# SSL 证书

# 操作指南

# 产品文档

腾讯云

# 文档目录

操作指南
域名验证指引
上传 SSL 证书
安全签章指引

# 操作指南
# 域名验证指引

最近更新时间：2024-03-06 17:31:47

## 操作场景

本文档指导您在申请域名型证书后，验证域名的所有权。

**注意：**

请尽快添加验证，若您在3天内未添加验证或验证不通过，审核机构将拒绝您此次证书申请。

验证通过后可以在 证书管理 下载并安装相关的证书。

域名的所有权可通过以下方式进行验证：

| 验证方式 | 使用场景 |
| --- | --- |
| 手动 DNS 验证 | 适用于在任何平台进行解析的域名。 |
| 文件验证 | 使用自动 DNS 验证和手动 DNS 验证存在限制的情况下。（操作过程比较复杂，需要一定的建站基础） |

## 前提条件

通过 手动 DNS 验证 方式验证，须完成域名型证书的申请。

通过 文件验证 方式验证，须获取登录服务器的帐号和密码。

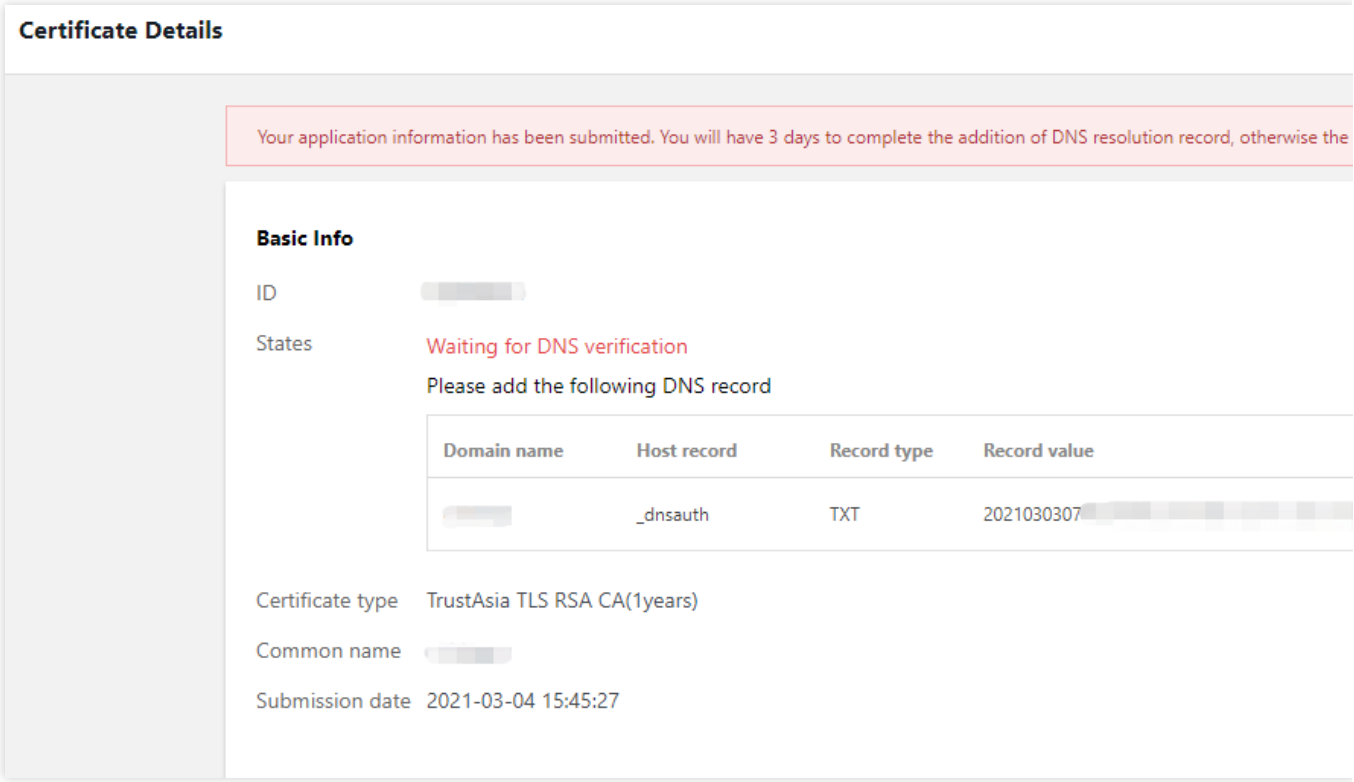
## 操作步骤

### 手动 DNS 验证

**注意：**

以下操作仅针对域名对应的**域名解析商**在腾讯云 DNSPod DNS 解析的情况下，若不在腾讯云 DNSPod DNS 解析，请您到域名对应的**域名解析商**处进行解析。

1. 登录 SSL 证书管理控制台。
2. 在**证书列表**页面，选择待查看证书详情的域名型证书 ID，进入**证书详情**页面。如下图所示：




3. 添加解析记录。

若您的域名（例如 `www.tencent.com`）对应的**域名解析商**在腾讯云 DNSPod DNS 解析。

3.1.1 请您先找到 证书详情 页面，获取主机记录以及记录值。

3.1.2 登录 DNS 解析控制台，查看已申请证书的域名，并单击操作栏的**解析**，进入**记录管理**页面。

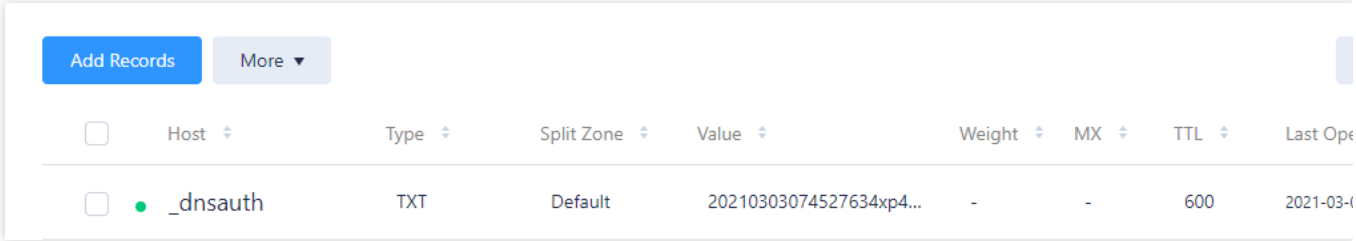
3.1.3 单击**添加记录**，添加记录类型。

若您的域名对应的**域名解析商**不在腾讯云，请您先找到 证书详情 页面，获取主机记录以及记录值，并到域名对应的**域名解析商**处添加解析记录。

4. 添加成功后，证书对应域名添加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。如下图所示：

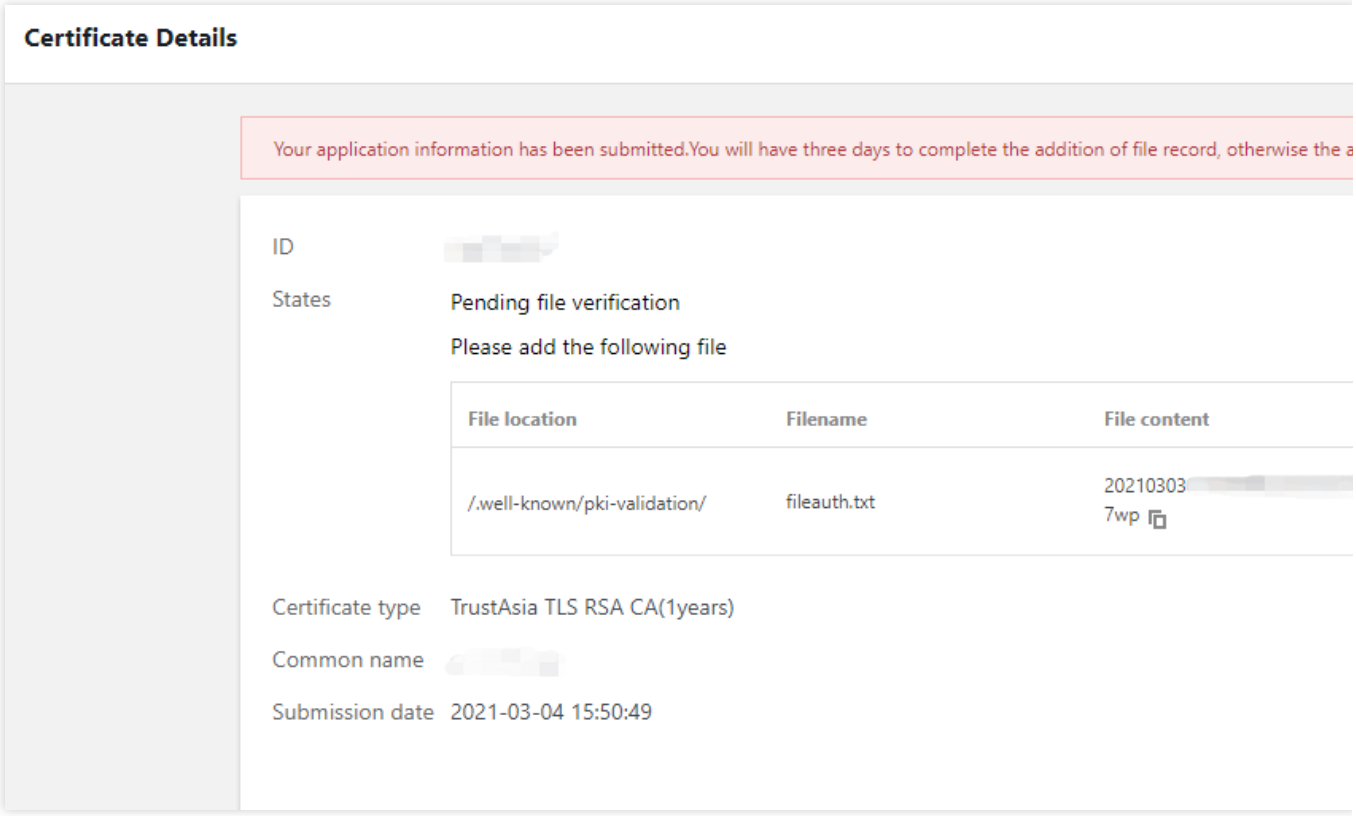
**说明：**

解析生效时间一般为**10分钟 - 24小时**，但各地解析的最终生效取决于各运营商刷新时间，请您耐心等待。




## 文件验证

1. 登录 SSL 证书管理控制台。
2. 在**证书列表**页面，选择待查看证书详情的域名型证书 ID，进入**证书详情**页面。如下图所示：




3. 请您登录服务器，并且确保域名已指向该服务器。

**说明：**

若您的域名对应的**域名解析商**在腾讯云 DNSPod DNS 解析，将域名指向您的服务器。

4. 在网站根目录下，创建指定的文件。该文件包括文件目录、文件名、文件内容。

**说明：**

网站根目录是指您在服务器上存放网站程序的文件夹，大致这几种表示名称：wwwroot、htdocs、public_html、webroot 等。文件名名称与文件内容请根据购买证书后域名验证详情页提示，确定文件名名称与文件内容。

**示例**

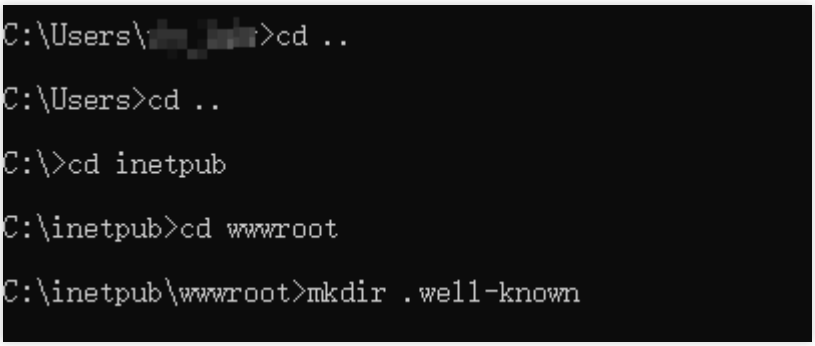
您的网站根目录为 `C:/inetpub/wwwroot`，您可以在 `wwwroot` 文件夹下创建一个如下表所示的文件：

| 文件目录 | 文件名 | 文件内容 |
| --- | --- | --- |
| /.well-known/pki-validation | fileauth.txt | 2019080603.....ep939jlu32alzeo |

**注意事项**

Windows 系统下，需通过执行命令行的方式创建以点开头的文件和文件夹。

例如，创建 `.well-known` 文件夹，请打开命令提示符，执行命令 `mkdir .well-known` 进行创建。如下图所示：




5. 打开浏览器，根据验证的域名类型，访问对应的链接地址。

**链接地址格式**：`http://域名/文件目录/文件名` 或者 `https://域名/文件目录/文件名`。

访问链接可获取到文件内容，例如 `2019080603......ep939jlu32alzeo`。

如果申请文件验证的域名是 `example.tencent.com`，进行验证访问的链接地址则是 `http://example.tencent.com/.well-known/pki-validation/fileauth.txt` 或者是 `https://example.tencent.com/.well-known/pki-validation/fileauth.txt`。

**说明：**

对于 www 开头的二级域名，例如 `www.tencent.com`，您需进行以下两步操作：

第一步对该二级域名添加 文件验证。

第二步对其主域名 `tencent.com` 添加 文件验证（不需要重新申请证书），验证方法按照**链接地址格式**进行验证，验证值显示一致。

如果申请文件验证的域名是泛域名 `*.tencent.com`，进行验证访问的链接地址是 `http://tencent.com/.well-known/pki-validation/fileauth.txt` 或者 `https://tencent.com/.well-known/pki-validation/fileauth.txt`。

**说明：**

支持 HTTP 和 HTTPS，任意一个均可访问。

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。

6. 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。

**说明：**

操作过程如果出现问题，请您 联系我们。

# 上传 SSL 证书

最近更新时间：2024-03-06 17:31:49

## 操作场景

若您需要将所有证书进行统一管理，您可以通过上传证书的方式，将您其他的证书进行上传管理。本文档将指导您如何上传证书。

**说明：**

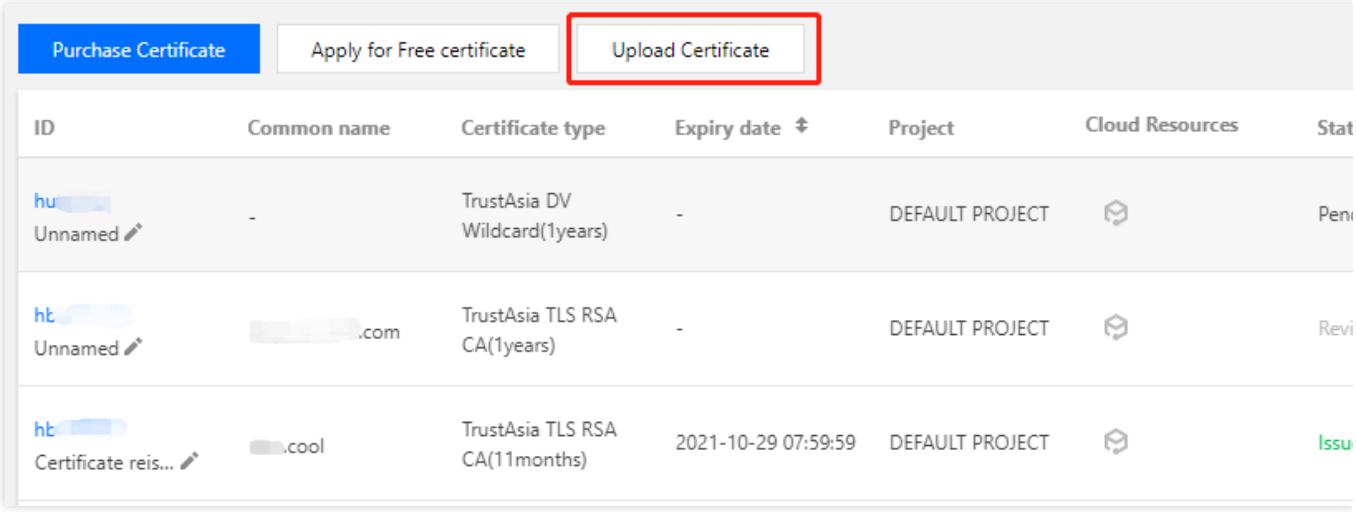
上传功能暂不支持国密标准（SM2）证书。

## 前提条件

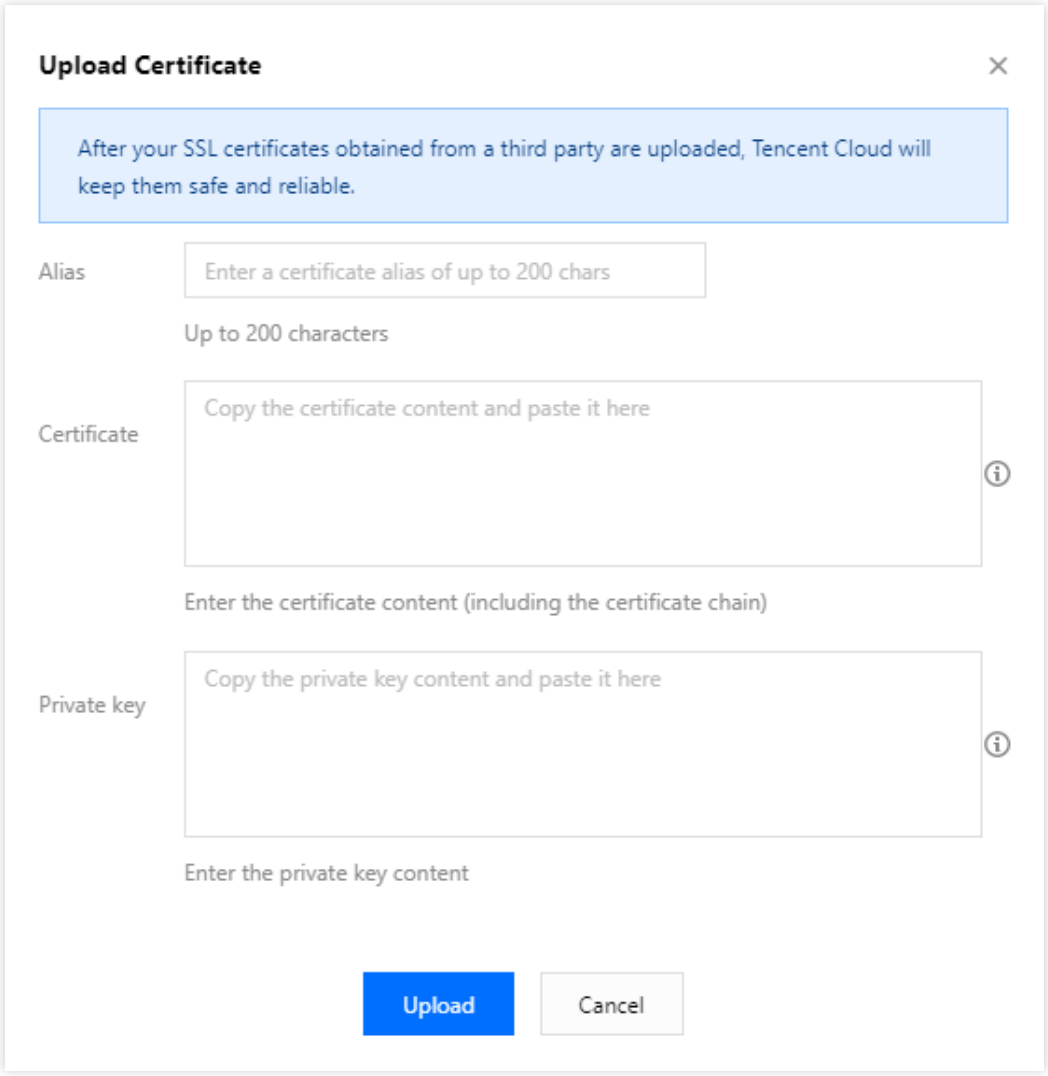
已登录 SSL 证书管理控制台。

## 操作步骤

1. 选择**我的证书**，单击**上传证书**。如下图所示：




2. 在弹出的**上传证书**的窗口中，根据要求填写相关内容。如下图所示：




**备注名**：请输入证书备注名。

**证书**：

通常证书是以 .crt 或 .pem 等为扩展名的文件，请使用相应文本编辑器打开证书文件并拷贝至证书对应的文本框中。

证书格式以 “-----BEGIN CERTIFICATE-----” 开头，以 “-----END CERTIFICATE-----” 结尾。

证书内容请包含完整的证书链。

**私钥**：

通常私钥是以 .key 或 .pem 等为扩展名的文件，请使用相应文本编辑器打开私钥文件并拷贝至私钥对应的文本框中。

私钥格式以 “-----BEGIN (RSA) PRIVATE KEY-----” 开头，以 “-----END (RSA) PRIVATE KEY-----” 结尾。

3. 单击**上传**，即可将证书上传至证书列表。

# 后续步骤

您可以将已上传托管的证书部署至云服务。

# 安全签章指引

最近更新时间：2024-03-06 17:31:47

## 什么是安全认证签章？

诺顿安全认证签章是由 SecureSite SSL 证书提供、互联网上最受认可的信任标记。由 SecureSite 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。
可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会在搜索结果中的可信网站链接旁显示诺顿安全认证签章。
SecureSite 强大的 PKI 基础架构包括金融级数据中心和灾难恢复站点，可以为客户数据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，由于电子商务站点必须验证其身份并且此签章是加密通过其站点的交易通信，从而可以保护客户数据。