

服务器 SSL 证书安装配置指南

Apache 2.4.x

更新日期：2016-11-7

第一步：生成证书请求文件(CSR)

进入 OpenSSL 安装的目录，运行如下命令生成私钥：

```
openssl genrsa -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
```

该命令执行后将会生成 `server.key` 私钥文件

运行如下命令生成证书请求文件（CSR）

```
openssl req -new -key server.key -out server.csr
```

如是 Windows 系统，请使用下面命令生成证书请求文件（CSR）

```
set OPENSSL_CONF=openssl.cnf
openssl req -new -key server.key -out server.csr
```

接下来提示输入申请证书的详细信息

```
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) []:CN
State or Province Name (full name) []:Shanghai
Locality Name (eg, city) []:Shanghai
Organization Name (eg, company) []:GlobalSign China Co., Ltd.

Organizational Unit Name (eg, section) []:IT Dept.
Common Name (eg, your websites domain name) []:cn.globalsign.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

从 Email 地址开始，下面的信息都不需要，请保留为空，直接回车即可。

需要输入的信息说明请见下表：

字段	说明	示例
Country Name	ISO 国家代码（两位字符）	CN
State or Province Name	所在省份	Shanghai
Locality Name	所在城市	Shanghai
Organization Name	公司名称	GlobalSign China Co., Ltd.
Organizational Unit Name	部门名称	IT Dept.
Common Name	申请证书的域名	cn.globalsign.com
Email Address	不需要输入	
A challenge password	不需要输入	

完成以上的操作后会在对应的目录下生成 server.key 和 server.csr，请妥善保存这两个文件。

第二步：提交 CSR，申请证书

递交证书申请表及相关资料，并把证书请求文件（CSR）提交给我们。
我们确认资料齐全后，三个工作日内完成证书颁发。

第三步：获取服务器证书

1. 获取 SSL 证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第一段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容保存为 server.cer（文本格式）。
2. 获取中级证书（此证书由 GlobalSign 系统通过 Email 方式发送给用户，邮件中第二段代码），证书文件的内容为（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”），请把此内容追加到 server.cer 内容后。最终 server.cer 内容如下：

```

1 -----BEGIN CERTIFICATE-----
2 MIIIE3zCCA8egAwIBAgIMZaTH1OGecTk1fJSSMA0GCSqGSIb3DQEBCwUAMEw
3 BgNVBAYTAKJFMRkwFwYDVQQKExBhbG99iYwXTawduIG52LXNhMSIwIAYDVQQK
4 bHB0YVNTTCBBDQSAIFNlIQTl1NiAtIEcyMB4XDTE2MDgxNTAzNDgyM1oXDTE
5 NjAzNDgyM1owPTEhMB8GA1UECXMtYRg9tYwluIENvbnRyb2wgVmFsaWRhdGV
6 FgYDVQDDA8qLmVsb2JhbHNpZ24uY24wgGEiMA0GCSqGSIb3DQEBAQUAA4I
7 ggEKAoIBAQA9Y7pJ3DY0gdOpdMdCtHj2ERP0eCINzhd1bAZnSwL46ffWt6
8 5e41IjryiypSVIHodzaGfgr3t48IRnxtYmXmmeUAA8j3QGFComLdNANEV3
9 +rFwzXvKqYawNP/ru9SGgtB4Y0/dPBbNdGw7FcfRFUgG04D8V1toNu0NTa
10 4nXhXERQmsnMfSY8z5fL4eAWJ0CNqEp94Qq1IARLfw1XBVrDPy6qcXJuoPL
11 pmjooGp72B0LqCUxXEKZPWAKj9GfkwqI1dTg9mKSNZdoeHR8311JLPdRKGH
12 NuxZ7Hu3M/9CKnYro51gJHhV8zOHULWNAgMBAAGjggHOMIIBYjAOBGNVHQ8
13 BAMCBAAwYkGCCsGAQUFBwEBBHB0wezBCBgggrBgEFBQcwoAoY2aHR0cDovL3N
14 ZTIuYXNjaWwzZ2wzY29tL2NhY2VydC9nc2FscGhhc2hhMmcyZjEuY3J0MDU
15 AQUFBzABh1lodHRwOi8vb2NzcdIuZ2xvYmFsc21nb15jb20vz3NhbHBoYXN
16 MjBxBG9NVHSAEUDBOMEIGCisGAQQBoDIBCgowNDAYBggrBgEFBQcCARYmaHR
17 Ly93d3cuZ2xvYmFsc21nb15jb20vcmVwb3NpdG9yeS8wCAYGZ4EMAQIBMAK
18 EwQCAAAwPgYDVR0fBDcWNTAzoDGL4YtaHR0cDovL2NybDIuYXNjaWwzZ2w
19 L2dzL2dzYXNjaWwzZ2wzY29tL2NhY2VydC9nc2FscGhhc2hhMmcyZjEuY3J0
20 MDUuZ2xvYmFsc21nb15jb20vZ3NhbHBoYXNjaWwzZ2wzY29tL2NhY2VydC9nc
21 2FscGhhc2hhMmcyZjEuY3J0MDUuZ2xvYmFsc21nb15jb20vZ3NhbHBoYXN
22 jAOBGNVHQ8BAMCBAAwYkGCCsGAQUFBwEBBHB0wezBCBgggrBgEFBQcwoAoY2aHR0cDovL3N
23 ZTIuYXNjaWwzZ2wzY29tL2NhY2VydC9nc2FscGhhc2hhMmcyZjEuY3J0MDU
24 Jx5Don6BrVQuXY7Rn4Qy8b1cU3aY530+UsV45U5ErZZ/43z4y5Wj7I/mCC9
25 SaYeRB1V6c79hD8HtbwZkmywxyVy3V21Rm7WRI1Q1cnTLmynIPhs0uVy11d
26 9XJyG4CskUr1jPEJXvmJAta1dbbdctE1kb2jNS+MdrIbYmsIYWQwESW60d
27 XCnHBv46wuxSuDyypcOrzdVjJ+hUYNS53F1pH/Tj5bTXXeS/RTTfuW4S5Y6G
28 PKNg
29 -----END CERTIFICATE-----
30 -----BEGIN CERTIFICATE-----
31 MIIEtTCCAzWgAwIBAgILBAAAAAABRE7wNjEwDQYJKoZIhvcNAQELBQAwVzE
32 A1UEBHMtQXNjaWwzZ2wzY29tL2NhY2VydC9nc2FscGhhc2hhMmcyZjEuY3J0
33 b3QgQ0EgGzAzBGNVBAWTEkdsb2JhbHNpZ24uY24uUm9vdCBBDQTAeFw0xNDAYMjA

```

请把 server.cer 和 server.key 这两个文件保存到同一个目录下，例如放到/etc/ssl/crt/目录下。

第四步：更新 httpd.conf 配置文件

用文本编辑器打开 httpd.conf 并更新以下内容

```
<VirtualHost xxx.xxx.xxx.xxx:443>
DocumentRoot "/var/www/html"
ServerName www.domain.com

SSLEngine on
SSLCertificateFile /etc/ssl/crt/server.cer           //公钥文件（GlobalSign 颁发）
SSLCertificateKeyFile /etc/ssl/crt/server.key       //私钥文件
</VirtualHost>
```

按照以上的步骤配置完成后，重新启动 Apache 后就可以使用 <https://www.domain.com> 来访问了。

如有任何疑问或问题请直接与我们联系，谢谢！