

# 服务器 SSL 证书安装配置指南

## Tomcat

更新日期：2016-11-7

**第一步：生成证书请求文件(CSR)**

进入 Java\_JRE\bin 目录，如 `cd C:\PROGRA~1\Java\jre1.5.0_06\bin`，运行如下命令：

```
keytool -genkey -alias tomcat -keyalg RSA -keysize 2048 -keystore
c:\server.jks 输入 keystore 密码：*****
```

输入 keystore 密码，务必牢记此密码，后面在 server.xml 的配置中需要使用到。

您的名字与姓氏是什么？

[Unknown]: cn.globalsign.com

您的组织单位名称是什么？

[Unknown]: IT Dept.

您的组织名称是什么？

[Unknown]: GlobalSign China Co., Ltd.

您所在的城市或区域名称是什么？

[Unknown]: Shanghai

您所在的州或省份名称是什么？

[Unknown]: Shanghai

该单位的两字母国家代码是什么

[Unknown]: CN

您的名字与姓氏是什么？（这里输入域名，如：cn.globalsign.com）

您的组织单位名称是什么？（这里输入部门名称，如：IT Dept）

您的组织名称是什么？（这里输入公司名称名称，如： GlobalSign China Co., Ltd.）

您所在的城市或区域名称是什么？（这里输入城市，如： Shanghai）

您所在的州或省份名称是什么？（这里输入省份，如： Shanghai）

该单位的两字母国家代码是什么？（这里输入 2 位国家代码，如： CN）

```
CN=cn.globalsign.com, OU=IT Dept, O= GlobalSign China Co., Ltd., L=Shanghai, ST=Shanghai, C=CN
正确吗？
```

[否]: Y

请核对信息，如果确认无误后请直接输入 Y 并回车

输入 <tomcat> 的主密码

（如果和 keystore 密码相同，按回车）：

不需要另外设置独立密码，这里回车即可，完成后在 C 盘根目录下就会生成一个 server.jks 的 JAVA 证书池文件，在证书办法并导入前请妥善保存此文件。

```
keytool -certreq -alias tomcat -keystore c:\server.jks -file
c:\certreq.csr 输入 keystore 密码：*****
```

输入密码后回车，这时会生成一个 certreq.csr 的文件，此文件为证书请求文件（CSR）。

## 第二步：提交 CSR，申请证书

递交证书申请表及相关资料，并把证书请求文件（CSR）提交给我们。  
我们确认资料齐全后，三个工作日内完成证书颁发。

## 第三步：获取并安装服务器证书

1. 获取中级证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第二段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 `intermediate.cer`（文本格式）。

```
keytool -import -trustcacerts -keystore c:\server.jks -alias inter -file intermediate.cer
```

2. 获取 SSL 证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第一段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 `server.cer`（文本格式）。

```
keytool -import -trustcacerts -keystore c:\server.jks -alias tomcat -file server.cer
```

第三步全部完成后，表示证书已经完全安装到 `server.jks` 这个文件中，请备份此文件并妥善保存，以后如有更换服务器或重装系统，就可以直接使用此文件。

## 第四步：更新 `server.xml` 配置文件

用文本编辑器打开 Tomcat 目录下的 `server.xml`  
找到去除注释并更新以下内容：

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector
    protocol="org.apache.coyote.http11.Http11NioProtocol"
    port="8443" maxThreads="200"
    scheme="https" secure="true"
    SSLEnabled="true" keystoreFile="c:\server.jks"
    keystorePass="changeit"
    clientAuth="false" sslProtocol="TLS"/>
```

如果你要使用默认的 SSL 端口，请将 8443 端口改为 443 端口，`keystoreFile` 和 `keystorePass` 是 JKS 文件对应的路径和密码。

注意：不同 tomcat 版本，修改 `server.xml` 的方式略有不同，请参考 tomcat 说明

```
tomcat 9.0 http://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html
tomcat 8.0 http://tomcat.apache.org/tomcat-8.0-doc/ssl-howto.html
tomcat 7.0 http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html
tomcat 6.0 http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html
tomcat 5.5 http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html
tomcat 4.1 http://tomcat.apache.org/tomcat-4.1-doc/ssl-howto.html
```

按照以上的步骤配置完成后，重新启动 TOMCAT 后就可以使用 `https://www.domain.com` 来访问了

如有任何问题或疑问请直接与我们联系，谢谢！