

---

# Apache SSL 证书部署指南



沃通电子认证服务有限公司

WoSignCA Limited

## 目 录

一、 安装 SSL 证书的环境 .....	3
1.1 SSI 证书安装环境简介 .....	3
1.2 网络环境要求 .....	3
二、 SSL 证书的安装 .....	3
2.1 获取 SSI 证书 .....	3
2.2 解压证书文件 .....	3
2.3 2018 年之前签发获取 SSI 证书 .....	3
2.4 安装 SSL 证书 .....	4
2.5 测试 SSL 证书 .....	5
三、 SSL 证书的备份 .....	5
四、 SSL 证书的恢复 .....	5

### 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 / 0755-26027859  
技术支持网页: <https://bbs.wosign.com>  
公司官网地址: <https://www.wosign.com>

## 一、安装 SSL 证书的环境

### 1.1 SSI 证书安装环境简介

Centos 6.4 操作系统;

Apache2.2.\*或以上版本;

Openssl 1.0.1+;

SSL 证书一张 (备注: 本指南使用 s.wosign.com 域名 OV SSL 证书进行操作,通用其它版本证书)。

### 1.2 网络环境要求

请确保站点是一个合法的外网可以访问的域名地址, 可以正常通过或 http://XXX 进行正常访问。

## 二、SSL 证书的安装

### 2.1 获取 SSI 证书

成功在沃通申请证书后, 会得到一个压缩包文件, 解压后得到四个文件: for Apache、for IIS、for Ngnix、for Other Server, 这个是证书的几种格式, Apache 上需要用到 for Apache 格式的证书。





 for apache.zip	← 解压此文件	2018/4/17 15:41	秒压压缩工具
 for iis.zip		2018/4/17 15:41	秒压压缩工具
 for nginx.zip		2018/4/17 15:41	秒压压缩工具
 for other server.zip		2018/4/17 15:41	秒压压缩工具

图 1

### 2.2 解压证书文件

解压 Apache 文件可以看到 2 个文件。包括公钥、证书链, 如图 2。



 root_bundle.crt	← 证书链	2017/11/27 15:27	安全证书	4 KB
 test.wosign.com.crt	← 公钥	2017/11/27 13:43	安全证书	2 KB

图 2

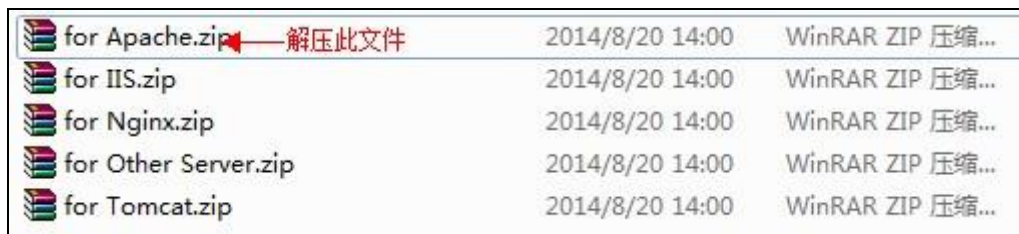
key 文件, 需要找到生成 CSR 一起生成出的两个文件, 如图 3, 其中一个是.key 文件, 若生成出来的是.com 文件, 修改一下后缀即可。



图 3

## 2.3 2018 年之前签发获取 SSI 证书

颁发的证书, 拿到证书后会得到一个有密码的压缩包文件, 输入证书密码后解压得到五个文件: for Apache、for IIS、for Nginx、for Tomcat、for Other Server, 这个是证书的几种格式, Apache 上需要用到 for Apache 格式的证书。



解压 Apache 文件可以看到 3 个文件。包括公钥、私钥、证书链, 如图 4

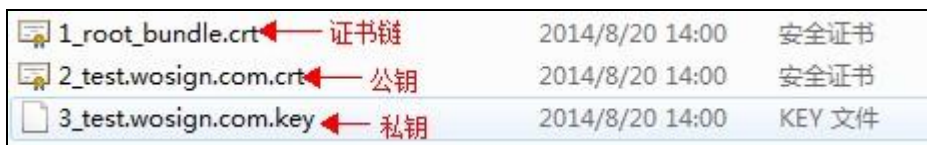


图 4

## 2.4 安装 SSL 证书

1、打开 apache 安装目录下 conf 目录中的 httpd.conf 文件, 找到 #LoadModule ssl\_module modules/mod\_ssl.so (如果找不到请确认是否编译过 openssl 插件)

```
#Include conf/extra/httpd_ssl.conf
```

删除行首的配置语句注释符号“#”

保存退出。

2、打开 apache 安装目录下 conf/extra 目录中的 httpd-ssl.conf 文件 (注释: yum 安装配置目录: conf.d/ssl.conf ubuntu/apache2 安装目录: conf/sites-enabled/\*.conf )

在配置文件中查找以下配置语句:

a. 添加 SSL 协议支持语句，关闭不安全的协议和加密套件

```
SSLProtocol all -SSLv2 -SSLv3
```

b. 修改加密套件如下

```
SSLCipherSuite ECDH:AESGCM:HIGH:!DH:!RC4:!aNULL:!eNULL;
```

c. 将服务器证书公钥配置到该路径下(在 conf 目录下创建 ssl 目录，将 for Apache 里面的三个证书文件拷贝到 ssl 目录下)

```
SSLCertificateFile conf/ssl/test.wosign.com.crt # (证书公钥)
```

d. 将服务器证书私钥配置到该路径下

```
SSLCertificateKeyFile conf/ssl/test.wosign.com.key # (证书私钥)
```

e. 将服务器证书链配置到该路径下

```
#SSLCertificateChainFile conf/ssl/root_bundle.crt # (证书链) 删除行首的“#”号注释符
```

保存退出，并重启 Apache。重启方式：

3、进入 Apache 安装目录下的 bin 目录，运行如下命令

```
./apachectl -k stop
```

```
./apachectl -k start
```

## 2.5 测试 SSL 证书

在浏览器地址栏输入：<https://s.wosign.com> (申请证书的域名)测试您的 SSL 证书是否安装成功，如果成功，则浏览器地址栏后方的安全锁标志。测试站点证书的安装配置。

备注：安装完 ssl 证书后部分服务器可能会有以下错误，请按照链接修复

a. 加密协议和安全套件：<https://bbs.wosign.com/thread-1284-1-1.html>

b. 部署 https 页面后出现排版错误，或者提示网页有不安全的因素，可参考以下链接：

<https://bbs.wosign.com/thread-1667-1-1.html>

## 三、SSL 证书的备份

请保存好收到的证书压缩包文件及密码，以防丢失。

## 四、SSL 证书的恢复

重复 2.4 操作即可。