

Hoe genereert u een zelf-ondertekend webcertificaat voor vManager

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een zichzelf ondertekend webcertificaat kunt genereren en installeren wanneer de bestaande certificering op een reeds aanwezige vManager is verlopen. Cisco ondertekent geen webcertificaten voor dergelijke implementaties, klanten moeten dit ondertekenen door een eigen certificeringsinstantie (CA) of een derde partij: CA.

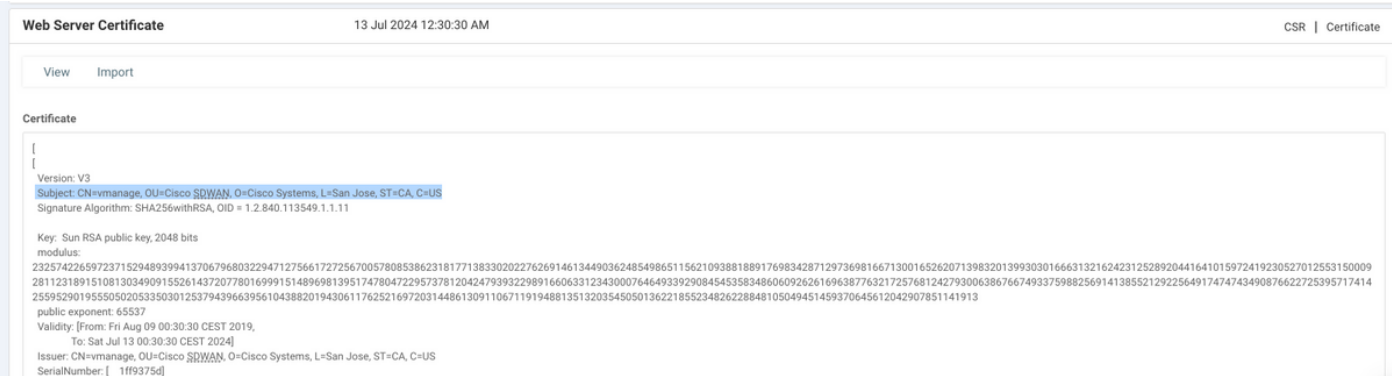
Probleem

vManager-webcertificaat vervalt of is al verlopen. De toegang tot de grafische gebruikersinterface (GUI) kan worden verloren of u kunt permanent alarm in GUI zien over certificaat verlopen.

Oplossing

Als u zich geen zorgen maakt over het veiligheidsaspect van zelfgetekend certificaatgebruik en u alleen alarmbericht en mogelijke problemen met vManager GUI-toegang wilt voorkomen vanwege verlopen certificaat, dan kunt u deze oplossing met zelf-ondertekend webcertificaat op vManager gebruiken.

1. In de vManager GUI, navigeer naar **Administratie > Instellingen > Webservercertificaat > Certificaat** en bewaar deze informatie vervolgens ergens over certificatenonderwerp, bijvoorbeeld **Onderwerp: CN=VC, OU=Cisco SDWAN, O=Cisco Systems, L=San Jose, ST=CA, C=US**.



The screenshot shows the 'Web Server Certificate' page in the vManager GUI. The page title is 'Web Server Certificate' and the timestamp is '13 Jul 2024 12:30:30 AM'. There are 'View' and 'Import' buttons. The 'Certificate' section displays the following details:

```
[
  {
    Version: V3
    Subject: CN=vmanage, OU=Cisco SDWAN, O=Cisco Systems, L=San Jose, ST=CA, C=US
    Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

    Key: Sun RSA public key, 2048 bits
    modulus:
    232574226597237152948939941370679680322947127566172725670057808538623181771383302022762691461344903624854986511562109388188917698342871297369816671300165262071398320139930301666313216242312528920441641015972419230527012553150009
    2811231891510813034909155261437207780169991514896981395174780472295737812042479393229891660633123430007646493392908454358348606926261696387763217257681242793006386766749337598825691413855212922564917474743490876622725395717414
    25595290195550502053350301253794396639561043882019430611762521697203144861309110671191948813513203545050136221855234826228848105049451459370645612042907851141913

    public exponent: 65537
    Validity: [From: Fri Aug 09 00:30:30 CEST 2019,
    To: Sat Jul 13 00:30:30 CEST 2024]
    Issuer: CN=vmanage, OU=Cisco SDWAN, O=Cisco Systems, L=San Jose, ST=CA, C=US
    SerialNumber: [ 1f9375d]
```

2. In de vManager GUI, navigeer naar **Administratie > Instellingen > Webservercertificaat > CSR** en selecteer **Generate** om een nieuw certificaatsignaalverzoek (CSR) te genereren. Zorg ervoor dat u de waarden van het **Onderwerp** invoert dat u op de vorige stap hebt opgenomen.

Web Server Certificate 13 Jul 2024 12:30:30 AM CSR | Certificate

Common Name
vmanage

Organizational Unit: Cisco SDWAN Organization: Cisco Systems

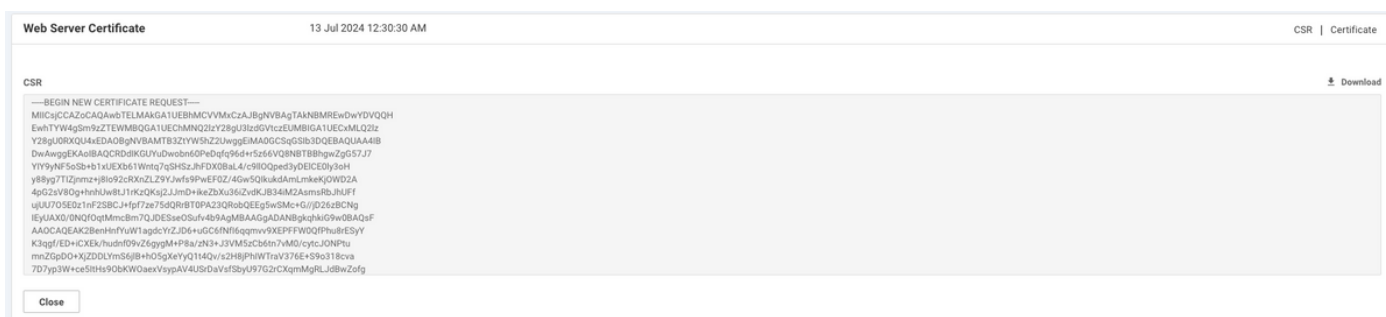
City: San Jose State: CA

2-Letter Country Code: US

Validity: 3 Years

Generate Cancel

3. Kopieer de nieuw gegenereerde CSR naar de kopie-goedbuffer, zoals in de afbeelding weergegeven.



4. En voer dan een **vshell** en plakbufferinhoud met CSR in het bestand op vManager met hulp van **echo** opdracht in.

```

vmanage#
vmanage# vshell
vmanage:~$ mkdir web
vmanage:~$ cd web
vmanage:~/web$ echo "-----BEGIN NEW CERTIFICATE REQUEST-----
> MIICs jCCAzoCAQAwbTElMAkGAlUEBhMCVVMxCzAJBgNVBAGTAkNBMRwDwYDVQOH
> EwhTYW4gSm9zZTEwMBQGA1UEChMNQ2l1Z28gU3l1ZG9VtCzEUMBIGAlUECMLQ2l1
> Y28gU0RXQU4xEDA0BgNVBAMTB3ZtYW5hZ2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
> DwAwggEKAoIBAQCRRdIKGUYuDwobn60PeDqf96d+r5z66VQ8NBTBBhgWZgG57J7
> YIY9yNF5oSb+blxUEXb61Wntq7qSHSszJhFDX0BaL4/c911OQped3yDElCE01y3oH
> y88yg7TIZjnmz+j8Io92cRXnZLZ9YJwfs9PwEF0Z/4Gw5QIkukdAmLmkeKjOWD2A
> 4pG2sV80g+hnhUw8tJ1rKzQKsj2JmD+ikeZbxu36iZvdKJB34iM2AsmsRbJhUff
> uJU705E0z1nF2SBCJ+fpf7ze75dQRrBT0PA23QRRobQEeg5wSMc+G//jD26zBCNg
> IEyUAX0/0NQfOqtMmcBm7QJDESseOSufv4b9AgMBAAGgADANBgkqhkiG9w0BAQSF
> AAOCAQEAK2BenHnfYuW1agdcYrZJD6+uGC6fNfI6qqmvv9XEPFFW0QfPhu8rESyY
> K3qgf/ED+iCXEk/hudnf09vZ6gygM+P8a/zN3+J3VM5zCb6tn7vM0/cytcJONPtU
> mnZGpDO+XjZDDLmS6j1B+h05gXeYyQ1t4Qv/s2H8jPhIWtraV376E+S9o318cva
> 7D7yp3W+ce5ItHs90bKWOaexVsyPAV4USrDaVsfSbyU97G2rCXqmMgRLJdBwZofg
> 04qsgRc8qG28aue1Q88XPa/HQtP0WB/Pxg7oe91s59Je/ETsMkR3vt7aglemyXAJ
> nal67+T/QWgLSJB2pQuPho51mBA55w==
> -----END NEW CERTIFICATE REQUEST-----" > web_cert.csr

```

5. Zorg ervoor dat CSR correct wordt opgeslagen met de hulp van **katteopdracht**.

```

vmanage:~/web$ cat web_cert.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICs jCCAzoCAQAwbTElMAkGAlUEBhMCVVMxCzAJBgNVBAGTAkNBMRwDwYDVQOH
EwhTYW4gSm9zZTEwMBQGA1UEChMNQ2l1Z28gU3l1ZG9VtCzEUMBIGAlUECMLQ2l1
Y28gU0RXQU4xEDA0BgNVBAMTB3ZtYW5hZ2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCRRdIKGUYuDwobn60PeDqf96d+r5z66VQ8NBTBBhgWZgG57J7

```

```
YIY9yNF5oSb+blxUEXb6lWntq7qSHSszJhFDX0BaL4/c91lOQped3yDElCE0ly3oH
y88yg7TIZjnmz+j8Io92cRXnZLZ9YJwfs9PwEF0Z/4Gw5QIkukdAmLmkeKjOWD2A
4pG2sV8Og+hnhUw8tJ1rKzQKsJ2JmD+iKeZbXu36iZvdKJB34iM2AsmsRbJhUff
ujUU705E0z1nF2SBCJ+fpf7ze75dQRrBT0PA23QRobQEEg5wSMc+G//jD26zBCNg
IEYUAX0/0NQfOqtMmcBm7QJDESseOSufv4b9AgMBAAGgADANBgkqhkiG9w0BAQsF
AAOCAQEAK2BenHnfYuWlagdcYrZJD6+uGC6fNfI6qqmvv9XEPFFW0QfPhu8rESyY
K3qgf/ED+iCXEk/hudnf09vZ6gygM+P8a/zN3+J3VM5zCb6tn7vM0/cytcJONPtU
mnZGpDO+XjZDDLYmS6j1B+h05gXeYyQ1t4Qv/s2H8jPhIWtraV376E+S9o318cva
7D7yp3W+ce5ItHs9ObKWOaexVsypAV4USrDaVsfSbyU97G2rCXqmMgRLJdBwZofg
04qsgRc8qG28aue1Q88XPa/HQtp0WB/Pxg7oe91s59Je/ETsMkR3vt7aglemyXAJ
nal67+T/QWgLSJB2pQuPHo51MBA55w==
-----END NEW CERTIFICATE REQUEST-----
```

```
vmanage:~/web$
```

6. Met behulp van **openssl**, genereert u een sleutel voor het wortelcertificaat met de naam **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. Generate Root CA certificaat genaamd **rootca.pem** en teken het met **rootca.key** die gegenereerd werd op de vorige stap.

```
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. Teken uw CSR met CA-certificaat en -toets.

```
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. Kopieer een nieuw ondertekend certificaat naar de kopie-pasta buffer. U kunt **kat** gebruiken om het ondertekende certificaat te kunnen bekijken.

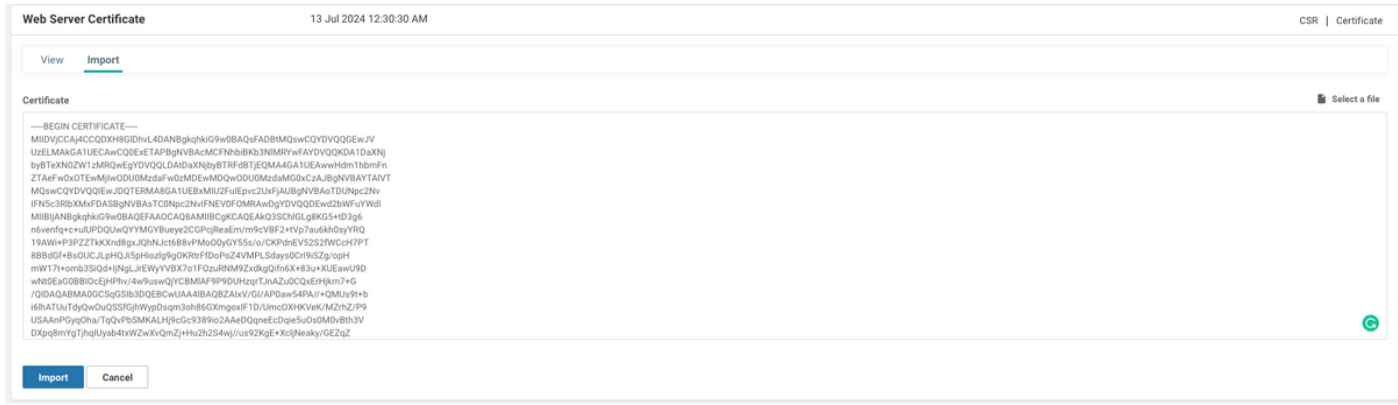
```
vmanage:~/web$ cat web_cert.crt
```

```

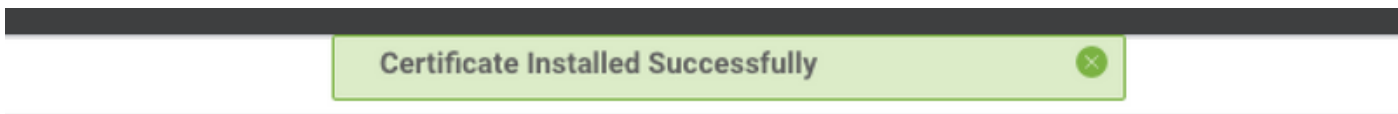
-----BEGIN CERTIFICATE-----
MIIDVjCCAj4CCQDXH8G1DhVl4DANBgkqhkiG9w0BAQsFADBTMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0EwETAPBgNVBACMCFNhb3N1MRyWfAYDVQQKDA1DaXNj
byBTeXN0ZW1zMzRwEgYDVQQLDAtDaXNjbyBTRFRfDBTjEQMA4GA1UEAwwHdm1hbmFn
ZTAeFw0xOTUwMjEwODU0MzdaFw0zMDUwMDQwODU0MzdaMG0xCzAJBgNVBAYTA1VT
MQswCQYDVQQIEwJDTERRMA8GA1UEBxMIU2FuIEpvc2UxZjAUBG9NVBAoTDUNpc2Nv
IFN5c3RlbXNkZDASBgNVBAsTC0Npc2NvIFNEV0FOMRAwDgYDVQQDEwd2bWZuYXdl
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKQ3SCh1GLg8KG5+tD3g6
n6venfq+c+ulUPDQUwQYYMGYBueye2CGPcJReaEm/m9cVBF2+tVp7au6kh0syYRQ
19AWi+P3PZZTtKXnd8gxJQhNjct6B8vPMo0yGY55s/o/CKPdnEV52S2fWCcH7PT
8BBdGf+BsoUCJLpHQJi5pHiozlg9gOKRtrFfDoPoZ4VMPLSdays0CrI9iSzg/opH
mW17t+omb3SiQd+IjNgLJrEwYVVBX7o1FOzuRNM9ZxdkgQifn6X+83u+XUEawU9D
wNt0EaG0BBI0cEjHPhv/4w9uswQjYCBMIAF9P9DUHzqrTJnAZu0CQxerHjkrn7+G
/QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBZAIxV/GI/AP0aw54PA//+QMUs9t+b
i6lhATUuTdyQwOuQSSfGjHwypDs3oh86GXmgoxIF1D/UmcOXHKVek/MZrhZ/P9
USAApGyqOha/TqQvPbSMKALHj9cGc9389io2AAeDQqneEcDqie5uOs0M0vBth3V
DXpq8mYgTjhgIUYab4txWZwXvQmZj+Hu2h2S4wj//us92KgE+XcljNeaky/GEZqZ
jWNNoWdGWeJdsM8x2QteHHBDTahuArVJf1p45eLIcJR1k01RL8TTroWaSt1bZCJZ
20aYK4S0K0nTkpsCuVrXHkwnN6Ka4q9/rVxnLzAflJ4E9DXoJpD3qNH
-----END CERTIFICATE-----

```

10. Importeer het certificaat in de vManager. Om dit te doen, navigeer naar **Beheer > Instellingen > Webservercertificaat > Importeren** en plak de inhoud van uw kopie-pasta buffer zoals in de afbeelding.



11. Als u alles juist hebt gedaan, toont vManager "certificaatgeïnstalleerd" zoals in de afbeelding.



12. Controleer ten slotte het resultaat en zorg ervoor dat de geldigheid van het certificaat goed is bijgewerkt zoals in de afbeelding wordt weergegeven.



Gerelateerde informatie

- [Webservercertificaat genereren](#)
- [OpenSSL-man](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)