
Tomcat SSL Certificate Deployment Guide



沃通电子认证服务有限公司

WoSign CA Limited

Content

1、 Installation of SSL certificate	3
1.1 Get SSL certificate.....	3
1.2 Install the environment of SSL certificate.....	3
1.3 Deploy SSL certificate	5
2. Install Secure signature	7
2.1 Install English Secure signature.....	7
3、 Backup of SSL certificate	7
4、 Restore of SSL certificate	7

Contact information of technical support

Email of technical support: support@wosign.com

Hotline of technical support: +86-755-8600 8688

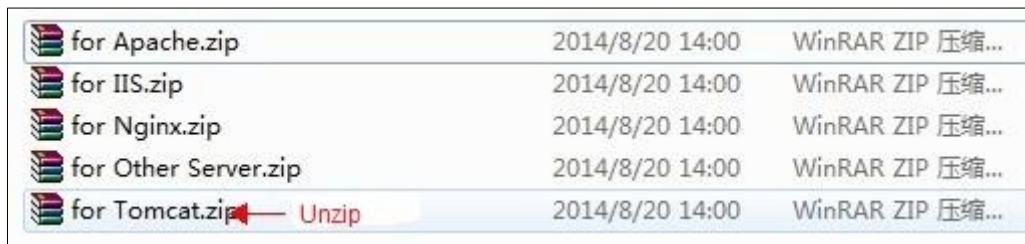
Website of technical support: <https://bbs.wosign.com>

Company official website address: <https://www.wosign.com>

1、 Installation of SSL certificate

1.1 Get SSL certificate

You will get a zip file with password after you apply the certificate from wosign successfully. You need to enter the password to extract the file, after extract the file you will get 5 files: **for Apache、 for IIS、 for Nginx、 for Other Server, for tomcat. These are different formats for different servers.** We will need to use the jks format certificate from for tomcat.



for Apache.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for IIS.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Nginx.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Other Server.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Tomcat.zip	2014/8/20 14:00	WinRAR ZIP 压缩...

Figure 1

1.2 Install the environment of SSL certificate.

First visit Tomcat official website (<http://tomcat.apache.org/>) We can download different application packages according to your system, we take the Windows system as an example. We download the apache-tomcat-7.0.29 version for the Windows version. Download Tomcat and extract it to one of the partition. Enter the root directory of apache-tomcat-7.0.29 execute “startup.bat”in bin. During the operation of the command window will appear as shown in Figure 2.

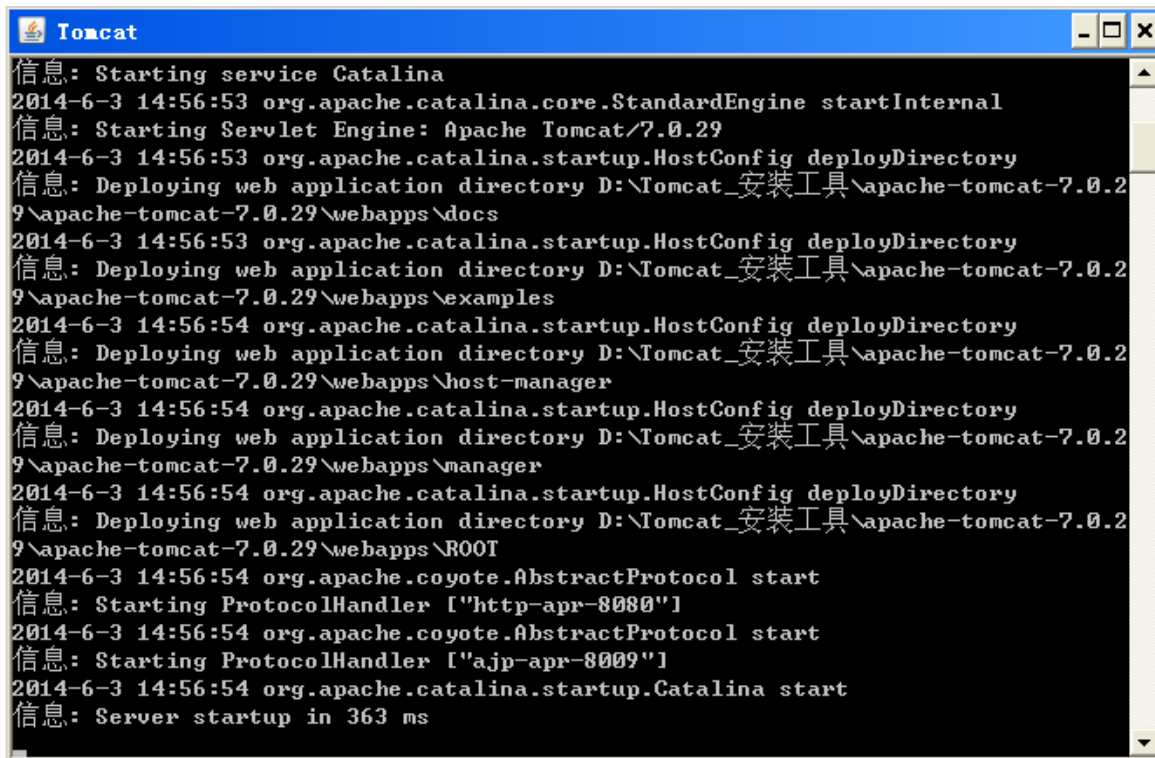


Figure 2

After starting the execution file, we will enter the default address for the Tomcat application service.:

<http://127.0.0.1:8080>

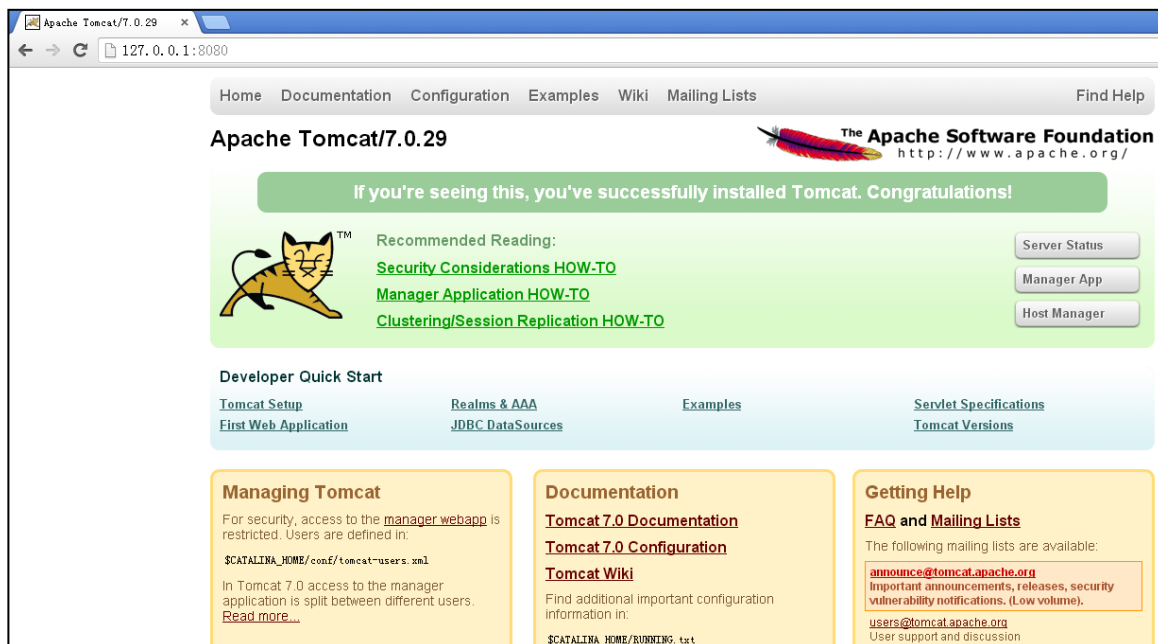
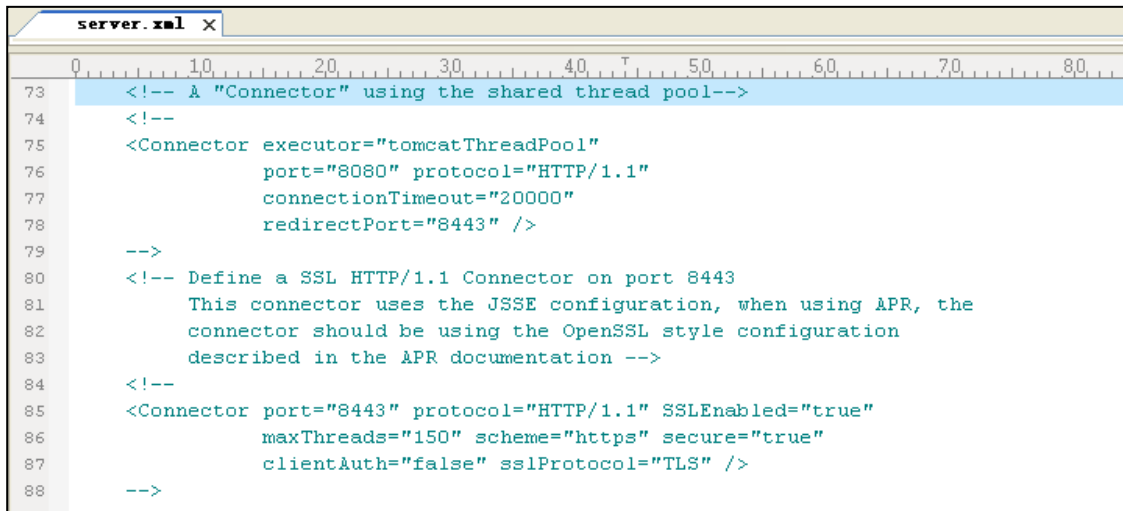


Figure 3

If there is a default Tomcat default this interface, it means that your current application service is running successfully.

1.3 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 shown as followed in figure 4

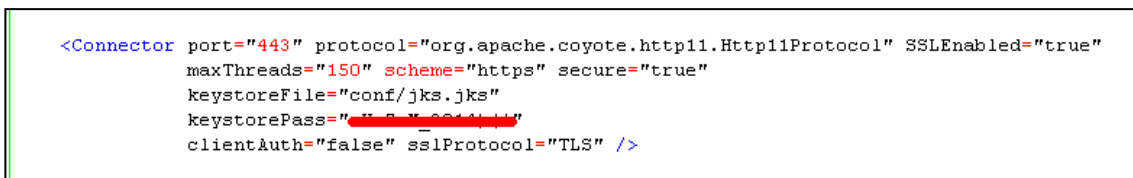


```
server.xml x
0 10 20 30 40 50 60 70 80
73 <!-- A "Connector" using the shared thread pool-->
74 <!--
75 <Connector executor="tomcatThreadPool"
76         port="8080" protocol="HTTP/1.1"
77         connectionTimeout="20000"
78         redirectPort="8443" />
79 -->
80 <!-- Define a SSL HTTP/1.1 Connector on port 8443
81     This connector uses the JSSE configuration, when using APR, the
82     connector should be using the OpenSSL style configuration
83     described in the APR documentation -->
84 <!--
85 <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
86         maxThreads="150" scheme="https" secure="true"
87         clientAuth="false" sslProtocol="TLS" />
88 -->
```

Figure 4

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
scheme="https"secure="true"clientAuth="false" sslProtocol="TLS" keystoreFile="keystore/SSL.jks"
keystorePass="XXXX" />
```

Usually <Connector port="8443".....> is commented, we delete“<!-- -->”, and edit it, like: port: port number; keystoreFile: Certificate path (like: **conf/SSL.jks**); keystorePass: Password of certificate. Figure5



```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
keystoreFile="conf/jks.jks"
keystorePass="XXXXXXXXXX"
clientAuth="false" sslProtocol="TLS" />
```

Figure 5

Finally save the configuration file, and then restart the Tomcat and visit the web site again. Like figure 6

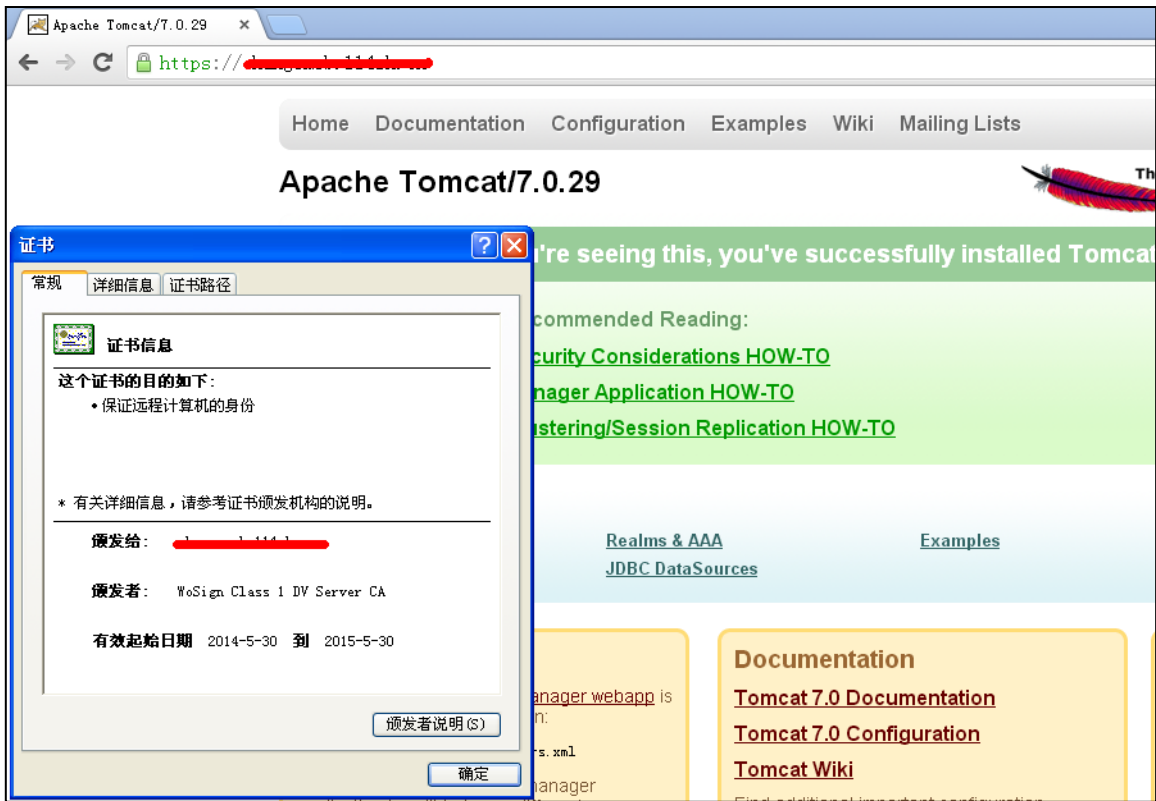


Figure 6

2. Install Secure signature

(**Secure signature only works on OV and EV SSL certificate now**)

2.1 Install English Secure signature

After you purchased the SSL WoSign certificate, you can get a trusted website security certification logo which shows your company's certificate information freely. It can greatly enhance the user's online trust, to facilitate more online transactions. So we suggest you to add the following code which can dynamically display the trusted site security certification logo on your homepage or other page.

If you want display the certificate logo on English website, add the code on the English web page below:

```
<SCRIPT LANGUAGE="JavaScript" TYPE="text/javascript" SRC="https://seal.wosign.com/tws-en.js"></SCRIPT>
```



3、 Backup of SSL certificate

Please save the file and password you receive.

4、 Restore of SSL certificate

Repeat 2.3 operation.