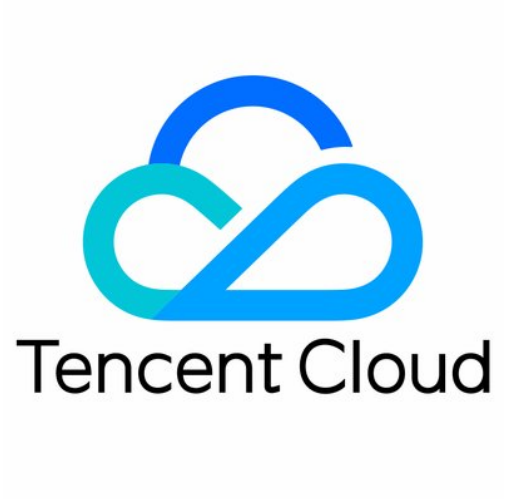
SSL Certificate Service

Certificate Management

Product Documentation



Contents

Certificate Management
Revoking an SSL Certificate

Last updated：2021-12-27 15:54:43

Overview

To facilitate the management of certificates that are no longer needed, Tencent Cloud provides the certificate revocation feature. You can apply for revocation of SSL certificates on Tencent Cloud.
Generally, you may revoke SSL certificates in the following scenarios:

- You do not need to continue using the issued certificates.
- For security reasons, the issued certificates are no longer used.

> Note：
> If an issued certificate has not expired, you can delete it from the certificate list only after the certificate is revoked. A certificate that has not been revoked cannot be deleted.

Notes

SSL Certificate Type	Notes
All certificates	After the application for revoking an SSL certificate is submitted, the certificate cannot be downloaded or deployed. In addition, certificate revocation cannot be canceled. Therefore, exercise caution when revoking a certificate.
	After the SSL certificate revocation application is submitted and approved, the SSL certificate is deregistered from the issuing authority. After the certificate is revoked, the encryption effect is lost and the browser does not trust the certificate any more.
	Tencent Cloud SSL certificate revocation supports only certificates issued on Tencent Cloud, and third-party certificates uploaded to the Tencent Cloud do not support revocation.
Non-Wotrus international standard certificates and DNSPod GM (SM2) certificates	A certificate that is valid within 30 days and is to be renewed cannot be revoked.
	A reissued certificate cannot be revoked. If revocation is required, you need to revoke the original certificate, and the reissued certificate will be automatically

	revoked together with the original certificate.
	The self-service revocation feature is temporarily unavailable for certificates issued before March 25, 2020. To revoke such certificates, please contact online technical support.

Prerequisite

You have logged in to the SSL Certificate Service console.

Directions

> Note：
> If the domain name bound to the SSL certificate you apply for has expired and been deleted, and you need to revoke the certificate and perform related parsing operations, please contact us.

Selecting the certificate to revoke

1. Go to the **My Certificates** page and select the certificate to revoke. Then, click **More** > **Revoke**, as shown in the following figure.

2. Go to the **Certificate Revocation Request** page and verify your certificate or submit the required materials based on your certificate type. For more information, please see Revoking different types of certificates.
   The following figure shows the revocation application page for a free TrustAsia DV SSL certificate.

> Note：
> After the certificate is revoked successfully, the certificate enters the revoked state, and you can log in to the SSL Certificate Service console, and delete the certificate from the Tencent Cloud system.

Revoking different types of certificates

Revoking DNSPod GM (SM2) DV and Wotrus certificates

1. On the **Certificate Revocation Request** page, enter the revocation reason in the **Revocation Information** area.
2. Click **Next** to complete the revocation application.

3. Reviewers manually review the revocation information. After the review is passed, the certificate will be formally revoked.

Revoking DNSPod GM (SM2) EV and OV certificates

1. On the **Certificate Revocation Request** page, enter the revocation reason in the **Revocation Information** area.
2. Click **Next** to upload the certificate revocation application.
3. Click **Download application template** and enter application information in the template.
4. Upload a photo or scan of the application stamped with the official seal.
5. Click **Upload** to upload the application and click **Next**.

> Note：
>
> - The application file must be smaller than or equal to 1.4 MB in JPG, GIF, or PDF format.
> - After the application file is uploaded, it cannot be uploaded again. Ensure that the application file is uploaded correctly.

6. Reviewers manually review the revocation information. After the review is passed, the certificate will be formally revoked.

Revoking other DV certificates

1. On the **Certificate Revocation Request** page, click **Next** to submit an SSL certificate revocation application.
2. After submitting the SSL certificate revocation application, configure the verification information as instructed as soon as possible.

> Note：
>
> - If your DV certificate is purchased from TrustAsia (2-year or 3-year wildcard domain) and you have configured automatic DNS or file validation for the domain you are applying for, ownership verification is not required.
> - If your certificate originally adopts the automatic DNS validation mode but now the conditions for automatic validation are not met, the manual DNS validation mode will be automatically adopted.
> - If the certificate adopts the DNS validation mode, please add DNS records within 3 days. Otherwise, the revocation will fail. The certificate will be revoked after successful validation.
> - If the certificate adopts the file validation mode, please add file records within 3 days and ensure that the files can be accessed successfully. Otherwise, the revocation will fail. The certificate will be revoked after the successful validation. For related operations, please see File Validation.

Revoking OV/EV certificates of other brands

1. On the **Certificate Revocation Request** page, enter the revocation reason in the **Revocation Information** area.
2. Click **Next** to upload the certificate confirmation letter.
3. Click to **download the confirmation letter template** and enter information in the confirmation letter.
4. Upload a photo or scan of the confirmation letter stamped with the official seal.
5. Click **Upload** to upload the confirmation letter and click **Next**.

> Note：
>
> - The confirmation letter file must be smaller than or equal to 1.4 MB in JPG, PNG, or PDF format.
> - If automatic DNS or file validation has been configured for the domain name applied for, you do not need to upload the confirmation letter.

6. Reviewers manually review the revocation information. After the review is passed, the certificate will be formally revoked.

Reissuing an SSL Certificate

Last updated：2022-09-14 17:31:16

Overview

This document describes how to reissue an SSL certificate, in case your certificate key has been compromised, or you need to generate a new certificate due to other reasons.

Note：

- Certificate reissue is only available if **your certificate has been issued and its remaining effective time is longer than 30 days**.
- Each free DV certificate can only be reissued once.
- If the certificate of a sub-domain under a primary domain is being reissued, certificates of other sub-domains under this primary domain cannot be reissued at the same time.
- During the reissue process, the reissue feature of this certificate is disabled, and you cannot apply for a reissue for this certificate again.
- Certificate reissue will not renew the certificate. In other words, the validity period will be the same as the original one,

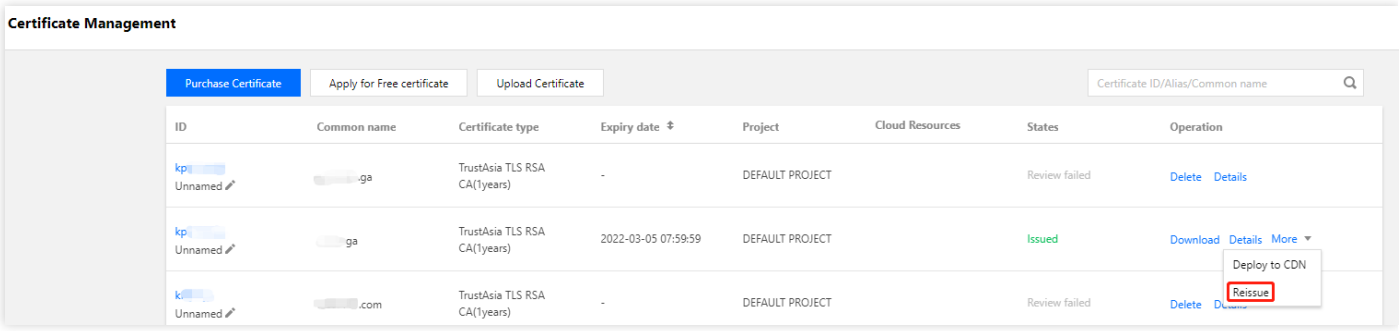
Preparations

Log in to the SSL Certificate Service console and successfully applied for an SSL certificate.

Directions

Selecting certificate reissue

1. Go to the **My Certificates** page and select the certificate to reissue. Then, click **More** > **Reissue**.



2. Go to the **Certificate re-issuance application** page and verify your certificate or submit the required materials based on your certificate type. For more information, see Reissuing different types of certificates.

Reissuing different types of certificates

- Wotrus/DNSPod（OV/EV）
- OV/EV certificates of other brands
- Paid DV certificates
- Free DV certificates

Reissuing Wotrus international standard certificates and DNSPod SM (SM2) OV/EV certificates

1. On the **Certificate re-issuance application** page, select a CSR algorithm, enter and confirm the configurations, and click **Next**.

- **Using the CSR of the original certificate**: Use the CSR of the original certificate.
- **Generating a CSR online**: Generate and manage the CSR by Tencent Cloud SSL Certificate Service.
- **Using an existing CSR**: Paste the content of an existing CSR to the certificate.
- **Binding the certificate to a domain**: Enter a single domain, such as `tencent.com` or `ssl.tencent.com`.
- **Selecting an algorithm**: Select the encryption algorithm for the certificate to be reissued.
- **Key length**: Select the key length for the certificate to be reissued.
- **Private key password**: To ensure the security of your private key, **password recovery is NOT supported**, so keep the password in mind.

Note：
If you need to deploy Tencent Cloud services such as CLB and CDN, don't enter the private key password.

- **Reissue reason**: Enter the reissue reason in brief.

2. In the pop-up window, click **Confirm**.
3. Validate the domain ownership on the "Domain Ownership Validation" page, and click **Validate Now** after operations are completed.
4. Manual approval is required upon domain ownership validation, and then the certificate will be reissued. For validation instructions, see Domain Ownership Validation.

Note：

- If you have successfully applied for this certificate, manual approval is omitted when the enterprise info submitted in re-application is consistent with that recorded in the system.
- If the span between the reissue submission time and original issue time is less than 3 days, domain ownership validation is not required.
- If the submitted CSR is different from that of the original certificate, domain ownership needs to be validated. If they are the same, validation is not needed.