





Apache SSL 数字证书安装指南

1. 签发证书，整合数字证书

一旦您申请的 SSL 证书成功颁发，签发机构会通过附件将数字证书发送到您的邮箱。附件包含 4 个证书文件，您需要按照 1-2-3-4 顺序将文件内容拷贝到一个文本文件，然后保存为 CRT 文件。

 AddTrustExternalCARoot.crt 4	2000/5/30 10:48	安全证书
 COMODORSAddTrustCA.crt 3	2000/5/30 10:48	安全证书
 COMODORSADomainValidationSecureServerCA.crt 2	2014/2/12 0:00	安全证书
 mydomain.crt 1	2017/10/27 0:00	安全证书

2. 安装证书

A. 把整合后的 SSL 证书和 Key 文件拷贝到 Apache 存放证书的目录中，如：`/usr/local/ssl/crt/ssl-bundle.crt`

B. 使用文本编辑器打开 `http.conf` 配置文件，添加数字证书和 Key 文件的路径参数，同时在 `VirtualHost` 标签添加端口号 `443`，如下：

- `SSLCertificateKeyFile`（数字证书的 Key 文件所在的目录路径）
- `SSLCertificateFile`（整合 CA Bundle 的 CRT 文件所在的路径）

VirtualHost 配置示例:

```
<VirtualHost 91.199.212.176:443>
    DocumentRoot /etc/httpd/htdocs
    ServerName comodo.com
    SSLEngine on
    SSLCertificateFile /usr/local/ssl/crt/ssl-bundle.crt
    SSLCertificateKeyFile /usr/local/ssl/private/private.key
</VirtualHost>
```

请注意： Apache 中含有 `https.conf` 和 `ssl.conf` 两个功能相同的文件，请只修改其中一个文件，否则会有冲突而使得 Apache 不能正常启动。

C. 保存修改。

D. 使用如下命令停止 Apache 后再启动 Apache, 以便 Apache daemon 能注册修改的参数, 您可以使用以下命令来重启:

```
/usr/sbin/apachectl stop /usr/sbin/apachectl startssl
```

或者:

```
/usr/sbin/httpd -k stop /usr/sbin/httpd -DSSL
```

3. 完成配置 **Setup the server**

请一定要分配 443 端口和一个固定的 IP 地址给主机(注意: 防火墙一定要开放 443 端口 TCP)。

在浏览器地址栏输入: <https://yourdomain.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, 则浏览器下方会显示一个安全锁标志。