

FXOS 새시 관리자용 신뢰할 수 있는 인증서 설치

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[CSR 생성](#)

[인증 기관 인증서 체인 가져오기](#)

[서버에 대한 서명 ID 인증서 가져오기](#)

[새 인증서를 사용하도록 새시 관리자 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 CSR을 생성하고 FP 4100/9300 시리즈 디바이스에서 FXOS용 새시 관리자와 함께 사용할 ID 인증서를 설치하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 명령줄에서 Firepower eXtensible 운영 체제(FXOS) 구성
- CSR(Certificate Signing Request) 사용
- PKI(Private Key Infrastructure) 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower(FP) 4100 및 9300 Series 하드웨어
- FXOS 버전 2.10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

초기 컨피그레이션 후 Chassis Manager 웹 애플리케이션에 사용할 자체 서명 SSL 인증서가 생성됩니다. 이 인증서는 자체 서명되므로 클라이언트 브라우저에서 자동으로 신뢰되지 않습니다. 새 클라이언트 브라우저가 처음으로 Chassis Manager 웹 인터페이스에 액세스하면 브라우저는 사용자의 연결과 유사한 SSL 경고를 발생시키며, 이는 비공개가 아니므로 사용자가 Chassis Manager에 액세스하기 전에 인증서를 수락해야 합니다. 이 프로세스에서는 신뢰할 수 있는 인증 기관에서 서명한 인증서를 설치할 수 있습니다. 그러면 클라이언트 브라우저에서 연결을 신뢰하고 경고 없이 웹 인터페이스를 불러올 수 있습니다.

구성

CSR 생성

디바이스의 IP 주소 또는 FQDN(Fully Qualified Domain Name)이 포함된 인증서를 가져오려면 다음 단계를 수행하십시오. 그러면 클라이언트 브라우저에서 서버를 올바르게 식별할 수 있습니다.

- 키링을 생성하고 개인 키의 모듈러스 크기를 선택합니다.

 참고: 키 링 이름은 모든 입력이 될 수 있습니다. 이 예에서는 firepower_cert가 사용됩니다.

다음 예에서는 키 크기가 1024비트인 키링을 생성합니다.

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

- CSR 필드를 구성합니다. CSR은 주체 이름과 같은 기본 옵션만으로 생성할 수 있습니다. 그러면 인증서 요청 비밀번호도 입력하라는 프롬프트가 표시됩니다.

이 예에서는 기본 옵션과 함께 키 링에 대한 IPv4 주소가 포함된 인증서 요청을 생성하여 표시합니다.

```
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
```

- CSR은 로케일 및 조직과 같은 정보를 인증서에 포함할 수 있는 고급 옵션을 사용하여 생성할


수도 있습니다.

```
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
```


- 인증 기관에 제공할 CSR을 내보냅니다. -----BEGIN CERTIFICATE REQUEST(시작 인증서 요청)로 시작하고 이----- 포함하는 출력을 복사합니다. 이 출력은 -----END CERTIFICATE REQUEST(종료 인증서 요청)로 -----.

```
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
gY0AMIGJAoGBALpKn1t8qMZ04UGqILKFXQc2c8b/vw2rnRF80PhKbhghLA1YZ1F
JqcYEG5Y11+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1Wsy1wUWV4
Ore/zgTk/WCd56RF0BvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBqkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWwMwNICeCsEiXjAN
BgkqhkiG9w0BAQQFAA0BgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWICtWgHhH8Bim0b/00KuG8kwfIGGsED1Av
TTYvUP+BZ90FiPbRIA718S+V8ndXr1HejiQGx1DNqoN+odCXPc5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----
```


인증 기관 인증서 체인 가져오기

 참고: 모든 인증서를 FXOS로 가져오려면 Base64 형식이어야 합니다. 인증 기관에서 받은 인증서 또는 체인이 다른 형식인 경우 먼저 OpenSSL과 같은 SSL 도구로 변환해야 합니다.

- 인증서 체인을 보유할 새 신뢰 지점을 만듭니다.

 참고: 신뢰 지점 이름은 모든 입력이 될 수 있습니다. 예제에서는 firepower_chain이 사용됩니다.

```
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-----
> MIIDMCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IE1uYy4xEzARBGNVBAsT
> C1R1c3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQe0GHemd66u2/XAoLx7YCCyU
> ZgAmivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzC190306Mg51zq1zXcz75+VFj2I6rH9asckC1d3mk0Vx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfualtv1WvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3n04MIGeBgNVHSMegZYwgZ0AFL1NjtcEMyZ+f7+3yh42
> 1ido3n04oXikdjBOMQswCQYDVQQKEwJ0dW92YSBTeXN0ZW1zIE1uYy4xFDASBgNV
> C1NhbnRhiENsYXJhMRswGQYDVQQKEwJ0dW92YSBTeXN0ZW1zIE1uYy4xFDASBgNV
> BAsTC0VuZ21uZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwdAYDVR0TBAlUwAwEB
> /zANBgkqhkiG9w0BAQQFAA0BgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYi04z42/j9Ijenh75tCKMhw51az8copP1EBm0cyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
```

 참고: 중간 인증서를 사용하는 인증 기관의 경우 루트 인증서와 중간 인증서를 결합해야 합니다. 텍스트 파일의 맨 위에 루트 인증서를 붙여넣고, 그 뒤에 체인의 각 중간 인증서(모든 BEGIN CERTIFICATE 및 END CERTIFICATE 플래그 포함)를 붙여 넣습니다. 그런 다음 ENDOFBUF 설명 앞에 전체 파일을 붙여넣습니다.

서버에 대한 서명 ID 인증서 가져오기

- 이전 단계에서 생성한 신뢰 지점을 CSR용으로 생성한 키링과 연결합니다.

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

- 인증 기관에서 제공하는 ID 인증서의 내용을 붙여넣습니다.

```

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/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGAlUE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBASt
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWElVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> 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

```

새 인증서를 사용하도록 새시 관리자 구성

인증서가 설치되었지만 웹 서비스가 아직 인증서를 사용하도록 구성되지 않았습니다.

```

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

```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

- `show https` - 출력에 HTTPS 서버와 연결된 키링이 표시됩니다. 앞서 언급한 단계에서 생성된 이름을 반영할 수 있습니다. 여전히 기본값이 표시되면 새 인증서를 사용하도록 업데이트되지 않은 것입니다.

```
<#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:+HIGH

- `show keyring <keyring_name> detail` - 가져온 인증서의 내용을 출력하며, 해당 인증서의 유효 여부를 표시합니다.

```
<#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-----
```

```
MIIE8DCCBJagAwIBAgITRQAAAAreh1UWgiTzvgAAAAACjAKBggqhkJOPQDAjBT MRUwEwYKCZImiZPyLQGByFbG9jYWwxGDAWBg
```

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

```
Zeroized: No
```

- 웹 브라우저의 주소 표시줄에 `https://<FQDN_or_IP>/`를 입력하고 Firepower 새시 관리자로 이동하여 새 신뢰할 수 있는 인증서가 표시되는지 확인합니다.

 경고: 브라우저에서는 주소 표시줄의 입력에 대해 인증서의 주체 이름을 확인하므로 인증서가 정규화된 도메인 이름으로 발급된 경우 브라우저에서 해당 이름으로 액세스해야 합니다. IP 주소를 통해 액세스하는 경우, 신뢰할 수 있는 인증서가 사용되더라도 다른 SSL 오류 (Common Name Invalid)가 발생합니다.

문제 해결

현재 이 구성의 문제를 해결하는 데 사용할 수 있는 특정 정보가 없습니다.

관련 정보

- [FXOS CLI 액세스](#)

- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.