



## Installing your Certificate on a Tomcat & Apache Server

### Step One

You will receive 3 files in a zip file from Comodo.

These must be imported in the correct order:

*Root*

*Intermediate CA*

*domain/site certificate*

In the following example please replace the example keystore name '*domain.key*' with your keystore name.

Use the keytool command to import the certificates as follows:

**keytool -import -trustcacerts -alias root -file (*insert root certificate file name*) - keystore *domain.key***

Use the same process for the Comodo certificate using the keytool command:

**keytool -import -trustcacerts -alias INTER -file (*insert intermediate CA file name*) - keystore *domain.key***

Use the same process for the site certificate using the keytool command, if you are using an alias then please include the alias command in the string. Example:

**keytool -import -trustcacerts -alias *yyy* (*where yyy is the alias specified during CSR creation*) -file *domain.crt* -keystore *domain.key***

### Step Two

Tomcat will first need a SSL Connector configured before it can accept secure connections.

Note: By default Tomcat will look for your Keystore with the file name *.keystore* in the home directory with the default password 'changeit'. The home directory is generally */home/user\_name/* on Unix and Linux systems, and *C:\Documents and Settings\user\_name\* on Microsoft Windows systems. -- It is possible to change the filename, password, and even location that Tomcat looks for the keystore. If you need to do this, pay special attention to #8 of Option 1 or #5 of Option 2 below.

#### Option 1 -- Add an SSL Connector using admintool:

1. Start Tomcat
2. Enter 'http://localhost:8080/admin' in a local browser to start admintool
3. Type a username and password with administrator rights
4. On the left select 'Service' (Java Web Services Developer Pack)
5. Select 'Create New Connector' from the drop-down list on the right
6. Choose 'HTTPS' in the 'Type' field
7. In the 'Port' field, enter '443'. This defines the TCP/IP port number on which Tomcat will listen for secure connections



8. Enter the Keystore Name and Keystore Password if (a.) your keystore is named something other than *.keystore*, (b.) if *.keystore* is located in a directory other than the home directory of the machine on which Tomcat is running, or if (c.) the password is something other than the default value of 'changeit'. If you have used the default values, you can leave these fields blank.
9. Select 'Save' to save the new Connector
10. Select 'Commit Changes' to save the new Connector information to the server.xml file so that it is available the next time Tomcat is started

**Option 2 -- Configure the SSL Connector in server.xml:**

1. Copy your keystore file (*your\_domain.key*) to the home directory (see the [Note](#) above)
2. Open the file Home\_Directory/conf/server.xml in a text editor
3. Uncomment the 'SSL Connector' Configuration
4. Make sure that the 'Connector Port' is 443
5. If your keystore filename is something other than the default file name (*.keystore*) and/or your keystore password is something other than default ('changeit') then you will need to specify the correct keystore filename and/or password in your connector configuration -- ex. `keypass="newpassword"`. When you are done your connector should look something like this:

```
<Connector port="443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreFile="/home/user_name/your_domain.key"
keypass="your_keystore_password"/>
```

6. Save the changes to server.xml
7. Restart Tomcat