Enabling HTTPS access

Instruction : To enable HTTPS for Tegsoft server you are going to prepare some files, transfer files to server and restart some services. Steps below will help to enable HTTPS access.

1) Prepare certificate files (all files are needed)
    a) Certificate public key (**certificate.crt**)
    b) Certificate private key (**certificate.key**)
    c) Certificate PEM format (**certificate.pem**) You can use certificate conversion tools / utilities to create PEM file from crt. A sample command line tool is below

```
openssl x509 -in certificate.crt -out certificate.pem -outform PEM
```

    d) Certificate root and parent keys (**bundle.crt**) If you do not have a bundle.crt file please create an empty file with a name bundle.crt
2) Make sure you have a proper configuration
    a) Connect to server via SSH with root user
    b) RUN command below

```
ls -lrth /etc/httpd/conf.d/tegsoft.conf
```

    c) If you see a file listed (like below) you can continue with step 3

```
 -rw-r--r-- 1 root root 1.3K Jul 10 05:32 /etc/httpd/conf.d/tegsoft.conf
```

    d) If you do not see a listed file and receive a message “No such file or directory” then please run the command below

```
rm -rf /root/custom_certificates
```

    e) Update Tegsoft to latest version and check again with step 2-b. If issue persists please contact with Tegsoft Software Support Team.
3) Configure Tegsoft software not to override configuration. You need to create a file (/root/custom_certificates) if you want to customize HTTP configuration
    a) Connect to server via SSH with root user
    b) Below command will disable auto-generation of server certificates and will notify the server to allow user to use custom certificates.

```
echo 1 > /root/custom_certificates
```

4) You are going to need a software to transfer files from local PC to server. WinSCP will be enough.
5) Transfer Certificate files from local folder to server /certificates (This folder must be created and all files must be transferred) All file names are case sensitive and they must match with the naming defined at step 1.
6) Restart http server to activate ssl engine.
    a) service httpd restart
7) Check https access by a browser
    a) Your https access must be over a DNS name