SSL 证书

产品公告

产品文档

腾讯云

【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

产品公告
SSL 证书域名验证策略变更通知

最近更新时间：2021-06-17 16:28:50

根据 CA/Browser Forum 规定，自**2021年12月01日**起域名验证策略将会有以下重大变更：

自2021年12月01日起，使用文件验证的域名，只能为当前被验证的域名签发 SSL 证书，不支持签发通配符 SSL 证书和其下级子域名 SSL 证书。

目前，腾讯云 SSL 证书允许对主域名（例如 dnspod.cn ）进行域名验证即可，适用于通配符证书（例如 *.dnspod.cn 或 *.sub.dnspod.cn 等）和其下级所有子域名（例如 sub.dnspod.cn 或 sub2.sub1.dnspod.cn 等）。

但从2021年12月01日起，对于使用文件验证方式的域名，只能为当前被验证的域名签发证书。例如，使用文件验证方式验证域名 dnspod.cn，则只能为 dnspod.cn 域名签发证书，不能为域名 *.dnspod.cn 或 sub.dnspod.cn 签发证书。

云资源托管说明

最近更新时间：2021-05-18 12:45:53

云资源托管提供了您在 SSL 证书续费签发成功（或免费证书重新申请）后，不需要重新将证书部署至云资源上的服务，即自动将新 SSL 证书部署至原 SSL 证书已部署的腾讯云云资源，例如负载均衡、内容分发网络等。

新申请 SSL 证书签发后即可开启云资源托管并绑定相关云资源，当该 SSL 证书进行续费操作生成新证书时，原证书上的关联云资源将自动绑定到新证书上。

> ⚠ 注意：
>
> - 云资源托管不会自动将新证书安装至您的服务器 Web 应用。因此，即使您的 SSL 证书已开启云资源托管服务，您仍然需要在获得续费签发的新证书后，手动将新证书安装到您的 Web 服务中（替换原证书）。如您的 SSL 证书仅用于部署至腾讯云云资源，则可通过开启云资源托管，实现全程自动化。
> - 云资源托管服务为免费服务，您无需支付任何费用，即可使用该功能。

云资源托管优势

针对 SSL 证书部署至云资源的场景，当您首次完成将证书部署至云资源并开启云资源托管后，证书再次申请则无需您再次手动部署到云资源，该操作将由腾讯云自动完成。

使用限制

- 原证书开启云资源托管后，申请的 SSL 证书必须与原证书的规格完全相同（包含域名类型、证书类型以及证书品牌完全相同），才能保证托管后可以正常自动部署至云资源服务。
- 原证书开启云资源托管后，支持付费证书续费签发后的证书自动部署至云资源。
- 原证书开启云资源托管后，支持免费证书重新申请签发的证书自动部署至云资源。

SSL 证书与证书监控 SSLPod 联合说明

最近更新时间：2021-09-08 16:16:22

为了让您有更好的体验，现提供腾讯云证书管理控制台与证书监控 SSLPod 联合集成功能，可快速帮助您检查使用 SSL 证书时的证书健康问题。

> 说明：
> 当您遇到问题需要咨询时，您可以直接通过 在线客服 进行提问，腾讯云工程师7 × 24小时在线为您提供服务。

功能概述

模块	说明
卡片式证书管理	卡片式证书管理帮助您更清晰的管理 SSL 证书，拥有更好的交互体验。您只需在证书管理控制台中，通过快捷的方式即可在横栏式与卡片式进行快速切换。
SSL 证书与证书监控 SSLPod 联合集成	SSL 证书与证书监控 SSLPod 联合集成后，您可以在 SSL 证书详情页或卡片式证书详情页快速查看 SSL 证书状态与监控报告。

使用卡片式证书管理

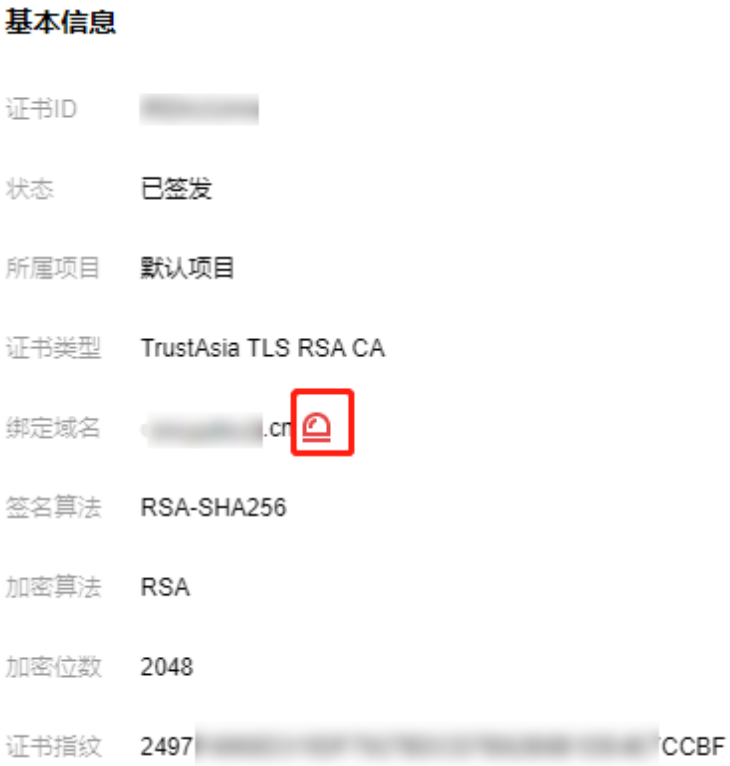
1. 登录 腾讯云证书管理控制台，单击左侧菜单栏的**我的证书**，即可进入 “证书列表” 管理页面。
2. 在 “证书列表” 管理页面中，单击 即可进行切换。如下图所示：

> 说明：
> 若您需切换横栏式证书管理，单击 图标即可进行切换。

SSL 证书与证书监控 SSLPod 联合集成

1. 登录 腾讯云证书管理控制台，单击左侧菜单栏的**我的证书**，即可进入 “证书列表” 管理页面。
2. 在 “证书列表” 管理页面中，单击 证书 ID，即可进入证书详情页。
3. 您可以通过以下两个方式查看证书监控状态：

- 证书详情页。



- 卡片式的证书详情页。

证书状态说明

图标	状态说明	操作
	目前该 SSL 证书状态异常	单击**查看监控报告**，即可跳转至健康报告页查看详情。
	该域名目前还开启未证书监控	单击**免费开通**，即可快速对该证书进行监控。
	目前该 SSL 证书状态良好	单击**查看监控报告**，即可跳转至健康报告页查看详情。

图标	状态说明	操作
	该域名正在使用其它证书	单击**查看监控报告**，即可跳转至健康报告页查看详情。

多年期 SSL 证书与自动审核更新说明

最近更新时间：2021-02-23 10:30:42

为了让您有更好的体验，腾讯云证书管理控制台 新增多年期证书购买和我的资料自动审核功能，可帮助您解决证书申请和续期需重新申请的问题。本文档将对多年期证书和我的资料自动审核功能进行简要说明。
如果在使用过程中有任何疑问、建议或意见，请 联系我们，感谢您的使用。

功能概述

> 说明：
> 具体操作以控制台显示为准。

模块	说明
我的资料	我的资料页可新增管理企业、管理人信息以及域名信息审核。包含以下功能： • **企业信息管理**：可在我的资料页下管理企业信息，如新增、修改、删除等操作。 • **域名信息管理**：可在我的资料页对应的企业信息下管理域名，如新增、修改、删除、验证域名所有权等操作。
多年期证书	您可以登录 腾讯云 SSL 证书购买页，购买特定品牌的多年期证书，腾讯云将在前一个证书有效期到期前为您签发下一张证书，解决 CA 机构减少证书有效期的困扰。

腾讯云 SSL 证书控制台更新说明

最近更新时间：2021-06-01 10:02:42

为了让您有更好的体验，腾讯云证书管理控制台 已全面升级，在原 SSL 证书控制台的基础上进行了合并与优化。新版控制台新增证书概览、操作记录、快速上手等功能模块，并与证书监控 SSLPod 协同使用，提供更全面更便捷的配置和管理。本文档将对新版 SSL 证书控制台的使用进行简要说明。
如果在使用过程中有任何疑问、建议或意见，请 联系我们，感谢您的使用。

> ⚠ 注意：
> SSL 新版控制台将采取逐步开放的形式同步更新，至**2020年12月15日前**将完成所有 SSL 新版控制台更新。

功能概述

模块	说明
证书概览	SSL 证书概览页可用于 SSL 证书申请状态与监控状态的查看与进行相关操作。包含以下功能： • 申请状态：可快速查看待提交、验证中、已签发、审核失败的 SSL 证书，并进行相关操作。 • 监控状态：可快速查看访问正常、访问异常、过期预警的 SSL 证书监控信息并查看对应的 SSLPod 监控报告。
我的证书	我的证书页面主要用于查看申请中、已签发、已过期的 SSL 证书查看与证书管理。包含但不限于以下功能： • 查看申请中、已签发、已过期的证书信息。 • 购买证书。 • 申请免费证书。 • 上传已有证书。 • 对证书进行相关管理，如提交申请资料，重颁发证书、续费等。
操作记录	操作记录主要用于对现有 SSL 证书的相关操作记录查看。包含以下功能： • 支持导出 CSV 与 JSON 格式的操作记录。 • 对操作记录进行相关条件筛选。
证书监控	主要用于 SSL 证书产品与监控 SSLPod 产品的协同使用，提供更便捷的管理与使用。

腾讯云即日起支持 DNSPod 品牌国密标准（SM2）SSL 证书购买通知

最近更新时间：2021-08-02 16:48:05

国密是国家商用密码的简称，是国家密码局认定的国产密码算法。而国产密码算法是保障我国网络安全自主可控的重要基础，腾讯云 DNSPod 品牌国密标准（SM2）证书支持 SM2 国产密码算法和国密安全协议，可以实现高强度 SSL 加密连接及服务器身份认证，适合对国密合规性有要求的网站。更多详情请查看：国密证书介绍。

腾讯云 DNSPod 品牌国密标准（SM2）证书

- **域名型（DV）**：域名型加密 SSL 证书，支持在国密浏览器中显示安全锁。对域名所有权进行验证，满足绑定多域名和泛域名的需求，快速颁发，经济实惠，保护网站数据安全，适合个人，中小企业应用。
- **企业型（OV）**：企业级加密 SSL 证书，支持在国密浏览器中显示安全锁及单位名称。对申请公司单位做严格的身份审核验证，保护内外部网络上敏感数据传输，是中小型企业应用、电商等服务的最佳选择。
- **增强型（EV）**：增强型加密 SSL 证书，支持在国密浏览器中直观显示绿色地址栏及单位名称。对申请者做最严格的身份审核验证，信任等级最高，适合大型企业、金融等机构平台。

购买流程

请您登录腾讯云账号，并进入 SSL 证书购买页 进行购买。

关于 CA 机构于2020年9月1日起停止签发为期两年 SSL 证书的通知

最近更新时间：2021-08-03 16:13:29

由于苹果和谷歌根存储政策的更改，自2020年9月1日起，政策禁止使用有效期超过13个月（397天）新颁发的SSL/TLS 证书。因此，自2020年9月1日起，全球 CA 认证机构不再签发2年期 SSL 证书，腾讯云将于2020年8月25日关闭2年期证书购买服务，如有2年期证书购买需求，请于服务下线前完成申请签发。

常见问题的问题如下：

这次政策更改带来了什么变化?

由于苹果和谷歌根存储政策的变化，自2020年9月1号开始，所有新的 SSL/TLS 证书的最长有效期不得超过13个月。

此变更何时生效?

2020年9月1号。

我刚刚购买了有效期为2年的 SSL 证书，2020年9月1号之后会被信任吗?

在2020年9月1号之前颁发且有效期大于397天的 SSL 证书将继续受到信任，使用不受影响。

更改生效后，重颁发现有的2年期证书会怎么样?

如果您在9月1号之后重颁发现有的2年期证书，我们需要把重颁发出来的新证书有效期限制为397天。

> 说明：
>
> - 感谢您对腾讯云的支持，我们将一如既往给您提供 HTTPS 专业服务！
> - 如您使用过程中遇到产品相关问题，您可咨询 在线咨询 寻求帮助。

关于 Symantec SSL 证书品牌名于2020年4月30日停止使用的通知

最近更新时间：2021-08-03 16:12:25

接原厂通知，Symantec SSL 证书品牌名将于2020年4月30日停止使用，您可以理解为该日期是 Symantec 品牌用于 SSL 证书的最后一天。

本次更新点

1. Symantec 品牌 SSL 证书更名为 DigiCert Secure Site 品牌 SSL 证书。如下图所示：

变更前LOGO　　变更后LOGO

2. 诺顿安全认证签章同步进行了更新。如下图所示：

旧 版

新 版

⚠ 注意：

- 此次更名对于证书交付和使用流程没有任何影响。
- 更名后，原有的产品功能和服务保持不变的基础上，Secure Site 品牌新增 Pro 版本支持抗量子算法功能。

原厂公告

以下是原厂公告：

Greetings APAC partners,

As part of the migration the Symantec logo cannot be used after 30 April 2020. However, the phrase DigiCert (formerly Symantec) or similar can be used in marketing collaterals and to an extent on product descriptions. Please keep in mind not to over-use the wording and ensure that it is not heavily emphasised.

If there's any further questions on this please email me directly.

Please stay safe during this period.

Regards,

Albert Cheng
Channel Marketing Manager, APAC
O +61 0 8866 8043 | M +61 423 585 290

digicert®

说明：

- 感谢您对腾讯云的支持，我们将一如既往给您提供 HTTPS 专业服务！
- 如您使用过程中遇到产品相关问题，您可咨询 在线咨询 寻求帮助。

关于私钥泄露导致被厂商吊销 SSL 证书的情况说明

最近更新时间：2021-07-22 16:04:31

接 DigiCert 机构通知，DigiCert 于今年4月底上线了私钥泄露检测系统，该系统会在 GitHub、SourceForge 等项目代码托管平台进行自动检测，检测到私钥泄露后机构会通知用户并在24小时后进行证书吊销操作。
为了保护您的网站及信息安全，请于申请完证书后妥善保管您的私钥。请勿将私钥上传至公网，以免出现证书被吊销或发生信息泄露等事件。

> 说明：
>
> - 感谢您对腾讯云的支持，我们将一如既往给您提供 HTTPS 专业服务！
> - 如您使用过程中遇到产品相关问题，您可咨询 在线咨询 寻求帮助。

关于免费域名型（DV）SSL 证书的申请额度限制通知

最近更新时间：2021-07-22 16:02:34

由于 CA 机构和证书代理商策略调整，自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（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）。之前已颁发的证书在有效期内使用不受影响。若您的业务因此次调整受限，建议您购买泛域名型 SSL 证书。

注意：

- 1个腾讯云 UIN 账户最多只能申请50张免费证书，证书签发后15个月内计算相关额度。
- 即将到期的证书需要在2018年1月1日以后重新申请时，会受到上述策略的限制。
- 感谢您对腾讯云的支持，我们将一如既往给您提供 HTTPS 专业服务！
- 如您使用过程中遇到产品相关问题，您可使用 在线咨询 寻求帮助。