

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)

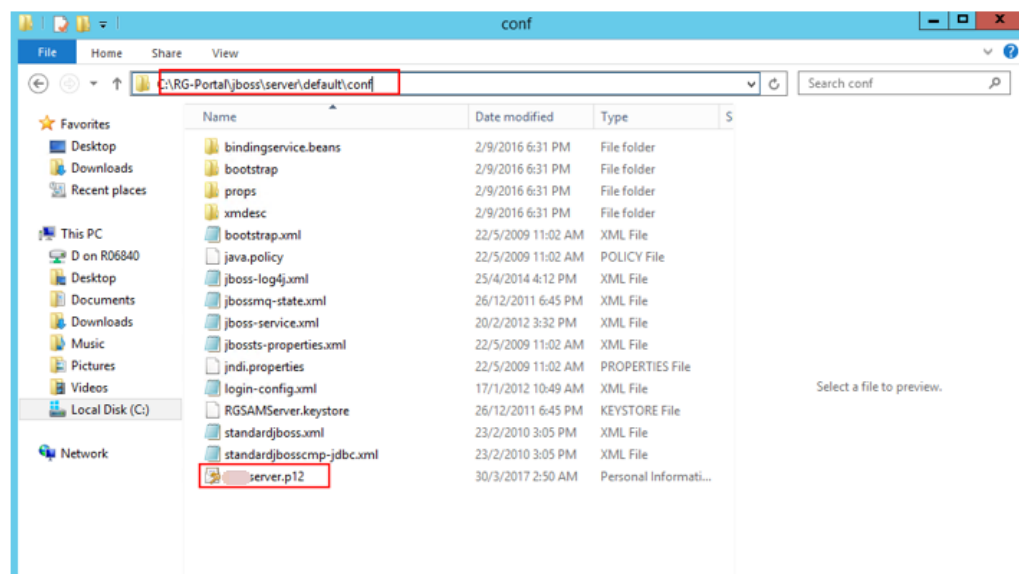
- **Utilize Java keytool to convert password protected PKCS12 certificate to JKS**

*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/>

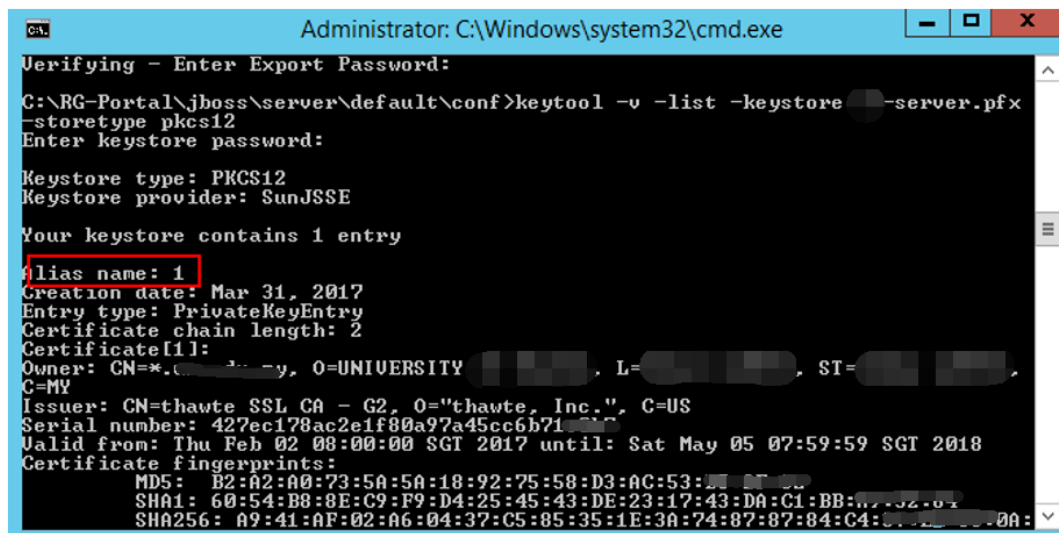
*All these steps should be carry out at RG-ePortal/RG-SMP server.

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 -storetype pkcs12



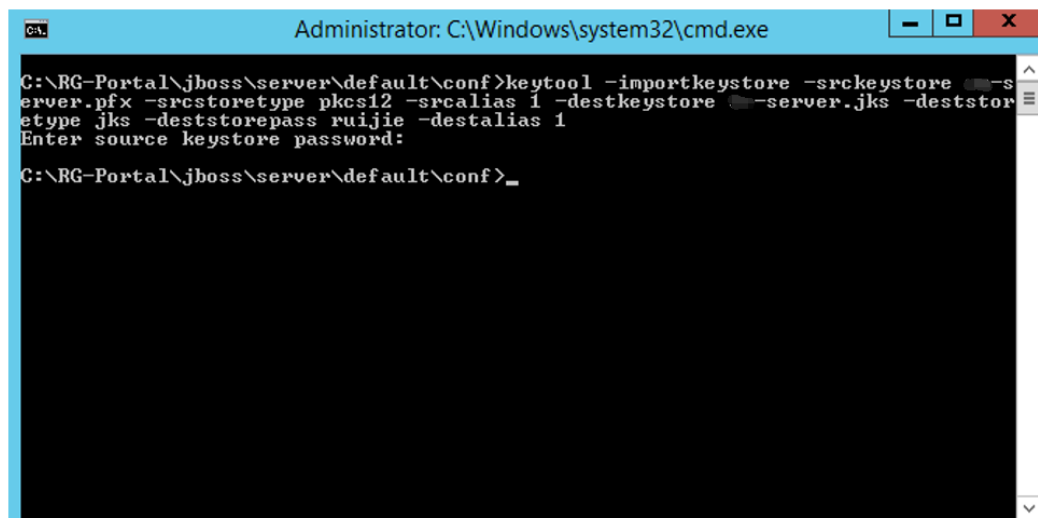
```
C:\RG-Portal\jboss\server\default\conf>keytool -v -list -keystore server.pfx
Enter keytool password:
Keystore type: PKCS12
Keystore provider: SunJSSE

Your keystore contains 1 entry

Alias name: 1
Creation date: Mar 31, 2017
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=*.com, O=UNIVERSITY, L=, ST=, C=MY
Issuer: CN=thawte SSL CA - G2, O="thawte, Inc.", C=US
Serial number: 427ec178ac2e1f80a97a45cc6b71
Valid from: Thu Feb 02 08:00:00 SGT 2017 until: Sat May 05 07:59:59 SGT 2018
Certificate fingerprints:
MD5: B2:A2:00:73:5A:5A:18:92:75:58:D3:AC:53:
SHA1: 60:54:B8:8E:C9:F9:D4:25:45:43:DE:23:17:43:DA:C1:BB:
SHA256: A9:41:AF:02:A6:04:37:C5:85:35:1E:3A:74:87:87:84:C4:0A:
```

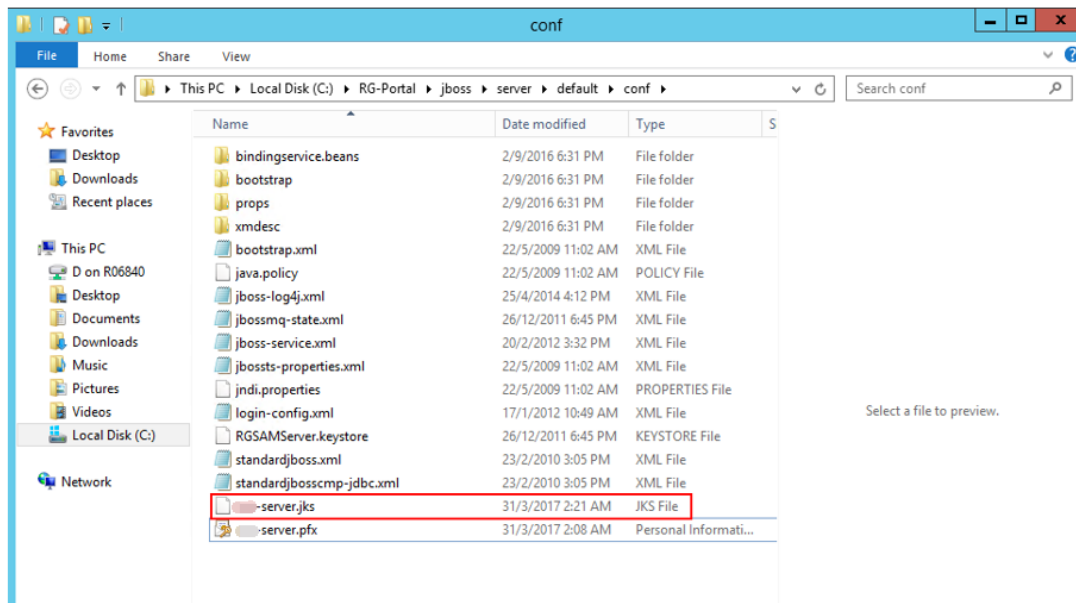
3. Issue command to convert the PKCS12 file to JKS, with alias name “1”, and JKS password “ruijie”

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



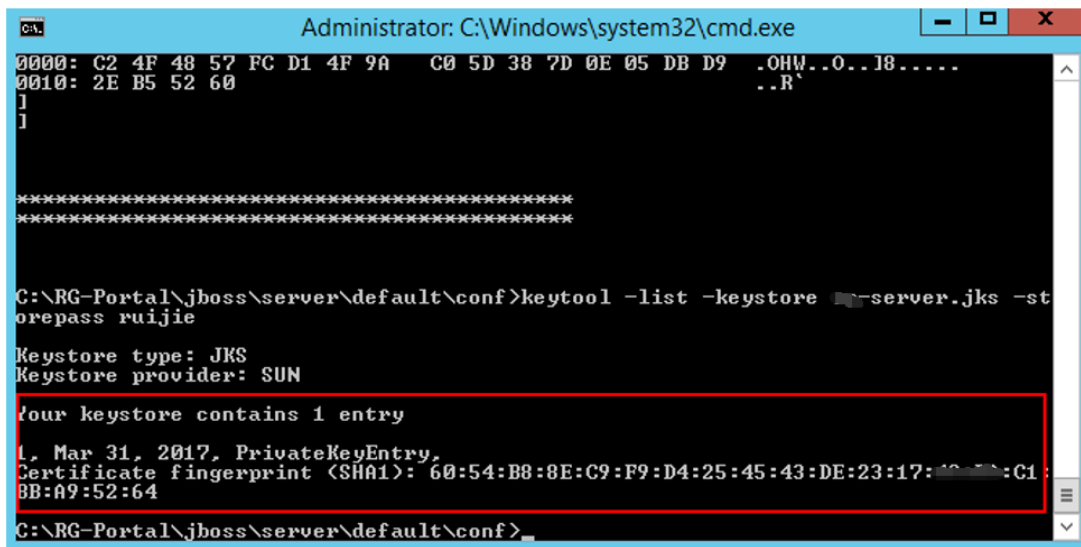
```
C:\RG-Portal\jboss\server\default\conf>keytool -importkeystore -srckeystore server.pfx -srcstoretype pkcs12 -srcalias 1 -destkeystore server.jks -deststoretype jks -deststorepass ruijie -destalias 1
Enter source keystore password:
C:\RG-Portal\jboss\server\default\conf>
```

The JKS file will be generated after the command executed

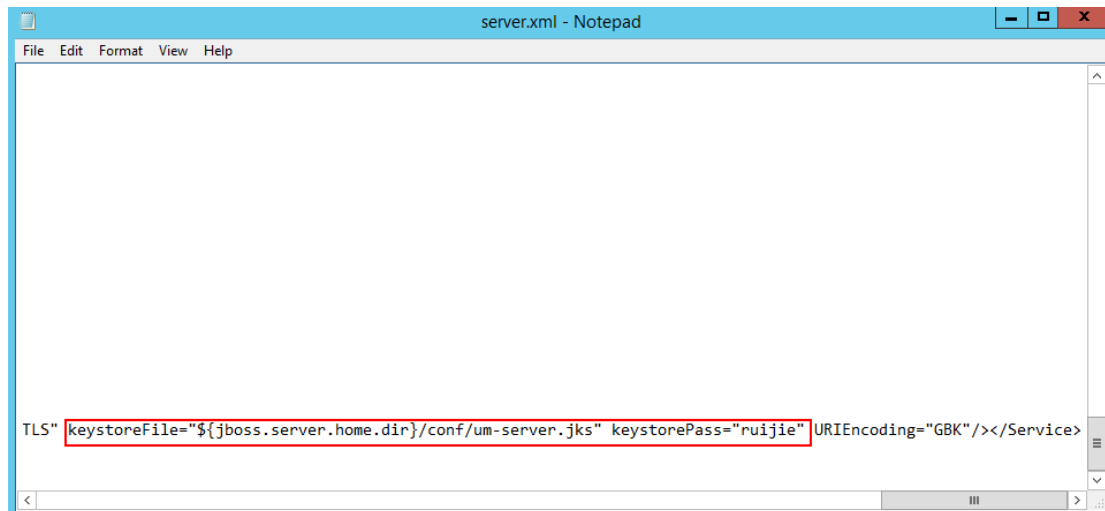


4. Verify the JKS keystore with password "ruijie"

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)



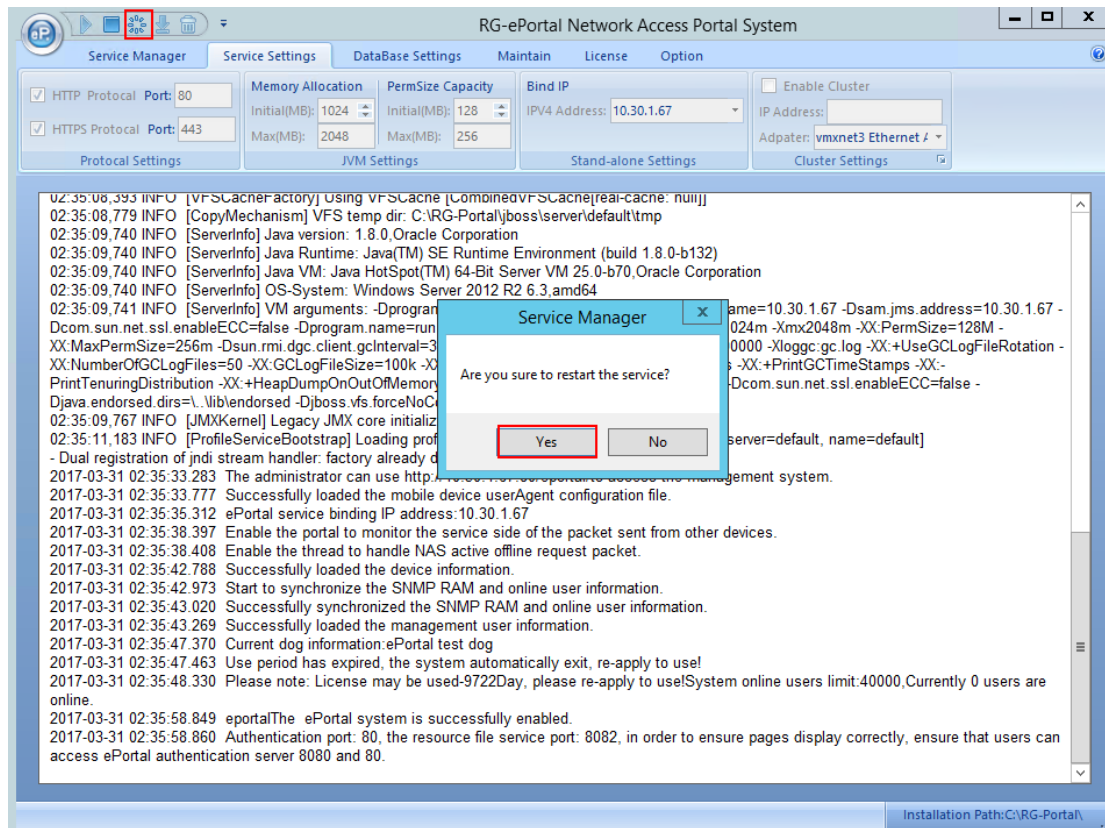
```
true" enableLookups="false" redirectPort="8443" acceptCount="100" connectionTimeout="20000" disableUploa
nnectionTimeout="20000" disableUploadTimeout="true" URIEncoding="GBK" ruijieType="5" />

th="false" keystoreFile="${jboss.server.home.dir}/conf/RG-SMP.keystore" keystorePass="ruijiesmp" sslProt
AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC

0000" disableUploadTimeout="true" URIEncoding="GBK" ruijieType="4" />

="false" keystoreFile="${jboss.server.home.dir}/conf/RG-SMP.keystore" keystorePass="ruijiesmp" sslProtoc
AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC
```

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



New certificate will be used after service started successfully.