**Demo SSL Configuration**

**To Open DemoIdentity file:**

keytool -v -list -keystore DemoIdentity.jks -storepass DemoIdentityKeyStorePassPhrase

* **Default Password:** DemoIdentityKeyStorePassPhrase

**To Open certificates:**

keytool -v -list -keystore cacerts -storepass changeit | less

* **Default Password:** changeit

**To check How many entries in Cacerts:**

keytool -v -list -keystore cacerts -storepass changeit | grep

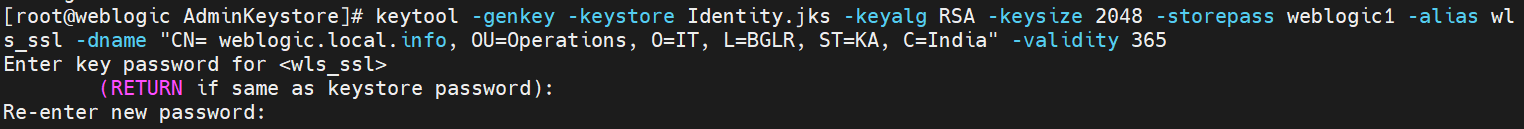
* **Default Password:** changeit

**To check How many Alias in Certificate:**

keytool -v -list -keystore Trust.jks -storepass weblogic1| grep -i Alias

**To Generate Identity store (Identity.jks):**

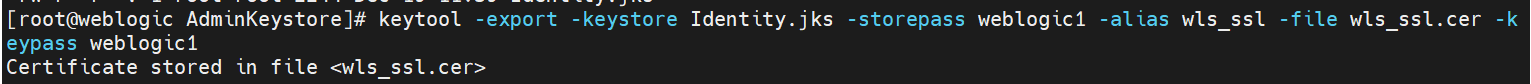
keytool -genkey -keystore Identity.jks -keyalg RSA -keysize 2048 -storepass weblogic1 -alias wls\_ssl -dname "CN= weblogic.local.info, OU=Operations, O=IT, L=BGLR, ST=KA, C=India" -validity 365





**Export Public Cert from Identity.jks file:**

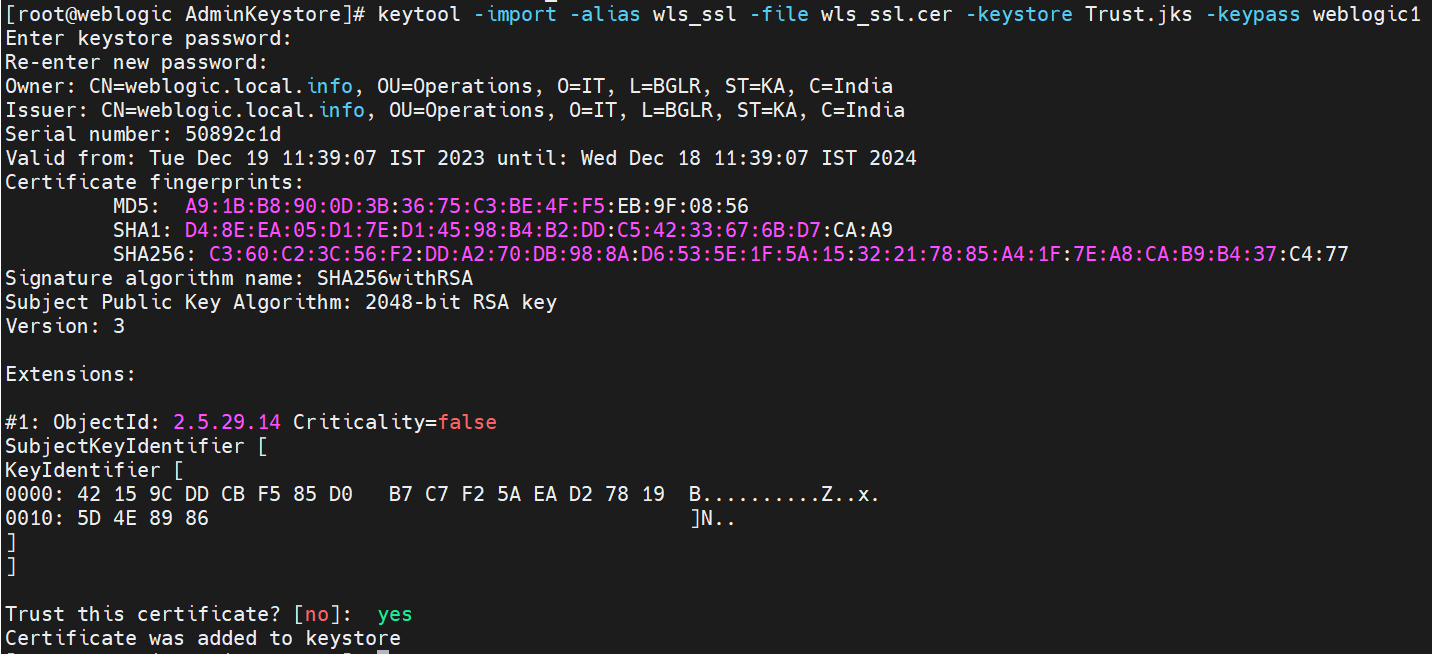
keytool -export -keystore Identity.jks -storepass weblogic1 -alias wls\_ssl -file wls\_ssl.cer -keypass weblogic1

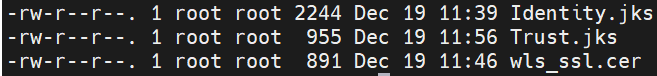




**Create Trust Keystore (Trust.jks):**

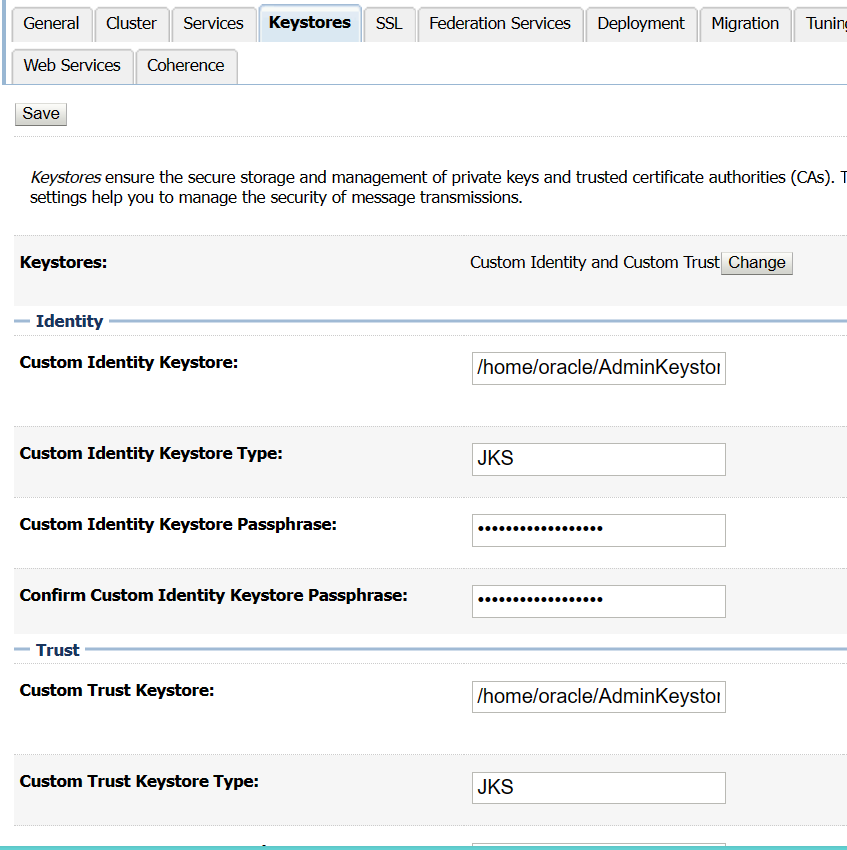
keytool -import -alias wls\_ssl -file wls\_ssl.cer -keystore Trust.jks -keypass weblogic1



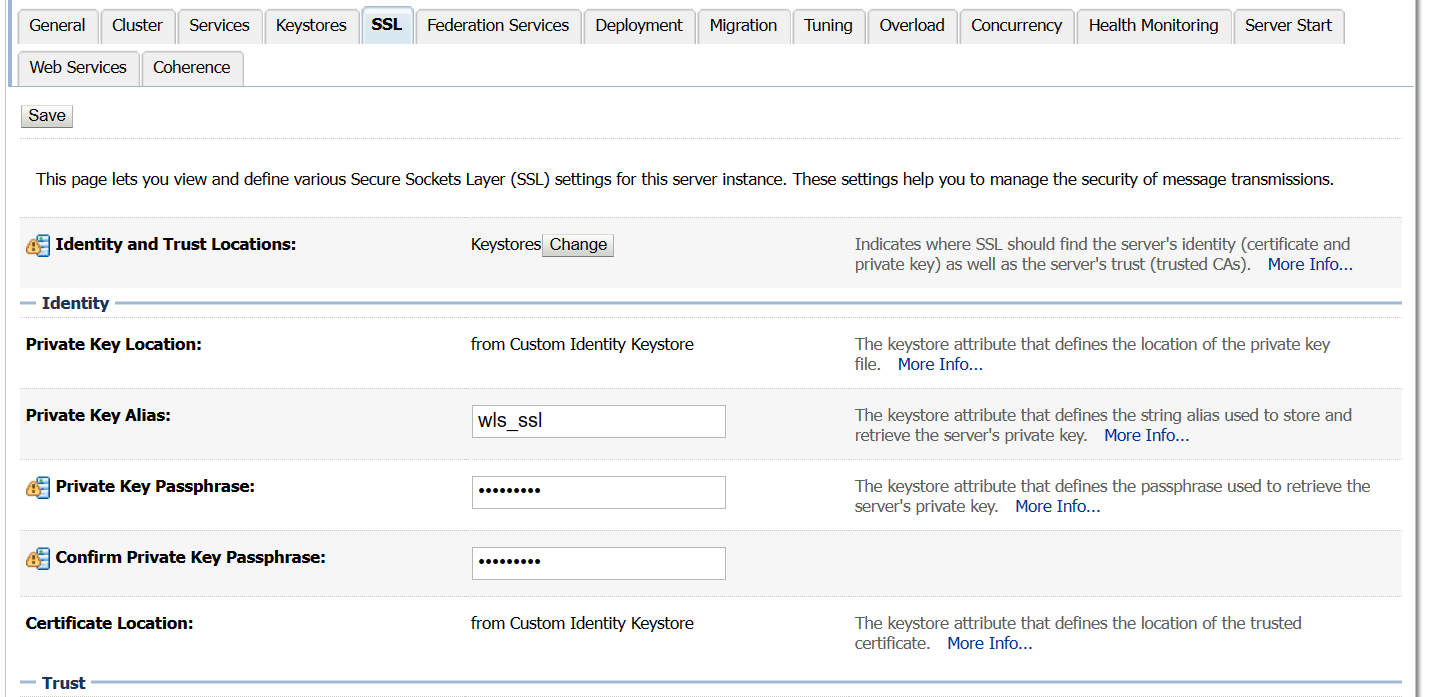


**In Console Change as below:**

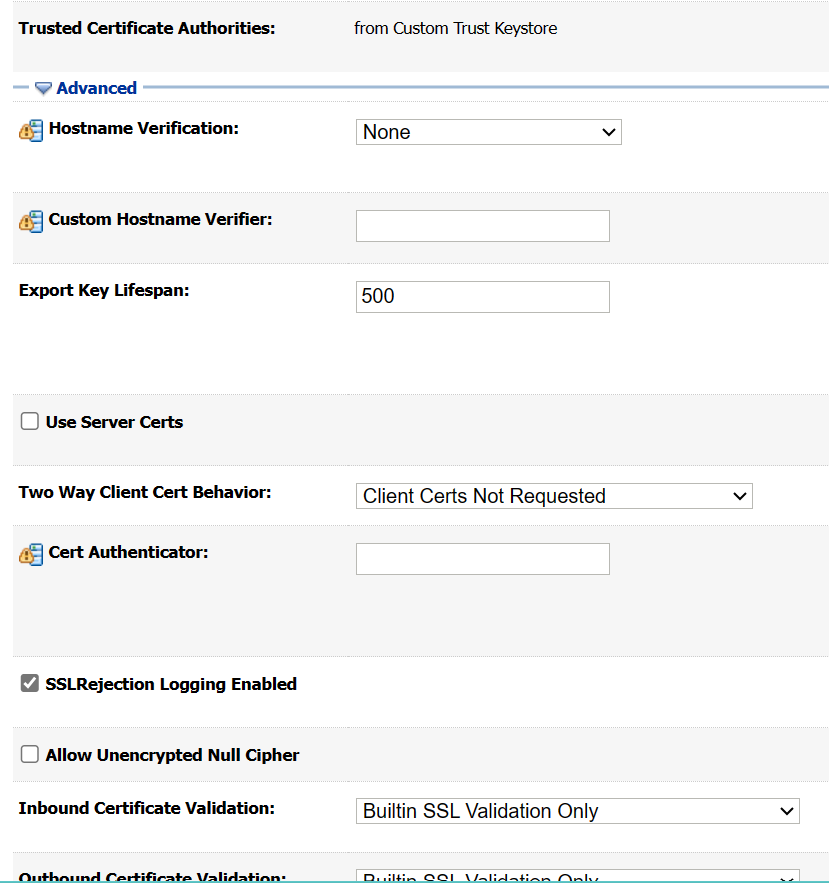
**KEYSTORES:** Update Identity & Trust store Locations.



**SSL:**



**In Advance Tab Disable Hostname Verification:**



**In General Tab Enable SSL Listen Port:** Port as per our availability

****

* We can provide same SSL configuration to managed servers by changing Identity & Trust location details.