
IIS7.0 SSL 证书部署指南



沃通电子认证服务有限公司

WoSignCA Limited

目 录

一、	安装 SSL 证书的环境	3
1.1	SSI 证书安装环境简介	3
1.2	网络环境要求	3
二、	SSL 证书的导入	3
2.1	获取 SSI 证书	3
2.2	2018 年之前签发获取 SSI 证书	3
2.3	导入 SSL 证书	5
2.4	分配服务器证书	5
2.5	测试是否安装成功	7
三、	SSL 证书的备份	7
四、	SSL 证书的恢复	7

技术支持

用户支持邮箱: support@wosign.com
技术支持热线电话: 0755-26027828 / 0755-26027859
技术支持网页: <https://bbs.wosign.com>
公司官网地址: <https://www.wosign.com>

一、安装 SSL 证书的环境

1.1 SSL 证书安装环境简介

安装 windows server 2008 IIS7.0 操作系统服务器一台，

web 站点一个

SSL 证书一张（备注：本指南使用 s.wosign.com 域名 OV SSL 证书进行操作）





1.2 网络环境要求

请确保站点是一个合法的外网可以访问的域名地址，可以正常通过或 http://XXX 进行正常访问。

二、SSL 证书的导入

2.1 获取 SSL 证书

最终沃通数字证书系统将会给您颁发证书文件（.zip）压缩格式，当中有包含四种证书格式如：for Apache、for IIS、for Nginx、for Other Server；此时不要解压 for IIS 包。IIS 应用服务器上需要 for Nginx 里面的 crt 证书文件，然后用工具合成 pfx 格式：

 for apache.zip	2018/4/17 15:41	秒压缩工具
 for iis.zip	2018/4/17 15:41	秒压缩工具
 for nginx.zip	2018/4/17 15:41	秒压缩工具
 for other server.zip	2018/4/17 15:41	秒压缩工具

打开 for Nginx 文件可以看到公钥，如图 2


 test.wosign.com_bundle.crt	2017/11/27 15:27	安全证书	6 KB
--	------------------	------	------

图 2

私钥 key 文件，需要找到生成 CSR 一起生成出的两个文件，如图 3，其中一个为 .key 文件，若生成出来的是 .com 文件，修改一下后缀即可。


 youdomain.com.csr	CSR文件
 youdomain.com.key	私钥文件

图 3

合成工具下载地址: <https://download.wosign.com/wosign/wosigncode.exe>

合成方式: 先把 key 文件放到 for nginx 里, 再双击下载的工具, 选择证书项, 操作选项, 选择证书格式转换, 源格式选择 PEM, 目标格式选择 PFX。

证书文件: 点击后面的选择按钮, 找到 for nginx 目录, 选择 yourdomain.com_bundle.crt, 点击确定。

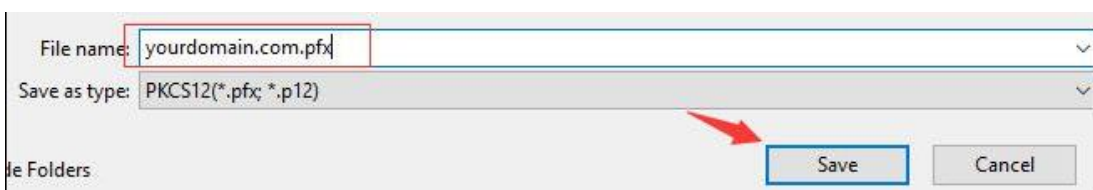
私钥文件: 点击后面的选择按钮, 找到 for nginx 目录, 选择 yourdomain.com.key, 点击确定。

私钥密码: 为空, 不用填写 (因为生成私钥的时候没有填写, 如果之前有填写过私钥密码, 这里也填写相同的私钥密码)

PFX 密码: 任意填写一个密码 (合成 PFX 格式证书后的密码, 之后在 IIS 上安装证书的时候需要使用到)



填写完毕后, 点击转换, 选择保存证书文件的位置, 填写证书名称, 推荐使用 yourdomain.com.pfx, 点击保存。



最后, 得到 pfx 格式证书。

yourdomain.com.key	12/5/2017 12:02 PM	KEY File	2 KB
yourdomain.com.pfx	3/6/2018 10:15 AM	Personal Informati...	6 KB
yourdomain.com_bundle.crt	12/5/2017 12:02 PM	Security Certificate	6 KB

2.2 2018 年之前签发获取 SSI 证书

颁发证书文件 (.zip) 压缩格式，当中有包含五种证书格式如：for Apache、for IIS、for Nginx、for Tomcat、for Other Server；IIS 应用服务器上只需要 for IIS 里面的 PFX 证书文件即可。

for Apache.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for IIS.zip ← 解压此文件	2014/8/20 14:00	WinRAR ZIP 压缩...
for Nginx.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Other Server.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Tomcat.zip	2014/8/20 14:00	WinRAR ZIP 压缩...

2.3 导入 SSL 证书

开始 -> 运行 -> MMC，启动控制台程序 -> 选择菜单“文件 -> 添加/删除管理单元” -> 列表中选择“证书” -> 点击“添加” -> 选择“计算机帐户” -> 点击完成。在控制台的左侧显示证书树形列表，选择“个人” - “证书”，右键单击，选择“所有任务-> 导入”，根据“证书导入向导”的提示，将.pfx 格式文件导入“**根据证书内容自动选择存储区**”。（注意导入过程中勾选该选项，并且需要输入密码）导入成功后，可以看到如图 1 所示的证书信息

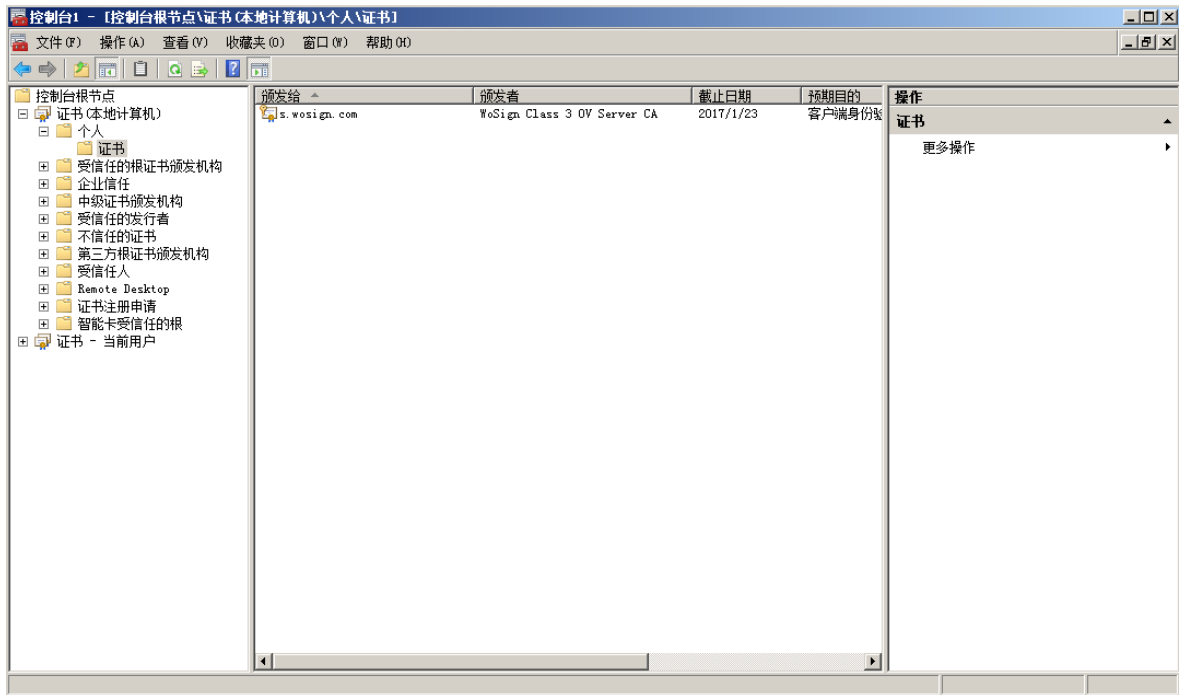


图 2

2.4 分配服务器证书

打开 IIS7.0 管理器面板，找到待部署证书的站点，点击“绑定”如图 3

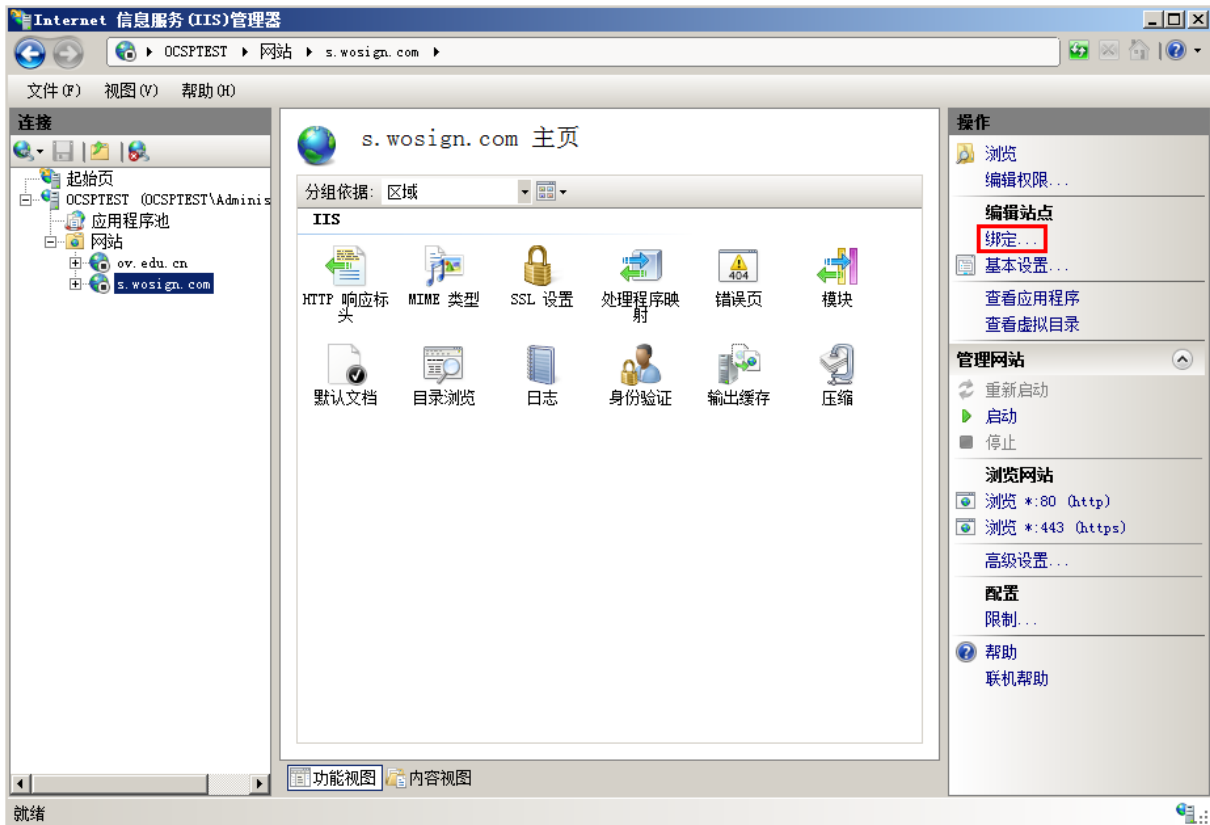


图 3

设置参数

选择“绑定”->“添加”->“类型选择 https”->“端口 443”->“ssl 证书【导入的证书名称】”->“确定”，SSL 缺省端口为 443 端口，（请不要随便修改。如果您使用其他端口如：8443，则访问时必须输入：https://www.domain.com:8443）。如图 4

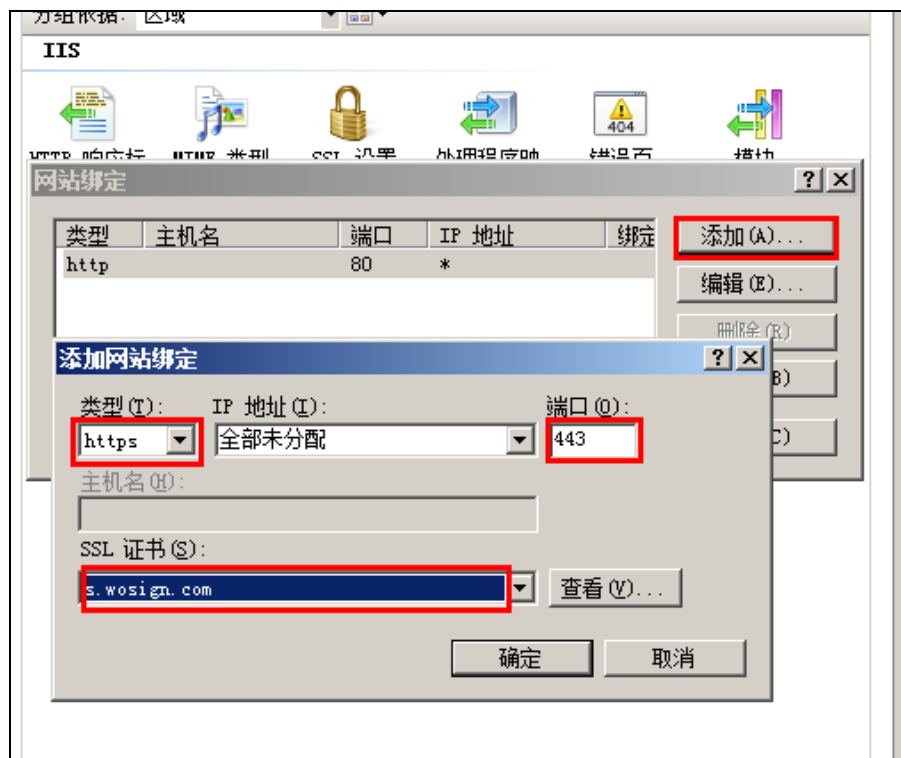


图 4

2.5 测试是否安装成功

重启 IIS7.0 服务，在浏览器地址栏输入：<https://www.yourdomain.com> (申请证书的域名)测试您的 SSL 证书是否安装成功，如果成功，则浏览器下方会显示一个安全锁标志。请注意：如果您的网页中有不安全的元素，则会提供“是否显示不安全的内容”，赶紧修改网页，删除不安全的内容(Flash、CSS、Java Script 和图片等)。

备注：安装完 ssl 证书后部分服务器可能会有以下错误，请按照链接修复

- a. 加密协议和安全套件：<https://bbs.wosign.com/thread-1284-1-1.html>
- b. 部署 https 页面后出现排版错误，或者提示网页有不安全的因素，可参考以下链接：<https://bbs.wosign.com/thread-1667-1-1.html>

三、SSL 证书的备份

请保存好收到的证书压缩包文件及密码，以防丢失

四、SSL 证书的恢复

重复 2.3-2.4 操作即可。