_or\\_IP>/](https://<FQDN_or_IP>/)を Webブラウザのアドレスバーで入力し、Firepower シャーシ マネージャに参照し、新しい信頼できる証明書が示されることを確認して下さい。

**警告：** ブラウザはまたアドレスバーの入力に対して証明書の subject-name を確認します、従って証明書がドメイン ネームの絶対表記に発行されれば、ことブラウザの方法アクセスする必要があります。それが IP アドレスによってアクセスされる場合、別の SSL エラーは信頼できる証明書が使用されても投げられます (無効な Common Name)。

## トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- [FXOS CLI にアクセスする方法](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)