

## IIS 服务器证书部署

### 环境说明

- 建议使用 IIS8（支持 SNI），一个站点一个端口允许同时部署多张证书
- Win7, server 2008 r2, win8, win2012 系统上关于加密套件的补丁  
<https://technet.microsoft.com/zh-CN/library/security/3042058.aspx?f=255&MSPPErr=-2147217396>
- 对于 IIS6, IIS7, IIS8, 操作具体通用性

### 获取证书

这里需要 pfx/p12（pkcs12）格式的证书。

MPKI 方式：

1. 登录 <https://mpki.trustasia.com>
2. 证书下载 pkcs12 格式（得到一个 pfx 后缀的证书文件）。此 pfx 文件密码就是证书密码

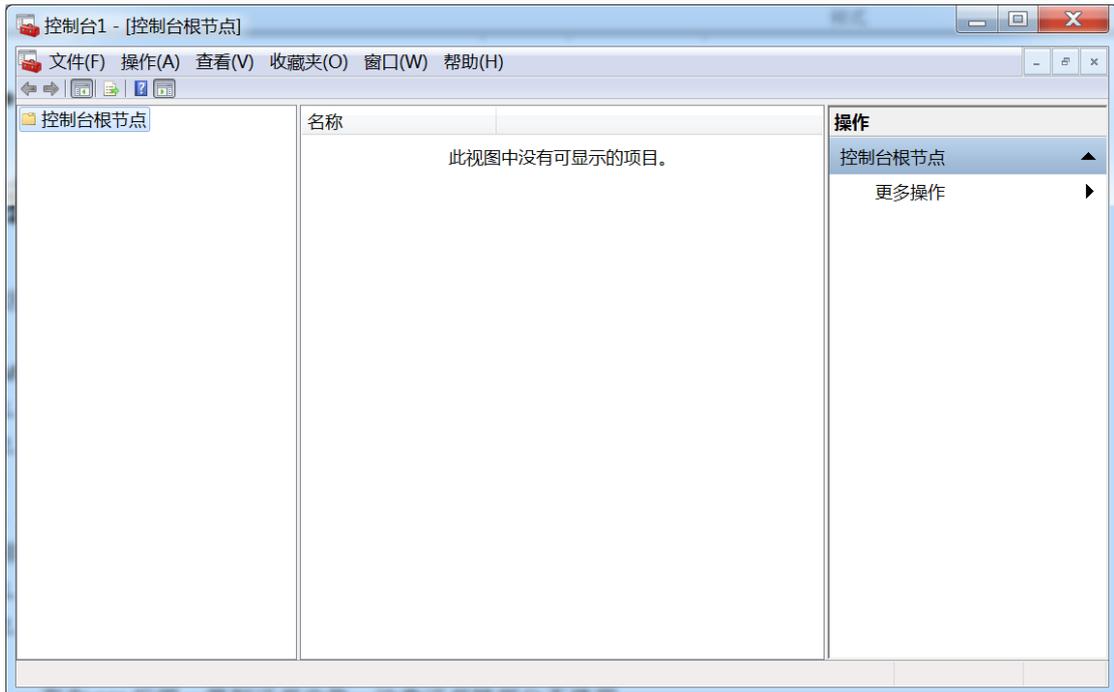
非 MPKI

1. CSR 对应的 key 文件
2. 证书邮件里提取代码，里面可能有多段代码，把第一段-----BEGIN CERTIFICATE-----到-----END CERTIFICATE-----（包括开头和结尾，不用换行）复制到 txt 文本文件里，然后保存为 cer 后缀，得到证书文件。注意证书链部分不使用。
3. 使用工具 [https://myssl.com/cert\\_convert.html](https://myssl.com/cert_convert.html)，进行格式转换，选择 pem 转 pkcs12。

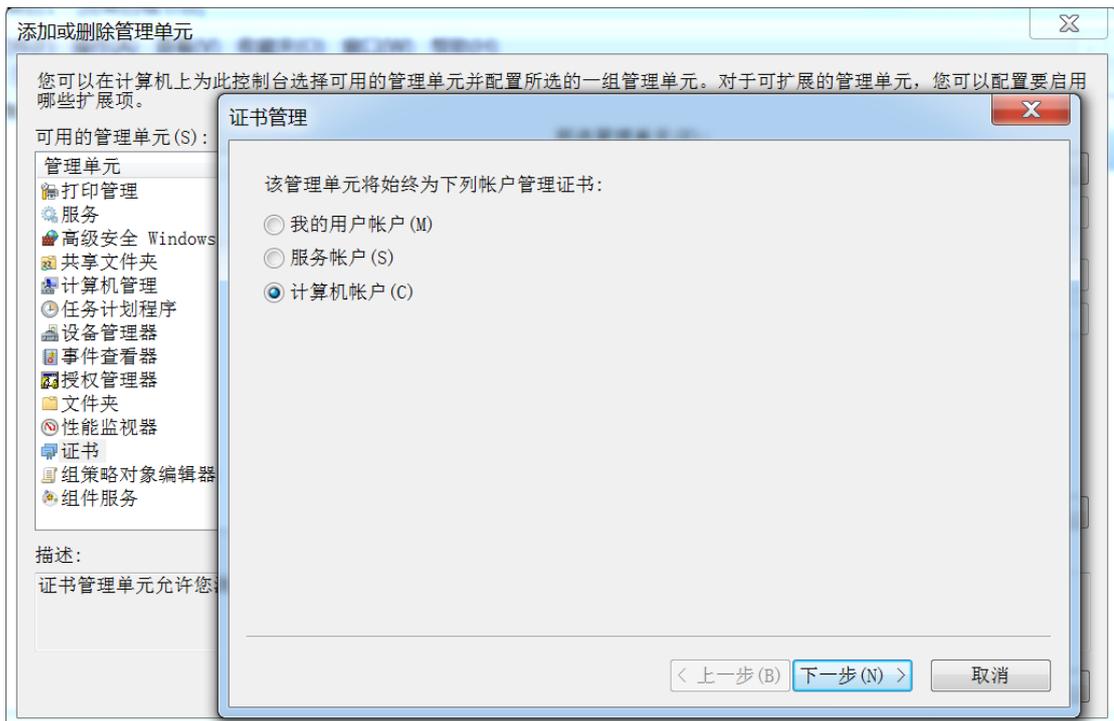
### 导入证书

IIS 使用的是系统证书库中的证书。所以证书是要导入系统的。导入到 mmc 中

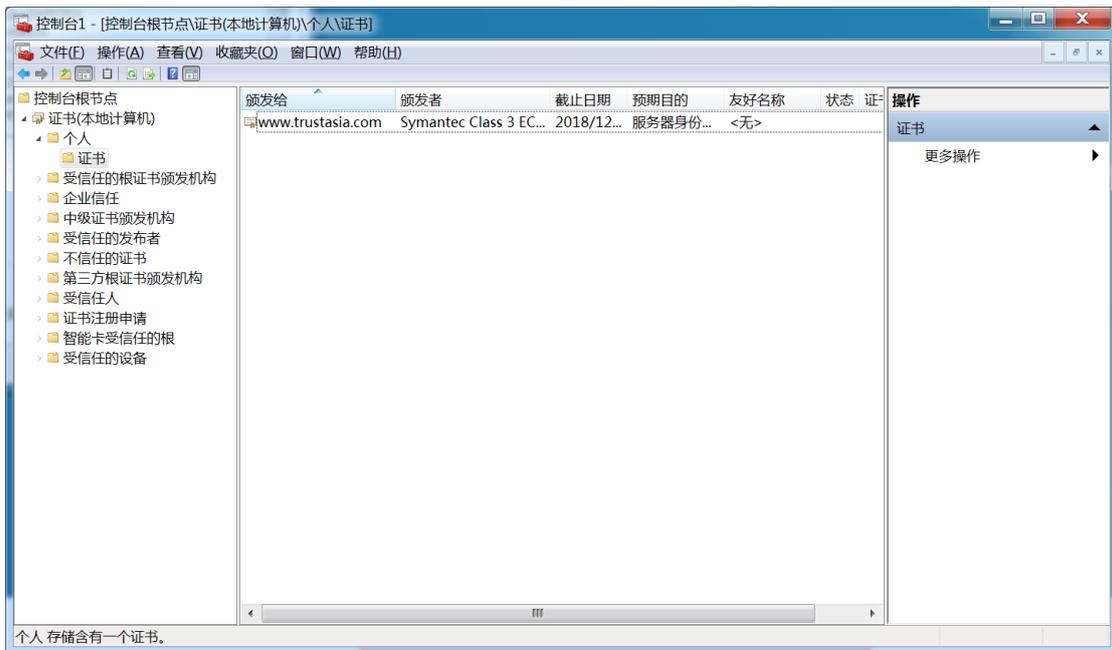
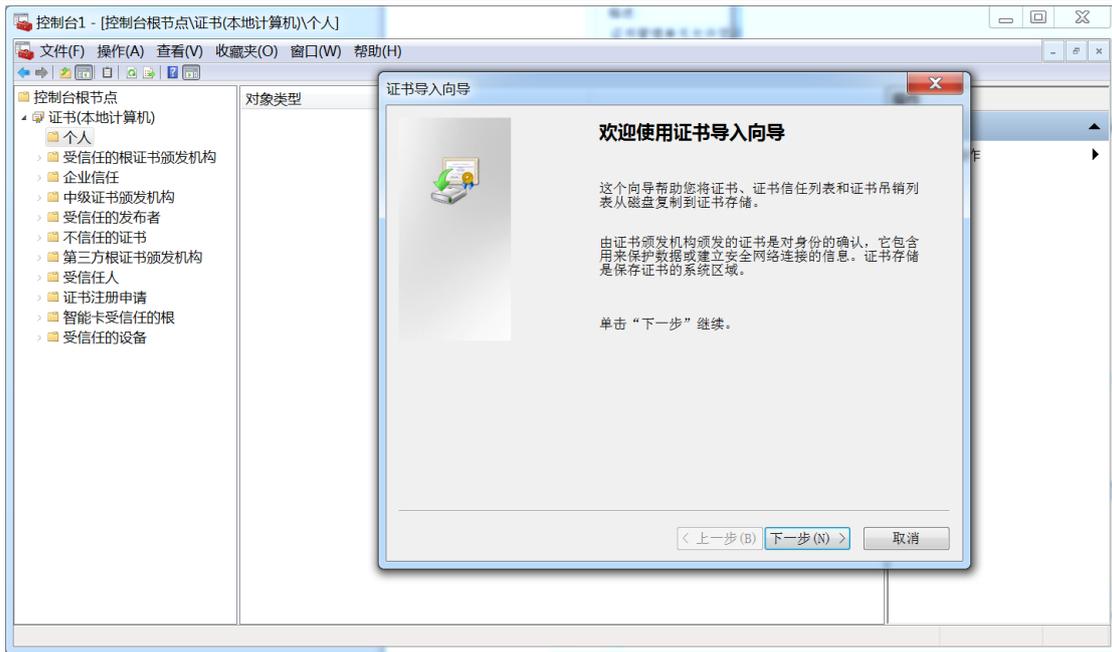
1. 运行 mmc



2. 使用计算机账户添加证书单元。主要是计算机账户，其他保持默认设置即可。



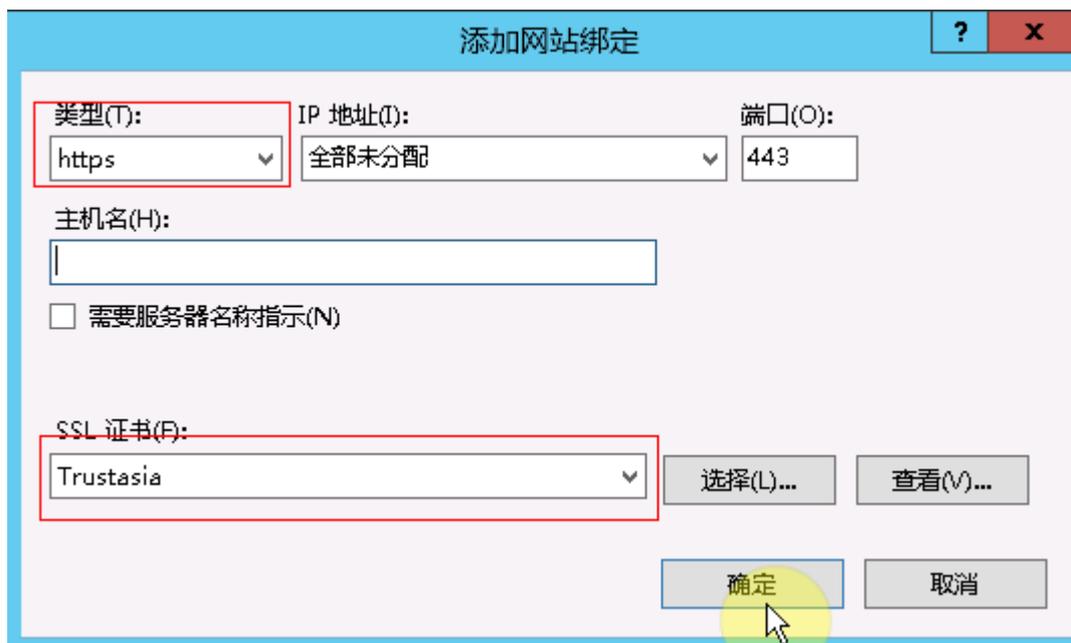
3. 在“个人”下面的证书中导入 pfx 文件。
4. 所有任务—>导入证书



5. 调整证书链。将中级证书剪切到 “中级证书颁发机构” 下的 “证书” 中。

## SSL 配置

到 IIS 中绑定导入的证书



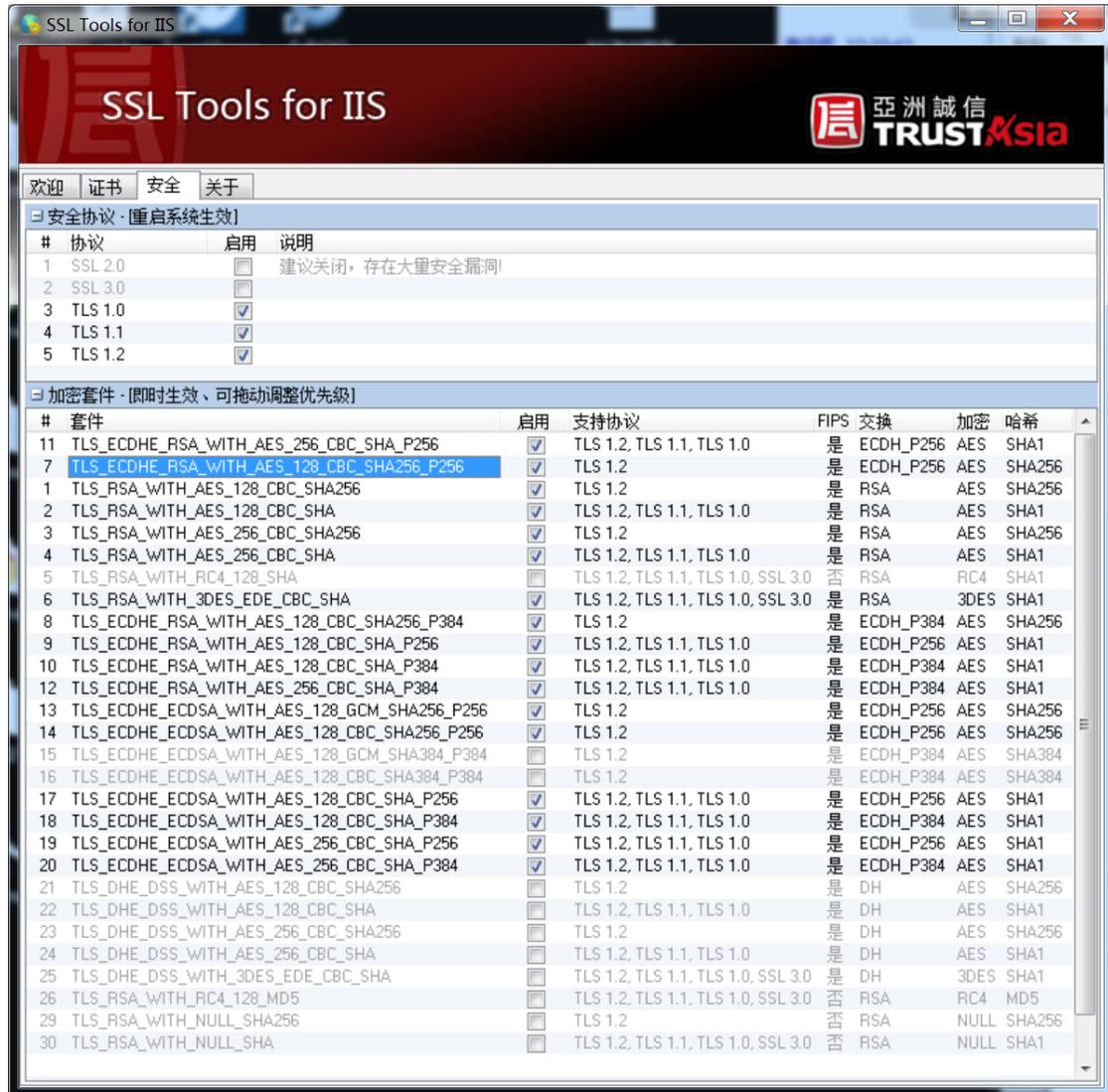
## 优化 SSL

运行工具: <http://www.trustasia.com/download/ssltools.zip>

协议部分: 只勾选 TLS1.0 TLS1.1 TLS1.2

套件部分: 去掉带 DHE,RC4,NULL,MD5 (ECDHE 的保留)

然后重启系统。



## http 跳转 https（建议非强制）

安装 rewrite 模块，下载模块

<https://www.iis.net/downloads/microsoft/url-rewrite>


 编辑入站规则

名称 (N):

强制HTTPS

**匹配 URL**

请求的 URL (R):  使用 (S):

模式 (M):  [测试模式 \(T\)...](#)

忽略大小写 (I)

**条件**

逻辑分组 (G):

输入	类型	模式
{HTTPS}	与模式匹配	^OFF\$

跨条件跟踪捕获组 (K)

操作: [添加...](#) [编辑...](#) [删除](#) [上移](#) [下移](#)

**操作**

操作类型 (Y):

操作属性

重定向 URL:

附加查询字符串 (Q)

重定向类型:

# 检测

https 的端口没做限制后（防火墙放行，端口转发正常），到 <https://myssl.com> 进行检测

The screenshot shows the MySSL.com interface for a security assessment of myssl.com. The header includes the MySSL.com logo, the domain name in the search bar, and a 'DNS诊断工具 new!' button. The main content area displays the domain 'myssl.com' with a lock icon, IP address '54.223.178.8:443 (北京)', server 'openresty', title 'SSL/TLS安全评估报告', and detection time '2017-09-26 10:51:04 (耗时: 16秒)'. Below this is a '概述' (Overview) section with a sub-header and a description: '检测部署SSL/TLS的服务是否符合行业最佳实践, PCI DSS支付卡行业安全标准, Apple ATS规范。'. A grade scale from A+ to T is shown, with a green pin indicating the current grade is A+. Below the scale, 'PCI DSS' and 'ATS' are both marked as '合规' (Compliant). At the bottom, there is a '证书信息' (Certificate Information) section.

评级达到 B 以上，在安全和兼容方面是较不错的。