Apache SSL Certificate Deployment Guide

沃通电子认证服务有限公司

WoSignCA Limited

Content

Contact information of technical support

Email of technical support：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.Installation of SSL certificate

2.1 Get SSL certificate

You will 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 5 files: for Apache、for IIS、for Nginx、for Other Server, for tomcat. These are different formats for different servers. We will need to use the certificate from for Apache.

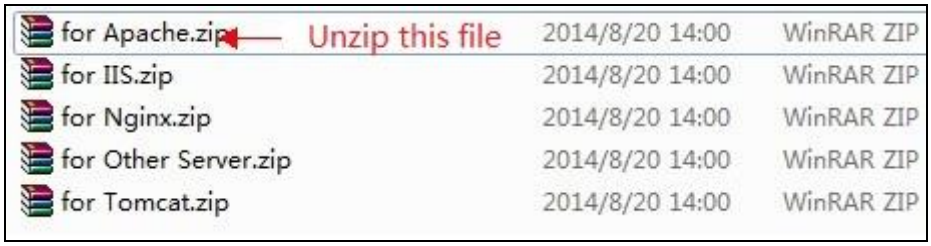

Figure 1

2.2 Extract SSL certificate

Open the file for Apache, you can see three files, including public key, private key, certificate chain, as shown in Figure 2

Figure 2

2.3 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(certificate chain) delete the char "#"

3、Enter the Apache installation directory under the bin directory, run the following command
./apachectl -k stop
./apachectl -k start

2.4 Test the SSL certificate.

Access to https://yourdomian.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.

3.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 Enlgish 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>

4.Backup of SSL certificate

Please save the file and password you receive.

5.Restore of SSL certificate

Repeat 2.3 operation。