

Erstellen eines selbstsignierten Webzertifikats für vManage

Inhalt

[Einführung](#)

[Problem](#)

[Lösung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie ein selbstsigniertes Webzertifikat generieren und installieren, wenn das vorhandene auf einem Vor-Ort-vManage abgelaufen ist. Cisco signiert für solche Bereitstellungen keine Webzertifikate, Kunden müssen diese über eine eigene Zertifizierungsstelle (Certificate Authority, CA) oder eine Zertifizierungsstelle eines Drittanbieters unterzeichnen.

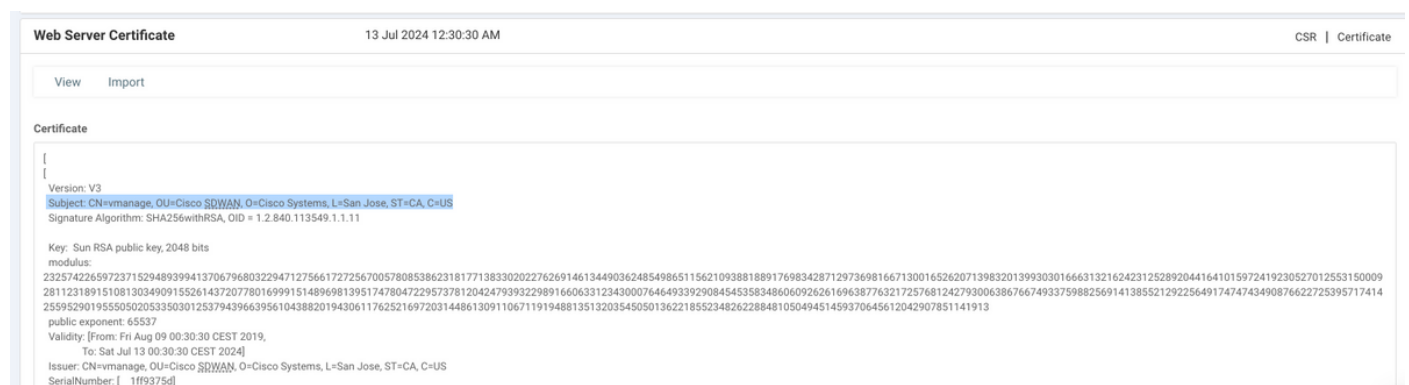
Problem

Das vManage-Webzertifikat läuft ab oder ist bereits abgelaufen. Der Zugriff auf die grafische Benutzeroberfläche (GUI) kann verloren gehen, oder es wird ein permanenter Alarm in der GUI über das abgelaufene Zertifikat angezeigt.

Lösung

Wenn Sie sich nicht um den Sicherheitsaspekt der Verwendung selbstsignierter Zertifikate kümmern und nur Alarmmeldungen und mögliche Probleme mit dem vManage-GUI-Zugriff aufgrund eines abgelaufenen Zertifikats vermeiden möchten, können Sie diese Lösung mit selbstsigniertem Webzertifikat in einem vManage verwenden.

1. Navigieren Sie in der vManage-GUI zu **Administration > Settings > Web Server Certificate > Certificate (Verwaltung > Einstellungen > Webserverzertifikat > Zertifikat)**, und speichern Sie diese Informationen dann irgendwo über das Zertifikatsfach, z. B. **Betreff: CN=vmanager, OU=Cisco SDWAN, O=Cisco Systems, L=San Jose, ST=CA, C=US**.



The screenshot shows the 'Web Server Certificate' configuration page in vManage. The page title is 'Web Server Certificate' and the date is '13 Jul 2024 12:30:30 AM'. The page has a 'View' and 'Import' button. The 'Certificate' section displays the following details:

```
[
[
Version: V3
Subject: CN=vmanager, 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
2811231891510813034909155261437207780169991151489698139517478047229573781204247939322989166063312343000764649339290845453583486060926261696387763217257681242793006386766749337598825691413885212922564917474743490876622725395717414
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=vmanager, OU=Cisco SDWAN, O=Cisco Systems, L=San Jose, ST=CA, C=US
SerialNumber: [ 1f9375d]
```

2. Navigieren Sie in der vManage-GUI zu **Administration > Settings > Web Server Certificate > CSR**, und wählen Sie **Generate (Generate)** aus, um eine neue CSR-Anfrage (Certificate Signing Request) zu erstellen. Stellen Sie sicher, dass Sie die Werte aus dem **Betreff** eingeben, das Sie im vorherigen Schritt erfasst haben.

3. Kopieren Sie neu generierte CSR in den Kopieren-Puffer, wie im Bild gezeigt.

4. Geben Sie dann ein **vshell** ein, und fügen Sie mithilfe des **echo**-Befehls Pufferinhalte mit CSR in die Datei von vManage ein.

```
vmanage#
vmanage# vshell
vmanage:~$ mkdir web
vmanage:~$ cd web
vmanage:~/web$ echo "-----BEGIN NEW CERTIFICATE REQUEST-----
> MIICsjCCAzoCAQAwbTElMAkGA1UEBhMCVVMx CzAJBgNVBAGTAkNBMRwDwYDVQOH
> EwhTYW4gSm9zZTEWMBQGA1UEChMNQ2l zY28gU3lzdGVtczEUMBIGA1UECxMLQ2l z
> Y28gU0RXQU4xEDAoBgNVBAMTB3ZtYW5hZ2UwggeiMA0GCSqGSIb3DQEBAQUAA4IB
> DwAwggEKAoIBAQCRRdIKGUyudwobn60PeDqf q96d+r5z66VQ8NBTBBhgwZgG57J7
> YIY9yNF5oSb+b1xUEXb61Wntq7qSHS zJhFDX0BaL4/c911OQped3yDE1CE0ly3oH
> y88yg7TIZjnmz+j8Io92cRXnZLz9YJwfs9PwEF0Z/4Gw5QIkukdAmLmkeKjOWD2A
> 4pG2sV8Og+hnhUw8tJ1rKzQKs j2JmD+i keZbXu36iZvdKJB34iM2AsmsRbJhUff
> ujuU705E0z1nF2SBCJ+fpf7ze75dQRrBT0PA23QRobQEEg5wSMc+G//jD26zBCNg
> IEyUAX0/0NQfOqtMmcBm7QJDESseOSufv4b9AgMBAAGgADANBqkqhkiG9w0BAQsF
> AAOCAQEAK2BenHnfYuW1agdcYrZJD6+uGC6fNfI6qqmv9XEPFFW0QfPhu8rESyY
> K3qgf/ED+iCXEk/hudnf09vZ6gygM+P8a/zN3+J3VM5zCb6tn7vM0/cytcJONPt u
> mnZGpDO+XjZDDLYmS6j1B+h05gXeYyQ1t4Qv/s2H8jPhIWTraV376E+S9o318cva
> 7D7yp3W+ce5ItHs9ObKWOaexVsyypAV4USrDaVs fSbyU97G2rCXqmMgRLJdBwZofg
> 04qsgRc8qG28aue1Q88XPa/HQt p0WB/Pxg7oe91s59Je/ETsMkR3vt7ag1emyXAJ
> nal67+T/QWgLSJB2pQuPHo51MbA55w==
> -----END NEW CERTIFICATE REQUEST-----" > web_cert.csr
```

5. Stellen Sie sicher, dass CSR mithilfe des Befehls **cat** richtig gespeichert wird.

```
vmanage:~/web$ cat web_cert.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICsjCCAzoCAQAwbTElMAkGA1UEBhMCVVMx CzAJBgNVBAGTAkNBMRwDwYDVQOH
```

```
EwhTYW4gSm9zZTEWMBQGA1UEChMNQ2l2Y28gU3l2dGVtczEUMBIGA1UECxMLQ2l2
Y28gU0RXQU4xEDA0BgNVBAMTB3ZtYW5hZ2UwggeiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCRRdIKGUYuDwobn60PeDqfq96d+r5z66VQ8NBTBBhgWZgG57J7
YIY9yNF5oSb+blxUEXb61Wntq7qSHSszJhFDX0BaL4/c911OQped3yDELCE0ly3oH
y88yg7TIZjnmz+j8Io92cRXnZLZ9YJwfs9PwEF0Z/4Gw5QIkukdAmLmkeKjOWD2A
4pG2sV8Og+hnhUw8tJ1rKzQKsj2JmD+iKeZbXu36iZvdKJB34iM2AsmsRbJhUff
uJU705E0z1nF2SBCJ+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/QWgLSJB2pQuPH051MbA55w==
-----END NEW CERTIFICATE REQUEST-----
```

```
vmange:~/web$
```

6. Erstellen Sie mithilfe von **openssl** einen Schlüssel für das Root-Zertifikat mit dem Namen **rootca.key**.

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

7. Generieren Sie das Zertifikat der Stammzertifizierungsstelle mit dem Namen **rootca.pem** und signieren Sie es mit **rootca.key**, der im vorherigen Schritt generiert wurde.

```
vmange:~/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) []:vmange
Email Address []:
vmange:~/web$ ls
rootca.key  rootca.pemweb_cert.csr
vmange:~/web$
```

8. Signieren Sie Ihren CSR mit dem Zertifikat und dem Schlüssel der Stammzertifizierungsstelle.

```
vmange:~/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=vmange
Getting CA Private Key
vmange:~/web$ ls
rootca.key  rootca.pemrootca.srl  web_cert.crt  web_cert.csr
vmange:~/web$
```

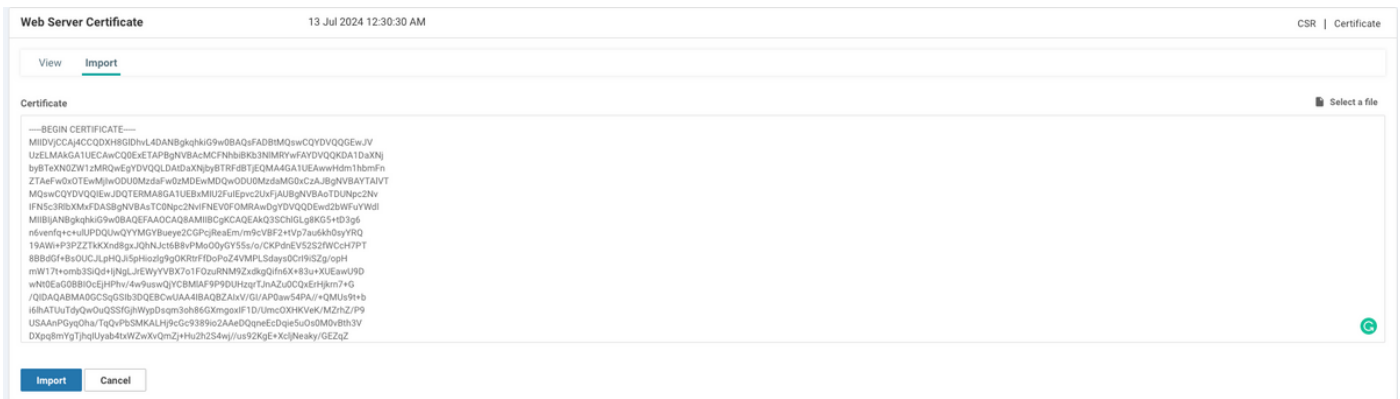
9. Kopieren Sie ein neues signiertes Zertifikat in den Kopiepuffer. Sie können **cat** verwenden, um das signierte Zertifikat anzuzeigen.

```

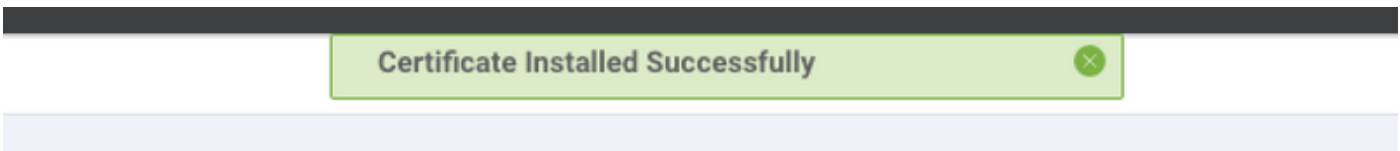
vmanage:~/web$ cat web_cert.crt
-----BEGIN CERTIFICATE-----
MIIDVjCCAj4CCQDXH8G1DhVl4DANBgdGkqhkiG9w0BAQsfADBTMQswCQYDVQGEwJV
UzELMAGAlUECAwCQDEwETAPBgNVBACMCFNhbiBkb3NlMRwvFAQDVQKDA1DaXNj
byBTeXN0ZW1zMRQwEgYDVQQLDADaXNjbyBTRFRFdBTjEQA4GA1UEAwwHdmlhbmFn
ZTAeFw0xOTcwOTUwODU0MzdaFw0zMDUwMDQwODU0MzdaMG0xCzAJBgNVBAYTA1VT
MQswCQYDVQGEwJQTERMA8GA1UEBxMIU2FuIEpvc2UxZjJlYUJlYUJlYUJlYUJlYU
IFN5c3R1bXNmFzASBgNVBASlC0Npc2NvIFNEV0FOMRAwDgYDVQDEwd2bWfuYWdl
MIIIBIjANBgdGkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKQ3SCh1GLg8KG5+td3g6
n6venfqc+uIUPDQWuQYYMGYBueye2CGPc jReaEm/m9cVBF2+tVp7au6kh0syYRQ
19AWi+P3PZZTtkXnd8gxJqHnJct6B8vPMo00yGY55s/o/CKPdnEV52S2fWCcH7PT
8BBdGf+BsOUJLpHQjI5phiozlg9gOKRtrFfDoPoZ4VMPLSdays0CrI9iSzg/opH
mW17t+omb3SiQd+I jNgLJrEWyYVBX7o1FOzuRNM9ZxdkgQifn6X+83u+XUEawU9D
wNt0EaG0BBI0CejHPhv/4w9uswQjYCBM1AF9P9DUHzqrTjnAZu0CQxerHjkRN7+G
/QIDAQABMA0GCSqSIB3DQEBCwUAA4IBAQBZAIXv/GI/AP0aw54PA//+QMUS9t+b
i6lhaTUuTdyQwOuQSSfgjhwYpDsqm3oh86GXmgoxIF1D/UmcOXHKVek/MZrhZ/P9
USAAnPgYqOha/TqQvPbSMKALHj9cGc9389io2AAeDQqneEcDqie5u0s0M0vBth3V
DXpq8mYgTjhgIUYab4txWzXvQmZj+Hu2h2S4wj//us92Kge+XcljNeaky/GEZqZ
jwN0wDgWeJdsM8x2Qt eHHBDTahuArVJflp45eLJCJR1k0lRL8TTroWaST1bZCJz
20aYk4S0K0nTkpScuVirXhkwnN6Ka4q9/rVxnLzAflJ4E9DXo jpd3qNH
-----END CERTIFICATE-----

```

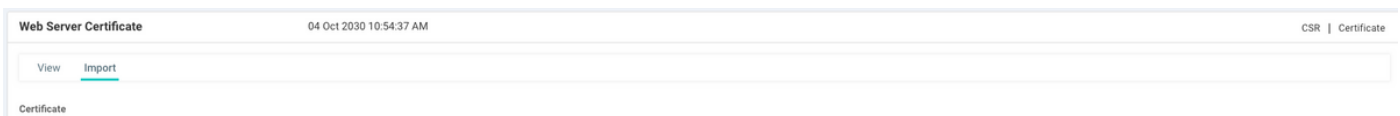
10. Importieren Sie das Zertifikat in vManage. Navigieren Sie dazu zu **Administration > Settings > Web Server Certificate > Import** und fügen Sie den Inhalt des Kopiepuffers ein, wie im Bild gezeigt.



11. Wenn Sie alles richtig gemacht haben, wird in vManage die Meldung **"Certificate Installed Successfully"** (Zertifikat erfolgreich installiert) angezeigt, wie im Image gezeigt.



12. Überprüfen Sie abschließend das Ergebnis, und stellen Sie sicher, dass das Gültigkeitsdatum des Zertifikats wie im Bild gezeigt erfolgreich aktualisiert wurde.



Zugehörige Informationen

- [Generieren eines Webserverzertifikats](#)

- [OpenSSL-Mann](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)