IIS7&8 SSL Certificate Deployment Guide



沃通电子认证服务有限公司

WoSignCA Limited

©沃通电子认证服务有限公司 WoSign CA Limited All Rights Reserved





Content

| 1. The environment for installing the SSL certificate |
|--|
| 1.1 Brief introduction of SSL certificate installation environment |
| 1.2 Network environment requirements |
| 2. Import SSL certificate |
| 2.1 Get SSL certificate |
| 2.2 Import SSL certificate |
| 2.3 Distribution server certificate |
| 2.4 Test the SSL certificate7 |
| 3. Install Secure signature |
| 4. Backup of SSL certificate |
| 5. Restore of SSL certificate |

Contact information of technical support

Email of technical support: support@wosign.com Hotline of technical support: 0755-26027828 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

IIS8.0 operating system server

A website

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. Import 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. After we extra the zip file from for IIS, we can get a certificate www.xxx.com.pfx. We need to use pfx format certificate on IIS8.0.

| 🔚 for Apache.zip | 2014/8/20 14:00 | WinRAR ZIP | |
|-------------------------------|-----------------|------------|--|
| ■ for IIS.zip Unzip this file | 2014/8/20 14:00 | WinRAR ZIP | |
| E for Nginx.zip | 2014/8/20 14:00 | WinRAR ZIP | |
| tor Other Server.zip | 2014/8/20 14:00 | WinRAR ZIP | |
| 🔚 for Tomcat.zip | 2014/8/20 14:00 | WinRAR ZIP | |
| | | | |

Figure 1

2.2 Import SSL certificate

Start -> Run -> MMC, Start console -> Select menu file -> Add / remove management unit-> Select the certificate in the list->click"add"-> choose "Computer account" -> Click Finish. On the left side of the console display certificate tree list, choose "Individual"- "certificate", Right click, choose "All tasks -> Import", According to the certificate Import Wizard, import the pfx format certificate to "Automatically select the storage area according to the certificate successfully, you can see the certificate information as shown in Figure2.



| | | | x |
|---|--|-----------------------|--|
| 📀 🍠 Certificat | e Import Wizard | | |
| Certificate Stor Certificate | e stores are system areas where certificates are kept. | | |
| Windows of the certific | an automatically select a certificate store, or you can spec ate. | cify a location f | for |
| Aut | matically select the certificate store based on the type of | certificate | |
| O Plac | e all certificates in the following store | | |
| Pe | incate store: sonal | Browse | |
| File Action View Favorites File C I I I I I I I I I I I I I I I I I I | Console1 - [Console Root\Certificates (Local Computed Window Help | uter)\Personal\(| Certificates] |
| Console Root | Issued To | Expiration Date | Intended Purnoses |
| ✓ Certificates (Local Computer) ✓ Personal ✓ Certificates ▷ Trusted Root Certification ▷ Trusted Publishers ▷ Untrusted Certificates ▷ Trusted Publishers ▷ Untrusted Certificates ▷ Trusted People ▷ Client Authentication Issu ▷ Remote Desktop ▷ Certificate Enrollment Req ▷ Smart Card Trusted Roots ▷ Trusted Devices ▷ Web Hosting | WoSign Class 3 OV Server CA | 1/23/2017 2/9/2017 | Client Authenticati Client Authenticati |
| , | | | |
| < | | | > |

Figure 2



2.3 Distribution server certificate

Open the IIS8.0 manager panel, find the site to be deployed certificate, click on the "binding" as shown in Figure 3



Figure 3

Setting parameters

Select "binding" -> "add" -> "Type selection HTTPS" -> "Port 443" -> "SSL certificate [the name of the imported certificate]" -> "Determine", SSL default port 443 port, (Please don't make any changes. If you use other ports such as: 8443, you must enter the https://www.domain.com:8443). Seen as figure 4.



| | | | Site Bi | ndings | | ? X |
|--------------------------------|--------------------------------------|------------------|-----------------|-------------------------|--------|----------------|
| Type http | Host Name s.wosign.com | Port 80 | IP Address * | Binding Informa | [| Add |
| Add Site Binding ? X | | | | | | Edit Remove |
| <u>T</u> ype: https | <u>I</u> P addr ✓ All Un | ess: assigned | | P <u>o</u> rt: ✓ 443 | | Browse |
| Host nar | ne: re Server <u>N</u> ame Indica | ition | | | | |
| SSL certi <u>i</u> s.wosign | ficate: com | | ~ | Select | View | |
| | | | | ОК | Cancel | Close |

Figure 4

2.4 Test the SSL certificate.

Input the address in browser address bar: https://s.wosign.com (the domain of the applied SSL certificate) Test your SSL certificate is installed successfully or not. If successful, the browser address bar will display a safety lock sign. Please notice: if there is unsafe content in your web site, it will show "Do you want to show the content that is not secure". Please modify your website delete the unsafe content (like Flash、CSS、Java Script, picture and so on).



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 2.2 operation.