

# SSL 证书

## 常见问题

## 产品文档



腾讯云

## 【 版权声明 】

©2013–2021 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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默示的承诺或保证。

## 【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

## 文档目录

### 常见问题

#### 选择 SSL 证书相关

- 如何选择 SSL 证书?
- SSL 证书支持绑定 IP 的证书有哪些?
- 未开启网站服务前是否可以申请 SSL 证书?

#### SSL 证书申请相关

- 免费 SSL 证书名额相关问题
- 如何填写 SSL 证书申请中的绑定域名?
- 不会申请 SSL 证书或域名验证、资料审核不通过怎么办?
- 泛域名 SSL 证书相关问题
- 为什么收到 CA 机构的通知, 但订单状态没有变化?
- SSL 证书配置的 TXT 解析是否可以删除?
- 什么是 CSR?
- 如何制作 CSR 文件?
- 忘记私钥密码怎么办?
- 私钥丢失了怎么办?
- SSL 证书是否支持吊销?
- 提交 SSL 证书吊销申请时, 控制台提示“证书已关联云资源, 无法吊销”怎么办?

#### SSL 证书安装相关

- IIS 下设置 https 主机名灰色无法编辑怎么办?
- 服务器如何开启 443 端口?
- 访问站点提示连接不安全?
- 如何安装 OpenSSL?
- 如何设置 SSL 证书的 TLS 协议版本?
- 如何补全 SSL 证书链?

#### SSL 证书地域相关

- SSL 证书安装存在地域限制吗?

#### SSL 证书审核相关

- 安全审核失败的原因?
- 免费 SSL 证书一直在待验证怎么办?
- 申请 SSL 证书审核失败的原因及处理方法
- 已购 SSL 证书提交申请审核后需要做什么?
- 域名未通过安全审核该怎么办?
- 如何查看域名型 (DV) SSL 证书域名验证结果?

#### SSL 证书生效相关

电脑或手机中的浏览器提示 SSL 证书不可信怎么办？

服务器 IP 地址更换后原来的 SSL 证书能否生效？

如何在浏览器中检查 SSL 证书是否生效？

GlobalSign 证书 Windows 7 系统下不受信任怎么办？

SSL 证书收费和购买相关

域名型（DV）SSL 证书是否永久免费？

SSL 证书有效期相关

SSL 证书过期了怎么办？

SSL 证书过期后未及时更新有哪些影响？

查看 SSL 证书到期相关问题

SSL 证书成功续费后可以继续服务吗？

SSL 证书域名相关

域名验证提供哪几种方式？

# 常见问题

## 选择 SSL 证书相关

### 如何选择 SSL 证书？

最近更新时间：2020-08-28 10:49:18

#### 如何选择证书种类？

- 如果您的网站主体是个人（即没有企业营业执照），只能申请域名型（DV）免费证书或域名型（DV）付费证书。
- 对于金融、支付类企业，建议购买 EV 型证书。
- 对于一般企业，建议购买 OV 型及以上类型的 SSL 证书。
- 若作为移动端网站或接口调用，也建议您购买 OV 型及以上类型的 SSL 证书。

#### 如何选择证书品牌？

您可以根据各 SSL 证书品牌浏览器兼容性测试报告以及企业的业务情况进行购买。

具体请查看 [浏览器兼容性测试报告](#)。

#### 如何选择支持域名数量？

腾讯云提供以下四种域名类型，具体区别请查看如下内容：

- **单域名**：只支持绑定1个域名，可以是二级域名 `tencent.com`，也可以是三级域名 `example.tencent.com`，均可以支持，但不支持二级域名下的所有子域名。域名级数最多可以支持100级。
- **多域名**：单个证书可以绑定多个域名，最多可以支持域名数量以官网售卖为准。
- **泛域名**：支持绑定一个且只有一个泛域名，泛域名只允许添加一个通配符，例如 `*.tencent.com`、`*.example.tencent.com`，最多支持100级；`*.*.tencent.com` 多个通配符的泛域名是不支持的。
- **通配符多域名**：支持绑定多个泛域名，泛域名只允许添加一个通配符，例如 `*.tencent.com`、`*.example.tencent.com`，最多支持100级；`*.*.tencent.com` 多个通配符的泛域名是不支持的。

# SSL 证书支持绑定 IP 的证书有哪些？

最近更新时间：2021-03-03 11:28:48

## 支持绑定 IP 的证书品牌与类型有那些？

腾讯云支持绑定 IP 的 SSL 证书请参考下表：

证书品牌	企业型 (OV)	企业型专业版 (OV Pro)	域名型 (DV)	域名型免费版 (DV)	增强型 (EV)	增强型专业版 (EV Pro)
SecureSite	不支持	不支持	不支持	不支持	不支持	不支持
GeoTrust	不支持	-	-	-	不支持	-
TrustAsia	不支持	-	不支持	-	不支持	-
GlobalSign	不支持	-	-	-	不支持	-
Wotrus	不支持	-	不支持	-	不支持	-
DNSPod	支持				支持	-

# 未开启网站服务前是否可以申请 SSL 证书？

最近更新时间：2020-07-28 18:33:08

## 未开启网站服务前是否可以申请 SSL 证书？

已拥有域名并且具有解析权限，即可申请 SSL 证书（付费证书与免费证书都可申请）。

### 注意：

如果您申请证书时还未购买云服务资源，证书验证时将不支持文件验证的方式。

# SSL 证书申请相关

## 免费 SSL 证书名额相关问题

最近更新时间：2020-12-07 10:48:48

### 免费证书有多少个免费名额？

由于 CA 机构和证书代理商策略调整，从2018年1月1日起，同一主域最多只能申请20张亚洲诚信品牌免费型 DV 版 SSL 证书。之前已颁发的证书在有效期内使用不受影响。

#### ⚠ 注意：

- 二级域名及其子域名均属于同一主域，例如，tencent.com、ssl.tencent.com、ssl.ssl.tencent.com 都属于同一主域。
- 若即将到期的证书需要在2018年1月1日以后重新申请，会受到上述策略的限制。
- 一个账号下的免费证书额度只有50个。

### 免费证书吊销或到期后删除是否仍占用20个免费名额？

若您的证书已颁发，吊销后仍会计算免费证书额度。

亚洲诚信品牌免费型 DV 版 SSL 证书目前按照15个月内的证书订单进行额度统计。



# 如何填写 SSL 证书申请中的绑定域名？

最近更新时间：2021-03-01 16:38:49

## 如何填写证书申请中的绑定域名？

当完成 SSL 证书购买后，您需要在 [腾讯云证书管理控制台](#) 提交证书申请的审核资料。证书管理控制台将会根据您购买的证书提示您需要输入的域名类型和数量。如下图所示：

1 提交资料 > 2 上传确认函 > 3 通过人工审核 > 4 签发证书

CSR生成  在线生成  粘贴CSR  
推荐使用在线生成CSR，由平台生成和管理您的私钥和公钥证书文件，避免私钥文件丢失

算法选择  RSA算法  ECC算法

密钥长度  2048  4096

证书绑定域名

即绑定证书的域名，请填写单个域名。例如tencent.com、ssl.tencent.com。

其他域名

每行请输入一个域名，例如：  
qcloud.com  
ssl.qcloud.com  
example.ssl.qcloud.com

请输入证书绑定的其他域名，注意不要与通用名称重复，提交CA机构后将无法修改

私钥密码(选填)

为了保障私钥安全，目前不支持密码找回功能，请您牢记私钥密码。  
如需部署腾讯云负载均衡、CDN等云服务，请勿填写私钥密码。

### 说明：

需正确填写证书绑定的域名信息，才可保证您的 SSL 证书顺利颁发并正常使用 HTTPS 服务。

腾讯云 SSL 证书服务，将会根据您购买的品牌和申请时填写的绑定域名，为您赠送相对的上级域，详情如下表：

证书类型	GlobalSign	TrustAsia (OV/EV)	TrustAsia (DV)	GeoTrust
赠送规则				

	GlobalSign	TrustAsia (OV/EV)	TrustAsia (DV)	GeoTrust
绑定域名不带 www. 开头，赠送 www. 子域	不赠送	绑定域名为主域时赠送 www. 子域	绑定域名为主域时赠送 www. 子域	绑定域名为主域时赠送 www. 子域
绑定普通域名和通配符泛域名，赠送上级域	赠送	赠送	赠送	赠送

## 什么是泛域名？

带通配符的域名，例如：`*.tencent.com`、`*.cloud.tencent.com` 均为泛域名，包含同一级的全部子域名。

### 注意：

域名不支持跨级，例如 `*.tencent.com` 不包含 `*.cloud.tencent.com` 下一层级域名。

# 不会申请 SSL 证书或域名验证、资料审核不通过怎么办？

最近更新时间：2020-07-28 18:38:24

## 不会申请证书或域名验证、资料审核不通过怎么办？

如果您急需对证书选型、证书域名验证、安装证书过程中任何操作上的指导，您可前往 [腾讯云市场](#) 购买证书相关服务。

# 泛域名 SSL 证书相关问题

最近更新时间：2020-11-02 10:28:48

## 泛域名证书都支持哪些域名？

腾讯云 SSL 证书支持泛域名证书，您可以通过泛域名证书保护服务器的单个主域名和该主域名下同级别的所有别子域名。泛域名企业型（OV）和域名型（DV）类型证书都支持泛域名。

如果您拥有多个同级别子域名服务器，使用泛域名证书无需为每个子域名单独购买和安装证书。

- 泛域名证书支持的域名包含二级域名。
- 泛域名证书只支持一个通配符主域名，不支持多个主域名。
- 泛域名证书目前仅支持通配符类型的域名、不支持普通域名（非通配符域名）。如需一张证书能包含多个通配符域名和一个或一个以上普通域名，建议购买通配符多域名类型 SSL 证书。

## 泛域名证书匹配域名的规则是什么？

泛域名证书只能匹配同级别的子域名，不能跨级匹配。例如，三级泛域名 `*.tencent.com` 不支持四级域名 `www.ssl.tencent.com`。

# 为什么收到 CA 机构的通知，但订单状态没有变化？

最近更新时间：2020-07-28 18:38:35

## 为什么收到 CA 机构的通知，但订单状态没有变化？

在资料审核环节和证书颁发环节，CA 机构可能会发送一封邮件通知您申请证书的进展。如果您发现腾讯云 SSL 证书控制台中的订单状态还没有发生变化，这是由于 CA 机构给腾讯云推送的订单状态会有延迟，建议您耐心等待一段时间才能看到订单的状态变化。

# SSL 证书配置的 TXT 解析是否可以删除？

最近更新时间：2020-07-28 18:38:41

## 证书配置的 TXT 解析是否可以删除？

证书颁发完成后，您可以删除证书配置的 TXT 解析，对证书无影响。

# 什么是CSR?

最近更新时间：2020-06-29 15:24:02

## 什么是 CSR?

CSR 即证书签名申请 (Certificate Signing Request)，获取 SSL 证书，需要先生成 CSR 文件并提交给证书颁发机构 (CA)。CSR 包含了公钥和标识名称 (Distinguished Name)，通常从 Web 服务器生成 CSR，同时创建加解密的公钥私钥对。

在创建 CSR 过程中，需要提供相关组织机构信息，web 服务器会根据提供的信息创建证书的标识名称，用来识别证书，内容如下：

### 国家或地区代码

您的组织机构依法注册所在的国家或地区的代码，以国际标准化组织 (ISO) 的两字母格式表示。

### 省或市或自治区

您的组织机构所在的省或市或自治区。

### 城市或地区

您的组织机构注册所在的城市或地区。

### 组织机构

您的企业依法注册所用的名称。

### 组织机构单位

此字段用于区分组织机构中的各部门，例如“工程部”或“人力资源部”。

### 通用名称

在 CSR 的通用名称字段中输入的名称必须是您要为其使用证书的网站的完全限定域名 (FQDN)，例如“www.domainnamegoeshere”。

但是腾讯云采用了在线生成 CSR 的方式，无需您生成和提交 CSR 文件，域名型证书仅需要提交通用名称即可申请，帮助您简化申请流程。

# 如何制作 CSR 文件?

最近更新时间：2020-07-10 15:03:28

## 如何制作 CSR 文件?

本文档指导您如何制作 CSR ( Certificate Signing Request ) 文件。

### 前提条件

申请数字证书之前，您需要准备生成证书的密钥文件和 CSR 文件。CSR 文件是您的公钥证书原始文件，包含了您的服务器信息和您的单位信息，需要提交给 CA 认证中心进行审核。建议您使用系统创建的 CSR 文件，避免出现输入信息错误而导致审核失败。若您选择手动生成 CSR 文件，请务必妥善保管并备份您的密钥文件，手动生成 CSR 文件时需要注意以下信息：

- 输入的中文信息需要使用 UTF-8 编码格式，请在编辑 OpenSSL 工具时，指定支持 UTF-8 编码格式。
- 证书服务系统对 CSR 文件的密钥长度有严格要求，密钥长度必须是 2048bit，密钥类型必须是 RSA。
- 如果申请证书是多域名或者通配子域名，在 Common Name 或 What is your first and last name? 区域只需要输入一个域名。

### 使用 OpenSSL 工具生成 CSR 文件

1. 登录运行 Linux 系统的一台本地计算机或服务器。
2. 安装 OpenSSL 工具，详情可参考 [如何安装 OpenSSL?](#)
3. 执行以下命令，即可生成 CSR 文件。

```
openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout [$Key_File] -out [$OpenSSL_CSR]
```

#### 🔍 说明：

- **new**：指定生成一个新的 CSR 文件。
- **nodes**：指定密钥文件不被加密。
- **sha256**：指定摘要算法。
- **newkey rsa:2048**：指定密钥类型和长度。
- **[\$Key\_File]**：密钥文件名称。
- **[\$OpenSSL\_CSR]**：加密后文件的存放路径。

4. 根据系统返回的提示，输入生成 CSR 文件所需的信息。以下是关于提示的说明：

- **Organization Name**：公司名称，可以是中文或英文。
- **Organizational Unit Name**：部门名称，可以是中文或英文。



- **Country Code:** 申请单位所属国家，只能是两个字母的国家码。例如，中国填写为 CN。
- **State or Province Name:** 州名或省份名称，可以是中文或英文。
- **Locality Name:** 城市名称，可以是中文或英文。
- **Common Name:** 申请 SSL 证书的具体网站域名。
- **Email Address:** 可选择不输入。
- **Challenge Password:** 可选择不输入。

5. 按照命令提示输入相应内容后，即可在当前目录下获取密钥文件和 CSR 文件。

# 忘记私钥密码怎么办？

最近更新时间：2020-11-03 16:30:46

## 忘记私钥密码怎么办？

腾讯云不会替您保存证书的私钥密码，请牢记私钥密码。

如果遗失私钥密码，请 [提交工单](#)，选择【其他问题】，提交给腾讯云工程师，协助您删除该证书后重新申请对应域名的证书。

# 私钥丢失了怎么办？

最近更新时间：2020-09-08 11:42:17

## 私钥丢失了怎么办？

场景1：如果您的证书是付费证书，购买/续费时选择**在线生成 CSR**的方式，或者您的证书是免费证书，若存在丢失私钥文件的情况，请按如下操作：

1. 请登录 [SSL 证书管理控制台](#)。
2. 选择您需要获取私钥的证书，单击操作栏的【下载】，将压缩包解压即可获得对应私钥。

场景2：如果您的证书是付费证书，购买/续费时选择**粘贴 CSR**的方式，则私钥是您外部生成的，无法获取私钥，此时您可通过重颁发，并且选择**在线生成 CSR**的方式，即可生成新的证书和私钥。请按如下操作：

1. 请登录 [SSL 证书管理控制台](#)。
2. 选择您需要获取私钥的证书，选择【操作】>【更多】>【重颁发】。
3. 选择【在线生成 CSR】，确认信息并提交，即可获得新的证书和私钥。

# SSL 证书是否支持吊销？

最近更新时间：2020-10-10 16:35:53

## 证书是否支持吊销？

支持吊销，吊销流程请参考 [证书吊销指引](#)。

# 提交 SSL 证书吊销申请时，控制台提示“证书已关联云资源，无法吊销”怎么办？

最近更新时间：2021-02-25 17:56:22

## 提交 SSL 证书吊销申请时，控制台提示“证书已关联云资源，无法吊销”怎么办？

请您检查需要吊销的 SSL 证书是否已绑定腾讯云云资源，例如 CLB、CDN 等。如已绑定相关资源，请先进行解绑后再进行吊销证书操作。

# SSL 证书安装相关

## IIS 下设置 https 主机名灰色无法编辑怎么办?

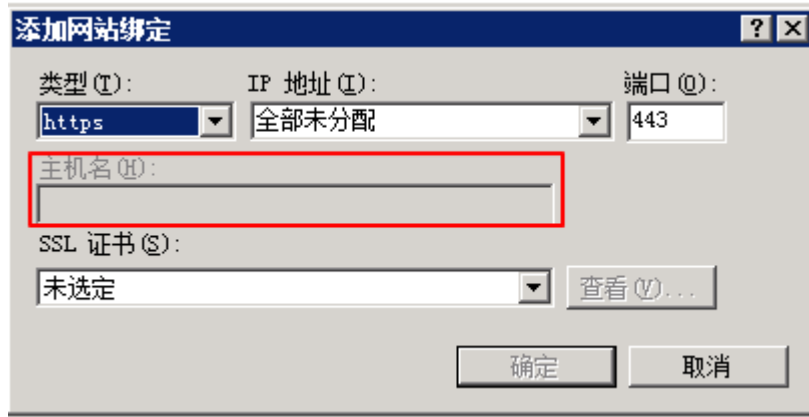
最近更新时间：2020-08-03 17:41:33

### IIS 下设置 https 主机名灰色无法编辑怎么办?

在安装证书时，若您使用 IIS 管理器进行安装，将 pfx 证书文件导入后，在添加网站绑定域名过程中，类型选择为“https”时，出现主机名显示无法编辑的情况，您可以通过以下步骤解决该问题。

#### 场景

在 IIS 设置中，选择 https，选择相应的 SSL 证书，主机名无法填写。如下图所示：



#### 解决办法

1. 请按路径 C:\Windows\system32\inetsrv\config\applicationHost.config 打开 applicationHost.config 文件。
2. 修改内容如下：

##### 说明：

- 以“tencent.com”域名为例。
- 将 `<binding protocol="https" bindingInformation="*:443:" />` 修改为 `<binding protocol="https" bindingInformation="*:443:tencent.com" />`。
- 文件无法直接修改时，可以尝试使用管理员权限进行修改或复制文件到桌面修改后，进行替换。

```
<site name="example.tencent.com" id="8">  
<application path="/">
```

```
<virtualDirectory path="/" physicalPath="D:\web\tencent" />
</application>
<bindings>
<binding protocol="http" bindingInformation="*:80:example.tencent.com" />
<binding protocol="http" bindingInformation="*:80:www.tencent.com" />
<binding protocol="https" bindingInformation="*:443:" />
</bindings>
</site>
```

3. 文件保存后，重新添加网站绑定即可。

# 服务器如何开启443端口?

最近更新时间：2020-07-23 17:03:32

## 服务器如何开启443端口?

- 若您使用的是腾讯云云服务器，请参考文档 [添加安全组规则](#) 开启443端口。
- 若您使用的是其他云厂商云服务器，请参考云厂商提供的相关文档。



# 访问站点提示连接不安全？

最近更新时间：2020-11-03 16:33:19

## SSL 证书部署以后，访问站点提示“连接不安全”，是否是证书部署失败？

证书已成功部署，也会出现这个问题，是因为采用 HTTPS 协议的站点访问。如果网页中包含未经加密的 HTTP 内容时，会被浏览器认为是不安全的，需要对代码进行改造。

前端改造上，可以有参考以下几点：

- 使用相对路径引用资源。
- 引用绝对路径时，采用 // 引用资源，例如 //img.qcloud.com/example.png，表示遵从当前页面的协议，浏览器会自动补齐。

# 如何安装 OpenSSL?

最近更新时间：2020-08-03 17:42:15

## 如何安装 OpenSSL?

OpenSSL 是用于安全通信的著名开源密码学工具包，包括主要的密码算法、常见密码和证书封装功能。

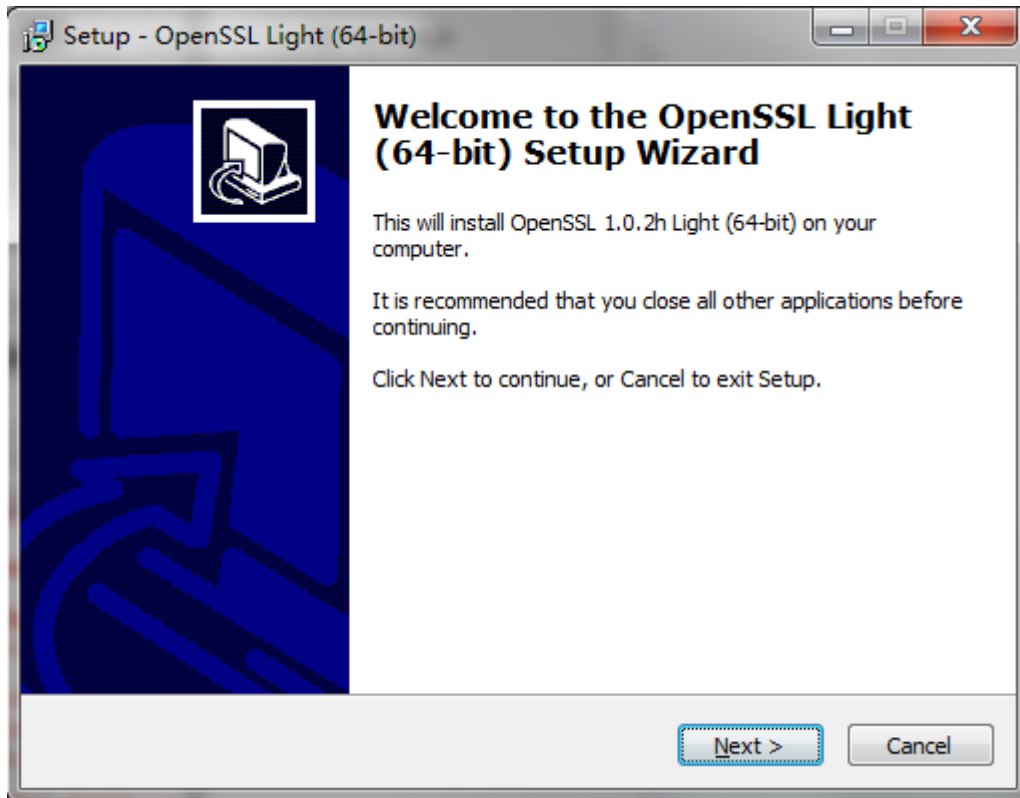
### OpenSSL 官网

官方下载地址：[请单击此处](#)。

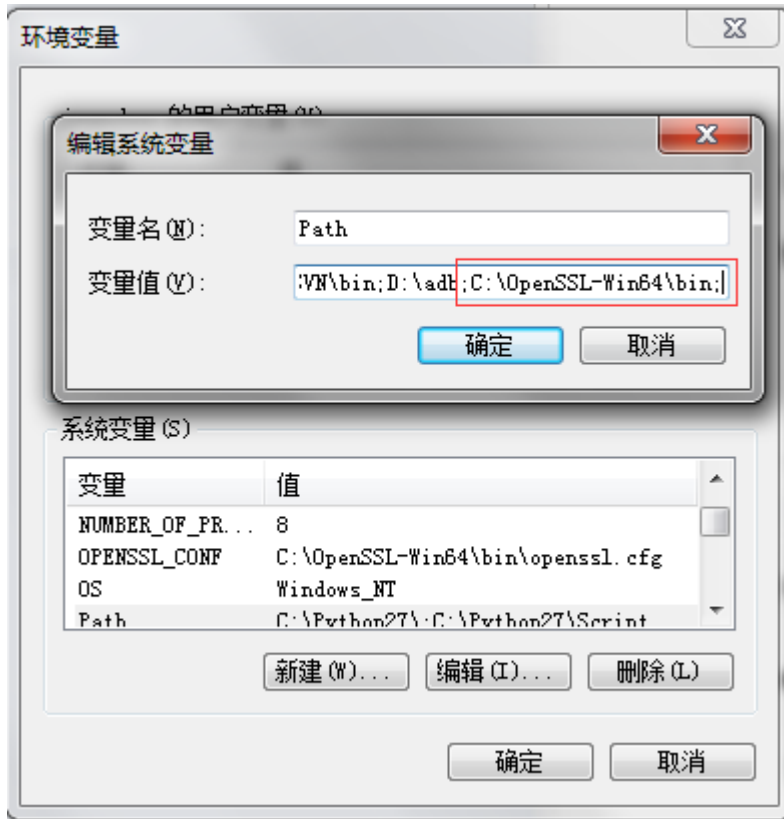
### Windows 安装方法

OpenSSL 官网没有提供 Windows 版本的安装包，可以选择其他开源平台提供的工具。[请单击此处](#)，以该工具为例，安装步骤和使用方法如下：

1. 选择32位或者64位合适的版本下载，例如 Win64openssl\_Light-1\_0\_2h.exe。如下图所示：



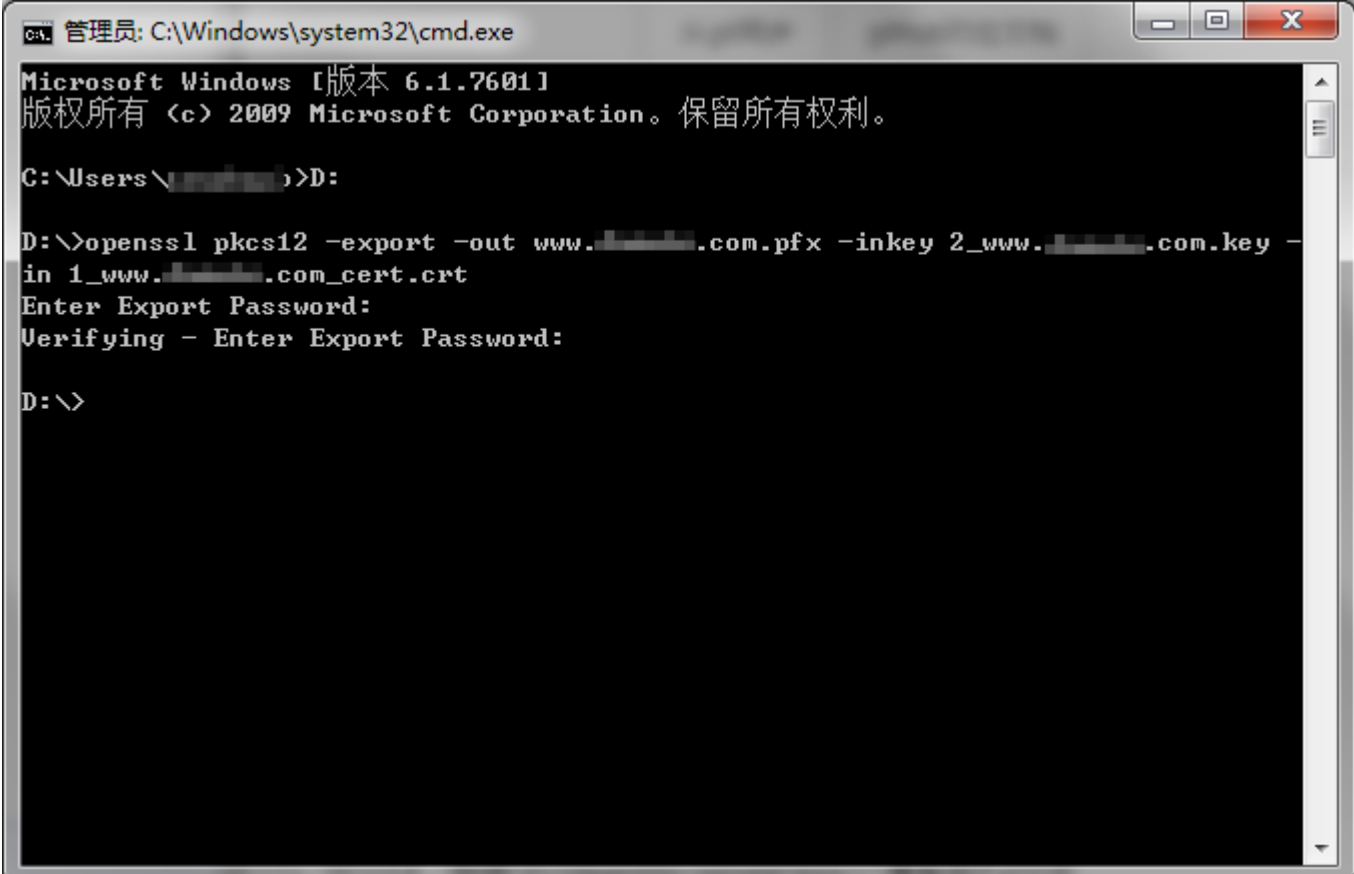
2. 设置环境变量，例如，工具安装在 C:\openssl-Win64，则将 C:\openssl-Win64\bin；复制到 Path 中。如下图所示：



3. 打开命令行程序 cmd (以管理员身份运行)，进入 2\_www.tencent.com.key、1\_www.tencent.com\_cert.crt 文件所在目录，运行以下命令。

```
openssl pkcs12 -export -out www.tencent.com.pfx -inkey 2_www.tencent.com.key -in 1_www.tencent.com_cert.crt
```

例如，key 和 crt 文件保存在 D:\，运行情况如下：



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\>D:

D:\>openssl pkcs12 -export -out www. .com.pfx -inkey 2_www. .com.key -
in 1_www. .com_cert.crt
Enter Export Password:
Verifying - Enter Export Password:

D:\>
```

**注意：**

Export Password 不需要的情况下，请直接回车不进行输入。

4. 在 D:\ 已生成的 www.tencent.com.pfx 文件，可以继续完成在 IIS 管理器中的证书安装。

# 如何设置 SSL 证书的 TLS 协议版本?

最近更新时间：2021-02-19 14:21:56

TLS 协议版本包括 TLSv1.0、TLSv1.1、TLSv1.2、TLSv1.3 等，您可根据您的实际需求在腾讯云相关产品或服务器 Web 服务上设置证书的 TLS 协议版本。

## 腾讯云相关产品

如果您的证书部署到以下腾讯云产品，请参考以下文档进行配置：

- 负载均衡 (CLB)：[HTTPS 转发配置入门指南](#)
- 内容分发网络 (CDN)：[TLS 版本配置](#)

## 服务器 Web 服务

如果您的证书安装在服务器 Web 服务上，请在 Web 服务的证书配置文件中找到 `ssl_protocols TLSv1 TLSv1.1 TLSv1.2`，并根据实际需求进行修改。

例如：您的证书需要支持 TLSv1.1 和 TLSv1.2 版本，则在 `ssl_protocols TLSv1 TLSv1.1 TLSv1.2` 中去掉 `TLSv1` 即可。

# 如何补全 SSL 证书链？

最近更新时间：2021-02-23 15:35:13

通常情况下 PC 端浏览器都可以通过 Authority Info Access（权威信息访问）的 URL 链接获得中间证书，但在部分 Android 系统的浏览器上访问时会出现证书不可信或无法访问等问题。

主要原因在于部分 Android 系统的浏览器并不支持通过 Authority Info Access（权威信息访问）的 URL 链接获得中间证书，这时您需要把证书链文件按照 SSL 证书链的结构合并为一个文件重新部署到服务器上，浏览器在与服务器连接时将会下载用户证书和中间证书，使您的浏览器访问时显示为可信证书。SSL 证书链结构如下所示：

```
-----BEGIN CERTIFICATE-----
```

网站证书

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

CA 中间证书机构

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

CA 根证书机构

```
-----END CERTIFICATE-----
```

## 🔍 说明：

- SSL 证书链的结构，一般是由【CA 根证书机构 -> CA 中间证书机构 -> 网站证书】构成，中间证书还可能存在多层关系。
- 腾讯云提供的 SSL 国际标准证书为完整的证书链，无需进行补齐即可正常使用。

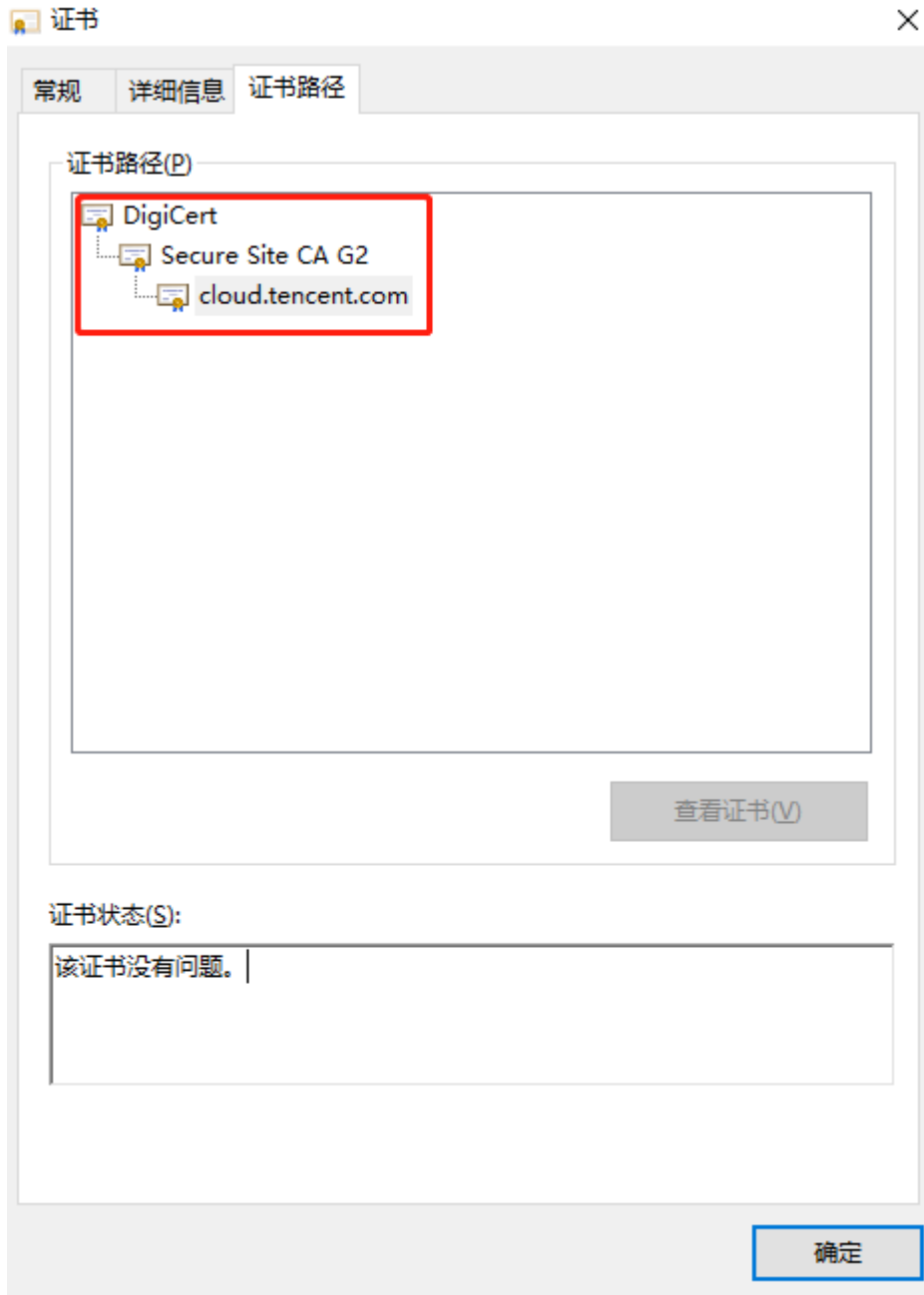
## 如何查看 SSL 证书链？

1. 打开 Chrome 浏览器访问安装部署 SSL 证书成功的网站。此处以 Chrome 浏览器为例。

2. 在浏览器地址栏单击🔒小锁图标，并在弹出的信息卡片中，单击【证书】。如下图所示：



3. 在弹出的“证书”信息窗口中，单击【证书路径】，即可查看 SSL 证书链。如下图所示：





---

# SSL 证书地域相关

## SSL 证书安装存在地域限制吗？

最近更新时间：2020-07-28 18:33:24

### SSL 证书安装存在地域限制吗？

证书购买和颁发后，安装部署不受地域的限制。

# SSL 证书审核相关 安全审核失败的原因？

最近更新时间：2020-11-03 16:32:30

## 安全审核失败的原因是什么？

申请域名型（DV）SSL 证书时，出现如下提示，说明申请域名的安全审核失败，SecureSite CA 机构的快速审核流程不支持对该域名颁发域名型 SSL 证书，请购买付费证书。如下图所示：



## 安全审核失败的具体原因：

由于 CA 机构的反钓鱼机制，一般是域名信息中包含敏感词，例如 bank、pay 等，会引起安全审核失败，具体敏感词由 CA 机构定义，同时部分不常用的根域名也可能会审核失败，例如，www.qq.pw、www.qcloud.pw 等以 .pw 根域名后缀的无法通过审核。

### 说明：

域名型 SSL 证书通过自动认证快速签发，不会人工介入审核，会用较为严格的敏感词来加强审核标准。

# 免费 SSL 证书一直在待验证怎么办？

最近更新时间：2020-12-07 10:50:13

## 免费证书一直在待验证怎么办？

免费证书具有自主诊断功能，若一直处于待验证状态，您可以通过该证书的详情页提示自主查看域名验证状态，通过验证后，请您耐心等待，证书状态的更新需要一定时间，通常将在10分钟 - 24小时内颁发证书。

# 申请 SSL 证书审核失败的原因及处理方法

最近更新时间：2020-07-28 18:33:43

## 申请证书审核失败的原因及处理方法

本文主要介绍申请证书审核失败的可能原因和解决方法。

### 验证文件配置错误

#### 说明：

建议您执行 `curl -k -v` 命令或者 `wget -S` 命令验证文件 URL 是否生效。同时，需要分别对 HTTPS 和 HTTP 两种协议的 URL 进行验证。

#### 问题原因：

如果您在提交 SSL 证书审核时使用文件验证方式进行域名验证，可能会因为此问题造成订单审核失败。该场景下的 SSL 证书审核申请失败的可能原因如下：

- 站点部分页面已启用 HTTPS 访问方式，而验证文件仅部署在 HTTP 服务路径下，并没有部署在 HTTPS 服务路径下，导致用 HTTPS 协议请求时找不到对应的文件。
- 访问验证文件时，站点返回错误代码。
- 启用了 CDN 服务，而 CDN 服务节点未完成境外同步。

#### 解决方法：

- 将验证文件部署在 HTTP 及 HTTPS 服务路径下，确认可以通过 HTTPS 协议访问。或者暂时关闭该站点所有页面的 HTTPS 服务。
- 确认通过 CA 机构中心指定的验证文件 URL 能够直接访问到正确的验证文件内容，并确认最终的验证文件不是通过重定向等方式显示在 Web 浏览器中。

#### 说明：

可通过浏览器地址是否发生变化来检测是否存在重定向。

- 将验证文件同步到境外 CDN 服务节点，或者临时关闭 CDN 境外加速服务。

#### 说明：

如果无法对 CDN 节点服务器进行变更操作，建议您改用 DNS 验证方式进行域名验证。

### DNS 配置错误

#### 问题原因

如果您在提交 SSL 证书审核时使用 DNS 验证方式进行域名验证，可能会因为此问题造成订单审核失败。该场

景下的 SSL 证书审核申请失败可能存在的部分原因如下：

- DNS 解析记录值配置错误。
- 使用部分域名解析服务商的服务时，因域名解析服务商对不存在的主机记录的查询返回值与预期的返回值不同，导致CA 机构中心验证返回值不准确。
- DNS 解析记录超时，您提交申请信息后。您将有三天时间完成 DNS 解析记录的添加，否则审核将会失败。
- 启用了动态域名解析服务，相应的 TXT 解析记录值未能及时同步到境外权威 DNS 服务器。

#### • 解决方法

- 配置正确的 DNS 主机记录及记录值。
- 忽略域名解析设置提示的相关错误，按要求配置 DNS 的解析记录，完成域名验证。
- 重新提交申请信息，并在3个自然日时间内完成 DNS 解析记录的添加。
- 请确认动态解析服务正常，并确保境外的解析服务能够正常解析新增的 TXT 解析记录。

#### ❓ 说明：

修改已存在的 TXT 记录值时，解析记录值会根据 TTL 值决定生效时间，而新增 TXT 记录值则可以很快生效。因此建议您通过新增 TXT 记录值完成验证。待域名验证通过后，可删除相关的 TXT 解析记录信息。

### 单位的电话号码不能为空或不正确

当您申请 OV、EV 类型数字证书时，如果您未填写单位电话号码，将收到该审核失败信息。

#### • 问题原因

OV、EV 类型证书产品，单位电话号码为必填字段。当单位电话号码为空、或填写不符合规则时，需要重新填写。

#### • 解决方法

请填写能够及时联系到您的单位电话号码，以确保在 CA 机构中心进行组织信息验证时能够联系到您。

### CSR 文件已用于其他订单

#### • 问题原因

出于证书密钥安全考虑，在请求一个全新的订单时，不允许使用之前已使用过的 CSR 信息。

#### • 解决方法

如果之前已使用一个 CSR 文件成功提交过订单，在后续的新订单中，请重新生成新的 CSR 文件。确保每张 SSL 证书都有其唯一的密钥对，有助于提升证书应用中的安全性。

### 证书绑定的域名格式不正确

#### • 问题原因

合法的域名仅允许包含字母+数字+“-”的任意组合，且域名的最大长度不得超过64个字符。

#### • 解决方法

请检查 CSR 请求文件及订单中填写的域名信息，确保您使用了正确的域名提交订单。

## 主域名不能为空

### • 问题原因

创建 CSR 文件时未正确填写 Common Name 字段。

#### 🔍 说明：

Common Name 必须是绑定域名中的其中一个域名。

### • 解决方法

建议您使用系统提供的在线生成 CSR 文件功能。

## 域名安全审核失败

当您申请 SSL 证书时，您可能收到以下审核返回结果，如下图所示：

### 温馨提示



抱歉，该域名未通过CA机构安全审查，无法申请域名型证书。请 [购买企业型或增强型证书](#)，您也可尝试使用其他域名申请证书。 [查看安全审核详情](#)

重新申请

取消

### • 问题原因

由于 CA 机构的反钓鱼机制，一般是域名信息中包含敏感词，例如 bank、pay 等，会引起安全审查失败，具体敏感词由 CA 机构定义，同时部分不常用的根域名也可能会审核失败，例如，www.qq.pw、www.qcloud.pw 等以 .pw 根域名后缀的无法通过审核。

### • 解决方法

建议更换域名中的主机名部分，重新尝试提交订单。如果多次更换主机名，仍提示以上错误，则建议选择收费证书产品，或选择更换主域名申请证书。

#### 🔍 说明：

域名型 SSL 证书通过自动认证快速颁发，不会人工介入审核，会用较为严格的敏感词来加强审核标准。

# 已购 SSL 证书提交申请审核后需要做什么？

最近更新时间：2020-12-15 17:10:28

## 已购证书提交申请审核后需要做什么？

您购买 SSL 证书后需申请证书并提交审核，审核通过后才能使用该证书并将证书部署到您的云服务资源上。

当您购买的是付费型证书时，提交审核后，CA 机构工作人员会联系您确认证书审核的相关信息。请您随时保持手机畅通（提交审核时填写的手机号码），并及时查看您的邮箱（提交审核时填写的邮箱），以免错过 CA 机构发送的确认通知。

当您的证书订单提交审核后，您可以登录 [证书管理控制台](#)，在证书列表中查看您证书审核申请的状态和后续流程。您的证书订单提交审核后，包含以下两种状态：

- **待验证**：证书申请为待验证的状态时，请您单击【详情】，进入证书详情页面查看域名验证方式，完成验证后，等待证书状态为【已颁发】才能使用该证书。

### 说明：

有关域名验证方式请参考 [域名验证指引](#)。

- **审核失败**：证书审核失败时，请您单击【详情】，进入证书详情页面确认证书审核失败的原因，并根据失败原因修改证书申请信息，修改完成后您需要重新提交申请。

## 不同证书类型颁发时长为多长时间？

- **OV、EV 类型证书审核时长**：OV 型证书颁发等待时间为 3 - 5 个工作日，EV 型证书颁发等待时间为 5 - 7 个工作日。
- **DV 型或免费型证书审核时长**：DV 型证书颁发等待时间为 10 分钟 - 24 小时。

### 说明：

免费型证书申请后会在 1 个自然日内颁发。由于 CA 机构中心审核流程耗时不同，您的证书有可能会在几个小时内就完成颁发，也有可能需要 1 个自然日才能完成颁发，请您耐心等待。

# 域名未通过安全审核该怎么办？

最近更新时间：2020-07-28 18:33:54

## 域名未通过安全审核该怎么办？

申请免费 DV 型数字证书的订单审核失败并收到以下提示：

该域名未通过 CA 机构安全审核，无法申请域名型证书。请购买企业型或增强型证书，您也可尝试使用其他域名申请证书。

- **问题原因**

域名中包含敏感词汇。

- **解决方案**

- 通过购买收费型数字证书绑定您的域名。
- 使用该免费证书后，绑定其它不包含敏感词的域名。



# 如何查看域名型（DV）SSL 证书域名验证结果？

最近更新时间：2020-12-15 17:10:39

## 如何查看 DV 型证书域名验证结果？

在您提交证书申请后，CA 机构中心将对您的域名及所提交的信息进行审核。域名验证成功后，CA 机构中心才会对证书进行颁发，若您的证书一直未颁发，建议您根据以下内容检验域名验证结果。

### 说明：

腾讯云 SSL 证书服务提供的主机记录是全域名的，如果您的域名管理系统不支持全域名的主机记录，请去掉根域名的后缀部分。

## DNS 验证类型

1. 请登录您的域名服务器，执行 dig 命令查询域名 DNS 解析。
2. 执行 dig + 记录类型 + @119.29.29.29 命令指定使用 DNSPod 的 DNS 进行验证。

例如 dig txt cloud.tencent.com @119.29.29.29

```
[root@centos ~]# dig txt cloud.tencent.com @119.49.49.49
;<<>> DiG 9.11.4-P2-RedHat-9.11.4-9.P2.el7 <<>> txt cloud.tencent.com @119.49.49.49
;; global options: +cmd
;; connection timed out; no servers could be reached
[root@centos ~]# dig txt cloud.tencent.com @119.29.29.29
;<<>> DiG 9.11.4-P2-RedHat-9.11.4-9.P2.el7 <<>> txt cloud.tencent.com @119.29.29.29
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 6986
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cloud.tencent.com.          IN      TXT

;; ANSWER SECTION:
cloud.tencent.com.         120     IN      TXT     "201703142045[REDACTED]iyy9pvmr2uykauiw4mh17"

;; Query time: 140 msec
;; SERVER: 119.29.29.29#53(119.29.29.29)
;; WHEN: Thu Jul 16 14:32:13 CST 2020
;; MSG SIZE rcvd: 123
```

- 如果返回结果中存在类似图示中的 TXT 记录，且记录值与证书控制台中证书详情页面中的记录值一致，表示您的 DNS 配置正确且已生效。
- 如果返回结果中不存在 TXT 记录，可能是 DNS 解析配置有误或者配置未生效。  
若 DNS 解析配置错误，请登录 [证书管理控制台](#)，单击【待验证】页签，进入该证书的详情页面。将证书详情中的记录值复制，并在您的 DNS 域名解析服务商更新解析。如果配置长时间未生效，请联系您的域名托管商。

问，如果浏览器提示“证书不可信”或者显示的内容不正确，请您暂时关闭该域名的 HTTPS 服务。

- 确保证 URL 地址在任何一个地方都能正确访问。由于每个品牌证书的检测服务器区域不同，请确认您的站点是否有国外镜像，或者是否使用了智能 DNS 服务等。
- 文件验证需要直接响应200状态码和文件内容，不支持任何形式的跳转。检查该验证 URL 地址是否存在301或302跳转。如存在此类重定向跳转，请取消相关设置关闭跳转。

 说明：

您可执行 `wget -S URL 地址` 命令检测该验证 URL 地址是否存在跳转。

# SSL 证书生效相关

## 电脑或手机中的浏览器提示 SSL 证书不可信怎么办？

最近更新时间：2020-07-28 18:34:10

### 电脑或手机中的浏览器提示证书不可信怎么办？

本文提供两种排查方法，以下是详细内容。

#### 方法1：排查终端类型

如果电脑浏览器或手机浏览器提示证书不可信的情况，请确认您所购买的 SSL 证书品牌和提示证书不可信的终端类型。部分品牌的数字证书在某些终端上是不被支持的，具体请参考 [浏览器兼容性测试报告](#)。

#### 方法2：排查证书的配置与部署

若 SSL 证书与终端兼容，请您使用检查工具 [亚洲诚信 SSL 状态检测](#) 数字证书。

- 如果检查结果中的证书品牌、证书类型以及域名与您购买的证书配置不一致，请您确认在服务器安装的 SSL 证书信息是否正确。
- 如果检查结果显示证书链信息不完整，请您确认在服务器安装的 SSL 证书信息是否正确。

#### 🔍 说明：

- 检查服务器站点的网页是否引用了 HTTP 资源。在部分浏览器中，HTTPS 站点引用 HTTP 资源会被视为不安全操作。
- 如果一个域名被解析到多台服务器中，请确认每台服务器都已正确部署证书。

---

# 服务器 IP 地址更换后原来的 SSL 证书能否生效？

最近更新时间：2020-07-28 18:34:15

## 服务器 IP 地址更换后原来的 SSL 证书能否生效？

如果您的 SSL 证书是绑定域名的，则不受服务器更换 IP 地址的影响。

证书绑定的域名不变，可以重新解析到新的 IP 地址，原来的 SSL 证书仍然可以生效，不需要更换新的证书。

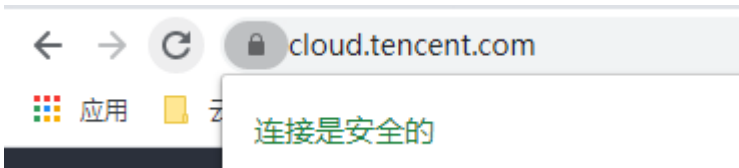
# 如何在浏览器中检查 SSL 证书是否生效？

最近更新时间：2020-07-28 18:34:21

## 如何在浏览器中检查 SSL 证书是否生效？

证书安装成功并解析至服务器 IP 后，您可以按照以下步骤检查 SSL 证书生效情况：

1. 打开浏览器（本文以 Chrome 浏览器为例），在浏览器地址栏中以 https 格式输入 SSL 证书绑定的域名地址。
2. 按回车键，访问域名地址。检查是否具备以下情况：
  - 域名地址可以成功访问网站。
  - 浏览器地址栏左侧显示安全锁标志，则说明您的 SSL 数字证书已生效。如下图所示：



# GlobalSign 证书 Windows 7 系统下不受信任怎么办？

最近更新时间：2020-09-29 17:49:29

## 背景

2019年5月27日，GlobalSign 正式使用新的中级 CA 为 SSL 证书产品签名。因 Windows 7 系统中没有新根支持，致使 Windows 7 系统访问2019年5月27日之后签发（包括更新或者重颁发的证书）的 GlobalSign 证书时，网站不受信任。详情可查看：[关于 GlobalSign 迁移签发 SSL 证书的中级 CA 的通知](#)。

## 解决办法

请使用文本编辑器，打开已下载证书中 Nginx 目录下的 .crt 文件，将以下交叉证书复制粘贴放置于证书链最后位置。重启 Nginx 服务，证书即可正常使用。

交叉证书下载请 [单击此处](#)。

# SSL 证书收费和购买相关

## 域名型（DV）SSL 证书是否永久免费？

最近更新时间：2020-09-21 16:32:10

### 域名型证书是否永久免费？

首先，SSL 证书无论是免费的域名型或者是付费的企业型，CA 机构都规定了有效期的，从安全性上考虑，不能保证一个合法网站永远不会成为一个钓鱼站点，CA 机构需要定期审核，所以不会颁发永久有效的证书。

其次，当网站的私钥丢失时可以申请吊销，CA 机构会将吊销的证书加入证书吊销列表（Certificate Revocation List，简称：CRL），每次 HTTPS 站点被访问时，浏览器会向 CA 机构获取 CRL，判断是否能信任该证书；然而永久有效的证书会导致 CRL 不断增加，不会减少，会增加浏览器的请求流量压力，所以指定证书的有效期限是更科学的处理方式。

腾讯云目前提供免费的域名型证书，型号为 **TrustAsia DV SSL CA - G5**，证书有效期时长**1年**。证书过期前**一个月**即可重新申请，域名型证书能在一个工作日内快速颁发，您有充足的时间为站点切换证书。

# SSL 证书有效期相关

## SSL 证书过期了怎么办？

最近更新时间：2020-11-09 10:59:42

### SSL 证书过期了怎么办？

SSL 证书过期之后将无法继续使用，您需要在证书到期前及时续费，并重新绑定域名和提交审核。

审核通过后，您将获得一张新的证书，您需要在服务器上重新安装新的证书替换即将过期的证书。

#### 🔍 说明：

- 如果您使用的是免费域名型（DV）证书需重新申请。详细信息请参见 [域名型（DV）证书申请流程](#)。
- 证书到期前您需预留3 - 10个工作日进行重新购买，避免因证书过期导致证书审核未通过。详细信息请参见 [付费型 SSL 证书续费流程](#)。



# SSL 证书过期后未及时更新有哪些影响？

最近更新时间：2020-07-28 18:34:37

## SSL 证书过期后未及时更新有那些影响？

如果SSL证书过期，没有及时更新证书，可能会产生如下影响：

- 用户访问网站时，浏览器会提示网站的安全证书已过期的告警信息。
- 用户收到上述告警信息后，可能对该网站失去信任，甚至选择停止访问该网站，对企业的品牌形象、用户量等有不不利影响。
- 黑客等不法分子可能会利用过期的 SSL 证书，篡改或窃取浏览器和服务器之间传输的信息和数据，从而影响用户的数据安全。
- 证书到期导致的业务意外中断，无法正常运营，导致资金损失。
- 损害网站的 SEO 排名等。

# 查看 SSL 证书到期相关问题

最近更新时间：2020-09-21 16:33:48

## 如何收到 SSL 证书到期的系统通知？

证书到期前，您可在 [腾讯云 SSL 证书控制台](#) 的证书信息状态列查看证书到期的相关信息。

您也可以通过消息订阅来设置接收证书相关的系统消息通知。

### ② 说明：

如未设置消息订阅，您将不会收到证书到期的站内信、邮箱或手机短信通知。

**证书到期提醒时间：**证书到期前30天开启到期提醒。

## 如何设置接收证书相关的系统消息通知？

1. 请您登录 [消息中心控制台](#)。
2. 在【消息订阅】管理页面，您可在【产品消息】>【SSL 证书相关通知】勾选您需要的通知类型。

具体操作也可参考：[消息订阅管理](#)。

---

# SSL 证书成功续费后可以继续服务吗？

最近更新时间：2020-07-28 18:34:50

## 证书成功续费后可以继续服务吗？

不能。证书续费后，您需要重新提交证书申请审核并等待新证书颁发后重新部署到您的云服务资源上。

# SSL 证书域名相关 域名验证提供哪几种方式？

最近更新时间：2021-02-26 09:36:46

## 域名验证提供哪几种方式？

腾讯云 SSL 证书提供以下五种域名验证方式：

- 自动添加 DNS
- DNS 验证
- 文件验证
- 自动 DNS 验证
- 自动文件验证

详细操作请查看：[域名验证指引](#)。