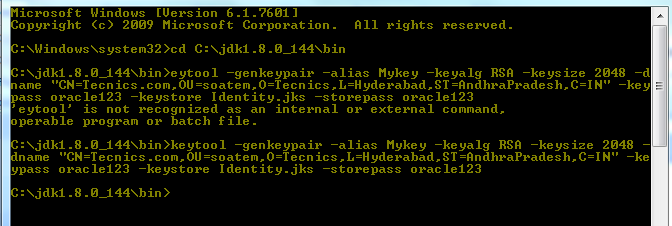
**Weblogic SSL Configuration using Java Keystore**

Step1: Navigate to the path Java/bin (For Eg:C:\jdk1.8.0\_144\bin)

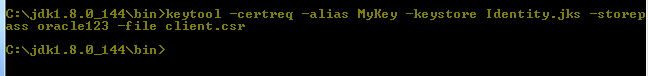
Step2: Run the below cmd In cmd prompt for generating keystore

**keytool -genkeypair -alias Mykey -keyalg RSA -keysize 2048 -dname "CN=tecnics.com,OU=tecnics,O=tecnics,L=Hyderabad,ST=AndhraPradesh,C=IN" -keypass oracle123 -keystore Identity.jks -storepass oracle123**

****

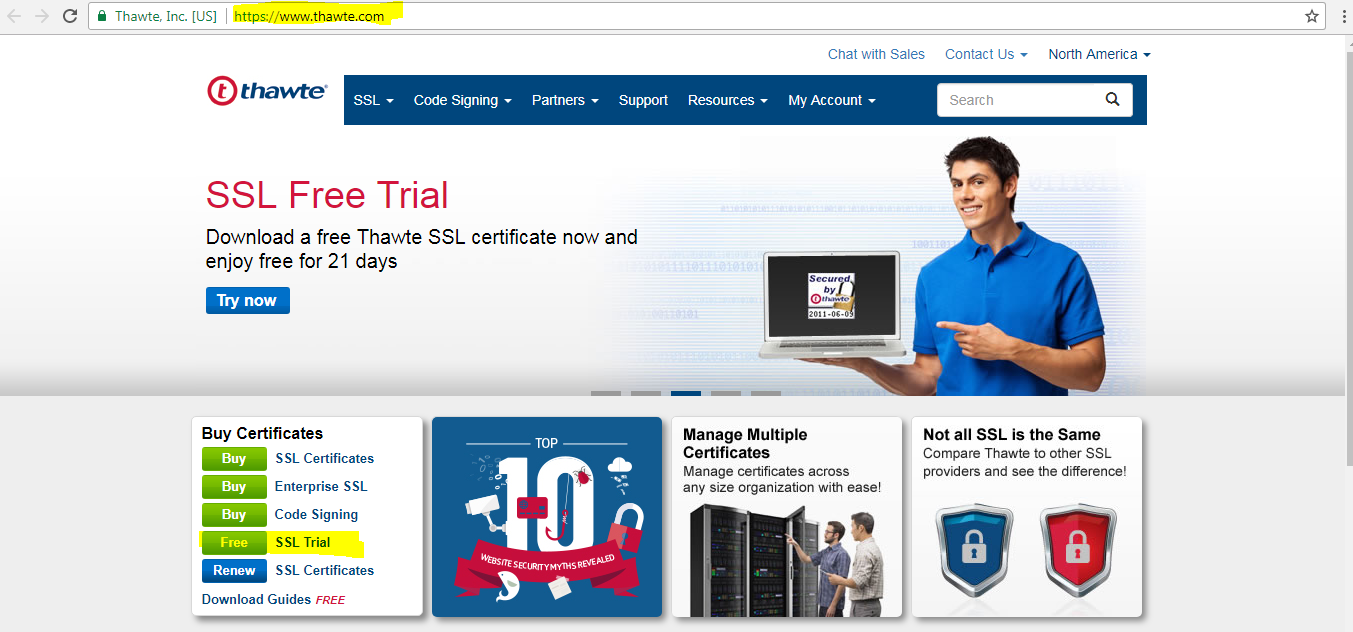
Step 3: Run the below command in cmd prompt for generating client .csr file

**keytool -certreq -alias Mykey -keystore Identity.jks -storepass oracle123 -file client.csr**

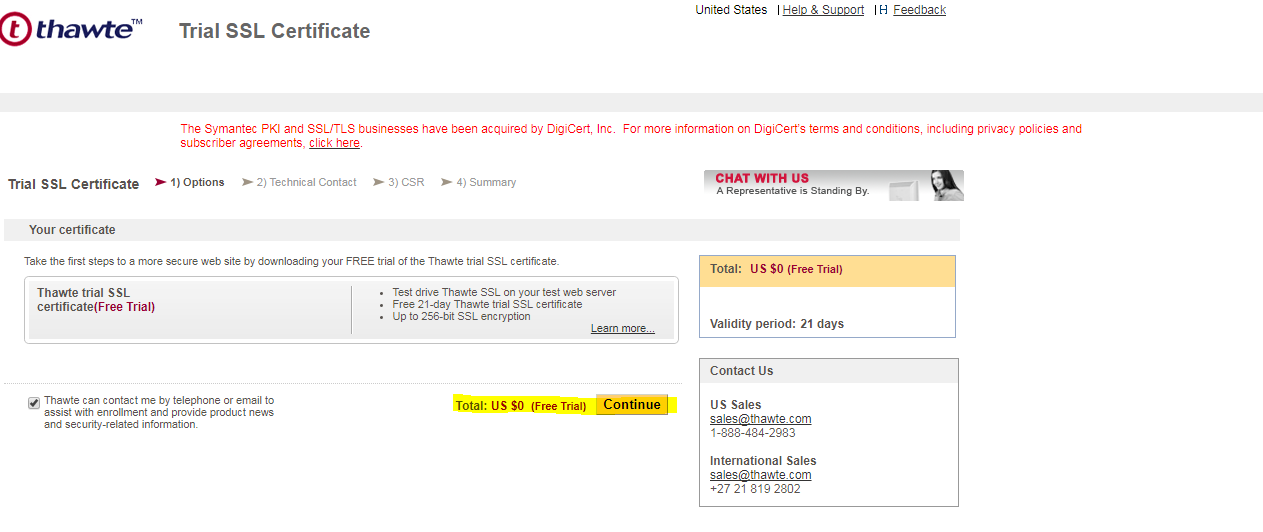


Step 4: for third party trusted and root certificates browse to below mentioned site for free trail

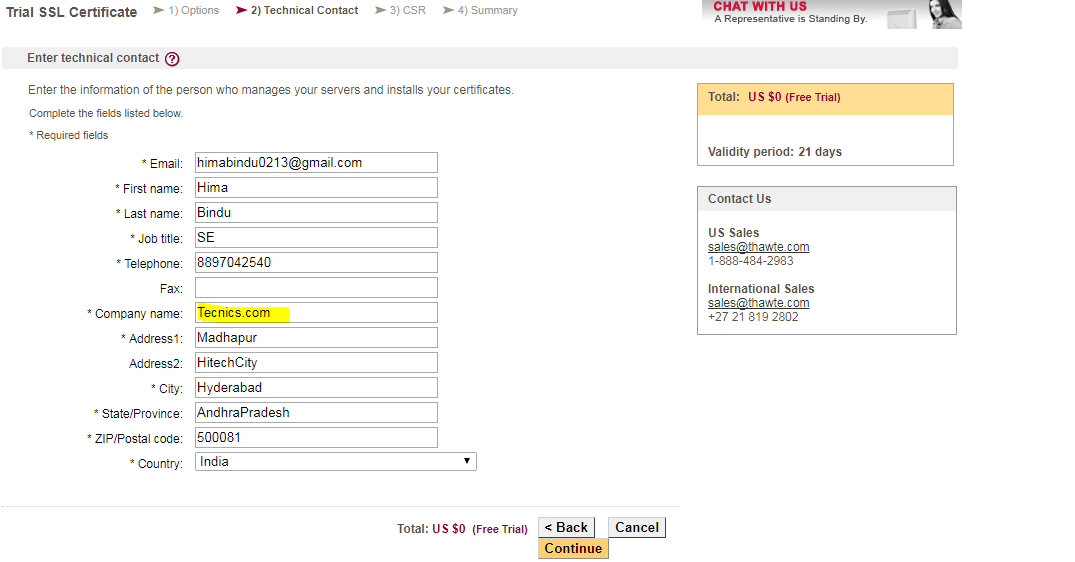
<http://www.thawte.com/>



Step 5: click on SSL free trail as highlighted

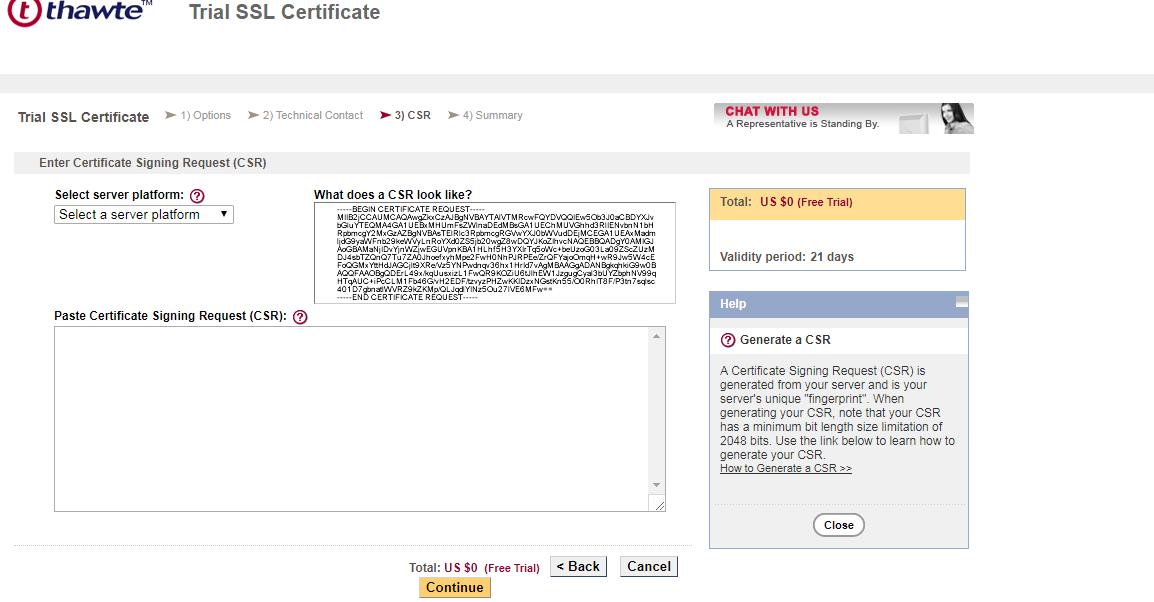


Step6: click on continue button and proceed by filling the details as given.



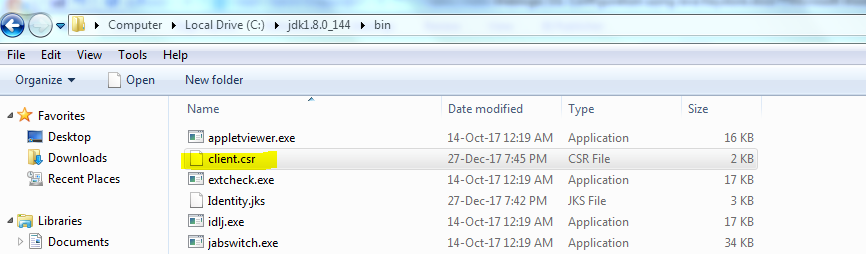
While giving company name, it should match with CN while generating keystore as mentioned in step 2.

Step7: click on continue button



Select the server platform as **‘Weblogic’** and paste the CSR file by navigating to the below folder

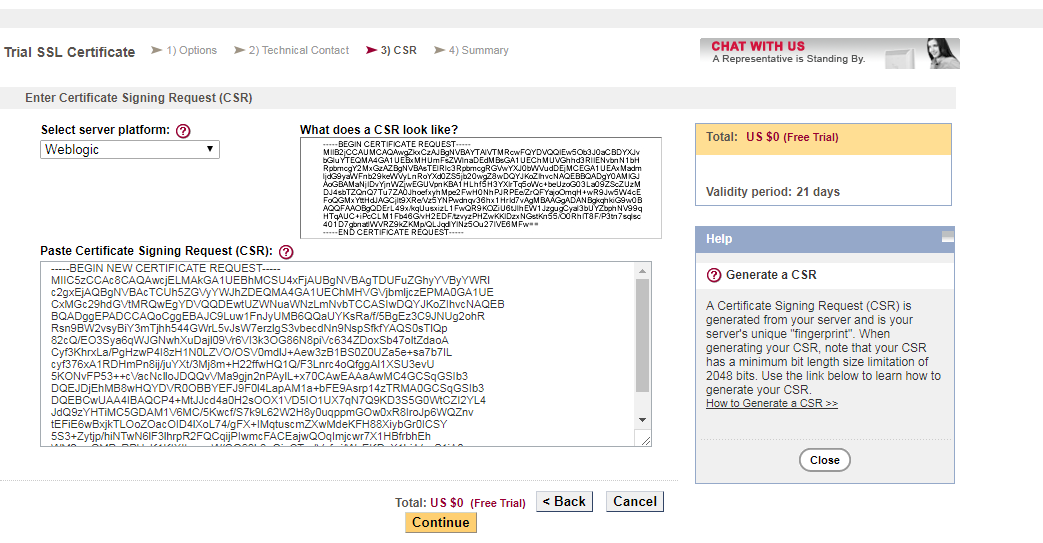
Eg: C:\jdk1.8.0\_144\bin\client.csr

****

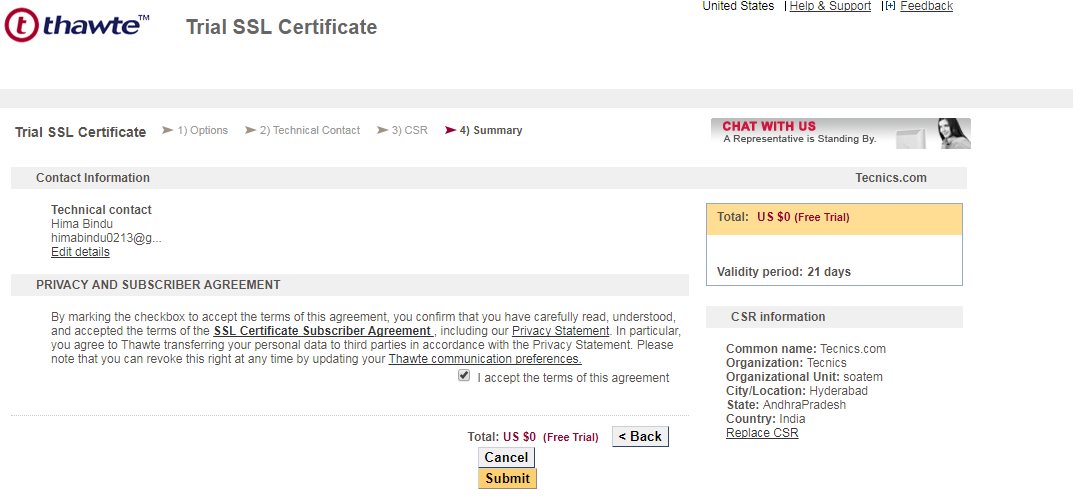
Open the clent.csr file in Notepad++



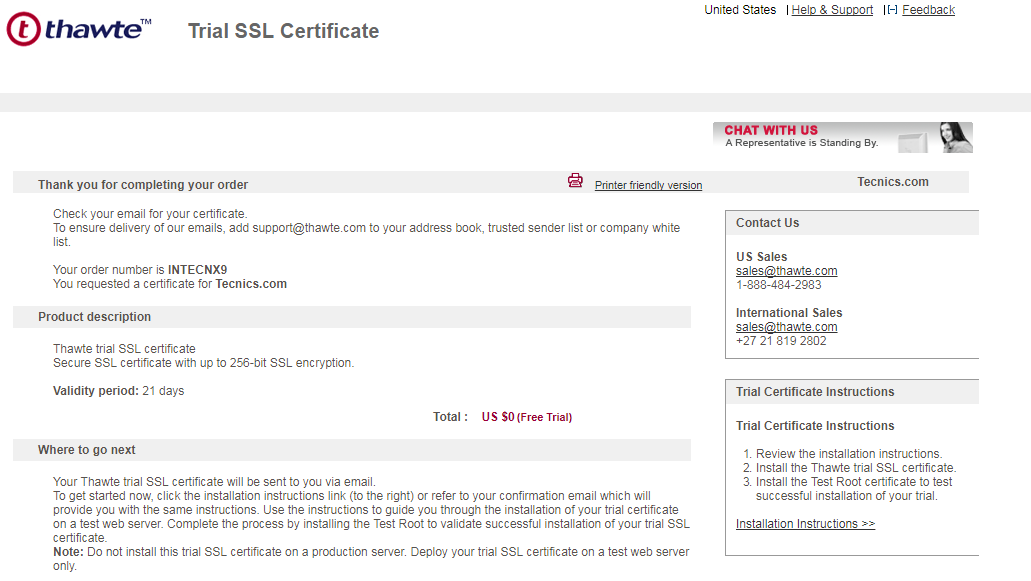
Paste the .csr file in paste certificate signing request block



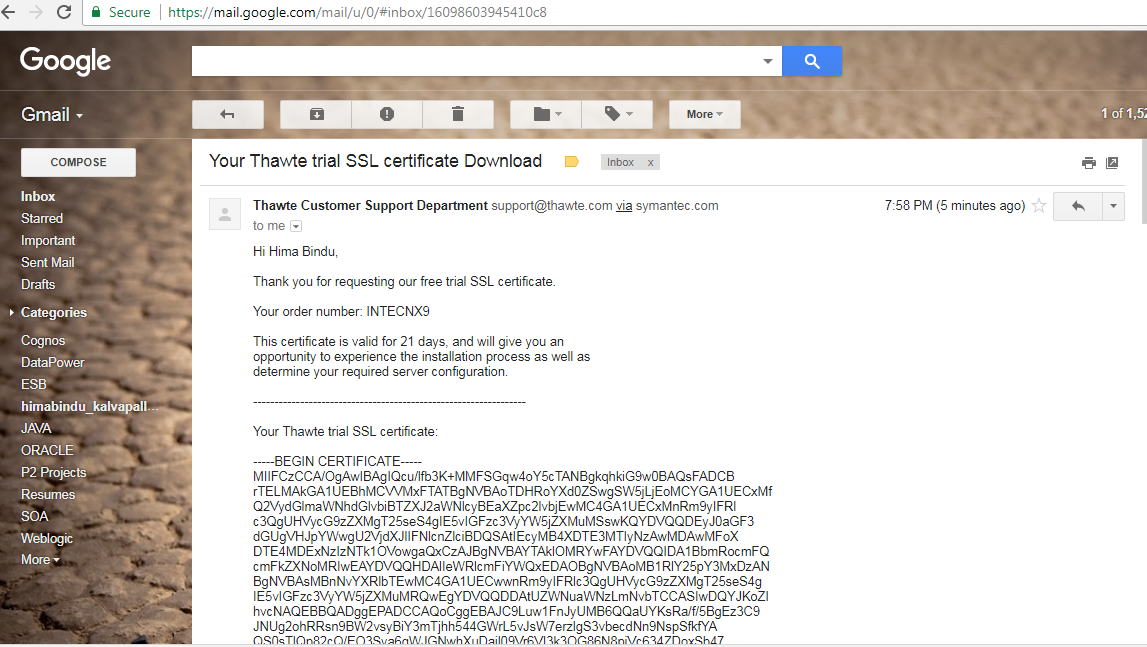
Step 8: Click on continue button and accept the terms and conditions and click on submit.



We will receive an confirmation with the order number as follows

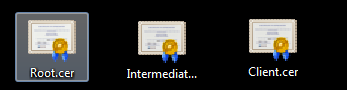


Step 9: we will get an confirmation email to the given mail id



Step 10:

From mail, save Root, Intermediate and client certificates with .cer extensions



Move the above three certificate files to java/bin directory (Eg: C:\jdk1.8.0\_144\bin)

Step 11 : Import intermediate ,Root and client certificates to Identity Keystore

Note: Follow the same order while importing (Intermediate, Root and client)

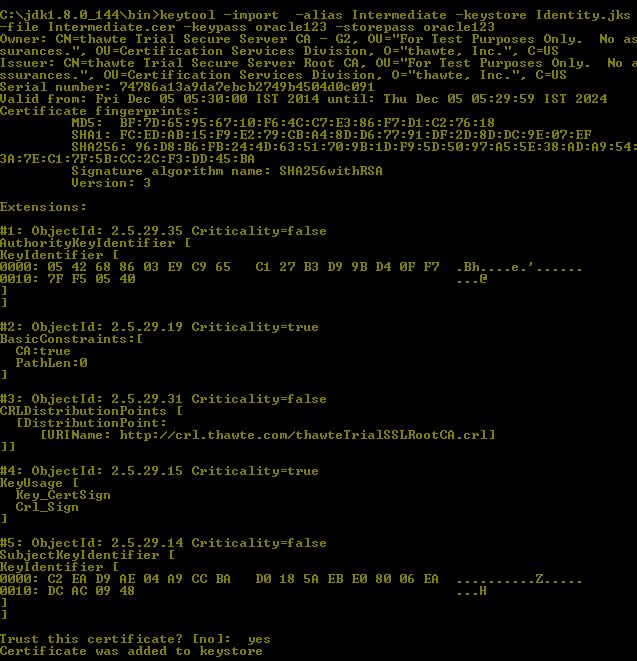
* keytool -import -alias Intermediate -keystore Identity.jks -file Intermediate.cer -keypass oracle123 -storepass oracle123
* keytool -import -alias Root -keystore Identity.jks -file Root.cer -keypass oracle123 -storepass oracle123
* keytool -import -alias Mykey -keystore Identity.jks -file Client.cer -keypass oracle123 -storepass oracle123

Note : Alias name must be same as name mentioned in step2 for importing client .cer

Step12: Import Intermediate and Root certificates to Trust keystore

* keytool -import -alias Intermediate -keystore Trust.jks -file Intermediate.cer -keypass oracle123 -storepass oracle123
* keytool -import -alias Root -keystore Trust.jks -file Root.cer -keypass oracle123 -storepass oracle123

step 13: Import the Intermediate certificate cmd and press yes option to trust the certificate and finally we will get msg as certificate was added to keystore.

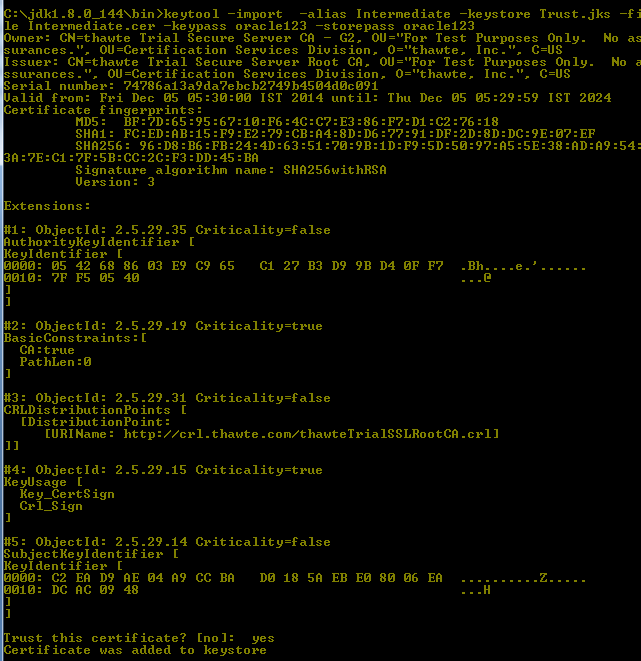


Step 14: Import Root and client certificate file same as above





Step 15: Import intermediate and Root certificates to trust keystore.





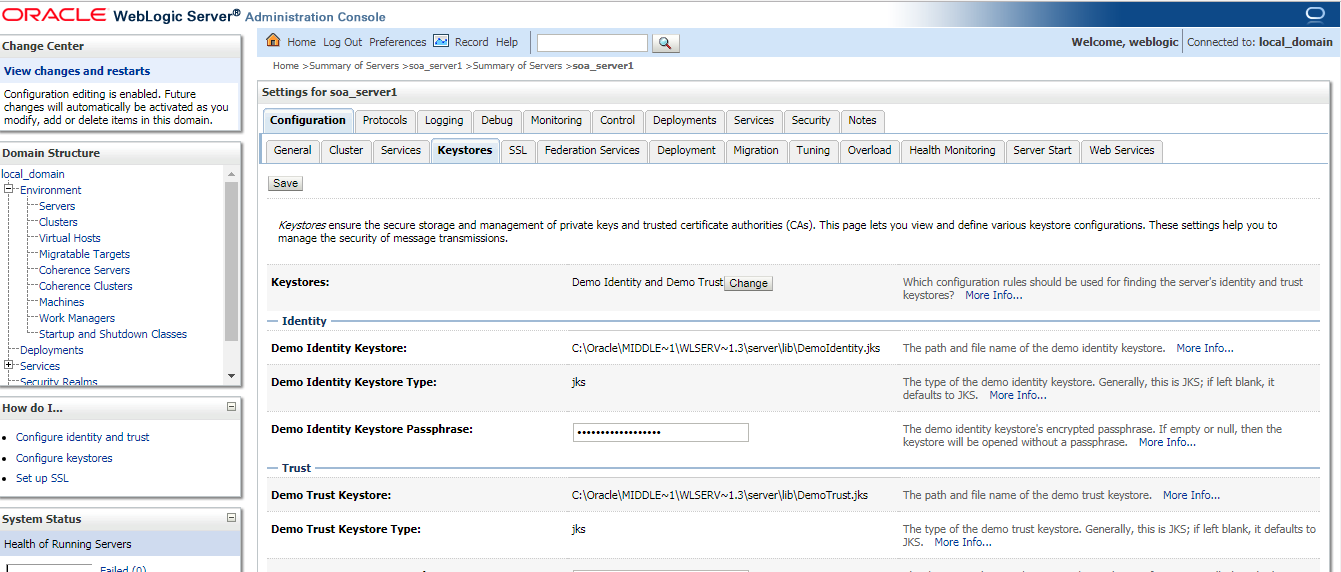
Step 16 : Navigate to Java/bin and copy Identity.jks and Trust.jks files to $weblogic\_Home/Server/lib

Eg: C:\Oracle\Middleware1117\wlserver\_10.3\server\lib (To)

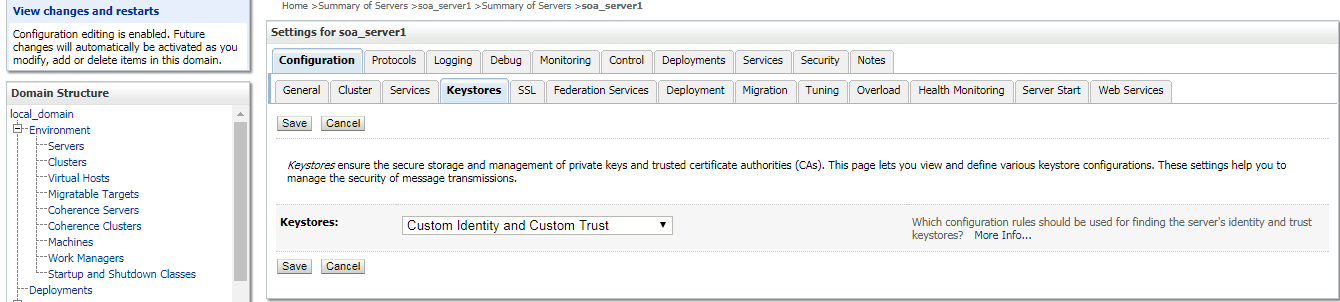
Eg : C:\jdk1.8.0\_144\bin (From)

Step 17: Login into weblogic console

Environment 🡪servers 🡪Soa\_server 🡪 Keystore



Change the keystore type to Custom Identity and Custom trust and click on save



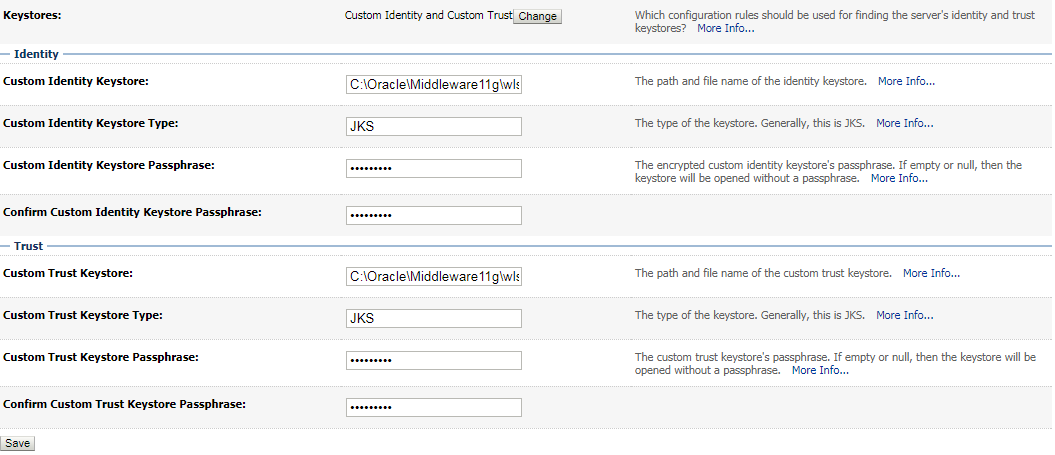
Fill the Identity and trust keystore file details as follows and click on save .

Custom identity keystore file path : C:\Oracle\Middleware1117\wlserver\_10.3\server\lib\Identity.jks

Custom Trust Keystore file path : C:\Oracle\Middleware1117\wlserver\_10.3\server\lib\Trust.jks

Passphrase: oracle123 (Both for identity and Trust)

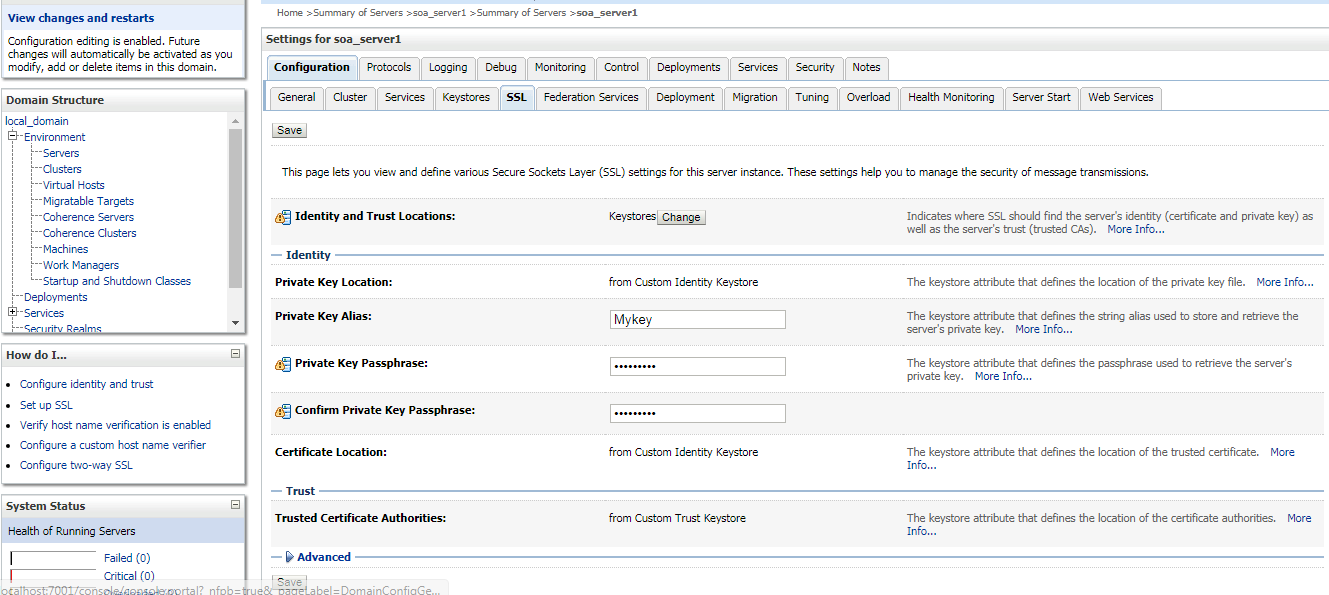
Keystore Type : JKS (Both for identity and Trust)



Step 18 : Navigate to Environment 🡪servers 🡪Soa\_server 🡪 SSL

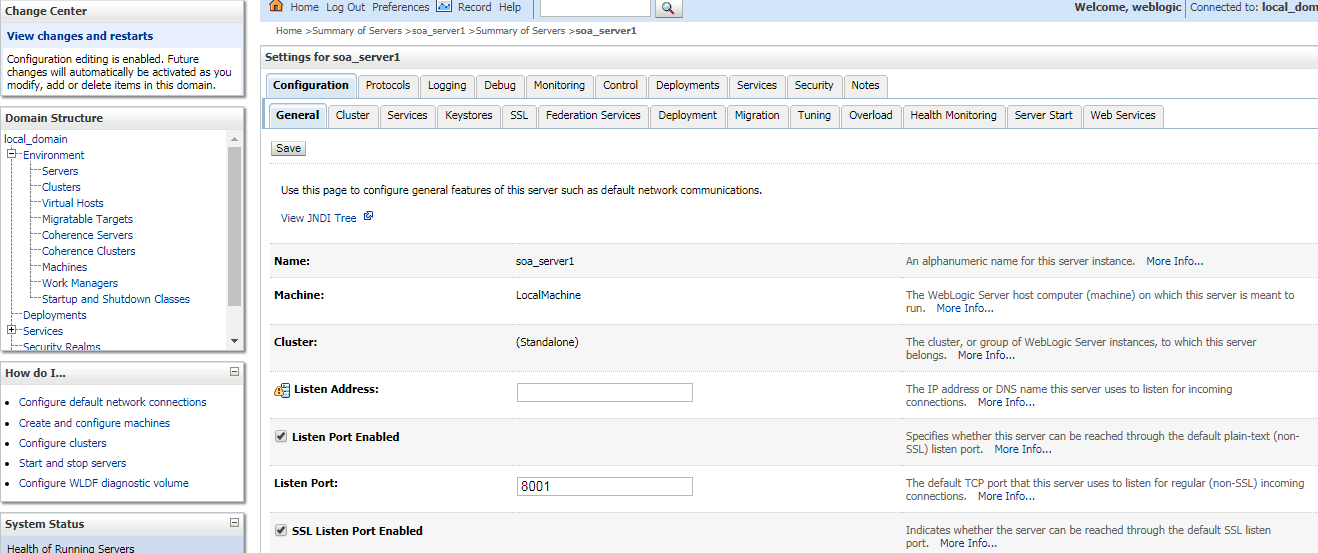
Fill the details as follows and click on save .

Private key alias Name: Mykey (As mentioned in step 2)



Step 19: Navigate to Environment 🡪servers 🡪Soa\_server 🡪 General

Make sure to enable the check box SSL listen port.

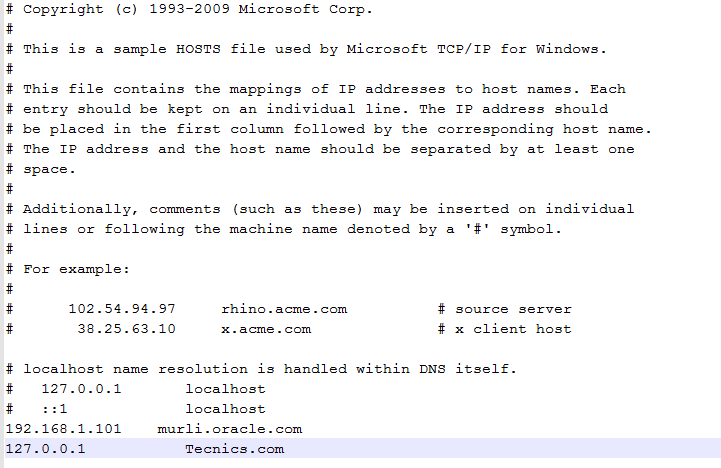


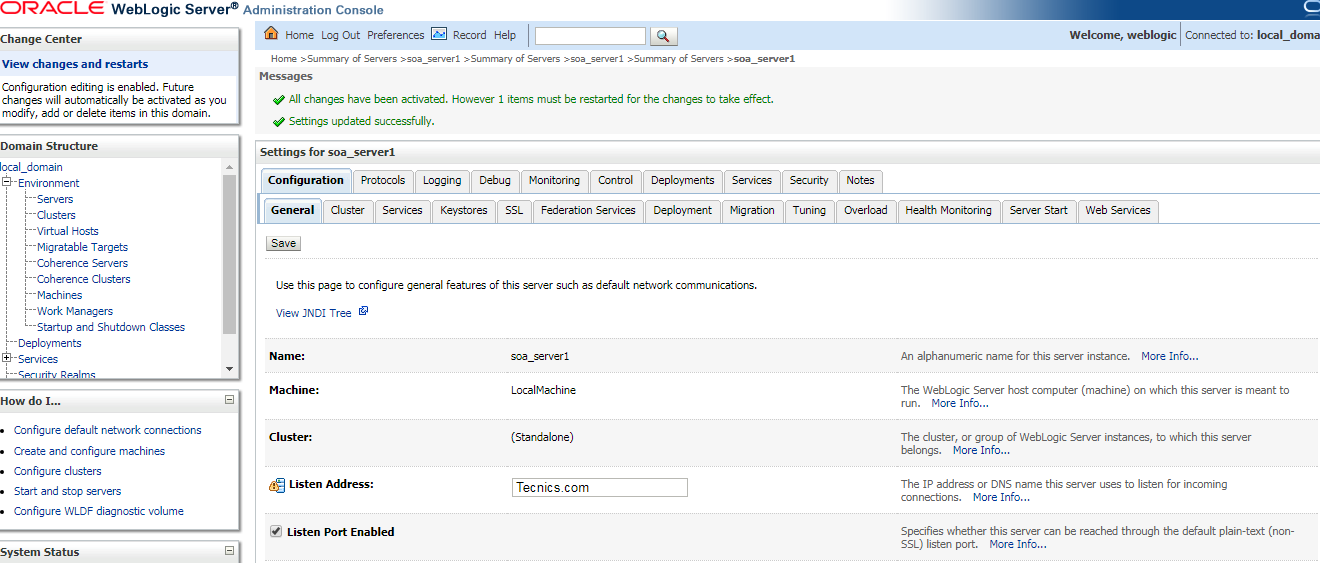
Step 20 : Navigate to path C:\Oracle\Middleware1117\user\_projects\domains\local\_domain\bin and edit setdomainenv.cmd file set EXTRA\_JAVA\_PROPERTIES=%EXTRA\_JAVA\_PROPERTIES% -Dsoa.archives.dir=%SOA\_ORACLE\_HOME%\soa -Dsoa.oracle.home=%SOA\_ORACLE\_HOME% -Dsoa.instance.home=%DOMAIN\_HOME% -Dtangosol.coherence.clusteraddress=227.7.7.9 -Dtangosol.coherence.clusterport=9778 -Dtangosol.coherence.log=jdk -Djavax.xml.soap.MessageFactory=oracle.j2ee.ws.saaj.soap.MessageFactoryImpl -Dweblogic.transaction.blocking.commit=true -Dweblogic.transaction.blocking.rollback=true -Djavax.net.ssl.trustStore=%WL\_HOME%\server\lib\**Trust.jks**

Step 21 : Bounce the server (soa\_server1)

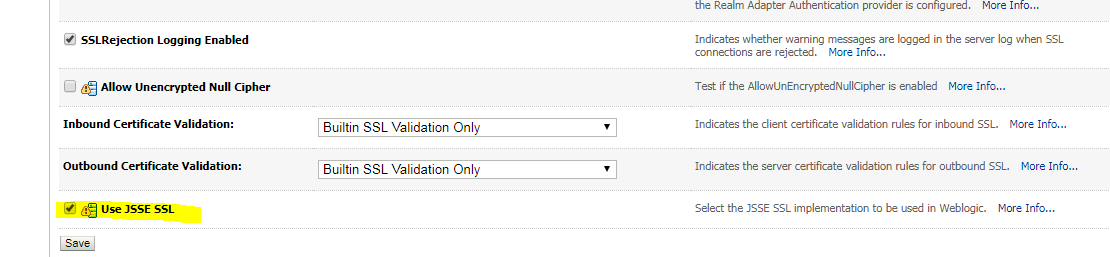
Note : Suppose if there is any issue with the browser we can change the listen address in weblogic console by editing the hosts (C:\Windows\System32\drivers\etc\Hosts) file.

**Eg : 127.0.0.1 Tecnics.com**





Weblogic 🡪 Managed server -🡪 SSL



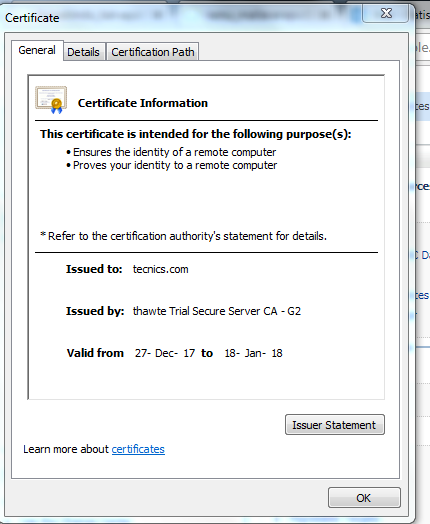
Need to enable JSSE SSL option (For weblogic 11g) or we can edit setdomainenv.cmd file (C:\Oracle\Middleware1117\user\_projects\domains\local\_domain\bin)

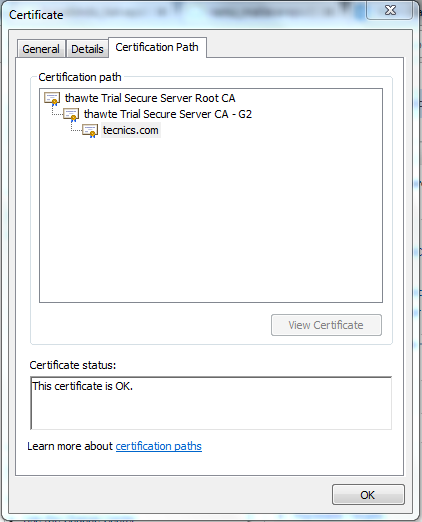
**set EXTRA\_JAVA\_PROPERTIES=%EXTRA\_JAVA\_PROPERTIES% -Dweblogic.ssl.JSSEEnabled=true -Dweblogic.security.SSL.enableJSSE=true**

**Testing :**

Login to below URL

<https://tecnics.com:7002/console/>





Note : Private key --- client

Publick Key ---Root and Intermediate

\*\*\*\*Command to delete certificate which is already imported \*\*\*\*

**Keytool –delete –alias Mykey –keystore Identity.jks –storepass oracle123**