





Java Tomcat 数字证书安装指南

证书成功签发后，您将收到如下 4 个数字证书文件，请按照根证书，中级证书，域名证书的顺序依次安装

 AddTrustExternalCARoot.crt	2000/5/30 10:48	安全证书
 COMODORSAAAddTrustCA.crt	2000/5/30 10:48	安全证书
 COMODORSADomainValidationSecureServerCA.crt	2014/2/12 0:00	安全证书
 mydomain.crt	2017/10/27 0:00	安全证书

1. 导入根证书，AddTrustExternalCARoot.crt 是根证书，使用 Keytool 命令导入

```
-> keytool -import -trustcacerts -alias AddTrustExternalCARoot -file  
AddTrustExternalCARoot.crt -keystore mydomain.keystore
```

2. 导入中级证书，COMODORSA 开头的两个文件是中级证书，使用 Keytool 命令导入：

```
-> keytool -import -trustcacerts -alias COMODORSAAAddTrustCA -file  
COMODORSAAAddTrustCA.crt -keystore mydomain.keystore
```

```
-> keytool -import -trustcacerts  
-alias COMODORSADomainValidationSecureServerCA -file  
COMODORSADomainValidationSecureServerCA.crt -keystore mydomain.keystore
```

3. 导入域名证书，mydomain.crt 是域名证书，使用 Keytool 命令导入：

```
-> keytool -import -trustcacerts  
-alias mykey -file myDomainName.crt -keystore domain.keystore
```

如果安装成功，系统会提示: **Certificate reply was installed in keystore**，如果没有安装成功请检查步骤 1,2。

注意: 如果您在签发证书之前用 Tomcat 生成 CSR 时，对 alias 别名进行了定义，可以用具体的名字代替上面的 **mykey**

4. 重启服务器服务

Note: 在重启服务器服务前，请检查 Connector 文件配置，确保 keystone 文件的路径和密码正确填写，格式如下。

```
<Connector port="443" maxHeaderSize="8192" maxThreads="150"  
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"  
disableUploadTimeout="true" acceptCount="100" scheme="https"  
secure="true" SSLEnabled="true" clientAuth="false"  
sslProtocol="TLS" keyAlias="server"  
keystoreFile="/home/user_name/your_site_name.jks"  
keystorePass="your_keystore_password" />
```