Configure SSL on campusM Connect Layer

- **Product:** campusM
- **Operating system:** iOS, Android,Web

---

1) Make sure you have a separate file for the server key and the server certificates (including all certificates in the CA chain) for example:
a) certificate.key
b) certificate.crt
c) ca1.crt
d) root.crt

2) Concatenate all the certificates into one file:

cat certificate.crt ca1.crt root.crt > all.crt

3) convert the base64 encoded key file and certificates file to .p12 file
openssl pkcs12 -export -out keyStore.p12 -inkey certificate.key -in all.crt

Provide a password to the P12 file
Enter Export Password: changeit
Verifying - Enter Export Password: changeit

4) Create a JKS file with the server key and certificate files
keytool -importkeystore -srckeystore keyStore.p12 -destkeystore certificate.jks -srcstoretype pkcs12

Provide the password to the p12 file as well as the newly created jks file:
Importing keystore keyStore.p12 to certificate.jks...
Enter destination keystore password: changeit
Re-enter new password: changeit
Enter source keystore password: changeit
Entry for alias 1 successfully imported.

5) Modify the tomcat_home/conf/server.xml file and add the jks to the SSL enabled connector, for example:

```
<!-- Define an SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector
        protocol="org.apache.coyote.http11.Http11NioProtocol"
        port="8443" maxThreads="200"
        scheme="https" secure="true" SSLEnabled="true"
        keystoreFile="/opt/tomcat/conf/certificate.jks" keystorePass="changeit"
        clientAuth="false" sslProtocol="TLS"/>
```

- **Article last edited:** 09-Mar-2022