

# Gerar um CSR para certificado e instalação de terceiros no CMX

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificar](#)

## Introduction

Este documento descreve como gerar uma Solicitação de Assinatura de Certificado (CSR - Certificate Signing Request) para obter um certificado de terceiros e como fazer o download de um certificado em cadeia para o Cisco Connected Mobile Experiences (CMX).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Linux
- Public Key Infrastructure (PKI)
- Certificados digitais

## Componentes Utilizados

As informações neste documento são baseadas na versão 10.3 do 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

### Gerar o CSR

Etapa 1. Conecte-se ao CLI do CMX, acesse como raiz, mova-se para o diretório do certificado e crie uma pasta para o CSR e o arquivo-chave.

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

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

**Note:** O diretório padrão para certificados no CMX é /opt/haproxy/ssl/.

## Etapa 2. Gere o CSR e o arquivo-chave.

```
[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
```

## Etapa 3. Obtenha o CSR assinado por terceiros.

Para obter o certificado do CMX e enviá-lo para terceiros, execute o comando **cat** para abrir o CSR. Você pode copiar e colar a saída em um arquivo .txt ou alterar a extensão com base nos requisitos de terceiros. Exemplo:

```
[root@cmx newcert]# cat cert.crt
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwYsxCzAJBgNVBAYTAk1YMREwDwYDVQQIDAhUbgGF4Y2FsYTER
MA8GA1UEBwwIVGxheGNhbGExdDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQQLDANUQUMx
GDAWBgNVBAMMD2NteC5leGftcGx1LmNvbTEeMBwGCsqGSIB3DQEJARYPY214QGV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA2YybDkDR
vRSwD19EVaJehsnjG9Cyo3vQPOPcAAdgjFBpUHMT8QNgn6YFdHYZdpKaRTJXhztm
fa/7Nevb1IP/pSBgYRxHXQEh19Gj4DT0gT2T+AZ8j3J9KMSe8Bakj4qY8Ua7GCdC
A62NzVcDxDm83gUD92oGbxOF9VFE2hiRvCQc+d6gBRuTOXxyLBAtcL3hkiOEQx7
sDA55CwZU7ysMdWHUBn4AglzIlgPyzlmT3dwr0gfOSYN4j5+H0nrYtrPBZSUBZaa
8pGXVu7sFtV8bahgtNyiCUtiz9J+k5V9DBjqPszYzb3+KxeAA+g0iV3J1VzsLNT7
mVocT9oPaOEI8wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAI6Q/A4zTfrWP2uS
xtN8X6p6aP8guU0bTWhGEMBEgBQd0bBWYdhxaItGt1altDncIGLACeMPuk7WpsiH
rUs5kiIj1Ac2/ANBao6/nlv56vhGUx0d0q0fk/g1brKL+a8Lx9ixtee77aPZ1xVD
A/n3FdNdSiidWH0M4q8JunxbT33vM9h8H6oqe/JI3BDnw4tRnkYaGWJsyWU1PCuO
TWPMagMkntv0JaEOHLg4/JZyVsDdiTnmb/U8cEH2RrcUP8iwjykDpb/V4tb4VtgM
7+9HKxQRQhQ5Qjji8/QyMG6ctoD+B7k6UpzXvi5FpvpqQWwXJNC52suAt0QeeZj1J
rpudLU=
-----END CERTIFICATE REQUEST-----
[root@cmx newcert]#
```

## Etapa 4. Crie a cadeia de certificados para importação no CMX.

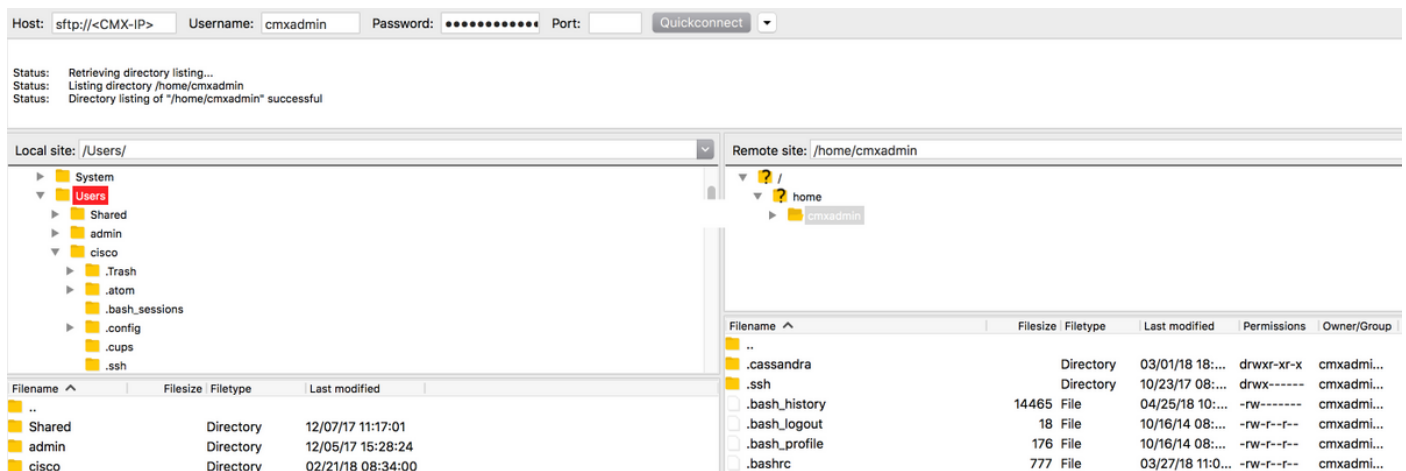
Para criar o certificado final, copie e cole o certificado assinado em um arquivo .txt com a chave privada, o certificado intermediário e o certificado raiz. Certifique-se de guardá-lo como um ficheiro .pem.

Este exemplo mostra o formato do certificado final.

```
-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEAA2gXgEo7ouyBfWwCkctYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed certificate
MIIFEzCCAavugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCVVMx
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----
```

Etapa 5. Transfira o certificado final para CMX.

Para transferir o certificado final para o CMX do computador, abra o aplicativo SFTP e conecte-se ao CMX com as credenciais de administrador. Você deve ser capaz de exibir as pastas do CMX como mostrado na imagem.



Em seguida, arraste e solte o certificado em cadeia para a pasta /home/cmxadmin/.

**Note:** O diretório padrão quando você abre uma conexão SFTP para CMX é /home/cmxadmin/.

Etapa 6. Alterar a permissão do certificado final e do proprietário. Em seguida, mova-o para a pasta que contém a chave privada. Exemplo:

```
[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]#
```

**Passo 7. Certifique-se de que tudo esteja bem construído.**

```
[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
```

**Você deve receber uma mensagem OK.**

**Etapa 8. Instale o certificado final e reinicialize o CMX.**

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

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

**Etapa 9 (Opcional). Se você executar o CMX 10.3.1 ou superior, poderá ser afetado por este bug:**

- [CSCVh21464](#) : O CMX WEBUI não usa o certificado de terceiros ou autoassinado instalado


Este bug impede que o CMX atualize o caminho do certificado. A solução alternativa para resolver esse problema é criar dois soft-links para apontar para o novo certificado e chave privada e recarregar o CMX. Aqui está um exemplo:

```
[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
```

## Verificar

Abra a GUI do CMX; nesse caso, o Google Chrome é usado. Abra o certificado clicando na guia **Secure** próxima ao URL e revise os detalhes como mostrado na imagem.

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