# SSL证书申请及绑定操作

SSL证书可实现网站HTTPS化，加密用户与网站间的交互访问，强化网站用户侧可信展示程度，防劫持、防篡改、防监听。

本文档简要概述如何为服务器上的站点申请SSL证书，以及如何在IIS8下将证书绑定网站，启用https。

1. 申请ssl证书

Ssl证书主要分为DV、OV和EV，安全级别依次递增。

**DV SSL**:免费数字证书,最多保护一个明细子域名,不支持通配符，一个阿云帐户最多签发20张免费证书;

**专业版OV SSL**:OV SSL,提供加密功能,对申请者做严格的身份审核验证,提供可信身份证明；

**增强型OV SSL**：增强型OV SSL(支持ECC椭圆曲线算法),提供站点加密功能，需要核验组织注册信息，证书中显示组织名称。组织信息验证通过后，3工作日内颁发

**高级版EV SSL**：EV SSL,提供加密功能,对申请者做最严格的身份审核验证,提供最高度可信身份证明,提供浏览器绿色地址栏

**增强型EV SSL**：增强型EV SSL(支持ECC椭圆曲线算法),提供站点加密功能，浏览器绿色地址栏显示组织信息强化信任。组织信息验证通过后，7工作日内颁发

概要说明如下：（具体详细信息可转至阿里云控制平台查看：https://common-buy.aliyun.com/?commodityCode=cas#/buy）



备注：保护一个明细域名,例如: buy.example.com,或next.buy.example.com, 各个明细子域名都算一个域名



备注：保护多个明细域名,例如: buy1.example.com, buy2.example.com, next.buy.example2.com, 上述三个明细子域名计算为三个域名



备注：保护一个带通配符域名（该\*号同级别的全部明细域名）。申请证书时，如申请\*.example.com,那么该证书支持a.example.com, a1.example.com, a2.example.com...以此类推，但是不支持b.a.example.com（另一级）, b1.a.example.com...以此类推。如需支持，需另外再申请一张\*.a.example.com证书。此外，当前阿云线上售卖不支持多域名通配证书，即一张证书包含多个通配符证书，如申请一张包含\*.example.com, \*.a.example.com, \*.a1.example.com, \*.example1.com这样包含4个通配符的证书时，需通过提交工单签发该多域名通配符证书

**下面介绍的是申请免费的DV SSL证书（只验证网站域名所有权的简易型（Class 1级）**SSL证书，能起到加密传输的作用，但无法向用户证明网站的真实身份。）

1. 登录阿里云控制台(https://www.aliyun.com/),进入控制台，找到左侧菜单栏中的“安全(云盾)->证书服务->购买证书”
2. 选择免费DV SSL



1. 确认订单去支付>确认支付



1. 支付完成>证书控制台



1. 补全订单的证书信息



输入要绑定的网站的域名：注意,SSL证书服务商将会对您的域名（example.com）的管理员邮箱进行验证。(一封附有验证码邮件)



1. 填写真实的个人信息>下一步



1. 提交审核

此处如果是OV级别的证书，则会要求上传公司的营业执照等公司相关资质信息



1. 回到证书服务》我的订单下，可以看到刚刚申请的证书订单，点击右侧的进度，按照提示进行操作。

此处如果是OV级别的证书，不需要做此步骤操作，CA机构将会根据上传的资料中的电话核实公司信息，同时，邮箱收到一份需要回传企业资料的邮件。



按照提示，在域名解析平台中添加对应的DNS记录（解析记录）即可。

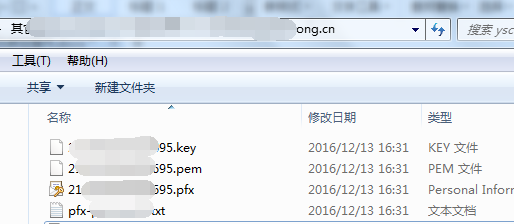
1. 稍微等待一段时间，证书即会签发，如下图：



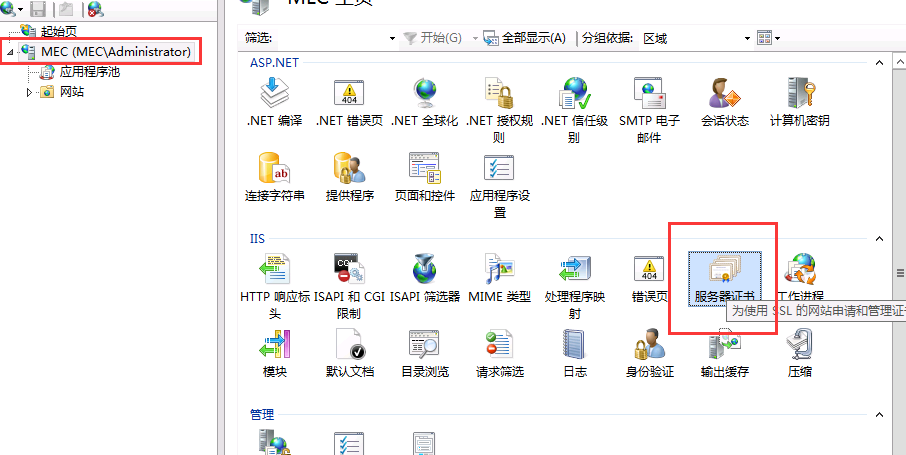
1. 点击下载,选择对应的宿主即可，此文档中我们演示的为iis8.



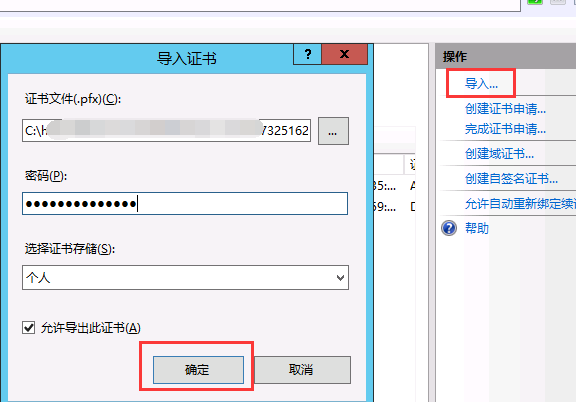
1. 将下载的证书文件压缩包解压拷贝到服务器某个目录下。



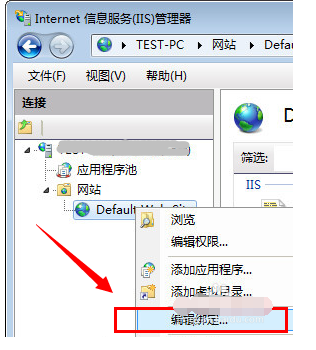
1. 绑定ssl证书，启用Https访问
2. 打开IIS（internet信息服务器），（一般在开始菜单旁边，服务器管理器，服务器角色），打开之后， 点击“服务器名”---右侧选择“服务器证书”



1. 选择右侧操作>导入。选择刚刚放置的证书目录文件，密码也在此证书目录下一个名称为pfx-password.txt文件中。



1. 打开你需要启用SSL证书的网站，右键选择“编辑绑定‘设置网站主机头，如下图



1. 在网站编辑绑定对话框，找到点击添加如下图（**选择https类型）**，选择刚刚导入的证书，填写主机头。这样就ok了



1. 一些补充

IIS7下面默认HTTPS绑定是无法指定主机头的，但我们可以通过手工修改IIS配置来实现主机头绑定。

打开C:\Windows\system32\inetsrv\config\applicationHost.config

定位到如下位置：

<bindings>

<binding protocol="https" bindingInformation="\*:443" />

<binding protocol="http" bindingInformation="\*:80:abc.demo.com" />

</bindings>

找到https的配置项目，修改为：

<binding protocol="https" bindingInformation="\*:443:abc.demo.com" />

注意这里的abc.demo.com要换成你自己的域名，之后保存即可。

阿里下载的证书签名算法是sha256 那密码套件要把这一串排到最前

还有系统环境是windows server 2008 iis7.5 默认不开启 tlsv1.2 要修改注册表 ，然后修改ssl密码套件顺序。修改参考资料：

http://jackstromberg.com/2013/09/enabling-tls-1-2-on-iis-7-5-for-256-bit-cipher-strength/?spm=5176.7748151.2.5.4A62ky。