SSL Configuration in DBSync Tomcat

In order to secure the connection to tomcat and all the routes via DBSync tomcat we can setup SSL certificate on the server and within the tomcat. Please follow the steps to configure:

1. Before configuring the SSL certificate make sure to keep the following handy

a.The root certificate
b.The CA bundle or the intermediate certificates
c.The private key

1. Export the above three items into a single PKCS#12 or PFX format file by executing the following command:

```
pkcs12 -export -in <<certificate>>.crt -inkey <<certificate>>.key -chain -CAfile <<CA-bundle>> -name "<<required-certificate-name>>" -out <<certificate>>.p12
```

You will be prompted to enter a password for exporting, enter and verify it again by retyping the same password when prompted

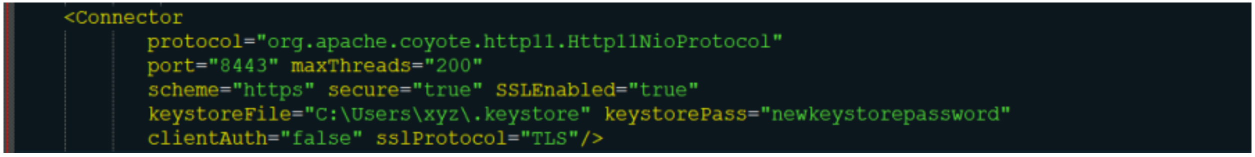
1. Once you have generated the p12 file successfully we need to import into the keystore by executing the following command

```
keytool -importkeystore -deststorepass <<newkeystorepassword>> -destkeystore .keystore -srckeystore <<certificate>>.p12 -srcstoretype PKCS12
```

At this point we have the .keystore file created which needs to be imported into the tomcat.

1. Now go to the folder path *<<DBSync-install-dir>>/conf* and edit the file *server.xml*

Edit the connector property as below,



```
    <Connector
           protocol="org.apache.coyote.http11.Http11NioProtocol"
           port="8443" maxThreads="200"
           scheme="https" secure="true" SSLEnabled="true"
           keystoreFile="C:\Users\xyz\.keystore" keystorePass="newkeystorepassword"
           clientAuth="false" sslProtocol="TLS"/>
```

Specify the path to the keystore file that we created earlier at ***keystoreFile*** and the password we used while generating the keystore file in ***keystorePass***
We have successfully configured SSL in the DBSync tomcat and the connections are now secure.