
Apache SSL 证书申请部署指南



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	4
1.1	SSI 证书安装环境简介	4
1.2	网络环境要求	4
二、	生成证书请求文件	5
2.1	生成请求文件 csr	5
2.1.1	查看 openssl	5
2.1.2	生成 key 私钥文件	5
2.1.3	生成 csr 文件	5
三、	提交 CSR 文件	7
3.1	登录 wosign 站点	7
3.2	选择证书类型	7
3.3	填写资料	7
3.4	验证域名邮箱	7
3.5	确认订单信息	7
3.6	支付订单	7
3.7	上传证明材料	7
3.8	等待证书签发	7
四、	安装 SSL 证书	8
4.2	获取 SSI 证书	8
4.3	证书文件	8
4.4	安装 SSL 证书	8
4.5	测试 SSL 证书	9
五、	SSL 证书的备份	9
六、	SSL 证书的恢复	9

技术支持联系方式

技术支持邮箱: 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、生成证书请求文件

2.1 生成请求文件 csr

首先下载 openssl 软件，可以去 openssl 官网下载：<http://www.openssl.org/source/> 下载后安装到本地计算机。

2.1.1 查看 openssl

在终端输入 `openssl version` 查看 openssl 当前版本。

```
[root@localhost ~]# openssl version
OpenSSL 1.0.1e-fips 11 Feb 2013
```

图 1

2.1.2 生成 key 私钥文件

使用以下命令来生成私钥：`openssl genrsa -des3 -out www.mydomain.com.key 2048`，生成的私钥保存在当期目录。

```
[root@localhost ~]# openssl genrsa -des3 -out www.mydomain.com.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for www.mydomain.com.key:
Verifying - Enter pass phrase for www.mydomain.com.key:
[root@localhost ~]# ls
123.txt  dev  lib  media  proc  selinux  tmp  www.mydomain.com.key
bin      etc  lib64  mnt    root  srv      usr
boot    home lost+found  opt    sbin  sys      var
[root@localhost ~]#
```

图 2

2.1.3 生成 csr 文件

使用以下命令来生成私钥：`openssl req -new -key www.mydomain.com.key -out www.mydomain.com.csr`

```
[root@localhost /]# openssl req -new -key www.mydomain.com.key -out www.mydomain.com.csr
Enter pass phrase for www.mydomain.com.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:GuangDong
Locality Name (eg, city) [Default City]:ShenZhen
Organization Name (eg, company) [Default Company Ltd]:Wosign CA Limited
Organizational Unit Name (eg, section) []:Wosign Support
Common Name (eg, your name or your server's hostname) []:www.wosign.com
Email Address []:support@wosign.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:
[root@localhost /]# █
```

图 3

Country Name (2 letter code) [GB]: 输入国家地区代码，如中国的 CN

State or Province Name (full name) [Berkshire]: 地区省份

Locality Name (eg, city) [Newbury]: 城市名称

Organization Name (eg, company) [My Company Ltd]: 公司名称

Organizational Unit Name (eg, section) []: 部门名称

Common Name (eg, your name or your server's hostname) []: 申请证书域名

Email Address []: 电子邮箱

随后可能会提示输入密码，一般无需输入，直接回车即可

三、 提交 CSR 文件

3.1 登录 wosign 站点

登录 <https://login.wosign.com/>; 输入密码和验证码, 选择客户端证书登录在线购买系统。

3.2 选择证书类型

点右上边橙色“申请证书”连接, 选择您要申请的 SSL 证书, 点“立即申请”,

3.3 填写资料

需要填写: 证书绑定的域名, 申请年限, 是否需要发票, 并设置证书安装密码。

3.4 验证域名邮箱

进入域名验证, 可以选择邮箱验证、DNS 验证或者网站验证方式, 进入下一步;

3.5 确认订单信息

用记事本打开生成好的 csr 文件, 提交生成的 csr 文件, 然后确认订单信息。

3.6 支付订单

可您以在线转账, 也可以选择线下转账

3.7 上传证明材料

根据要求上传材料

3.8 等待证书签发

证书申请提交成功。待客服和鉴证审核, 您可以联系您的客服专员咨询订单审核情况。

四、安装 SSL 证书

4.2 获取 SSI 证书

成功在沃通申请证书后，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四个文件：**for Apache**、**for IIS**、**for Nginx**、**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。

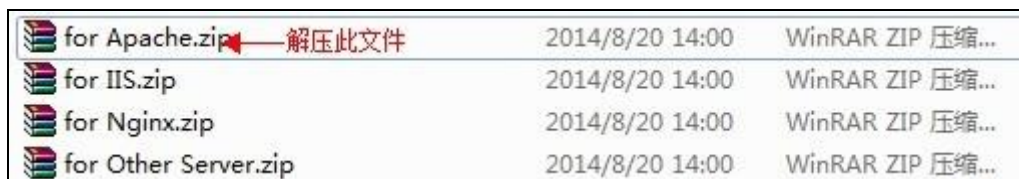


图 5

4.3 证书文件

解压 Apache 文件可以看到 3 个文件。包括公钥、证书链，如图 6



图 6

4.4 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)

```
#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，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 AESGCM:ALL:!DH:!EXPORT:!RC4:+HIGH:!MEDIUM:!LOW:!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/www.mydomain.key (证书私钥,生成csr时的key文件)
```

e. 将服务器证书链配置到该路径下

```
#SSLCertificateChainFile conf/ssl.crt/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
```

4.5 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会显示一个安全锁标志。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>

五、SSL 证书的备份

请保存好收到的证书压缩包文件和证书私钥及密码, 以防丢失。

六、SSL 证书的恢复

重复第四步操作即可。