

Generar una CSR para certificado de terceros e instalación en CMX

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

Introducción

Este documento describe cómo generar una solicitud de firma de certificado (CSR) para obtener un certificado de terceros y cómo descargar un certificado encadenado a Cisco Connected Mobile Experiences (CMX).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de Linux
- Public Key Infrastructure (PKI)
- Certificados digitales

Componentes Utilizados

La información de este documento se basa en la versión 10.3 de CMX

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Generar CSR

Paso 1. Conéctese a la CLI de CMX, acceda como raíz, vaya al directorio de certificados y cree una carpeta para la CSR y el archivo de clave.

```
[cmxadmin@cmx]$ su -
```

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

Nota: El directorio predeterminado para los certificados en CMX es /opt/haproxy/ssl/.

Paso 2. Genere el CSR y el archivo de clave.

```
[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
```

Paso 3. Consiga la CSR firmada por un tercero.

Para obtener el certificado de CMX y enviarlo a terceros, ejecute el comando **cat** para abrir la CSR. Puede copiar y pegar el resultado en un archivo .txt o cambiar la extensión según los requisitos de terceros. Aquí está un ejemplo.

```
[root@cmx newcert]# cat cert.crt
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwYsxCzAJBgNVBAYTAk1YMREwDwYDVQQIDAhUbgGF4Y2FsYTER
MA8GA1UEBwwIVGxheGNhbGExdDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQQLDANUQUxMx
GDAWBgNVBAMMD2NteC5leGftcGx1LmNvbTEeMBwGCsqGSIB3DQEJARYPY214QGV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE2YybDkDR
vRSwD19EVaJehsNjG9Cyo3vQPOPcAAdgjFBpUHMT8QNgn6YFdHYZdpKaRTJXhztm
fa/7Nevb1IP/pSBgYRxHXQEh19Gj4DT0gT2T+AZ8j3J9KMSe8Bakj4qY8Ua7GCdC
A62NzVcDxDM83gUD92oGbxOF9VFE2hiRvCQc+d6gBRuTOXxyLBAtcL3hkiOEQx7
sDA55CwZU7ysMdWHUBn4AglzIlgPyzlmT3dwr0gfOSYN4j5+H0nrYtrPBZSUBzAa
8pGXVu7sFtV8bahgtNyiCUTiz9J+k5V9DBjqPszYzb3+KxeAA+g0iV3J1VzsLNT7
mVocT9oPaOEI8wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAI6Q/A4zTfrWP2uS
xtN8X6p6aP8guU0bTWhGEMBEgBQd0bBWYdhxaItGt1altNcIGLACeMPuk7WpsiH
rUs5kiIj1Ac2/ANBao6/nlv56vhGUx0d0q0fk/g1brKL+a8Lx9ixtee77aPZ1xVD
A/n3FdNdSiidWH0M4q8JunxbT33vM9h8H6oqe/JI3BDnw4tRnkYaGwJsyWU1PCuO
TWPMagMkntv0JaEOHLg4/JZyVsDdiTnmb/U8cEH2RrcUP8iwjykDpb/V4tb4VtgM
7+9HKxQRQhQ5Qji8/QyMG6ctoD+B7k6UpzXvi5FpvpqQWwXJNC52suAt0QeeZj1J
rpudLU=
-----END CERTIFICATE REQUEST-----
[root@cmx newcert]#
```

Paso 4. Cree la cadena de certificados para importar a CMX.

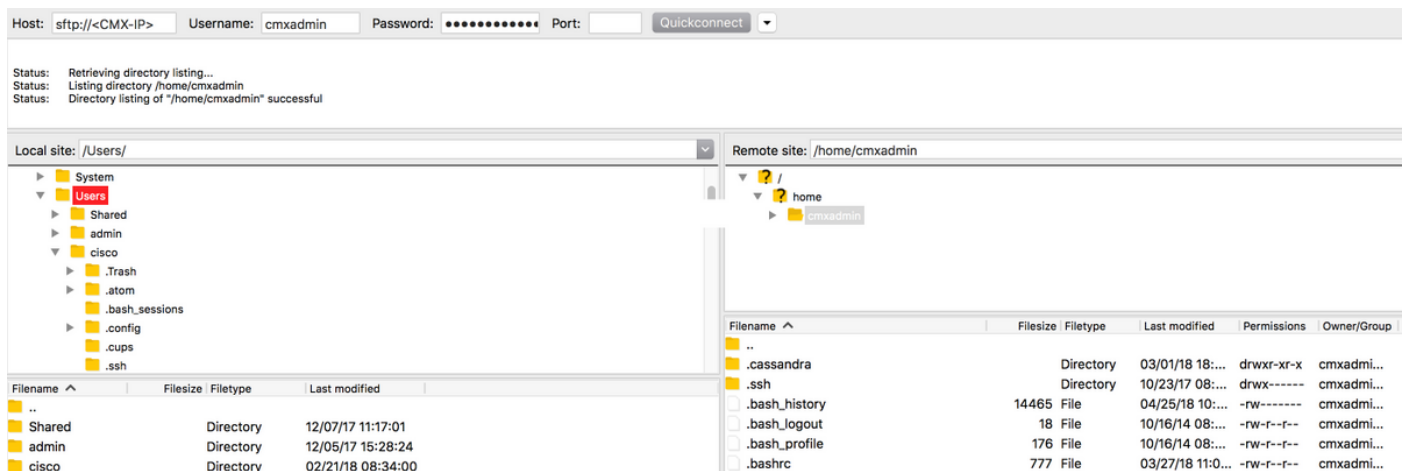
Para crear el certificado final, copie y pegue el certificado firmado en un archivo .txt con la clave privada, el certificado intermedio y el certificado raíz. Asegúrese de guardarlo como un archivo .pem.

Este ejemplo muestra el formato del certificado final.

```
-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEAA2gXgEo7ouyBfWwCkctYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed certificate
MIIFEzCCAavugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCMVMx
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----
```

Paso 5. Transferir el certificado final a CMX.

Para transferir el certificado final a CMX desde su equipo, abra la aplicación SFTP y conéctese a CMX con las credenciales de administrador. Debe poder ver las carpetas de CMX como se muestra en la imagen.



A continuación, arrastre y suelte el certificado encadenado a la carpeta /home/cmxadmin/.

Nota: El directorio predeterminado cuando se abre una conexión SFTP a CMX es /home/cmxadmin/.

Paso 6. Cambie el permiso del certificado final y del propietario. A continuación, muévalo a la carpeta que contiene la clave privada. Aquí está un ejemplo.

```
[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]#
```

Paso 7. Asegúrese de que todo está construido correctamente.

```
[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
```

Debe recibir un mensaje OK.

Paso 8. Instale el certificado final y reinicie CMX.

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

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

Paso 9 (opcional). Si ejecuta CMX 10.3.1 o superior, puede verse afectado por este error:

- [CSCvh21464](#) : CMX WEBUI no utiliza el certificado autofirmado instalado o de terceros


Este error evita que CMX actualice la trayectoria del certificado. La solución temporal para resolver este problema es crear dos links de software para apuntar al nuevo certificado y la clave privada, y recargar CMX. Aquí tiene un ejemplo:

```
[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
```

Verificación

Abra la GUI de CMX, en este caso se utiliza Google Chrome. Abra el certificado haciendo clic en la pestaña **Secure** que se encuentra junto a la URL y revise los detalles como se muestra en la imagen.

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