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。

1. **安装PFX格式证书**
2. 根据《证书文件介绍及安装前准备》文档转换证书格式，准备好PFX格式的证书；
3. 在Tomcat安装目录下新建cert目录，将证书文件拷贝到cert目录下。
4. 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"/>

1. 保存server.xml文件配置。
2. （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>

1. 重启Tomcat。
2. **安装JKS格式证书**
3. 转换证书格式为JKS：
4. 输入以下java JDK命令将PFX格式的证书转换成JKS格式：

keytool -importkeystore -srckeystore **domain** **name**.pfx -destkeystore **domain** **name**.jks -srcstoretype PKCS12 -deststoretype JKS

**说明：** Windows系统中，需在 %JAVA\_HOME%/jdk/bin目录下执行该命令。

1. 根据《证书文件介绍及安装前准备》文档转换好JKS格式的证书，转换工具：<https://www.chinassl.net/ssltools/convert-ssl.html>。（原格式选PEM）
2. 回车后输入PFX证书密码和JKS证书密码。

**说明：** JKS证书密码等同于PFX证书密码。两个密码不同的时候会导致Tomcat重启失败。

1. 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。
2. 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\_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"/>

1. 保存server.xml文件配置。
2. 重启Tomcat。