
IIS7.0&8.0SSL 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. Generate the CSR	4
2.1 Generate the private key files and CSR files	4
2.2 Complete the production of the private key and CSR file.....	5
2.3 Submit CSR file.....	6
3. Import SSL certificate.....	7
3.1 Get SSL certificate.....	7
3.2 Import SSL certificate.....	7
3.3 Distribution server certificate	9
3.4 Test the SSL certificate.....	10
4. Install Secure signature.....	11
5. Backup of SSL certificate	12
6. Restore of SSL certificate	13

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

IIS 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.)

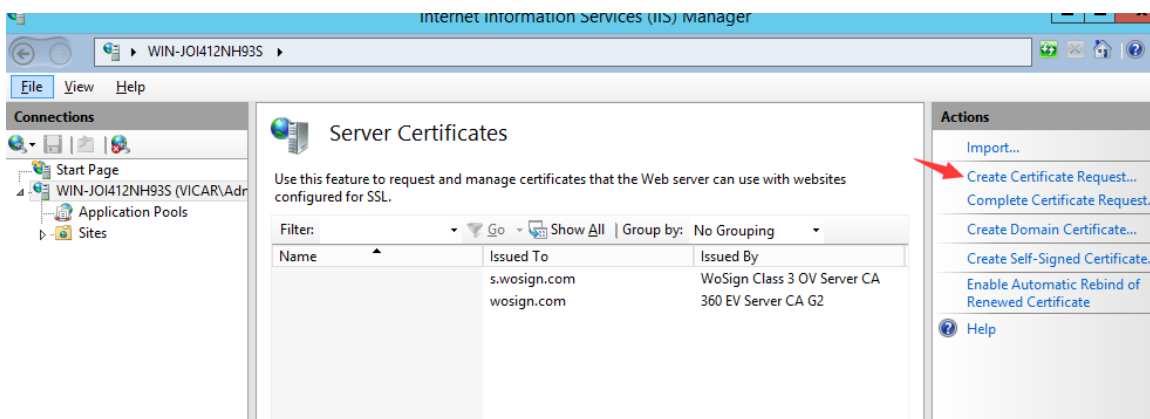
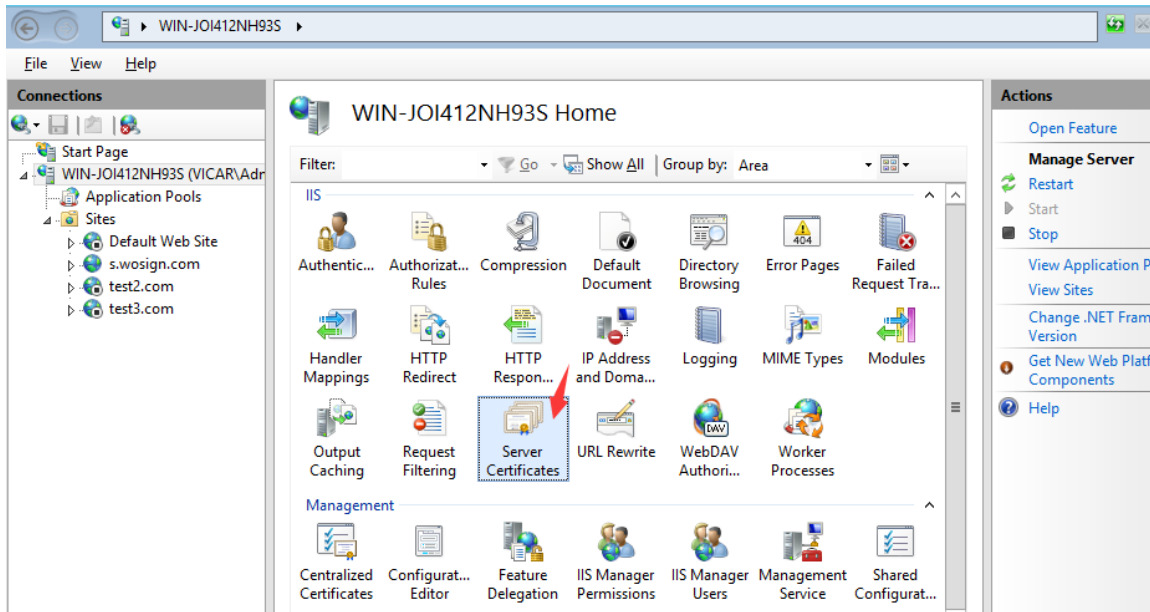
1.2 Network environment requirements

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

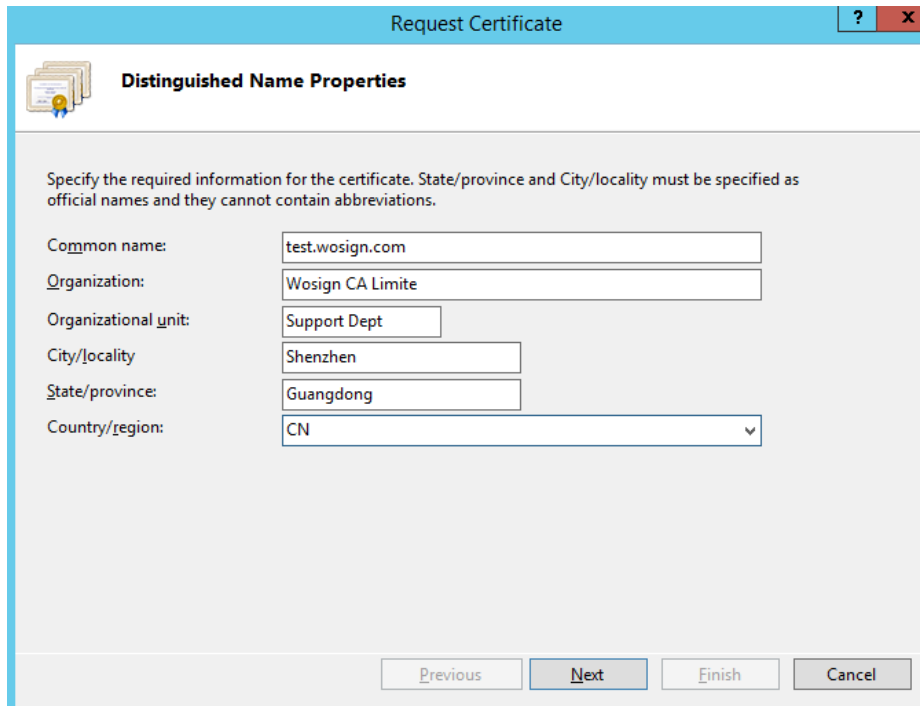
2. Generate the CSR

2.1 Generate the private key files and CSR files

Enter the IIS Manager, and select the server certificate settings option like following figures.



Fill in the certificate details

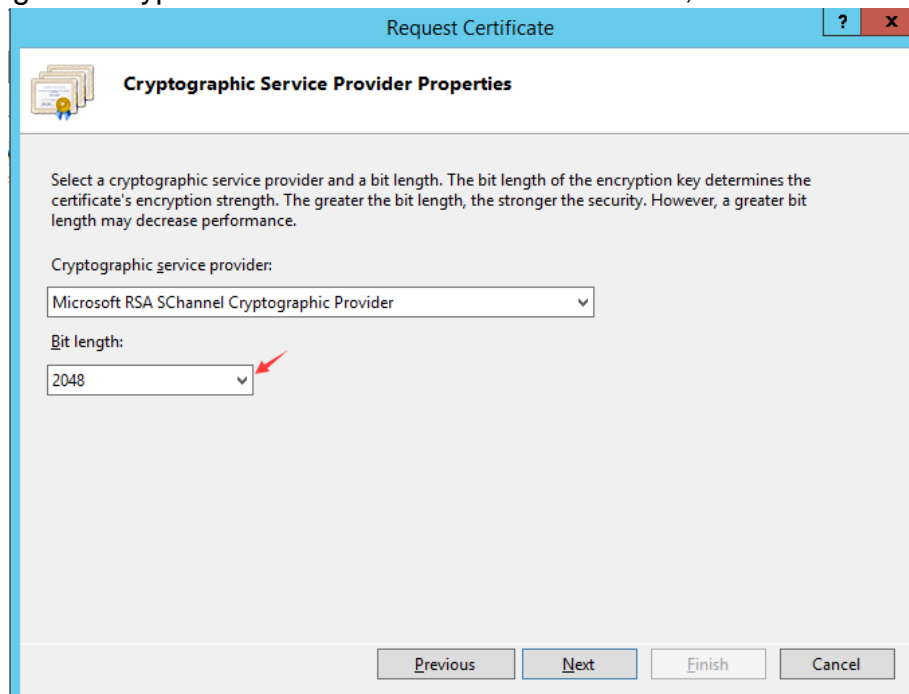


The dialog box is titled "Request Certificate" and "Distinguished Name Properties". It contains the following fields:

Common name:	test.wosign.com
Organization:	Wosign CA Limite
Organizational unit:	Support Dept
City/locality:	Shenzhen
State/province:	Guangdong
Country/region:	CN

Buttons at the bottom: Previous, Next, Finish, Cancel.

Select the Bit length of the key, default length is 1024, please select the 2048 to ensure the encryption strength. Encryption services choose the default one, and Click "next",



The dialog box is titled "Request Certificate" and "Cryptographic Service Provider Properties". It contains the following fields:

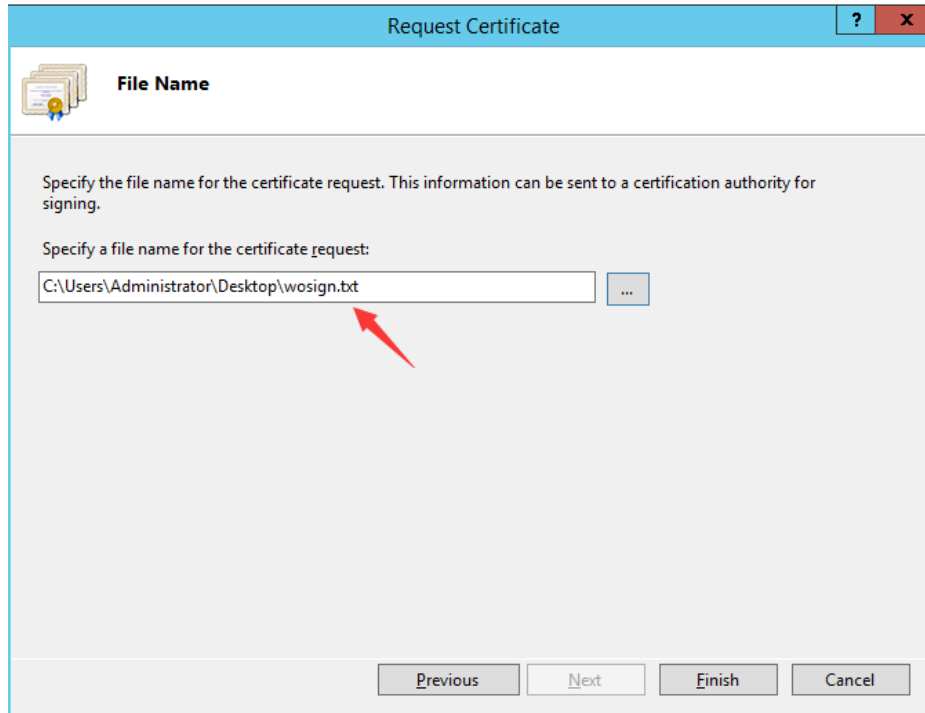
Cryptographic service provider:	Microsoft RSA SChannel Cryptographic Provider
Bit length:	2048

Buttons at the bottom: Previous, Next, Finish, Cancel.

2.2 Complete the production of the private key and CSR file

After generate the CSR file, it is recommended that you test the generated CSR file is correct,

please click here to test your CSR file. Please send the CSR file to WoSign. Please do not do any change of your server and wait for the certificate issued.



2.3 Submit CSR file





When you apply the certificate on <https://buy.wosign.com/free/?lan=en> You can choose generate CSR file by yourself after you do the domain verification. Choose option 2 below.




SSL Certificate signing request(CSR) Generation Instructions'. A large text area is labeled 'Please paste Certificate Signing Request'. To the right of the text area, there is a 'Please notice:' section with two points: '1. System don't care the CSR content and signature algorithm except the key length that must be equal to or greater than 2048 bits;' and '2. No need to enter other information while you generate the CSR file.' At the bottom, there are two green buttons: 'Check CSR' and 'Submit'." data-bbox="229 590 739 870"/>

3. Import SSL certificate

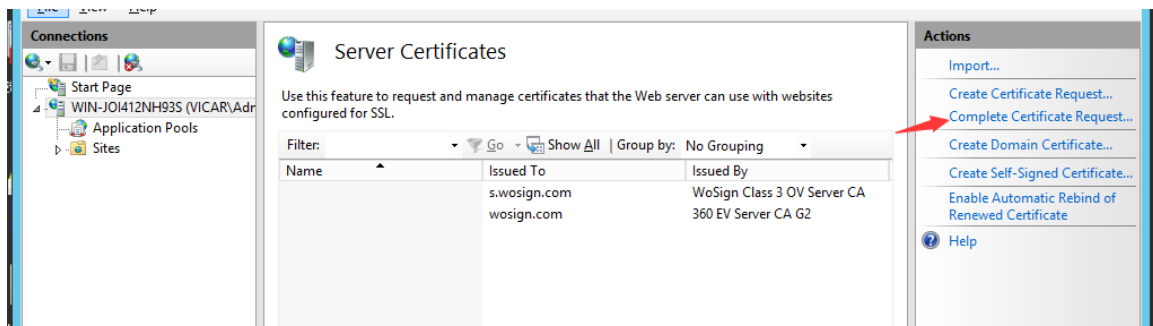
3.1 Get SSL certificate

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 4 files: **for Apache、for IIS、for Nginx、for Other Server. These are different formats for different servers.** After we extra the zip file from for IIS, we can get 3 crt certificate.

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

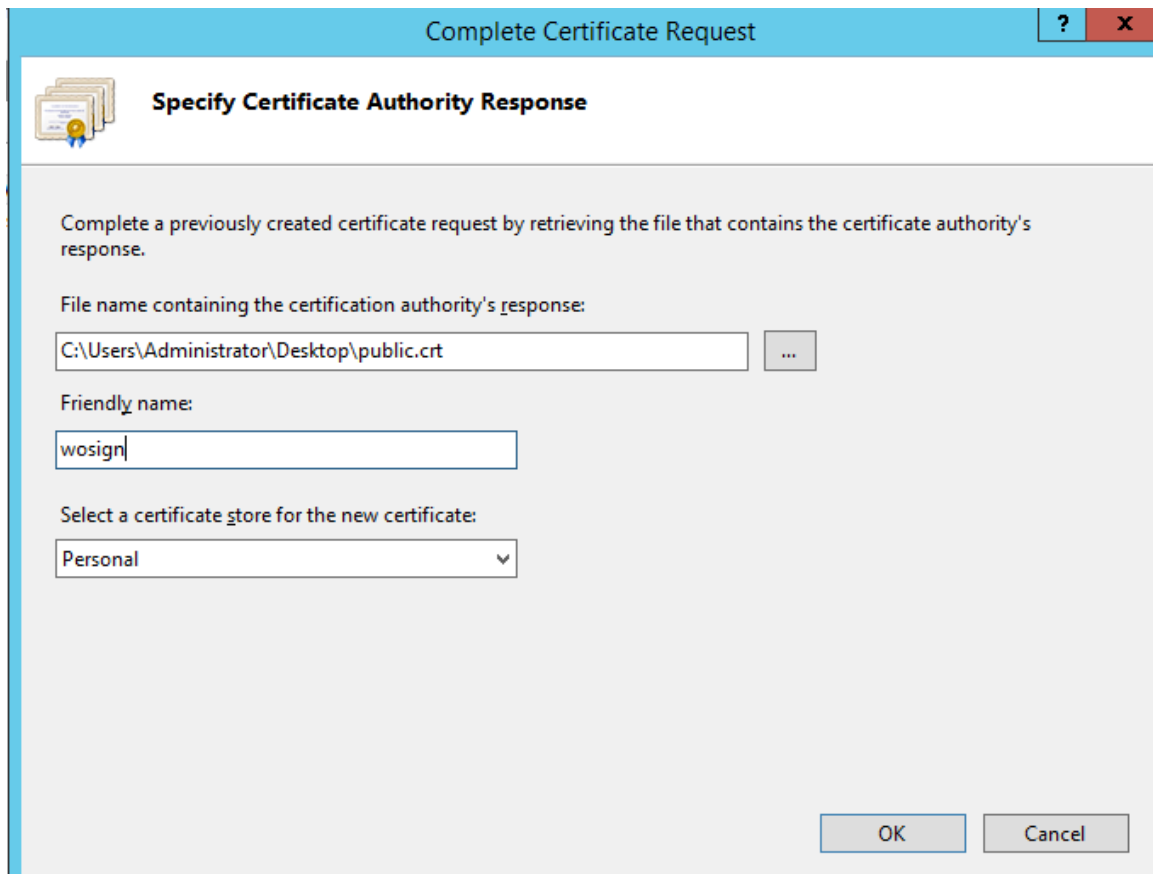
 1_cross_Intermediate.crt	2015/6/16 10:17	安全证书
 2_issuer_Intermediate.crt	2015/6/16 10:17	安全证书
 3_test.wosign.com.crt	2015/6/16 10:17	安全证书

3.2 Import SSL certificate



Extract the file 3_yourdomain.crt, upload it to your server. And click "Browse" to select the Certificate documents.

Select the certificate file, and set a name for the certificate, and complete the import of the certificate.



Import the intermediate certificate in your local MMC.

Start→Run→MMC, file→Add/remove management unit”→Select the certificate→click “add” → choose “Computer account”→Click Finish. On the left side of the console display certificate tree list, select Intermediate Certification Authorities certificate, right click, choose “All tasks”→”Import”. Import 1_cross_Intermediate.crt, 2_issuer_Intermediate.crt(File of For IIS) into the ‘Intermediate Certification Authorities’.

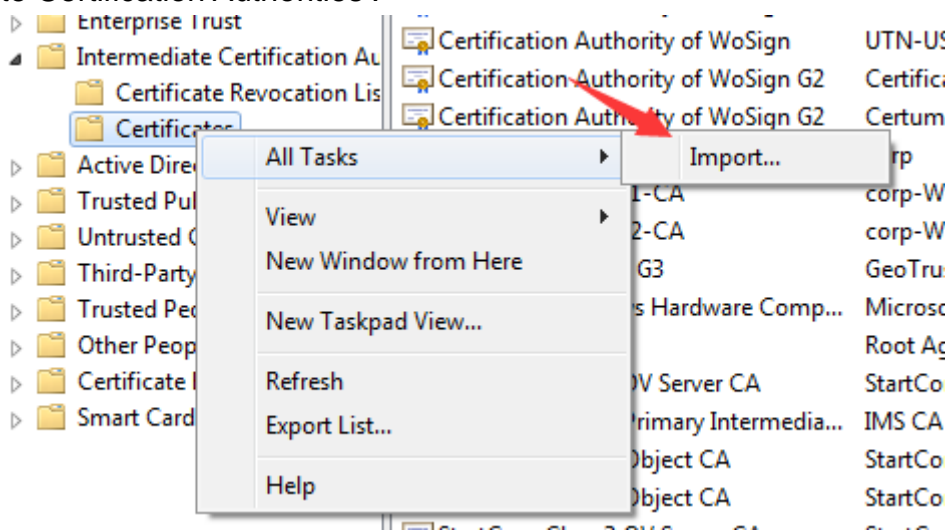


Figure 2

3.3 Distribution server certificate

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

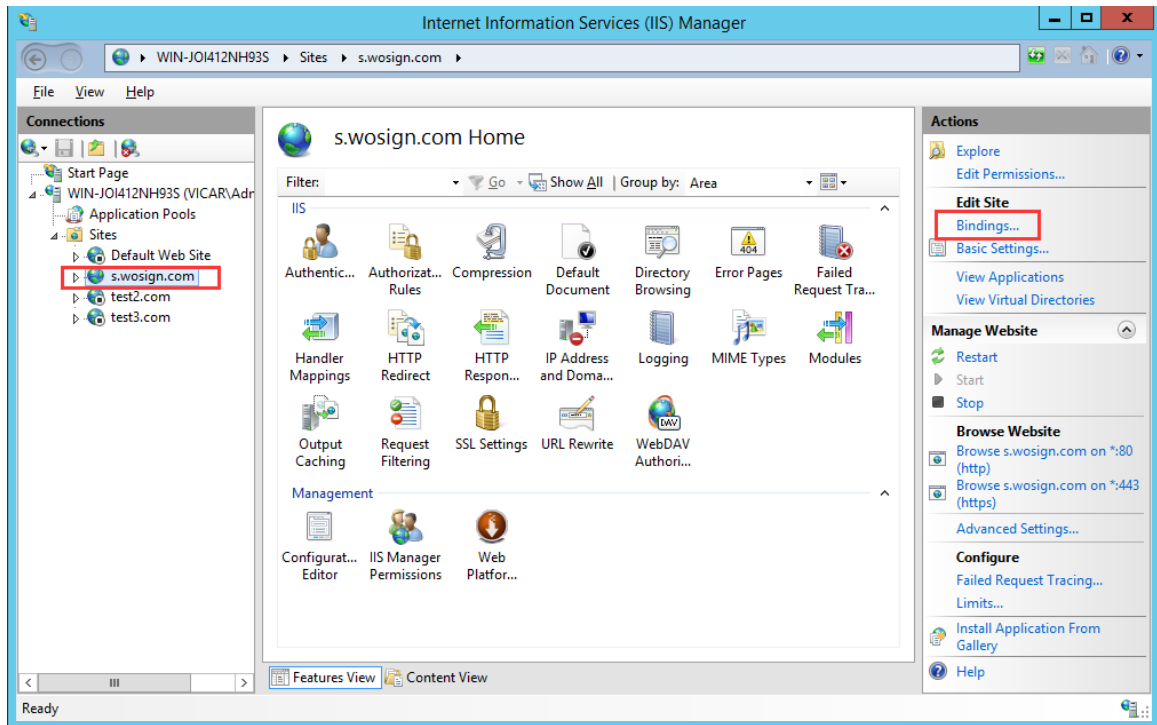


Figure 3

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.

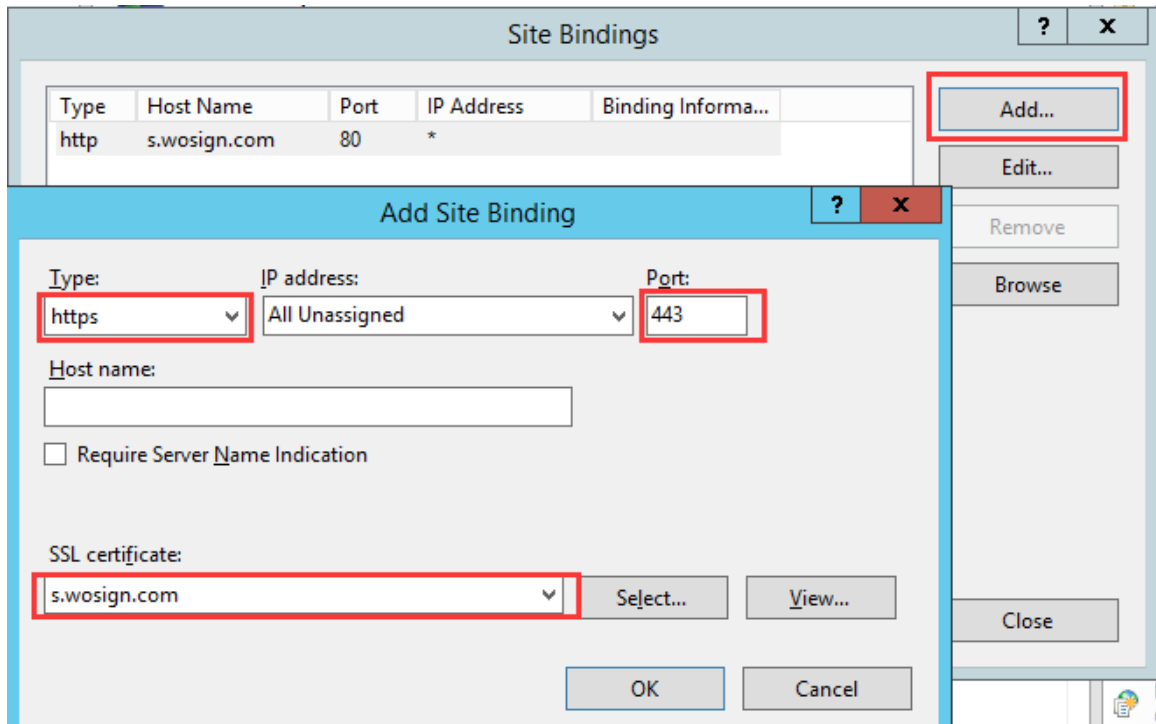


Figure 4

3.4 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).

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.

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



5. Backup of SSL certificate

When you have finished installing the certificate, please backup your certificate as follow.

1. Back to Console1, go Certificates (Local Computer)→Personal→Certificates, choose your certificate just you have installed. Right click → All Tasks → Export.

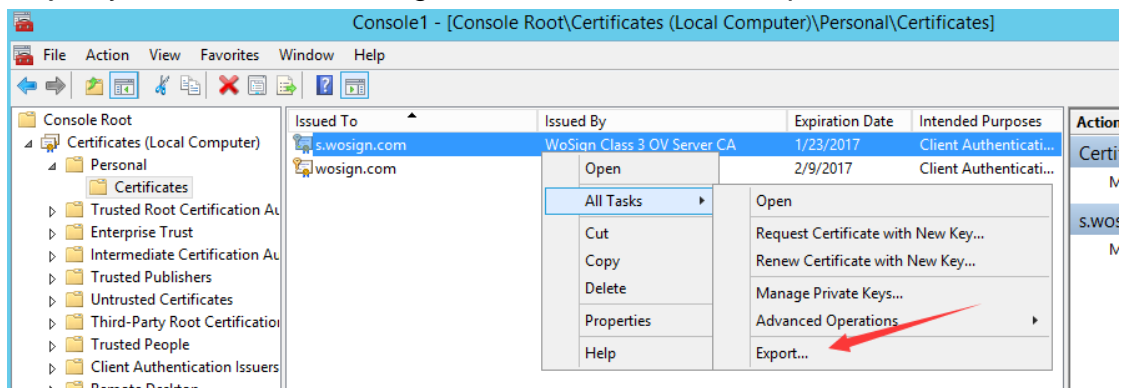
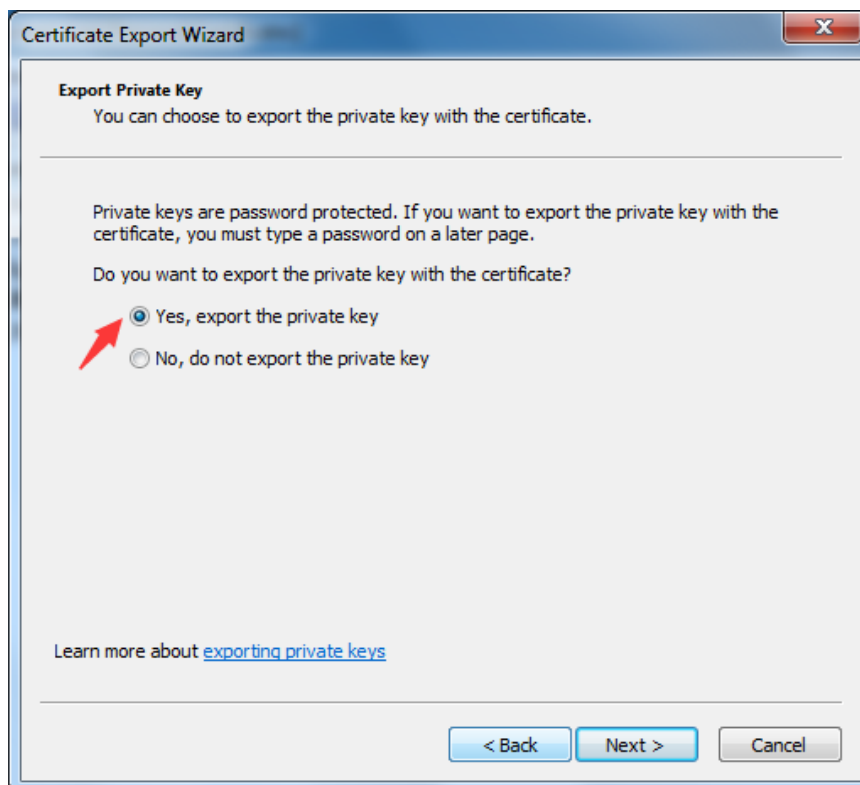
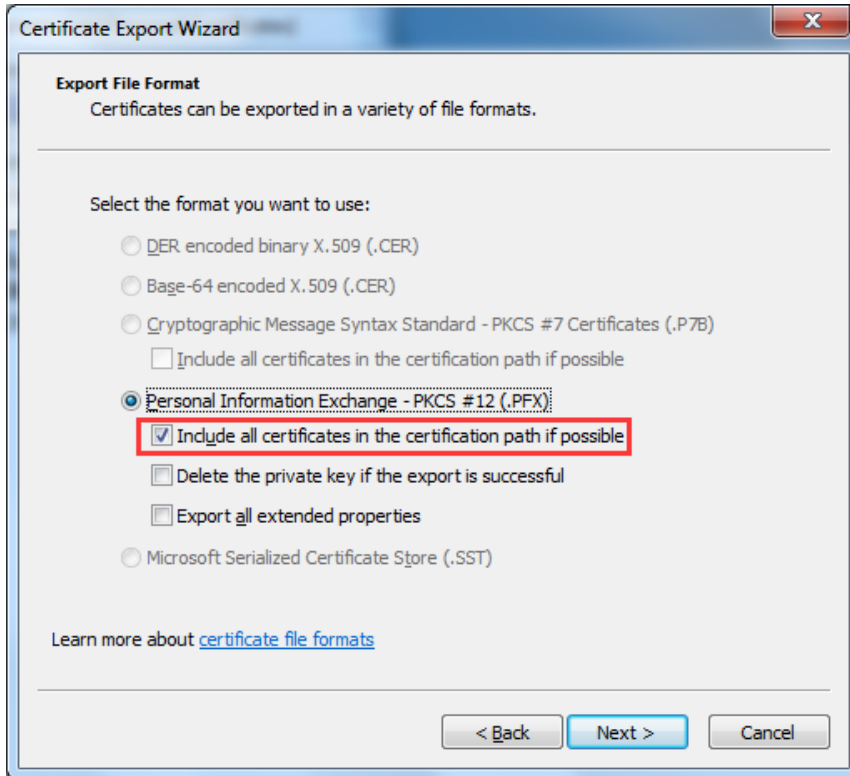


Figure 12

2. Then attend to check 'Yes, export the private key',click next.



3. Check 'Include all certificates in the certification path if possible', click next.



4. Type and confirm your password, Specify a name and path of this file, you will get a certificate PFX format. keep these in mind.

6. Restore of SSL certificate

Please reference "[IIS7.0&8.0 SSL.pdf](#)".