

腾讯云SSL 证书

操作指南

产品文档



腾讯云

【版权声明】

©2013-2017 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

文档声明.....	2
操作指南.....	4
域名型证书申请流程.....	4
域名验证指引.....	8
自动诊断结果查看指引.....	15
域名身份如何自动验证.....	16
部署证书到负载均衡指引.....	17
私钥密码指引.....	20
证书安装指引.....	21
域名型证书吊销指引.....	34
苹果ATS特性服务器配置指南.....	36
安全签章指引.....	44

操作指南

域名型证书申请流程

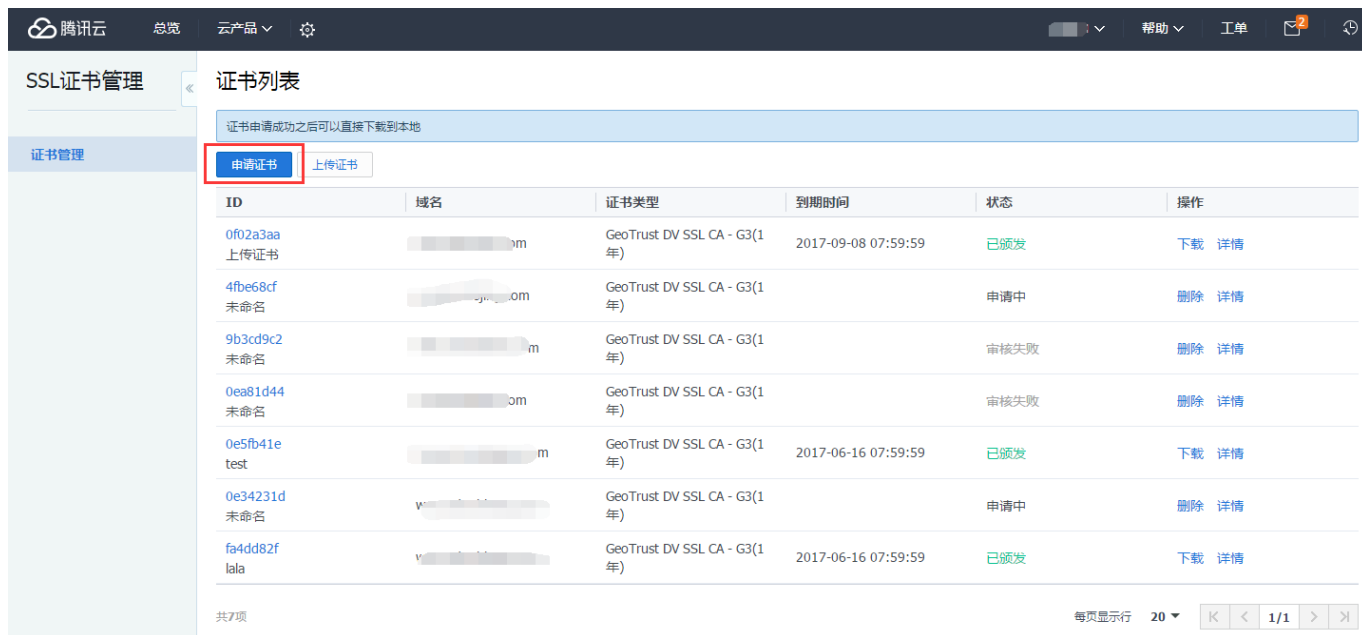
申请域名型（DV）SSL证书

1. 申请入口

进入SSL证书管理控制台



点击【申请证书】



查看申请域名型证书型号，点击【确定】



2. 填写申请

填写申请域名，例如qcloud.com，www.qcloud.com，demo.test.qcloud.com。



3.1 手动DNS验证方式

证书默认支持收到DNS验证，验证方法可查看[详情](#)。



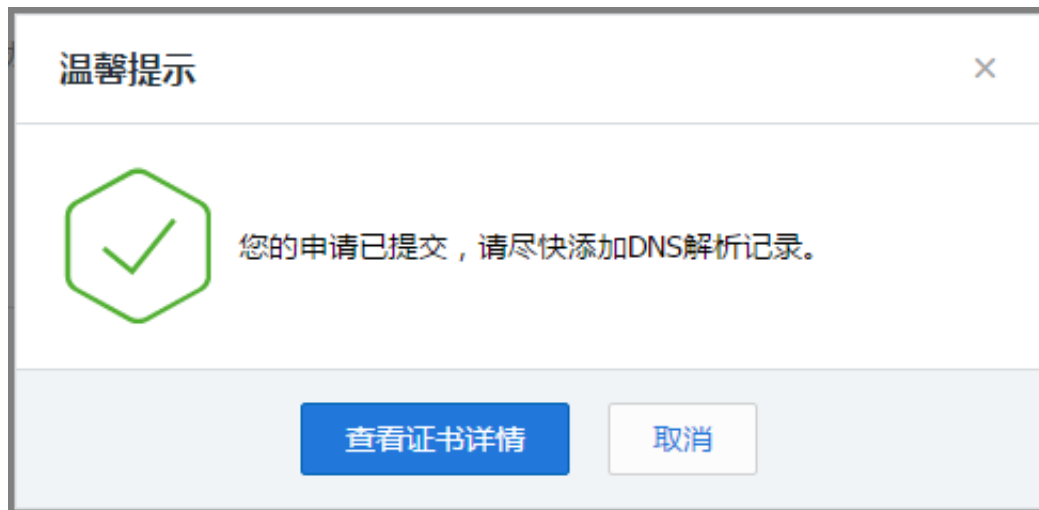
3.2 选择自动DNS验证方式

如果所申请域名成功添加[云解析平台](#)，可以支持自动DNS验证，验证方法可查看[详情](#)。



4.1 提交申请后验证身份

提交申请成功后弹窗提示如下，需要前往【证书详情页】获取CName记录添加解析：

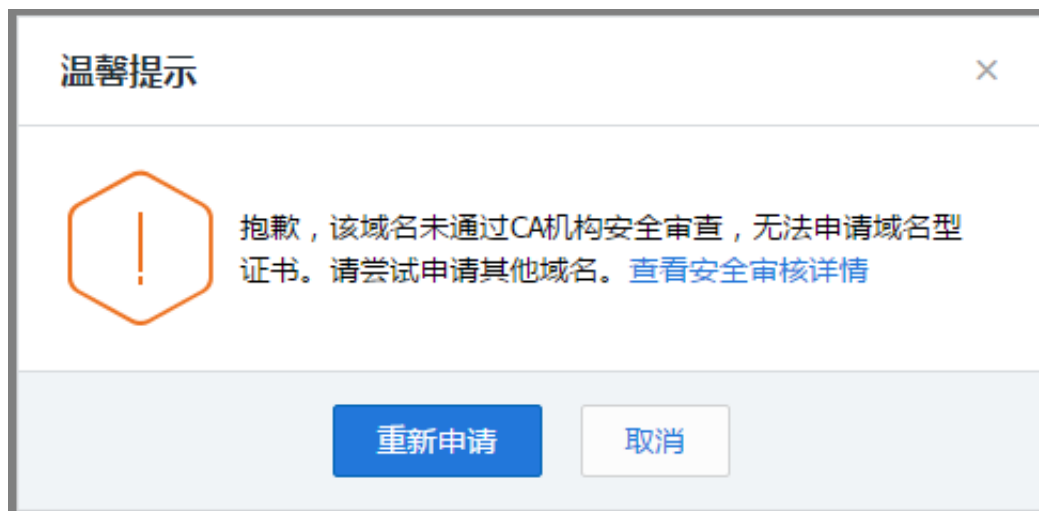


获取CName记录如Tips中显示，需要尽快成功添加解析，方可通过CA机构审核：



4.2 提交申请失败

如遇到下图所示弹窗，是提交域名未通过CA机构安全审核，具体原因参考[安全审核失败原因](#)。



域名验证指引

申请域名型证书，可以通过以下方式验证域名的所有权：

1. 手动DNS验证

通过解析指定的DNS记录验证您的域名所有权，指定如

主机记录 -> TXT记录类型 -> 记录值

的解析格式。

例如为申请证书的域名 `www.domain.com` 添加一条记录类型为TXT的DNS记录，

`www.domain.com -> TXT -> 201704262209564gw0...hj37i4xai8m7uii2a23l`

:

SSL证书管理

证书管理

[返回列表](#) | 证书详情

您的申请信息已提交。请尽快添加DNS解析记录，扫描认证通过后即可颁布证书。

ID

AdVNf4pM

状态

待DNS验证

请添加如下解析记录 [操作指引](#)

域名	主机记录	记录类型	记录值
domain.com	@	TXT	201704262209564gw0...hj37i4xai8m7uii2a23l

[自助诊断](#) [查询](#)

证书类型

TrustAsia DV SSL CA - G5(1年)

通用名称

www.domain.com

提交时间

2017-04-27 22:09:56

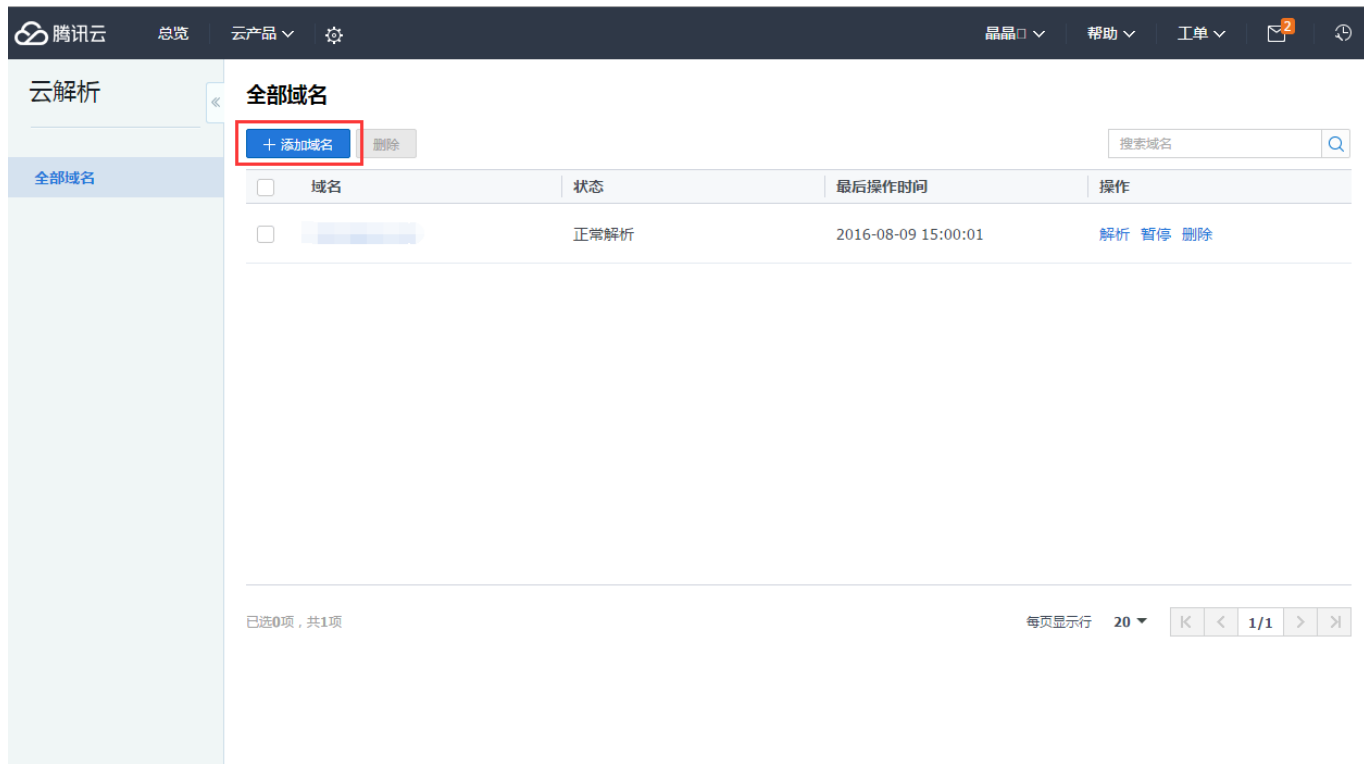
以腾讯云云解析平台为例说明如何进行操作：

1.1 添加域名

点击【添加域名】，输入您要解析域名的主域名

domain.com

, 并点【确定】



腾讯云控制台云解析全部域名页面。左侧导航栏显示“云解析”和“全部域名”。顶部操作栏包含“+ 添加域名”（红色框标注）、“删除”按钮和搜索框。表格列出了域名、状态、最后操作时间和操作按钮。当前显示1项记录。

域名	状态	最后操作时间	操作
domain.com	正常解析	2016-08-09 15:00:01	解析 暂停 删除

1.2 添加解析记录

点击刚添加的域名【解析】



腾讯云控制台云解析一级域名页面。左侧导航栏显示“云解析”和“一级域名”。顶部操作栏包含“+ 添加域名”、“删除”、“更多操作”按钮和搜索框。表格列出了域名、状态、解析套餐、最后操作时间和操作按钮。当前显示1项记录。

域名	状态	解析套餐	最后操作时间	操作
zdeubles.com	正常解析	免费套餐	2017-04-18 22:24:18	解析 暂停 升级套餐 更多

点击【添加记录】



1.3 完成指定的TXT记录添加

TXT记录是对域名进行标识和说明的一种方式：

- 记录类型选择为TXT
- 主机记录根据证书详情填入，如：

_dnsauth

- 线路类型选择默认
- 记录值为系统提供的文本内容，此处为

201712270743...t5bfctnq

，注意记录值须完整填写

- TTL选择默认值10分钟即可

[< 返回列表](#) | 证书详情

您的申请信息已提交。请尽快添加DNS解析记录，扫描认证通过后即可颁布证书。

基本信息

ID

备注名 测试

状态 待DNS验证

请添加如下解析记录 [操作指引](#)

域名	主机记录	记录类型	记录值
	_dnsauth	TXT	201712270743392cd8mtrqk950jy1wdq2hap9dji6t5bftcnq

[+ 添加记录](#) [新手快速添加](#) [暂停](#) [开启](#) [删除](#) [分配至项目](#)

☐ 主机记录	记录类型	记录类型	记录值	MX优先级	TTL (秒)	最后操作时间	操作
_dnsauth	TXT	默认	jy1wdq2hap9dji6t5bftcnq	-	600	-	保存 取消

提示
一般用于 Google、QQ等企业邮箱的反垃圾邮件设置；填写文本，字符长度限制255

解析添加成功后如下：

[+ 添加记录](#) [新手快速添加](#) [暂停](#) [开启](#) [删除](#) [分配至项目](#)

☐ 主机记录	记录类型	记录类型	记录值	MX优先级	TTL (秒)	最后操作时间	操作
☐							修改 删除
☐							修改 删除
☐ _dnsauth	TXT	默认	201712270743392cd8	-	600	2017-12-28 16:00:34	修改 暂停 删除

www.domain.com

TXT记录值的系统会定时检查，若能检测到并且与指定的值匹配，即可完成域名所有权验证。

2. 自动DNS验证

注：仅限使用云解析的域名

如果申请证书的域名已经在云解析平台进行解析，可以选择自动验证。

系统会为该域名自动添加指定的DNS解析记录，记录被检测匹配成功，完成域名所有权验证后，该记录将自动清除。

3. 文件验证

3.1 指定目录下创建文件

按指定文件目录、文件名、文件内容新增文件，例如

文件目录	文件名	文件内容
/.well-known/pki-validation	fileauth.txt	201608241742072yvt8bxp9jv0yc ginrnnebwgy1nvwgvxtssucy39w7 b20nelfa

如果申请文件验证的域名是

example.www.domain.com

，那么进行验证访问的链接地址是

<http://example.www.domain.com/.well-known/pki-validation/fileauth.txt>

或者

<https://example.www.domain.com/.well-known/pki-validation/fileauth.txt>

对于www开头的二级域名，如：

www.domain.com

，在对该域名本身添加文件验证信息之外，还需增加对其主域名

domain.com

的文件验证，验证值与验证方法与该二级域名文件验证相同。

如果申请文件验证的域名是泛域名

`*.domain.com`

，那么进行验证访问的链接地址是

`http://domain.com/.well-known/pki-validation/fileauth.txt`

或者

`https://domain.com/.well-known/pki-validation/fileauth.txt`

访问链接可获取到内容为

`201608241742072yvt8bxp9jv0ycginrnnbwgy1nvwgvxtssucy39w7b20nelfa`

。

http和https访问支持任意一个均可；

文件验证不支持任何形式的跳转，需要直接响应200状态码和文件内容。

3.2 等待审核

建立完成文件后，请耐心等待CA机构扫描审核。证书颁发完成后，文件和目录即可清除。

3.3 Window系统不支持创建/.well-known目录问题

在Windows下无法通过

右键=>新建

命令来创建以点开头的文件和文件夹，例如

.log

，会提示必须输入文件名。

可以通过命令行来创建：

新建文件夹

`mkdir .well-known`

自动诊断结果查看指引

如果选择了手动DNS验证方式没有通过审核，可以通过自助诊断排查域名的解析问题：

1. 检查域名状态是否正常

请先确定域名可以正常解析。例如域名未实名认证时、域名刚刚购买入手时，都存在无法正常解析的情况。

2. 检查DNS服务器

请先确认在正确的解析服务商处添加了解析。例如DNS服务器为万网的服务器，则在腾讯云云解析添加了TXT解析是无法生效的。

3. 检查解析记录

如果域名解析正常、也在正确的解析服务商处添加了解析，仍然没有审核通过，很可能是手误输入了主机记录、记录值等，如果确认TXT记录已经完整无误添加了，请耐心等待24个小时。

如果超过24个小时仍未审核通过，可以工单联系腾讯云工程师协助您处理。

域名身份如何自动验证

1. 自动DNS验证原理

提交证书申请后，CA机构会指定添加一条CNAME解析记录来验证域名的所有权，如果该域名在腾讯云云解析平台进行解析，则可以立即自动添加指定的CNAME解析记录，等待CA机构的定时扫描审核，以最快最便捷的方式完成证书申请。

2. 云解析添加域名

如果您的域名不在云解析平台进行解析，可以参考如下流程将域名加入云解析：

[添加域名到云解析](#)

3. 修改DNS服务器

切记，完成添加域名后，需要修改域名的DNS服务器为腾讯云指定的DNS地址，解析方可生效。

参考 [修改域名DNS指引](#)

部署证书到负载均衡指引

SSL证书支持部署到负载均衡，步骤如下所示：

1. 选择证书

首先成功申请获取证书（参考[如何免费申请域名型证书](#)），或者选择上传的证书，展开【更多】操作，选择【部署到负载均衡】。

腾讯云 总览 云产品 CDN 设置 qcloud 帮助 工单 155

SSL证书管理 证书列表

证书申请成功之后可以直接下载到本地

申请证书 上传证书

ID	域名	证书类型	到期时间	状态	操作
ca861922 未命名	example.com	GeoTrust DV SSL CA - G3(1年)	2017-10-12 07:59:59	已颁发	下载 详情 更多 部署到负载均衡
c915db06 未命名	example.com	GeoTrust DV SSL CA - G3(1年)	2017-10-12 07:59:59	已颁发	下载 详情 更多
f9a1569b test	example.com	TrustAsia DV SSL CA - G5(1年)		审核失败	删除 详情
b57e1306 未命名	example.com	TrustAsia DV SSL CA - G5(1年)	2017-09-22 07:59:59	上传托管	下载 删除 详情 更多
dff103d lalalal	example.com	TrustAsia DV SSL CA - G5(1年)		审核失败	删除 详情
7bb4fc1b Highwinds-Ping	example.com	TrustAsia DV SSL CA - G5(1年)	2017-09-14 07:59:59	已颁发	下载 详情 更多
f0830dbf 拖哥的证书	example.com	clue test(10年)	2026-08-23 22:58:44	上传托管	下载 删除 详情 更多
f072fbcd clue的证书	example.com	clue test(10年)	2026-08-23 22:58:44	上传托管	下载 删除 详情 更多
e6654916	example.com	GeoTrust DV SSL CA - G3(1年)	2017-09-22 07:59:59	已颁发	下载 详情 更多

共16项 每页显示行 20 1/1

2. 选择LB实例

根据项目和地区筛选LB实例（目前不支持华南地区-深圳金融），且只能选择一个实例。

部署到负载均衡



证书ID: BB73JGnP(TestKMS)

证书类型: ca1

选中LB实例:

默认项目

华南地区 (广州)

可输入VIP或云主机内网IP搜索



ID		VIP	所属网络
lb-61s3opol	华南地区 (深圳金融...)	111.230.79.206	vpc-k8aux2cr
lb-myaluvfl	华东地区 (上海)	111.230.79.110	vpc-k8aux2cr
lb-hnxm3six	华东地区 (上海金融...)	111.230.78.221	vpc-l12bfw9t
lb-9wz8syx5	华北地区 (北京)	111.230.4.176	vpc-a2hcwbl5
lb-gc9grq4j		111.230.79.106	vpc-mnd20y33
lb-cbgrrgi3		111.230.75.187	vpc-mnd20y33

共 14 项

每页显示行 20

确定

取消

3. 创建监听器

跳转到负载均衡控制台，打开创建监听器弹窗，并且监听协议端口已切换到Https，服务器证书为已选中的证书，然后完成剩余的基本配置。



4. 继续完成配置

继续完成创建监听器的其他配置，即可实现负载均衡的Https。

私钥密码指引

私钥密码是申请证书时的选填项，如图所示：

The screenshot shows the 'SSL证书管理' (SSL Certificate Management) console. The left sidebar has '证书管理' (Certificate Management) selected. The main area is titled '证书列表 | 证书申请' (Certificate List | Certificate Application). A green step indicator '1 免费证书申请' (1 Free Certificate Application) is shown. The form includes fields for '绑定域名 *' (Bind Domain Name) with value 'www.domain.com', '证书备注名' (Certificate Remark Name) with value '一个DV证书', '私钥密码' (Private Key Password) with masked input, and '确认密码' (Confirm Password) with masked input. A red box highlights the password fields. A note states: '目前 暂不支持密码找回 功能，若您忘记密码则需重新申请证书' (Currently, the password recovery function is not supported. If you forget your password, you need to re-apply for the certificate). A '下一步' (Next Step) button is at the bottom.

注意事项：

- 1、如果填写了私钥密码，请您牢记该密码，该密码不支持找回和修改；
- 2、该密码在证书下载完成进行解压时需要输入；
- 3、在您的服务器上进行证书导入、导出、安装等操作时可能会需要输入；
- 4、如果私钥密码不慎遗忘，请[工单联系](#)腾讯云工程师删除该证书，然后重新申请该域名证书。

证书安装指引

下载得到的 `www.domain.com.zip` 文件，解压获得3个文件夹，分别是Apache、IIS、Nginx 服务器的证书文件，

下面提供了4类服务器证书安装方法的示例：

1. Apache 2.x 证书部署

1.1 获取证书

Apache文件夹内获得证书文件 `1_root_bundle.crt`，`2_www.domain.com_cert.crt` 和私钥文件

`3_www.domain.com.key`,

`1_root_bundle.crt` 文件包括一段证书代码 “-----BEGIN CERTIFICATE-----” 和 “-----END CERTIFICATE-----” ,

`2_www.domain.com_cert.crt` 文件包括一段证书代码 “-----BEGIN CERTIFICATE-----” 和 “-----END CERTIFICATE-----” ,

`3_www.domain.com.key` 文件包括一段私钥代码 “-----BEGIN RSA PRIVATE KEY-----” 和 “-----END RSA PRIVATE KEY-----” 。

1.2 证书安装

编辑Apache根目录下 `conf/httpd.conf` 文件，

找到

```
#LoadModule ssl_module modules/mod_ssl.so
```

和

```
#Include conf/extra/httpd-ssl.conf
```

，去掉前面的

```
#
```

号注释；

编辑Apache根目录下 conf/extra/httpd-ssl.conf 文件，修改如下内容：

```
<VirtualHost 0.0.0.0:443>
    DocumentRoot "/var/www/html"
    ServerName www.domain.com
    SSLEngine on
    SSLCertificateFile /usr/local/apache/conf/2_www.domain.com_cert.crt
    SSLCertificateKeyFile /usr/local/apache/conf/3_www.domain.com.key
    SSLCertificateChainFile /usr/local/apache/conf/1_root_bundle.crt
</VirtualHost>
```

配置完成后，重新启动 Apache 就可以使用

<https://www.domain.com>

来访问了。

注：

配置文件参数	说明
SSLEngine on	启用SSL功能
SSLCertificateFile	证书文件
SSLCertificateKeyFile	私钥文件
SSLCertificateChainFile	证书链文件

2. Nginx 证书部署

2.1 获取证书

Nginx文件夹内获得SSL证书文件 1_www.domain.com_bundle.crt 和私钥文件 2_www.domain.com.key, 1_www.domain.com_bundle.crt 文件包括两段证书代码 “-----BEGIN CERTIFICATE-----” 和 “-----END CERTIFICATE-----” , 2_www.domain.com.key 文件包括一段私钥代码 “-----BEGIN RSA PRIVATE KEY-----” 和 “-----END RSA PRIVATE KEY-----” 。

2.2 证书安装

将域名 `www.domain.com` 的证书文件 `1_www.domain.com_bundle.crt`

、私钥文件 `2_www.domain.com.key` 保存到同一个目录，例如 `/usr/local/nginx/conf` 目录下。

更新Nginx根目录下 `conf/nginx.conf` 文件如下：

```
server {  
    listen 443;  
    server_name www.domain.com; #填写绑定证书的域名  
    ssl on;  
    ssl_certificate 1_www.domain.com_bundle.crt;  
    ssl_certificate_key 2_www.domain.com.key;  
    ssl_session_timeout 5m;  
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2; #按照这个协议配置  
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE; #按照这个套件配置  
    ssl_prefer_server_ciphers on;  
    location / {  
        root html; #站点目录  
        index index.html index.htm;  
    }  
}
```

配置完成后，先用

```
bin/nginx -t
```

来测试下配置是否有误，正确无误的话，重启nginx。就可以使

`https://www.domain.com`

来访问了。

注：

配置文件参数	说明
listen 443	SSL访问端口号为443
ssl on	启用SSL功能
ssl_certificate	证书文件
ssl_certificate_key	私钥文件
ssl_protocols	使用的协议
ssl_ciphers	配置加密套件，写法遵循openssl标准

2.3 使用全站加密，http自动跳转https（可选）

对于用户不知道网站可以进行https访问的情况下，让服务器自动把http的请求重定向到https。

在服务器这边的话配置的话，可以在页面里加js脚本，也可以在后端程序里写重定向，当然也可以在web服务
器来实现跳转。Nginx是支持rewrite的（只要在编译的时候没有去掉pcre）

在http的server里增加

```
rewrite ^(.*) https://$host$1 permanent;
```

这样就可以实现80进来的请求，重定向为https了。

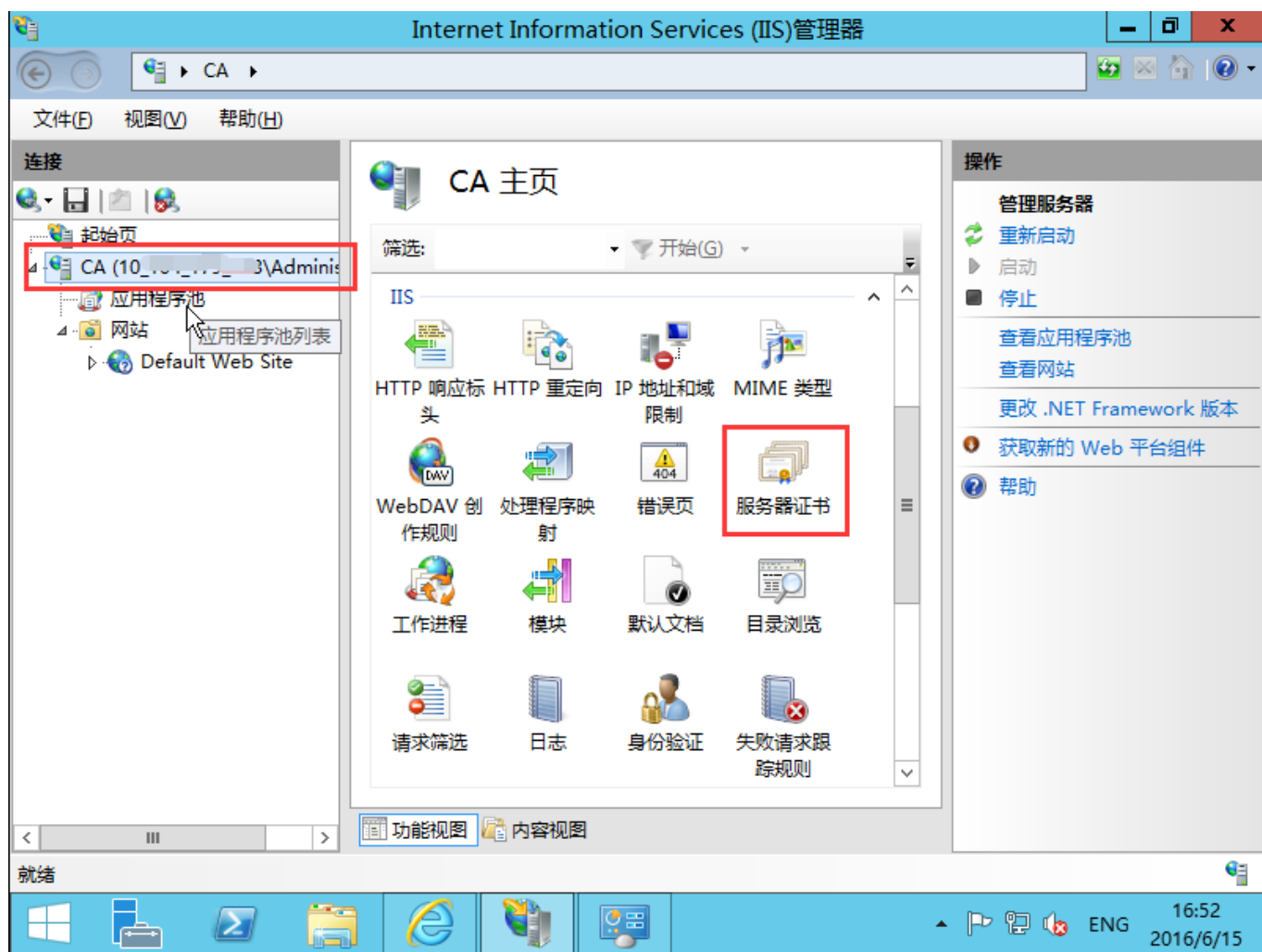
3. IIS 证书部署

3.1 获取证书

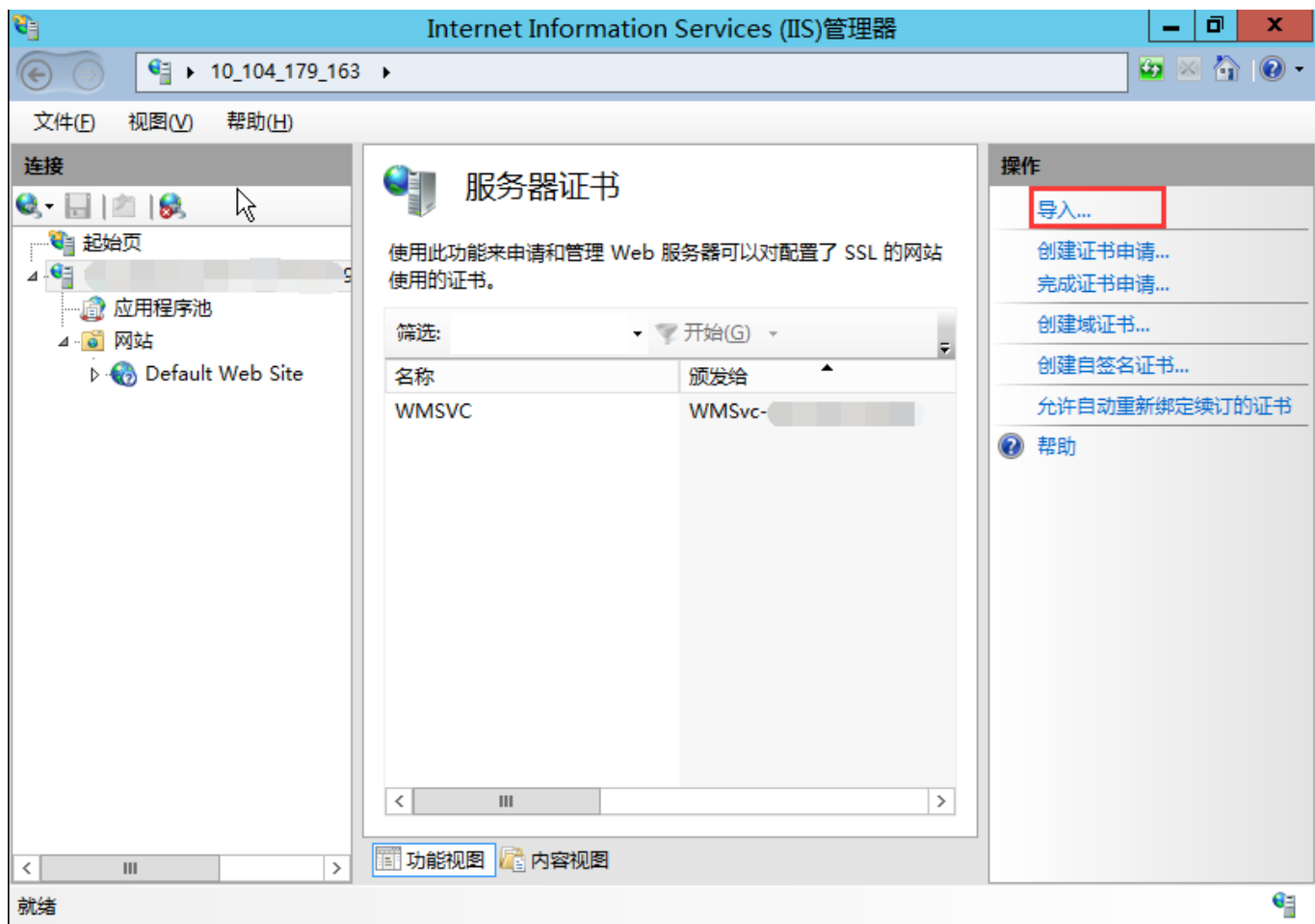
IIS文件夹内获得SSL证书文件 www.domain.com.pfx。

3.2 证书安装

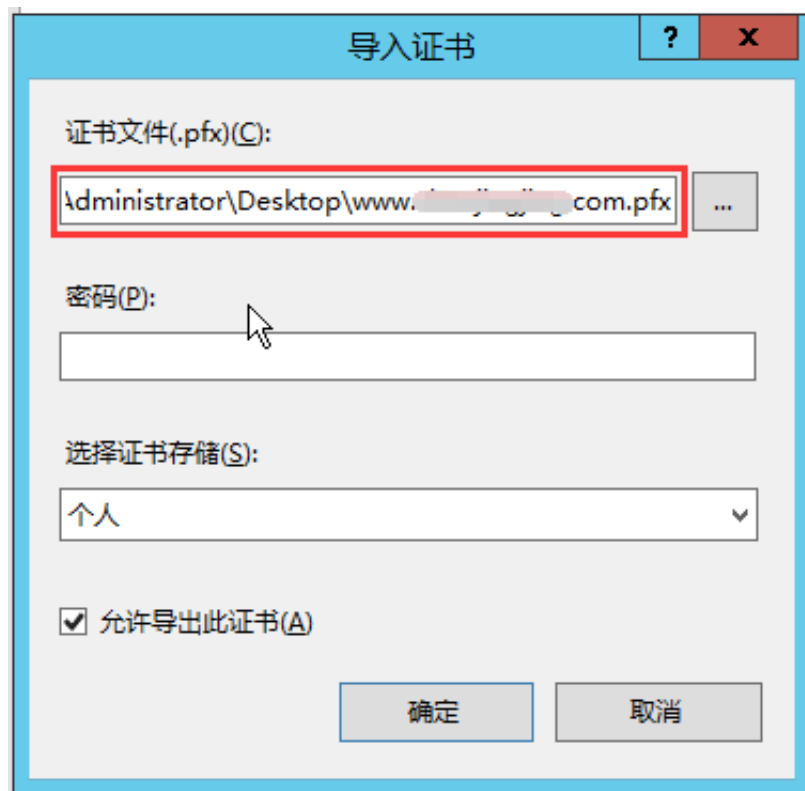
1、打开IIS服务管理器，点击计算机名称，双击‘服务器证书’



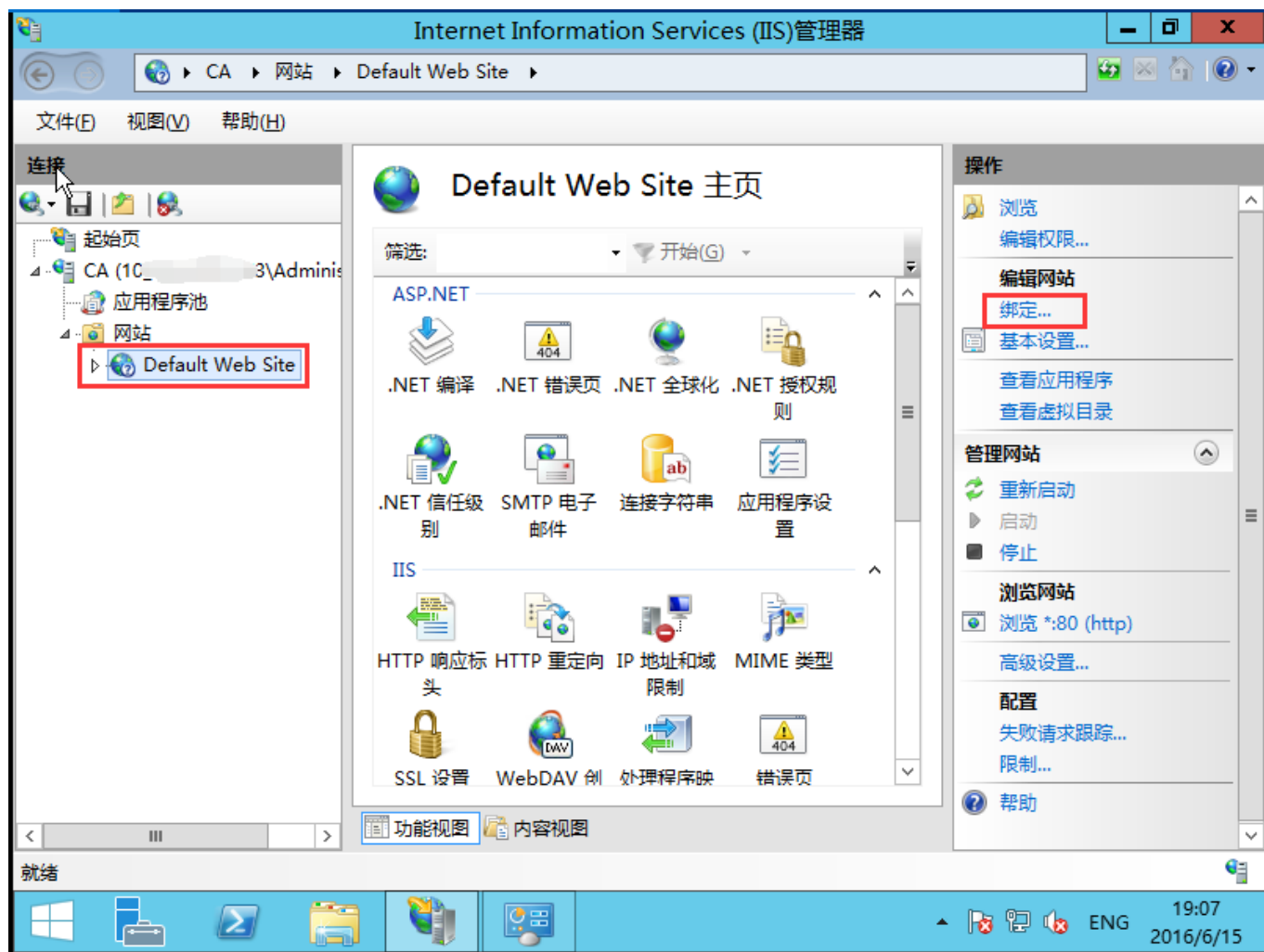
2、双击打开服务器证书后，点击右则的导入



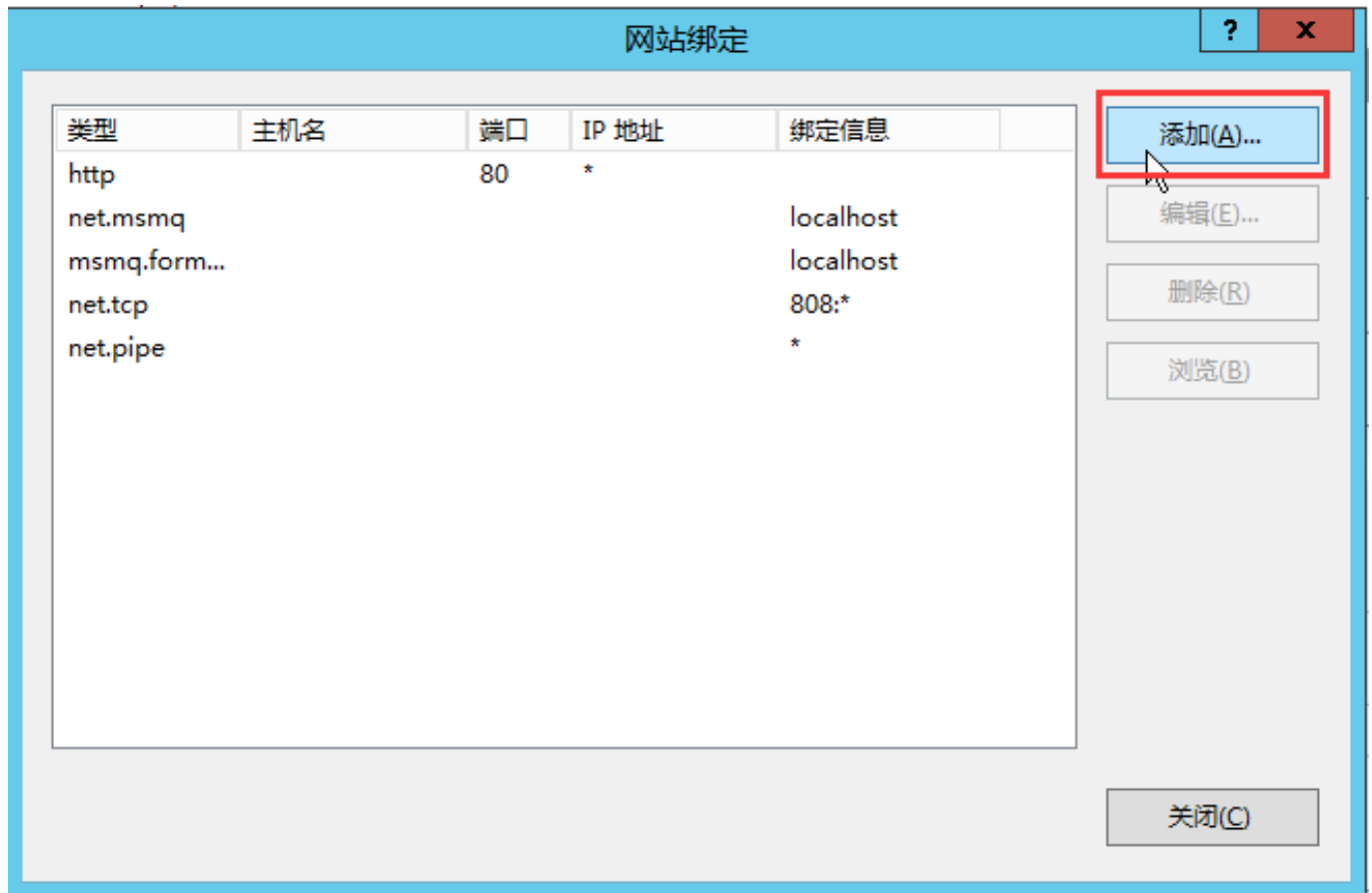
3、选择证书文件，如果输入申请证书时有填写私钥密码需要输入密码，否则输入文件夹中密码文件keystoreP
ass.txt的密码内容，点击确定。[参考私钥密码指引](#)



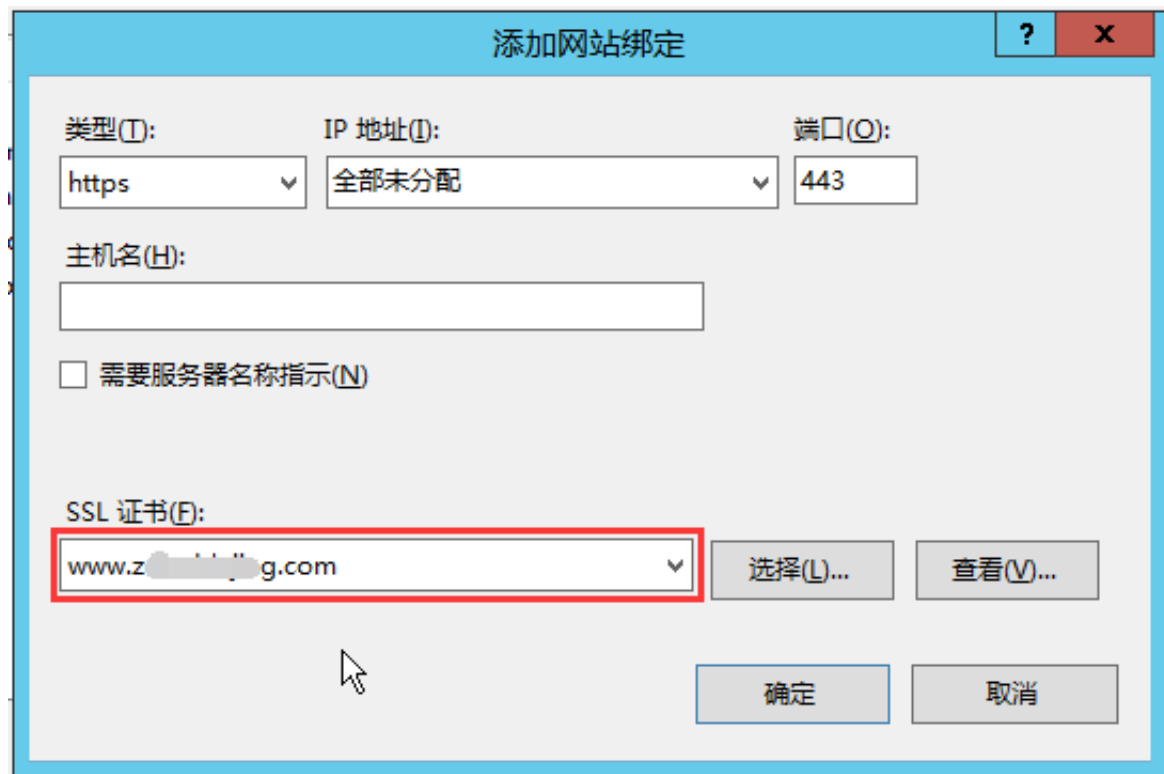
4、点击网站下的站点名称，点击右侧的绑定



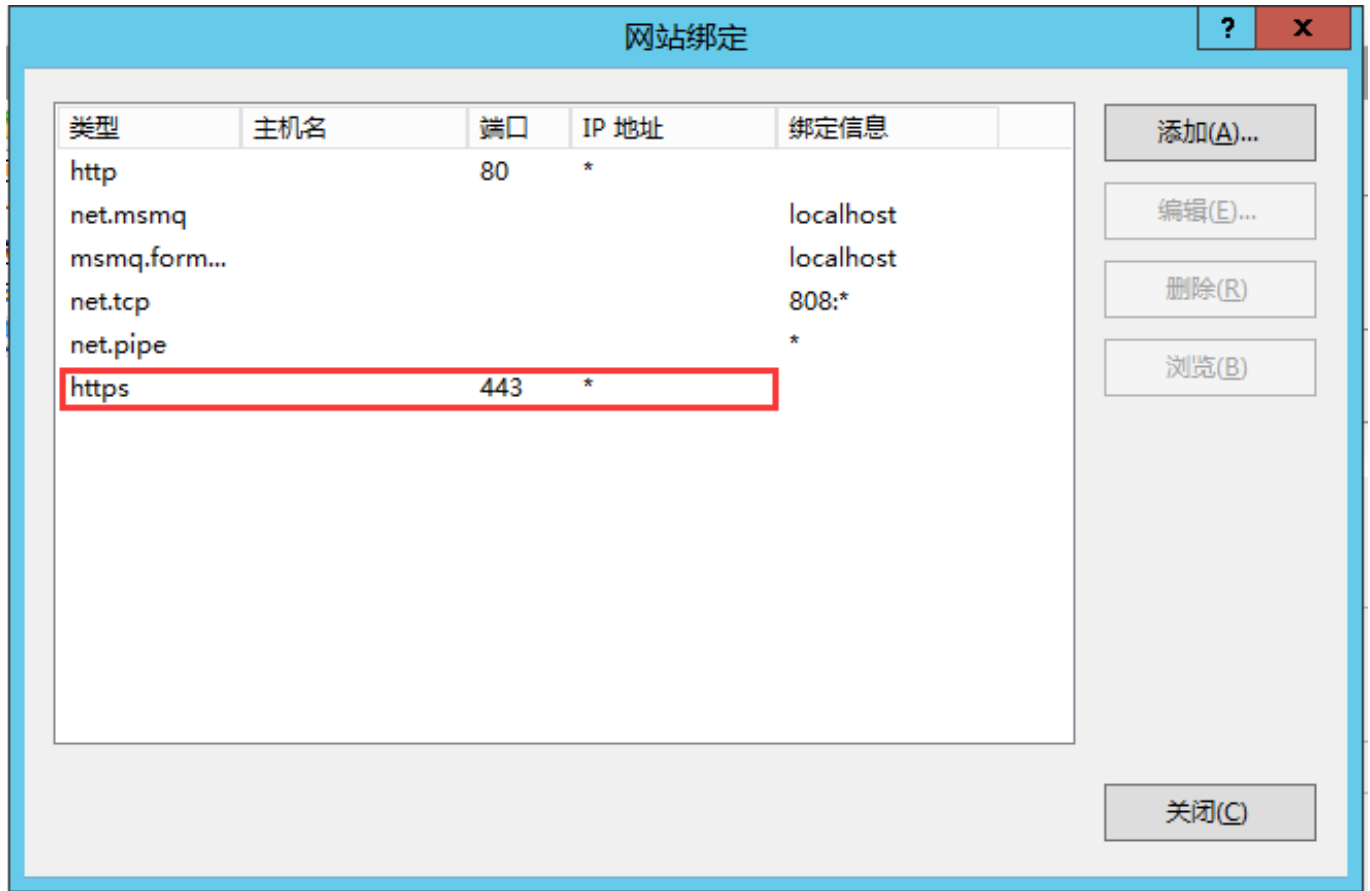
5、打开网站绑定界面后，点击添加



6、添加网站绑定内容：选择类型为https，端口443和指定对应的SSL证书，点击确定



7、添加完成后，网站绑定界面将会看到刚刚添加的内容



4. Tomcat 证书部署

4.1 获取证书

如果申请证书时有填写私钥密码，下载可获得Tomcat文件夹，其中有密钥库 `www.domain.com.jks`；

如果没有填写私钥密码，证书下载包的Tomcat文件夹中包括密钥库文件`www.domain.com.jks`

与密钥库密码文件`keystorePass.txt`

当用户选择粘贴CSR时，不提供Tomcat证书文件的下载，需要用户手动转换格式生成,操作方法如下：

可以通过 Nginx 文件夹内证书文件和私钥文件生成jks格式证书

转换工具：<https://www.trustasia.com/tools/cert-converter.htm>

使用工具时注意填写 密钥库密码，安装证书时配置文件中需要填写。

4.2 证书安装

配置SSL连接器，将

www.domain.com.jks

文件存放到conf目录下，然后配置同目录下的

server.xml

文件：

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
keystoreFile="conf/www.domain.com.jks"
keystorePass="changeit"
clientAuth="false" sslProtocol="TLS" />
```

注：

配置文件参数	说明
clientAuth	如果设为true，表示Tomcat要求所有的SSL客户出示安全证书，对SSL客户进行身份验证
keystoreFile	指定keystore文件的存放位置，可以指定绝对路径，也可以指定相对于（Tomcat安装目录）环境变量的相对路径。如果此项没有设定，默认情况下，Tomcat将从当前操作系统用户的用户目录下读取名为“.keystore”的文件。
keystorePass	密钥库密码，指定keystore的密码。（如果申请证书时有填写私钥密码，密钥库密码即私钥密码，否则填写密钥库密码文件中的密码）
sslProtocol	指定套接字（Socket）使用的加密/解密协议，默认值为TLS

4.3 http自动跳转https的安全配置

到conf目录下的web.xml。在

```
</welcome-file-list>
```

后面，

```
</web-app>
```

，也就是倒数第二段里，加上这样一段

```
<login-config>
  <!-- Authorization setting for SSL -->
  <auth-method>CLIENT-CERT</auth-method>
  <realm-name>Client Cert Users-only Area</realm-name>
</login-config>
<security-constraint>
  <!-- Authorization setting for SSL -->
  <web-resource-collection>
    <web-resource-name>SSL</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

这步目的是让非ssl的connector跳转到ssl的connector去。所以还需要前往server.xml进行配置：

```
<Connector port="8080" protocol="HTTP/1.1"
  connectionTimeout="20000"
  redirectPort="443" />
```

redirectPort改成ssl的connector的端口443，重启后便会生效。

域名型证书吊销指引

1. 提交工单

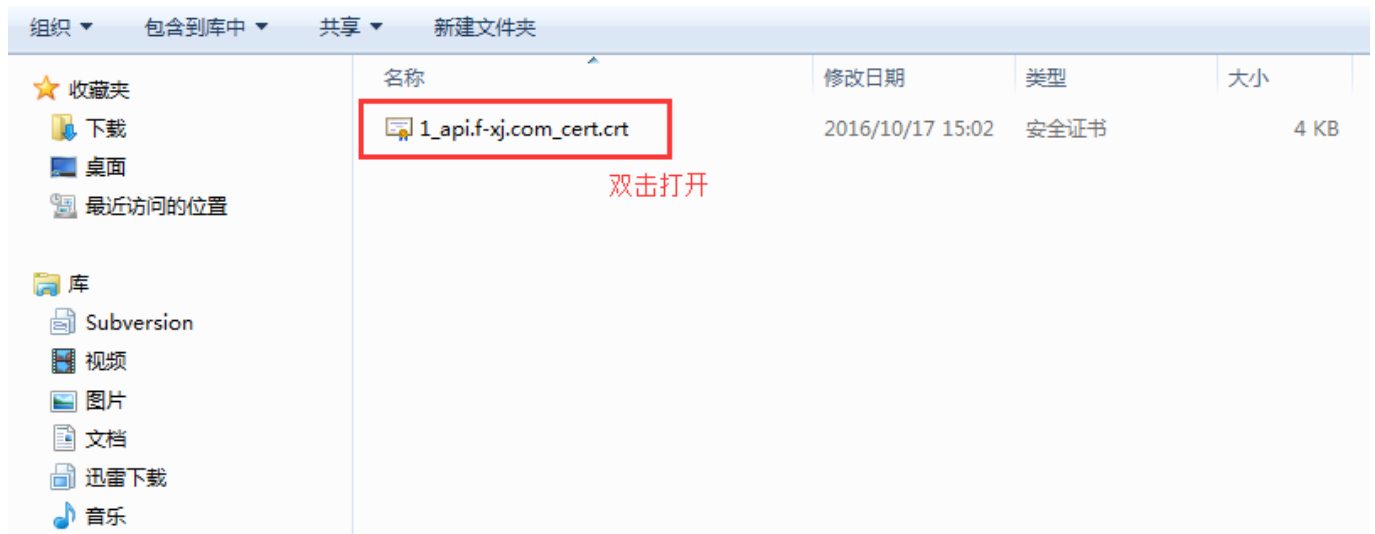
[提交工单](#) 寻求腾讯云工程师协助您完成证书吊销。

2. 提供相关信息

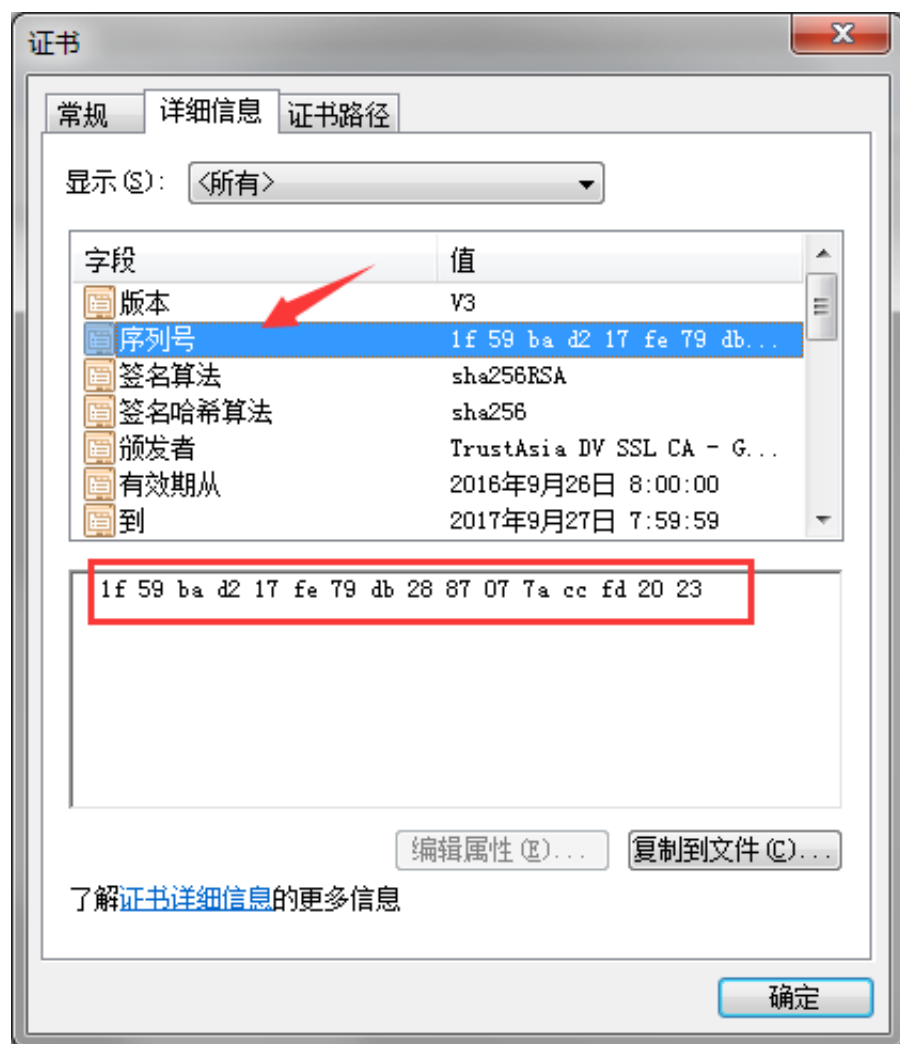
提供证书信息：包括证书ID、域名、证书序列号。

3. 证书序列号获取方法

3.1 下载证书到本地，双击打开



3.2 切换到【详细信息】，获取证书序列号



4. 重新验证域名身份

腾讯云工程师会要求您完成相应的DNS验证或者文件验证，完成身份验证后，CA机构方可继续完成证书吊销流程。

苹果ATS特性服务器配置指南

配置指南：

1. 需要配置符合PFS规范的加密套餐，目前推荐配置：

ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4

2. 需要在服务端TLS协议中启用TLS1.2，目前推荐配置：

TLSv1 TLSv1.1 TLSv1.2

1.Nginx 证书配置

更新Nginx根目录下 conf/nginx.conf 文件如下：

```
server {  
    ssl_ciphers ECDHE-RSA-AES128-GCM-  
SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4;  
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;  
}
```

2.Apache 证书配置

更新Apache根目录下 conf/httpd.conf 文件如下：

```
<IfModule mod_ssl.c>  
    <VirtualHost *:443>  
        SSLProtocol TLSv1 TLSv1.1 TLSv1.2  
        SSLCipherSuite ECDHE-RSA-AES128-GCM-
```

```
SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4
```

```
</VirtualHost>
```

```
</IfModule>
```

3.Tomcat 证书配置

更新 %TOMCAT_HOME%\conf\server.xml 文件如下：

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
```

```
scheme="https" secure="true"
```

```
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
```

```
SSLCipherSuite="ECDHE-RSA-AES128-GCM-
```

```
SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4" />
```

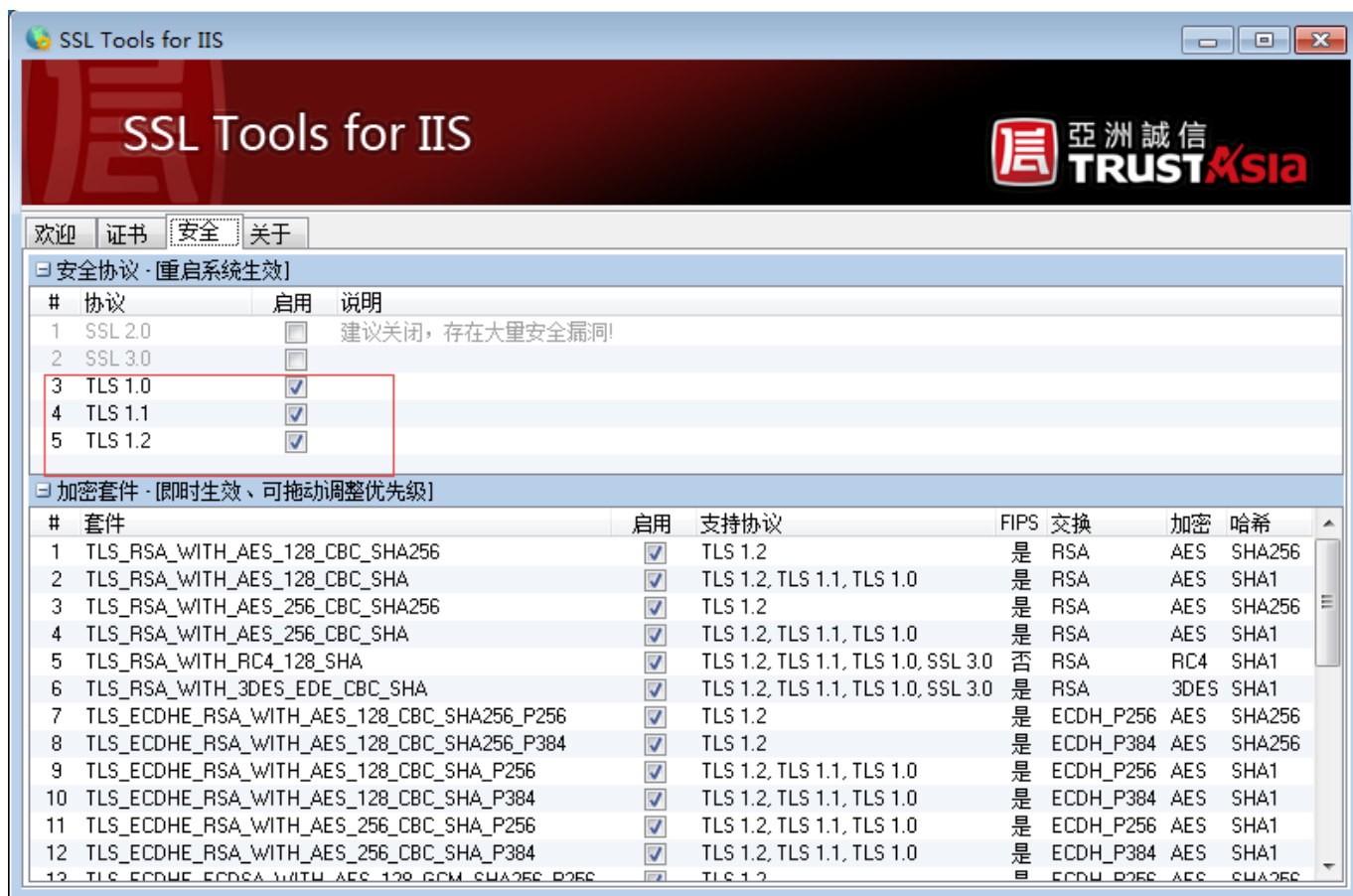
4.IIS 证书配置

4.1 方法一

Windows 2008及更早的版本不支持TLS1_2协议 所以无法调整 2008R2 TLS1_2协议默认是关闭的
需要启用此协议达到ATS要求

以2008 R2为例，导入证书后没有对协议及套件做任何的调整。

证书导入后检测到套件是支持ATS需求的，但协议TLS1_2没有被启用，ATS需要TLS1_2的支持。可使用的ssltools工具（亚洲诚信提供，[点击下载](#)）启用TLS1_2协议



勾选三个TLS协议并重启系统即可。

如果检查到PFS不支持，在加密套件中选中带ECDHE和DHE就可以了。

4.2 方法二

开始——运行 输入regedit

找到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols右键->新建->项->新建TLS 1.1,TLS 1.2

TLS 1.1和TLS 1.2 右键->新建->项->新建Server, Client

在新建的Server和Client中都新建如下的项(DWORD 32位值), 总共4个

DisabledByDefault [Value = 0]

Enabled [Value = 1]

The following tables represent the registry data shown in the screenshots:

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enable	REG_DWORD	0x00000001 (1)

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enable	REG_DWORD	0x00000001 (1)

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enable	REG_DWORD	0x00000001 (1)

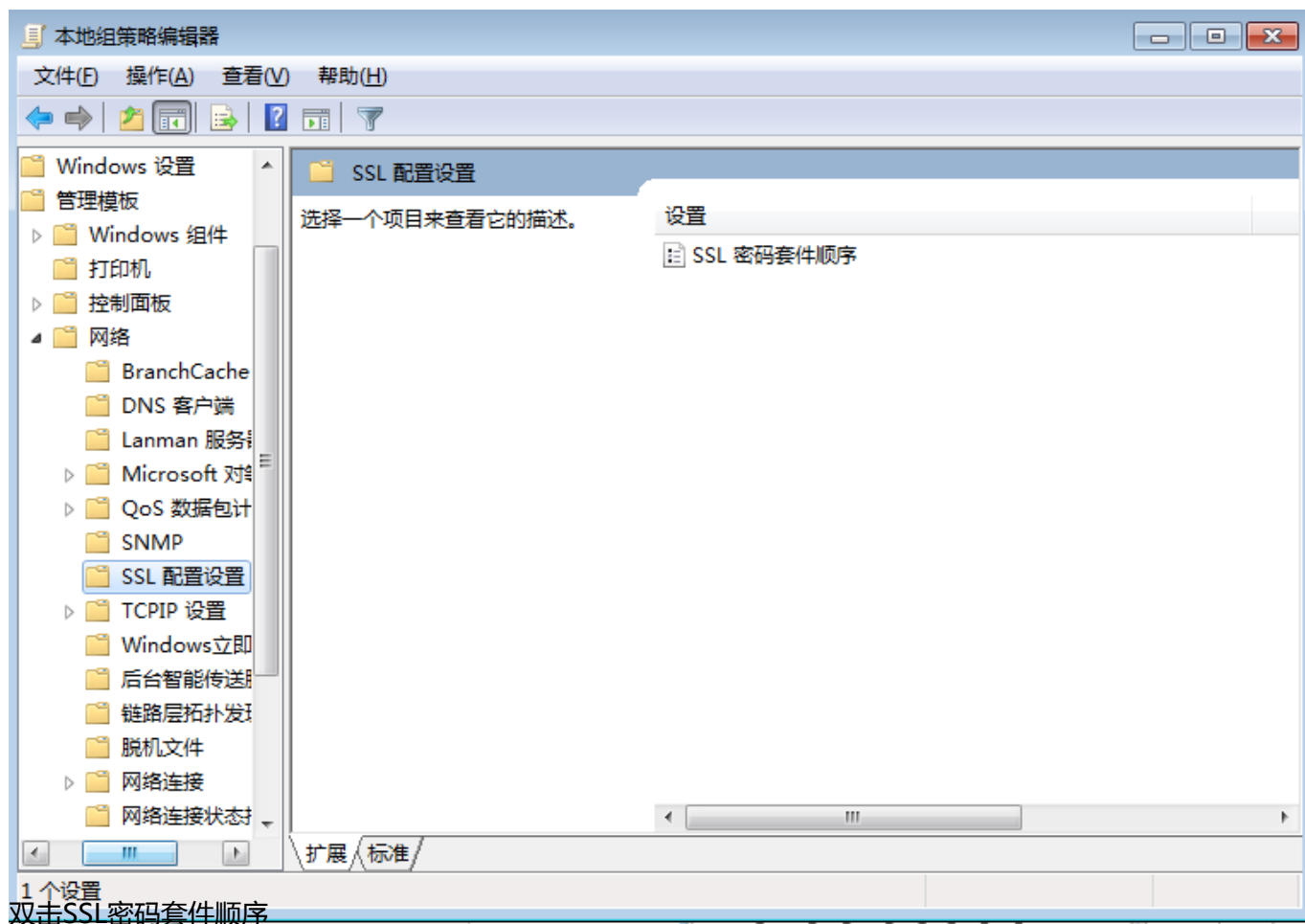
名称	类型	数据
(默认)	REG_SZ	(数值未设置)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enable	REG_DWORD	0x00000001 (1)

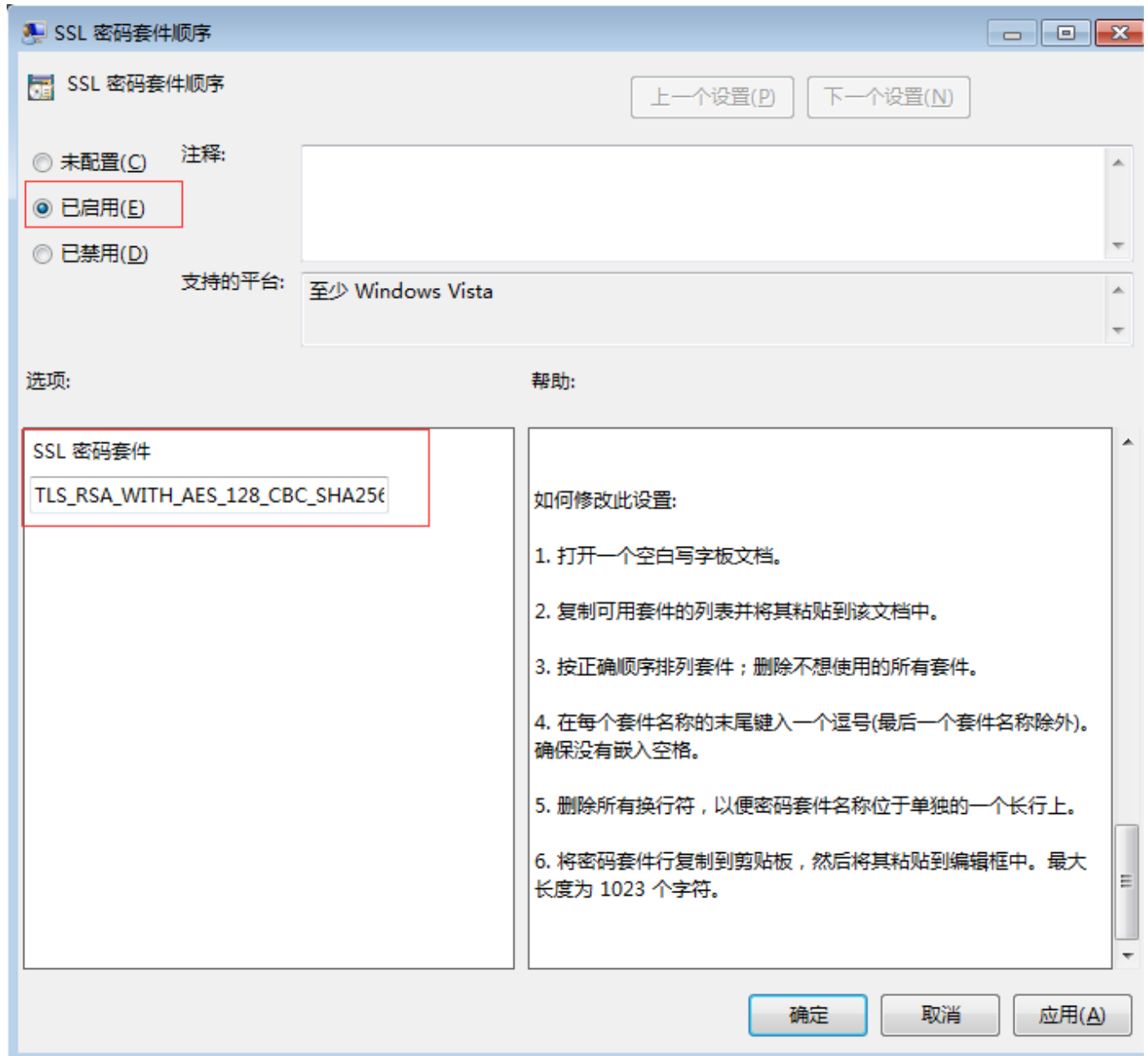
完成后重启系统

加密套件调整

对于前向保密加密套件不支持的话可通过组策略编辑器进行调整。

开始菜单——运行、输入gpedit.msc 进行加密套件调整 在此操作之前需要先开启TLS1_2协议





把支持的ECDHE加密套件加入SSL密码套件中 以逗号 (,) 分隔

打开一个空白写字板文档。

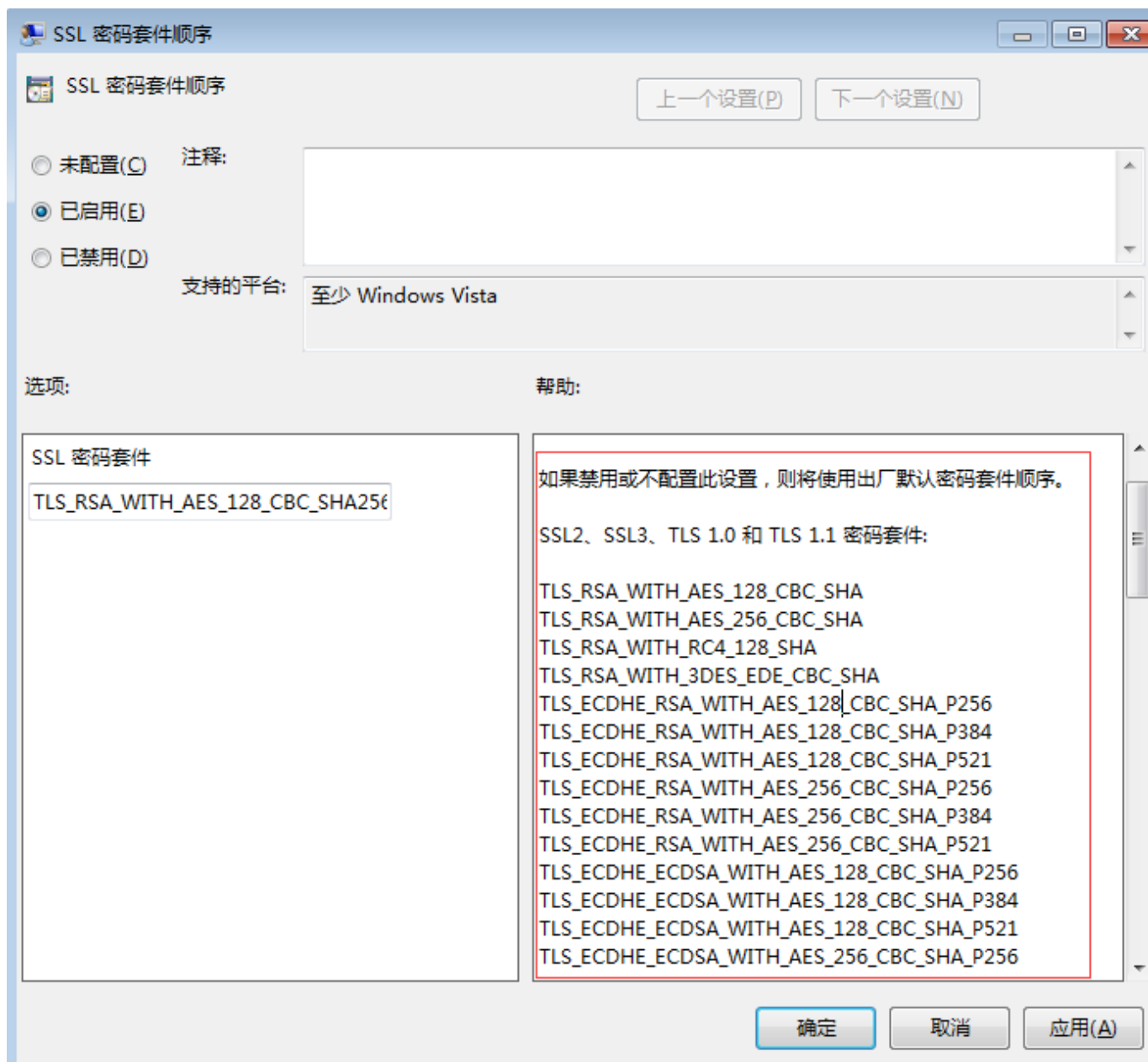
复制下图中右侧可用套件的列表并将其粘贴到该文档中。

按正确顺序排列套件；删除不想使用的所有套件。

在每个套件名称的末尾键入一个逗号(最后一个套件名称除外)。确保没有嵌入空格。

删除所有换行符，以便密码套件名称位于单独的一个长行上。

将密码套件行复制到剪贴板，然后将其粘贴到编辑框中。最大长度为 1023 个字符。



可将以下套件加入密码套件中

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

附:

推荐套件组合：

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

安全签章指引

什么是安全认证签章？

诺顿安全认证签章是由Symantec SSL证书提供、互联网上最受认可的信任标记。由赛门铁克开展的个人用户调查表明，诺顿安全认证签章保留了电子商务网站所有人和其他注重隐私的网站所有人所重视的高知名度和信赖度。2013年1月展开的独立调查也显示，诺顿安全认证签章让个人用户对互联网的信任度达到最高。



使用安全认证签章的原因

诺顿安全认证签章在 170 个国家或地区每天显示近 10 亿次。

通过获得客户认可来拓展在线业务：根据一个国际在线消费者研究报告，90% 的调查对象表示如果在结账流程中看到诺顿安全认证签章，他们很可能会继续在线购买，这一数字高于任何其他签章或没有签章显示的情况。

在全球范围内，有超过 4000

多万台使用诺顿网页安全的台式机在搜索结果中的可信网站链接旁显示诺顿安全认证签章。

赛门铁克强大的 PKI 基础架构包括军用级数据中心和灾难恢复站点，可以为客户端提供无与伦比的保护和可用性，让客户高枕无忧。

此签章是您致力于执行 PCI

遵从的可见图像证明，因为电子商务站点必须验证其身份并加密通过其站点的交易通信，从而保护客户端数据。

签章安装说明

用户可以通过诺顿安全签章[在线生成工具](#)，输入自己的域名来获取相应的安全签章代码。

如下所示，

www.domain.com

网站的安全签章代码：

```
<div id="symantecSeal" style="text-align: center" title="单击即可验证 - 该站点选择 SymantecSSL  
实现安全的电子商务和机密通信">  
<script type="text/javascript" src=  
"https://seal.verisign.com/getseal?host_name=www.domain.com&amp;size=L&amp;use_flash=YES&  
amp;use_transparent=YES&amp;lang=zh_cn"> </script>  
</div>
```