

Generare un CSR per il certificato di terze parti e l'installazione su CMX

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come generare una richiesta di firma di certificato (CSR) per ottenere un certificato di terze parti e come scaricare un certificato concatenato in Cisco Connected Mobile Experience (CMX).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Linux
- PKI (Public Key Infrastructure)
- Certificati digitali

Componenti usati

Le informazioni fornite in questo documento si basano sulla versione 10.3 di CMX

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Genera CSR

Passaggio 1. Connettersi alla CLI di CMX, accedere come root, spostarsi nella directory dei certificati e creare una cartella per il CSR e il file di chiave.

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

Nota: La directory predefinita per i certificati in CMX è /opt/haproxy/ssl/.

Passaggio 2. Generare il file CSR e la chiave.

```
[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
```

Passaggio 3. Firmare il CSR da terze parti.

Per ottenere il certificato da CMX e inviarlo a terze parti, eseguire il comando **cat** per aprire il CSR. È possibile copiare e incollare l'output in un file txt o modificare l'estensione in base ai requisiti di terze parti. Ecco un esempio.

```
[root@cmx newcert]# cat cert.crt
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwYsxCzAJBgNVBAYTAk1YMREwDwYDVQQIDAhUbgGF4Y2FsYTER
MA8GA1UEBwwIVGxheGNhbGExdJAMBgNVBAoMBUNpc2NmMQwwCgYDVQQQLDANUQUxMx
GDAWBgNVBAMMD2NteC5leGFtcGxlLmNvbTEeMBWGCsGSIb3DQEJARYPY214QGV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE2YybDkDR
vRSwD19EVaJehsnjG9Cyo3vQPOPcAAAdjfFBpUHMT8QNgn6YFdHYZdpKaRTJXhztm
fa/7Nevb1IP/pSBgYRxxHXQEH19Gj4DT0gT2T+AZ8j3J9KMSe8Bakj4qY8Ua7GcdC
A62NzVcDxDm83gUD92oGbxOF9VFE2hiRvcQc+d6gBRuTOXxyLBAtcL3hkiOEQx7
sDA55CwZU7ysMdWHUBn4AglzIlgPyzlmT3dwr0gfOSYN4j5+H0nrYtrPBZSUBZaa
8pGXVu7sFtV8bahgtnYiCUTiz9J+k5V9DBjqPszYzb3+KxeAA+g0iV3J1VzsLnt7
mVocT9oPaOEI8wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAI6Q/A4zTfrWP2uS
xtN8X6p6aP8guU0bTWhGEMBEgBQd0bBWYdhxaItGt1a1tdNcIGLACeMPuk7WpsiH
rUs5kiIj1Ac2/ANBao6/nlv56vhGUx0d0q0fk/g1brKL+a8Lx9ixtee77aPZ1xVD
A/n3FdNdSiidWH0M4q8JunxbT33vM9h8H6oqe/JI3BDnw4tRnkYaGWJsyWU1PCuO
TWPMagMkntv0JaEOHLg4/JZyVsDdiTnmb/U8cEH2RrcUP8iwjykDpb/V4tb4VtgM
7+9HKxQRQhQ5Qjji8/QyMG6ctoD+B7k6UpzXvi5FpvpqGQWwXJNC52suAt0QeeZj1J
rpudLUs=
-----END CERTIFICATE REQUEST-----
[root@cmx newcert]#
```

Passaggio 4. Creare la catena di certificati per l'importazione in CMX.

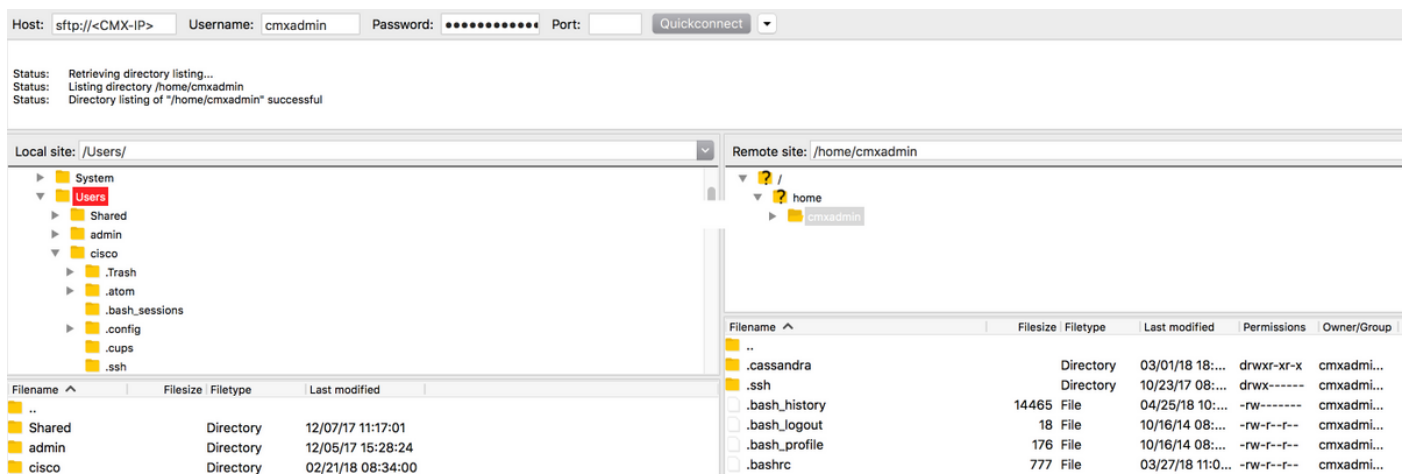
Per creare il certificato finale, copiare e incollare il certificato firmato in un file txt con la chiave privata, il certificato intermedio e il certificato radice. Assicurarsi di salvarlo come file **.pem**.

In questo esempio viene illustrato il formato del certificato finale.

```
-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEA2gXgEo7ouyBfWwCkctcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed certificate
MIIFEzCCAvugAwIBAgIBFzANBqkqhkiG9w0BAQsFADCB1DELMAkGA1UEBhMVCVVMx
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----
```

Passaggio 5. Trasferire il certificato finale in CMX.

Per trasferire il certificato finale in CMX dal computer, aprire l'applicazione SFTP e connettersi a CMX con le credenziali di amministratore. È necessario essere in grado di visualizzare le cartelle di CMX come illustrato nell'immagine.



Trascinare quindi il certificato concatenato nella cartella `/home/cmxadmin/`.

Nota: La directory predefinita quando si apre una connessione SFTP a CMX è `/home/cmxadmin/`.

Passaggio 6. Modificare l'autorizzazione del certificato finale e del proprietario. Quindi spostarlo nella cartella che contiene la chiave privata. Ecco un esempio.

```
[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]#
```

Passaggio 7. Verificare che tutto sia stato creato correttamente.

```
[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
```

Deve ricevere un messaggio OK.

Passaggio 8. Installare il certificato finale e riavviare CMX.

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

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

Passaggio 9 (facoltativo). Se si esegue CMX 10.3.1 o versione successiva, il bug potrebbe interessare:


- [CSCvh21464](#) : CMX WEBUI non utilizza il certificato autofirmato o di terze parti installato. Questo bug impedisce a CMX di aggiornare il percorso del certificato. Per risolvere il problema, creare due collegamenti soft che puntino al nuovo certificato e alla nuova chiave privata e ricaricare CMX. Di seguito è riportato un esempio:

```
[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
```

Verifica

Aprire la GUI di CMX, in questo caso viene utilizzato Google Chrome. Aprire il certificato facendo clic sulla scheda **Secure** (Protetto) accanto all'URL e rivedere i dettagli come mostrato nell'immagine.

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