VeraLab SSL Configuration

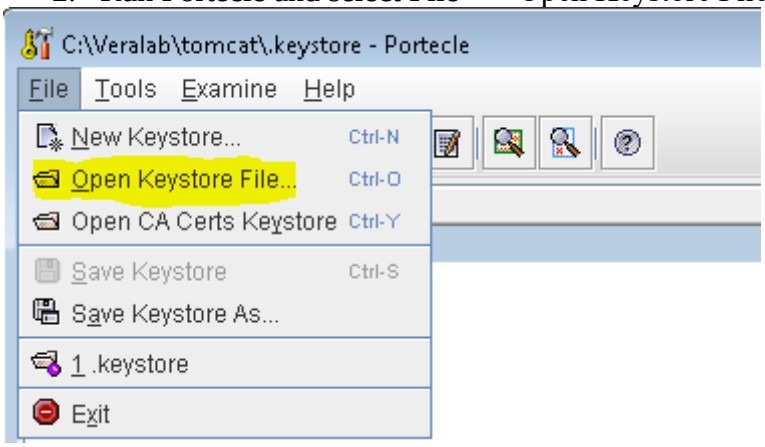
Contents

Enabling SSL for Web Interface

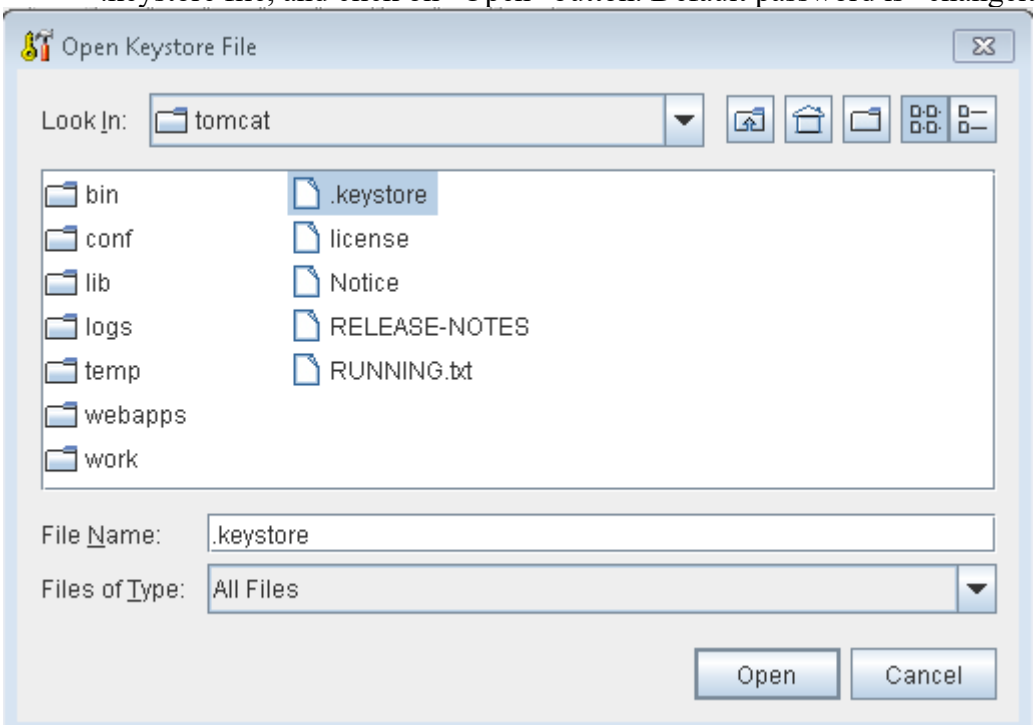
To enable SSL for VeraLab web application you need to obtain a certificate either from commercial certification authority (CA) or from your own institution CA server.

First you need to generate a certificate signing request (CSR). It can be generated with java keytool utility or GUI application such as Portecle available from the following URL: http://portecle.sourceforge.net/. If you prefer using keytool you can find more information on Oracle web site http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html or on Apache Tomcat site https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html.
Below steps show how to use Portecle application as an example.

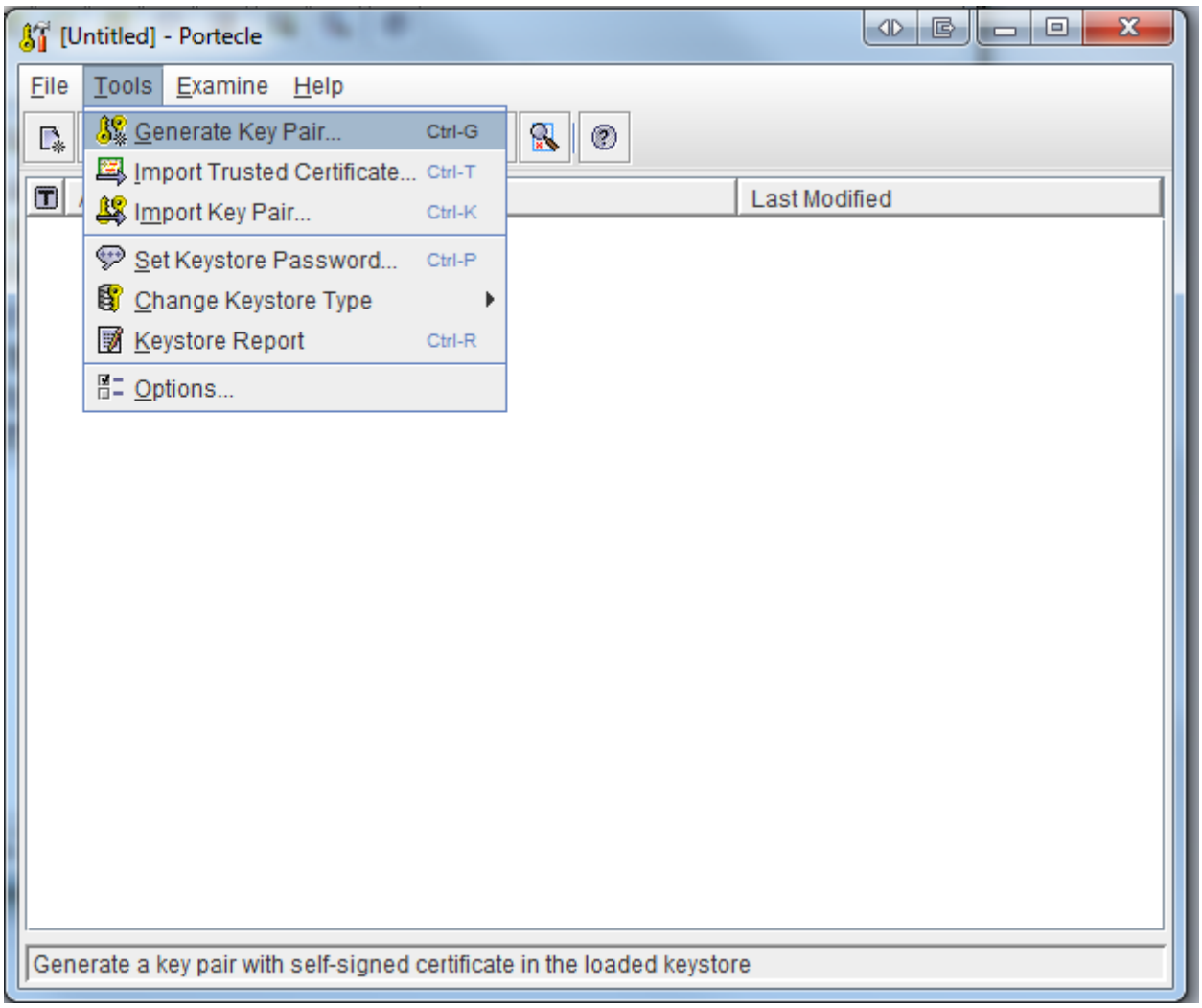
1. First take a backup of .keystore file under C:\Veralab\tomcat (where C:\Veralab is default VeraLab home on your server).
2. Run Portecle and select File -> "Open Keystore File…".



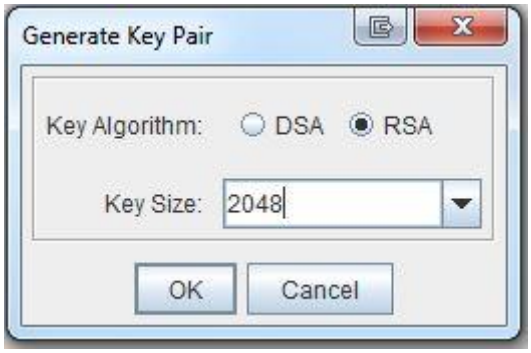
3. Navigate to C:\Veralab\tomcat directory, change "Files of type" to "All Files", select .keystore file, and click on "Open" button. Default password is "changeit".



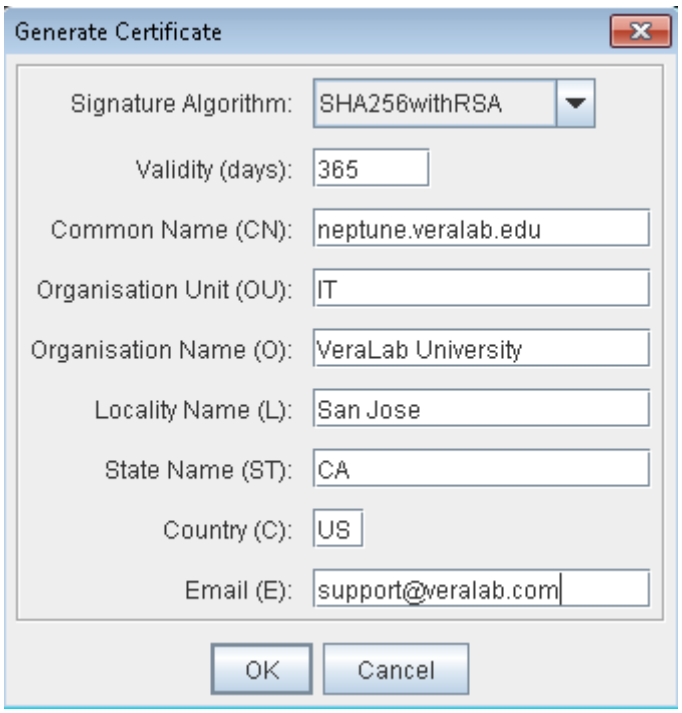
4. Select Tools -> "Generate Key Pair".



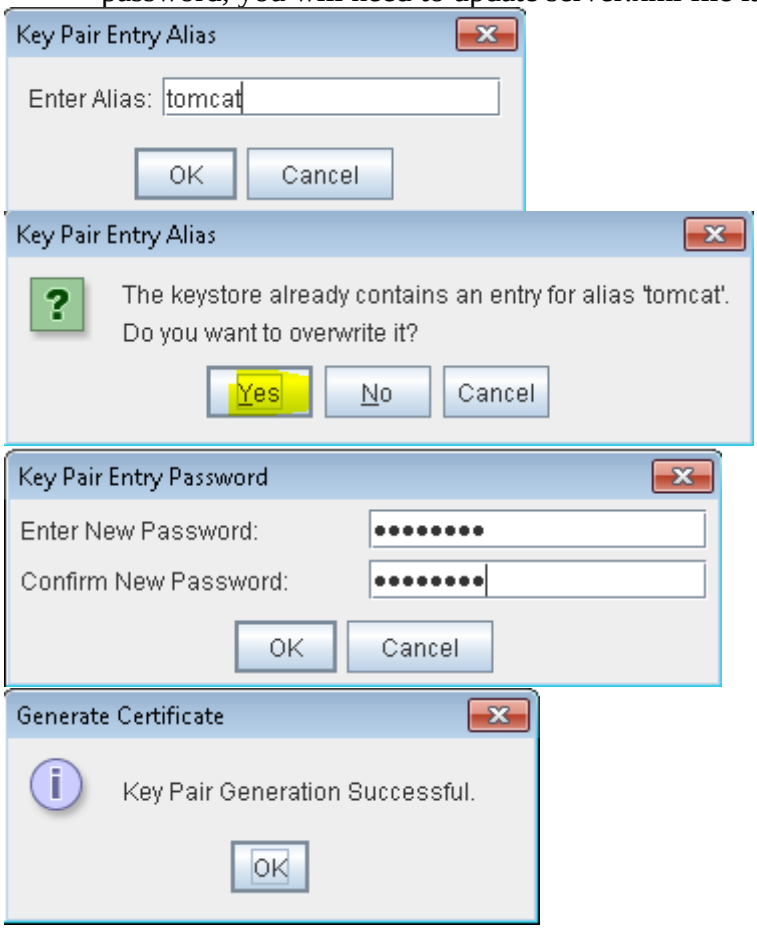
5. Select RSA and 2048 (this is minimum recommended) or 4096 key size in the pop up window.



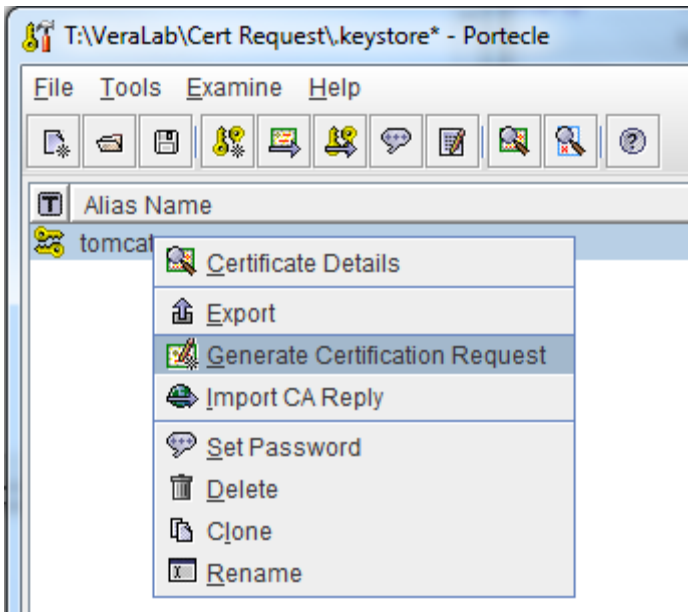
6. Keep default signature algorithm “SHA256withRSA”. Enter your VeraLab server and Organization details. Common Name must be equal to your VeraLab server fully qualified domain name (FQDN).



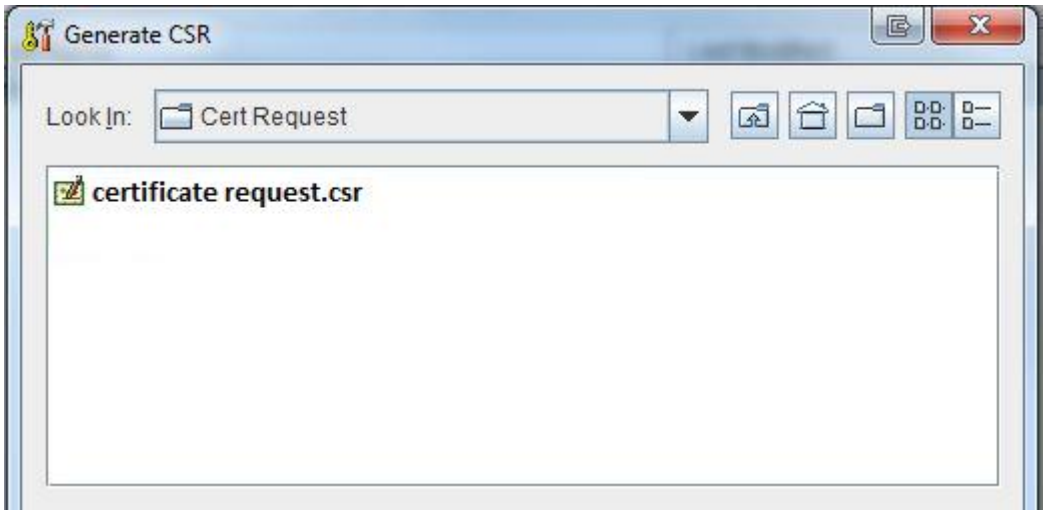
7. You can give your private key any alias name, e.g. keep default “tomcat” or name it veralab. Default password is “changeit”. If you decide not to use default alias or/and password, you will need to update server.xml file later with respective attributes.



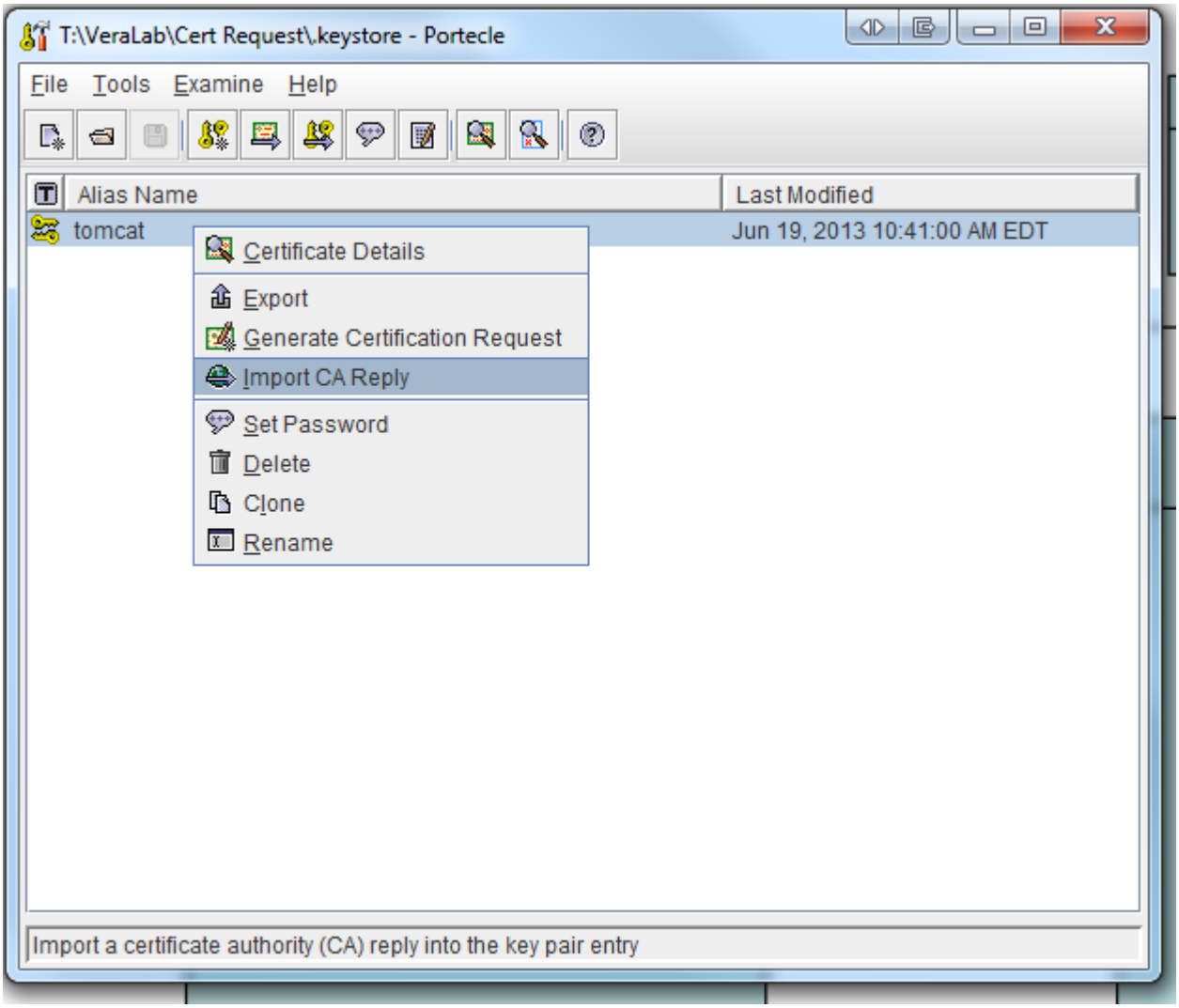
8. Chose “Generate Certification Request” by right clicking on “tomcat” entry.



9. Save the “certificate request.csr” file and then submit it to CA of your choice to get new SSL certificate.



10. After receiving new SSL certificate, chose Import CA Reply, by right clicking on the “tomcat” entry.

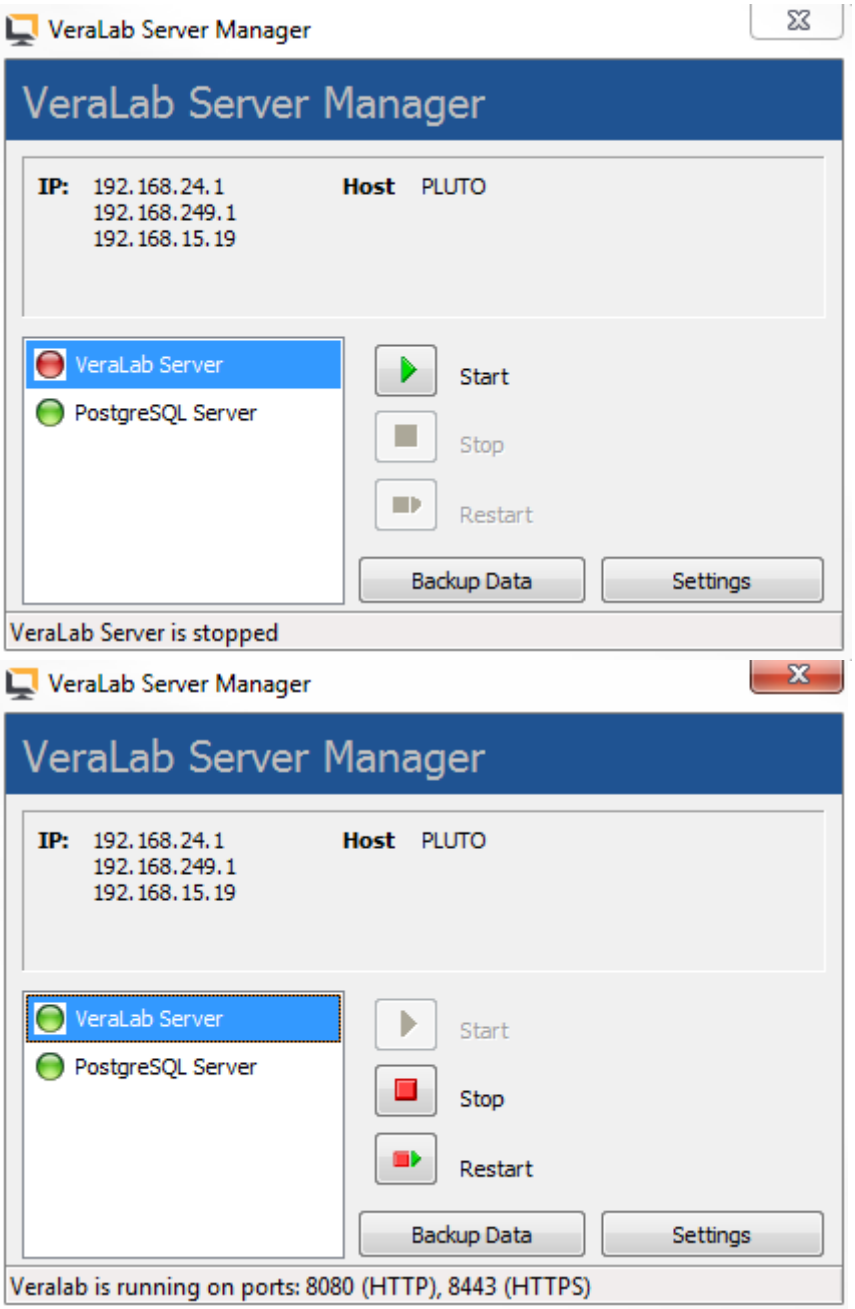


11. Save the .keystore file with the new imported CA certificate/Reply. You can save .keystore file to an alternative location and then copy it and replace existing C:\Veralab\tomcat\.keystore file.
12. If you changed keystore alias name, key and keystore passwords you will need to open C:\Veralab\tomcat\conf\server.xml file in a test editor, e.g. Notepad and update the tag that start with ***Connector port=”8443”*** and has ***scheme="https" secure="true"*** attributes. Add keystorePass, keyPass, and keyAlias attributes with respective custom passwords and alias name used in Step 7. Passwords are case sensitive!

server.xml *

```
<Server port="8005" shutdown="SHUTDOWN">
        <GlobalNamingResources>
                <!-- Used by Manager webapp -->
                <Resource name="UserDatabase" auth="Container" type="org.apache.catalina.UserDatabase" description="User
                pathname="conf/tomcat-users.xml"/>
        </GlobalNamingResources>
        <Service name="Catalina">
                <Connector maxThreads="1000" maxConnections="1000" protocol="org.apache.coyote.http11.Http11NioProtocol"
                <Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150" scheme="https" secure="true" clientAuth=
                sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" keystorePass="newpassword" keyAlias="veralab"/>
                <!-- This is here for compatibility only, not required -->
                <Connector port="8009" protocol="AJP/1.3"/>
                <Engine name="Catalina" defaultHost="localhost">
                        <Realm className="org.apache.catalina.realm.UserDatabaseRealm" resourceName="UserDatabase"/>
                        <Host name="localhost" appBase="webapps"/>
                </Engine>
        </Service>
</Server>
```

13. Open VeraLab Server Manager and restart VeraLab Server.



14. Open your VeraLab web application URL on HTTPS port and verify you are not getting SSL error in the browser.

Enabling SSL for LDAP Integration

If your LDAP server is running on secure port, e.g. default is 636, follow below steps to import SSL certificate on VeraLab server.

1. Download this package: https://veralab.com/veralab/files/InstallCert.zip.
2. Unzip above package on your VeraLab server into C:\Veralab\jre\lib directory.
3. Open command prompt window and execute below command:
C:\veralab\jre\bin\java -jar C:\Veralab\jre\lib\InstallCert.jar your_LDAP_server_name:636
In above command "C:\veralab"is your VeraLab Home directory and your_LDAP_server_name is your LDAP server FQDN, which is SSL enabled. It should download and install SSL certificate.

You may need to run the same command a couple of times. First it may throw an exception, which means it does not trust that certificate. You need to press 1 to add it.
Execute the same second time, and it should say everything is successful and you can press q to quit.
4. Restart VeraLab Tomcat service and test connection and your LDAP authentication should work well for SSL.