

Tomcat 支持 PFX 格式和 JKS 两种格式的证书，您可根据您 Tomcat 的版本择其中一种格式的证书安装到 Tomcat 上。

一、 安装 PFX 格式证书

- 1、 准备好 PFX 格式的证书；
- 2、 在 Tomcat 安装目录下新建 cert 目录，将证书文件拷贝到 cert 目录下。
- 3、 打开 Tomcat > conf > server.xml 文件，在 server.xml 文件中添加以下属性（其中 port 属性请根据您的实际情况修改，其中 protocol 建议为：

protocol="org.apache.coyote.http11.Http11Protocol") ：

```
<Connector port="443"
  protocol="HTTP/1.1"
  SSLEnabled="true"
  scheme="https"
  secure="true"
  keystoreFile="domain name.pfx"    #此处 keystoreFile 代表证书文件的路径，请用您证书的文件名替换 domain name。
  keystoreType="PKCS12"
  keystorePass="证书密码"    #请用您证书密码替换文件中的内容。
  clientAuth="false"
  SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
  ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256"/>
```

- 4、 保存 server.xml 文件配置。
- 5、 （可选步骤）配置 web.xml 文件开启 HTTP 强制跳转 HTTPS。

#在</welcome-file-list>后添加以下内容：

```
<login-config>
  <!-- Authorization setting for SSL -->
  <auth-method>CLIENT-CERT</auth-method>
  <realm-name>Client Cert Users-only Area</realm-name>
</login-config>
<security-constraint>
  <!-- Authorization setting for SSL -->
  <web-resource-collection >
    <web-resource-name >SSL</web-resource-name>
```

```
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

6、 重启 Tomcat。

二、 安装 JKS 格式证书

- 1、 准备好 JKS 格式的证书：
- 2、 在 Tomcat 安装目录下新建 cert 目录，将证书和密码文件拷贝到 cert 目录下。
- 3、 打开 Tomcat 安装目录 > conf 文件夹 > server.xml 文件，在 server.xml 文件中找

到 <Connector port="443" 标签并添加以下参数：

```
keystoreFile="cert/domain name.jks"    #此处 keystoreFile 代表证书文件的路径，请用您证书
的文件名替换 cert/后面的内容。
keystoreType="PKCS12"
keystorePass="证书密码"    #请输入您的证书密码。
```

参考以下完整配置（其中 port 属性请根据您的实际情况修改）：

```
<Connector port="443"
protocol="HTTP/1.1"
SSLEnabled="true"
scheme="https"
secure="true"
keystoreFile="cert/domain name.jks"
keystoreType="PKCS12"
keystorePass="证书密码"
clientAuth="false"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH
E_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256"/>
```

- 4、 保存 server.xml 文件配置。
- 5、 重启 Tomcat。