
Tomcat SSL 证书部署指南



沃通电子认证服务有限公司

WoSignCA Limited

目录

一、 生成证书请求文件	3
1.1 服务器环境架设	3
1.2 生成 Csr 和 Keystore 文件	4
1.2.1 生成 Server 私钥	4
1.2.2 生成 Csr 文件	5
1.2.3 成功生成文件	5
二、 提交 CSR 文件	7
2.1 登录 wosign 站点	7
2.2 选择证书类型	7
2.3 填写资料	7
2.4 验证域名	7
2.5 确认订单信息	7
2.6 支付订单	7
2.7 上传证明材料	7
2.8 等待证书签发	7
三、 安装 SSL 证书	8
3.1 导入中级根证书	8
3.2 导入服务器证书:	8
3.3 配置部署 SSL 证书	9
3.3.1 Tomcat 8.5 之前版本	9
3.3.2 Tomcat 8.5 及之后版本	11
四、 SSL 证书的恢复	13

技术支持联系方式

技术支持邮箱: support@wosign.com
技术支持热线电话: 0755-26027828
技术支持网页: <https://bbs.wosign.com>
公司官网地址: <https://www.wosign.com>

一、 生成证书请求文件

1.1 服务器环境架设

Tomcat 安装 SSL 证书, 首先先确认 tomcat 和 jdk 的版本, tomcat8.5 前后版本证书部署方式不一样, 安装 SSL 证书的时候, 找到相应指导, 另外 jdk1.6 及之前版本, 不支持新的加密套件和 TLS1.1 和 TLS1.2 协议, 建议申请 JDK1.7 以上版本。

确认 tomcat 能正常运行, 进入 tomcat 根目录下找到 bin 文件中此执行文件 windows:“startup.bat” (linux:“startup.sh”)。

启动执行文件后, 我们将输入 Tomcat 应用服务默认的地址如: <http://127.0.0.1:8080>

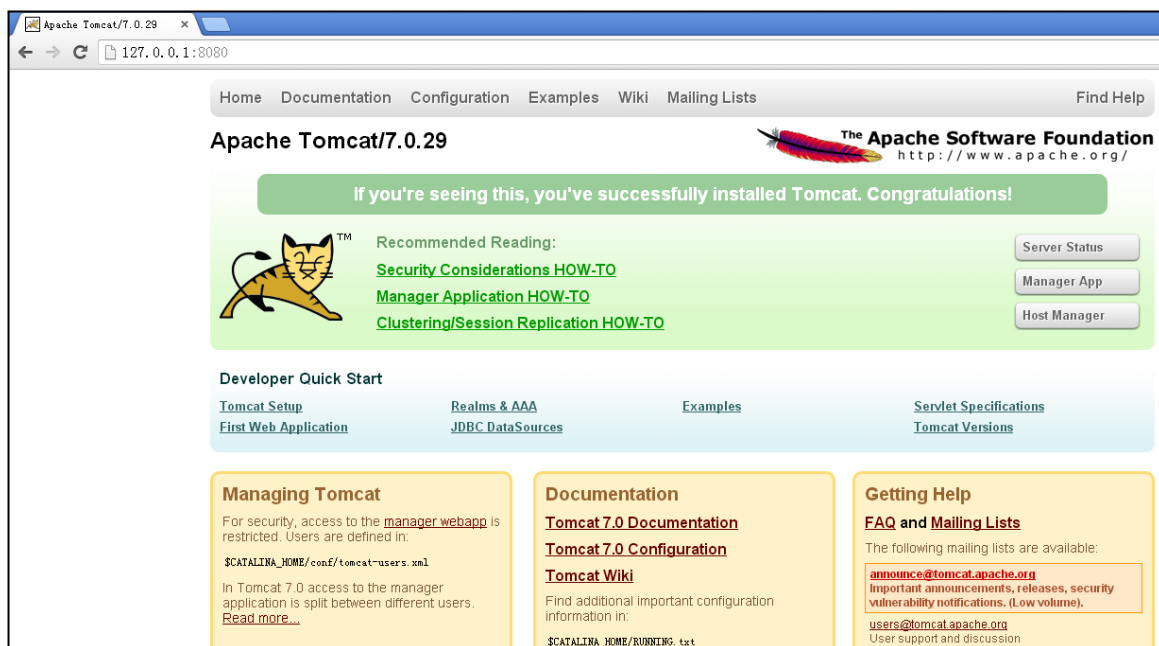


图 1

1.2 生成 Csr 和 Keystore 文件

进入 DOS 命令行具体如下：

开始-> 运行-> cmd->cd 到您安装的 jdk 的目录这里我是

C:\Program Files\Java\jdk1.5.0_04\bin 图 2

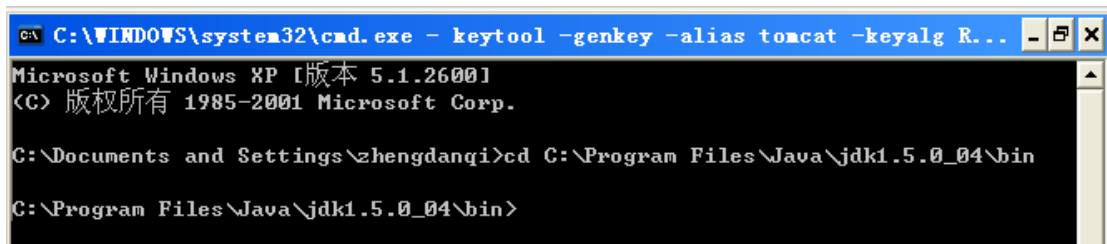


图 2

1.2.1 生成 Server 私钥

Keytool -genkey -alias [keyEntry_name] -keyalg RSA -keystore [keystore_name]

-keysize 2048 图 3

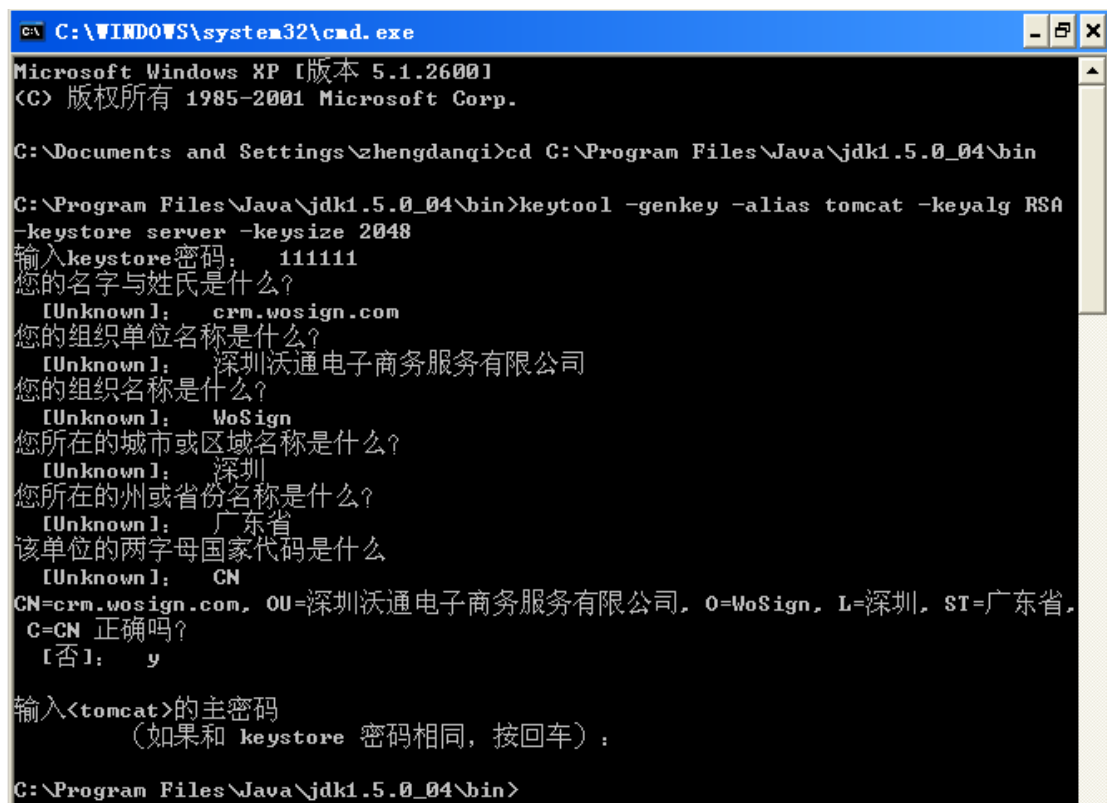


图 3

以上如图所示此命令将生成 2048 位的 RSA 私钥，私钥文件名为：**server**，系统会提示您输入 keystore 密码，缺省密码为：changeit，您可以指定一个新的密码，但请一定要记住。

接着会提示 “What is your first and last name?”，请输入您要申请 SSL 证书的域名，而不是真的输入您的个人姓名，如果您需要为 www.domain.com 申请 SSL 证书就不能只输入 domain.com。SSL 证书是严格绑定域名的。

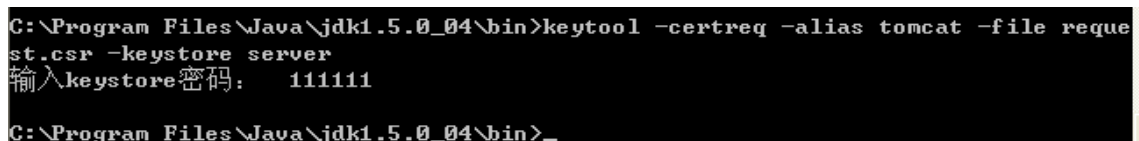
接着，输入您的部门名称、单位名称、所在城市、所在省份和国家缩写(中国填：CN，其他国家填其缩写)，单位名称一定要与证明文件上的名称一致。除国家缩写必须填 CN 外，其余都可以是英文或中文。

最后，要求您输入私钥密码，请一定要为 keystore 和 keyEntry 输入一样的密码，否则您重新启动 Tomcat 后会提示错误信息：java.security.UnrecoverableKeyException: Cannot recover key。同时，请一定要记住密码！

1.2.2 生成 Csr 文件

请使用以下命令来生成 CSR

Keytool -certreq -alias [keyEntry name] -file request.csr -keystore [keystore name] 图 4



```
C:\Program Files\Java\jdk1.5.0_04\bin>keytool -certreq -alias tomcat -file request.csr -keystore server
输入keystore密码: 111111
C:\Program Files\Java\jdk1.5.0_04\bin>
```

图 4

如上图所示此命令将生成 CSR 文件，这样就完成了 CSR 和私钥的生成。

1.2.3 成功生成文件

您现在已经成功生成了密钥对，私钥文件：**server** 保存在您的服务器中，请把 CSR 文件：**request.csr** 发给 WoSign 即可。（注释：此时两个文件默认存放路径在安装 jdk1.5.0_04 目录中的 bin 文件夹中

如 server 和 request.csr)

如果您想测试您的 CSR 文件是否成功您可以通过记事本打开。如下图 5:



图 5

然后通过复制里面所有的内容粘贴到如下地址:

https://www.wosign.com/support/check_csr.htm 来验证您里面的信息是否您要申请的资料, 请把测试成功的 CSR 文件发给 WoSign 即可。请一定不要再动您的服务器, 等待证书的颁发。测试结果如下图 6:

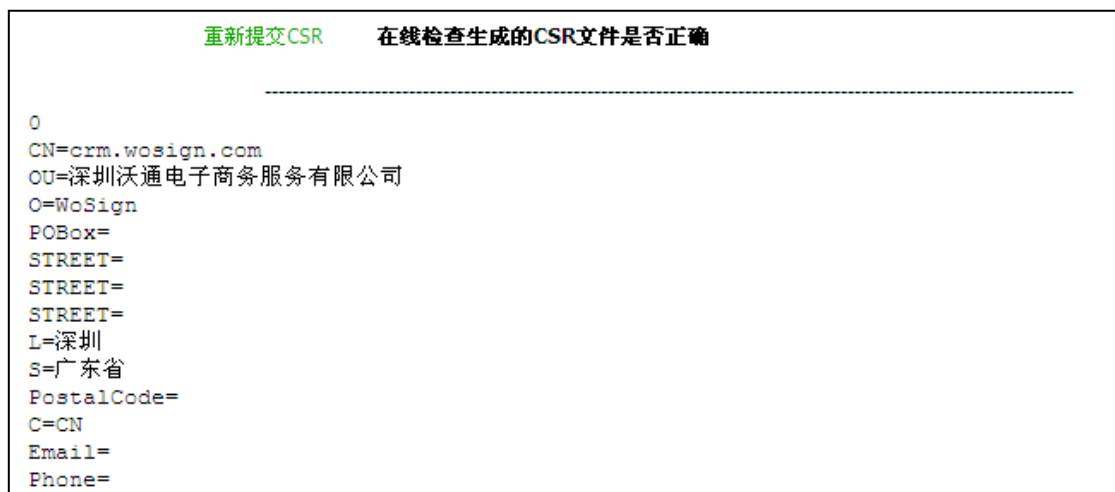


图 6

二、 提交 CSR 文件

2.1 登录 wosign 站点

登录 <https://login.wosign.com/>；输入密码和验证码，选择客户端证书登录在线购买系统。

2.2 选择证书类型

点右上边橙色“申请证书”连接，选择您要申请的 SSL 证书，点“立即申请”，

2.3 填写资料

需要填写：证书绑定的域名，申请年限，是否需要发票，并设置证书安装密码。

2.4 验证域名

进入域名验证，可以选择邮箱验证、DNS 验证或者网站验证方式，进入下一步；

2.5 确认订单信息

用记事本打开生成好的 csr 文件，提交生成的 csr 文件，然后确认订单信息。

2.6 支付订单

可您以在线转账，也可以选择线下转账

2.7 上传证明材料

根据要求上传材料

2.8 等待证书签发

证书申请提交成功。待客服和鉴证审核，您可以联系您的客服专员咨询订单审核情况。

三、 安装 SSL 证书

3.1 导入中级根证书

首先 WoSign 将根据您提交的 Csr 文件给您签发服务器证书。此时您拿到手的压缩文件，解压里面的 for other server.zip 文件，会得到里面则包含了以下证书，如图 11

 cross.crt	← 交叉根	2016/12/7 9:41	安全证书
 issuer.crt	← 中级根	2016/12/7 9:41	安全证书
 root.crt	← 顶级根	2016/12/7 9:41	安全证书
 test.wosign.com.crt	← 公钥	2016/12/7 9:41	安全证书

图 11

现在可以通过命令来导入您服务器证书，

比如：

Tomcat 安装(先导入根证书，用户证书最后导入)：

Tomcat 安装时需把顶级根、交叉根、中级根、用户证书全部导入到 keystore 中

(注意：keystore 等同于 server 文件，后面会把 keystore 名称改为：server. jks 或 yourdomain. jks)

命令如下：

Keytool -import -trustcacerts -alias [keyEntry_name] -file xxx.cer -keystore

[keystore_name]

[keyEntry_name] ： 别名；

xx.cer ： 表示根证书文件名；

[keystore_name] ： 证书容器 server；

keytool -import -trustcacerts -alias root -file root.crt -keystore keystore

keytool -import -trustcacerts -alias cross -file corss.crt -keystore keystore

keytool -import -trustcacerts -alias issue -file issue.crt -keystore keystore

3.2 导入服务器证书：

```
Keytool -import -trustcacerts -alias [keyEntry_name] -file user_domian.crt -keystore  
[keystore_name]
```

[keyEntry_name]: 别名；您制作 CSR 时候输入的别名；

xx.crt : 表示服务器证书名称；

[keystore_name]: 证书容器 server；

```
keytool -import -trustcacerts -alias 别名 -file xx.crt -keystore keystore
```

在运行此命令时会提示您输入密码，也就是您在生成 server 时设置的密码。（注：
当您导入证书的时候如果“提示错误：无法从回复中建立链接”此时解决的方式是：检
查证书的别名是否正确，中级根证书是否已经导入）

当导入证书到您的 server 时，一定要使用生成 CSR 时一样的别名(-alias)，同时使用
-trustcacerts 参数。如果不指定一样的别名，将不能安装成功！

验证检查证书

最终导入中级根证书和服务证书文件后，可以通过以下命令检查是否包含了四级证书
链接。命令行：keytool -list -v -keystore [证书文件]

3.3 配置部署 SSL 证书

3.3.1 Tomcat 8.5 之前版本

找到 Tomcat 安装目录 conf 下的“Server.xml”，用文本编辑器打开，找到如下图示位置 如图
12:

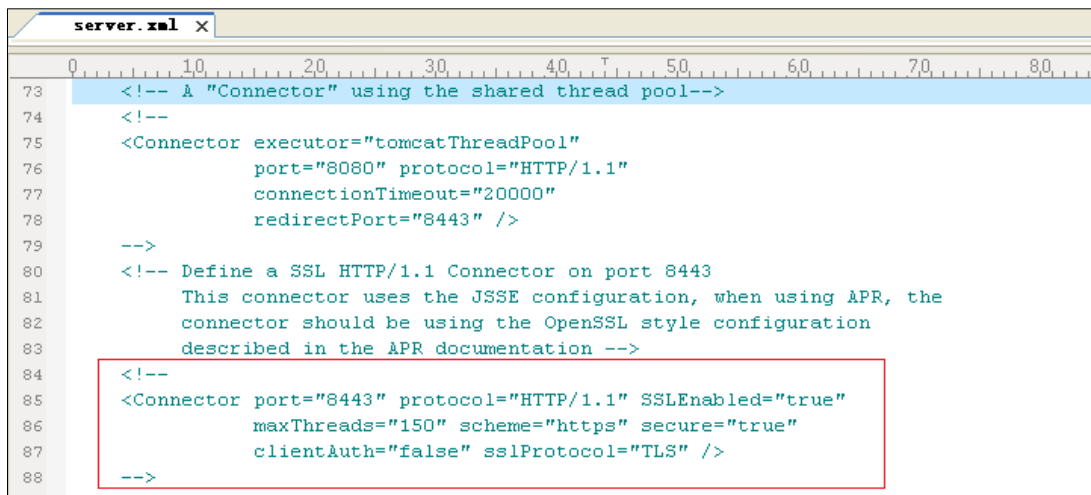


图 12

默认情况下<Connector port= “8443”.....>是被注释的，我们可以把“<!-- -->”去掉，然后对其节点进行相应的修改，比如：

配置示例如下：

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
keystoreFile="keystore/domain.jks" keystorePass="证书密码"
clientAuth="false" sslProtocol="TLS"
ciphers="TLS_RSA_WITH_AES_128_GCM_SHA256,
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
        TLS_RSA_WITH_AES_128_CBC_SHA,
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
        TLS_RSA_WITH_AES_128_CBC_SHA256,
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
        SSL_RSA_WITH_3DES_EDE_CBC_SHA,
        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA" />
```

备注：port：端口号；

keystoreFile：证书路径(例如：**conf/name.jks**)； keystorePass：证书密码。

最后保存该配置文件，然后重启 Tomcat 后再次访问。如图 13：

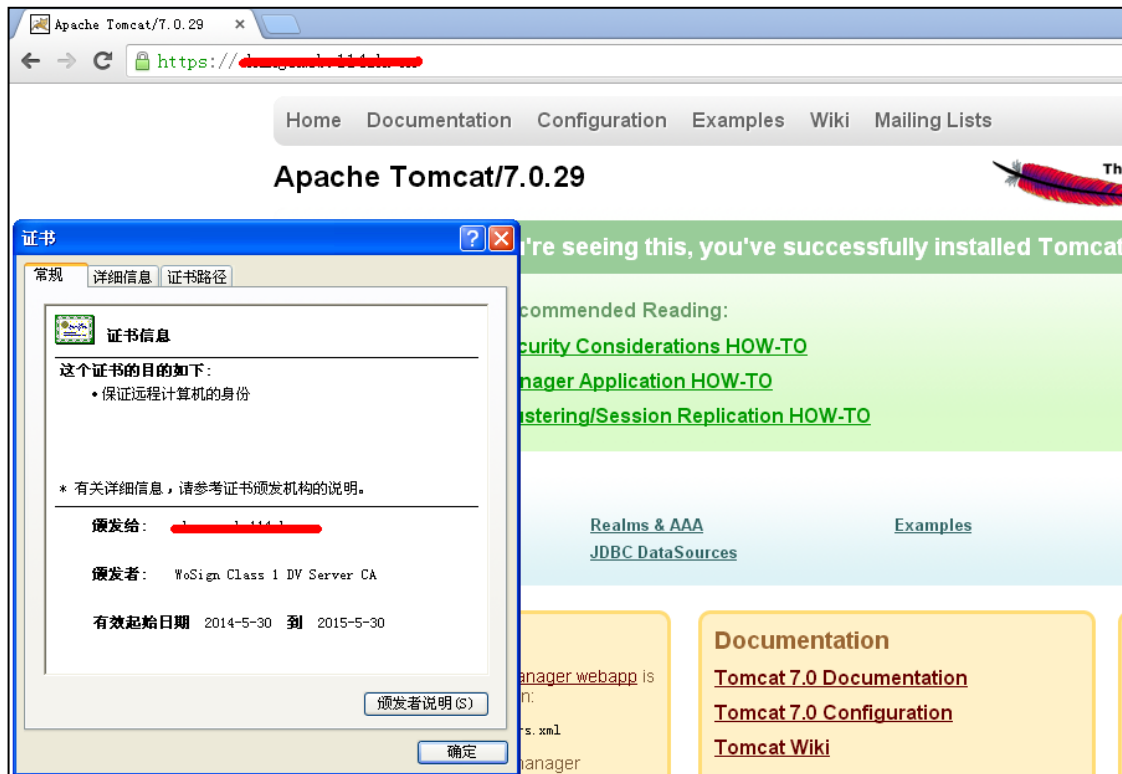


图 13

3.3.2 Tomcat 8.5 及之后版本

找到 Tomcat 安装目录 conf 下的“Server.xml”，用文本编辑器打开，找到如下图所示位置 如图 14：

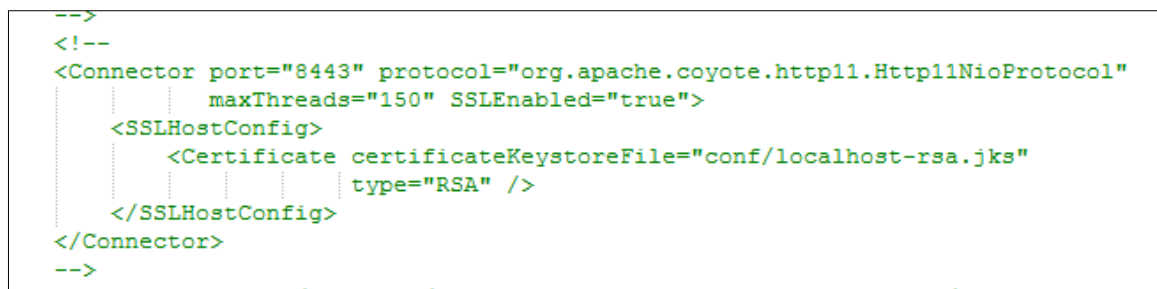


图 14

默认情况下<Connector port= “8443”.....>是被注释的，我们可以把“<!-- -->”去掉，并进行相应的修改，比如：

配置示例如下：

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
```

```
maxThreads="150" SSLEnabled="true">
```

```
<SSLHostConfig>
```

```
<Certificate certificateKeystoreFile="F:\Tomcat 9.0\conf\name.jks"
```

```
certificateKeyAlias="alias"
```

```
certificateKeystorePassword="证书密码"
```

```
type="RSA" />
```

```
</SSLHostConfig>
```

```
</Connector>
```

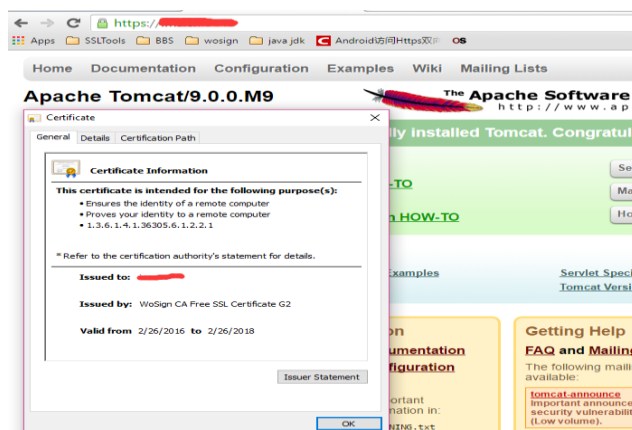
备注：port：端口号；

certificateKeystoreFile：证书路径(例如：**conf/name.jks**)；

certificateKeystorePassword：证书密码；

certificateKeyAlias：证书别名

最后保存该配置文件，然后重启 Tomcat 后再次访问即可。如图 15：



SSL 证书的备份

请保存好生成的 jks 文件及密码，以防丢失

四、 SSL 证书的恢复

重复第三步操作即可。