

为第三方证书生成CSR并在CMX上安装

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

简介

本文档介绍如何生成证书签名请求(CSR)以获取第三方证书，以及如何将链接证书下载到思科互联移动体验(CMX)。

先决条件

要求

Cisco 建议您了解以下主题：

- Linux基础知识
- 公用密钥基础结构 (PKI)
- 数字证书

使用的组件

本文档中的信息基于CMX版本10.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

生成CSR

步骤1.连接到CMX的CLI，以根用户身份访问，移动到证书目录并为CSR和密钥文件创建文件夹。

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

注意：CMX上证书的默认目录是/opt/haproxy/ssl/。

步骤2.生成CSR和密钥文件。

```
[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
```

步骤3.获得第三方签署的CSR。

要从CMX获取证书并将其发送到第三方，请运行**cat**命令以打开CSR。您可以将输出复制并粘贴到.txt文件中，或根据第三方的要求更改扩展名。下面是一个示例。

```
[root@cmx newcert]# cat cert.crt
-----BEGIN CERTIFICATE REQUEST-----
MIICOTCCAbkCAQAwgYsxCzAJBgNVBAYTAk1YMREwDwYDVQQIDAhUbgGF4Y2FsYTER
MA8GA1UEBwwIVGxheGNhbGExdGJAMBgNVBAoMBUNpc2NmMQwwCgYDVQQQLDANUQUx
GDAWBgNVBAMMD2NteC5leGFtcGxlLmNvbTEeMBWGCsGSIb3DQEJARYPY214QGv4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2YybDkDR
vRSwD19EvaJehsNjG9Cyo3vQPOpCAAdg jFBpUHMt8QNgn6YFdhYZdpKaRTJXhztm
fa/7Nevb1IP/pSBgYRxBHXQEHl9Gj4DT0gT2T+AZ8j3J9KMSe8Bakj4qY8Ua7GCdC
A62NzVcDxDm83gUD92oGbxOF9VFE2hiRvCQc+d6gBRuTOXxtyLBAtcL3hkiOEQx7
sDA55CwZU7ysMdWHUBn4AglzI1gPyzlmT3dwr0gfOSYN4j5+H0nrYtrPBZSUbZaa
8pGXVu7sFtV8bahgtNyiCUTiz9J+k5V9DBjqpsZyZb3+KxeAA+g0iV3J1VzsLnt7
mVocT9oPaOEI8wIDAQABoAAAwDQYJKoZIhvcNAQEFBQADggEBAI6Q/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]#
```

步骤4.创建证书链以导入CMX。

要创建最终证书，请将签名证书复制并粘贴到包含私钥、中间证书和根证书的.txt文件中。确保将其另存为.pem文件。

此示例显示最终证书的格式。

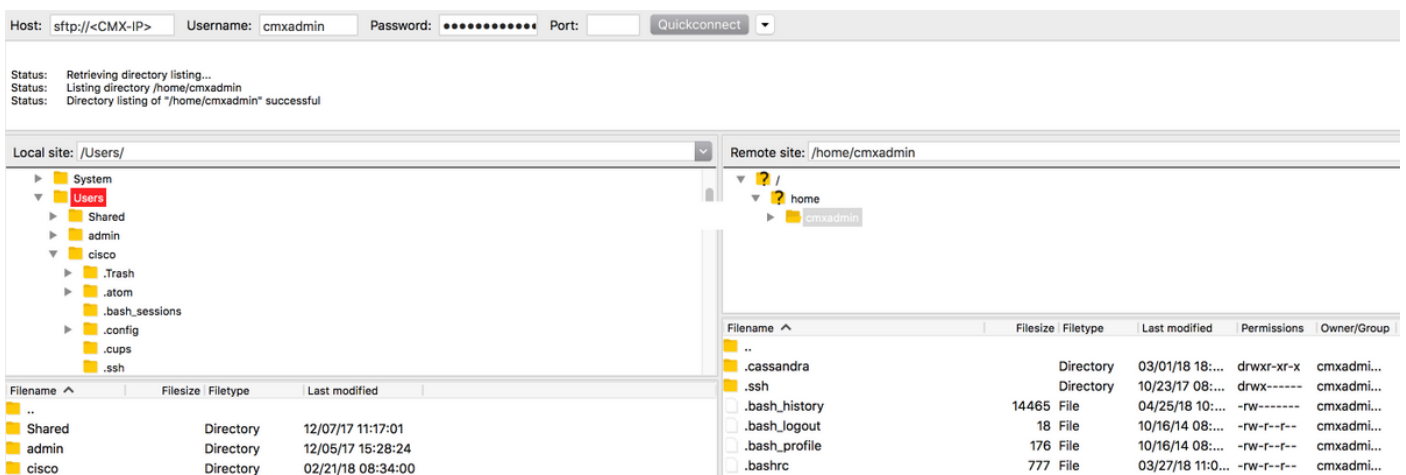
```

-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEAg2gXgEo7ouyBfWwCkctcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed certificate
MIIFEzCCAvugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCB1DELMAkGAlUEBhMCVVMx
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----

```

步骤5.将最终证书传输到CMX。

要将最终证书从计算机传输到CMX，请打开SFTP应用并使用管理员凭证连接到CMX。您必须能够查看CMX的文件夹，如图所示。



然后，将链接的证书拖放到文件夹/home/cmxadmin/。

注意：打开与CMX的SFTP连接时，默认目录是/home/cmxadmin/。

步骤6.更改最终证书和所有者的权限。然后将其移动到包含私钥的文件夹。下面是一个示例。

```

[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]#

```

步骤7.确保所有设备都正确构建。

```
[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
```

您必须收到OK消息。

步骤8.安装最终证书并重新启动CMX。

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

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

步骤 9 (可选) 。 如果运行CMX 10.3.1或更高版本，则可能受此Bug影响：

- [CSCvh21464](#) :CMX WEBUI不使用已安装的自签名或第三方证书


此漏洞阻止CMX更新证书路径。解决此问题的解决方法是创建两个指向新证书和私钥的软链路，然后重新加载CMX。示例如下：

```
[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
```

验证

打开CMX的GUI，在本例中使用Google Chrome。单击URL旁边的**Secure**选项卡打开证书，并查看详细信息，如图所示。

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