SSL Certificate Service

Certificate Management

Product Documentation

Contents

Certificate Management
Tencent Cloud Certificate Benefit Point Package Management

Last updated：2024-03-06 17:44:06

Overview

With Tencent Cloud resource hosting, a new SSL certificate can be automatically deployed to the same Tencent Cloud resources such as CLB and CDN as the original certificate after successful renewal and issue (or reapplication for a free certificate).
After a new SSL certificate is issued, you can enable Tencent Cloud resource hosting and bind relevant Tencent Cloud resources. When this SSL certificate is renewed and a new certificate is generated, the Tencent Cloud resources bound to the original certificate will be automatically bound to the new one.
Note:
Tencent Cloud resource hosting will not automatically install a new certificate to the web application on your server. Therefore, you still need to manually install the new certificate issued after the renewal to your web service (to replace the original one) even if Tencent Cloud resource hosting is enabled. If your SSL certificate is only deployed to Tencent Cloud resources, this hosting feature will automate the entire process.
Tencent Cloud resource hosting is free of charge.

Strengths of Tencent Cloud resource hosting

For SSL certificate deployment to Tencent Cloud resources, after you have deployed a certificate to Tencent Cloud resources for the first time and enabled resource hosting, Tencent Cloud will take over the deployment of additional certificates you apply for.

Use limits

After Tencent Cloud resource hosting is enabled for the original certificate, automatic deployment to Tencent Cloud resources will take effect only if the SSL certificate applied for has the same specifications as the original one, including domain type, certificate type, and certificate brand.
After Tencent Cloud resource hosting is enabled for a paid certificate, the certificate issued after this certificate is renewed can be automatically deployed to Tencent Cloud resources.

After Tencent Cloud resource hosting is enabled for a free certificate, the certificate issued after this certificate is reapplied for can be automatically deployed to Tencent Cloud resources.

Directions

1. Log in to the SSL Certificate Service console and go to the **My Certificates** page.
2. On the **My Certificates** page, select the target certificate and click the **Certificate Name** to enter the **Certificate Details** page.
3. In the **Basic Info** module, click **View** in **Tencent Cloud Resource Hosting**.
4. In the **Tencent Cloud Resource Hosting** pop-up window, select the target Tencent Cloud resources.
5. Click **OK** to complete the operation.

Uploading (Hosting) an SSL Certificate

Last updated：2024-03-06 17:44:08

Overview

You can upload all your SSL certificates to the SSL Certificate Service console for unified management. This document describes how to upload certificates.

Directions

Note:
If your certificate failed to be uploaded, troubleshoot as instructed in "DNS Query Failed. Check Whether the Certificate Conforms to the Standard" Is Prompted During Certificate Upload.

Uploading an international standard certificate

1. Log in to the SSL Certificate Service console, go to the **My Certificates** page, and click **Upload Certificate**.
2. In the **Upload Certificate** pop-up window, select **International standard** and enter the relevant information as shown below:

Note:
If you download the certificate from Tencent Cloud, upload it by using files in the Nginx folder.
If you download the certificate from another service provider, contact it for assistance.
Certificate Name: Enter a certificate name.
Signature Certificate:
A certificate is usually a file with an extension such as .crt or .pem. Please use a text editor to open the certificate file and copy the certificate to the **Certificate** text box.
The certificate should start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----".
The certificate content should include the complete certificate chain.
Signature Private Key:
A private key is usually a file with an extension such as .key and .pem. Please use a text editor to open the private key file and copy the private key to the corresponding text box.
The private key starts with "-----BEGIN (RSA) PRIVATE KEY-----" and ends with "-----END (RSA) PRIVATE KEY-----".
Tag: Select your tag key and tag value to better manage existing Tencent Cloud resources by category.
Note:
You can add a tag as instructed in Querying Resources by Tag.

Project: Select a project for the certificate.

3. Click **Upload** to upload the certificate to the certificate list.

Uploading a Chinese SM (SM2) certificate

1. Log in to the SSL Certificate Service console, go to the **My Certificates** page, and click **Upload Certificate**.

2. In the **Upload Certificate** pop-up window, select **Chinese SM (SM2)** and enter the relevant information as shown below:

Note:

If you download the certificate from Tencent Cloud, upload it by using files in the Nginx folder.

If you download the certificate from another service provider, contact it for assistance.

Certificate Name: Enter a certificate name.

Signature Certificate:

A certificate is usually a file with an extension such as .crt or .pem. Please use a text editor to open the certificate file and copy the certificate to the **Certificate** text box.

The certificate should start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----".

The certificate content should include the complete certificate chain.

Signature Private Key:

A private key is usually a file with an extension such as .key and .pem. Use a text editor to open the private key file and copy the private key to the corresponding text box of the certificate.

The private key starts with "-----BEGIN EC PRIVATE KEY-----" and ends with "-----END PRIVATE KEY-----".

Encryption Certificate:

A certificate is usually a file with an extension such as .crt or .pem. Please use a text editor to open the certificate file and copy the certificate to the **Certificate** text box.

The certificate should start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----".

The certificate content should include the complete certificate chain.

Encryption Private Key:

A private key is usually a file with an extension such as .key and .pem. Use a text editor to open the private key file and copy the private key to the corresponding text box of the certificate.

The private key starts with "-----BEGIN PRIVATE KEY-----" and ends with "-----END PRIVATE KEY-----".

Note:

A private key file with an extension such as .key or .pem is provided by default for a DNSPod Chinese SM certificate. It is required for both the signature private key and encryption private key.

Tag: Select your tag key and tag value to better manage existing Tencent Cloud resources by category.

Note:

You can add a tag as instructed in Querying Resources by Tag.

Project: Select a project for the certificate.

3. Click **Upload** to upload the certificate to the certificate list.

Subsequent Operations

You can deploy the uploaded certificate to a cloud service.

Reminding Reviewers to Review an SSL Certificate Application

Last updated：2024-03-06 17:44:06

Overview

This document describes how to send a reminder in the SSL Certificate Service console after purchasing a paid certificate and submitting the information to accelerate the review progress if needed.
You can send a reminder for the following certificates:

Note:
Currently, you cannot send a reminder for DNSPod Chinese SM certificates, and all you need to do is wait for the approval after submitting the information.

Certificate Brand	OV	OV Pro	DV	Free DV	EV	EV Pro
SecureSite	Supported	Supported	-	Supported	Supported	Supported
GeoTrust	Supported	-	-	-	Supported	-
TrustAsia	Supported	-	Supported	-	Supported	-
GlobalSign	Supported	-	-	-	Supported	-
WoTrus	Not supported	-	Not supported	-	Not supported	-

Directions

1. Log in to the SSL Certificate Service console and go to the **Certificate Overview** page.
2. On the overview page, select the **Validating** tab, select the target certificate order, and click **View Validation**.
3. On the **Certificate Application** page, click **Send reminder** to accelerate the review progress as shown below.

The following takes a SecureSite OV certificate as an example:

Note:
Validating a DV certificate usually takes one business day, and the **reminder** option will become available 24 hours after the information is submitted.
Reviewing an OV certificate usually takes 3–5 business days, and the **reminder** option will become available 72 hours after the confirmation letter is uploaded.

Reviewing an EV certificate usually takes 5–7 business days, and the **reminder** option will become available 96 hours after the confirmation letter is uploaded.

Revoking an SSL Certificate

Last updated：2024-03-06 17:44:06

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.

Must-Knows

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.
	You can use the SSL certificate revocation feature to revoke only certificates issued in Tencent Cloud but not any uploaded third-party certificates.
Non-WoTrus international standard certificates and DNSPod Chinese SM (SM2) certificates	You cannot revoke certificates that will expire within 30 days and are in the "to be renewed" status.
	To revoke a reissued order, you need to revoke the original one, and the reissued order will be automatically revoked along with the original one.
	You cannot revoke certificates issued before March 25, 2020 on your own. If you have such needs, contact us for assistance.

Prerequisites

You have logged in to the SSL Certificate Service console.

Directions

Note:
If the domain 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, contact us for assistance.

Selecting the certificate to revoke

1. Go to the **My Certificates** page, select the target certificate, and click **More** > **Revoke**.
2. On the **Certificate Revocation Request** page, validate your certificate or submit the required information based on your certificate type. For more information, see Revoking different types of certificates.

Note:
After the certificate is revoked successfully, the certificate enters the revoked status. 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 Chinese SM (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 can be up to 1.4 MB in JPG, GIF, or PDF format.
After the application file is uploaded, it cannot be uploaded again. Make sure 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, add DNS records within three days; otherwise, the revocation will fail. The certificate will be revoked after the successful validation. For detailed directions, see DNS Validation.

If the certificate adopts the file validation mode, add file records within three days and make sure that the files can be accessed successfully; otherwise, the revocation will fail. The certificate will be revoked after the successful validation. For detailed directions, 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 can be up to 1.4 MB in JPG, PNG, or PDF format.

If automatic DNS or file validation has been configured for the domain 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.

Deleting an SSL Certificate

Last updated：2024-03-06 17:44:08

Overview

This document describes how to permanently delete an expired or revoked SSL certificate from the certificate list in the SSL Certificate Service console.

Prerequisites

The SSL certificate has expired or been revoked or its review has been canceled.

Note:

You can delete an expired certificate at any time.

If a certificate has not expired, you must revoke it before deleting it. Revoking a certificate is deregistering an issued certificate from the issuing authority. After the certificate is revoked, the encryption effect is lost and the browser does not trust the certificate any more. For detailed directions, see Revoking an SSL Certificate.

If you have applied for a certificate, you can delete it only after the review is canceled.

You can delete a third-party certificate manually uploaded to the SSL Certificate Service for management at any time.

Note:

Make sure that the SSL certificate has not been deployed on any Tencent Cloud product such as WAF and CDN.

If a certificate has been deployed on a Tencent Cloud product, deleting it may interrupt the business of that product.

Directions

1. Log in to the SSL Certificate Service console and click **My Certificates** on the left sidebar.
2. On the **My Certificates** page, view the target certificate and perform the corresponding operation based on its status:

For a certificate uploaded for hosting: Click **More** > **Delete**.

For an expired or revoked certificate or a certificate with its review canceled: Click **Delete**.

3. In the **Note** pop-up window, click **OK**.

Reissuing an SSL Certificate

Last updated：2024-03-06 17:44:06

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 available only if your certificate **has been issued and will expire in more than 30 days**.

Each free DV certificate can be reissued only once.

If the certificate of a subdomain under a primary domain is being reissued, certificates of other subdomains under this primary domain cannot be reissued at the same time.

In the reissue process, the reissue feature of the 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.

Prerequisites

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

Directions

Selecting the certificate to be reissued

1. Go to the **My Certificates** page, select the target certificate, and click **More** > **Reissue**.
2. Go to the **Certificate Reissue Application** page and verify your certificate or submit the required information based on your certificate type. For more information, see Reissuing different types of certificates.

Reissuing different types of certificates

WoTrus/DNSPod (OV/EV)

Reissuing WoTrus international standard certificates and DNSPod Chinese 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 the SSL certificate to Tencent Cloud services such as CLB and CDN, do not 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. After your domain is validated, wait for manual approval, upon which the certificate will be reissued. For more information on how to validate a domain, see Domain Validation Guide.
Note:
If you have successfully applied for this certificate and the organization information submitted in the re-application is consistent with that recorded in the system, manual approval is not required.
If the span between the reissue submission time and original issue time is less than three days, domain validation is not required.
If the submitted CSR is different from that of the original certificate, domain validation is required; otherwise, it is not required.

Other brands (OV/EV)

Reissuing OV/EV certificates of other brands
1. On the **Certificate re-issuance application** page, select a CSR algorithm, confirm other 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 the SSL certificate to Tencent Cloud services such as CLB and CDN, do not enter the private key password.

Reissue reason: Enter the reissue reason in brief.

2. In the pop-up window, click **Confirm**.

3. CA will contact you offline for identity verification. Please pay heed to your emails and phone calls.

(DV) Paid

Reissuing paid DV certificates

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

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 the SSL certificate to Tencent Cloud services such as CLB and CDN, do not enter the private key password.

Reissue reason: Enter the reissue reason in brief.

2. In the pop-up window, click **Confirm**.

3. On the **Validate Domain** page, verify the domain ownership and click **Validate**. For more information on how to validate a domain, see Domain Validation Guide.

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.

4. After the domain is verified, the reissue is completed.

Note:

In the last 13 months, if domain identity verification has been completed for the certificate to be reissued using the same organization name, domain validation will not be performed.

If the span between the reissue submission time and original issue time is less than three days, domain validation is not required.

If the submitted CSR is different from that of the original certificate, domain validation is required; otherwise, it is not required.

(DV) Free

Reissuing free DV certificates

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

Selecting an algorithm: Select the encryption algorithm 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 the SSL certificate to Tencent Cloud services such as CLB and CDN, do not enter the private key password.

2. In the pop-up window, click **Confirm**.

3. Go to the **Domain ownership validation** page. The validation method that is used when you first applied for this certificate will be used. You can perform validation as you did before.

4. After your domain is validated successfully, the certificate will be reissued. For more information on how to validate a domain, see Domain Validation Guide.

Ignoring SSL Certificate Notifications

Last updated：2024-03-06 17:44:08

Overview

This document describes how to enable or disable certificate ignoring, a feature provided by the SSL Certificate Service to ignore or re-receive the messages of a specified SSL certificate for effective certificate message management.

Note:

You can ignore only certificates that will expire soon.

Directions

Disabling certificate messages

1. Log in to the SSL Certificate Service console and go to the **My Certificates** page.
2. On the **My Certificates** page, select the target certificate and click **More** > **Ignore**.
3. In the pop-up window, click **OK**.

Enabling certificate messages

1. Log in to the SSL Certificate Service console and go to the **My Certificates** page.
2. On the **My Certificates** page, select the target certificate and click **More** > **Unignore** to receive the messages of the certificate.

Customizing SSL Certificate Expiration Notifications

Last updated：2024-03-06 17:44:06

Overview

This document describes how to configure alarms for the `e79vbLDZ` SSL certificate instance to have alarms sent to specified recipients via SMS and email when it will expire within 30 calendar days.

Note:

You can set the number of days, interval, and recipients to receive alarm messages for the expiration of the SSL certificate.

Prerequisites

1. Log in to the Cloud Monitor console.
2. On the left sidebar, click **Alarm Configuration** > **Alarm Policy**.
3. Click **Add** to enter the **Create Policy** page and configure relevant information.

Directions

Step 1. Configure the basic information

In the **Basic Info** module, enter the relevant information.

Policy Name: Enter a custom policy name.

Remarks: Enter the remarks.

Monitoring Type: It is **Cloud Product Monitoring** by default.

Policy Type: Select **SSL Certificate/Expiration Time**.

Project: You can select **Default Project** or another as needed.

Step 2. Configure the alarm policy

1. In the **Alarm Policy** module, configure the **Alarm Object**, select **Instance ID**, and select the target SSL certificate instance.
2. Set **Trigger Condition** to **Configure manually** and configure the following conditions.

Condition: Select **any**.

Threshold: Select **Static**.

"Metric alarm" condition: Set the condition to receive only one alarm message if the expiration time is within 30 days under the statistical period of 1 minute.

Note:

You can set the alarm trigger condition as needed.

Step 3. Configure alarm notifications

In the **Configuring Alarm Notification** module, preferably set **Notification Template** to **Select template** and add [Recipient]/[Recipient Group] of the alarm. The figure takes the preset notification template as an example:

Note:

If no templates are created, click **Create template** to create one. Then, you can specify the recipient to receive the expiration alarm.

Step 4. Configure advanced settings

1. In the **Advanced Settings** module, set whether to trigger the auto scaling policy after the alarm conditions are met.
2. Click **Complete**.
3. After the configuration, if the `e79vbLDZ` SSL certificate instance will expire within 30 calendar days, the specified recipient will be notified via SMS and email.

Note:

For more information, see Cloud Monitor documentation.