RG-ePortal/RG-SMP is hosting with Jboss application server, the SSL certificate is managed by Java Keytool. Java keytool is installed by default with RG-ePortal/RG-SMP system. Below are the steps to import custom certificate for RG-ePortal system.(Same as RG-SMP)

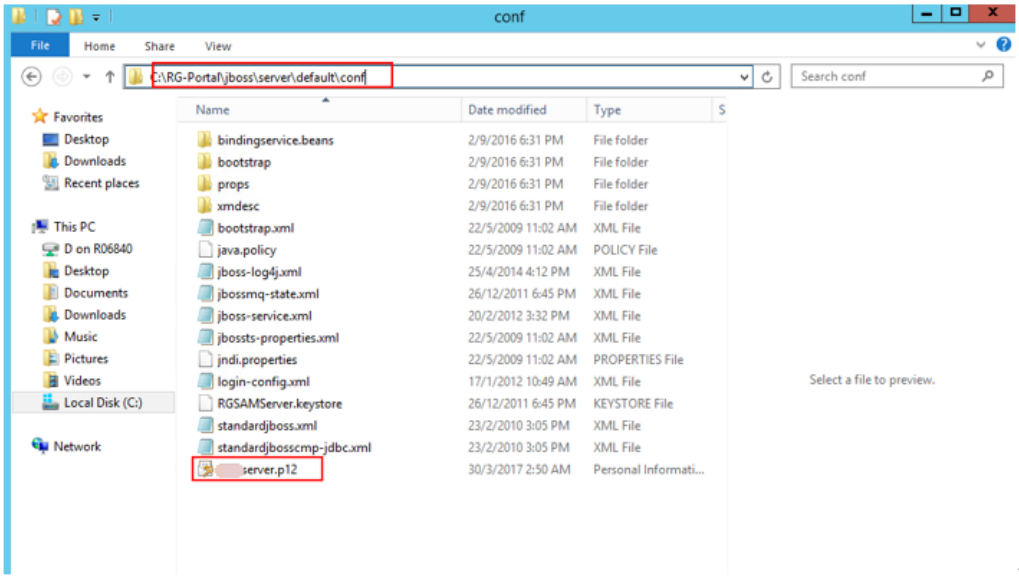
- **Utilize Java keytool to convert password protected PKCS12 certificate to JKS**

*As of security measurement, keytool only support to convert password protected PKCS12 to JKS, hence should request administrator to provide protected PKCS12 certificate. You may follow this guide to re-export the non password protected PKCS12 to password protected.

http://www.1st-setup.nl/wordpress/howto-change-password-on-pfx-certificate-using-openssl/

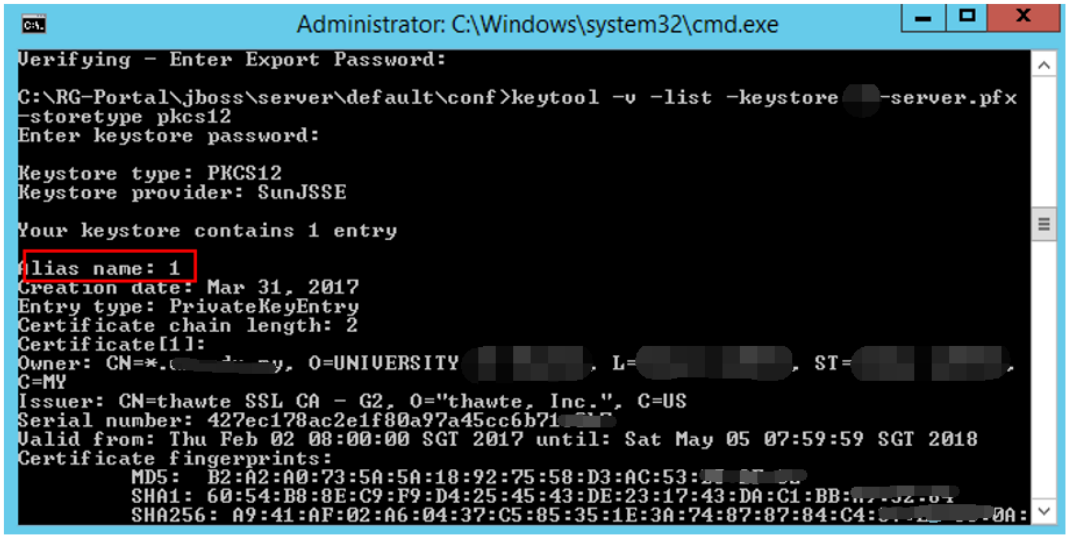
*All these steps should be carry out at RG-ePortal/RG-SMP server.

1. **Copy password protected PKCS12 format certificate file "XX-server.pfx" to C:\RG-Portal\jboss\server\default\conf**
   (SMP: C:\RG-SMP\jboss\server\default\conf)



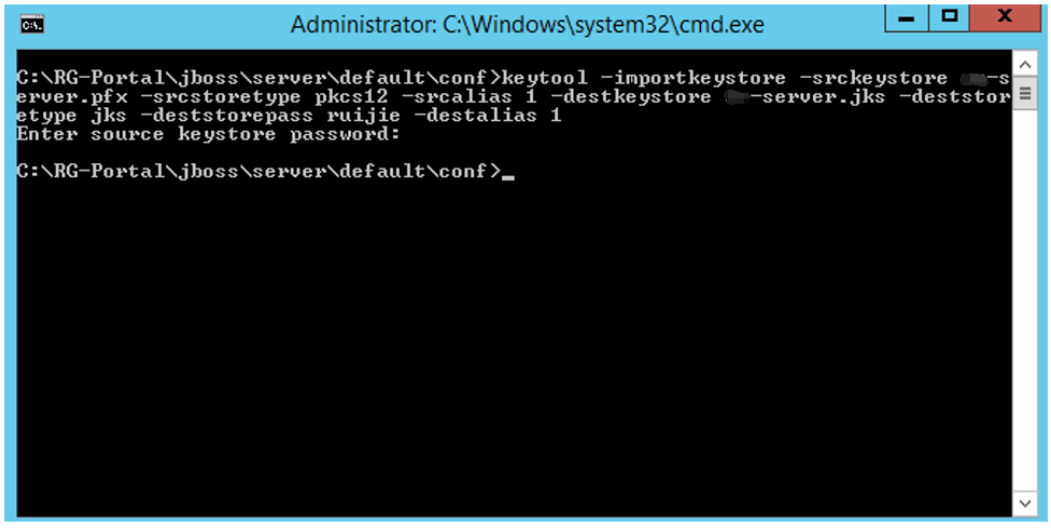
2. **Start command prompt, issue command to identify the certificate alias name**

Keytool -v -keystore XX-server.pfx -list -storestype pkcs12

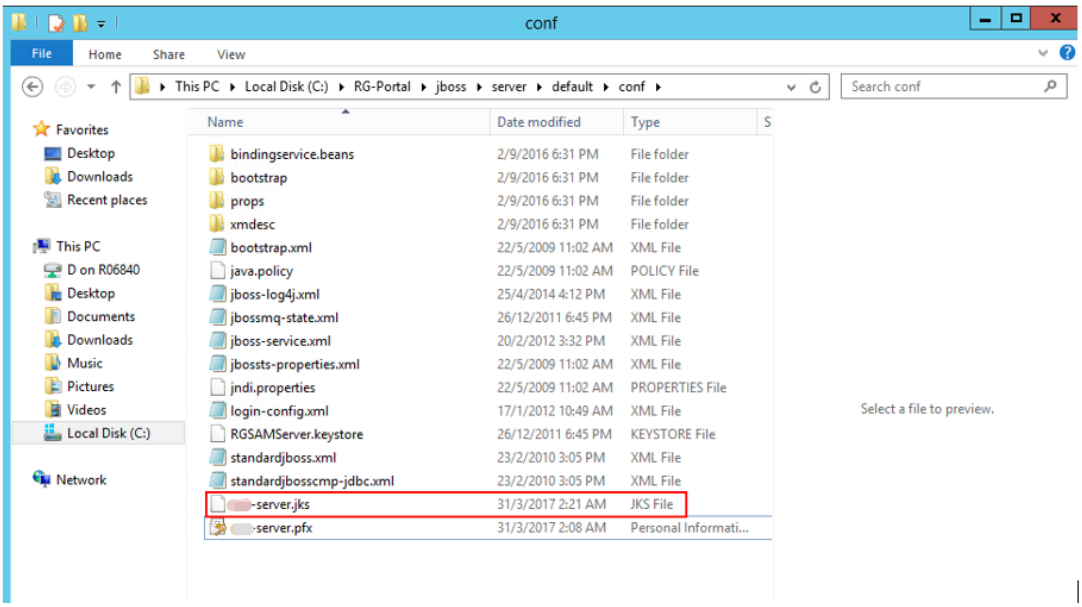


3. **Issue command to convert the PKCS12 file to JKS, with alias name "1", and JKS password "ruijie"**

keytool -importkeystore -srckeystore XX-server.pfx -srcstoretype pkcs12 -srcalias 1 destkeystore XX-server.jks -deststoretype jks -deststorepass Ruijie -destalias 1

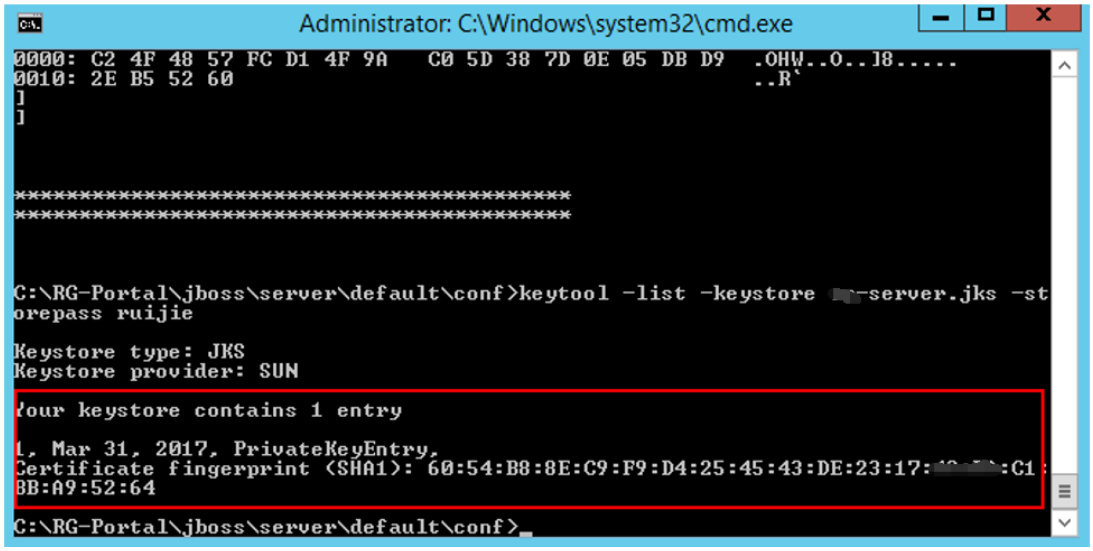


The JKS file will be generated after the command executed

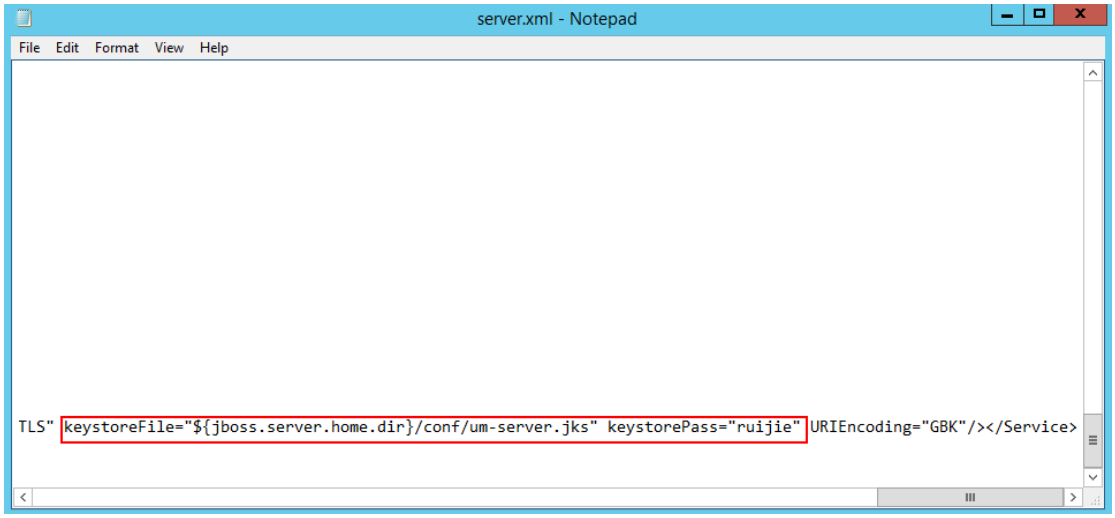


4. **Verify the JKS keystore with password "ruijie"**

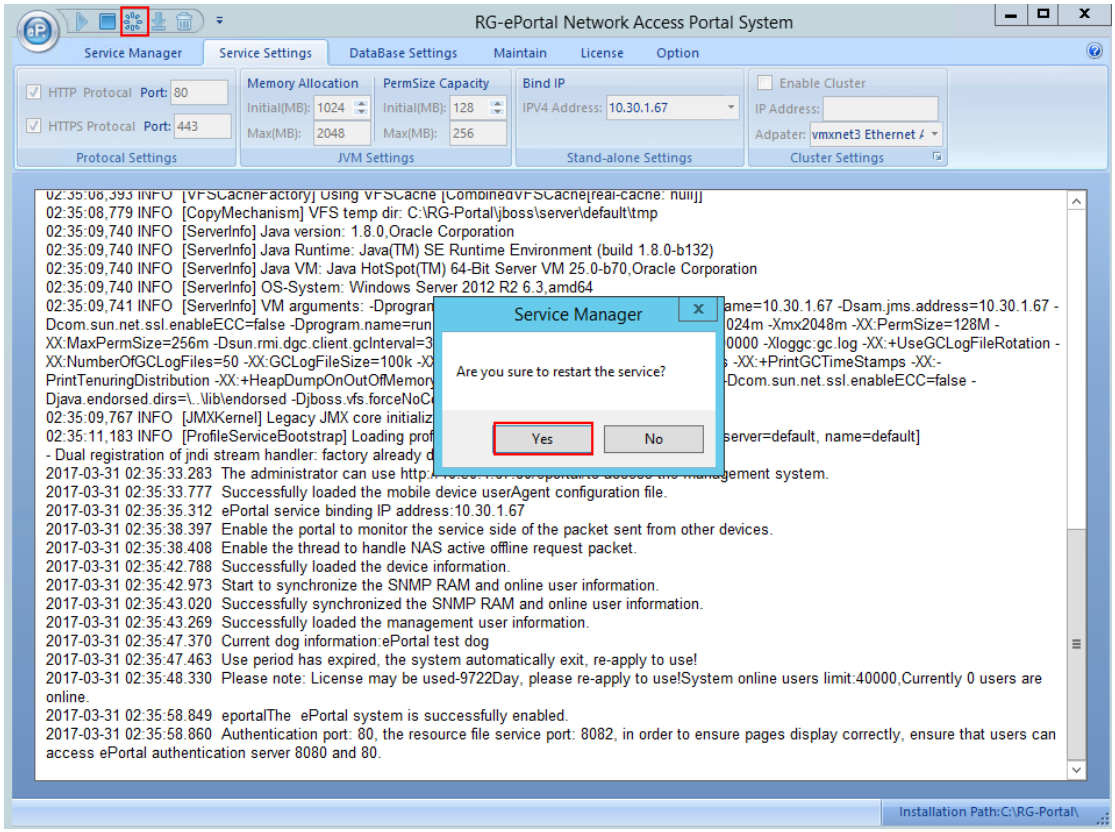
Keytool -list -keystore xx-server.jks -storepass ruijie



5. **Edit C:\RG-Portal\jboss\server\default\deploy\jbossweb-tomcat.sar\server.xml to use the new jks**
   (SMP: C:\RG-SMP\jboss\server\default\deploy\jbossweb.sar\server.xml, port 8443 and 433)



6. **Restart RG-ePortal service from the desktop service console**



New certificate will be used after service started successfully.