

Java Based Web Servers CSR Creation and Installation

How to generate a CSR using Java Keytool

Step A -- Create a new Keystore

1. You will be using the keytool command to create your new key-CSR pairing. Enter the following:

```
keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore yourdomain.jks
```

'Yourdomain' is the name of the domain you are securing. However, if you are ordering a Wildcard Certificate, do not include * in the beginning of the filename as this is not a valid filename character.

2. You will be prompted for the DN information. Please note: when it asks for first and last name, this is not YOUR first and last name, but rather your domain name and extension(i.e., www.yourdomain.com). If you are ordering a Wildcard Certificate this must begin with *. (example: *.yourdomain.com)
3. Confirm that the information is correct by entering 'y' or 'yes' when prompted. Next you will be asked for your password to confirm. Make sure to remember the password you choose.

Step B -- Generate your CSR with your new keystore

1. Next, use keytool to actually create the Certificate Signing Request. Enter the following:

```
keytool -certreq -alias server -keyalg RSA -file yourdomain.csr -keystore yourdomain.jks
```

Again, 'yourdomain' is the name of the domain you are securing. (without the * character if you are ordering a Wildcard Certificate).

2. Enter the keystore password.
3. Then the SSL Certificate CSR file is created. Please [send the CSR file to us](#) for our process.

Installing the certificate to your Java Keystore

1. Save your SSL Certificate bundle file (your_domain_name.p7b) you received to the same folder where your keystore is. The one .p7b file contains all of the necessary certificates for your keystore.

*****NOTE***:** The certificate must be installed to the same keystore that was used to generate your CSR. You will get an error if you try to install it to a different keystore.

2. Type the following command to install the certificate file:

```
keytool -import -trustcacerts -alias server -file your_domain_name.p7b -keystore your_site_name.jks
```

If the certificate is installed correctly, you will receive a message stating "**Certificate reply was installed in keystore**"

If it asks if you want to trust the certificate. Choose **y** or **yes**.

Your keystore file (your_site_name.jks) is now ready to use on your server. Just configure your server to use it.