Installing the Certificates to the Keystore

1. Download your certificate files from your certificate authority and save them to the same directory as the keystore that you created during the CSR creation process. The certificate will only work with the same keystore that you initially created the CSR with.

   The certificates must be installed to your keystore in the correct order.

2. **Install the Root Certificate file**: Every time you install a certificate to the keystore you must enter the keystore password that you chose when you generated it. Enter the following command to install the Root certificate file:

   ```
   keytool -import -trustcacerts -alias root -file RootCertFileName.crt -keystore keystore.key
   ```

   If you receive a message that says "Certificate already exists in system-wide CA keystore under alias <...> Do you still want to add it to your own keystore? [no]:", select Yes. If successful, you will see "Certificate was added to keystore".

3. **Install the Intermediate Certificate file**: If your certificate authority provided an intermediate certificate file, you will need to install it here by typing the following command:

   ```
   keytool -import -trustcacerts -alias intermediate -file IntermediateCertFileName.crt -keystore keystore.key
   ```

   If successful, you will see "Certificate was added to keystore".

4. **Install the Primary Certificate file**: Type the following command to install the Primary certificate file (for your domain name):

   ```
   keytool -import -trustcacerts -alias tomcat -file PrimaryCertFileName.crt -keystore keystore.key
   ```

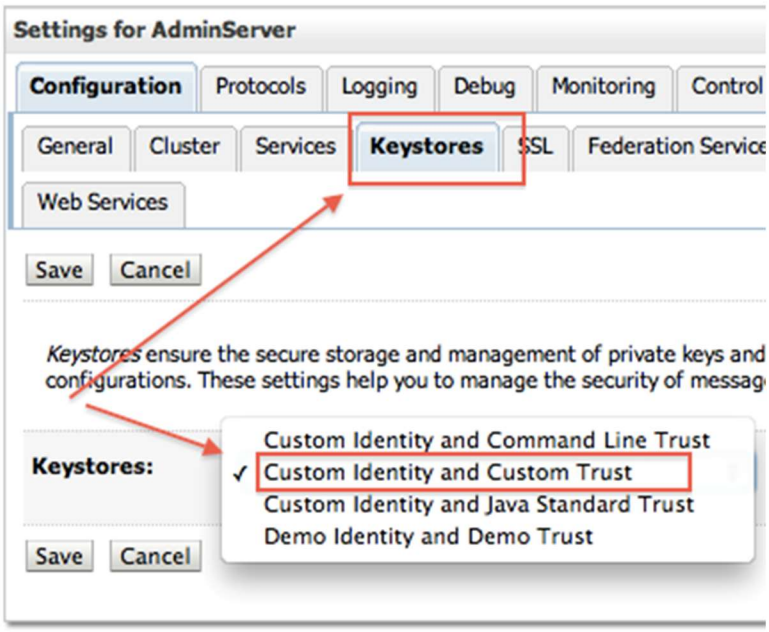
   If successful, you will see "Certificate reply was installed in keystore". You now have all the certificates installed to the keystore file. You just need to configure your server to use the keystore file.

A keystore file called mykeystore is created in the current directory. Copy this file to your domain directory and set the permissions appropriately.

5. **Enable the keystore in Weblogic** Phew! We finally have a keystore to use for SSL. Now it's time to configure it in Weblogic.

Change KeyStore type from "**Demo Identity and Demo Trust"** to "**Custom Identity and Custom Trust**"

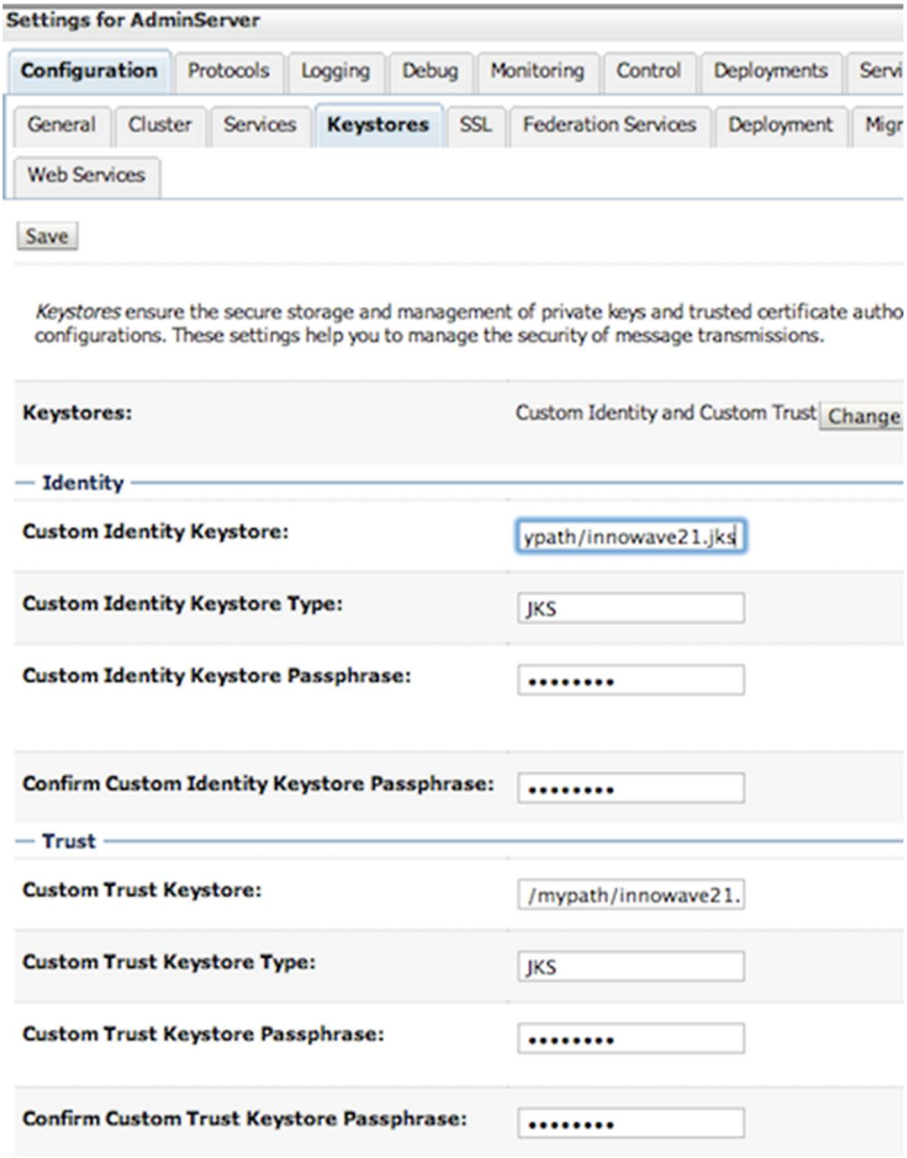
WebLogic Server Console -> Name of Server (for which you wish to configure SSL) -> Configuration -> KeyStores -> change (next to Key Stores)



1.2 Specify path of Identity KeyStore and Trust KeyStore

In steps above Trust Store (store containing Root and Intermediate CA) and Identity Store (store containing server certificate) are same i.e. **[keystore_name].jks** (innowave21.jks in my case)**.**

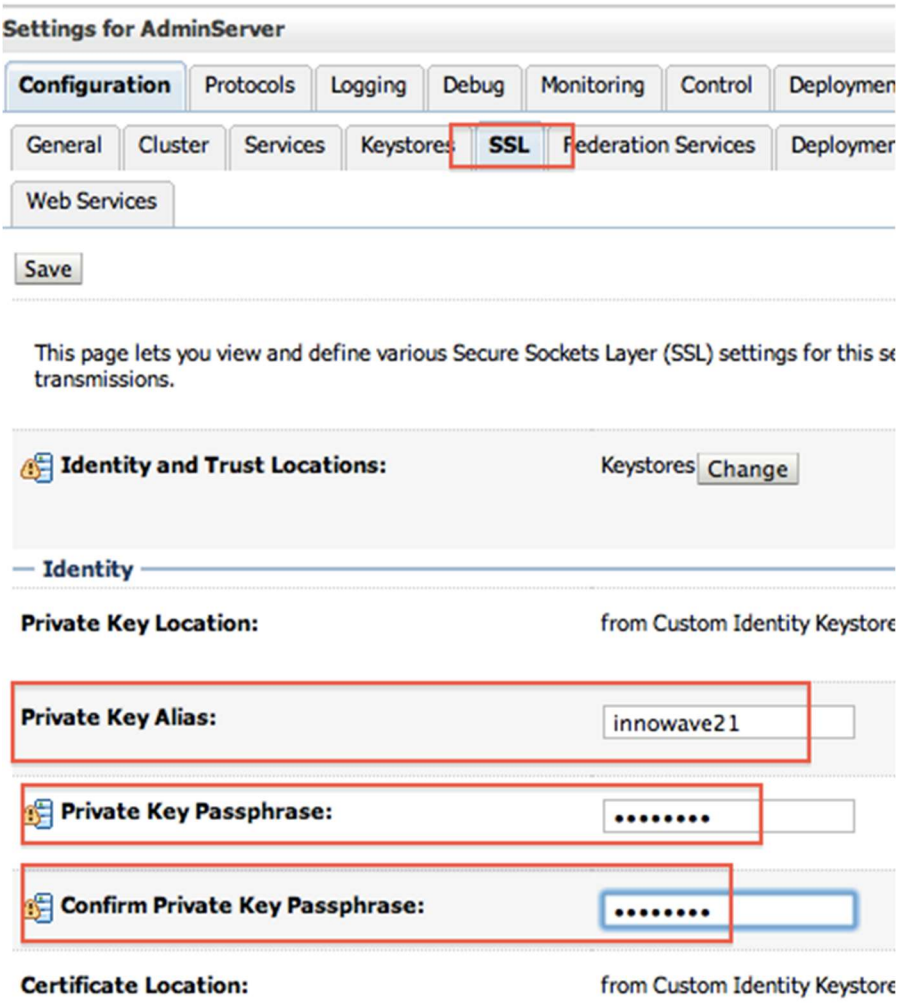
- Specify passphrase as password used for KeyStore



1.3 Specify Private Key Alias in WebLogic Server

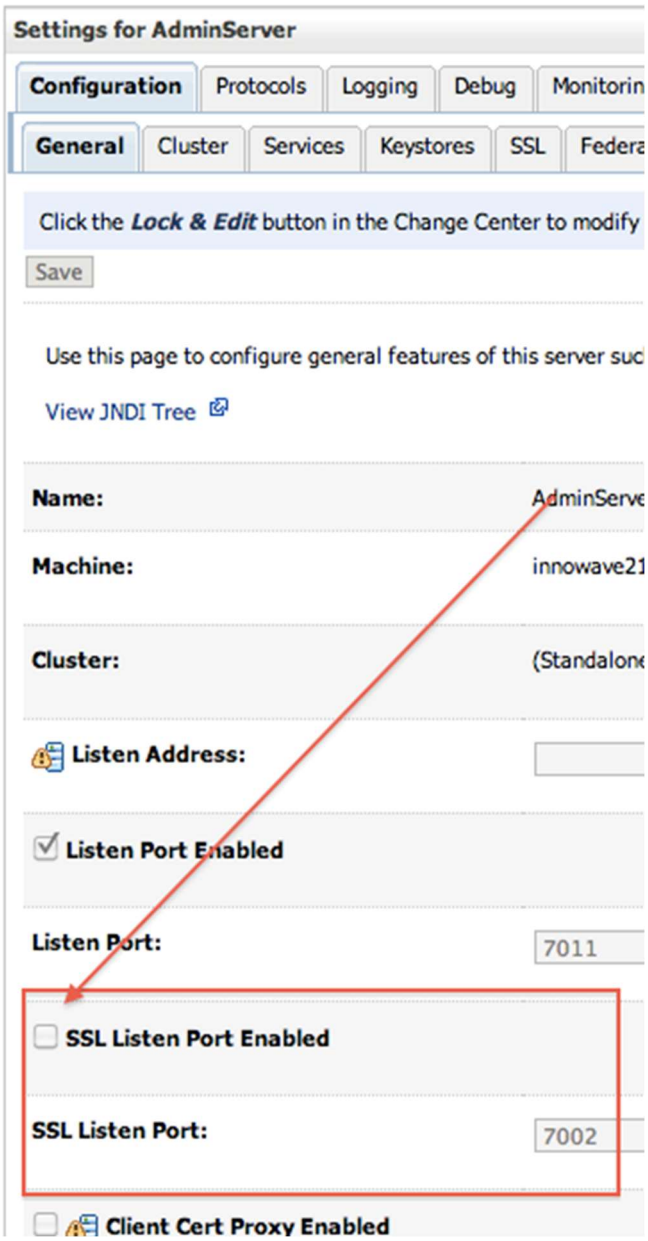
Enter the Alias you used during creation of certificate request and password of KeyStore

WebLogic Server Console -> Name of Server (for which you wish to configure SSL) -> Configuration -> SSL



1.4 Enable SSL in WebLogic Server

Finally enable SSL in WebLogic Server ; WebLogic Server Console -> Name of Server (for which you wish to configure SSL) -> Configuration -> General



9. Test SSL in WebLogic Server

https://: