

為CMX上的第三方證書和安裝生成CSR

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[驗證](#)

簡介

本文說明如何產生憑證簽署請求(CSR)，以便取得第三方憑證，以及如何將鏈結憑證下載到思科連線行動體驗(CMX)。

必要條件

需求

思科建議您瞭解以下主題：

- Linux基礎知識
- 公開金鑰基礎架構 (PKI)
- 數位憑證

採用元件

本檔案中的資訊是根據CMX版本10.3

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。

設定

產生CSR

步驟1.連線到CMX的CLI，以根使用者身份訪問，移動到證書目錄並為CSR和金鑰檔案建立資料夾。

```
[cmxadmin@cmx]$ su -  
Password:  
[root@cmx]# cd /opt/haproxy/ssl/  
[root@cmx]# mkdir newcert  
[root@cmx]# cd newcert
```

附註：CMX上證書的預設目錄是/opt/haproxy/ssl/。

步驟2.產生CSR和金鑰檔案。

```
[root@cmx newcert]# openssl req -nodes -days 365 -newkey rsa:2048 -keyout
/opt/haproxy/ssl/newcert/private.key -out /opt/haproxy/ssl/newcert/cert.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/opt/haproxy/ssl/newcert/private.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:MX
State or Province Name (full name) []:Tlaxcala
Locality Name (eg, city) [Default City]:Tlaxcala
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (eg, your name or your server's hostname) []:cmx.example.com
Email Address []:cmx@example.com
```

步驟3.讓第三方簽署CSR。

若要從CMX取得憑證並將其傳送至第三方，請執行**cat**命令以開啟CSR。您可以將輸出複製並貼上到.txt檔案中，也可以根據第三方的要求更改副檔名。以下提供範例。

```
[root@cmx newcert]# cat cert.crt
-----BEGIN CERTIFICATE REQUEST-----
MIICOTCCAbkCAQAwgYsxCzAJBgNVBAYTAklYMREwDwYDVQQIDAhUbgGF4Y2FsYTER
MA8GA1UEBwwIVGxheGNhbGExdDjAMBgNVBAoMBUNpc2NmMQwwCgYDVQQLDANUQUMx
GDAWBgNVBAMMD2NteC5leGFtcGxlLmNvbTEeMBWGCsGSIb3DQEJARYPY214QGv4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2YybDkDR
vRSwD19EvaJehsNjG9Cyo3vQPOpCAAdg jFBpUHMt8QNg6YFdhYZdpKaRTJXhztm
fa/7Nevb1IP/pSBgYRxxHXQEHl9Gj4DT0gT2T+AZ8j3J9KMSe8Bakj4qY8Ua7GCdC
A62NzVcDxDm83gUD92oGbxOF9VFE2hiRvCQc+d6gBRuTOXxtyLBAtcL3hkiOEQx7
sDA55CwZU7ysMdWHUBn4AglzIlgPyzlmT3dwr0gfOSYN4j5+H0nrYtrPBZSUbZaa
8pGXVu7sFtV8bahgtnYiCUTiz9J+k5V9DBjqPSzYzb3+KxeAA+g0iV3J1VzsLnt7
mVocT9oPaOEI8wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAI6Q/A4zTfrWP2uS
xtN8X6p6aP8guU0bTWhGEMBEGBQd0bBWYdhxaItGt1a1tdNcIGLACeMPuk7WpsiH
rUs5kiIj1Ac2/ANBao6/nlv56vhGUx0dOq0fk/g1brKL+a8Lx9ixtee77aPZ1xVD
A/n3FdNdSIidWH0M4q8JunxbT33vM9h8H6oqe/JI3BDnw4tRnkYaGwJsyWU1PCuO
TWPMagMkntv0JaEOHlg4/JZyVSdDiTnmb/U8cEH2RrcUP8iwjykDpb/V4tb4VtgM
7+9HKxQRQHq5Qji8/QyMG6ctoD+B7k6UpzXvi5FpvqGQWwXJNC52suAt0QeeZj1J
rpudLUs=
-----END CERTIFICATE REQUEST-----
[root@cmx newcert]#
```

步驟4.建立用於匯入CMX的證書鏈。

若要建立最終憑證，請將簽署好的憑證複製貼上到包含私密金鑰、中間憑證和根憑證的.txt檔案中。確保將其另存為.pem文件。

此範例顯示最終憑證的格式。

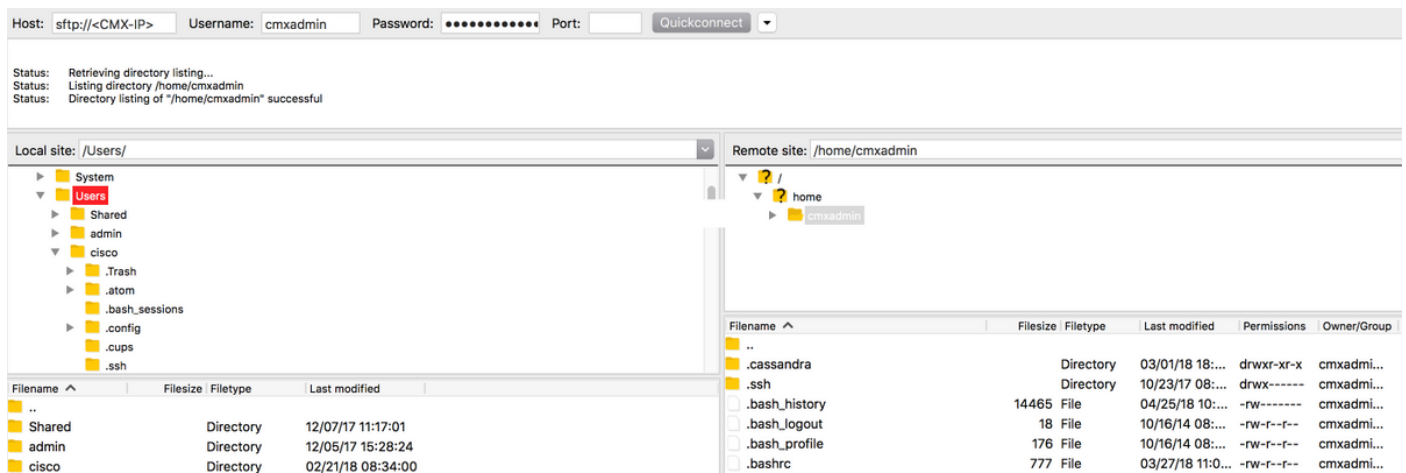
```

-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEAg2gXgEo7ouyBfWwCkctcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed certificate
MIIFEzCCAavugAwIBAgIBfzANBgkqhkiG9w0BAQsFADCB1DELMAkGAlUEBhMCCVVMx
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----

```

步驟5.將最終憑證傳輸到CMX。

若要將最終憑證從您的電腦傳輸到CMX，請開啟SFTP應用程式，並使用管理員憑證連線到CMX。您必須能夠檢視CMX的資料夾，如下圖所示。



然後將鏈結憑證拖放到/home/cmxadmin/資料夾。

附註：開啟CMX的SFTP連線時的預設目錄為/home/cmxadmin/。

步驟6.更改最終證書和所有者的許可權。然後將其移動到包含私鑰的資料夾中。以下提供範例。

```

[root@cmx ~]# cd /home/cmxadmin/
[root@cmx cmxadmin]# chmod 775 final.pem
[root@cmx cmxadmin]# chown cmx:cmx final.pem
[root@cmx cmxadmin]# mv final.pem /opt/haproxy/ssl/newcert/
[root@cmx cmxadmin]# cd /opt/haproxy/ssl/newcert/
[root@cmx newcert]# ls -la
total 16
drwxr-xr-x 2 root root 4096 Apr 25 12:30 .
drwxr-xr-x 4 cmx cmx 4096 Apr 25 09:25 ..
-rw-r--r-- 1 root root 1054 Apr 25 11:01 cert.crt
-rwxrwxr-x 1 cmx cmx 0 Apr 25 12:29 final.pem
-rw-r--r-- 1 root root 1708 Apr 25 11:01 private.key
[root@cmx newcert]#

```

步驟7.確保正確構建所有元件。

```
[root@cmx newcert]#openssl verify -CAfile /opt/haproxy/ssl/newcert/final.pem
/opt/haproxy/ssl/newcert/final.pem
/opt/haproxy/ssl/newcert/final.pem: OK
```

您必須收到OK消息。

步驟8.安裝最終證書並重新啟動CMX。

```
[root@cmx newcert]#cmxctl node sslmode enable --pem /opt/haproxy/ssl/newcert/final.pem
enabling ssl
ssl enabled
```

```
[root@cmx newcert]#reboot
```

第9步 (可選)。 如果執行CMX 10.3.1或以上版本，可能會受到以下錯誤的影響：

- [CSCvh21464](#) :CMX WEBUI不使用已安裝的自簽名證書或第三方證書


此錯誤會阻止CMX更新憑證路徑。解決此問題的解決方法是建立兩個軟連結以指向新憑證和私密金鑰，然後重新載入CMX。以下是範例：

```
[root@cmx ~]# cd /opt/haproxy/ssl/
[root@cmx ssl]# mkdir backup
[root@cmx ssl]# mv host.pem backup/
[root@cmx ssl]# mv host.key backup/
[root@cmx ssl]# ln -s /opt/haproxy/ssl/newcert/final.pem host.pem
[root@cmx ssl]# ln -s /opt/haproxy/ssl/newcert/private.key host.key
[root@cmx ssl]#
[root@cmx ssl]# ls -la
total 16
drwxr-xr-x 4 cmx cmx 4096 Apr 25 12:59 .
drwxr-xr-x 6 cmx cmx 4096 Mar 31 2017 ..
lrwxrwxrwx 1 root root 36 Mar 26 09:58 host.key -> /opt/haproxy/ssl/newcert/private.key
lrwxrwxrwx 1 root root 38 Mar 26 09:58 host.pem -> /opt/haproxy/ssl/newcert/final.pem
drwxr-xr-x 2 root root 4096 Apr 25 12:30 newcert
[root@cmx ssl]#
[root@cmx ssl]# reboot
```

驗證

開啟CMX的GUI，本例中使用的是Google Chrome。按一下URL旁邊的**Secure**索引標籤以開啟憑證，並檢視詳細資訊，如下圖所示。

CA-KCG-lab
cmx.example.com

 **cmx.example.com**
Issued by: CA-KCG-lab
Expires: Tuesday, January 19, 2021 at 13:50:21 Central Standard Time
✔ This certificate is valid

▼ **Details**

Issuer Name	
Country	MX
State/Province	Nuevo Leon
Locality	Guadalupe
Organization	mex-wireless
Organizational Unit	lab-mex-wireless
Common Name	CA-KCG-lab

OK

CA-KCG-lab
cmx.example.com

Subject Name	
Country	MX
State/Province	Tlaxcala
Locality	Tlaxcala
Organization	Cisco
Organizational Unit	TAC
Common Name	cmx.example.com
Email Address	cmx@example.com
Not Valid Before	Wednesday, April 25, 2018 at 14:50:21 Central Daylight Time
Not Valid After	Tuesday, January 19, 2021 at 13:50:21 Central Standard Time

OK