Tomcat SSL Certificate Deployment Guide (generate CSR by customer)

StartCom CA Limited

Contents

1.Generate the CSR by yourself

1.1 Generate the private key files

Use following command to generate private key file: Keytool -genkey -alias alias_name -keyalg RSA -keystore your_keystore -keysize 2048.

```
[root@localhost admin]# keytool -genkey -alias alias -keyalg RSA -keystore keyst
ore -keysize 2048
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  demo.startcom.com
What is the name of your organizational unit?
  [Unknown]:  StartCom
What is the name of your organization?
  [Unknown]:  support
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]:  IL
Is CN=demo.startcom.com, OU=StartCom, O=support, L=Unknown, ST=Unknown, C=IL cor
rect?
  [no]:  y

Enter key password for <alias>
        (RETURN if same as keystore password):
[root@localhost admin]#
```

1.2 Generate CSR file

Use following command to generate CSR file: Keytool -certreq -alias alias_name -file request.csr -keystore your_keystore.

```
[root@localhost local]# keytool -certreq -alias alias -file csr.csr -keystore ke
ystore
Enter keystore password:
[root@localhost local]# ls
```

1.3 Submit CSR file

When you apply the certificate on https://startssl.com/Account, submit your CSR .

Please submit your Certificate Signing Request (CSR):

You can use StartComTool.exe to generate the CSR.

Please paste CSR

CSR can not be empty

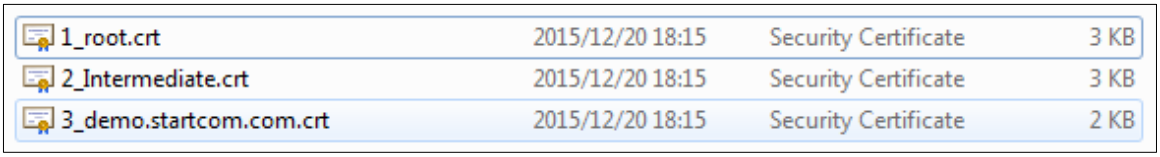
Generated by PKI system

submit

2.Installation of SSL certificate

2.1 Get SSL certificate

You will get a zip file after you apply the certificate from StartCom successfully. You should to extract the file, after extract the file you will get 4 files. We will need unzip the zip file Other server and we can get following files.



Import root CA, intermediate CA and public certificate into keystore.

For example:

keytool -import -trustcacerts -alias ***alias_name*** -file ***xxx.crt*** -keystore ***keystore_name***

1. Import root CA.

keytool -import -trustcacerts -alias ***root*** -file 1_root.crt -keystore ***your_keystore***

2. Import intermediate CA.

keytool -import -trustcacerts -alias ***intermediate*** -file 2_Intermediate.crt -keystore ***your_keystore***

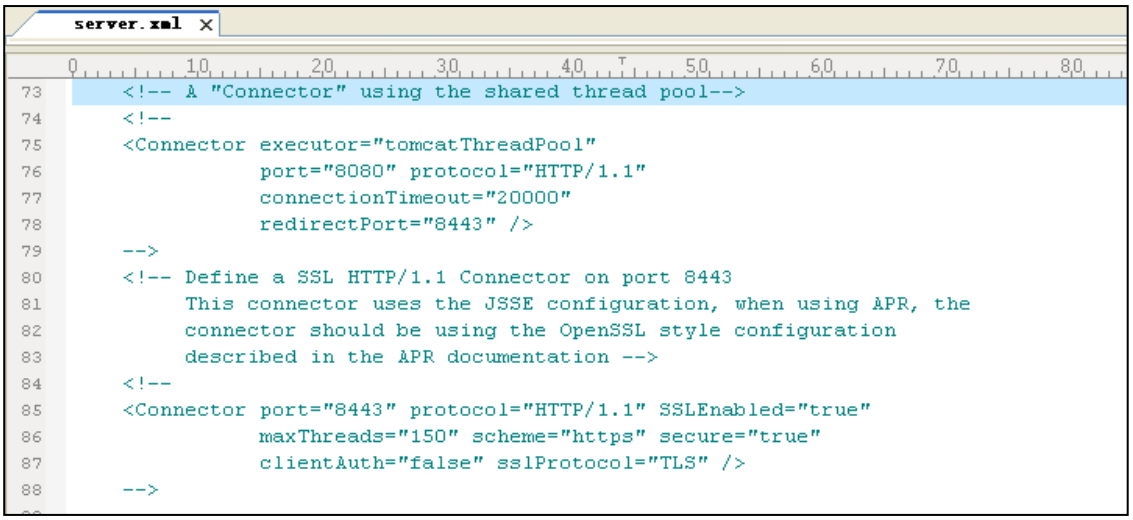
3. Import public certificate.

Keytool -import -trustcacerts -alias ***alias_name*** -file 3_domain.com.crt -keystore ***your_keystore***

(note: alis_name same to your_keystore alias_name)

2.2 Deploy SSL certificate

Find the file “Server.xml” in the Tomcat directory, which usually in conf file. Then open the file in a text editor, and then find the code.



<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="path/to/keystore" keystorePass="password" />

Usually <Connector port=“8443”……> is commented, we delete“<!-- -->”,and edit it, like: port, keystoreFile, keystorePass.

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol"
           maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS" KeystoreFile="conf/keystore" KeystorePass="password" />
```

Finally save the ‘server.xml’, and then restart the Tomcat and visit https://domain.com.

2.3 Test the SSL certificate.

Input the address in browser address bar: https://domain.com (the domain of the applied SSL certificate) Test your SSL certificate is installed successfully or not. If successful, the browser address bar will display a safety lock sign.

You could test your website’s certificate and configuration by https://www.ssllabs.com/ssltest/.

3.Backup of SSL certificate

Please save your_keystore file and remember your password.

4.Restore of SSL certificate

Repeat 2.2 operation.