

Instalar um Certificado de Confiabilidade para o Gerenciador de Chassi FXOS

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Gerar aCSR](#)

[Importar a cadeia de certificados da autoridade de certificação](#)

[Importar o Certificado de Identidade Assinado para o Servidor](#)

[Configurar o gerenciador de chassis para usar o novo certificado](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como gerar um CSR e instalar o certificado de identidade para uso com o Chassis Manager para FXOS em dispositivos FP 4100/9300 series.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configurar o sistema operacional extensível (FXOS) Firepower a partir da linha de comando
- Usar CSR (Certificate Signing Request, Solicitação de assinatura de certificado)
- Conceitos da infraestrutura de chave privada (PKI)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Hardware Firepower (FP) 4100 e 9300 Series
- FXOS versões 2.10

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Após a configuração inicial, um certificado SSL autoassinado é gerado para uso com o aplicativo da Web Gerenciador de chassis. Como esse certificado é autoassinado, ele não é automaticamente confiável para navegadores clientes. Na primeira vez que um novo navegador cliente acessa a interface da Web do Gerenciador de chassis, o navegador lança um aviso SSL semelhante à sua conexão, dizendo que ela não é privada e exige que o usuário aceite o certificado antes de você acessar o Gerenciador de chassis. Esse processo permite que um certificado assinado por uma autoridade de certificação confiável seja instalado, o que permite que um navegador cliente confie na conexão e ative a interface da Web sem avisos.

Configurar

Gerar um CSR

Execute estas etapas para obter um certificado que contenha o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do dispositivo (que permite que um navegador cliente identifique o servidor adequadamente):

- Crie um chaveiro e selecione o tamanho do módulo da chave privada.



Observação: o nome do chaveiro pode ser qualquer entrada. Nesses exemplos, `firepower_cert` é usado.

Este exemplo cria um chaveiro com um tamanho de chave de 1024 bits:

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
```

- Configure os campos de CSR. O CSR pode ser gerado apenas com opções básicas, como um nome de assunto. Isso também solicita uma senha de solicitação de certificado.

Este exemplo cria e exibe uma solicitação de certificado com um endereço IPv4 para um toque de chave, com opções básicas:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
```

```
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
```


- O CSR também pode ser gerado com opções mais avançadas que permitem que informações como localidade e organização sejam incorporadas no certificado.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set "ip 192.168.200.123"
Firepower-chassis /security/keyring/certreq* # set subject-name "sjc04"
Firepower-chassis /security/keyring/certreq* # set country "US"
Firepower-chassis /security/keyring/certreq* # set dns "bg1-samc-15A"
Firepower-chassis /security/keyring/certreq* # set email "test@cisco.com"
Firepower-chassis /security/keyring/certreq* # set locality "new york city"
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name "Testing"
Firepower-chassis /security/keyring/certreq* # set state "new york"
Firepower-chassis /security/keyring/certreq* # commit-buffer
```


- Exporte o CSR para fornecer à sua autoridade de certificação. Copie a saída que começa com (e inclui) -----BEGIN CERTIFICATE REQUEST----- termina com (e inclui) -----END CERTIFICATE REQUEST-----.

```
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZ04UGqILKFXQQc2c8b/vW2rnRF80PhKbhghLA1YZ1F
JqcYEG5Y11+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1Wsy1wUWV4
Ore/zgTk/WCd56Rf0BvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQA6CBnNhbwMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAA0BgQCcsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWlctWgHhH8Bim0b/00KuG8kwfIGGsED1Av
TTYvUP+BZ90FiPbRIA718S+V8ndXr1HejiQGx1DNqoN+odCXPc5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----
```


Importar a cadeia de certificados da autoridade de certificação

 Observação: todos os certificados devem estar no formato Base64 para serem importados para FXOS. Se o certificado ou a cadeia recebido da Autoridade de Certificação estiver em um formato diferente, você deverá primeiro convertê-lo com uma ferramenta SSL, como OpenSSL.

- Crie um novo ponto confiável para manter a cadeia de certificados.
-

 Observação: o nome do ponto confiável pode ser qualquer entrada. Nos exemplos, `firepower_chain` é usado.

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADBOMQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IE1uYy4xEzARBgNVBAS
> Tc1Rlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQe0GHemd66u2/XAoLx7YCCyU
> ZgAmIvyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzC190306Mg51zq1zXcz75+VFj2I6rH9asckC1d3mk0Vx5gJU
> Ptt5CVQpNgNLdvbDPSSxretysOhqHmp9+CLv8FDuy1CDYfualtv1WvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3n04MIGeBgNVHSMegZYwgZ0AFL1NjtcEMyZ+f7+3yh42
> 1ido3n04oXikdJBOMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAc
> Tc1NhbhRiIENsYXJhMRswGQYDVQQKEwJ0dW92YSBTeXN0ZW1zIE1uYy4xFDASBgNV
> BAsTC0VuZ21uZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GAQAwdAYDVROTBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAA0BgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYi04z42/j9Ijenh75tCKMhW51az8copP1EBm0cyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
```

 Observação: para uma Autoridade de Certificação que usa certificados intermediários, a raiz e os certificados intermediários devem ser combinados. No arquivo de texto, cole o certificado raiz na parte superior, seguido por cada certificado intermediário na cadeia (que inclui todos os sinalizadores BEGIN CERTIFICATE e END CERTIFICATE). Em seguida, cole o arquivo inteiro antes da delimitação ENDOFBUF.

Importar o Certificado de Identidade Assinado para o Servidor

- Associe o ponto confiável criado na etapa anterior ao chaveiro criado para o CSR.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
```

- Cole o conteúdo do certificado de identidade fornecido pela Autoridade de Certificação.

```
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAQgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGAlUE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZkxhbnBzZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWElHVZZXJAZXhhbnBzZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YccYU
> ZgAMivYCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMBkPayVlQjbg4MD2dx2+H8EH3LMtdZrgKvPxPTE+bf5wZVNAGMBAAGGJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl90306Mg51zq1zXcz75+VFj2I6rH9asckClD3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSSxretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L4317IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
```

Configurar o gerenciador de chassis para usar o novo certificado

O certificado foi instalado, mas o serviço Web ainda não está configurado para usá-lo.

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- show https - A saída exibe o chaveiro associado ao servidor HTTPS. Ele pode refletir o

nome criado nas etapas mencionadas anteriormente. Se ele ainda mostrar o padrão, significa que não foi atualizado para usar o novo certificado.

```
<#root>
```

```
Firepower-chassis /system/services #
```

```
show https
```

```
Name: https Admin State: Enabled Port: 443 Operational port: 443 Key Ring: kring7984
```

```
Cipher suite mode: Medium Strength Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HI
```

- `show keyring <keyring_name> detail` - A saída exibe o conteúdo do certificado que é importado e mostra se é válido ou não.

```
<#root>
```

```
fp4120 /security #
```

```
scope security
```

```
fp4120 /security #
```

```
show keyring kring7984
```

```
detail
```

```
Keyring
```

```
kring7984
```

```
: RSA key modulus: Mod2048 Trustpoint CA: tPoint10
```

```
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:
```


```
-----BEGIN CERTIFICATE-----
```


```
MIIE8DCBjAgAwIBAgITRQAAAAreh1UWgiTzvgAAAAACjAKBggqhkjOPQDAjBT MRUwEwYKCZImiZPyLQGGRYFbG9jYWwxGDAWBg
```

```
-----END CERTIFICATE-----
```

```
Zeroized: No
```

- Insira `https://<FQDN_or_IP>/` na barra de endereços de um navegador da Web, navegue até o Firepower Chassis Manager e verifique se o novo certificado confiável é apresentado.

 **Aviso:** os navegadores também verificam o nome da entidade de um certificado em relação à entrada na barra de endereços. Portanto, se o certificado for emitido para o nome de domínio totalmente qualificado, ele deverá ser acessado dessa forma no navegador. Se for

 acessado via endereço IP, um erro SSL diferente será lançado (Nome comum inválido) mesmo que o certificado confiável seja usado.

Troubleshooting

No momento, não há informações específicas disponíveis para solucionar esse problema de configuração.

Informações Relacionadas

- [Acessando a CLI FXOS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.