SSL 证书

证书管理

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 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】

腾讯云

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或95716。

文档目录

证书管理
- SSL 证书托管指引
- 上传 SSL 证书指引
- 上传 SSL 证书自动托管指引
- SSL 证书自动续费指引
- SSL 证书催审指引
- SSL 证书吊销指引
- SSL 证书删除指引
- SSL 证书重颁发指引
- SSL 证书消息忽略指引
- SSL 证书自定义过期告警
- SSL 证书消息通知设置
- 腾讯云证书权益点包管理

版权所有：腾讯云计算（北京）有限责任公司

证书管理
SSL 证书托管指引

最近更新时间：2023-08-11 14:29:51

概述

SSL 证书默认有效期为1年，您必须在证书到期前的30个自然日内续费并更新证书。**腾讯云证书托管服务**在检测到续费的新证书（或指定证书）后，可以帮助您自动更新证书（自动将新证书部署到旧证书关联的腾讯云云产品），无需您再手动替换，节省您的证书维护时间。

> **注意**
> - 在腾讯云申请的免费证书或购买的正式证书可以支持托管；
> - **如果旧证书没有关联云资源可不使用托管功能；**
> - 如果您的 SSL 证书仅用于部署至腾讯云云资源，开启云资源托管，可实现新证书自动更新到云资源；如果您的证书**用在非腾讯云云资源**，即使您的 SSL 证书已开启证书托管服务，仍然需要手动将新证书安装到您的 Web 服务中（替换原证书）。

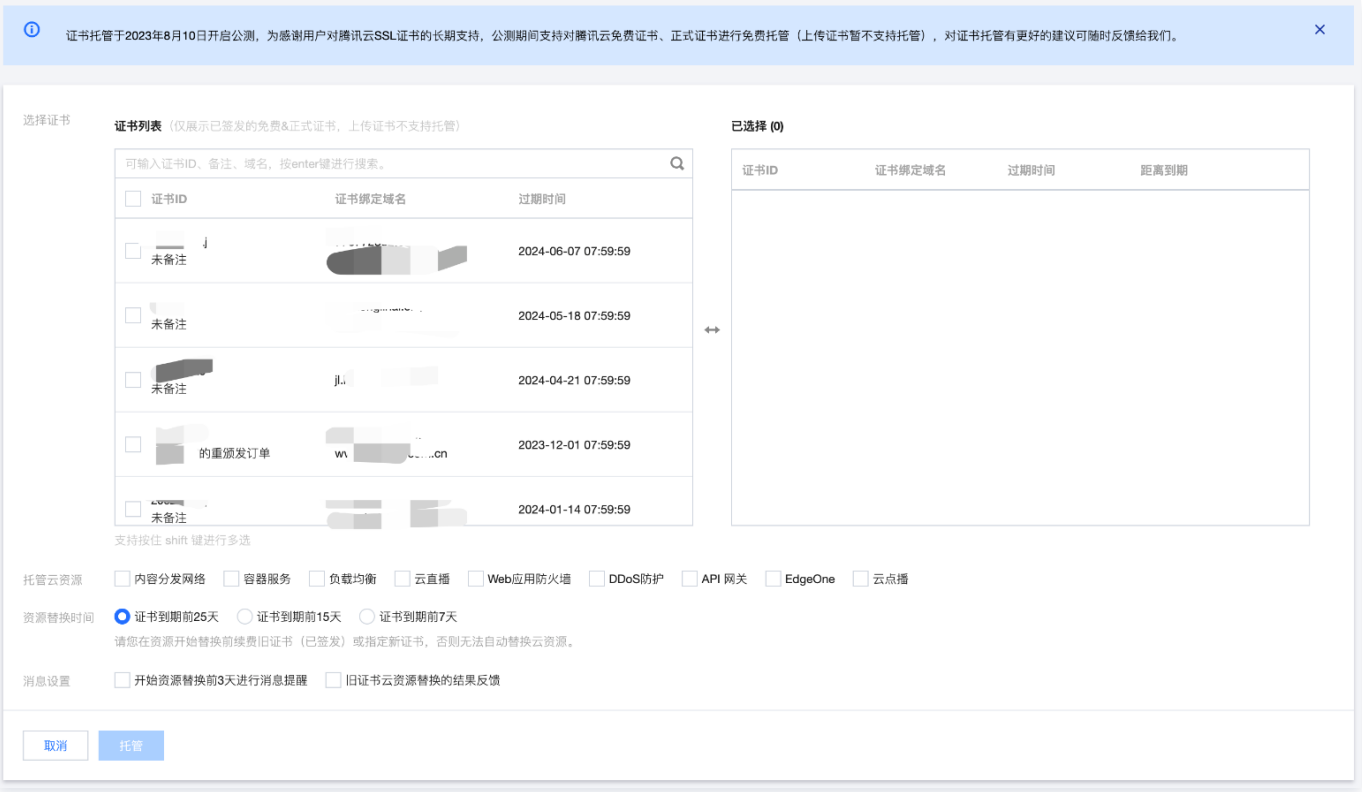
优势

- SSL 证书**开启自动续费 + 证书托管**，即可实现自动化管理证书（OV/EV 证书还需要额外的组织信息认证）。
- 除了续费的证书，还可手动指定任意证书，在旧证书到期前可进行自动替换部署到云资源。

操作指南

1. 登录腾讯云 SSL 证书管理控制台，进入 证书托管 页面。

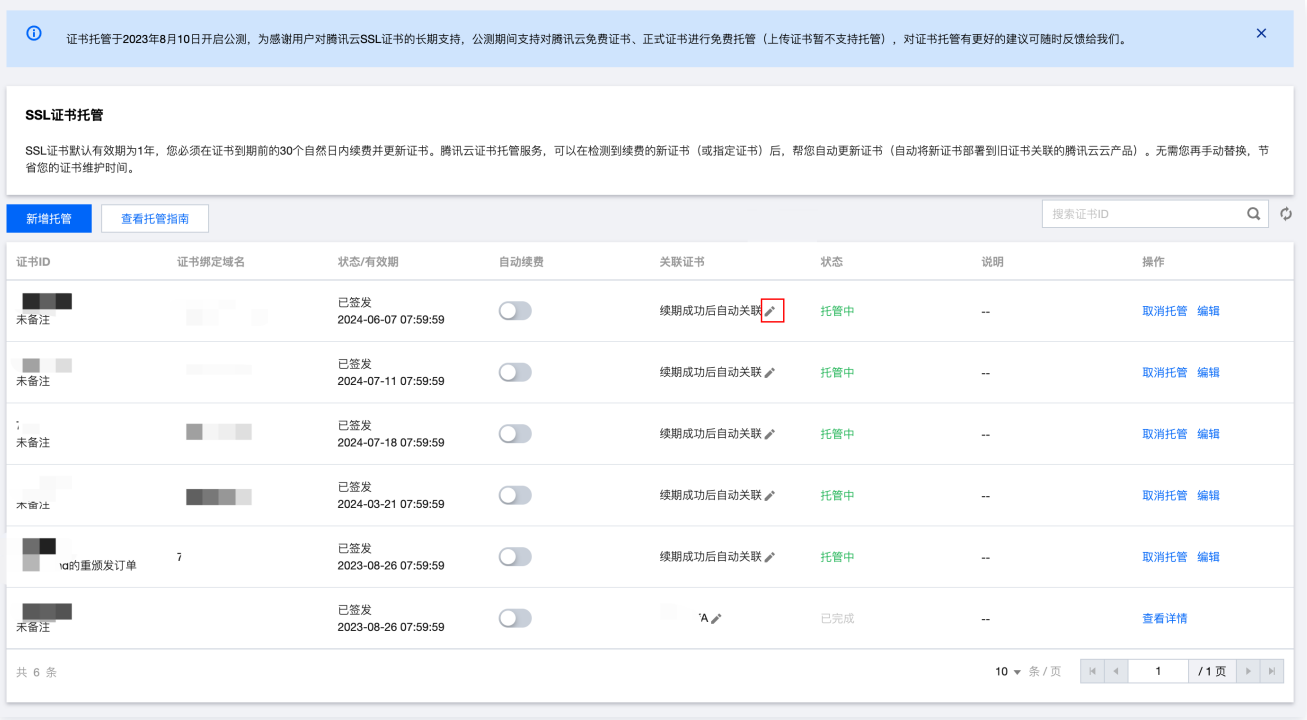
2. 单击**新增托管**，选择需要托管的证书，勾选托管的云资源类型。



- 选择证书：选择需要托管的证书；
- 托管云资源：旧证书到期前会将续费的新证书（或指定的证书）在预设的云资源上替换旧证书。如原证书没有关联云资源可不使用托管功能；
- 资源替换时间：设置自动替换新证书的时间（请务必保证新证书在资源替换前已完成签发，否则将托管失败），**旧证书的有效期不能少于资源替换的时间**（例如证书还有7天到期，则无法设置到期前25天替换云资源）；
- 消息设置：会通过邮件/站内信/短信三个渠道，告知您托管的相关信息（建议开启，如果证书较多可手动在设置中关闭）。

3. 选择关联的证书。

3.1 证书托管默认使用自动续费的 SSL 证书，如果新证书是通过重新购买，可单击“关联证书”列中的 指定新证书。



3.2 在弹出的窗口，指定新购买的证书，单击**保存**即可。

警告：

指定证书请务必保证新旧证书绑定的域名一致。如果新旧证书域名不一致，替换云资源后有可能直接影响业务。

上传 SSL 证书指引

最近更新时间：2024-11-27 17:28:52

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。

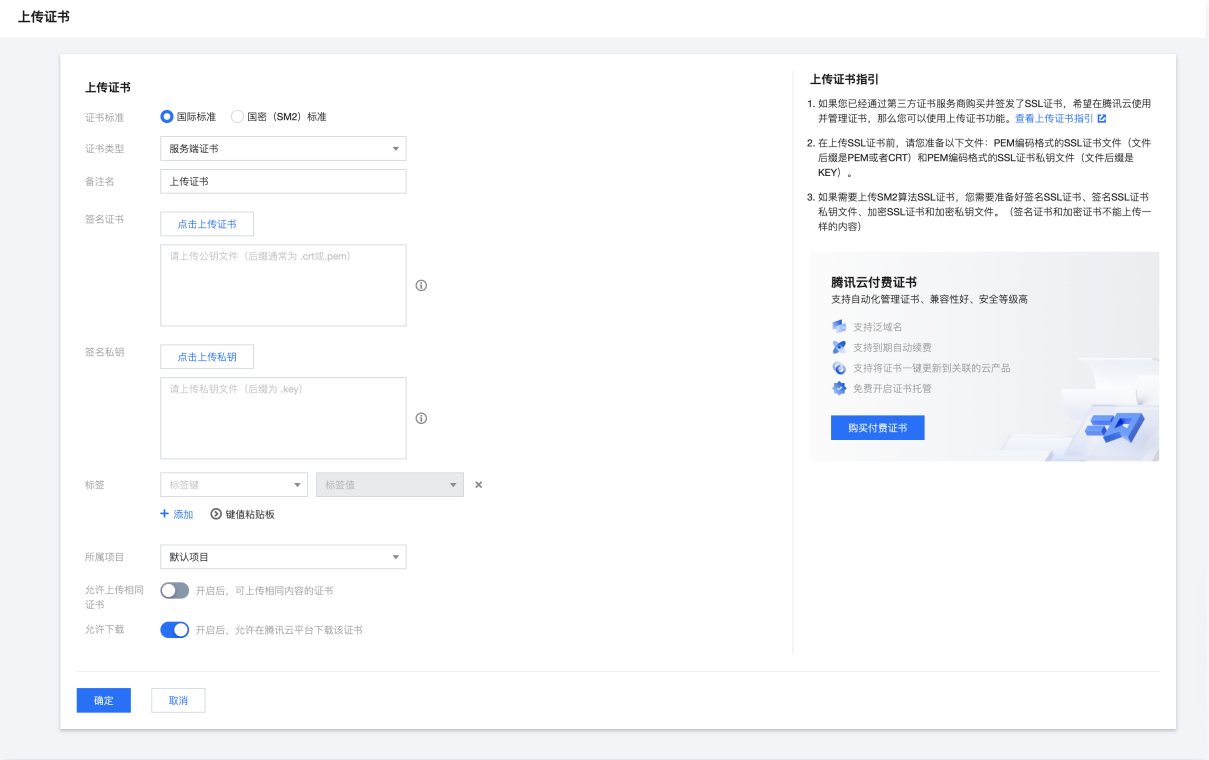
操作步骤

> **说明：**
> 若您的证书上传失败，您可参考文档 上传证书时提示 “解析失败，请检查证书是否符合标准” 检查相关原因。

上传国际标准证书

1. 登录 SSL 证书控制台，进入**我的证书**页面，并单击**上传证书**。
2. 在**上传证书**页面，请选择**国际标准**，并填写相关内容。如下图所示：

> **说明：**
> - 如您是从腾讯云下载证书，请使用 Nginx 文件夹内容进行上传。
> - 如您是从其他服务商下载证书，请咨询对应服务商。



- **证书类型：**
  - 服务端证书：常见的SSL证书类型。
  - CA证书：是SSL证书的根证书，通常是为了实现双向认证。
- **备注名：**请输入证书备注名。
- **签名证书：**
  - 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。
- **签名私钥：**

- 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。

- **标签**：请选择您的标签键和标签值，方便您管理腾讯云已有的资源分类。

> **说明**
> 如需添加标签，请参考 管理标签 。

- **所属项目**：请选择证书所属项目。

3. 单击**确定**，即可将证书上传至证书列表。

上传国密（SM2）标准证书

1. 登录 SSL 证书控制台，进入**我的证书**页面，并单击**上传证书**。
2. 在弹出的**上传证书**的窗口中，请选择**国密（SM2）标准**，并填写相关内容。如下图所示：

> **说明：**
> - 如您是从腾讯云下载证书，请使用 Nginx 文件夹内容进行上传。
> - 如您是从其他服务商下载证书，请咨询对应服务商。

- **证书类型**：
  - 服务端证书：常见的SSL证书类型。
  - CA证书：是SSL证书的根证书，通常是为了实现双向认证。
- **备注名**：请输入证书备注名。

- **签名证书：**
  - 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。
- **签名私钥：**
  - 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证书对应的文本框中。
  - 私钥格式以 “-----BEGIN EC PRIVATE KEY-----” 开头，以 “-----END PRIVATE KEY-----” 结尾。
- **加密证书：**
  - 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。
- **加密私钥：**
  - 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证书对应的文本框中。
  - 私钥格式以 “-----BEGIN PRIVATE KEY-----” 开头，以 “-----END PRIVATE KEY-----” 结尾。

> **说明：**
> 腾讯云 DNSPod 国密证书默认仅提供一个 .key 或 .pem 等为扩展名的文件，签名私钥和加密私钥都需填写这个私钥文件。

- **标签：**请选择您的标签键和标签值，方便您管理腾讯云已有的资源分类。

> **说明：**
> 如需添加标签，请参考 管理标签 。

- **所属项目：**请选择证书所属项目。

3. 单击**确定**，即可将证书上传至证书列表。

上传 CA 证书

1. 登录 SSL 证书控制台 ，进入**我的证书**页面，并单击**上传证书**。
2. 在弹出的**上传证书**的窗口中，选择**国际标准**，证书类型选择 **CA 证书**，并填写相关内容。如下图所示：

- **备注名：**请输入证书备注名。
- **签名证书：**
  - 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。

后续步骤

您可以将已上传托管的证书部署至云服务。具体操作指导请参见 部署至云服务 。

上传 SSL 证书自动托管指引

最近更新时间：2025-06-13 15:43:32

> **说明：**
> 自2025年6月13日起，上传到腾讯云的第三方证书在距离到期30天前，可免费使用“证书托管”功能，实现次年证书自动续费并自动更新到关联的腾讯云资源。

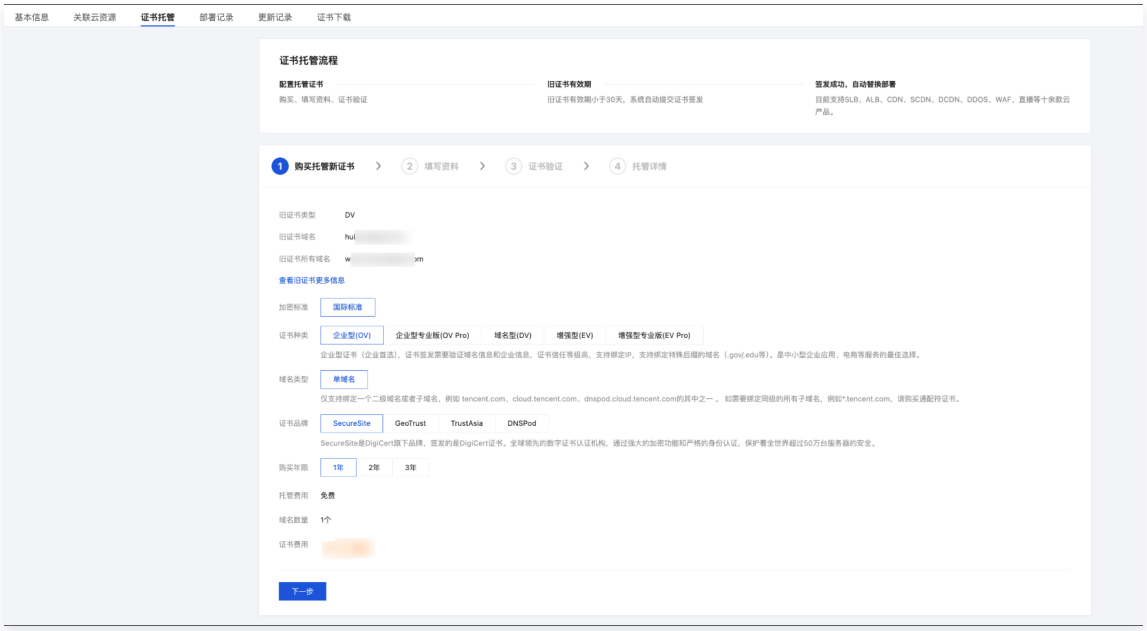
操作场景

已上传到腾讯云 SSL 证书的第三方证书，若需要自动续费、自动更新到关联的腾讯云资源，可参考该文档操作，自动托管已上传的 SSL 证书。

操作步骤

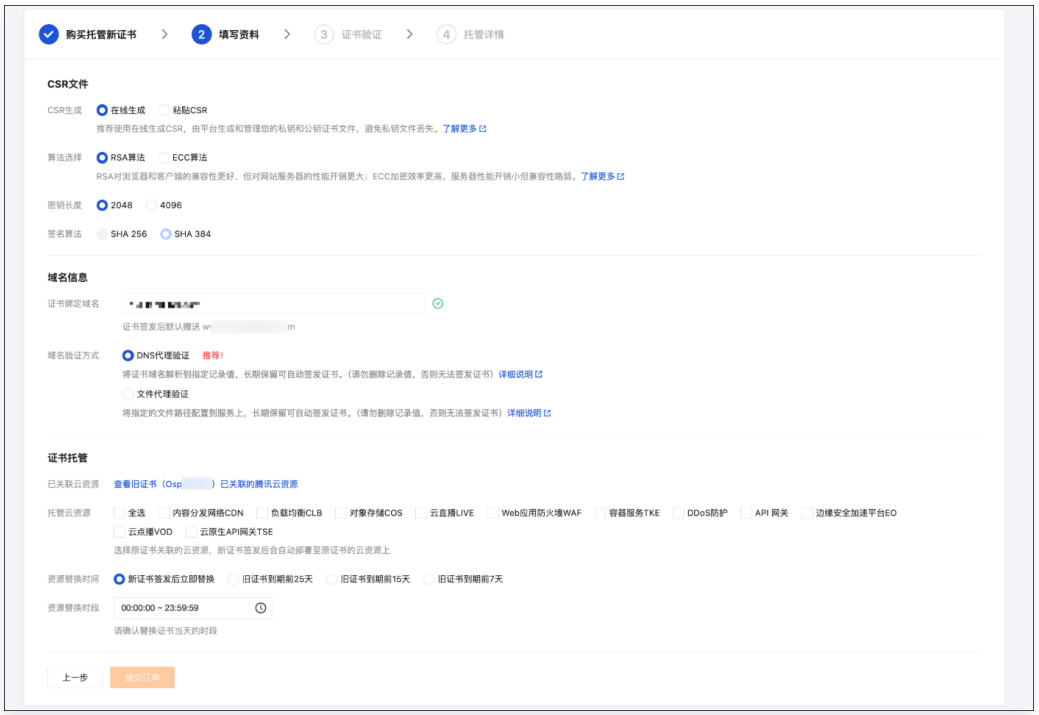
1. 登录 SSL 证书控制台，进入**我的证书**页面，按需选择**已上传证书**，单击**去托管**。

2. 在**证书托管**页面，选购次年自动续费的 SSL 证书，系统会自动根据上传第三方证书的类型，为您推荐适合您的证书。



3. 提前完善新证书的资料，勾选需要自动更新的云资源。

> **说明：**
> 提前完善资料，预选证书类型。待旧证书临近到期时，系统自动提交新证书签发，待新证书签发后自动替换到关联的腾讯云资源。



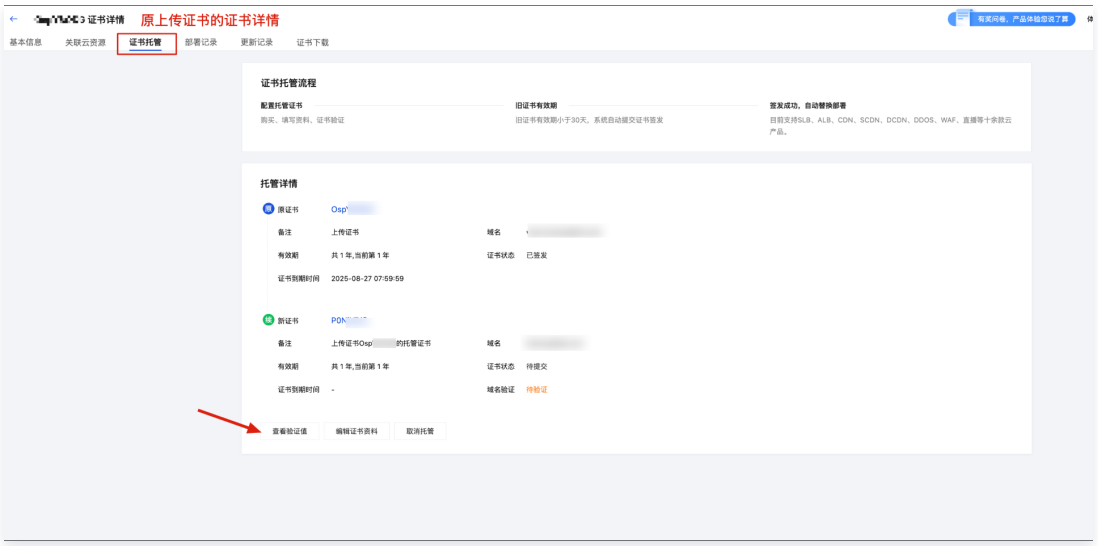
> **域名验证方式说明：**
>
> - **DV 型证书域名验证方式：**
> - DNS 代理验证：将证书域名解析到指定记录值，长期保留可自动签发证书。（请勿删除记录值，否则无法签发证书）
> - 文件代理验证：将指定的文件路径配置到服务上，长期保留可自动签发证书。（请勿删除记录值，否则无法签发证书）
> - **OV 型证书域名验证方式：**DNS 验证、文件验证。

4. 资料填写完成后，单击**提交订单**并按页面指引完成支付。

5. 支付完成后，SSL 证书控制台会生成一张新的证书。由于原上传证书未到期，所以证书托管生成的 SSL 证书不会直接签发，您无法在新证书提交资料。**您需要单击原上传证书 ID，进入原上传证书详情页 > 证书托管页面完善资料。**

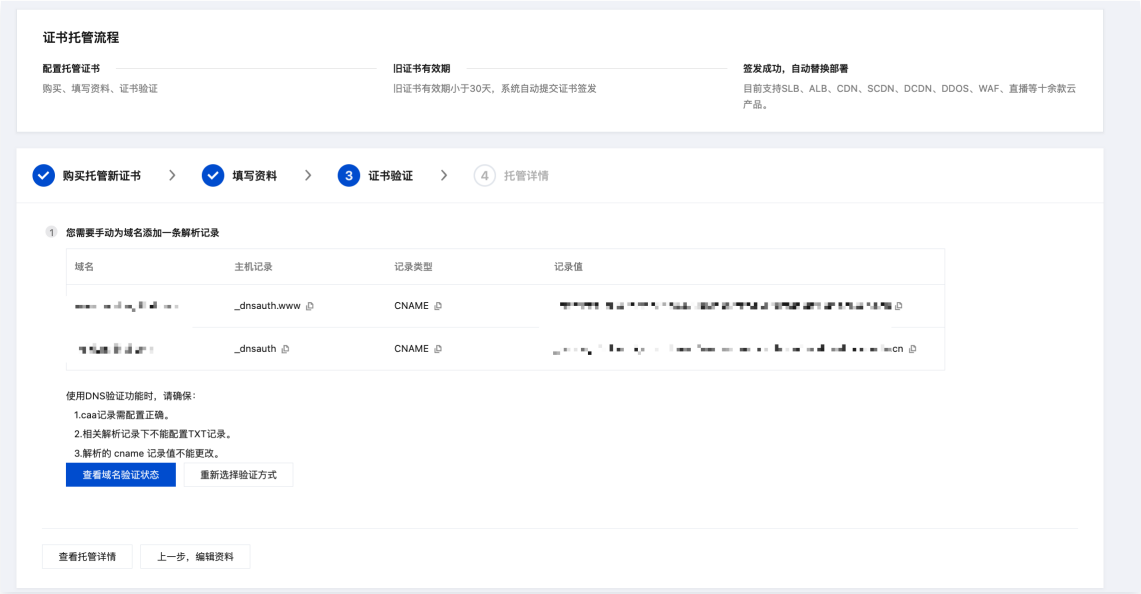
> **注意：**
>
> **原上传证书托管生成的新证书会在原上传证书临近到期29天时自动提交订单，无需您手动提交。**

6. 在原上传证书的证书详情页，查看域名验证值。



7. 根据页面指引，添加域名验证值。

> **禁止：**
> 域名验证值添加后，请勿删除。否则等到原上传证书临近到期，系统自动提交新证书的订单时，会因为缺少验证值导致新证书无法签发。



8. 域名验证值配置完成，原上传证书已加入证书托管。待原上传证书临近到期29天时，系统自动提交。可在**我的证书**列表查看。

9. 在**证书托管**页面，查看原上传证书是否托管成功。

> **说明：**
> 若未托管成功，请咨询 在线客服 。

SSL证书托管
SSL证书默认有效期为1年，您必须在证书到期前的30个自然日内续费并更新证书。腾讯云证书托管服务，可以在检测到续费的新证书（或指定证书）后，帮您自动更新证书（自动将新证书部署到旧证书关联的腾讯云云产品）。无需您再手动替换，节省您的证书维护时间。
新增托管
查看托管指南
搜索证书ID
证书ID
证书绑定域名
状态/有效期
自动续费
关联证书
状态
标签
资源部署状态
说明
操作
上传证书
证书已签发
2025-08-27
07:59:59
托管中
等待部署
--
取消托管
编辑

SSL 证书自动续费指引

最近更新时间：2025-03-04 14:39:02

SSL 证书默认有效期默认为1年。为了避免因忘记续费证书，导致证书到期后业务无法正常使用，腾讯云为您提供了证书自动续费服务，本文介绍如何对证书开启自动续费。

适用对象

腾讯云申请的 SSL 证书（不支持上传证书）。

证书品牌	DNSPod		TrustAsia	WoTrus
证书种类	DV 型		DV 型	DV 型
域名类型	单域名	通配符	通配符	通配符
是否支持自动续费	支持	支持	支持	支持

注意事项

- 距离 SSL 证书过期前14天（含14天）才可开启自动续费，距离证书过期14天内无法开启自动续费。
- 账号扣款失败，自动续费会终止，您需要手动完成续费。
- 证书签发后还需要您手动更新到云资源上。

自动续费流程

步骤1：进入证书列表开启自动续费

1. 付费证书在**过期前14天（含14天）**可开启自动续费，您可在 SSL 证书控制台 > **我的证书**中，找到对应证书，开启**自动续费**。
2. 弹出 SSL 证书的自动续费提示后，单击**开启自动续费**。

步骤2：预留充足账号余额

- 若您在证书过期前29天~14天之间（含14天）开启自动续费，系统将在您续费当天进行扣款。
- 若您在证书过期前30天（含30天）及更早的时间开启自动续费，并不会马上扣款，系统将在**证书到期前30天**开始扣款。

请您务必保障账号余额充足，续费金额仅供参考，最终以实际扣款为准。

> **注意：**
> 若因账号余额不足导致扣款失败，该证书的自动续费会终止，请您务必手动进行续费。

步骤3：生成新的待验证证书（未签发）

系统扣款成功后，证书续费成功，自动生成一张新的**待验证证书（未签发）**。

- 若您在证书过期前29天~14天之间（含14天）开启自动续费，系统会在开启自动续费当天生成新证书。
- 若您在证书过期前30天（含30天）及更早的时间开启自动续费，系统将在证书到期前30天生成新证书。

> **说明：**
> 续费后新证书的有效期将基于旧证书到期时间增加一年。例如，您待续费的旧证书于2021年11月01日过期，您在2021年10月1日完成续费和签发，那么新证书的有效期为2021年10月1日~2022年11月01日。

步骤4：签发新证书（可能需要人工介入）

如果您证书绑定的域名托管在腾讯云，系统会自动添加 DNS 验证；如果域名托管在第三方平台，**需要您手动添加 DNS 验证**。

> **注意：**
> - **超过三天未添加域名验证值，续费的新证书会审核失败，无法颁发，可能会影响到您后续业务。**

- 如果您的证书是 OV 型或 EV 型，可能还需要您上传确认函，上传确认函流程请参见 上传确认函指引 。

步骤5：证书签发成功，手动将新证书部署到云资源

证书签发成功后，请您务必**手动将新证书**更新到关联云资源。

SSL 证书催审指引

最近更新时间：2024-06-25 17:45:21

操作场景

若您已在腾讯云购买付费证书并提交相关资料，因自身或其他原因需要进行催审，您可以在腾讯云证书控制台进行催审操作，可达到快速审核的效果。
支持催审的证书如下：

> **说明：**
> DNSPod 品牌国密证书暂不支持催审，请您在提交资料后耐心等待审核通过。

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	支持	支持	–	–	支持	支持
GeoTrust	支持	–	–	–	支持	–
TrustAsia	支持	–	支持	支持	支持	–
GlobalSign	支持	–	–	–	支持	–
Wotrus	不支持	–	不支持	–	不支持	–

操作指南

1. 登录 证书管理控制台，进入**概览**页面。
2. 在**概览**页面中，单击**验证中**的数字，在打开的窗口，选择需要催审的证书订单。如下图所示：

3. 进入**证书申请**页面，单击**催审**按钮即可帮助您加快审核进度。以 SecureSite 企业型（OV）为例。如下图所示：

> **说明**
> - DV 型证书验证操作一般会持续1个工作日，在提交资料24小时后则会开放**催审**。
> - OV 型证书审核操作一般会持续 3 – 5个工作日，在上传确认函72小时后则会开放**催审**。
> - EV 型证书审核操作一般会持续5 – 7个工作日，在上传确认函96小时后则会开放**催审**。

证书申请
提交资料
选择验证方式
3 验证域名
4 签发证书
验证方式
DNS验证
需您手动为域名添加一条解析记录，操作简单，验证速度较快。
验证操作
您将有7天时间完成DNS解析记录的添加，否则审核将会失败。请您尽快添加DNS解析记录，扫描认证通过后即可颁布证书。
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
.com
_dnsauth
TXT
20210
4swtpo
查看域名验证状态
催审

SSL 证书吊销指引

最近更新时间：2024-03-28 14:32:11

操作场景

为让您方便管理您不再需要使用的证书，腾讯云提供了吊销证书功能，您可以在腾讯云申请吊销 SSL 证书操作。
一般情况下，您可能会在以下场景进行吊销 SSL 证书：

- 无需继续使用已签发的证书。
- 出于安全因素考虑，不再使用已签发的证书。

注意事项

证书类型	注意事项
全部证书	SSL 证书吊销申请提交后，该 SSL 证书无法再进行下载与部署等相关操作。
	SSL 证书吊销申请提交并审核成功后，该 SSL 证书将从签发机构处注销，证书吊销后将失去加密效果，浏览器不再信任该证书。
	腾讯云 SSL 证书吊销功能仅支持在腾讯云进行签发的证书，上传的第三方证书不支持吊销。
非 Wotrus 品牌国际标准证书与 DNSPod 品牌国密标准（SM2）证书	有效期30天之内，状态为待续费状态证书不能进行吊销操作。
	重颁发后的订单不能进行吊销操作。如需吊销，需吊销原订单，重颁发订单与原订单将一同自动吊销。
	签发时间在2020年3月25日前暂无法使用自主吊销功能，如需吊销请通过 在线咨询 联系客服进行处理。

前提条件

已登录 SSL 证书控制台 。

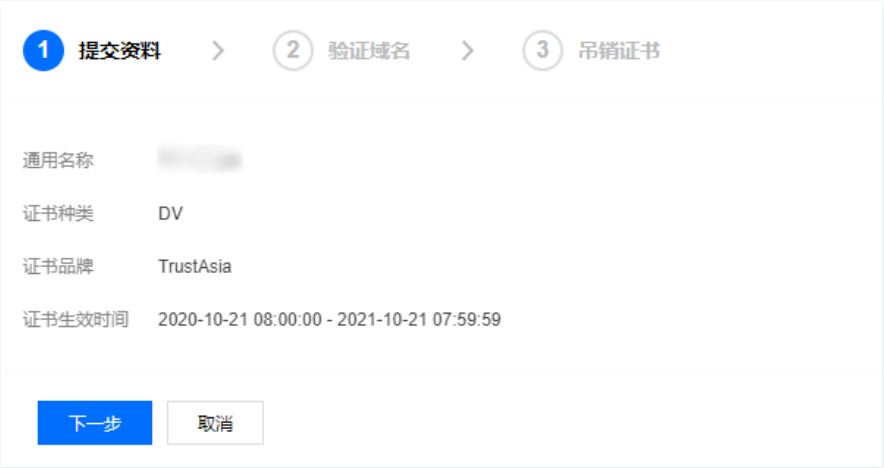
操作步骤

> **说明**
> 申请 SSL 证书绑定的域名已过期并被删除的情况下，如需吊销该证书，并涉及相关解析操作，请您进入 在线客服 咨询，会有技术人员帮助您处理。

选择证书吊销

1. 进入**我的证书**页面，选择需要进行吊销的证书，单击**更多 > 吊销**。如下图所示：

2. 在 “证书吊销申请” 页面，根据不同类型的证书进行验证或提交材料。详情请参见 不同类型证书吊销指引 。
   例如，亚洲诚信（TrustAsia）域名型免费证书（DV）吊销申请页面，如下图所示：



> **说明**
> 证书吊销成功后，进入已吊销状态。您可登录 SSL 证书控制台，删除该证书，该 SSL 证书将从腾讯云系统中删除。

不同类型证书吊销指引

DNSPod 品牌国密标准（SM2）DV 型与 Wotrus 品牌证书吊销流程

1. 在 “证书吊销申请” 页面，请在 “吊销信息” 模块，填写吊销原因。
2. 单击**下一步**，即可完成吊销申请。
3. 业务人员将人工审核吊销信息，审核通过后证书正式吊销。

DNSPod 品牌国密标准（SM2）EV、OV 证书吊销流程

1. 在 “证书吊销申请” 页面，请在 “吊销信息” 模块，填写吊销原因。
2. 单击**下一步**，上传证书吊销申请书。
3. 单击**下载申请书模板**，进行申请书信息补充填写。
4. 完成申请书填写后，申请书加盖公章后使用扫描件或拍摄清晰照片上传。
5. 单击**上传**，上传填写后的申请书，单击**下一步**，即可完成吊销申请。

> **说明**
> - 申请书支持 .jpg、.gif、.pdf 等文件格式，大小需在1.4M以内。
> - 申请书上传后，不支持重新上传，请确保上传正确。

6. 业务人员将人工审核吊销信息，审核通过后证书正式吊销。

其他品牌 DV 型证书吊销流程

1. 在 “证书吊销申请” 页面，单击**下一步**，即可提交吊销 SSL 证书申请。
2. 证书申请吊销后，请尽快按照详情指引配置吊销验证信息。

> **说明**
> - 若您购买的是 TrustAsia 品牌域名型（DV）（泛域名2年期或3年期）付费证书并已配置申请域名选择的自动 DNS 验证或自动文件验证，则无需进行域名所有权验证。
> - 若此证书原采用自动添加 DNS 的方式，现不满足自动 DNS 验证条件，则会变成 DNS 验证方式。
> - 若此证书采用 DNS 验证的方式，请在3天内添加 DNS 解析记录，否则此次吊销操作将会失败，扫描认证通过后证书即可被吊销。相关操作请参见 DNS 验证。
> - 若此证书采用文件验证的方式，请在3天内添加文件记录并访问成功，否则此次吊销操作将会失败，扫描认证通过后证书即可被吊销。相关操作请参见 文件验证。

其他品牌 OV/EV 证书提交流程

1. 在 “证书吊销申请” 页面，请在 “吊销信息” 模块，填写吊销原因。
2. 单击**下一步**，上传证书吊销确认函。
3. 单击**下载确认函模板**，进行确认函信息填写。
4. 完成确认函填写后，申请书加盖公章后使用扫描件或拍摄清晰照片上传。
5. 单击**上传**，上传填写后的确认函，单击**下一步**，即可完成吊销申请。

> **说明**
> - 确认函支持 .jpg、.png、.pdf 等文件格式，大小需在1.4M以内。
> - 申请域名已配置对应的自动 DNS 验证或自动文件验证，则无需上传确认函。

6. 业务人员将人工审核吊销信息，审核通过后证书正式吊销。

SSL 证书删除指引

最近更新时间：2024-12-26 16:26:12

概述

删除证书指在 SSL 证书控制台 的证书列表中，将某SSL证书删除。本文将介绍如何删除 SSL 证书。

前提条件

- SSL 证书已无关联的腾讯云资源（如果存在关联的云资源需要先解绑云资源）

> **说明：**
> - 若证书已过期，您可以随时删除证书。
> - 免费的测试证书任何状态都可以删除证书，若证书是付费证书，您必须在吊销证书后，才可删除该证书。证书吊销是指将已经签发的证书从签发机构处注销，证书吊销后将失去加密效果，不再被浏览器信任。具体操作请参见 SSL 证书吊销指引 。
> - 若已申请证书，待验证的证书取消审核后，才可删除该证书。

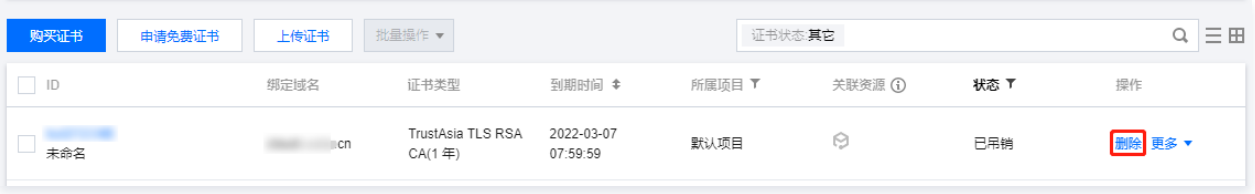
- 手动上传至 SSL 证书服务进行管理的第三方证书，支持随时删除证书。

> **注意：**
> - 请确保 SSL 证书未被部署在腾讯云云产品上，例如 WAF、CDN 等云服务。
> - 若存在云产品部署的情况下直接删除证书，可能会引起云产品业务中断。

操作步骤

1. 登录 SSL 证书控制台，并在左侧菜单栏单击**我的证书**，进入**我的证书**页面。
2. 在**我的证书**页面，查看您需要删除的证书，并根据您的证书状态类型，进行相应操作：
   - 上传托管证书：单击**更多** > **删除**。

   - 已过期、已吊销证书、已取消审核：单击**删除**。



3. 在弹出的**温馨提示**中，单击**确定**即可删除该证书。

SSL 证书重颁发指引

最近更新时间：2024-08-29 14:42:01

操作场景

若您的证书私钥泄露或其他需求需要重新生成一个新的证书，则需要进行重颁发操作。本文档指导您重颁发 SSL 证书。

> **说明：**
> - 证书处于**已签发状态且距过期时间大于30天**才可进行重颁发操作。
> - 1张免费域名型（DV）证书只能进行1次重颁发操作。
> - 相同主域名，若其中有1个子域名证书正在进行重颁发，该主域名下的其他子域名无法同时进行重颁发操作。
> - 证书重颁发过程中，该证书的重颁发功能关闭，不能再次申请重颁发。
> - 证书重颁发是指重新颁发一张证书，无法进行续期，颁发后有效时长仍为原证书有效时长。

前提条件

已登录 SSL 证书控制台，且成功申请获取 SSL 证书。

操作步骤

选择证书重颁发

1. 进入**我的证书**页面，选择需要进行重颁发的证书，单击**更多 > 重颁发**。如下图所示：

2. 进入**证书重颁发申请**页面，根据不同类型的证书进行验证或提交材料。详情请参见 不同类型证书重颁发指引 。

不同类型证书重颁发指引

Wotrus/DNSPod（OV/EV）

Wotrus 品牌国际标准证书与 DNSPod 品牌国密标准（SM2）OV/EV 型证书重颁发流程

1. 在 “证书重颁发申请” 页面，选择 CSR 方式，确认并填写相关信息，单击**下一步**。
   - **复用原证书 CSR**：使用该证书重颁发前的 CSR。
   - **在线生成 CSR**：由平台生成和管理您的 CSR。
   - **粘贴已有 CSR**：使用已有的 CSR 内容添加到该证书。
   - **证书绑定域名**：请填写单个域名。例如 `tencent.com` 、 `ssl.tencent.com` 。
   - **算法选择**：选择重颁发后证书的加密算法。
   - **密钥长度**：选择重颁发后证书的密钥长度。
   - **私钥密码**：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。

     > **说明：**
     > 如需部署腾讯云负载均衡、CDN 等云服务，请勿填写私钥密码。

   - **颁发原因**：请简要填写进行证书重颁发的原因。
2. 在弹出的提示窗口中，单击**确定**。

3. 进入 “验证域名” 页面，进行域名所有权认证，完成操作后，可单击**立即验证**。
4. 验证后需等待人工审核，人工审核通过后，即可完成证书重颁发。域名验证方法请参考 域名验证指引 。

> **说明：**
> - 若您公司已经有过该证书申请且成功过的记录，再次申请时提交的公司信息与成功申请公司信息一致，则不需要人工审核。
> - 重颁发提交时间距离已签发时间小于3天时，无需进行域名验证。
> - 若提交的 CSR 与旧证书的 CSR 不相同，则需要进行验证域名，若重新提交相同的 CSR，则无需验证域名。

其他品牌（OV/EV）

其他品牌 OV/EV 型证书重颁发流程

1. 在 “证书重颁发申请” 页面，选择 CSR 方式，确认相关信息，单击**下一步**。
   - **复用原证书 CSR**：使用该证书重颁发前的 CSR。
   - **在线生成 CSR**：由平台生成和管理您的 CSR。
   - **粘贴已有 CSR**：使用已有的 CSR 内容添加到该证书。
   - **证书绑定域名**：请填写单个域名。例如 `tencent.com` 、 `ssl.tencent.com` 。
   - **算法选择**：选择重颁发后证书的加密算法。
   - **密钥长度**：选择重颁发后证书的密钥长度。
   - **私钥密码**：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。

     > **说明：**
     > 如需部署腾讯云负载均衡、CDN 等云服务，请勿填写私钥密码。

   - **颁发原因**：请简要填写进行证书重颁发的原因。
2. 在弹出的提示窗口中，单击**确定**。
3. 证书审核机构将通过线下的方式联系您完成身份认证，届时请您注意电话和邮件。

域名型（DV）付费

域名型 DV 付费证书重颁发流程

1. 在 “证书重颁发申请” 页面，选择 CSR 方式，确认并填写相关信息，单击**确认颁发**。
   - **复用原证书 CSR**：使用该证书重颁发前的 CSR。
   - **在线生成 CSR**：由平台生成和管理您的 CSR。
   - **粘贴已有 CSR**：使用已有的 CSR 内容添加到该证书。
   - **证书绑定域名**：请填写单个域名。例如 `tencent.com` 、 `ssl.tencent.com` 。
   - **算法选择**：选择重颁发后证书的加密算法。
   - **密钥长度**：选择重颁发后证书的密钥长度。
   - **私钥密码**：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。

     > **说明：**
     > 如需部署腾讯云负载均衡、CDN 等云服务，请勿填写私钥密码 。

   - **颁发原因**：请简要填写进行证书重颁发的原因。
2. 在弹出的提示窗口中，单击**确定**。
3. 进入 “验证域名” 页面，进行域名所有权认证，完成操作后，可单击**立即验证**。域名验证方法请参考 域名验证指引 。

> **说明：**

> 若您购买的是 TrustAsia 品牌域名型（DV）（泛域名2年期或3年期）付费证书并已配置申请域名选择的自动 DNS 验证或自动文件验证，则无需进行域名所有权验证。

4. 验证域名通过后，即可完成证书重颁发。

> **说明：**
> - 若您重颁发的证书以相同公司名称并在13个月内完成过域名身份验证，将不执行域名验证操作。
> - 重颁发提交时间距离已签发时间小于3天时，无需进行域名验证。
> - 若提交的 CSR 与旧证书的 CSR 不相同，则需要进行验证域名，若重新提交相同的 CSR，则无需验证域名。

域名型（DV）免费

域名型 DV 免费证书重颁发流程

1. 在 “证书重颁发申请” 页面，确认并填写相关信息，单击**下一步**。
   - **算法选择**：选择重颁发后证书的加密算法。
   - **私钥密码**：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。

     > **说明：**
     > 如需部署腾讯云负载均衡、CDN 等云服务，请勿填写私钥密码 。

2. 在弹出的提示窗口中，单击**确定**。
3. 进入 “验证域名” 页面，系统将采用该证书首次申请时的域名验证方式，您按照原来的方式进行验证即可。
4. 域名验证成功后，即可完成重颁发。域名验证方法请参考 域名验证指引 。

SSL 证书消息忽略指引

最近更新时间：2025-03-28 11:30:12

操作场景

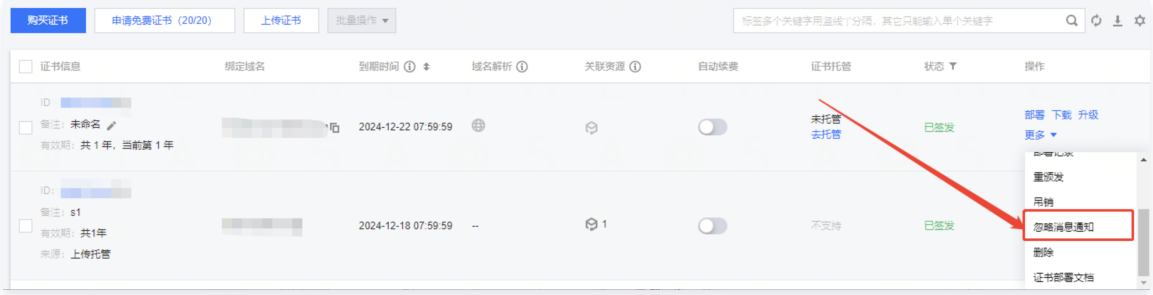
忽略证书是腾讯云 SSL 证书提供的消息忽略功能，通过该功能您可以在证书控制台中忽略指定的 SSL 证书的相关消息或重新接收消息，有效进行证书消息管理。本文将指导您如何开启或关闭忽略证书。

> **注意：**
> 忽略某一证书的消息提醒后，自忽略当天起所有消息提醒（含过期提醒）都不再推送，请您务必注意。

操作指南

关闭证书消息

1. 登录腾讯云 SSL 证书控制台，即可进入**我的证书**页面。
2. 在**我的证书**页面中，选择您需要进行关闭消息接收的证书，并单击**更多 > 忽略消息通知**。如下图所示：



3. 在弹出的**操作成功**窗口中，单击**确定**，即可完成设置。如下图所示：

开启证书消息

1. 登录腾讯云 SSL 证书控制台，即可进入**我的证书**页面。
2. 在**我的证书**页面中，选择您需要重新开启消息接收的证书，并单击**更多 > 重新关注**，即可接收该证书的消息。如下图所示：

SSL 证书自定义过期告警

最近更新时间：2024-11-27 17:28:52

操作场景

本文以 SSL 证书实例 `e79vbLDZ` 为例子展示如何配置告警，如需要在 SSL 证书实例 `e79vbLDZ` 的到期天数小于30个自然日时发送消息（短信、邮件）告警至指定账户联系人，可按照以下步骤进行操作。

> **说明：**
> 通过**腾讯云可观测平台**可以设置 SSL 证书过期告警消息的天数、间隔时间并指定告警人。

前提条件

1. 登录 腾讯云可观测平台 。
2. 在左侧菜单栏中，单击**告警管理** > **告警配置**，进入**告警配置**页面。
3. 单击**新增策略**，进入**新建告警策略**页面，并配置相关信息。

操作步骤

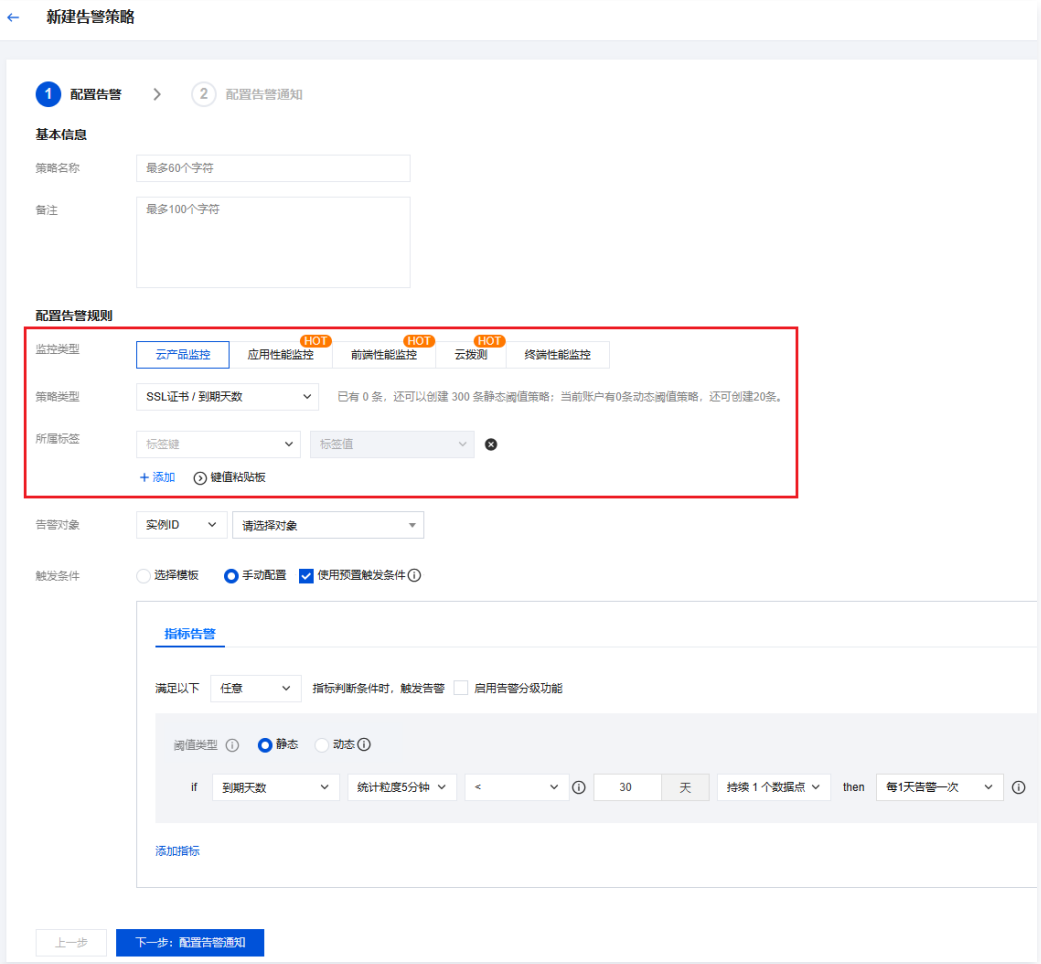
步骤1：配置基本信息

在**基本信息**模块，填写相关信息，如下图所示：

- **策略名称**：可自定义填写您配置的策略名称。
- **备注**：填写备注信息。

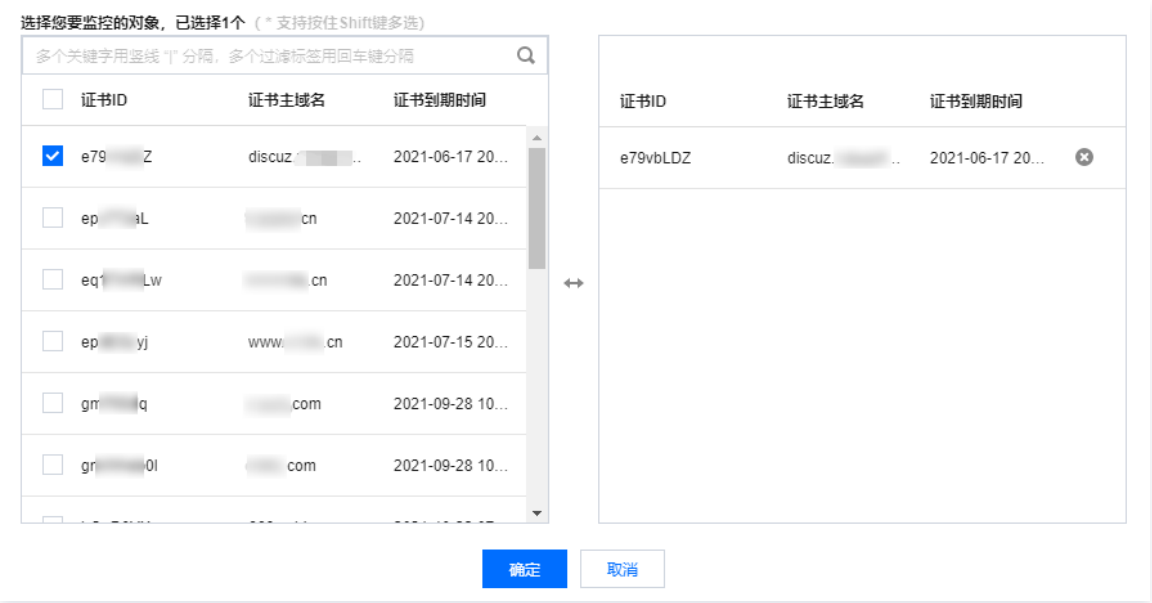
步骤2：配置告警规则

1. 在**配置告警规则**模块，配置相关信息。



- 监控类型：选择**云产品监控**。
- 策略类型：选择 **SSL 证书/到期天数**。
- 所属标签：按需选择策略所属标签，方便您根据标签对策略进行管理。支持为策略关联多个标签。如需创建标签，请参见 标签管理 。

2. 配置**告警对象**，勾选**实例 ID**，并选择需要监控的 SSL 证书实例。如下图所示：



3. 配置**触发条件**，选择**手动配置**，并配置如下条件。如下图所示：

- **判断条件**：选择**任意**。
- **阈值类型**：选择**静态**。
- **“指标告警”条件**：选择 `到期天数` 、 `统计周期1分钟` < `30天持续1个周期只告警一次` 。

> **说明：**
> 您可以根据自己的实际需求自定义告警触发条件。

步骤3：配置告警通知

在**配置告警通知**模块，通知模板可优先**选择模板**，添加告警「接收人」/「接收组」。图中以系统预设通知模板为例：

> **说明：**
> 若未创建，请单击**新增模板**进行创建，创建后您可以指定需要接收过期告警的接收人。

步骤4：高级设置

1. 在**高级设置**模块，根据您实际情况勾选达到告警条件后是否触发弹性伸缩策略。
2. 单击**完成**，即可完成配置告警的全部内容。
3. 配置完成后，当 SSL 证书实例 `e79vbLDZ` 的到期天数小于30个自然日时，即可发送消息（短信、邮件）告警至指定账户联系人。

> **说明：**
> 更多操作请查看 腾讯云可观测平台 相关文档。

SSL 证书消息通知设置

最近更新时间：2024-12-05 15:11:02

操作场景

SSL 证书到期、审核通过等通知，腾讯云将会通过短信、站内信、企业微信、邮件等多种渠道发送至您在腾讯云账号下所设置的联系方式。为避免未及时收到 SSL 证书相关信息，您可参考本文设置联系信息。

前提条件

已 注册腾讯云 账号。

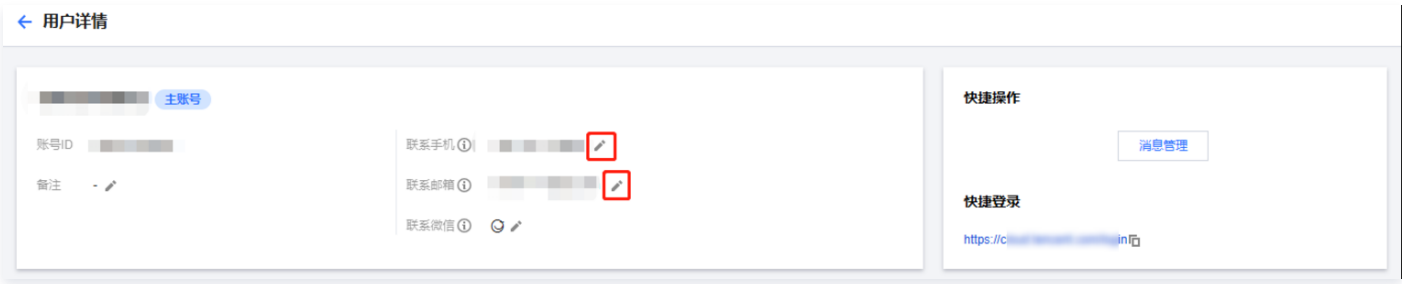
操作步骤

> **说明：**
> 以下操作仅为设置腾讯云主账号联系方式，子账号、协作者等联系方式设置与消息订阅详情请参见访问管理文档（例如：子用户订阅消息、协作者订阅消息）。

步骤1：设置联系手机和邮件

1. 登录腾讯云 访问管理控制台，进入 用户列表 页面。
2. 单击需要设置联系方式的**用户名称**，进入**用户详情**页面。

3. 在**用户详情**页面中，您可以单击 编辑联系手机与联系邮箱，确保您能够接收短信和邮件，如下图所示：

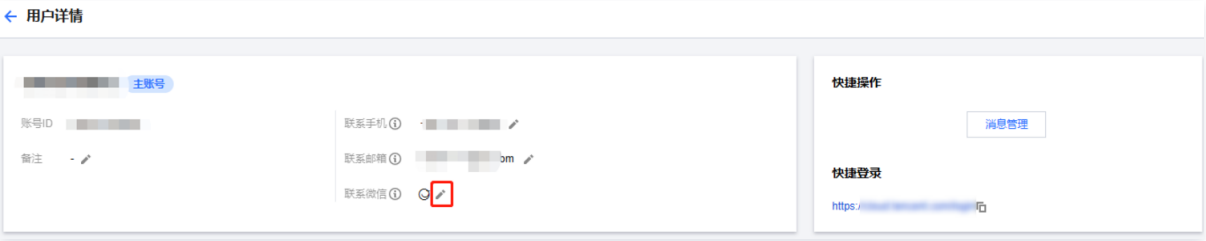


步骤2：设置联系微信

1. 登录腾讯云 访问管理控制台，进入 用户列表 页面。

2. 在**用户列表**页面，单击**用户类型**为 “主账号” 的**用户名称**，并单击 ，即可设置 “主账号” 的联系微信，如下图所示：

3. 在**用户详情**页面中，您可以单击 编辑联系微信，如下图所示：



4. 在弹出的**编辑信息**窗口中，单击**确定**。您的邮箱将收到一封包含二维码的邮件。

步骤3：验证微信

使用微信扫一扫邮件里的二维码，并关注 “腾讯云助手” 公众号。

> **注意：**
> 未扫码或扫码但未关注公众号都会导致微信验证不成功，若未关注公众号，则无法通过微信接收消息。

腾讯云证书权益点包管理

最近更新时间：2024-10-22 17:13:32

操作场景

权益点包适用于购买 SSL 证书、邮件证书等数字证书产品，以优惠价方式出售。如您有长期、批量购买数字证书相关产品的需求，可提前购买腾讯云数字证书权益点包，并在后续购买数字证书时，选择 “使用权益点购买证书” 进行抵扣即可。本文档将指导您如何使用与管理权益点包。

操作指南

使用腾讯云数字证书权益点包

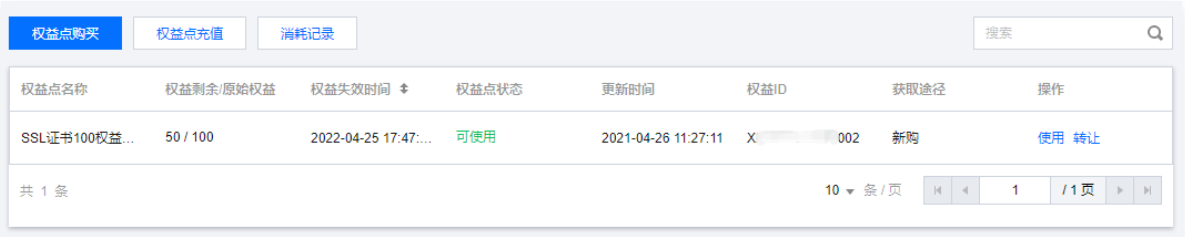
1. 登录 SSL 证书购买页面，选择您需要购买的证书类型。
2. 在**高级设置 > 权益点**处勾选**使用权益点购买证书**，并选择需要使用的权益点包。如下图所示：

3. 确认相关信息后，单击**核对信息并支付**，即可使用权益点购买证书。如下图所示：

> **说明：**
> 使用权益点购买证书成功后，您可以前往 SSL 证书控制台 提交资料申请证书文件。详情请参见 SSL 资料提交流程 。

转让腾讯云数字证书权益点包

1. 登录 SSL 证书控制台，并在左侧菜单栏单击**我的权益**。
2. 在**我的权益**页面中选择需要转让的权益点，并单击操作栏的**转让**。如下图所示：



3. 在弹出的**权益点转让**窗口中，输入相关的转让信息。如下图所示：

- **转让 UIN**：请输入待转让腾讯云用户 UIN（即账号 ID），具体可前往 账号中心 进行查看。
- **转让点数**：请输入您需要转让的权益点数。

4. 单击**确定**，即可转让腾讯云数字证书权益点。如下图所示：

> **说明：**
> 完成转让腾讯云数字证书权益点操作后，您还需将获取的转让码信息提供至已转让的用户 UIN，已转让的用户 UIN 完成充值操作后才可正常使用。

充值腾讯云数字证书权益点包

1. 登录 SSL 证书控制台，并在左侧菜单栏单击**我的权益**。
2. 在**我的权益**页面中，单击**权益点充值**。如下图所示：

3. 在弹出的**权益点转让**窗口中，输入充值码或者转让码。如下图所示：

4. 单击**确定**，即可充值腾讯云数字证书权益点。