

---

# Resin SSL 安装操作指南



沃通电子认证服务有限公司

## 目录

一、	生成证书请求文件.....	4
1.1	申请 SSL 证书指南.....	4
1.2	生成 Csr 和 Keystore 文件.....	4
1.3	生成 Server 私钥.....	4
1.4	生成 Csr 文件.....	6
1.5	成功生成文件.....	6
二、	提交 CSR 文件.....	7
2.1	登录 wosign 站点.....	7
2.2	选择证书类型.....	8
2.3	填写资料.....	8
2.4	验证域名.....	8
2.5	确认订单信息.....	8
2.6	支付订单.....	8
2.7	上传证明材料.....	8
2.8	等待证书签发.....	8
三、	安装 SSL 证书.....	8
3.1	导入中级根证书.....	9
3.2	导入服务器证书: .....	10
3.3	验证检查证书.....	10
3.4	服务器安装 SSL 证书环境.....	10

---

3.5 配置部署 SSL 证书.....	12
3.5.1 启动 SSL 端口.....	12
3.5.2 配置证书路径.....	13
3.5.3 验证安装结果.....	14
四、 SSL 证书的备份.....	14
五、 SSL 证书的恢复.....	14

## 技术支持联系方式

技术支持邮箱：[support@wosign.com](mailto: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>

## 致谢

感谢您使用我们的产品及操作手册，如果您对我们的产品或操作手册有什么意见和建议，您可以通过电话或邮件反馈给我们，我们将由衷感谢

## 声明

此文档仅做参考使用，相应的配置需根据当前的配置进行调整。

## 一、生成证书请求文件

### 1.1 申请 SSL 证书指南

首先访问 Oracle 官网（

<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>）当前可根据您的系统下载不同的 JDK 包，我们以 Windows 系统为例。下载后安装到您的系统目录下

### 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 1

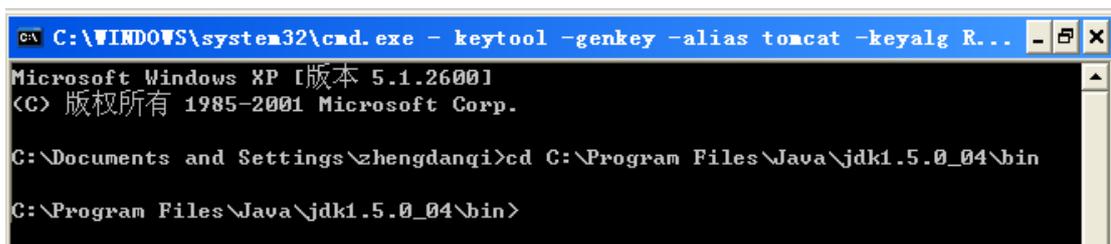
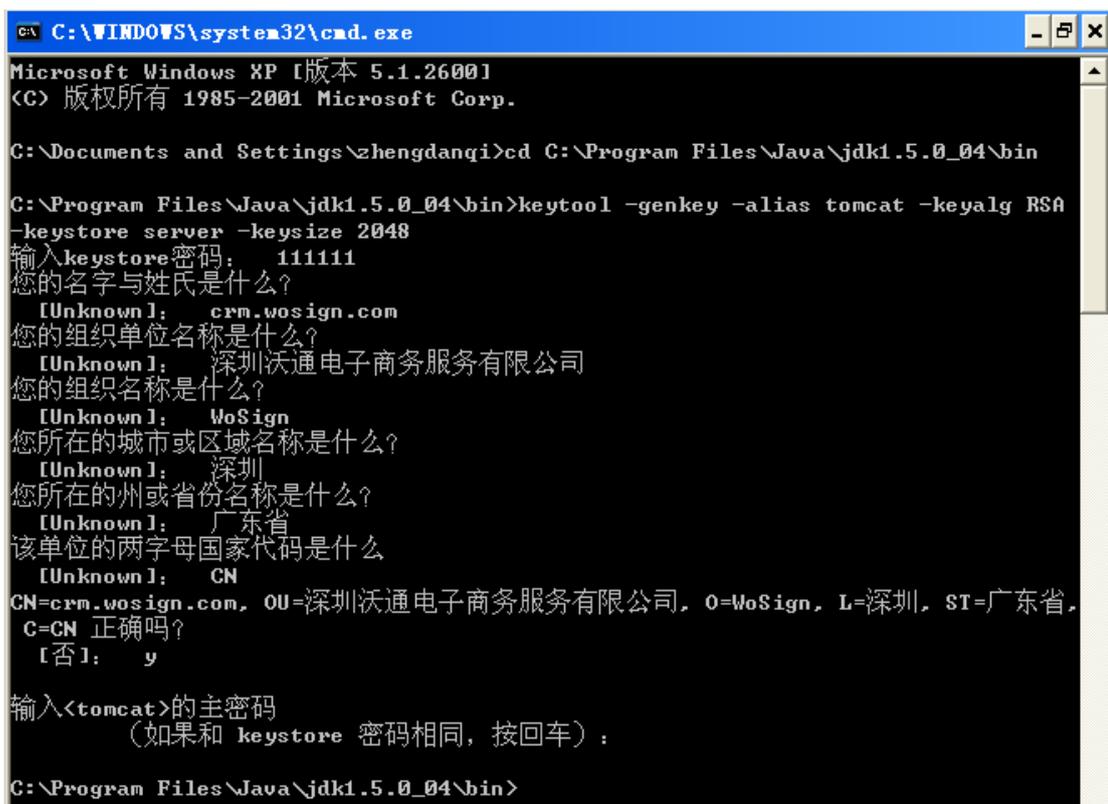


图 1

### 1.3 生成 Server 私钥

`Keytool -genkey -alias [keyEntry_name] -keyalg RSA -keystore [keystore_name] -keysize 2048` 图 3



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\zhengdanqi>cd C:\Program Files\Java\jdk1.5.0_04\bin

C:\Program Files\Java\jdk1.5.0_04\bin>keytool -genkey -alias tomcat -keyalg RSA
-keystore server -keysize 2048
输入 keystore 密码: 111111
您的名字与姓氏是什么?
[Unknown]: crm.wosign.com
您的组织单位名称是什么?
[Unknown]: 深圳沃通电子商务服务有限公司
您的组织名称是什么?
[Unknown]: WoSign
您所在的城市或区域名称是什么?
[Unknown]: 深圳
您所在的州或省份名称是什么?
[Unknown]: 广东省
该单位的两字母国家代码是什么?
[Unknown]: CN
CN=crm.wosign.com, OU=深圳沃通电子商务服务有限公司, O=WoSign, L=深圳, ST=广东省,
C=CN 正确吗?
[否]: y

输入 <tomcat> 的主密码
(如果和 keystore 密码相同, 按回车):

C:\Program Files\Java\jdk1.5.0_04\bin>
```

图 2

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。

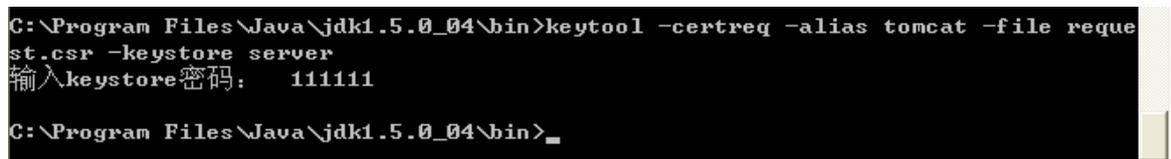
接着，输入您的部门名称、单位名称、所在城市、所在省份和国家缩写(中国填：**CN**，其他国家填其缩写)，单位名称一定要与证明文件上的名称一致。除国家缩写必须填 **CN** 外，其余都可以是英文或中文。

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！

## 1.4 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 3

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。

## 1.5 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：

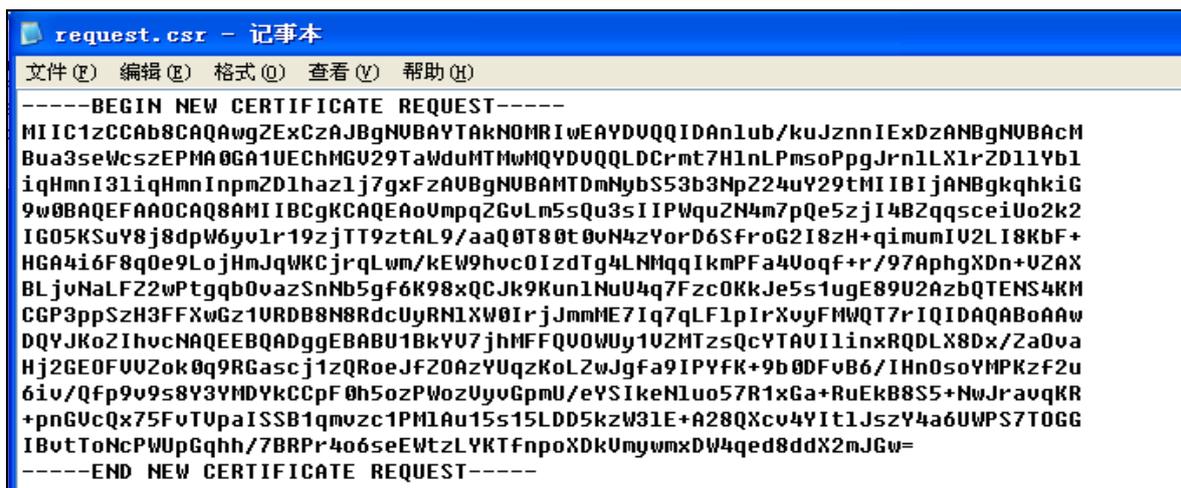


图 4

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](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：

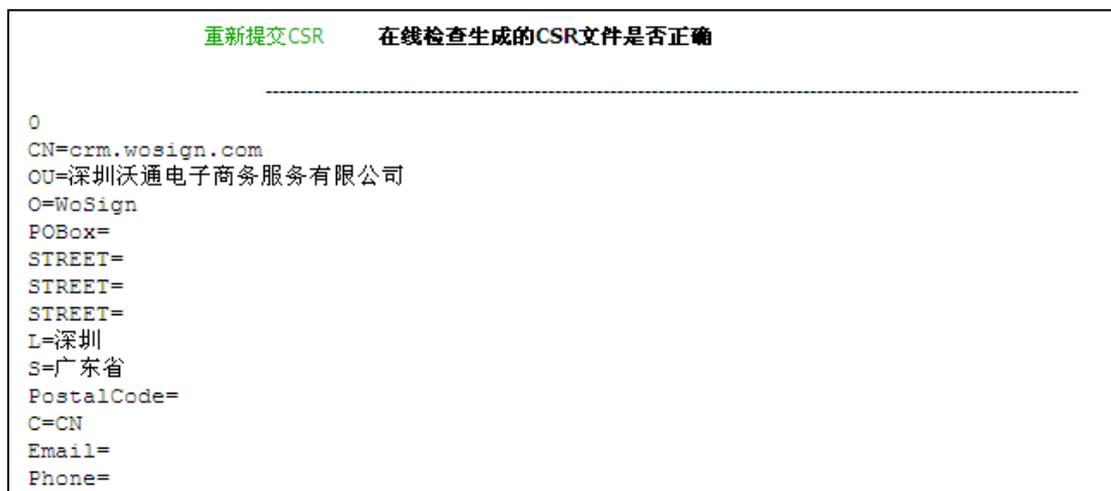


图 5

## 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，如下图

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 7

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 jks. 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 xxx.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！

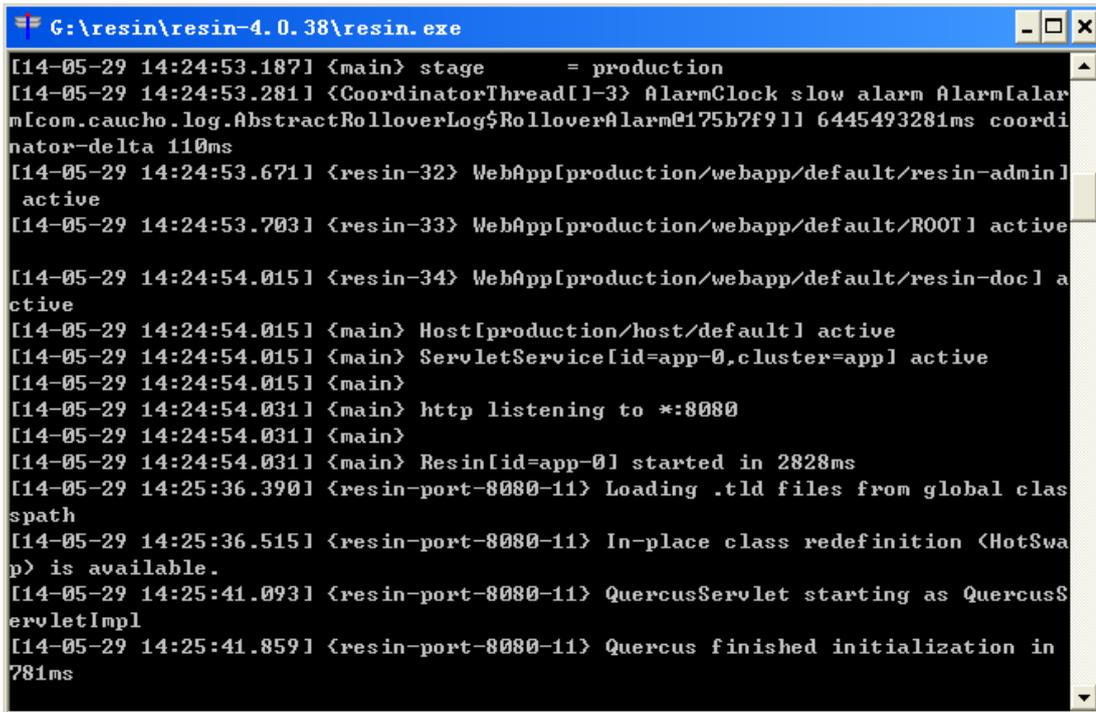
### 3.3 验证检查证书

最终导入中级根证书和服务器证书文件后，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]

### 3.4 服务器安装 SSL 证书环境

首先访问 Resin 官网 (<http://www.caucho.com>) 当前可根据您的系统下载不同的应用程序包，我们以 Windows 系统为例。所以下载 Windows 版本的 Resin-4.0.38 版本。

下载 Resin 解压到其中一个盘符下后，进入 Resin-4.0.38 根目录下找到 resin.exe 文件，运行期间将出现如图 1 所示的命令提示符窗口。



```
G:\resin\resin-4.0.38\resin.exe
[14-05-29 14:24:53.187] <main> stage = production
[14-05-29 14:24:53.281] <CoordinatorThread[1-3] AlarmClock slow alarm Alarm[alarm[com.caucho.log.AbstractRolloverLog$RolloverAlarm@175b7f91] 6445493281ms coordinator-delta 110ms
[14-05-29 14:24:53.671] <resin-32> WebApp[production/webapp/default/resin-admin] active
[14-05-29 14:24:53.703] <resin-33> WebApp[production/webapp/default/ROOT] active
[14-05-29 14:24:54.015] <resin-34> WebApp[production/webapp/default/resin-doc] active
[14-05-29 14:24:54.015] <main> Host[production/host/default] active
[14-05-29 14:24:54.015] <main> ServletService[id=app-0,cluster=app] active
[14-05-29 14:24:54.015] <main>
[14-05-29 14:24:54.031] <main> http listening to *:8080
[14-05-29 14:24:54.031] <main>
[14-05-29 14:24:54.031] <main> Resin[id=app-0] started in 2828ms
[14-05-29 14:25:36.390] <resin-port-8080-11> Loading .tld files from global classpath
[14-05-29 14:25:36.515] <resin-port-8080-11> In-place class redefinition (HotSwap) is available.
[14-05-29 14:25:41.093] <resin-port-8080-11> QuercusServlet starting as QuercusServletImpl
[14-05-29 14:25:41.859] <resin-port-8080-11> Quercus finished initialization in 781ms
```

图 8

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

点击/resin-admin 图 2 图 3

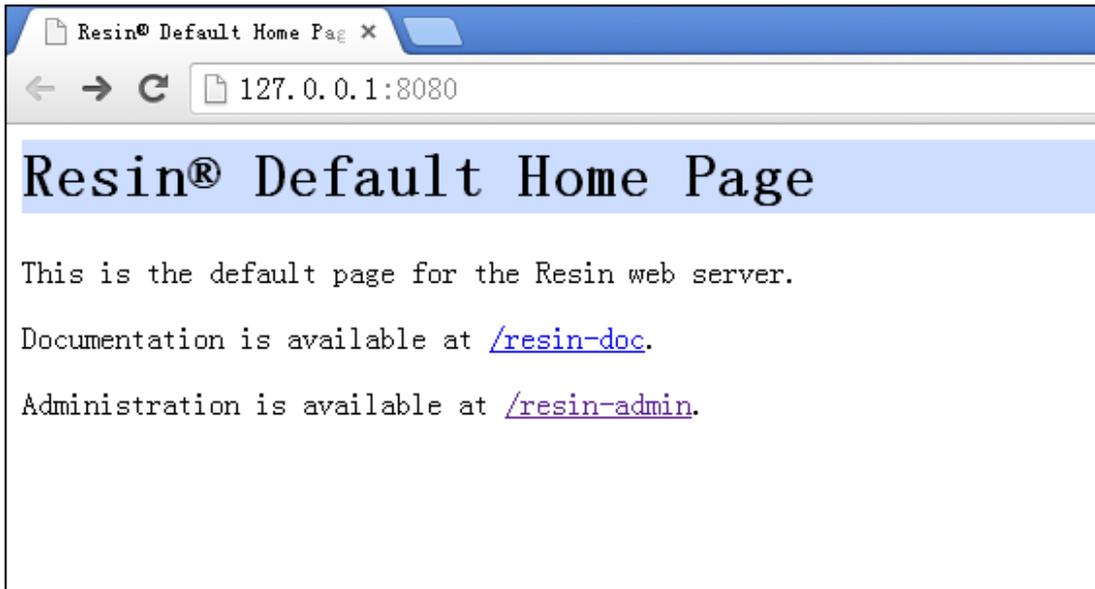


图 9

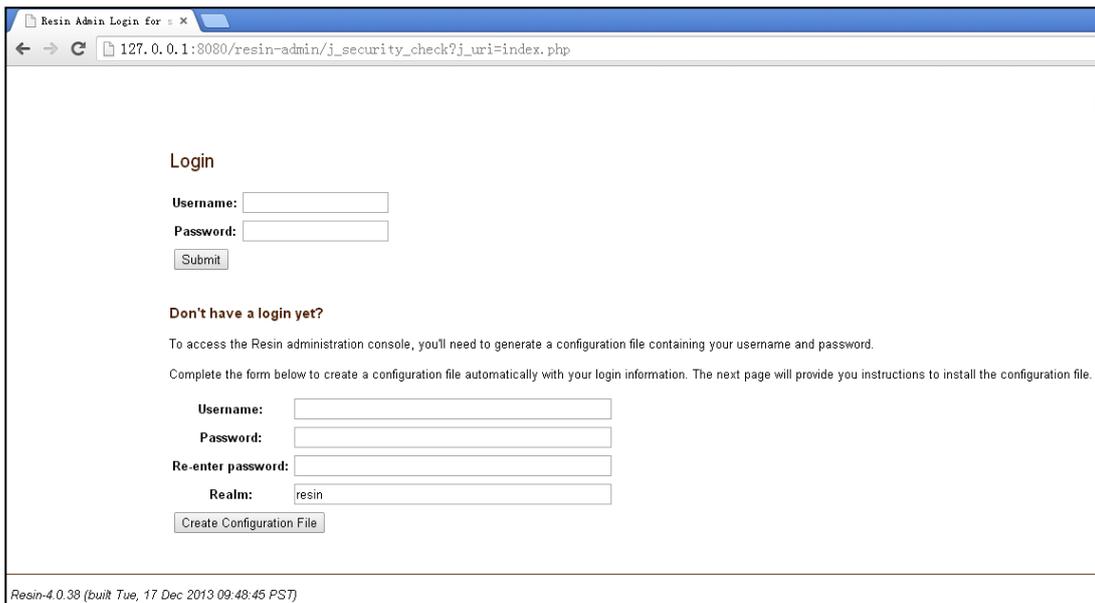


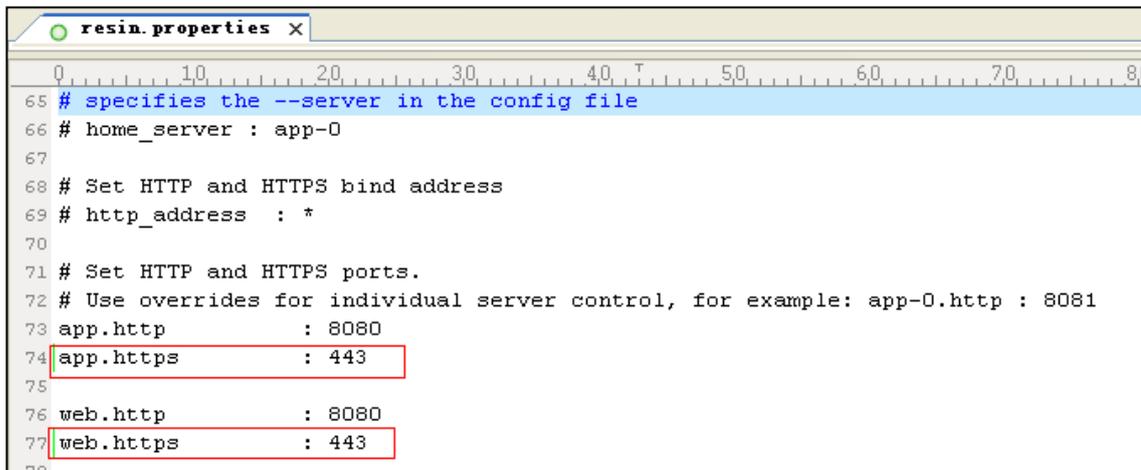
图 10

## 3.5 配置部署 SSL 证书

### 3.5.1 启动 SSL 端口

首先找到安装 Resin 目录下该配置文件“Resin.properties”，一般默认路径都是在

Conf 文件夹中。然后用文本编辑器打开该文件，接着找到如下所示 图 4



```
resin.properties x
0 10 20 30 40 50 60 70 80
65 # specifies the --server in the config file
66 # home_server : app-0
67
68 # Set HTTP and HTTPS bind address
69 # http_address : *
70
71 # Set HTTP and HTTPS ports.
72 # Use overrides for individual server control, for example: app-0.http : 8081
73 app.http : 8080
74 app.https : 443
75
76 web.http : 8080
77 web.https : 443
78
```

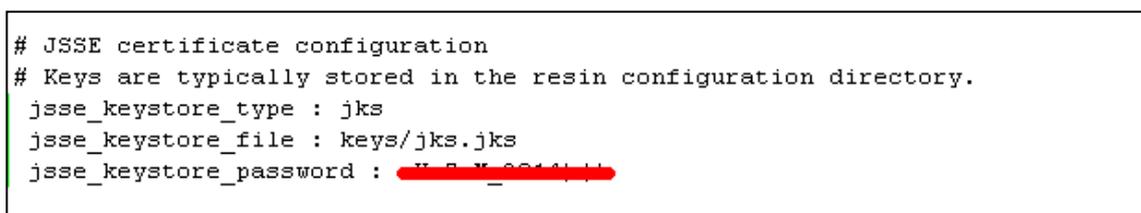
图 11

默认情况下 app.https 和 web.https : 8443 是用“#”注释掉的。所以我们可以去掉“#”然后把 8443 修改为：443。

**注释：**（因为版本繁多没能一一去下载来检查，只能通过在此说明。根据不同的版本寻找不同的配置文件如“Resin.properties”或是“resin.xml”文件进行配置。）

### 3.5.2 配置证书路径

其次同一个文件中在找到如图 5



```
# JSSE certificate configuration
# Keys are typically stored in the resin configuration directory.
jsse_keystore_type : jks
jsse_keystore_file : keys/jks.jks
jsse_keystore_password : XXXXXXXXXX
```

图 12

默认情况下：Jsse\_keystore\_tye: jks 证书类型；

Jsse\_keystore\_file: keys/xx.jks 证书存放路径；

Jsse\_keystore\_password: changeme 证书密码；

(注: 图片中的 `jks.jks` 是以上所说的导入根证书和服务器证书后的 `server` 文件。)

三行都是“#”注释状态, 所以我们可以去掉“#”, 最后只要改成您的证书路径(例如: `keys/SSL.jks`)、证书密码(您申请证书时所设置密码)。

### 3.5.3 验证安装结果

最后保存重启 Resin 应用服务就 OK。测试访问效果图 6



图 13

## 四、 SSL 证书的备份

请保存好生成的 `jks` 文件及密码, 以防丢失

## 五、 SSL 证书的恢复

重复第三步操作即可。