

Exchange 2013 + SSL 证书安装文档



沃通电子认证服务有限公司

WoTrus CA Limited

目录

一、 获取 SSL 证书.....	2
1.1、选择 SSL 证书.....	2
1.2、合成 SSL 证书.....	3
二、 安装 SSL 证书.....	4
2.1、导入 SSL 证书.....	4
2.2、绑定 SSL 证书.....	6
三、 测试 SSL 访问.....	7
四、 备份 SSL 证书.....	7

技术支持联系方式

技术支持邮箱: support@wosign.com

技术支持热线电话: 0755-26027828 / 0755-26027859 / 0755-26027827

技术支持论坛: <https://bbs.wosign.com>

公司官网地址: <https://www.wosign.com>

一、获取 SSL 证书

1.1、选择 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：

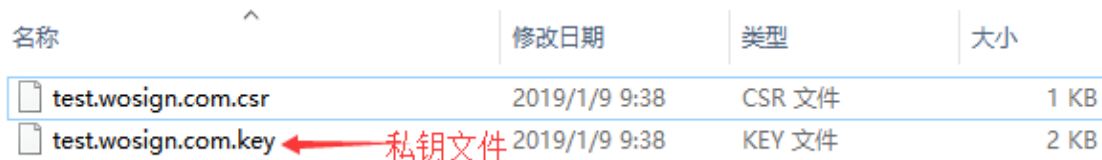
ApacheServer、NginxServer、OtherServer，不同服务器或设备要求不同的格式，Exchange 需要用到 NginxServer 里面的证书文件，如下图。



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

名称	修改日期	类型	大小
test.wosign.com_bundle.crt	2017/4/6 20:58	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)



名称	修改日期	类型	大小
test.wosign.com.csr	2019/1/9 9:38	CSR 文件	1 KB
test.wosign.com.key	2019/1/9 9:38	KEY 文件	2 KB

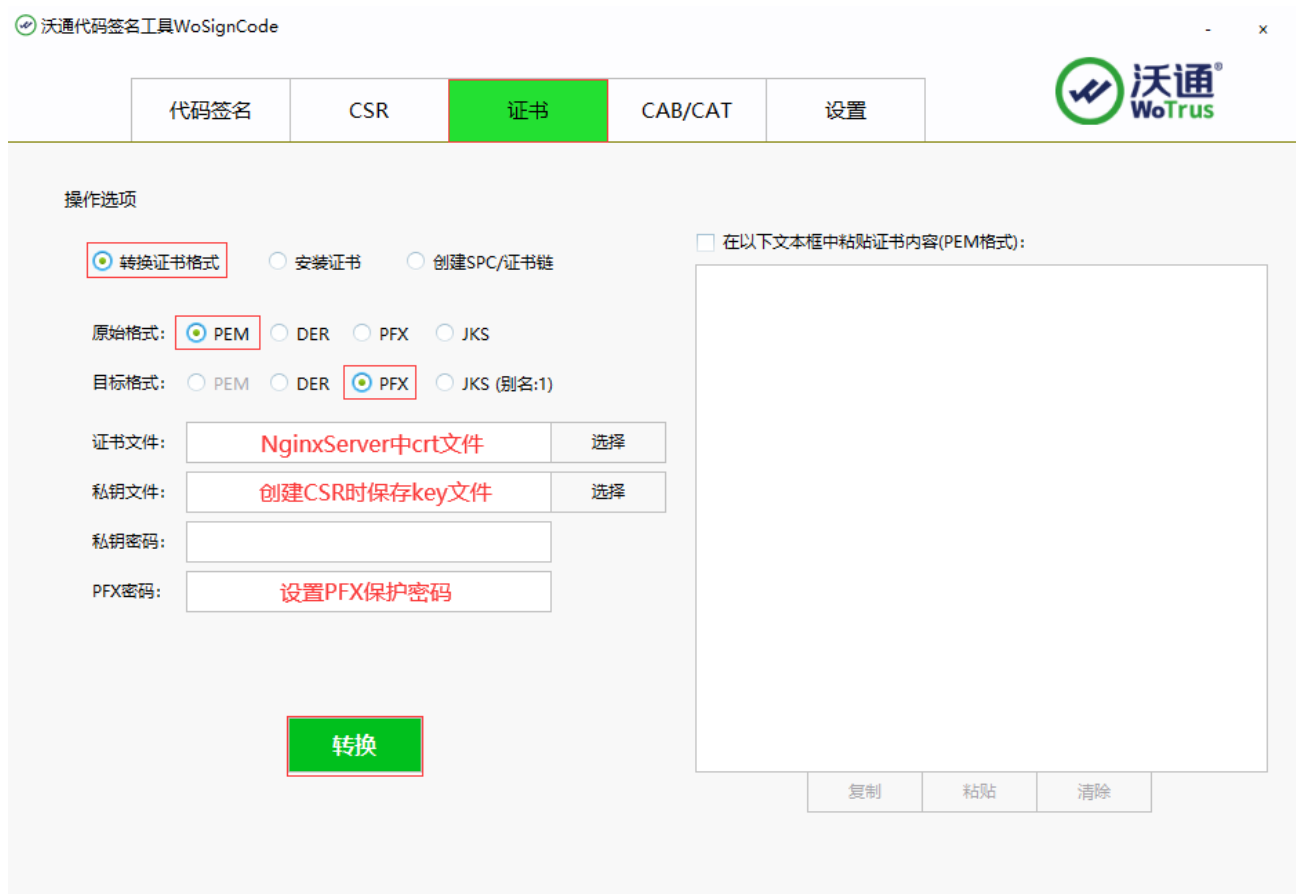
1.2、合成 SSL 证书

由于 Exchange 服务器要求导入 PFX 格式的证书，所以要将上面说的两个文件合成.pfx 格式的文件，具体步骤如下：

合成工具下载：

<https://download.wotrus.com/wotrus/wosigncode.exe>

下载并运行 wosigncode.exe 工具，点击证书，选择转换证书格式，原始格式 pem，目标格式 pfx，证书文件选择 NginxServer 中的.crt 文件，私钥选择创建 CSR 过程保存的私钥.key 文件，设置 pfx 密码，点击转换，输入名称，保存下来即可，详情可见下图：



注意:私钥密码一般为空，若创建 CSR 时设置了私钥密码，则此处私钥密码和 PFX 密码请与之前设置的私钥密码保持一致。

二、安装 SSL 证书

2.1、导入 SSL 证书

1.登录到 Exchange 所在的服务器(多台请重复执行后面步骤)，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；

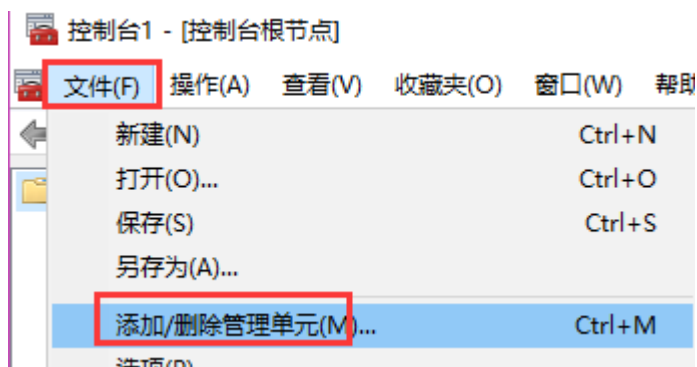


图 3

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；

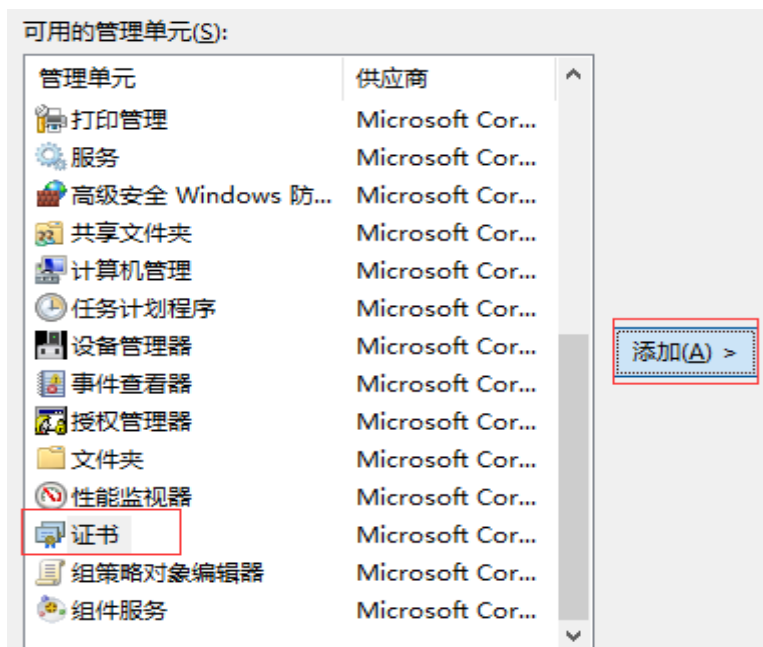


图 4

证书管理单元

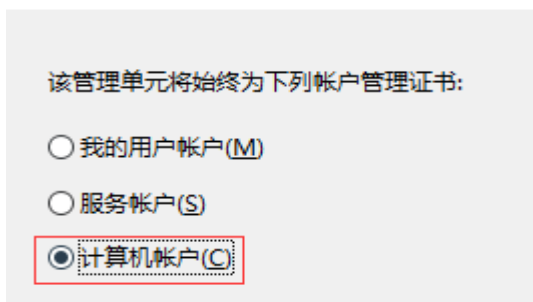


图 5

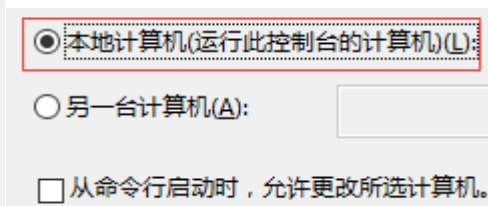


图 6

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；

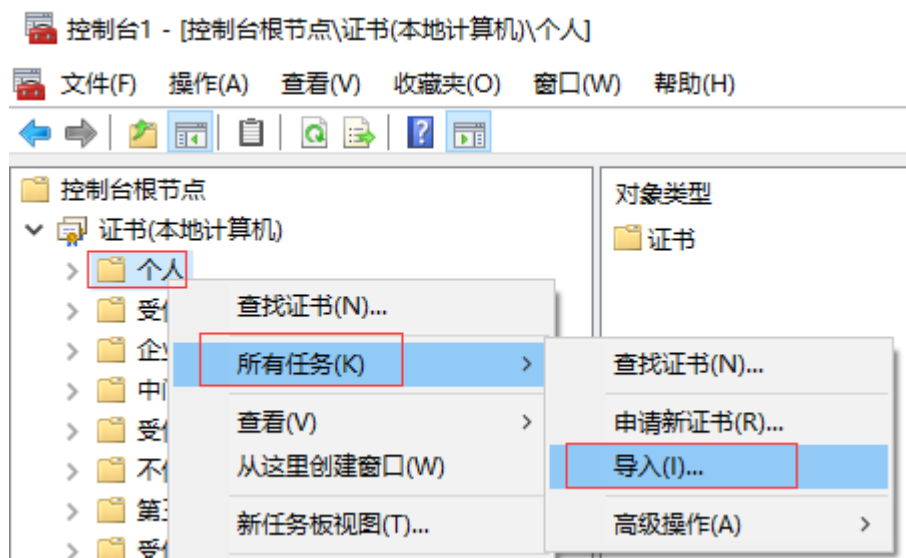


图 7

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；

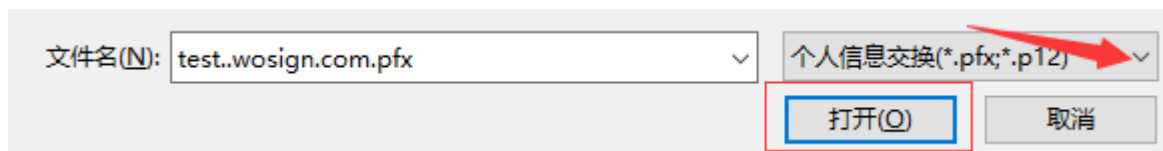


图 8

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；

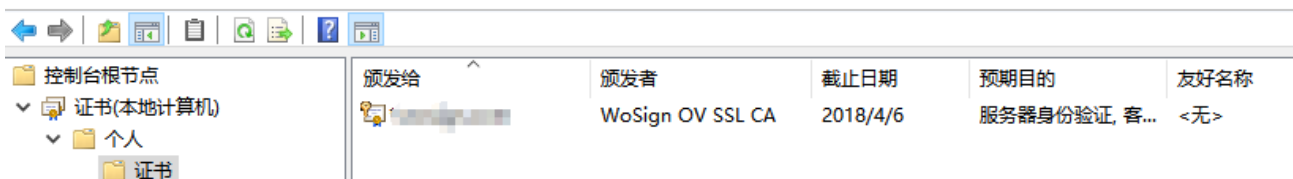
Windows 可以自动选择证书存储，你也可以为证书指定一个位置。

根据证书类型，自动选择证书存储(U)

将所有的证书都放入下列存储(P)

图 9

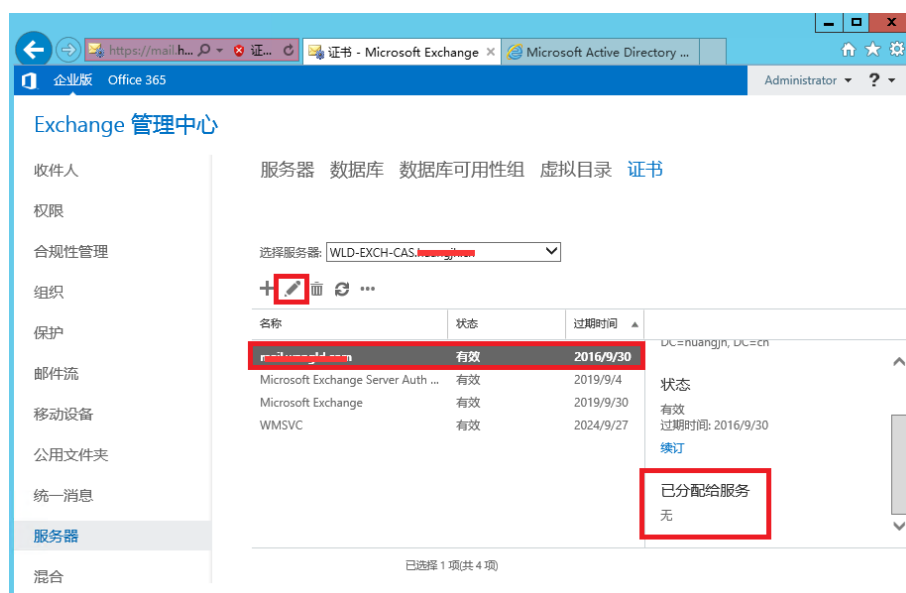
证书导入完成后，在“个人”-“证书”目录下，可见到该域名证书



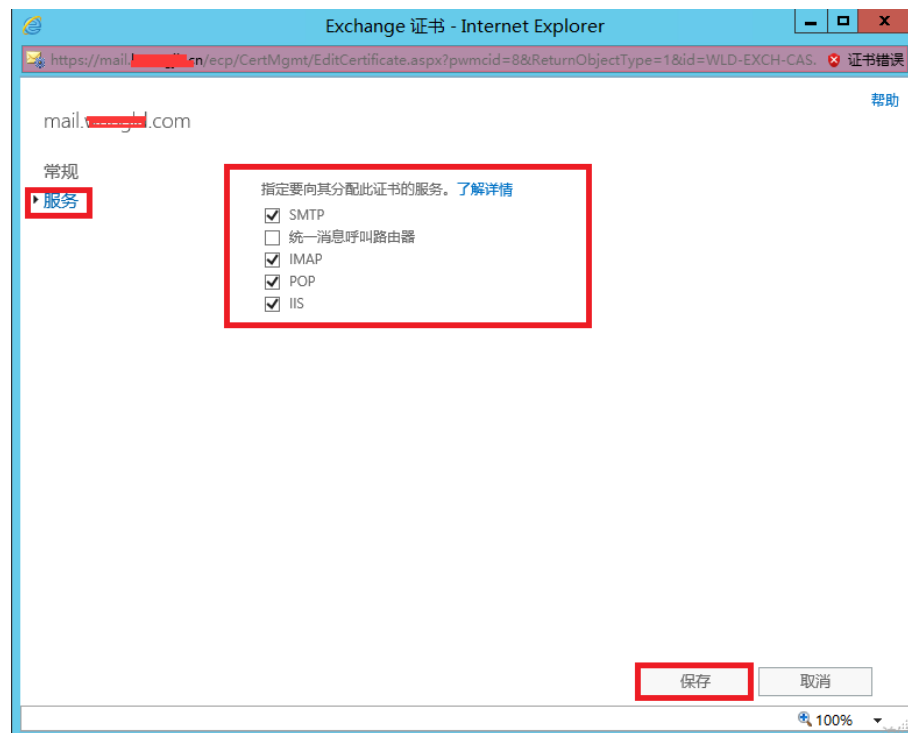
按照上述设置后，接下来就可以去 Exchange 2013 服务器上分配证书啦！

2.2、分配 SSL 证书

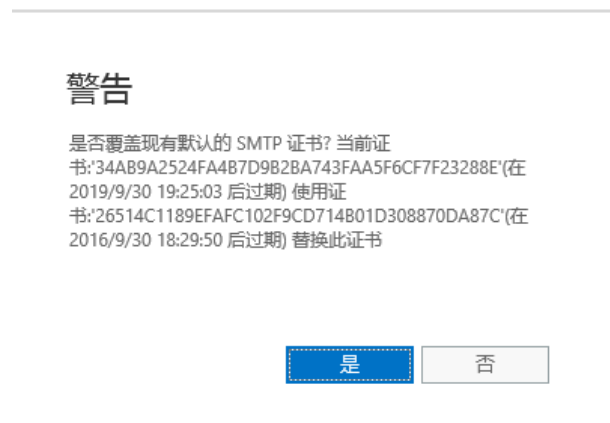
打开 Exchange 2013 管理控制台，在“服务器”-“证书”中，选择正确服务器，找到导入的证书，选择该证书，点击“编辑”。



点击“服务”，分配服务，默认勾选 IIS、SMTP、POP3、IMAP 共四个服务，点击“保存”。



弹出覆盖提示，确认无误后点击“是”：



至此，证书配置完成了。

三、测试 SSL 访问

打开浏览器，输入 `https://yourdomain.com`（证书绑定的实际域名），如浏览器地址栏显示加密小锁，则表示证书配置成功。若显示无法连接，请确保防火墙或安全组等策略有放行 443 端口（SSL 配置端口）。

四、备份 SSL 证书

请将下载的.zip 压缩包和自主生成的私钥.key 文件备份，以防丢失，影响后续使用！