SSL Certificate – Tomcat

Installation Guide

webnic
accelerate your business

Please select your version

Installation Instructions for Tomcat using PKCS#7 format

Installation Instructions for Tomcat using X.509 format

Installation Instructions for Tomcat using PKCS#7 format

NOTE: When using the PKCS#7 format there is no need to download and install
the Intermediate CA Certificates separately as this format
already includes all files: Your End Entity Certificate and Intermediate CA certificate.

Step 1: Download the SSL Certificate

Sign into your **Symantec Trust Center** account and download the certificate by following the steps here.

NOTE: Ensure that the **PKCS#7 format** has been selected when downloading the certificate.

Make sure there are 5 dashes to either side of the BEGIN PKCS#7 and END PKS#7 and that no white space, extra line breaks or additional characters have been inadvertently added.

To follow the naming convention for Tomcat, rename the certificate filename with
the **.p7b** extension. For example: **ssl_cert.p7b**

NOTE: If you want to install the Certificate sent from Symantec via e-mail, follow the installation instructions from <a href=”https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&actp=CROSSLINK&id=INFO234”>here</a>.

Step 2: Import the SSL Certificate into the Keystore:

Enter the following command to import your SSL Certificate:

```
keytool -import -alias your_alias_name -trustcacerts -file ssl_cert.p7b -keystore
your_keystore_filename
```

NOTE: The **alias name** and **Keystore name** in this command must be the **same** as the alias name and Keystore name
used during the **generation of the private key and CSR**.

NOTE: During the import you might get following error: Error: "java.lang.Exception: Input not an X.509 certificate".

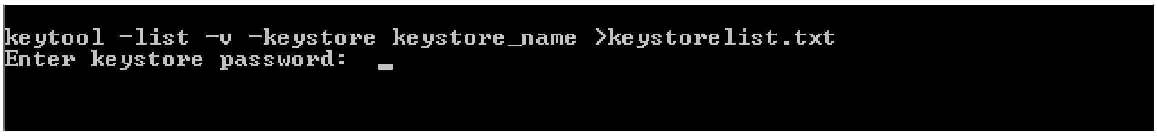
To troubleshoot the error please refer to the steps from here.

Step 3: Confirm the contents of the keystore

Enter the following command to list the contents of the keystore:

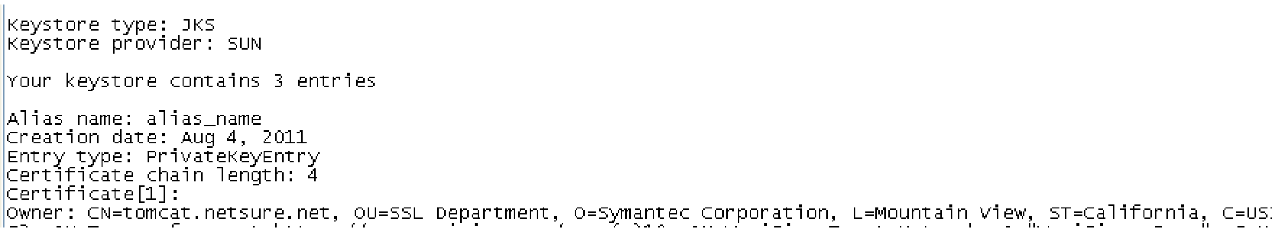
keytool -list -v -keystore your_keystore_filename >output_filename

For Example:



```
keytool -list -v -keystore keystore_name >keystorelist.txt
Enter keystore password:  _
```

View the contents of the output file.



```
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 3 entries

Alias name: alias_name
Creation date: Aug 4, 2011
Entry type: PrivateKeyEntry
Certificate chain length: 4
Certificate[1]:
Owner: CN=tomcat.netsure.net, OU=SSL Department, O=Symantec Corporation, L=Mountain View, ST=California, C=US:
```

Verify the following information:

The SSL certificate is imported into the alias with the "Entry Type" of **PrivateKeyEntry** or **KeyEntry**. If not, please import the certificate into the Private Key alias.

The **Certificate chain length** is **4**

Step 4: Configure Tomcat server

Once the certificates are imported into the keystore, configure your server.xml to enable SSL following the steps here.

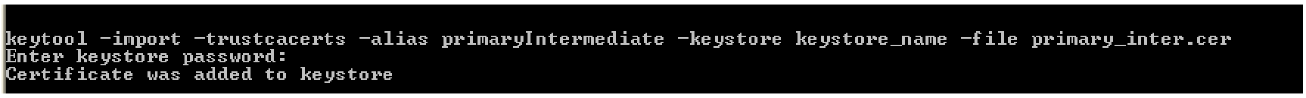
Installation Instructions for Tomcat using X.509 format

Step 1: Download and Install Symantec CA Certificates:

1. Download the Intermediate CA certificate.
2. Select the appropriate Intermediate CA certificate for your SSL Certificate type.
3. Copy the Intermediate CA certificate and paste it in a text editor such as Notepad or Vi.
4. Save the file as **intermediate.cer**
5. Use the following command to import this Certificate into the keystore:

   keytool -import -trustcacerts -alias Intermediate -keystore your_keystore_filename -file intermediate.cer

   For Example:



```
keytool -import -trustcacerts -alias primaryIntermediate -keystore keystore_name -file primary_inter.cer
Enter keystore password:
Certificate was added to keystore
```

Step 2: Obtain and Install the SSL Certificate

1. Symantec will send the SSL Certificate via e-mail. If the certificate is an attachment (Cert.cer), you can use the file.
   If the certificate is in the body of the email, copy and paste it into a text file using Vi or Notepad.

   When downloading the certificate, select the **X.509** format and copy only the **End Entity Certificate**.

   The text file should look like:

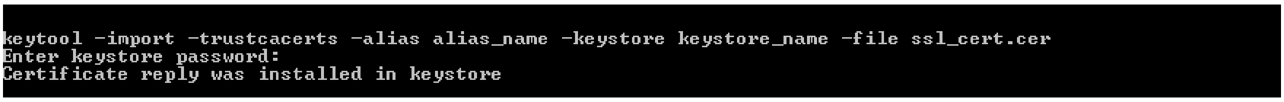
   -----BEGIN CERTIFICATE-----

   [encoded data]
   -----END CERTIFICATE-----

2. To follow the naming convention for Tomcat, rename the certificate filename with the **.cer** extension. For example: **ssl_cert.cer**
3. Enter the following command to import your SSL Certificate:

   keytool -import -trustcacerts -alias your_alias_name -keystore your_keystore_filename -file your_certificate_filename

   For Example:



```
keytool -import -trustcacerts -alias alias_name -keystore keystore_name -file ssl_cert.cer
Enter keystore password:
Certificate reply was installed in keystore
```

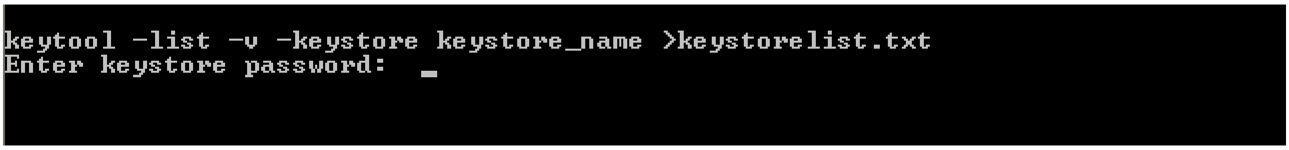
NOTE: The alias name in this command must be the same as the alias name used during the generation of the private key and CSR.

Step 3: Confirm the contents of the keystore

1. Enter the following command to list the contents of the keystore:

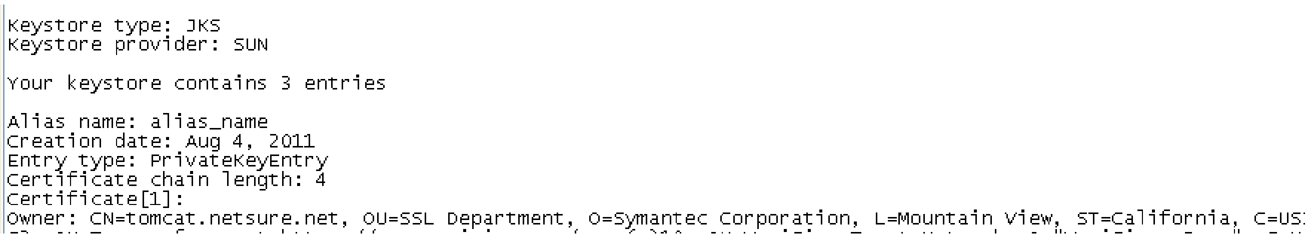
   keytool -list -v -keystore your_keystore_filename >output_filename

   For Example:



```
keytool -list -v -keystore keystore_name >keystorelist.txt
Enter keystore password:  _
```

2. View the contents of the output file



```
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 3 entries

Alias name: alias_name
Creation date: Aug 4, 2011
Entry type: PrivateKeyEntry
Certificate chain length: 4
Certificate[1]:
Owner: CN=tomcat.netsure.net, OU=SSL Department, O=Symantec Corporation, L=Mountain View, ST=California, C=US
```

3. Verify the following information:

   The SSL certificate is imported into the alias with the "Entry Type" of **PrivateKeyEntry** or **KeyEntry**. If not, please import the certificate into the Private Key alias.

   The **Certificate chain length** is **4**.

Step 4: Configure Tomcat server

Once the certificates are imported into the keystore, configure your server.xml to enable SSL following the steps here.