

Instructions of HTTPS and SSL configuration on TomCat

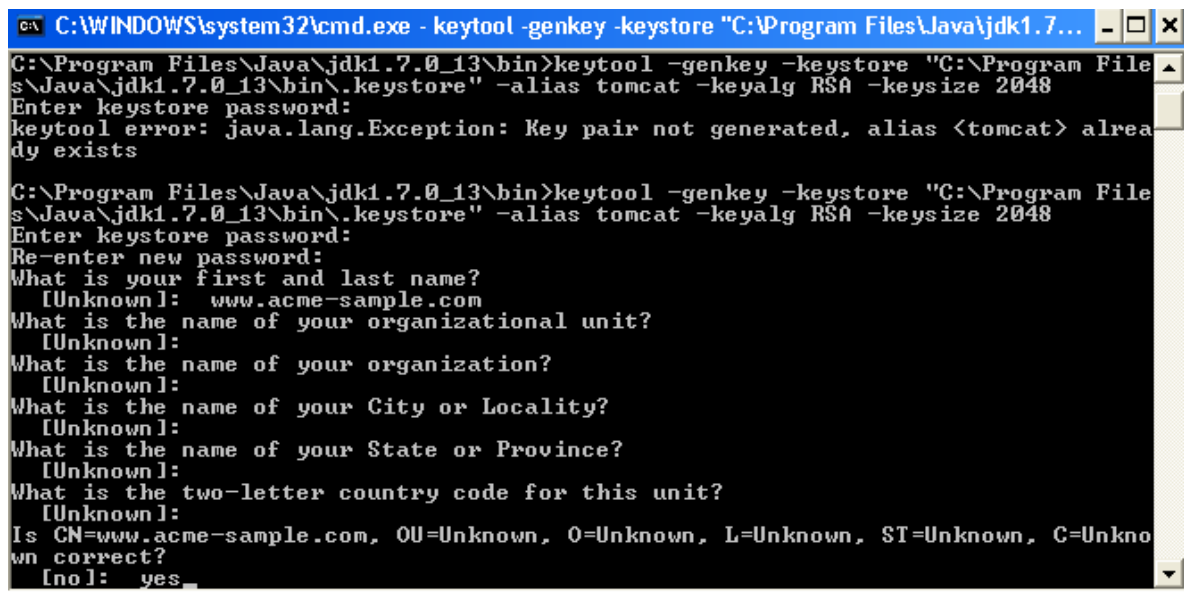
The following steps are strongly recommended to be followed for secure connection settings on TomCat 7 Server. This is a simulation. For real configuration, it would be necessary to ask for a certificate to any legal authority like Comodo or Let's Encrypt. Otherwise, The steps for real situation will be also indicated.

Step 1. We first go to Java Development Kit folder. For that, we have to make use of the Command Terminal.

```
"cd C:\Program Files\Java\jdk.1.7.0_13\bin"
```

Step 2. We have to generate a certificate which is only going to be used for our webpage. Every certificate is unique for each webpage.

```
keytool -genkey -keystore "C:\Program Files\Java\jdk1.7.0_13\bin\keystore" -alias tomcat -keyalg RSA -keysize 2048
```



```
C:\WINDOWS\system32\cmd.exe - keytool -genkey -keystore "C:\Program Files\Java\jdk1.7...
C:\Program Files\Java\jdk1.7.0_13\bin>keytool -genkey -keystore "C:\Program File
s\Java\jdk1.7.0_13\bin\keystore" -alias tomcat -keyalg RSA -keysize 2048
Enter keystore password:
keytool error: java.lang.Exception: Key pair not generated, alias <tomcat> alrea
dy exists

C:\Program Files\Java\jdk1.7.0_13\bin>keytool -genkey -keystore "C:\Program File
s\Java\jdk1.7.0_13\bin\keystore" -alias tomcat -keyalg RSA -keysize 2048
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: www.acme-sample.com
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=www.acme-sample.com, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unkno
wn correct?
[no]: yes_
```



Step 3. Generating Certificate from our domain. This will let us to get a real certificate.

```
keytool -certreq -keyalg RSA -alias tomcat -file csr.csr -keystore .keystore
```

Step 4. Importing certificate given by authority

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

Step 5. We have to modify server.xml file from TomCat with the following lines

```
<Connector SSLEnabled="true" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" keyAlias="tomcat"
keystoreFile="C:\Program Files\Java\jdk1.7.0_13\bin\KeyStore.jks"
keystorePass="T0mC@t=Admin1$trat0R"
maxThreads="150" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true" sslProtocol="TLS" />
```

Now, restart TomCat Server.

Step 5. Once Tomcat is restarted, we will be asked for confirmation. This happens because our keystore does not contain any of the legal certificates mentioned in this document's header.

For the access, we will use <https://localhost:8443/Acme-Madruga>

Extra step. Listing certificates from KeyStore

```
keytool -list -v -keystore .keystore
```