Come generare un certificato Web autofirmato per vManage

Sommario

Introduzione

In questo documento viene descritto come generare e installare un certificato Web autofirmato quando quello esistente è scaduto in un vManage locale. Cisco non firma i certificati Web per queste distribuzioni. I clienti devono firmarli con la propria CA (Certification Authority) o con una CA di terze parti.

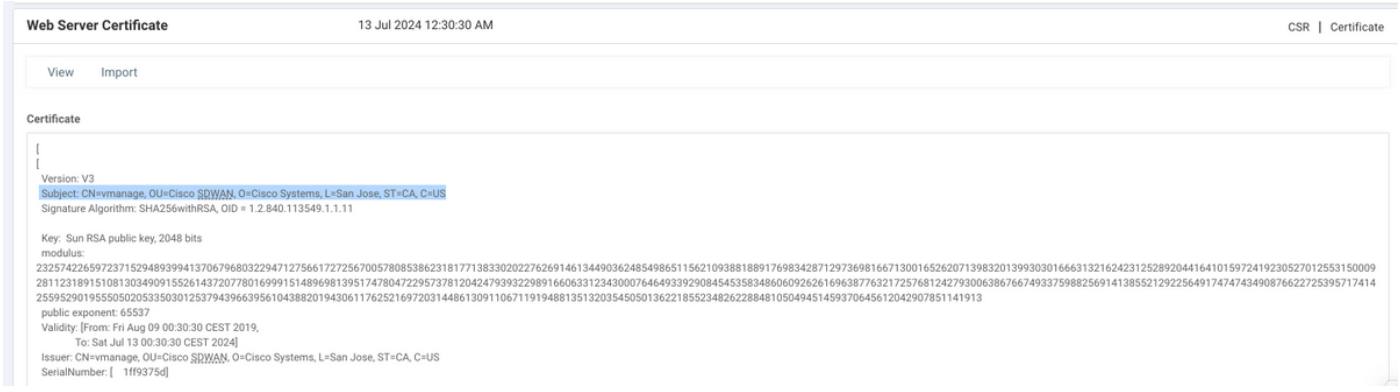
Problema

Il certificato Web vManage sta per scadere o è già scaduto. L'accesso all'interfaccia grafica dell'utente (GUI) può essere interrotto o è possibile visualizzare un avviso permanente sulla scadenza del certificato.

Soluzione

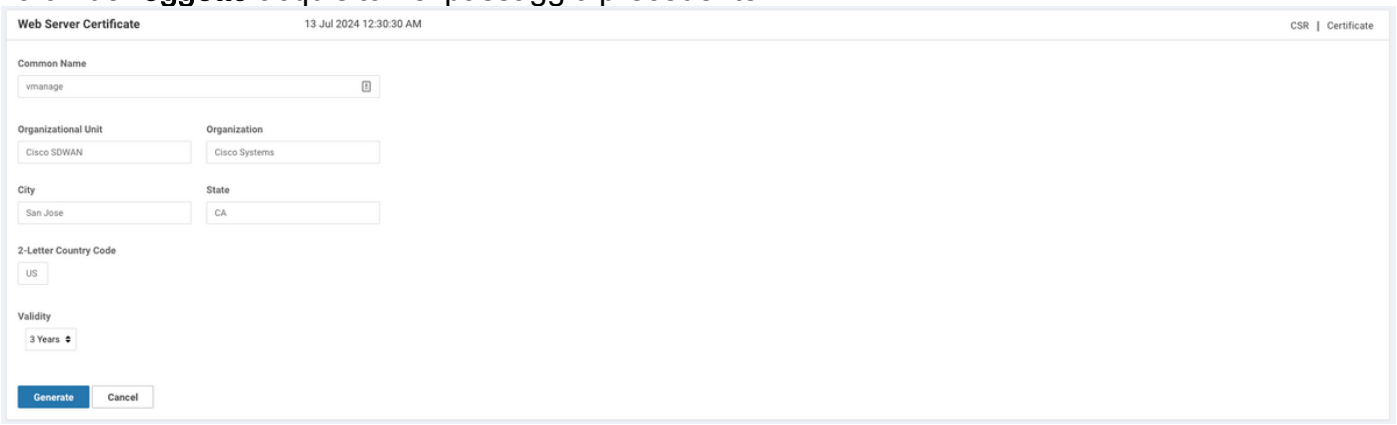
Se non si è preoccupati per l'aspetto della sicurezza dell'utilizzo dei certificati autofirmati e si desidera semplicemente evitare messaggi di allarme e possibili problemi di accesso alla GUI di vManage a causa di un certificato scaduto, è possibile utilizzare questa soluzione con un certificato Web autofirmato su un vManage.

1. Nell'interfaccia utente di vManage, selezionare **Administration > Settings > Web Server Certificate > Certificate** (Amministrazione > Impostazioni > Certificato server Web > Certificato) e quindi salvare le informazioni relative all'oggetto del certificato, ad esempio **Subject (Oggetto): CN=vmanage, OU=Cisco SDWAN, O=Cisco Systems, L=San Jose, ST=CA, C=US**.

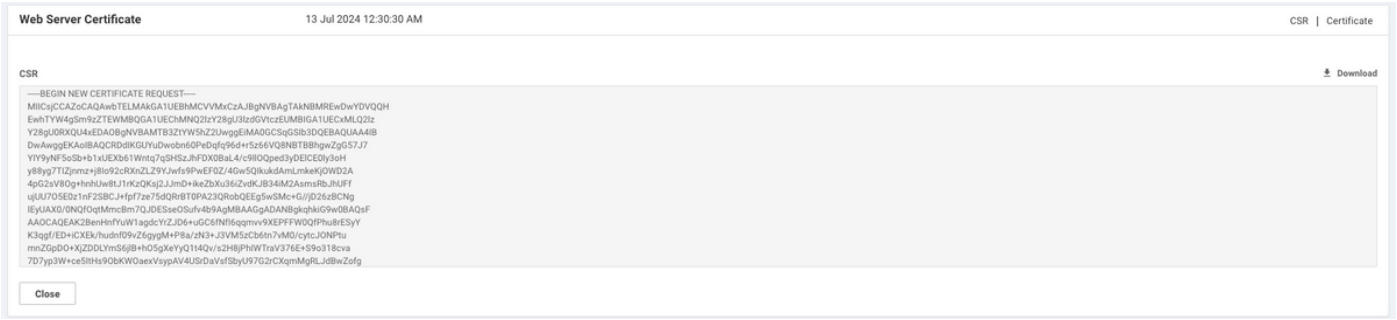


2. Nell'interfaccia utente di vManage, selezionare **Administration > Settings > Web Server**

Certificate > CSR (Amministrazione > Impostazioni > Certificato server Web > CSR) e selezionare **Generate** per generare una nuova richiesta di firma del certificato (CSR). Accertarsi di immettere i valori dell'**oggetto** acquisito nel passaggio precedente.



3. Copiare il CSR appena generato nel buffer di copia e incolla come mostrato nell'immagine.



4. Quindi immettere una **shell** e incollare il contenuto del buffer con CSR nel file su vManage con l'aiuto del comando **echo**.

```
vmanage#
vmanage# vshell
vmanage:~$ mkdir web
vmanage:~$ cd web
vmanage:~/web$ echo "-----BEGIN NEW CERTIFICATE REQUEST-----
> MIICsjCCAZoCAQAwbTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMREwDwYDVQQH
> EwhTYW4gSm9zZTEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczEUMBIGA1UECxMLQ2lz
> Y28gU0RXQU4xEDAOBgNVBAMTB3ZtYW5hZ2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
> DwAwggEKAoIBAQCRDdIKGUYuDwobn60PeDqfq96d+r5z66VQ8NBTBBhgwZgG57J7
> YIY9yNF5oSb+b1xUEXb61Wntq7qSHSzJhFDX0BaL4/c9llOQped3yDElCE0ly3oH
> y88yg7TIZjnmz+j8Io92cRXnZLZ9YJwfs9PwEF0Z/4Gw5QIkukdAmLmkeKjOWD2A
> 4pG2sV8Og+hnhUw8tJ1rKzQKsj2JJmD+ikeZbXu36iZvdKJB34iM2AsmsRbJhUFf
> ujUU7O5E0z1nF2SBCJ+fpf7ze75dQRrBT0PA23QRobQEEg5wSMc+G//jD26zBCNg
> IEyUAX0/0NQfOqtMmcBm7QJDESseOSufv4b9AgMBAAGgADANBgkqhkiG9w0BAQsF
> AAOCAQEAK2BenHnfYuW1agdcYrZJD6+uGC6fNfI6qqmvv9XEPFFW0QfPhu8rESyY
> K3qgf/ED+iCXEk/hudnf09vZ6gygM+P8a/zN3+J3VM5zCb6tn7vM0/cytcJONPtu
> mnZGpDO+XjZDDLYmS6jlB+hO5gXeYyQ1t4Qv/s2H8jPhIWTraV376E+S9o318cva
> 7D7yp3W+ce5ItHs9ObKWOaexVsypAV4USrDaVsfSbyU97G2rCXqmMgRLJdBwZofg
> 04qsgrC8qG28aue1Q88XPa/HQtp0WB/Pxg7oe91s59Je/ETsMkR3vt7aglemyXAJ
> nal67+T/QWgLSJB2pQuPHo51MbA55w==
> -----END NEW CERTIFICATE REQUEST-----" > web_cert.csr
```

5. Verificare che CSR sia stato salvato correttamente con l'aiuto del comando **cat**.

```
vmanage:~/web$ cat web_cert.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICsjCCAZoCAQAwbTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMREwDwYDVQQH
EwhTYW4gSm9zZTEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczEUMBIGA1UECxMLQ2lz
```

```
Y28gU0RXQU4xEDAOBgNVBAMTB3ZtYW5hZ2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCRDdIKGUYuDwobn60PeDqfq96d+r5z66VQ8NBTBBhgwZgG57J7
YIY9yNF5oSb+b1xUEXb61Wntq7qSHSzJhFDX0BaL4/c9llOQped3yDElCE0ly3oH
y88yg7TIZjnmz+j8Io92cRXnZLZ9YJwfs9PwEF0Z/4Gw5QIkukdAmLmkeKjOWD2A
4pG2sV8Og+hnhUw8tJ1rKzQKsj2JJmD+ikeZbXu36iZvdKJB34iM2AsmsRbJhUFf
ujUU7O5E0z1nF2SBCJ+fpf7ze75dQRrBT0PA23QRobQEEg5wSMc+G//jD26zBCNg
IEyUAX0/0NQfOqtMmcBm7QJDESseOSufv4b9AgMBAAGgADANBgkqhkiG9w0BAQsF
AAOCAQEAK2BenHnfYuW1agdcYrZJD6+uGC6fNfI6qqmvv9XEPFFW0QfPhu8rESyY
K3qgf/ED+iCXEk/hudnf09vZ6gygM+P8a/zN3+J3VM5zCb6tn7vM0/cytcJONPtu
mnZGpDO+XjZDDLYmS6jlB+hO5gXeYyQ1t4Qv/s2H8jPhIWTraV376E+S9o318cva
7D7yp3W+ce5ItHs9ObKWOaexVsypAV4USrDaVsfSbyU97G2rCXqmMgRLJdBwZofg
04qsgrC8qG28aue1Q88XPa/HQtp0WB/Pxg7oe91s59Je/ETsMkR3vt7aglemyXAJ
nal67+T/QWgLSJB2pQuPHo51MbA55w==
-----END NEW CERTIFICATE REQUEST-----

vmanage:~/web$
```

6. Con l'aiuto di **openssl**, generare una chiave per il certificato radice denominata **rootca.key**.

```
vmanage:~/web$ openssl genrsa -out rootca.key 2048
Generating RSA private key, 2048 bit long modulus
..
..........
e is 65537 (0x10001)
vmanage:~/web$ ls
rootca.key  web_cert.csr
vmanage:~/web$
```

7. Generare il certificato CA radice denominato **rootca.pem** e firmarlo con **rootca.key** generato nel passaggio precedente.

```
vmanage:~/web$ openssl req -x509 -new -nodes -key rootca.key -sha256 -days 4000 -out rootca.pem
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) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:Cisco SDWAN
Common Name (e.g. server FQDN or YOUR name) []:vmanage
Email Address []:
vmanage:~/web$ ls
rootca.key  rootca.pemweb_cert.csr
vmanage:~/web$
```

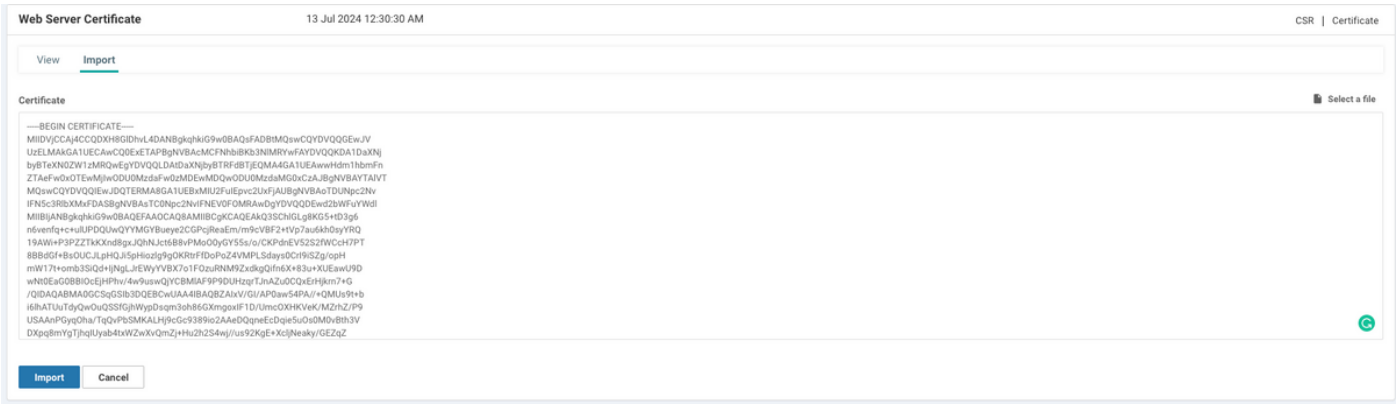
8. Firmare il CSR con il certificato e la chiave CA radice.

```
vmanage:~/web$ openssl x509 -req -in web_cert.csr -CA rootca.pem -CAkey rootca.key -
CAcreateserial -out web_cert.crt -days 4000 -sha256
Signature ok
subject=/C=US/ST=CA/L=San Jose/O=Cisco Systems/OU=Cisco SDWAN/CN=vmanage
Getting CA Private Key
vmanage:~/web$ ls
rootca.key  rootca.pemrootca.srl  web_cert.crt  web_cert.csr
vmanage:~/web$
```

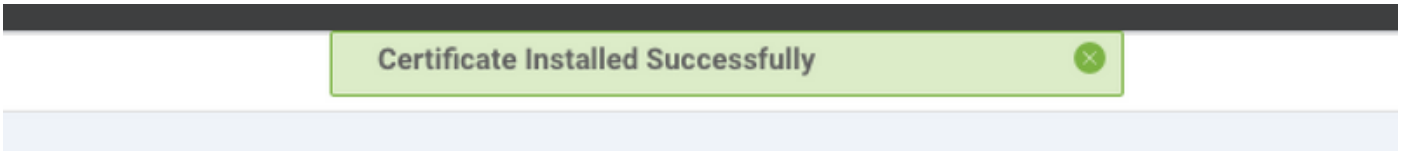
9. Copiare un nuovo certificato firmato nel buffer di copia e incolla. È possibile utilizzare **cat** per visualizzare il certificato firmato.

```
vmanage:~/web$ cat web_cert.crt
-----BEGIN CERTIFICATE-----
MIIDVjCCAj4CCQDXH8GlDhvL4DANBgkqhkiG9w0BAQsFADBtMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCFNhbiBKb3NlMRYwFAYDVQQKDA1DaXNj
byBTeXN0ZW1zMRQwEgYDVQQLDAtDaXNjbyBTRFdBTjEQMA4GA1UEAwwHdm1hbmFn
ZTAeFw0xOTEwMjIwODU0MzdaFw0zMDEwMDQwODU0MzdaMG0xCzAJBgNVBAYTAlVT
MQswCQYDVQQIEwJDQTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2Nv
IFN5c3RlbXMxFDASBgNVBAsTC0Npc2NvIFNEV0FOMRAwDgYDVQQDEwd2bWFuYWdl
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkQ3SChlGLg8KG5+tD3g6
n6venfq+c+ulUPDQUwQYYMGYBueye2CGPcjReaEm/m9cVBF2+tVp7au6kh0syYRQ
19AWi+P3PZZTkKXnd8gxJQhNJct6B8vPMoO0yGY55s/o/CKPdnEV52S2fWCcH7PT
8BBdGf+BsOUCJLpHQJi5pHiozlg9gOKRtrFfDoPoZ4VMPLSdays0CrI9iSZg/opH
mW17t+omb3SiQd+IjNgLJrEWyYVBX7o1FOzuRNM9ZxdkgQifn6X+83u+XUEawU9D
wNt0EaG0BBIOcEjHPhv/4w9uswQjYCBMlAF9P9DUHzqrTJnAZu0CQxErHjkrn7+G
/QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBZAIxV/GI/AP0aw54PA//+QMUs9t+b
i6lhATUuTdyQwOuQSSfGjhWypDsqm3oh86GXmgoxIF1D/UmcOXHKVeK/MZrhZ/P9
USAAnPGyqOha/TqQvPbSMKALHj9cGc9389io2AAeDQqneEcDqie5uOs0M0vBth3V
DXpq8mYgTjhqIUyab4txWZwXvQmZj+Hu2h2S4wj//us92KgE+XcljNeaky/GEZqZ
jWNoWDgWeJdsm8hx2QteHHbDTahuArVJf1p45eLIcJR1k0lRL8TTroWaST1bZCJz
20aYK4S0K0nTkpscuVIrXHkwNN6Ka4q9/rVxnLzAflJ4E9DXojpD3qNH
-----END CERTIFICATE-----
```

10. Importare il certificato in vManage. A tale scopo, selezionare **Amministrazione > Impostazioni > Certificato server Web > Importa** e incollare il contenuto del buffer di copia e incolla come mostrato nell'immagine.



11. Se tutte le operazioni sono state eseguite correttamente, vManage visualizza "**Certificato installato correttamente**" come mostrato nell'immagine.



12. Infine, controllare il risultato e verificare che la data di validità del certificato sia stata aggiornata correttamente come mostrato nell'immagine.

Informazioni correlate

- Genera certificato server Web
- Uomo OpenSSL

- Documentazione e supporto tecnico – Cisco Systems