How to generate a self-signed certificate with custom root CA

1. Generate self-signed root certificate files. To do that, run the command "/etc/scripts/gencert.sh root 7300". 7300 is the number of days before the certificate expires. Input the country code, state, and company name. Keep the challenge password field empty.

```
root@CM685V:~# /etc/scripts/gencert.sh root 7300
mkdir: can't create directory '/tmp/mycert/': File exists
Generating RSA private key, 2048 bit long modulus
.......................................................+++
.......................+++
e is 65537 (0x10001)
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]:AU
State or Province Name (full name) [Some-State]:VIC
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:COMSET
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

Signature ok
subject=/C=AU/ST=VIC/O=COMSET
Getting Private key
root@CM685V:~#
root@CM685V:~#
```

2. Run the command **ls /tmp/mycert/**. Here you can see rootca.crt, which will be imported into the web browser.

```
root@CM685V:~# ls /tmp/mycert/
rootca.crt  rootca.csr  rootca.key
root@CM685V:~#
```

3. Generate the router certificates by entering the command **/etc/scripts/gencert.sh cm685v cm685v.dyndns.org 123.150.170.69 192.168.1.1 7300**

cm685v	-	Certificate file name.
cm685v.dyndns.org	-	DDNS host name. If there is no DDNS, use "" instead.
123.150.170.69	-	Static WAN IP. If there is no Static WAN IP, use "" instead.
192.168.1.1	-	Router LAN IP.
7300	-	Number of days before the certificate expires (20 years)

```
root@CM685V:~# /etc/scripts/gencert.sh cm685v cm685v.dyndns.org 123.150.170.69 192.168.1.1 7300
Generating RSA private key, 2048 bit long modulus
.................................+++
.....................................................................................................
e is 65537 (0x10001)
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]:AU
State or Province Name (full name) [Some-State]:VIC
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:COMSET
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

Signature ok
subject=/C=AU/ST=VIC/O=COMSET
Getting CA Private Key
root@CM685V:~#
root@CM685V:~#
```

4. Generate certificates for the second router “cm685v-site2”, by entering the command **/etc/scripts/gencert.sh cm685v-site2 cm685v-site2.dyndns.org “” 192.168.1.1 7300**
   <u>Note</u>: The symbol **“”** is used when there is no Static WAN IP.

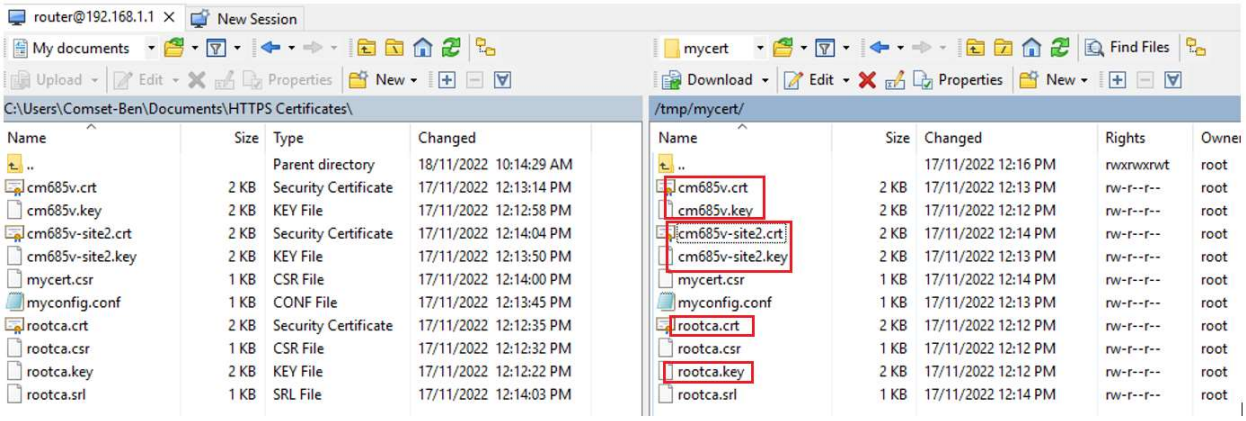
```
root@CM685V:~# /etc/scripts/gencert.sh cm685v-site2 cm685v-site2.dyndns.org "" 192.168.1.1 7300
Generating RSA private key, 2048 bit long modulus
.............................................................+++
.....................................................................................................+++
e is 65537 (0x10001)
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]:AU
State or Province Name (full name) [Some-State]:VIC
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:COMSET
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Signature ok
subject=/C=AU/ST=VIC/O=COMSET
Getting CA Private Key
root@CM685V:~#
```

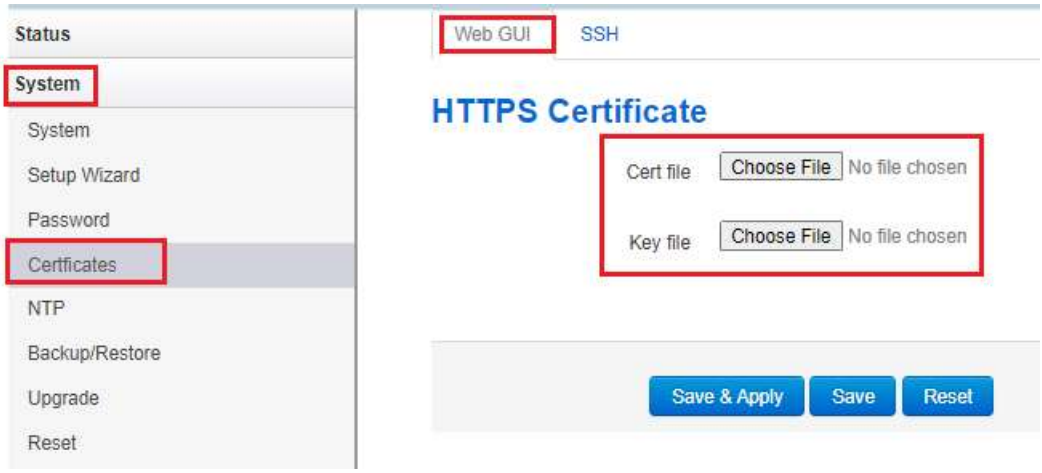
5. Check the router certificates at /tmp/mycert/, by entering the command **ls –l /tmp/mycert**

```
root@CM685V:~# ls -l /tmp/mycert/
-rw-r--r--    1 root     root          1119 Nov 17 12:14 cm685v-site2.crt
-rw-r--r--    1 root     root          1679 Nov 17 12:13 cm685v-site2.key
-rw-r--r--    1 root     root          1111 Nov 17 12:13 cm685v.crt
-rw-r--r--    1 root     root          1679 Nov 17 12:12 cm685v.key
-rw-r--r--    1 root     root           924 Nov 17 12:14 mycert.csr
-rw-r--r--    1 root     root           182 Nov 17 12:13 myconfig.conf
-rw-r--r--    1 root     root          1042 Nov 17 12:12 rootca.crt
-rw-r--r--    1 root     root           924 Nov 17 12:12 rootca.csr
-rw-r--r--    1 root     root          1675 Nov 17 12:12 rootca.key
-rw-r--r--    1 root     root            17 Nov 17 12:14 rootca.srl
root@CM685V:~#
```

6. Download the certificates via WinSCP. The same certificates rootca.* can be used again for generating more router certificates. The certificates cm685v.* and cm685v-site2.* can now be uploaded into the routers.



7. Upload the cm685v.crt and cm685v.key certificates into the router. After you hit “Save & Apply”, the http/https service will restart.



8. Please refer to the document “How to import Root CA certificate into Google Chrome” for importing rootca.crt into your web browser to allow HTTPS access.