1. Create keystore “tomcat”. Move all the certs and keys generated to the keystore using the following commands.

**keytool -import -alias root -keystore tomcat.jks -trustcacerts -file ca/root-ca.crt**

**keytool -import -alias signing-ca  -keystore tomcat.jks -trustcacerts -file ca/signing-ca.crt**

**keytool -import -alias tomcat -keystore tomcat.jks -file certs/fred.crt**

Note that the fred certificate is stored with the alias tomcat and it is not of type truststore.

1. Once we have the keystore we need to configure the tomcat to use the keystore. This is done by changing the configuration of the tomcat server. Add the following lines. Make sure the path to keystore is correctly specified.

**<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"**

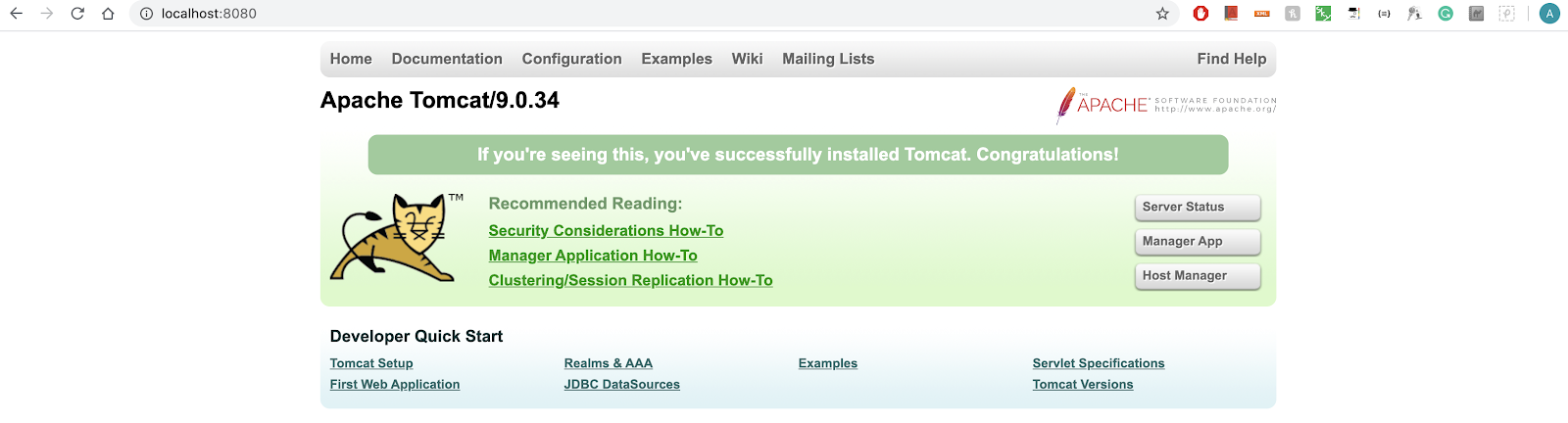
**maxThreads="150" scheme="https" secure="true"**

**keystoreFile="/Users/Shared/tomcat.jks" keystorePass="changeit"**

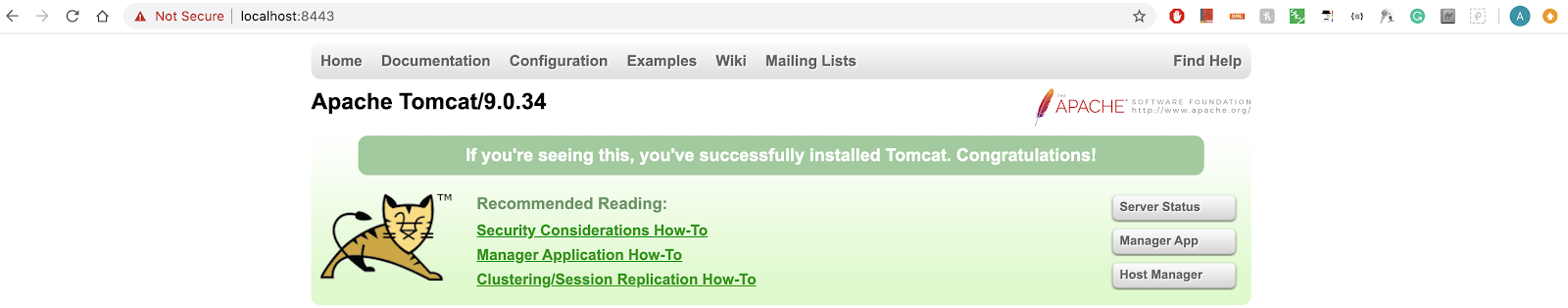
**clientAuth="false" sslProtocol="TLS" sslVerifyClient="optional"**

**sslEnabledProtocols="TLSv1.2,TLSv1.1,SSLv2Hello"/>**

1. Now run the tomcat server using the command **catalina run**
2. The default port for non SSL connection is 8080. So, hit **http://localhost:8080** and you should see the following page



1. Note that we have configured SSL connection on port 8443 from the configuration we have set. Now we hit the endpoint [**https://localhost:8443**](https://localhost:8443) and you should see the following screen.



You see that we are now able to use certificates generated previously and hit the https:// endpoint which means SSL works as expected.