

购买、下载并上传自有 SSL 证书

使用自有证书配置自定义域名时，需要先购买或申请 SSL 证书，再下载 Nginx 格式证书包，并在保利威后台上传证书文件和私钥文件。

开始前准备

购买或上传证书前，请确认：

- 可登录证书服务商后台。
- 已确认需要配置到保利威后台的自定义域名。
- 如已有证书，请确认证书未过期，且证书绑定的域名与保利威后台填写的自定义域名一致。

常见证书服务商入口

如果证书由云服务商签发或托管，可进入对应平台的 SSL 证书管理页面下载证书文件。下载时请选择 Nginx 格式证书包。

平台	入口或帮助文档	说明
阿里云数字证书管理服务	下载 SSL 证书至本地	适用于在阿里云申请或托管 SSL 证书的情况
腾讯云 SSL 证书	腾讯云 SSL 证书下载文档	适用于在腾讯云申请或托管 SSL 证书的情况
华为云云证书管理服务	华为云下载证书文档	适用于在华为云申请或托管 SSL 证书的情况

1. 购买或申请 SSL 证书

如果还没有可用于自定义域名的 SSL 证书，可先在证书服务商后台购买或申请证书。多数情况下，可在域名注册商、云服务商或证书服务商平台完成购买。

购买或申请时，请重点确认以下信息：

信息	填写或选择说明
证书绑定域名	填写需要配置到保利威后台的自定义域名，例如 <code>live.example.com</code>
证书类型	选择支持 HTTPS 访问的 SSL 证书；如无特殊安全合规要求，通常可选择域名型证书
域名数量	单个域名使用单域名证书；多个同级子域名可按需选择通配符证书
有效期	按实际需要选择。证书到期前需重新购买或续费，并在保利威后台更新证书
域名验证方式	按证书服务商要求完成域名验证，常见方式包括 DNS 验证和文件验证

通用操作流程如下：

1. 登录证书服务商后台。
2. 进入 SSL 证书或数字证书管理页面。
3. 选择购买、申请或创建证书。
4. 填写需要绑定的自定义域名。
5. 选择证书类型、证书规格和有效期。
6. 按页面要求完成购买或提交申请。
7. 按证书服务商要求完成域名验证。
8. 等待证书签发。证书状态变为已签发后，再下载 Nginx 格式证书包。

如果证书服务商提供免费测试证书，请确认有效期和使用限制。使用自有证书时，证书到期前需自行更新。

2. 下载 Nginx 格式证书包

1. 登录证书服务商后台。
2. 进入 SSL 证书或证书管理页面。
3. 找到需要用于自定义域名的证书。
4. 点击下载或部署相关入口。
5. 选择 Nginx 格式下载证书包。

6. 下载后解压证书包。

文件说明

文件类型	常见格式	用途
证书文件	<code>.pem</code> 、 <code>.crt</code>	用于证明域名证书信息
私钥文件	<code>.key</code>	用于和证书文件匹配完成 HTTPS 访问

3. 上传到保利威后台

在配置流程中选择【使用自有证书】后，按页面要求上传：

- 证书文件
- 私钥文件

证书文件和私钥文件需同时上传。文件未上传完整时，无法进入下一步。

注意事项

- 上传的证书需与当前配置的自定义域名匹配。
- 私钥文件需与证书文件匹配。
- 已过期证书无法用于配置。
- 不建议手动修改证书文件或私钥文件内容。
- 如果证书包中包含多个文件，请优先选择 Nginx 格式目录下的证书文件和私钥文件。
- 使用自有证书时，证书到期前需自行更新。