

vManage用の自己署名Web証明書の生成方法

内容

[概要](#)

[問題](#)

[解決方法](#)

[関連情報](#)

概要

このドキュメントでは、既存のWeb証明書がオンプレミスvManageで期限切れになったときに、自己署名Web証明書を生成してインストールする方法について説明します。シスコはそのような導入のWeb証明書に署名しないため、お客様は独自の認証局(CA)または一部のサードパーティCAを使用して署名する必要があります。

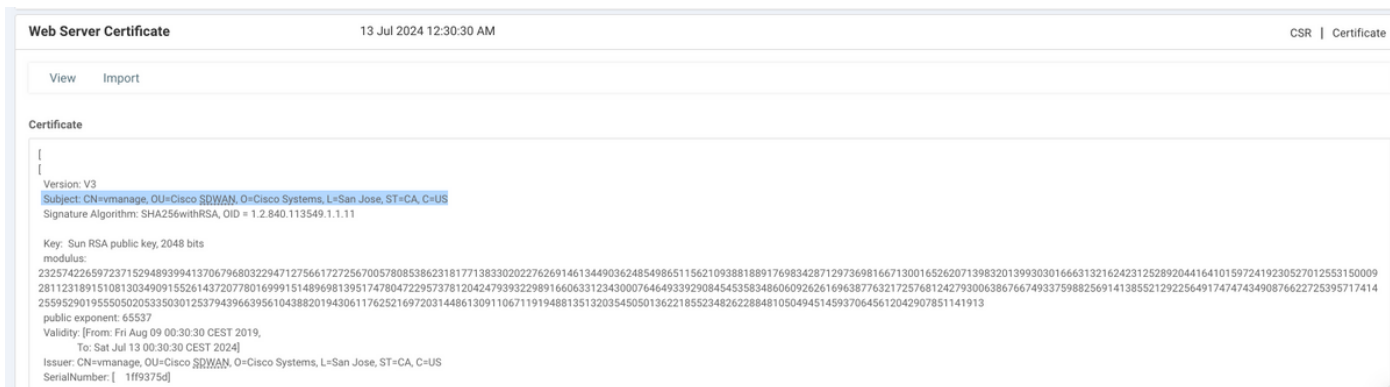
問題

vManage Web証明書が期限切れになるか、すでに期限切れになります。グラフィカルユーザインターフェイス(GUI)へのアクセスが失われたり、GUIで証明書の期限切れに関する永続的なアラームが表示されることがあります。

解決方法

自己署名証明書の使用のセキュリティ面に懸念がなく、アラームメッセージや、期限切れの証明書によるvManage GUIアクセスの問題を回避したい場合は、vManageでこのソリューションを自己署名Web証明書で使用できます。

1. vManage GUIで、[Administration] > [Settings] > [Web Server Certificate] > [Certificate]に移動し、証明書のサブジェクトに関する次の情報を保存します。例えば、[Subject:CN=vmanage, OU=Cisco SDWAN, O=Cisco Systems, L=San Jose, ST=CA, C=US]。



2. vManage GUIで、[Administration] > [Settings] > [Web Server Certificate] > [CSR]に移動し、[Generate]を選択して新しい証明書署名要求(CSR)を生成します。前のステップでキャプチャした件名の値を入力してください。

3.図に示すように、新しく生成されたCSRをコピーペーストバッファにコピーします。

4.次に、vshellを入力し、echoコマンドを使用してCSRを含むバッファコンテンツをvManageのファイルに貼り付けます。

```
vmanage#
vmanage# vshell
vmanage:~$ mkdir web
vmanage:~$ cd web
vmanage:~/web$ echo "-----BEGIN NEW CERTIFICATE REQUEST-----
> MIICs jCCAzoCAQAwbTElMAkGA1UEBhMCVVMx CzA JBgNVBAgTAKNBMRewDwYDVQQH
> EwhTYW4gSm9zZTEWMBQGA1UEChMNQ21zY28gU31zdGVtczEUMBIGA1UECxMLQ21z
> Y28gU0RXQU4xEDAoBgNVBAMTB3ZtYW5hZ2UwgGEMAOGCSqGSIb3DQEBAQUAA4IB
> DwAwggEKAoIBAQCRRdIKGUYuDwobn60PeDqf q96d+r5z66VQ8NBTBBhgWZgG57J7
> YIY9yNF5oSb+b1xUEXb61Wntq7qSHS zJhFDX0BaL4/c911OQped3yDE1CE01y3oH
> y88yg7TIZ jnmz+j8Io92cRXnZLZ9YJwfs9PwEF0Z/4Gw5QIkukdAmLmkeKjOWD2A
> 4pG2sV8Og+hnhUw8tJ1rKzQKs j2JJmD+i keZbXu36iZvdKJB34iM2AsmsRbJhUff
> u jUU705E0z1nF2SBCJ+fpf7ze75dQRrBT0PA23QRobQEeg5wSMc+G//jD26zBCNg
> IEyUAX0/0NQfOqtMmcBm7QJDESseOSufv4b9AgMBAAGgADANB gkqhkiG9w0BAQsF
> AAOCAQEAK2BenHnfYuW1agdcYrZJD6+uGC6fNfI6qqmv9XEPFFW0QfPhu8rESyY
> K3qgf/ED+iCXEk/hudnf09vZ6gygM+P8a/zN3+J3VM5zCb6tn7vM0/cytcJONPtU
> mnZGpDO+XjZDDLYmS6j1B+h05gXeYyQ1t4Qv/s2H8jPhIWTraV376E+S9o318cva
> 7D7yp3W+ce5ItHs90bKWOaexVsyPAV4USrDaVs fSbyU97G2rCXqmMgRLJdBwZofg
> 04qsgrC8qG28aue1Q88XPa/HQt p0WB/Pxg7oe91s59Je/ETsMkR3vt7aglemyXAJ
> nal67+T/QWgLSJB2pQuPHo51MbA55w==
> -----END NEW CERTIFICATE REQUEST-----" > web_cert.csr
```

5. catコマンドを使用して、CSRが正しく保存されていることを確認してください。

```
vmanage:~/web$ cat web_cert.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICs jCCAzoCAQAwbTElMAkGA1UEBhMCVVMx CzA JBgNVBAgTAKNBMRewDwYDVQQH
EwhTYW4gSm9zZTEWMBQGA1UEChMNQ21zY28gU31zdGVtczEUMBIGA1UECxMLQ21z
Y28gU0RXQU4xEDAoBgNVBAMTB3ZtYW5hZ2UwgGEMAOGCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCRRdIKGUYuDwobn60PeDqf q96d+r5z66VQ8NBTBBhgWZgG57J7
YIY9yNF5oSb+b1xUEXb61Wntq7qSHS zJhFDX0BaL4/c911OQped3yDE1CE01y3oH
y88yg7TIZ jnmz+j8Io92cRXnZLZ9YJwfs9PwEF0Z/4Gw5QIkukdAmLmkeKjOWD2A
```

```
4pG2sV8Og+hnhUw8tJ1rKzQKsj2JJmD+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. opensslの助けを借りて、rootca.keyという名前のルート証明書のキーを生成します。

```
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. rootca.pemという名前のルートCA証明書を生成し、前の手順で生成したrootca.keyで署名します。

```
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. ルートCA証明書とキーでCSRに署名します。

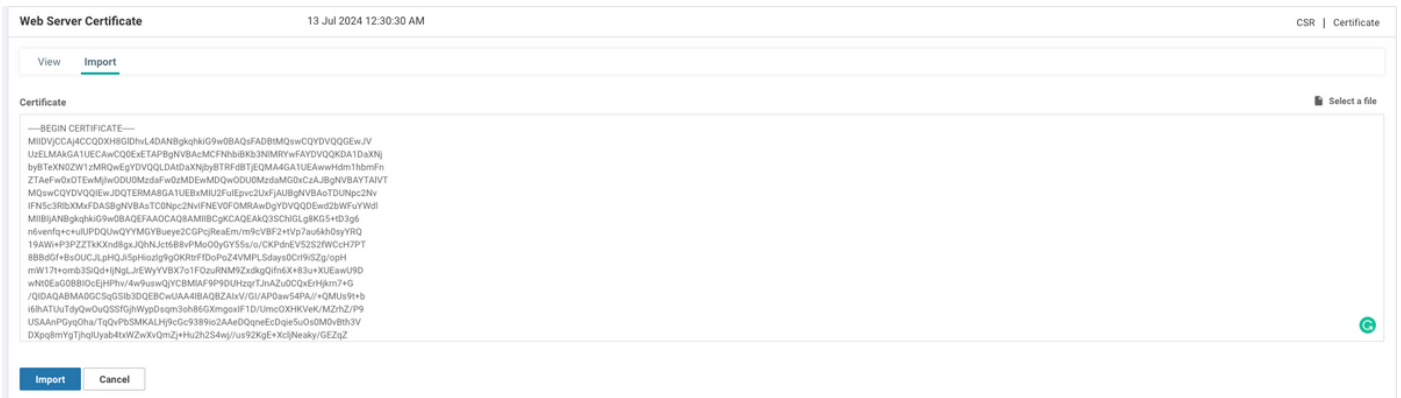
```
vmanage:~/web$ openssl x509 -req -in web_cert.csr -CA rootca.pem -CAkey rootca.key -
CAcreateserial -out web_cert.crt -days 4000 -sha256
Signature ok
subject=/C=US/ST=CA/L=San Jose/O=Cisco Systems/OU=Cisco SDWAN/CN=vmanage
Getting CA Private Key
vmanage:~/web$ ls
rootca.key  rootca.pemrootca.srl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

9. 新しい署名付き証明書をコピーペーストバッファにコピーします。catを使用すると、署名付き証明書を表示できます。

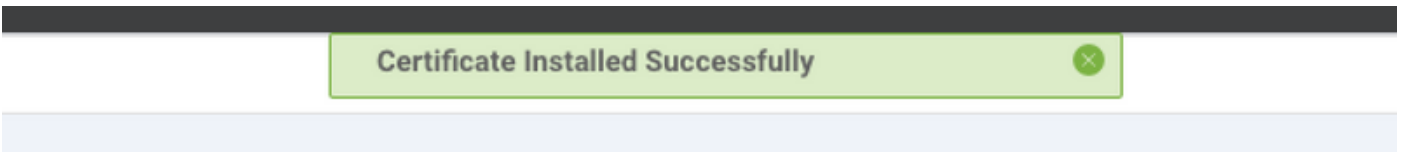
```
vmanage:~/web$ cat web_cert.crt
-----BEGIN CERTIFICATE-----
MIIDVjCCAj4CCQDXH8G1DhvL4DANBgkqhkiG9w0BAQsFADBtMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExETAPBgNVBACMFNhb3NlMRYwFAYDVQQKDA1DaXNj
```

```
byBTeXN0ZW1zMRQwEgYDVQQLDAtDaXNjbYBTRFdBtjEQMA4GA1UEAwHdm1hbmFn
ZTAeFw0xOTUwMjZlMzUwODU0MzdaFw0zMDUwMDQwODU0MzdaMG0xCzAJBgNVBAYTA1VT
MQswCQYDVQQQIEwJZDQTERMA8GA1UEBxMIU2FuIEpvc2UxZjAUBG9NVBAoTDUNpc2Nv
IFN5c3RlbXNkMzFASB9NVBAStC0Npc2NvIFNEV0FOMRAwDgYDVQDEwd2bWVudl
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKQ3SCh1GLg8KG5+tD3g6
n6venfq+c+ulUPDQwQYMYBueye2CGPcjReaEm/m9cVBF2+tVp7au6kh0syYRQ
19AWi+P3PZZTtKXnd8gxJQhNjct6B8vPMo0yGY55s/o/CKPdnEV52S2fWCcH7PT
8BBdGF+BsOUCJLpHQJi5pHiozlg9gOKRtrFfDoPoZ4VMPLSdays0CRI9iSzg/opH
mW17t+omb3SiQd+IjNgLJrEWYVVBX7o1FOzuRNM9ZxdkgQifn6X+83u+XUEawU9D
wNt0EaG0BBI0CejHPhv/4w9uswQjYCBMIAF9P9DUHzqrTJnAZu0CQxerHjkm7+G
/QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBZAIxV/GI/AP0aw54PA//+QMUs9t+b
i6lhATUuTdyQwOuQSSfGjHwypDs3oh86GXmgoxIF1D/UmcOXHKVek/MZrhZ/P9
USAApGyqOha/TqQvPbSMKALHj9cGc9389io2AAeDQqneEcDqie5uOs0M0vBth3V
DXpq8mYgTjhgIUYab4txWZwXvQmZj+Hu2h2S4wj//us92Kge+XcljNeaky/GEZqZ
jWNNoWdGWeJdsM8hx2QteHHBDTahurVJf1p45eLiCJR1k01RL8TTroWaSt1bZCJZ
20aYK4S0K0nTkpscuVlrXHkwNN6Ka4q9/rVxnLzAflJ4E9DXoJpD3qNH
-----END CERTIFICATE-----
```

10. 証明書をvManageにインポートします。これを行うには、図に示すように、[Administration] > [Settings] > [Web Server Certificate] > [Import]に移動し、コピーペーストバッファの内容を貼り付けます。



11. すべてを正しく行くと、図に示すようにvManageに「Certificate Installed Successfully」と表示されます。



12. 最後に、結果を確認し、図に示すように証明書の有効日付が正常に更新されたことを確認します。



関連情報

- [Webサーバ証明書の生成](#)
- [OpenSSLマン](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)