Cómo generar un certificado web firmado automáticamente para vManage

Contenido

Introducción

Este documento describe cómo generar e instalar un certificado web autofirmado cuando el existente caduca en un vManage in situ. Cisco no firma certificados web para tales implementaciones, los clientes deben firmarlos por su propia autoridad certificadora (CA) o por alguna entidad emisora de certificados de terceros.

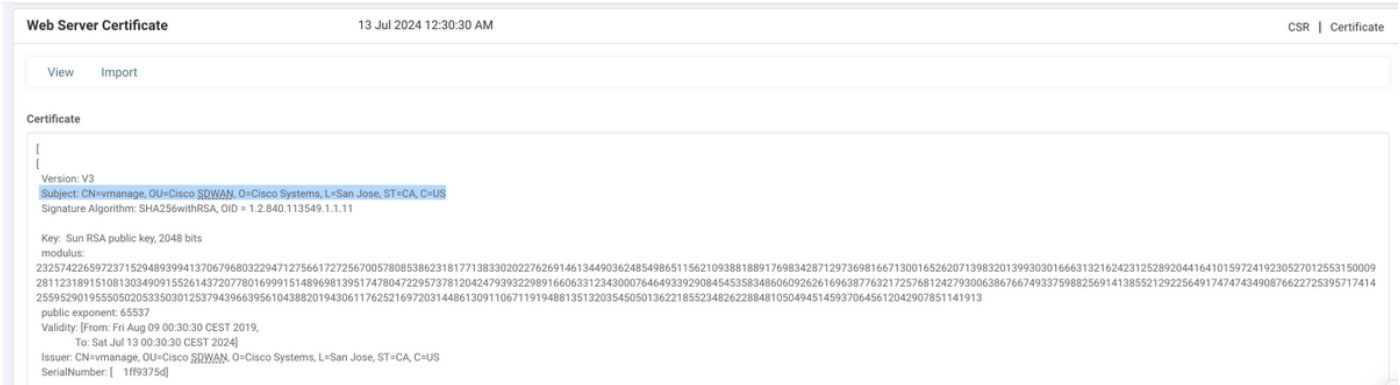
Problema

El certificado web de vManage caducará o ya lo ha hecho. El acceso a la interfaz gráfica de usuario (GUI) puede perderse o puede ver una alarma permanente en la interfaz gráfica de usuario sobre el certificado caducado.

Solución

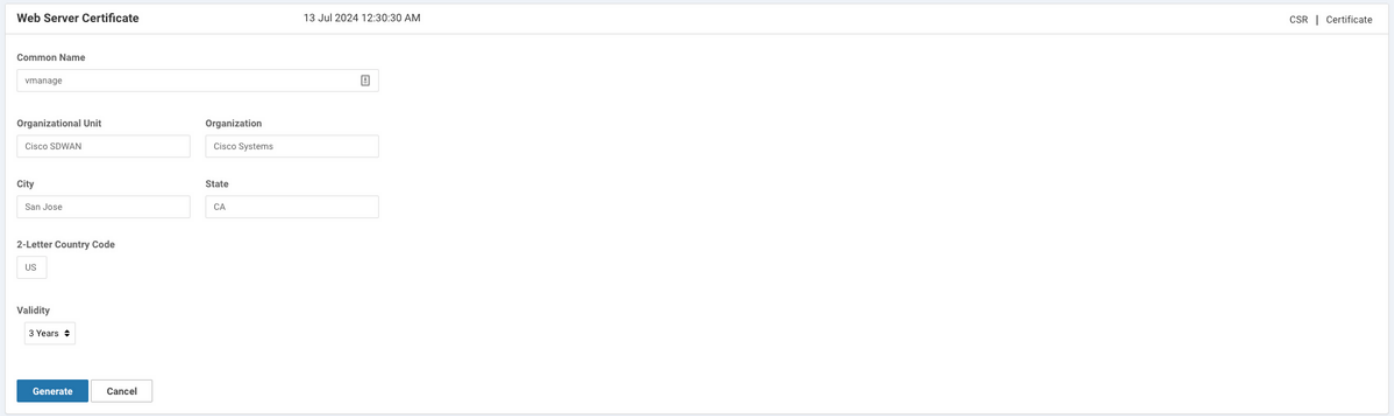
Si no le preocupa el aspecto de seguridad del uso de certificados autofirmados y solo desea evitar el mensaje de alarma y los posibles problemas con el acceso a la GUI de vManage debido a un certificado caducado, puede utilizar esta solución con un certificado web autofirmado en un vManage.

1. En la GUI de vManage, navegue hasta **Administration > Settings > Web Server Certificate > Certificate** y luego guarde esta información en algún lugar sobre el asunto del certificado, por ejemplo, **Subject: CN=vmanage, OU=Cisco SDWAN, O=Cisco Systems, L=San José, ST=CA, C=US**.

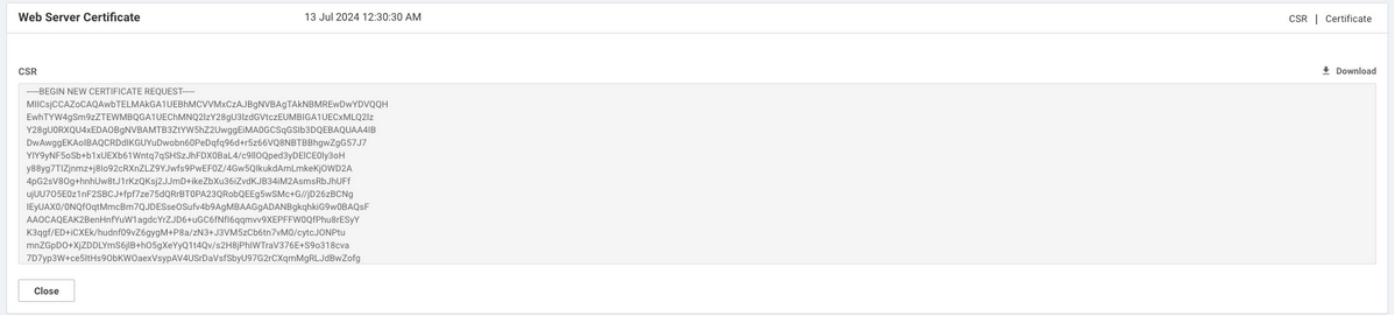


2. En la GUI de vManage, navegue hasta **Administration > Settings > Web Server Certificate >**

CSR y seleccione **Generate** para generar una nueva solicitud de firma de certificado (CSR). Asegúrese de introducir los valores del **Asunto** capturados en el paso anterior.



3. Copie la CSR recién generada al búfer de copia y pegado como se muestra en la imagen.



4. Y luego ingrese un **vshell** y pegue el contenido del búfer con CSR en el archivo en el vManage con la ayuda 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. Asegúrese de que la CSR se guarda correctamente con la ayuda 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 la ayuda de **openssl**, genere una clave para el certificado raíz denominado **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. Genere el certificado de CA raíz denominado **rootca.pem** y firme con **rootca.key** que se generó en el paso anterior.

```
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. Firme su CSR con el certificado y la clave de la CA raíz.

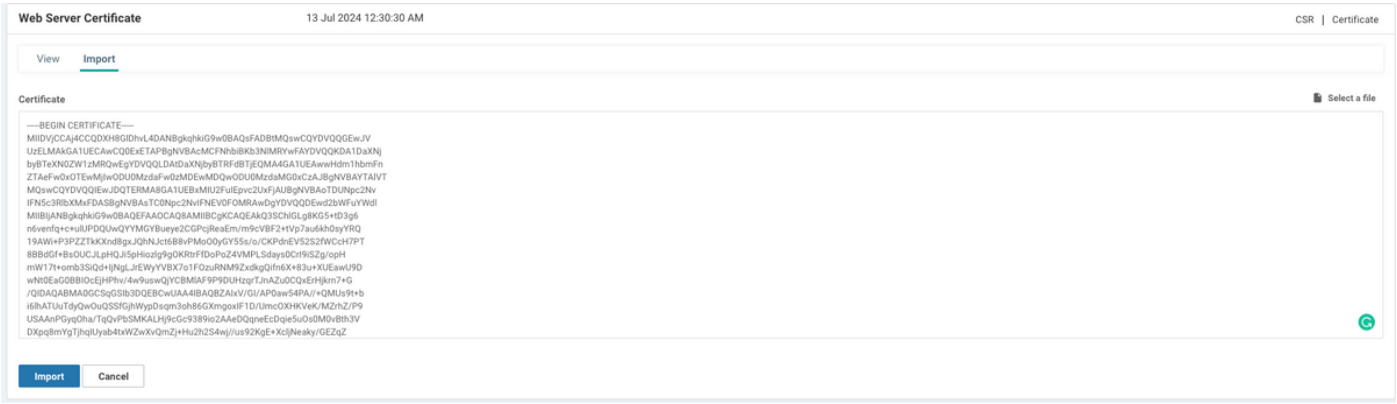
```
vmanage:~/web$ openssl x509 -req -in web_cert.csr -CA rootca.pem -CAkey rootca.key -
CAcreateserial -out web_cert.crt -days 4000 -sha256
Signature ok
subject=/C=US/ST=CA/L=San Jose/O=Cisco Systems/OU=Cisco SDWAN/CN=vmanage
Getting CA Private Key
vmanage:~/web$ ls
rootca.key  rootca.pemrootca.srl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

9. Copie un nuevo certificado firmado en el búfer de copia y pegado. Puede utilizar **cat** para ver el certificado firmado.

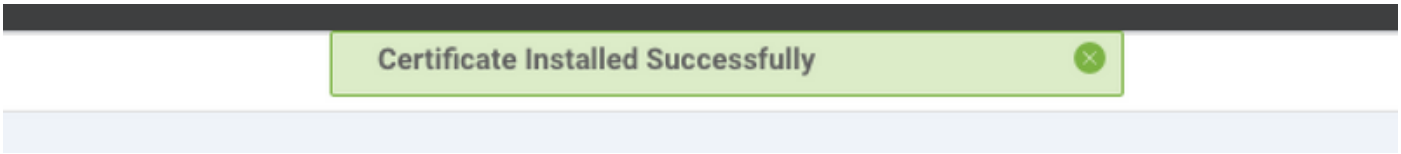
```
vmanage:~/web$ cat web_cert.crt
```

```
-----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. Importe el certificado en vManage. Para hacerlo, navegue hasta **Administration > Settings > Web Server Certificate > Import** y pegue el contenido de su búfer de copiar y pegar como se muestra en la imagen.



11. Si hizo todo bien, vManage muestra "**Certificado instalado correctamente**" como se muestra en la imagen.



12. Por último, verifique el resultado y asegúrese de que la fecha de validez del certificado se haya actualizado correctamente como se muestra en la imagen.

Información Relacionada

- Generar certificado de servidor web
- Hombre de OpenSSL
- Soporte Técnico y Documentación - Cisco Systems