

本教程使用 JDK 6 和 Tomcat 7，其他版本类似。

基本步骤：

1. 使用 java 创建一个 **keystore** 文件
2. 配置 Tomcat 以使用该 keystore 文件
3. 测试
4. 配置应用以便使用 SSL，例如 `https://localhost:8443/yourApp`

1. 创建 keystore 文件

执行 **keytool -genkey -alias tomcat -keyalg RSA** 结果如下

```
1 loiane:bin loiane$ keytool -genkey -alias tomcat -keyalg RSA
2 Enter keystore password: password
3 Re-enter new password: password
4 What is your first and last name?
5 [Unknown]: Loiane Groner
6 What is the name of your organizational unit?
7 [Unknown]: home
8 What is the name of your organization?
9 [Unknown]: home
10 What is the name of your City or Locality?
11 [Unknown]: Sao Paulo
12 What is the name of your State or Province?
13 [Unknown]: SP
14 What is the two-letter country code for this unit?
15 [Unknown]: BR
16 Is CN=Loiane Groner, OU=home, O=home, L=Sao Paulo, email=loiane.groner@gmail.com, c=BR?
17 [no]: yes
18
19 Enter key password for tomcat
20 (RETURN if same as keystore password): password
21 Re-enter new password: password
```

这样就在用户的主目录下创建了一个 .keystore 文件

2. 配置 Tomcat 以使用 keystore 文件

打开 server.xml 找到下面被注释的这段

```
1 <!--
2 <Connector port="8443" protocol="HTTP/1.1" SSLEnable
3     maxThreads="150" scheme="https" secure="true"
4     clientAuth="false" sslProtocol="TLS" />
5 -->
```

干掉注释，并将内容改为

1	Connector SSLEnabled="true" acceptCount="100" client
2	disableUploadTimeout="true" enableLookups="false"
3	port="8443" keystoreFile="/Users/loiane/.keysto
4	protocol="org.apache.coyote.http11.Http11NioPro
5 测试	secure="true" sslProtocol="TLS" />

启动 Tomcat 并访问 **https://localhost:8443**. 你将看到 Tomcat 默认的首页。

需要注意的是, 如果你访问默认的 8080 端口, 还是有效的。

4. 配置应用使用 SSL

打开应用的 web.xml 文件, 增加配置如下:

1	<security-constraint>
2	<web-resource-collection>
3	<web-resource-name>securedapp</web-resource
4	<url-pattern>/*</url-pattern>
5	</web-resource-collection>
6	<user-data-constraint>
7	<transport-guarantee>CONFIDENTIAL</transport
8	</user-data-constraint>
9	</security-constraint>

将 URL 映射设为 /*, 这样你的整个应用都要求是 HTTPS 访问, 而 transport-guarantee 标签设置为 CONFIDENTIAL 以便使应用支持 SSL。

如果你希望关闭 SSL, 只需要将 CONFIDENTIAL 改为 NONE 即可。a