

IIS7.0 SSL 证书部署指南



沃通电子认证服务有限公司

WoTrus CA Limited

©2004-2017 沃通电子认证服务有限公司 WoTrus CA Limited All Rights Reserved

目 录

一、SSL 证书的导入	3
1.1 获取 SSL 证书.....	3
1.2 导入 SSL 证书.....	5
1.3 分配服务器证书.....	8
1.4 测试是否安装成功.....	9
二、SSL 证书的备份	9
三、SSL 证书的恢复	9

技术支持联系方式

用户支持邮箱：support@wotrus.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、SSL 证书的导入

1.1 获取 SSL 证书

成功在沃通申请证书后，会得到一个.zip 压缩包文件，解压后得到三个文件夹：

ApacheServer、NginxServer、OtherServer，不同服务器或设备要求不同的格式，IIS 需要用到 NginxServer 里面的证书文件，并使用 wosigncode 工具合成 PFX 格式，如下图：

名称	修改日期	类型
ApacheServer	2023/3/31 16:38	文件夹
NginxServer	2023/3/31 16:38	文件夹
OtherServer	2023/3/31 16:38	文件夹

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

私钥 key 文件，需要找到生成 CSR 一起生成出的两个文件，如下图(若创建 CSR 时选择一键生成 CSR，私钥文件为当时浏览器自动下载的.key 文件)。



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

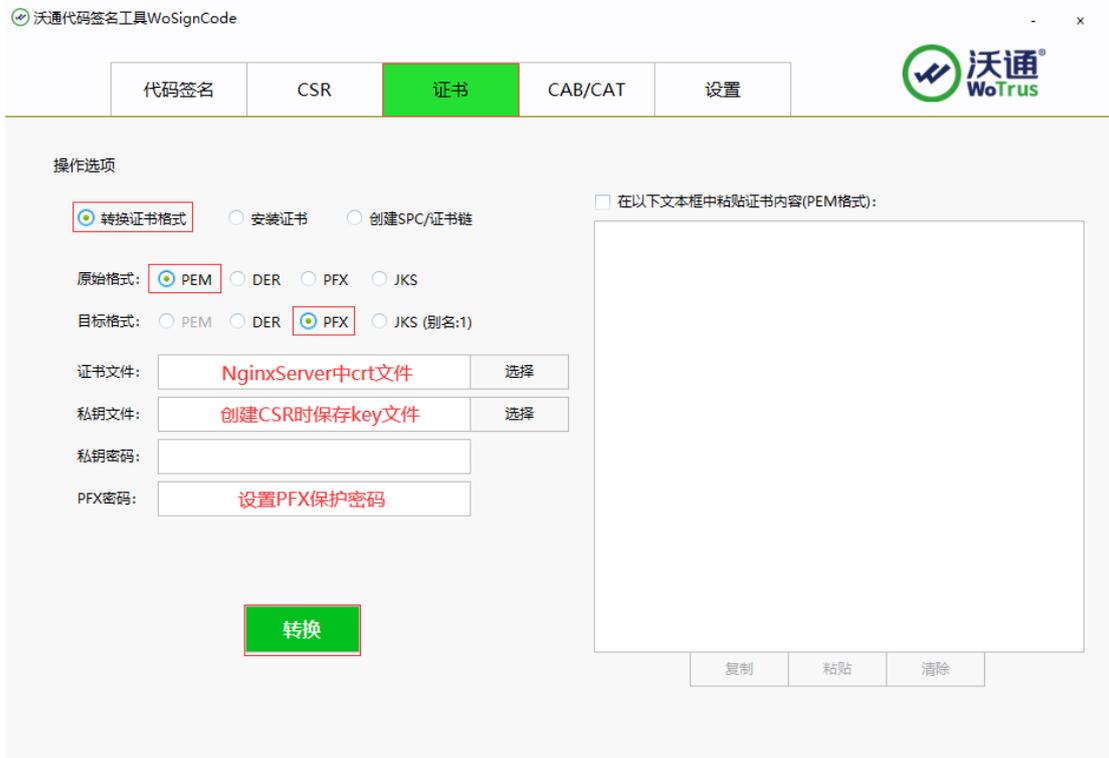
合成方式：双击下载的工具，选择证书项，操作选项，选择证书格式转换，源格式选择 PEM，目标格式选择 PFX。

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

私钥文件：点击后面的选择按钮，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）



沃通代码签名工具WoSignCode

代码签名 CSR **证书** CAB/CAT 设置

操作选项

转换证书格式 安装证书 创建SPC/证书链

原始格式: PEM DER PFX JKS

目标格式: PEM DER PFX JKS (别名:1)

证书文件: 选择

私钥文件: 选择

私钥密码:

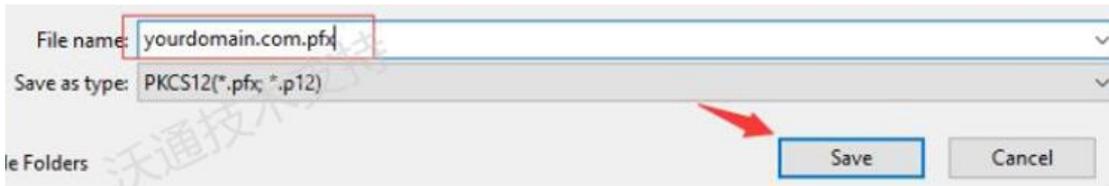
PFX密码:

转换

在以下文本框中粘贴证书内容(PEM格式):

复制 粘贴 清除

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。



File name:

Save as type: PKCS12(*.pfx; *.p12)

Save Cancel

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

1.2 导入 SSL 证书

1. 登录到 IIS7 (7.5) 所在的服务器，点击左下角的开始菜单，输入 MMC，运行 mmc.exe，具体见图 1、2；



图 1



图 2

2. 在弹出的控制台界面上，点击“文件” - “添加删除管理单元”，见图 3；

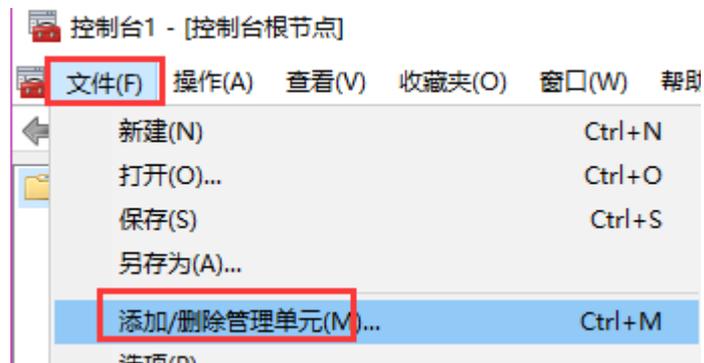


图 3

3. 在新弹出的界面左侧“可用的管理单元中”，找到“证书”，点击中间的“添加”，选择“计算机账户” - “本地计算机”，具体见图 4、5、6；

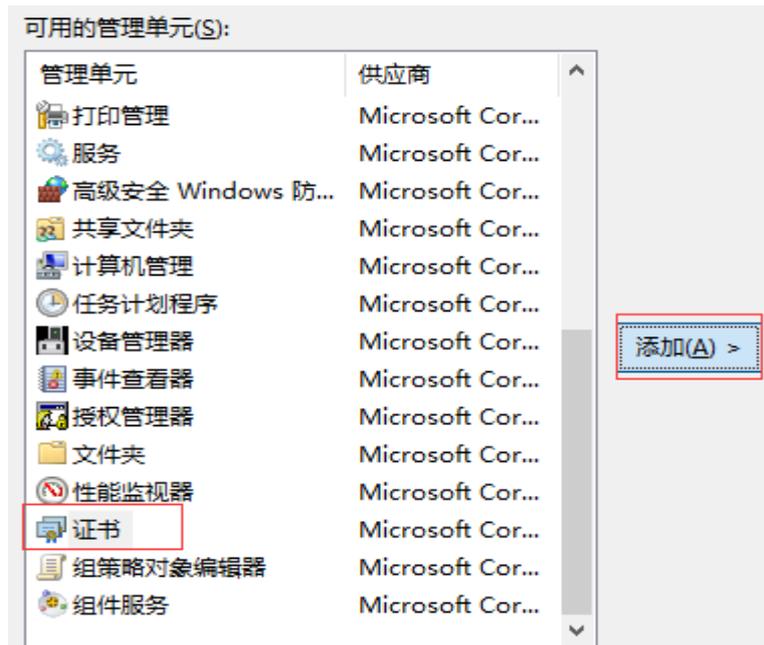


图 4

证书管理单元

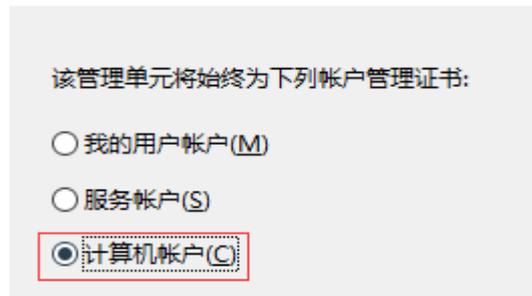


图 5

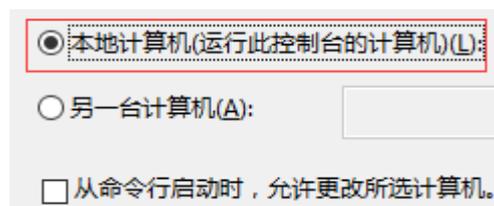


图 6

4. 双击控制台左侧的“证书(本地计算机)”，右键列表中的“个人”，选择“所有任务”
- “导入”，具体见图 7；

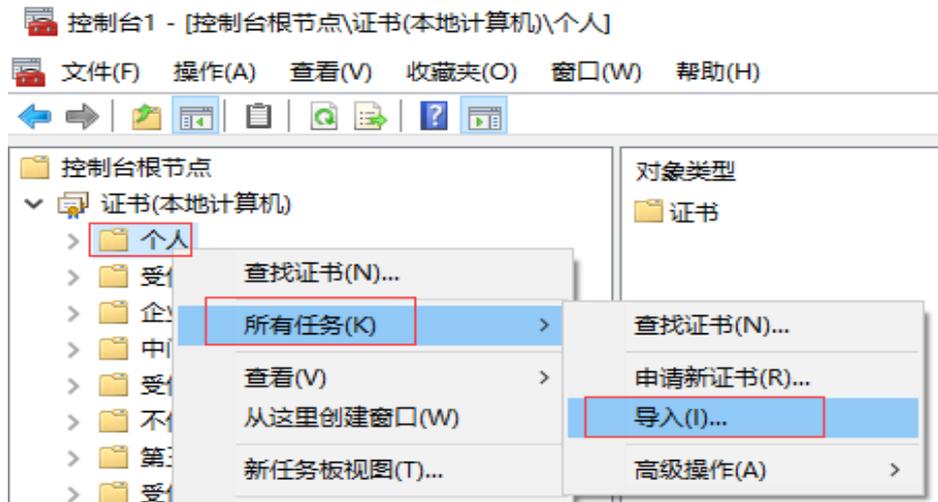


图 7

5. 点击“下一步”-“浏览”，选择“个人信息交换”，然后选择之前合成好的.pfx证书导入，具体见图 8；



图 8

6. 选择 pfx 证书后，点击“打开”-“下一步”，输入之前合成 pfx 时设置的密码，点击“下一步”，选择“根据证书类型，自动选择存储机构”，点击“下一步”-“完成”，具体见图 9；

Windows 可以自动选择证书存储，你也可以为证书指定一个位置。

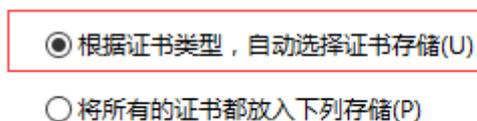


图 9

证书导入完成后，在“个人”-“证书”目录下，可见到该域名证书



1.3 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

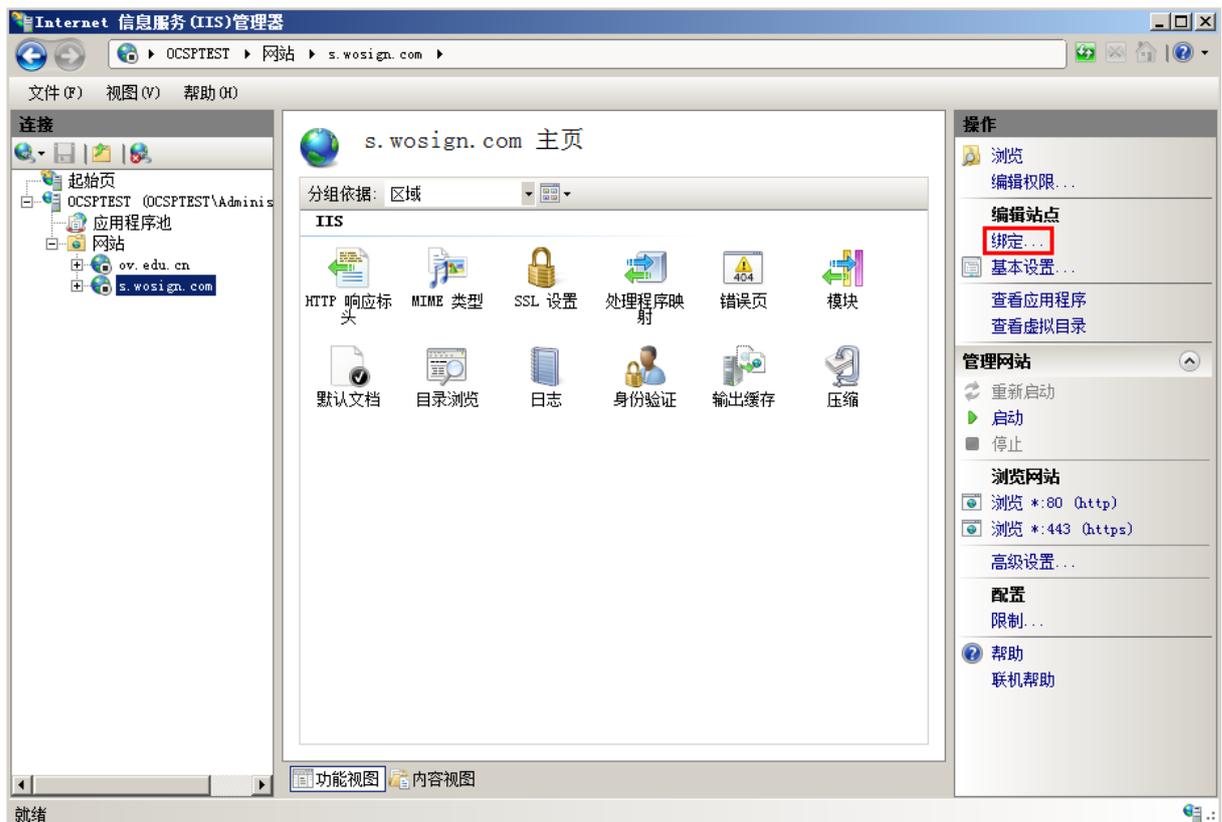


图 3

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

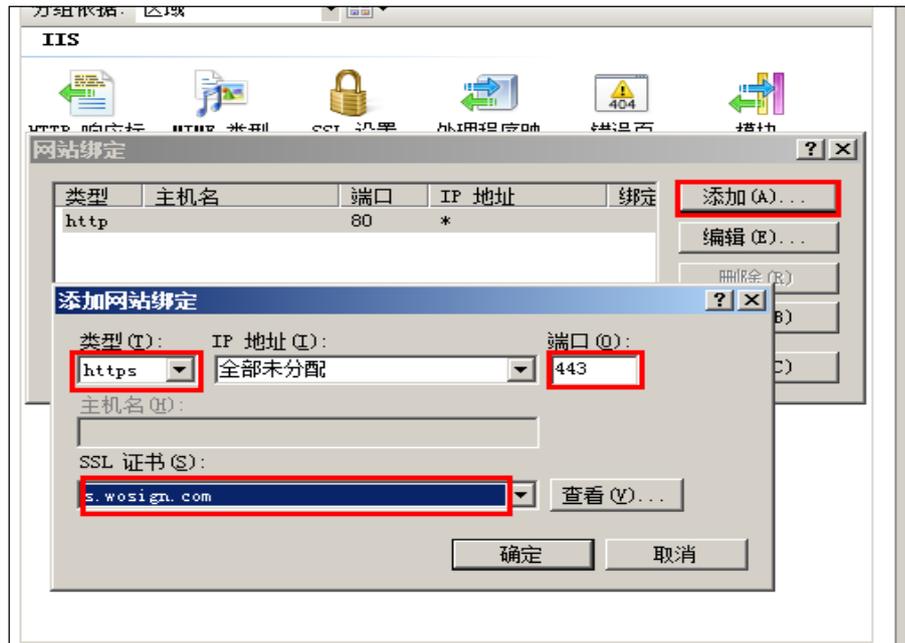


图 4

1.4 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

- 加密协议和安全套件：<https://bbs.wosign.com/thread-1284-1-1.html>
- 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>

二、SSL 证书的备份

请保存好收到的证书压缩包文件及自己生成 csr 一起的 .key 文件，以防丢失

三、SSL 证书的恢复

重复 1.2-1.3 操作即可。