

---

# Apache SSL Certificate Deployment Guide



沃通电子认证服务有限公司

WoSignCA Limited

## Content

1.The environment for installing the SSL certificate .....	3
1.1 Brief introduction of SSL certificate installation environment .....	3
1.2 Network environment requirements .....	3
2.Created a Certificate Signing Request (CSR).....	4
3.Installation of SSL certificate .....	5
3.1 Get SSL certificate.....	5
3.2 Extract SSL certificate.....	5
3.3 Install SSL certificate .....	5
3.4 Test the SSL certificate.....	6
4.Install Secure signature.....	7
5.Backup of SSL certificate.....	7
6.Restore of SSL certificate.....	7

### **Contact information of technical support**

Email of technical support: [support@wosign.com](mailto:support@wosign.com)

Hotline of technical support: +86-755-8600 8688

Website of technical support: <https://bbs.wosign.com>

Company official website address: <https://www.wosign.com>

## 1.The environment for installing the SSL certificate

### 1.1 Brief introduction of SSL certificate installation environment

Centos 6.4;

Install Apache version 2.2.\* or above;

Openssl 1.0.1+;

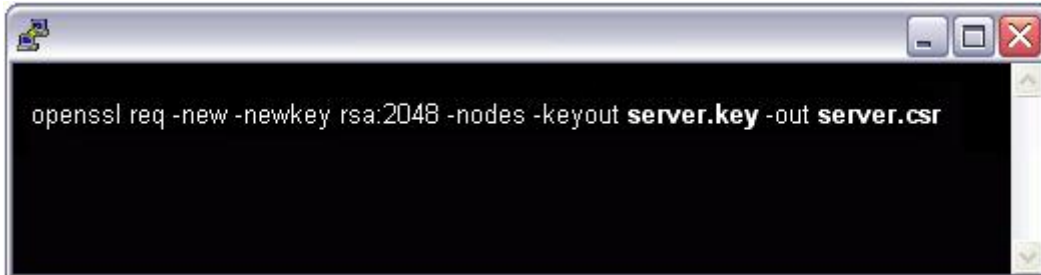
SSL certificate (Note: this guide uses the OV SSL certificate which the domain name is s.wosign.com to operate, other version of the certificate are also common.) .

### 1.2 Network environment requirements

Please ensure the site is a legitimate e domain address, which can normal access by typing it's domain name http://XXX.

## 2.Created a Certificate Signing Request (CSR)

1. Login to your server via your terminal client (ssh). At the prompt, type:  
`openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr`



```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
```

2. This will begin the process of generating two files: the Private-Key file for the decryption of your SSL Certificate, and a certificate signing request (CSR) file used to apply for your SSL Certificate.

## 3. Installation of SSL certificate

### 3.1 Get SSL certificate

When you get a zip file with password after you apply the certificate from wosign successfully. You need to enter the password to extract the file, after extract the file you will get 4 files: for Apache、for IIS、for Nginx、for Other Server. These are different formats for different servers. We will need to use the certificate from for Apache.



for Apache.zip	Unzip this file	2014/8/20 14:00	WinRAR ZIP
for IIS.zip		2014/8/20 14:00	WinRAR ZIP
for Nginx.zip		2014/8/20 14:00	WinRAR ZIP
for Other Server.zip		2014/8/20 14:00	WinRAR ZIP

Figure 2

### 3.2 Extract SSL certificate

Open the file for Apache, you can see three files, including public key, certificate chain, as shown in Figure 3



1_root_bundle.crt	Certificate chain	2014/8/20 14:00
2_test.wosign.com.crt	Public key	2014/8/20 14:00

Figure 3

### 3.3 Install SSL certificate

1、Open the file httpd.conf which is under the file conf in Apache directory, and you can find the code below.

```
#LoadModule ssl_module modules/mod_ssl.so
```

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

Delete the char “#”

Save and exit.

2、Open the file httpd-ssl.conf which is under the file conf/extra in Apache directory, find the following configuration statement in the configuration file:

a. Add the protocol and modify the ciphers.

SSLProtocol all -SSLv2 -SSLv3

SSLCipherSuite ALL:!DH:!EXPORT:!RC4:+HIGH:+MEDIUM:!LOW:!aNULL:!eNULL

b. Configure the server certificate public key to the path

SSLCertificateFile conf/ssl/test.wosign.com.crt (public key)

c. Configure the server certificate private key to the path

SSLCertificateKeyFile conf/ssl/test.wosign.com.key (private key)

e. Configure the server certificate chain to the path

#SSLCertificateChainFile conf/ssl/root\_bundle.crt(certification chain) delete the char “#”

3、 Enter the Apache installation directory under the bin directory, run the following command

./apachectl -k stop

./apachectl -k start

### 3.4 Test the SSL certificate.

Access to <https://yourdomain.com> (the domain of the applied SSL certificate) Test your SSL certificate is installed successfully or not. If successful, the browser will display a safety lock sign.

## 4. Install Secure signature

*(Secure signature only works on OV and EV SSL certificate now)*

After you purchased the SSL WoSign certificate, you can get a trusted website security certification logo which shows your company's certificate information freely. It can greatly enhance the user's online trust, to facilitate more online transactions. So we suggest you to add the following code which can dynamically display the trusted site security certification logo on your homepage or other page.

If you want display the certificate logo on English website, add the code on the English web page below:

```
<SCRIPT LANGUAGE="JavaScript" TYPE="text/javascript" SRC="https://seal.wosign.com/tws-en.js"></SCRIPT>
```



## 5. Backup of SSL certificate

Please save the file and password you receive.

## 6. Restore of SSL certificate

Repeat 3.3 operation.