SSL 证书

证书管理

产品文档

腾讯云

文档目录

证书管理
云资源托管指引

最近更新时间：2024-03-06 17:44:06

概述

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。

操作指南

1. 登录腾讯云 SSL 证书管理控制台，进入**我的证书**管理页面。
2. 在**我的证书**管理页面，选择您需要开启云资源托管的证书，并单击**证书名称**，进入**证书详情**管理页面。
3. 在**基本信息**模块的云资源托管处单击**查看**。

4. 在弹出的**云资源托管**窗口中，勾选您需开启的云资源。
5. 单击**确定**，即可完成操作。

上传（托管） SSL 证书指引

最近更新时间：2024-03-06 17:44:08

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 证书管理控制台，进入**我的证书**管理页面，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。

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**上传**，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 证书管理控制台，进入**我的证书**管理页面，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。

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**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。

SSL 证书催审指引

最近更新时间：2024-03-06 17:44:06

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	支持
GeoTrust	支持	-	-	-	支持	-
TrustAsia	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**证书概览**管理页面。
2. 在概览页中，选择**验证中**页签，选择需要催审的证书订单并单击**查看验证**。
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**。

SSL 证书吊销指引

最近更新时间：2024-03-06 17:44:06

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。
说明：
已签发证书若没有过期，则只有当该证书被吊销后，您才可以将证书从证书列表中删除；证书未被吊销的情况下，不支持删除。

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并且吊销操作无法取消，请谨慎操作。
	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 证书管理控制台。

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**管理页面，选择需要进行吊销的证书，单击**更多 > 吊销**。
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。详情请参考：不同类型证书吊销指引。

说明：

证书吊销成功后，进入已吊销状态。您可登录 SSL 证书管理控制台 ，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。相关操作可参考：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。相关操作可参考：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：2024-03-06 17:44:08

概述

删除证书指在 证书管理控制台 的证书列表中，将已经过期、已被吊销的 SSL 证书永久删除。本文将介绍如何删除 SSL 证书。

前提条件

SSL 证书已经过期、已被吊销、已取消审核。

说明：

若证书已过期，您可以随时删除证书。

若证书未过期，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 证书管理控制台，并在左侧菜单栏单击**我的证书**，进入**我的证书**管理页面。
2. 在**我的证书**管理页面，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：2024-03-06 17:44:08

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 证书管理控制台，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**管理页面，选择需要进行重颁发的证书，单击**更多 > 重颁发**。
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。详情请参考 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，则无需要验证域名。

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，则无需要验证域名。

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：2024-03-06 17:44:06

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：

只有处于即将过期状态的证书可以进行忽略操作。

操作指南

关闭证书消息

1. 登录腾讯云 证书管理控制台，即可进入**我的证书**管理页面。
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 > 忽略该证书**。
3. 在弹出的**操作成功**窗口中，单击**确定**，即可完成设置。

开启证书消息

1. 登录腾讯云 证书管理控制台，即可进入**我的证书**管理页面。
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。

SSL 证书自定义过期告警

最近更新时间：2024-03-06 17:44:06

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：

通过云监控可以设置 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 云监控控制台。
2. 在左侧菜单栏中，单击**告警配置 > 告警策略**，进入**告警策略**管理页面。
3. 单击**新增**，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。

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。

监控类型：默认为 “云产品监控”。

策略类型：选择 “SSL 证书/到期天数”。

策略所属项目：可选择 “默认项目”，也可根据您的实际需求选择相应项目。

步骤2：配置告警规则

1. 在**配置告警规则**模块，配置**告警对象**，勾选**实例 ID**，并选择需要监控的 SSL 证书实例。
2. 配置**触发条件**，选择**手动配置**，并配置如下条件。

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。