安裝FXOS機箱管理器的受信任證書

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[背景資訊](#)

[設定](#)

- [產生CSR](#)
- [匯入證書頒發機構證書鏈](#)
- [匯入伺服器的簽名身份證書](#)
- [配置機箱管理器以使用新證書](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文說明如何產生CSR和安裝身份憑證，以便在FP 4100/9300系列裝置上用於FXOS的機箱管理員。

必要條件

需求

思科建議您瞭解以下主題：

- 從命令列配置Firepower可擴展作業系統(FXOS)
- 使用憑證簽署請求(CSR)
- 私鑰基礎架構(PKI)概念

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower(FP)4100和9300系列硬體
- FXOS版本2.10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

初始配置後，將生成自簽名SSL證書，供機箱管理器Web應用程式使用。由於證書是自簽名的，因此客戶端瀏覽器不會自動信任該證書。新客戶端瀏覽器首次訪問機箱管理器Web介面時，瀏覽器會拋出與您的連線類似的SSL警告（非專用），並要求使用者在訪問機箱管理器之前接受證書。此過程允許安裝由受信任的證書頒發機構簽名的證書，這允許客戶端瀏覽器信任連線，並在沒有警告的情況下啟動Web介面。

設定

產生CSR

執行以下步驟以獲取包含裝置（允許客戶端瀏覽器正確識別伺服器）的IP地址或完全限定域名(FQDN)的證書：

- 建立金鑰環並選擇私鑰的模數大小。

 注意：金鑰環名稱可以是任何輸入。在這些示例中，使用firepower_cert。

此範例會建立金鑰大小為1024位元的金鑰環：

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

- 設定CSR欄位。可以只使用基本選項（如使用者名稱）來產生CSR。這也會提示輸入憑證要求密碼。

本示例建立並顯示一個證書請求，該請求帶有用於金鑰環的IPv4地址，並具有以下基本選項：

```
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
```

- 也可以使用更高級的選項來生成CSR，這些選項允許將區域設定和組織等資訊嵌入到證書中。

```
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
```

- 匯出CSR以提供給您的證書頒發機構。複製以（包括）-----BEGIN CERTIFICATE REQUEST)-----以（包括）-----END CERTIFICATE REQUEST)結尾-----。

```
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
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/OOKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXDOlZTL09H
BA==
-----END CERTIFICATE REQUEST-----
```

匯入證書頒發機構證書鏈

注意：所有證書必須採用Base64格式才能匯入到FXOS。如果從證書頒發機構接收的證書或鏈採用不同的格式，則必須首先使用SSL工具（如OpenSSL）對其進行轉換。

- 建立新的信任點以保留證書鏈。

注意：信任點名稱可以是任何輸入。示例中使用了firepower_chain。

```
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-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl9O3O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0OQGCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc4OwhuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
```

注意：對於使用中間證書的證書頒發機構，必須組合根證書和中間證書。在文本檔案中，將根憑證貼上在頂端，接著貼上鏈結中的每個中間憑證（包括所有BEGIN CERTIFICATE和END CERTIFICATE標誌）。然後，在ENDOFBUF劃分之前貼上整個檔案。

匯入伺服器的簽名身份證書

- 將在上一步中建立的信任點與為CSR建立的金鑰環相關聯。

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

- 貼上證書頒發機構提供的身份證書的內容。

```
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/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
```

```
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
```

配置機箱管理器以使用新證書

證書現在已安裝，但Web服務尚未配置為使用它。

```
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
```

驗證

使用本節內容，確認您的組態是否正常運作。

- show https - Output顯示與HTTPS伺服器相關聯的金鑰環。它可反映前面提到的步驟中建立的名稱。如果仍然顯示預設值，則未將其更新為使用新證書。

<#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 - Output顯示已匯入的憑證內容，並顯示其是否有效。

<#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-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkjOPQQDAjBT MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBg
-----END CERTIFICATE-----
 Zeroized: No
```

- 在Web瀏覽器的位址列中輸入https://<FQDN_or_IP>/，瀏覽到Firepower機箱管理器，並驗證是否顯示新的受信任證書。

警告：瀏覽器還根據位址列中的輸入來驗證證書的使用者名稱，因此，如果向完全限定的域名頒發證書，則必須在瀏覽器中通過這種方式訪問證書。如果通過IP地址訪問它，則即使使用受信任的證書，也會引發其他SSL錯誤（公用名無效）。

疑難排解

目前尚無特定資訊可用於排解此組態的疑難問題。

相關資訊

- 訪問FXOS CLI
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。