### Step 1: Use Keytool to Create a New Keystore

**Important:** We recommend you generate a new keystore following the process outlined in this section. Installing a new certificate to an old keystore often ends in installation errors or the SSL/TLS certificate not working properly. Before you begin this process, backup and remove any old keystores.

1. **Run Command**
   1. Navigate to the directory where you plan to manage your keystore and SSL/TLS certificate.
   2. Enter the command below.

**keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore your\_site\_name.jks**

* 1. In the command above, **your\_site\_name** should be the name of the domain you want to secure with this SSL/TLS certificate. When ordering a Wildcard certificate, do not include the asterisk (\*) in the filename (e.g., your\_site\_name). The asterisk is not a valid keytool character.
  2. **Create a Password**
     1. When prompted, create a password for your Keystore.
     2. **Note:** You will specify this password in your Tomcat configuration file and then use it to generate your CSR and to import your certificate.
     3. Store this password somewhere safe, such as a trusted and secured password manager.
  3. Enter your SSL/TLS certificate information.
  4. **Important:** When prompted for the first and last name, DO NOT type your first and last name. Instead, type the Fully Qualified Domain Name (FQDN) for the site you are securing with this certificate (e.g., *www.yourdomain.com*, *mail.yourdomain.com*). Are you are ordering a Wildcard Certificate? Then your FQDN must begin with an asterisk (\*). (e.g.,*\*.yourdomain.com*).
  5. Enter your Organization information.
  6. When prompted to verify your information, type **y** or **yes** to confirm.
  7. When asked for a "key password for <server>", press enter to use the password you just created for the keystore file.

1. Your keystore file, your\_site\_name.jks, is now created and in your current working directory.

### Step 2: Generate a Certificate Signing Request (CSR) from your New Keystore

1. **Run Command**

a.In Keytool, type the following command:

**keytool -certreq -alias server -file csr.txt -keystore your\_site\_name.jks**

In the command above, **your\_site\_name** should be the name of the keystore file you created in [Step 1: Use Keytool to Create a New Keystore](https://www.digicert.com/csr-ssl-installation/tomcat-keytool.htm#step_1)

b. When prompted, enter the password you created earlier (when you created your new keystore).

* 1. In your current directory, csr.txt (e.g., *your\_site\_domain.txt*) now contains your CSR.

1. **Save and Back-up Your Keystore File**
   1. Take note of the path to your keystore file (your\_site\_domain.jks) as your SSL/TLS certificate will be installed to it later.
   2. We recommend that you create a back-up copy of your Keystore file (your\_site\_domain.jks) before continuing. Having a back-up of the Keystore file can help resolve issues that may occur during certificate SSL/TLS installation.
2. **Order Your SSL/TLS Certificate**
   1. Open the .csr file you created with a text editor.
   2. Copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags, and paste it in to the any CA order form
   3. Make sure that when you **Select Server Software**, you select **Tomcat**.

**Tomcat SSL/TLS Certificates, Guides, & Tutorials**

* 1. [**BUY NOW**](https://www.digicert.com/order/order-1.php?prod=1)[**LEARN MORE**](https://www.digicert.com/tomcat-ssl.htm)

1. **Install Certificate**
2. After you’ve received your SSL/TLS certificate from CA, you can install it on your Tomcat server.

## II. Tomcat Server: Install and Configure Your SSL/TLS Certificate

Need to create your certificate signing request (CSR)? See [Tomcat Server: Create Your CSR with Java Keytool](https://www.digicert.com/csr-ssl-installation/tomcat-keytool.htm#create_csr_keytool).

After we've validated and issued your SSL/TLS certificate, you can install it on your Tomcat server (where the CSR was generated) and then configure the server to use the certificate.

### Step 1: Use Java Keytool to Install Your SSL/TLS Certificate to the Keystore

1. **Download Certificate**
   1. Log in to your any CA account.
   2. On the **My Orders** tab, click the order number and then click **Download**.
   3. Save the your\_domain\_com.p7b certificate to the same directory as your Java keystore.
   4. **Note:** If you used our Keytool CSR Command Generator or followed our instructions to generate your CSR, the Keystore file is named **your\_site\_name.jks**.
2. **Install the Certificate File in Your Keystore**
3. **Important:** You must install the SSL/TLS Certificate file to the same keystore and under the same alias name (e.g., "**-alias server**") that you used to generate your CSR. If you try to install the certificate to a different keystore or under a different alias, the import command will not work.
   1. Run the command below to import the certificate into your keystore.
   2. **keytool -import -alias server -file your\_site\_name.p7b -keystore your\_site\_name.jks**
   3. In the command above, **your\_site\_name.p7b** should be the name of the certificate file you downloaded, **your\_site\_name.jks** should be the name of the keystore file you created in [Step 1: Use Keytool to Create a New Keystore](https://www.digicert.com/csr-ssl-installation/tomcat-keytool.htm#step_1), should be the alias name you used when generating your CSR.
   4. You should get a confirmation that the ***"Certificate reply was installed in keystore***".
   5. If you are prompted to trust the certificate, type **y** or **yes**.
   6. The installation of this file loads all necessary certificates to your keystore.
4. Your keystore file (your\_site\_name.jks) is now ready to be used on your Tomcat Server. Now, you are ready to configure your server to use it.

### Step 2: Configure Your SSL/TLS Connector

Before your Tomcat server can accept secure connections, you need to configure an SSL Connector.

1. Use a text editor to open the Tomcat server.xml file.
2. Typically, the server.xml file is in the conf folder in your Tomcat’s home directory.
3. Locate the connector you want the new Keystore to secure.
4. Usually, a connector with port 443 or 8443 is used; see step 4. Note that you may need to uncomment the connector – remove the comment tags (<!-- and -->).
5. **Configure your Tomcat connector.**
6. Make sure to specify your new keystore filename and password in your connector configuration.
7. When you are done, your connector should look something like the example below.
8. **Note:** Are you using a version of Tomcat prior to Tomcat 7? Then you need to change the **keystorePass** to **keypass**.
9. **<Connector port="443" maxHttpHeaderSize="8192" maxThreads="100" minSpareThreads="25" maxSpareThreads="75" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" SSLEnabled="true" clientAuth="false" sslProtocol="TLS" keyAlias="server" keystoreFile="/home/user\_name/your\_site\_name.jks" keystorePass="your\_keystore\_password" />**
10. In the connector configuration above, **keystoreFile** is the full path to your keystore file, **keystorePass** is the password you used to create your keystore, and **keyAlias** is the same alias name (e.g., "server") that you used to generate your CSR.
11. Save your changes to the server.xml file.
12. Restart the Tomcat service.
13. Congratulations! You've successfully installed your SSL certificate.