SSL Certificates

FAQs

Copyright Notice

Trademark Notice

Tencent Cloud

Service Notice

This document provides an overview of the as–is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre–sales consultation and technical after–sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Is an SSL Certificate Still Available After I Renew It?

FAQs

SSL Certificate Selection

How Do I Choose a Certificate?

Last updated：2023-10-09 14:54:07

What type of certificate should one opt for?

- If the proprietor of your website is an individual (i.e., without a business license), you are only eligible to apply for either a free Domain Validation (DV) certificate or a paid Domain Validation (DV) certificate.
- For financial and payment enterprises, EV SSL certificates are recommended.
- For general enterprises, OV SSL certificates and SSL certificates with a higher trust level are recommended.
- For website URLs being called as a mobile websites or interface, OV SSL certificates and SSL certificates with a higher trust level are recommended.

How should one select a certificate provider?

Choose an appropriate certificate provider based on each SSL certificate’s browser compatibility test report and your enterprise’s business requirements.
For more information, see Browser Compatibility Test Report.

How do I choose a certificate based on the number of supported domain names?

Tencent Cloud provides the following four types of domain names:

- **Single-domain SSL certificate**: Only one domain name can be bound. This can be a second-level domain name like `tencent.com` or a third-level domain name like `example.tencent.com`. However, **sub-domains under the second-level domain are not supported**. The domain name can go down to 100 levels at most.
- **Multi-domain SSL certificate**: A single certificate can be bound to multiple domain names, subject to the maximum number of supported domain names stated on Tencent Cloud's official website.
- **Wildcard Domain**: Supports binding to one and only one wildcard domain, which allows the addition of a single wildcard. For instance, `*.tencent.com`, `*.example.tencent.com` are supported up to 100 levels. Multiple wildcard domains like `.` `.tencent.com` are not supported.
- **Multi-domain wildcard SSL certificate**: Supports binding multiple wildcard domain names, each of which can only include one wildcard, such as `*.tencent.com` and `*.example.tencent.com` (up to 100 levels). Multi-wildcard domain names like `.` `.tencent.com` are not supported.

Can I Apply for an SSL Certificate Before Activating Website Services?

Last updated：2023-10-09 14:54:42

Is it possible to apply for an SSL certificate prior to initiating website services?

You can apply for a paid or free SSL certificate only if you have a domain name and resolution permission.

> ⚠ **Note**
>
> If you apply for a certificate without having purchased cloud service resources, the certificate verification process will not support file validation.

CAA Record

Last updated：2023-10-09 14:55:03

What is CAA?

CAA (Certification Authority Authorization) is a control measure designed to reduce the erroneous issuance of SSL certificates, approved by the Internet Engineering Task Force (IETF) and listed as the IETF RFC6844 standard. In March 2017, the CA/Browser Forum passed proposal number 187, mandating that CA institutions implement compulsory CAA checks from September 8, 2017.

How Does CAA Work?

The domain name holder can set the CAA record to authorize a specific CA to issue an SSL certificate for it. The CA will mandatorily check the domain name’s CAA record under the regulations. If it’s not authorized, CA will reject issuing an SSL certificate for it to avoid certificate misissuance and security risks.

Note

- If a CAA record is not configured for the domain, any CA can issue an SSL certificate for this domain.
- If your domain is hosted with DNSPod, see CAA Record for specific operations.
- If a CAA record for a non-Tencent Cloud CA has been added to the domain you're applying for, the certificate cannot be issued normally. Before validating the domain, please check whether a CAA record has been added. If it has, please delete it before proceeding with domain validation.

Related to SSL Certificate Application

Common reasons for certificate issuance failure

Last updated：2023-10-09 14:55:53

What are the common reasons for certificate issuance failure?

1. The current domain has a CAA record.

The domain name holder has set a CAA record to authorize a specific CA to issue an SSL certificate. The CA, in compliance with the domain's CAA record, will refuse to issue an SSL certificate for the domain if it finds that it has not been authorized.

Solution

The domain name holder should go to the domain name resolution platform to delete the CAA record or add the certificate CA organization name to the CAA record. After the operation is completed, reapply for the certificate.

> ⚠ **Note:**
> Using the **GitHub Page** service to CNAME the domain to the github.io domain will synchronously reference the CAA policy of github.io, **thereby affecting** the issuance of the certificate. For this special situation, you can pause the CNAME record before issuing the certificate, or add trust-provider.com, globalsign.com, and sectigo.com to the CAA record.

> ⓘ **Note:**
> **What is a CAA record?**
> CAA (Certification Authority Authorization) is a control measure to reduce the misissuance of SSL certificates. Since September 8, 2017, CA organizations have strictly enforced mandatory CAA checks when issuing SSL certificates. Domain administrators can set CAA records in domain name resolution.

2. In file validation mode, the domain's website does not support access from outside the mainland.

The website bound to the certificate restricts access from overseas IP addresses. As the CA of international certificates are generally overseas organizations, they are unable to conduct file scanning reviews, leading to certificate issuance failure.

Solution

Ensure that the website port number is set to 80 or 443, and all regions can match the validation value. If your server restricts access from outside, you need to add the CA organization's IP to the access whitelist. After the certificate is issued or the domain name information is approved, the files and directories can be cleared.

> ⓘ **Note:**
> **Common IP of CA organization:**
> **91.199.212.132、91.199.212.133、91.199.212.148、91.199.212.151、91.199.212.176、54.189.196.217**

3. The certificate application involves high risk and has undergone manual review.

The certificate you applied for did not pass the risk control system check of the certificate issuing authority. Possible reasons include the bound domain name is suspected of involving industry brands, industry trademarks, prohibited words, and other risk control sensitive words. Therefore, the certificate has entered the manual review stage (not reviewed by Tencent Cloud).

Solution

Please patiently wait for the results of the manual review, if it does not pass, you can change the domain name and reapply. If you cannot change the domain name, you can choose to purchase Organization Validation (OV) or Extended Validation (EV) certificates. OV/EV certificates will undergo enterprise information review, and the certificate can be issued normally after passing the review.

Why does the order status remain unchanged despite receiving a notification from the CA institution?

During the review of your information and the issuance of your certificate, the CA may send an email to keep you updated on the progress of your certificate application. If you notice that the order status in the Tencent Cloud SSL Certificate Service Console remains unchanged, it could be due to a delay in the CA's update to Tencent Cloud. It is recommended that you patiently wait for a while to see the change in the order status.

Quota of Free SSL Certificates

Last updated：2023-10-09 14:58:14

How many free certificates can I apply for from Tencent Cloud?

Previously, individual accounts could only apply for a maximum of 20 free certificates. Now, individual accounts can apply for up to 50 free certificates (of which 20 free certificates support binding to domain names across the internet, and 30 free certificates can be bound to Tencent Cloud domain names). Becoming a Tencent Cloud V2 member can increase the quota for binding to domain names across the internet. If you wish to become a member, please proceed to Claim Tencent Cloud Membership.

Authentication Type	Account Type	Number of Free Certificates	Can be bound to Tencent Cloud domain names	Can bind any domain name
Individual	Standard/V1 Member Account	50 certificates	30	20
	V2 Member Account	50 certificates	50 (can be bound to any domain name)	
Enterprise	Standard/Membership Account	10	10 (can be bound to any domain)	

Note:

- Tencent Cloud Domains: Domains registered or transferred to Tencent Cloud platform.
- Any Domain: Domains registered on other cloud platforms (including Tencent Cloud domains)
- Quota Deduction Rules: If you apply for a certificate and the domain belongs to Tencent Cloud, one Tencent Cloud domain quota will be deducted first. If the Tencent Cloud domain quota is insufficient, the quota for domain names across the internet will be deducted. When binding to a domain name across the internet, one quota for domain names across the internet is directly deducted. If the quota for domain names across the internet is insufficient, it will not be possible to bind to a domain name across the internet.

What are the quota restrictions for free certificates?

Quota Name	Details	Release Rule
Tencent Cloud Account Quota	The maximum number of free certificates that can be applied for by a Tencent Cloud account (for specifics, please refer to How many free certificates can I apply for from Tencent Cloud)	The quota is released after the certificate is revoked or expires normally (deletion of the certificate does not release the quota).
Primary Domain Quota	A maximum of 20 subdomains can be bound under the same primary domain.	Quota is replenished after normal expiration (revocation or deletion of certificates does not replenish quota)

How is the quota of free certificates under a Tencent Cloud account replenished?

The quota of free certificates under a Tencent Cloud root account will be replenished within 24 hours after the certificates have been revoked or have expired normally.

How is the quota of free certificates under a primary domain replenished?

The quota of the primary domain occupied is released only after the normal expiration of the certificate (active revocation or deletion of the certificate will not release the primary domain quota). If the certificate is actively revoked before expiration, it will occupy the quota for 15 months, and a primary domain quota will only be released after 15 months.

> ⚠ **Note:**
> - A maximum of 20 free DV SSL certificates can be applied for under the same primary domain. Applying for the same primary domain's TrustAsia free DV SSL certificates on other platforms will also occupy the 20 free slots for the same primary domain.
> - Second-level domains and their subdomains all belong to the same primary domain. For instance, tencent.com, ssl.tencent.com, and ssl.ssl.tencent.com all fall under the same primary domain.

What is the difference between a free SSL certificate and an official SSL certificate?

> ⚠ **Note:**
> The compatibility of an official certificate is superior to that of a free certificate. For the stability of your business, it is imperative to use an official certificate for formal projects. Click here to select and purchase an official certificate.

Certificate Features	Free Certificate	Official Certificate
Domain Quota	Subject to Quota Limitations	No limit
Certificate Provider	-	• SecureSite（DigiCert） • DNSPod • GeoTrust • GlobalSign • TrustAsia • WoTrus
Supports binding to wildcard domains (wildcards)	Unavailable	This feature is supported.
Support binding IP	Unavailable	This feature is supported.
Multi-domain	Unavailable	This feature is supported.
Installation Consultation Services	Unavailable	This feature is supported.
After-sales service	Unavailable	This feature is supported.

What should I do if I am unable to apply for an SSL certificate, verify a domain name, or if my information fails to pass the review?

Last updated：2023-10-09 16:15:10

"What should I do if I am unable to apply for a certificate, verify a domain name, or if my information fails to pass the review?"

"If you urgently need guidance on any operations related to certificate selection, domain name verification for the certificate, or the certificate installation process, you can go to the Tencent Cloud Marketplace to purchase relevant certificate services."

Wildcard SSL Certificates

Last updated：2023-10-09 16:15:42

What domain names are supported by wildcard certificates?

Tencent Cloud SSL certificates can be wildcard certificates. A wildcard certificate can secure a single server domain name and all the sub-domain names of the same level.

- A wildcard certificate covers all sub-domain names of the same level. For example, both `*.tencent.com` and `*.cloud.tencent.com` are wildcard domain names.
- Currently, wildcard certificates only support wildcard domain names and do not support regular domain names (non-wildcard domain names). If you need a certificate that can include multiple wildcard domain names, it is recommended to purchase a multi-domain wildcard type SSL certificate.

What are the rules for matching a wildcard certificate with a domain name?

A wildcard certificate can only match sub-domains of the same level and cannot match across levels. For instance, the third-level wildcard domain `*.tencent.com` does not support the fourth-level domain `www.ssl.tencent.com`.

Why can't I use file verification when applying for wildcard certificates?

From December 1, 2021, file validation supports only issuing the SSL certificate for the current validated domain, but not wildcard SSL certificates as well as its subdomains. For more information, please see Domain Validation Policy Update.

Why Does the Order Status Not Changed After a Notification Email Is Received from a CA?

Last updated：2023-10-09 16:15:56

Why does the order status remain unchanged despite receiving a notification from the CA institution?

During the review of your information and the issuance of your certificate, the CA may send an email to keep you updated on the progress of your certificate application. If you notice that the order status in the Tencent Cloud SSL Certificate Service Console remains unchanged, it could be due to a delay in the CA's update to Tencent Cloud. It is recommended that you patiently wait for a while to see the change in the order status.

Can the TXT Records for Domain Name Resolution Configured in the Certificate Be Deleted?

Last updated：2023-10-09 16:16:10

Can the TXT records for domain name resolution configured in the certificate be deleted?

After an SSL certificate is issued, you can delete the TXT records for domain name resolution configured in the certificate. This has no impact on the certificate.

What is CSR?

Last updated：2023-10-09 16:16:43

What is CSR?

CSR, or Certificate Signing Request, is a prerequisite for obtaining an SSL certificate. It necessitates the generation of a CSR file, which must then be submitted to a Certificate Authority (CA). The CSR comprises a public key for certificate issuance, a distinguished name for identification (such as a domain name), and safeguards for authenticity and integrity (such as a digital signature). Typically, a CSR is generated from a web server, concurrently creating a pair of public and private keys for encryption and decryption.

During the creation of a CSR, pertinent organizational information must be provided. The web server will utilize this information to create a distinguished name for the certificate, serving as its identifier. The organizational information encompasses the following:

Country or region code

The code of the country or region where your organization is legally registered, represented in the two-letter format prescribed by the International Organization for Standardization (ISO).

Province, city, or autonomous region

The province, city, or autonomous region where your organization is located.

City or region

The city or region where your organization is registered.

Organization

The legally registered name of your enterprise.

Departments within the organization

This field is used to differentiate departments within an organization, such as "the engineering department" or "the human resources department".

Common Name

The name entered in the Common Name field of the CSR must be the Fully Qualified Domain Name (FQDN) of the website for which you intend to use the certificate, for example, "www.domainnamegoeshere".

However, Tencent Cloud generates CSR online without you having to generate and submit CSR files. To apply for a domain validation certificate, you simply need to submit a common name.

How does one create a CSR file?

This document provides guidance on how to create a Certificate Signing Request (CSR) file.

Preparations

Before applying for a digital certificate, you need to prepare the key files and CSR file for the certificate. The CSR file is the original file of your public key certificate, containing your server information and your organization's information, which needs to be submitted to the CA for review. It is advisable to use the CSR file created by the system to avoid review failure due to incorrect input information. If you choose to manually generate the CSR file, please ensure to properly store and back up your key files. Pay attention to the following information when manually generating the CSR file:

- The Chinese information entered must be in UTF-8 encoding format. Please specify support for UTF-8 encoding format when editing with the OpenSSL tool.
- The certificate service system imposes stringent requirements on the key length of the CSR file. The key length must be 2048 bits, and the key type must be RSA.
- If you are applying for a multi-domain or wildcard subdomain certificate, you only need to enter one domain name in the "Common Name" or "What is your first and last name?" field.

Generate a CSR file using the OpenSSL tool.

1. Log into a local computer or server running the Linux operating system.
2. Install the OpenSSL tool. For more details, refer to How do I install OpenSSL?
3. Execute the following command to generate a CSR file.

```
openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout [$Key_File] -out [$OpenSSL_CSR]
```

> **Note**
> - **New**: Specifies the creation of a new CSR file.
> - **nodes**: Specifies that the key file should not be encrypted.
> - **SHA256**: Specifies the digest algorithm.
> - **newkey rsa:2048**: Specifies the type and length of the key.
> - **[$Key_File]**: Name of the key file.
> - **[$OpenSSL_CSR]**: The storage path for the encrypted file. **New**: Specifies the creation of a new CSR file.

4. In accordance with the system's prompts, input the information required to generate a CSR file. The following are explanations of these prompts:
   - **Organization Name**: The name of the company, which can be in either Chinese or English.
   - **Organizational Unit Name**: The name of the department, which can be in either Chinese or English.
   - **Country Code**: The country to which the applying entity belongs, represented solely by a two-letter country code. For instance, Mainland China is denoted as CN.
   - **State or Province Name**: The name of the state or province, which can be in either Chinese or English.
   - **Locality Name**: The name of the city, which can be in either Chinese or English.
   - **Common Name**: The specific website domain for which the SSL certificate is being applied.
   - **Email Address**: Optional, may be left blank.
   - **Challenge Password**: Optional, may be left blank.
5. Upon entering the corresponding content as prompted by the command, you can obtain the key file and CSR file in the current directory.

What Is Private Key Password?

Last updated：2023-10-09 16:17:22

What is the private key password for an SSL certificate?

An SSL certificate employs public key encryption and symmetric encryption to secure data transmission between the client and server, ensuring the confidentiality, integrity, and authenticity of the communication. The exposure of an SSL certificate's private key can lead to the leakage of encrypted session keys, thereby posing a risk of website data leakage. The private key password for an SSL certificate serves to add an additional layer of protection to the private key, enhancing and ensuring its security.

When you apply for a Tencent Cloud SSL certificate, Tencent Cloud provides you with the option to specify a private key password. If you provide a private key password, the private key file in the issued SSL certificate will be protected using the password you provided. If you do not provide a password, Tencent Cloud will auto-generate one for you. The private key password file will be included in the download package, for instance, in the `keystorePass.txt` file.

When will I use a private key password?

Typically, you will use the private key password when installing and deploying an SSL certificate to a web service. For instance, when installing and deploying an SSL certificate on a Tomcat server, the `keystorePass=` field that needs to be filled in is the private key password.

What should I pay attention to regarding a private key password?

- If you select to fill in a private key password when applying for a Tencent Cloud SSL certificate, set a complex one.
- Safeguard your private key password diligently to prevent its disclosure from compromising the security of your SSL certificate.
- Keep your private key password confidential. Tencent Cloud will not store your private key password.

What do I do if I forgot the private key password?

Tencent Cloud does not keep your certificate private key password. Please remember your password.

If you forgot your private key password, you can:

- Reissue Certificate: If you lose your private key password, you can regenerate a certificate through the reissuance operation. For more details, please refer to the SSL Certificate Reissuance Guide.

  > **Note**
  > The reissued certificate needs to be deployed again. The effective period will be the same as that of the original one.

- Reapply for a certificate: If your private key password is lost, you may choose to reapply for a certificate.
  - For information on how to apply for a free certificate, please refer to the Application Process for Free DV SSL Certificates.
  - For more information about applying for a paid certificate, please see Purchasing Process.

Why do I frequently receive SSL Certificate Service upgrade notifications?

Last updated：2023-10-09 16:17:42

Notification Background

Tencent Cloud SSL Certificates support automatic deployment to various Tencent Cloud products and allow querying of certificates associated with different cloud products. Access to resources under a user's Tencent Cloud account for SSL Certificates is obtained through Cloud Access Management (CAM). For each function on the SSL Certificate console (automatic deployment/certificate update/certificate hosting, etc.), a new access authorization is required for each newly accessed cloud product. As this involves changes to the role permissions of the account, we will notify existing authorized users about these changes.

> **Note:**
> **No action is required from the user regarding the service upgrade notification for role permission changes, and it does not affect the SSL Certificate operations.**

Notification Format

Message Center, Email, SMS

Notification Audience

Users who have previously authorized SSL Certificates through Tencent Cloud Access Management

Notification Content

The following content is for reference only.

【Tencent Cloud SSL Certificates Service Upgrade Notification】
Dear Tencent Cloud user,
In order to provide you with a more comprehensive service, Tencent Cloud plans to upgrade the Tencent Cloud Certificate (SSL Certificates) service. After the upgrade, SSL certificates can be batch deployed to the Cloud Load Balancer (CLB). No action is required from the customer for this role permission change, and it does not affect the SSL Certificate operations. Details are as follows:
Time: 2023//10:00 - 18:00
Content: To provide enhanced certificate deployment capabilities, it is necessary to add read and write permissions for *resources, based on the original service-related role (SSL_QCSLinkedRoleInReplaceLoadCertificate).
Thank you for your support.

Is the revocation of SSL certificates supported?

Last updated：2023-10-09 16:17:56

Can a certificate be revoked?

Yes, revocation is supported. For the revocation process, please refer to Guidelines for Certificate Revocation.

What should I do if the console prompts that "The certificate is bound to Tencent Cloud resources and cannot be revoked" when I submit an SSL certificate revocation application?

Check whether the target SSL certificate is bound to any Tencent Cloud resources such as CLB and CDN, and if so, unbind them before the revocation.

What Should I Do If the Console Prompts That The Certificate Is Bound to Tencent Cloud Resources and Cannot Be Revoked When I Submit an SSL Certificate Revocation Application?

Last updated：2023-10-09 16:18:16

What should I do if the console prompts that "The certificate is bound to Tencent Cloud resources and cannot be revoked" when I submit an SSL certificate revocation application?

Check whether the target SSL certificate is bound to any Tencent Cloud resources such as CLB and CDN, and if so, unbind them before the revocation.

What are the differences between RSA and ECC?

Last updated：2023-10-09 16:18:48

What are the differences between the RSA and ECC encryption algorithms?

- RSA (Rivest-Shamir-Adleman) encryption algorithm: An international standard algorithm and one of the earliest to be applied. It has a broader universality compared to the ECC algorithm, with a wider range of applicability and better compatibility. It typically employs a 2048-bit encryption length, though it consumes more server performance.
- ECC (Elliptic-curve cryptography): A new mainstream algorithm. It is normally 256 bits in length (a 256-bit ECC key is equivalent to a 3072-bit RSA key), making it securer and able to offer stronger anti-attack capabilities. Moreover, the computation of ECC is faster than RSA, and thus it offers higher efficiency and consumes fewer server resources.

Differences between these two encryption algorithms are described as follows:

Comparison Item	ECC	RSA encryption
Key length	256 bits	2,048 bits
CPU usage	Less	Higher
Memory usage	Less	Higher
Network Usage	Less	Higher
Encryption Efficiency	Higher	Average
Resistance to Attacks	Stronger	Average
Compatibility Range	Supports new browsers and OS (some platforms such as cPanel are not supported)	Supports all

What’s the difference between certificate reissue and reapplication?

Last updated：2023-10-09 16:19:03

What’s the difference between certificate reissue and reapplication?

The difference mainly lies in whether the certificate is generated based on the original order.

- Reissued certificate: The expiration date will not be changed. Regardless of whether the certificate is free or paid, you cannot modify the domain name bound with it.
- Reapplied certificate: You can modify the certificate information. Reapplying for a free certificate will generate a new one and will use up another free tier. Reapplying for a paid certificate does not require additional payment, but you will need to resubmit information on the original certificate (only available if the review fails).

Which SSL Certificate Types Are Supported for Mini Programs?

Last updated：2023-10-09 16:19:22

Which SSL certificate types are supported for mini programs?

All certificates except Chinese SM ones are supported for mini programs.

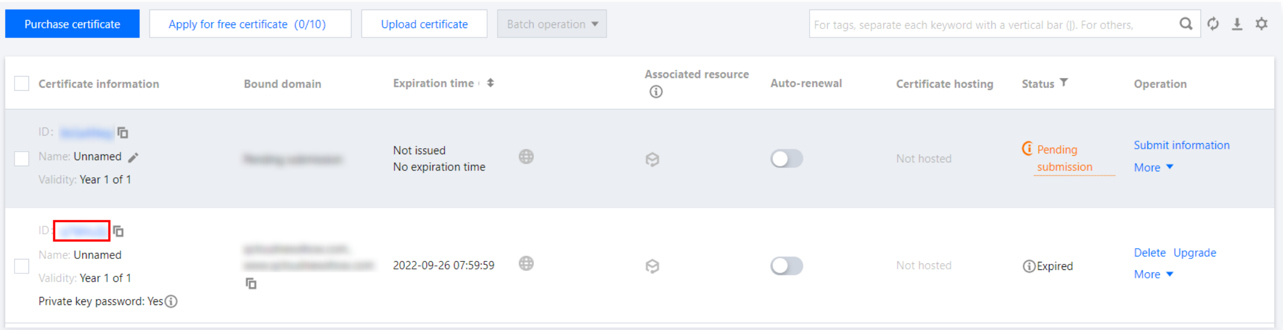
SSL Certificate Management

How do I view the certificate information?

Last updated：2023-10-09 16:26:21

How do I view the certificate information?

1. Log in to the Tencent Cloud SSL Certificate console, navigate to the **My Certificates** page, and click on the desired **Certificate ID** as shown in the figure below:

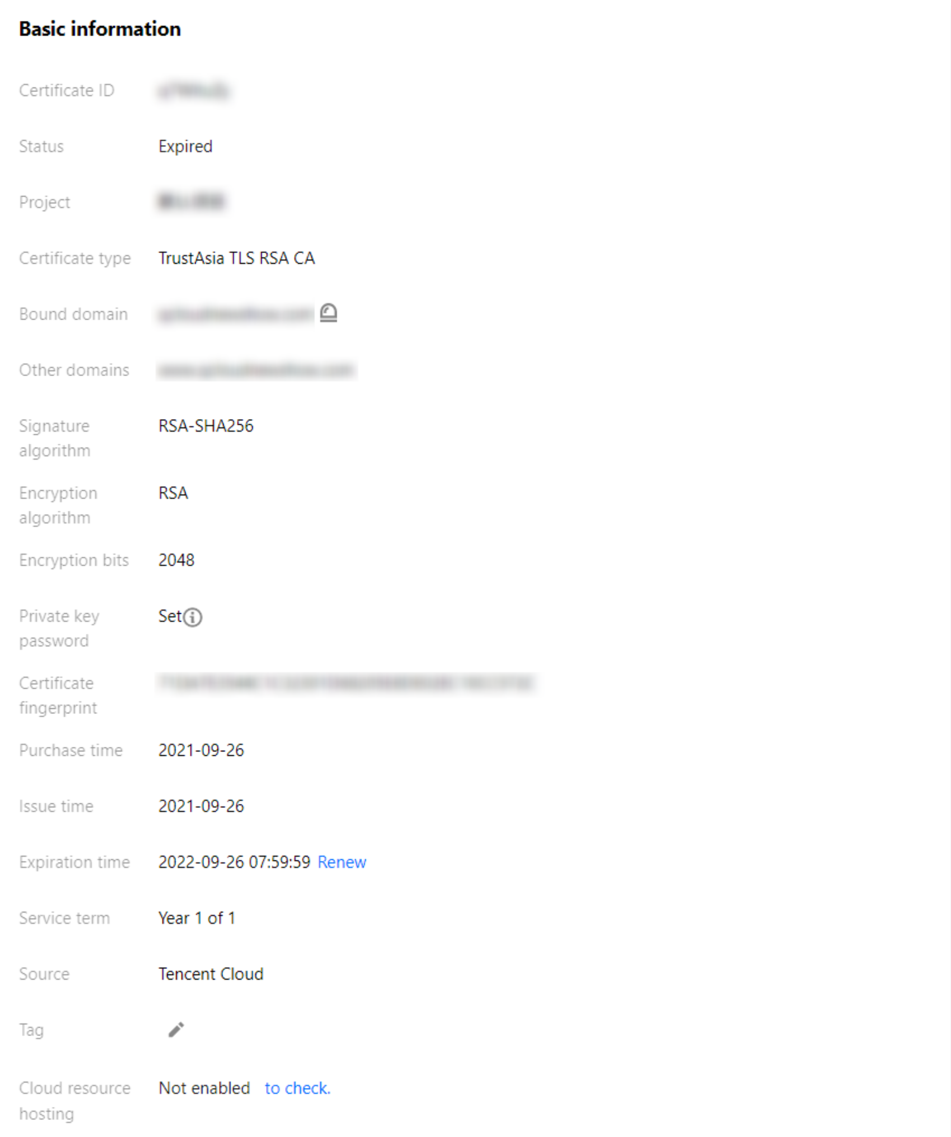


Purchase certificate
Apply for free certificate (0/10)
Upload certificate
Batch operation
For tags, separate each keyword with a vertical bar (|). For others,

□ Certificate information	Bound domain	Expiration time		Associated resource	Auto-renewal	Certificate hosting	Status	Operation
□ ID: [redacted] Name: Unnamed Validity: Year 1 of 1	[redacted]	Not issued No expiration time			○	Not hosted	Pending submission	Submit information More
□ ID: [redacted] Name: Unnamed Validity: Year 1 of 1 Private key password: Yes	[redacted]	2022-09-26 07:59:59			○	Not hosted	Expired	Delete Upgrade More

> **Note**
> If you are using the card-style console, you can directly click on the certificate card.

2. On the certificate details page, you can view the basic information of the certificate, including the certificate type, expiration date, and other details, as shown in the figure below:



Basic information

Certificate ID	[redacted]
Status	Expired
Project	[redacted]
Certificate type	TrustAsia TLS RSA CA
Bound domain	[redacted]
Other domains	[redacted]
Signature algorithm	RSA-SHA256
Encryption algorithm	RSA
Encryption bits	2048
Private key password	Set ⓘ
Certificate fingerprint	[redacted]
Purchase time	2021-09-26
Issue time	2021-09-26
Expiration time	2022-09-26 07:59:59 Renew
Service term	Year 1 of 1
Source	Tencent Cloud
Tag	
Cloud resource hosting	Not enabled to check.

What should I do if the quick HTTPS plan will expire soon?

Last updated：2023-10-09 17:41:11

What should I do if the quick HTTPS plan will expire soon?

If you wish to continue using the Quick HTTPS feature, you can renew or upgrade it on the SSL Certificate Service Console. For more details, please refer to the Quick HTTPS Renewal Process.
If you no longer wish to continue using the service, it is recommended to switch the domain name resolution to the source station before the Quick HTTPS package expires to avoid any disruption to normal access. If your domain name is resolved in DNSPod, you may follow the steps below:

1. Log in to the DNSPod Console.
2. Click on the **domain name** you have connected with Quick HTTPS to enter the "Record Management" page.
3. Find the CNAME record type of the access domain name and modify the record value to your source station address

> ⚠ **Note**
> If your source station address is an IP address, please change the record type to an A record and fill in your source station IP address in the record value field.

4. Click OK to complete the configuration.

My Profile

Last updated：2023-10-09 17:50:15

What should I do if I don't know where to modify an organization profile?

Currently, the organization profile of an SSL certificate cannot be modified or deleted; therefore, we recommend that you create a new one for review.

How many instances can be created in my profile?

Up to 10 organization profiles can be added. If you need to add more, contact us .

How long does it take to complete the review after submitting the organization profile?

The review is generally completed within one business day. Be sure not to miss the call from the CA.

> ⚠ **Note**
> Due to a high volume of review requests, the CA may be busy and will prioritize the review of organization profiles related to paid certificate applications.

SSL Certificate Review

How Long Will the Certificate Review Takes?

Last updated：2023-10-10 14:11:20

If the materials submitted to apply for an SSL certificate involve human review, you will need to wait for the review to complete. The time needed for each type of certificate is as follows:

Note

Since DV certificates do not require a manual review process, the CA typically issues the certificate as soon as it detects successful domain validation.

Certificate type	Period
DV certificate	-
OV certificate	3-5 business days
EV certificate	5-7 business days

What are the causes for the Security Audit failure?

Last updated: 2023-10-10 14:18:11

What are the reasons for the failure of the Security Audit?

When applying for a DV SSL certificate, if you encounter the following message, it indicates that the security review of the application domain has failed, **The rapid review process of SecureSite CA does not support the issuance of DV SSL certificates for this domain.** Please purchase a paid certificate.
The message is as follows:

```
Apologies, but this domain has failed the security review by the Certificate Authority (CA) and cannot be
used to apply for a Domain Validation (DV) certificate. Please consider purchasing an Organization Validation
(OV) or Extended Validation (EV) certificate, or you may try applying with a different domain.
```

Specific reasons for the failure of the security review:
Due to the anti-phishing mechanism of the Certificate Authority (CA), the domain information may contain sensitive words such as 'bank', 'pay', etc., which can lead to a failed security review. The specific sensitive words are defined by the CA. Additionally, some less commonly used top-level domains may also fail the review, for instance, domains with a .pw suffix like `www.qq.pw` , `www.qcloud.pw` cannot pass the review.
The following are examples of sensitive words in domain names that may lead to failure. The specific list is defined by the CA:

Private/Public IP	Host name	live (excluding the .live top-level domain name)	bank
banc	alpha	test	example
credit	pw (excluding the .pw top-level domain name)	apple	ebay
trust	root	amazon	android
visa	google	discover	financial
wordpress	pal	hp	lv
free	scp		

Note
DV SSL certificates are issued quickly through automatic validation, without manual intervention. A more stringent set of sensitive words is used to enhance the review standards.

What should I do if the domain fails the security review?

If the order review for a free DV digital certificate fails, it is generally due to the presence of sensitive words in the domain name. You can proceed as follows:

- Bind your domain by purchasing a premium digital certificate.
- After utilizing this free certificate, associate it with other domains that do not contain sensitive words.

What should I do if a free SSL certificate is always in Pending validation status?

Last updated：2023-10-10 14:14:14

What should I do if the free certificate remains unverified?

The free certificate has a self-diagnostic feature. If it remains in the verification pending status, you can independently check the domain verification status through the prompts on the certificate's detail page. After verification, please be patient as the update of the certificate status takes some time. The certificate is typically issued within 10 minutes to 24 hours.

Causes and Handling Methods for Certificate Review Failures

Last updated：2023-10-10 14:17:37

Causes and Handling Methods for Certificate Review Failures

This document describes the possible causes of and solutions for certificate review failures.

Verification file configuration error

> **Note**
> It is recommended that you execute the `curl -k -v` command or the `wget -S` command to verify whether the file URL is effective. Additionally, you need to validate the URLs for both HTTPS and HTTP protocols separately.

- **Possible Causes:**
  If you use the file verification method for domain verification when submitting an SSL certificate review, this issue may cause the order review to fail. The possible causes for the failure of the SSL certificate review application in this scenario are as follows:
  - Some pages of the site have enabled HTTPS access, but the verification file is only deployed under the HTTP service path and not under the HTTPS service path. This leads to the corresponding file not being found when requested via the HTTPS protocol.
  - The site returns an error code when accessing the verification file.
  - CDN service has been enabled, but the CDN service node has not completed overseas synchronization.
- **Solution:**
  - Deploy the verification file under the HTTP and HTTPS service paths, ensuring it can be accessed via the HTTPS protocol. Alternatively, temporarily disable the HTTPS service for all pages on the site.
  - Ensure that the correct validation file content can be directly accessed through the validation file URL specified by the CA center, and confirm that the final validation file is not displayed in the web browser through redirection or other means.

    > **Note**
    > Check whether the browser address has changed to determine whether you have been redirected.

  - Synchronize the verification file to the overseas CDN service node, or temporarily disable the CDN overseas acceleration service.

    > **Note**
    > If modification operations cannot be performed on the CDN servers, we recommend using DNS verification for domain verification instead.

DNS configuration error

- **Possible Causes**
  If you use the DNS verification method for domain verification when submitting an SSL certificate review, this issue may cause the order review to fail. Some possible reasons for the failure of the SSL certificate review application in this scenario are as follows:

  - The DNS record value is incorrectly configured.
  - When using the services of some domain name resolution service providers, the return value for queries of non-existent host records differs from the expected return value. This leads to inaccurate return values during validation by the certificate authority center.
  - DNS record timeout. After submitting your application, you have three natural days to complete the addition of the DNS record. Otherwise, the review will fail.
  - The dynamic domain name resolution service has been enabled, but the corresponding resolution record value has not been timely synchronized to the overseas authoritative DNS server.
- **Resolution**
  - Configure the correct DNS host record and record value.
  - Ignore the errors related to domain resolution settings, configure the DNS resolution record as required, and complete the domain verification.
  - Resubmit your application and complete the addition of the DNS record within three natural days.
  - Please ensure that the dynamic resolution service is functioning properly, and that overseas resolution services can correctly parse the newly added DNS records.

  > **Note**
  > When modifying an existing record value, the time it takes for the DNS record value to take effect is determined by the TTL value, whereas new record values can take effect quickly. Therefore, it is recommended that you complete the verification by adding new record values. Once the domain verification is passed, you can delete the relevant DNS record information.

Empty or invalid company phone number

For OV and EV SSL certificates, if you leave the company phone number field empty or set it to an invalid phone number when submitting the certificate order for review, the review will fail.

- **Reason for the issue**
  For OV and EV type certificate products, the company's phone number is a mandatory field. If the company's phone number is left blank or does not comply with the rules, it needs to be filled out again.
- **Solution**
  Please provide a business phone number that can reach you promptly to ensure that you can be contacted during the organization information verification by the CA center.

CSR file already used in other orders

- **Reason for the issue**
  For the sake of certificate key security, when requesting a brand new order, it is not permissible to use previously utilized CSR information.
- **Solution**
  If you have previously successfully submitted an order using a CSR file, please generate a new CSR file for subsequent new orders. Ensuring that each SSL certificate has its unique key pair will enhance the security of the certificate application.

Incorrect format of the domain name bound with the certificate

- **Possible Cause**
  A valid domain name can only contain any combination of **letters, numbers, and "-"**, and the maximum length of the domain name must not exceed 64 characters.
- **Solution**

Please check the domain information in the CSR request file and the order, and ensure that you have used the correct domain to submit the order.

Empty or incorrect primary domain name

- **Possible Cause**
  The `Common Name` field was not correctly filled out when creating the CSR file.

  > **Note**
  > The `Common Name` must be one of the domain names bound to the certificate.

- **Solution**
  We suggest you use the system's feature to generate a CSR file online.

Domain name security review failure

When you apply for an SSL certificate, you may receive a review failure message.
The message content is similar to the following:

```
Apologies, but this domain has failed the security review by the Certificate Authority (CA) and cannot be
used to apply for a Domain Validation (DV) certificate. Please consider purchasing an Organization Validation
(OV) or Extended Validation (EV) certificate, or you may try applying with a different domain.
```

- **Possible Causes**
  Due to the anti-phishing mechanism of the CA, domain information containing sensitive words, such as 'bank', 'pay', etc., can cause a security review failure. The specific sensitive words are defined by the CA. Additionally, some uncommon root domain names may also fail the review. For instance, domain names with a .pw root domain suffix, such as `www.qq.pw` , `www.qcloud.pw` , cannot pass the review.
  The following are examples of sensitive words in domain names that may cause a failure. The specific words are defined by the CA:

Private/Public IP	Host name	live (excluding the .live top-level domain name)	bank
banc	alpha	test	example
credit	pw (excluding the .pw top-level domain name)	apple	ebay
trust	root	amazon	android
visa	google	discover	financial
wordpress	pal	hp	lv
free	scp	-	-

- **Solution**
  It is suggested to change the hostname part of the domain and try to resubmit the order. If the above error still occurs after multiple changes to the hostname, it is recommended to choose a paid certificate product, or to change the main domain for certificate application.

  > **Note**

> Because DV SSL certificates are quickly issued through automatic authentication without manual intervention, we use stringent sensitive words filters to set the verification standard.

What Should I Do After Submitting the Order for Review for a Purchased Certificate?

Last updated：2023-10-10 14:18:39

What should be done after submitting the application for review of a purchased certificate?

Upon acquiring an SSL certificate, it is requisite to apply for the certificate and forward it for evaluation. Only after the successful completion of the review, the certificate can be utilized and integrated into your Tencent Cloud service resources.

When you purchase a paid certificate and submit it for review, the staff from the Certificate Authority (CA) will reach out to you to confirm the relevant information for the certificate review. It is crucial to keep your mobile phone (the number provided during the review submission) accessible at all times and regularly check your email (the email address provided during the review submission) to avoid missing any confirmation notifications from the CA.

After submitting a certificate order for review, log in to the SSL Certificate Service console to check the review status and subsequent processes in the certificate list. After a certificate order is submitted for review, it can be in either of the following states:

- **Under Verification:** When the certificate application is in a pending verification state, click on **Certificate Details** to view the domain verification method on the certificate details page. After completing the verification, wait for the certificate status to change to **Issued** before using the certificate.

> **Note**
> For more information on domain verification methods, please refer to the Domain Validation Guide.

- **Review Failed:** If the certificate review fails, click on **Certificate Details** to go to the certificate details page and identify the reason for the failure. Modify the certificate application information based on the failure reason. Once the modifications are complete, you need to resubmit the application.

How long does it take for different certificate types to be issued?

- **OV and EV certificates:** it takes 3-5 business days to issue an OV certificate and 5-7 business days to issue an EV certificate.
- **DV or free certificates:** it takes between 10 minutes and 24 hours to issue a DV certificate.

> **Note**
> Free certificate applications will be issued within one natural day. Due to varying processing times at the Certificate Authority (CA) center, your certificate may be issued within a few hours, or it may take up to one natural day. We appreciate your patience during this process.

How Do I View the Domain Validation Result of a DV SSL Certificate?

Last updated：2023-10-10 14:21:52

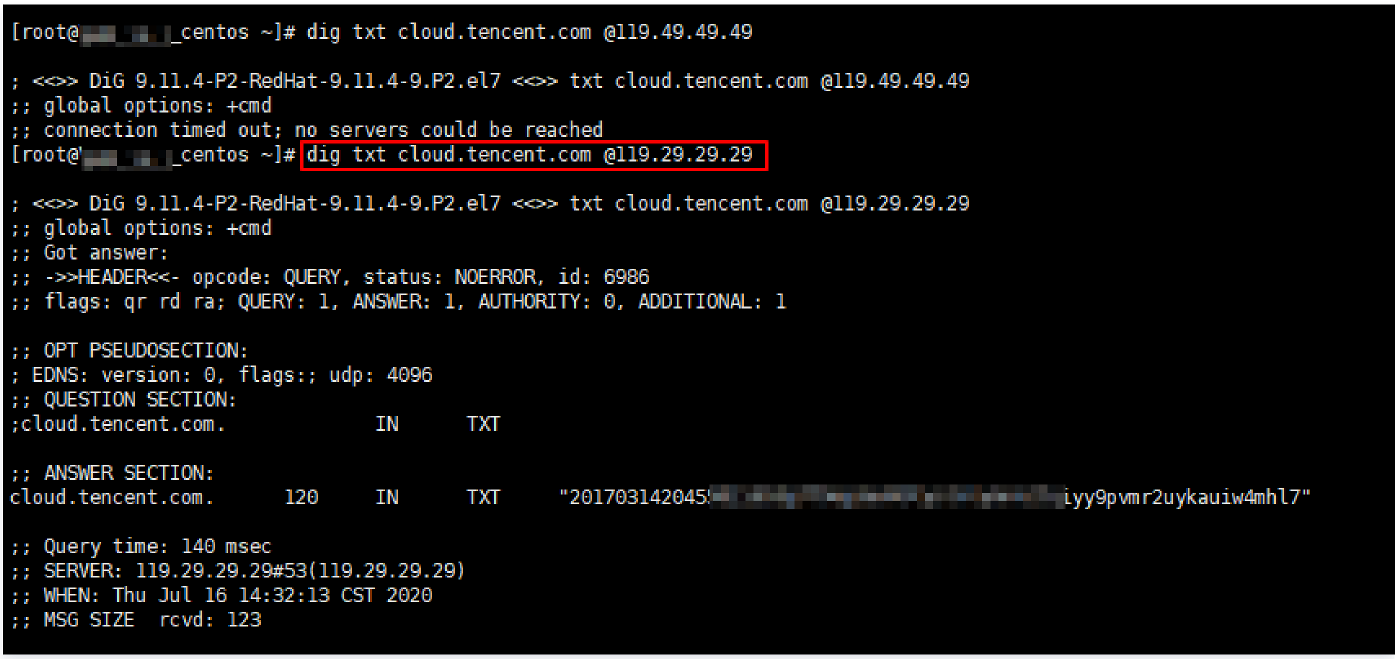
How do I view the domain validation result of a DV certificate?

Upon submission of your certificate application, the Certificate Authority (CA) will conduct a review of your domain and the information provided. Only after successful domain validation will the CA issue the certificate. If your certificate remains unissued, it is advisable to verify the domain validation result based on the following content.

> **Note**
> The host records provided by Tencent Cloud SSL Certificate Service are fully qualified domain names. If your domain management system does not support fully qualified domain name host records, please remove the suffix part of the root domain.

DNS Validation Type

1. Please log into your domain server and execute the dig command to query the DNS resolution of the domain.
2. Execute the `dig + record type + @119.29.29.29` command to specify the use of DNSPod's DNS for validation. For instance, `dig txt cloud.tencent.com @119.29.29.29`



```
[root@[redacted]_centos ~]# dig txt cloud.tencent.com @119.49.49.49

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-9.P2.el7 <<>> txt cloud.tencent.com @119.49.49.49
;; global options: +cmd
;; connection timed out; no servers could be reached
[root@[redacted]_centos ~]# dig txt cloud.tencent.com @119.29.29.29

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-9.P2.el7 <<>> txt cloud.tencent.com @119.29.29.29
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6986
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cloud.tencent.com.             IN      TXT

;; ANSWER SECTION:
cloud.tencent.com.      120     IN      TXT     "201703142045[redacted]iyy9pvmr2uykauiw4mhl7"

;; Query time: 140 msec
;; SERVER: 119.29.29.29#53(119.29.29.29)
;; WHEN: Thu Jul 16 14:32:13 CST 2020
;; MSG SIZE  rcvd: 123
```

- If the returned results contain a TXT record similar to the one shown in the illustration, and the record value matches the record value on the certificate details page in the certificate console, it indicates that your DNS configuration is correct and has taken effect.
- If the returned result does not contain a TXT record, it may be due to an error in the DNS configuration or the configuration has not taken effect. If the DNS configuration is incorrect, please log in to the SSL Certificate Service Console, click on the **Pending Verification** tab, and enter the details page of the certificate. Copy the record value from the certificate details and update the resolution at your DNS domain name resolution service provider. If the configuration does not take effect for a long time, please contact your domain hosting provider.

> **Note**
> For detailed directions, see DNS Validation.

File Validation Type

1. Please log in to the SSL Certificate Service Console, click on the **Pending Validation** tab, and enter the details page of the certificate.
2. Click to visit the validation URL. If the content displayed on the accessed page matches the validation file content on the certificate details page, it indicates normal access. If they do not match, please focus on checking the following aspects:
   - Check whether the validation URL already exists as an accessible HTTPS address. If it does, please re-access it using the HTTPS address in your browser. If the browser indicates "Untrusted Certificate" or displays incorrect content, please temporarily disable the HTTPS service for this domain.
   - Ensure that the validation URL can be correctly accessed from any location. As each brand certificate has different detection server regions, please confirm whether your site has overseas mirrors, or whether intelligent DNS services are being used, among other factors.
   - File validation requires a direct response with a 200 status code and file content, and does not support any form of redirection. Check if the validation URL has a 301 or 302 redirect. If such redirects exist, please cancel the relevant settings to disable the redirection.

> **Note**
> You can execute the `wget -S URL` command to check whether the validation URL has a redirect.

SSL Certificate Taking Effect
What should I do if the browser on my computer or mobile phone indicates that the SSL certificate is untrustworthy?

Last updated：2023-10-10 14:24:07

What should I do if the browser on my computer or mobile phone indicates that the certificate is untrustworthy?

This article provides two troubleshooting methods, detailed as follows.

Method 1: Check the Terminal Type

If your computer or mobile browser indicates that the certificate is untrustworthy, please verify the SSL certificate brand you purchased and the terminal type indicating the certificate is untrustworthy. Some brands' digital certificates are not supported on certain terminals. For more details, refer to the Browser Compatibility Test Report.

Method 2: Check the Certificate's Configuration and Deployment

If the SSL certificate is compatible with the terminal, please use the AsiaTrust SSL Status Check digital certificate inspection tool.

- If the certificate brand, certificate type, and domain name in the check results do not match the certificate configuration you purchased, please confirm whether the SSL certificate information installed on the server is correct.
- If the check results show that the certificate chain information is incomplete, please confirm whether the SSL certificate information installed on the server is correct.

> **Note**
> - Check whether the server site's web pages have referenced HTTP resources. In some browsers, HTTPS sites referencing HTTP resources are considered unsafe operations.
> - If a domain name is resolved to multiple servers, please ensure that each server has the certificate correctly deployed.

Is the Original SSL Certificate Still Valid After the Server IP Address Is Changed?

Last updated：2023-10-10 14:24:23

Is the original SSL certificate still valid after the server IP address is altered?

- Should your SSL certificate be tied to a domain name, it remains unaffected by any alterations to the server's IP address. Provided the domain name associated with the certificate remains constant, it can be re-routed to a new IP address, and the original SSL certificate will continue to function as intended, negating the need for a replacement.
- In the event that your SSL certificate is linked to an IP address, it will be impacted by any modifications to the server's IP. It will be necessary to apply for a new certificate, bind it to the new IP address, and deploy it to the server for it to become effective.

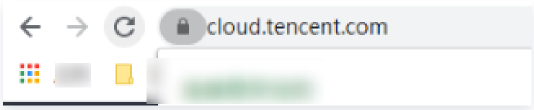
How Do I Check in a Browser Whether an SSL Certificate Has Taken Effect?

Last updated：2023-10-10 14:25:42

How can one ascertain in a browser whether an SSL certificate is operational?

Upon successful installation of the certificate and resolution to the server IP, you may follow the subsequent steps to verify the effectiveness of the SSL certificate:

1. Launch a browser (Chrome is utilized as an illustration in this context), and input the domain address associated with the SSL certificate in the https format into the browser's address bar.
2. Press the enter key to access the domain address. Verify whether the following conditions are met:
   - The domain name address successfully facilitates access to the website.
   - A security lock icon is displayed on the left of the address in the browser address box, which indicates that your SSL certificate has taken effect as shown in the following figure.



What Should I Do If GlobalSign Certificates Are Not Supported in Windows 7?

Last updated：2023-10-10 14:27:39

Example

On May 27, 2019, GlobalSign officially began using a new intermediate CA to sign SSL certificate products. Due to the lack of new root support in the Windows 7 system, websites are not trusted when accessing GlobalSign certificates issued (including updated or reissued certificates) after May 27, 2019, on a Windows 7 system.

Solution

Please use a text editor to open the .crt file in the Nginx directory of the downloaded certificate, and paste the following cross-certificate at the end of the certificate chain. After restarting the Nginx service, the certificate can be used normally.
To download the cross-certificate, please click here.

SSL Certificate Billing and Purchase
Are DV Certificates Permanently Free?

Last updated：2023-10-10 14:29:42

Are DV certificates perpetually complimentary?

Firstly, whether it's a complimentary DV certificate or a paid OV certificate, the CA has set an expiration date. Considering security, it cannot be guaranteed that a legitimate website will never turn into a phishing site. The CA needs to conduct regular audits, hence, it will not issue certificates with perpetual validity.

Secondly, when a website's private key is lost, a revocation can be requested. The CA will add the revoked certificate to the Certificate Revocation List (CRL). Each time an HTTPS site is accessed, the browser will fetch the CRL from the CA to determine whether the certificate can be trusted. However, certificates with perpetual validity would cause the CRL to continuously grow, never decreasing, thereby increasing the request traffic pressure on the browser. Hence, specifying a validity period for the certificate is a more scientifically sound approach.

Currently, Tencent Cloud offers a complimentary DV certificate, model **TrustAsia DV SSL CA - G5**, with a validity period of **1 year**. You can reapply for the certificate **one month** prior to its expiration. DV certificates can be swiftly issued within a single business day, providing you with ample time to transition the certificates for your site.

SSL Certificate Validity Period
What should I do if an SSL certificate is about to expire?

Last updated：2023-10-10 14:30:18

What should I do if an SSL certificate is about to expire?

Once an SSL certificate expires, it becomes unusable. It is essential to renew the certificate before its expiration, rebind it to the domain name, and submit it for review.
Upon approval, you will receive a new SSL certificate. This must be installed on the server to replace the soon-to-expire certificate.

> **Note**
> - If you are using a free Domain Validation (DV) certificate, you will need to reapply. For more information, please refer to Domain Validation (DV) Certificate Application Process.
> - You should allow 3 - 10 business days before the certificate expires to repurchase, to avoid certificate review failure due to expiration. For more information, please refer to Paid SSL Certificate Renewal Process.

What Is the Impact If an SSL Certificate Is Not Renewed in Time After It Expires?

Last updated：2023-10-10 14:30:32

What are the implications of not promptly updating an expired SSL certificate?

If an SSL certificate expires and is not updated in a timely manner, the following implications may arise:

- When users visit the website, the browser will display a warning message indicating that the site's security certificate has expired.
- Upon receiving the aforementioned warning, users may lose trust in the website, potentially choosing to cease their visit, which could negatively impact the company's brand image and user base.
- Malicious actors, such as hackers, may exploit the expired SSL certificate to tamper with or steal information and data transmitted between the browser and the server, thereby compromising user data security.
- The unexpected interruption of business operations due to certificate expiration can lead to operational abnormalities and financial losses.
- It could also damage the website's SEO ranking.

Viewing of SSL Certificate Expiration Time

Last updated：2023-10-10 14:31:23

How do I receive SSL certificate expiration notifications from the system?

Prior to the expiration of the certificate, you can view the relevant expiration information in the certificate information status column of the SSL Certificate Service Console. You can also set up to receive system message notifications related to the certificate through message subscriptions.

> **Note**
> - If you have not set up message subscriptions and have not selected **SSL Certificate Related Notifications** and **Product Service Related Notifications** in **Product Messages**, you will not receive in-site, email, or SMS notifications about certificate expiration.
> - For certificates of other vendors uploaded to Tencent Cloud, if message subscriptions are configured for them, you will also receive certificate expiration notifications.

Certificate Expiration Reminder Time: The renewal channel for the certificate will be opened within 30 days of its expiration. Expiration reminders will be sent out three times, specifically on the 29th, 15th, and 3rd day before expiration.

How do I receive certificate-related system notifications?

1. Please log in to the Message Center Console.
2. On the **Message Subscription** management page, you can select **SSL Certificate Related Notifications** and **Product Service Related Notifications** in **Product Messages**, as well as the type of notifications you need. For detailed operations, you can refer to: Message Subscription Management.

Why can a sub-account receive SSL certificate expiration reminders even if it has not set up message subscriptions?

Prior to the certificate's expiration, the sub-account that applied for or uploaded the certificate will receive expiration reminders. The timing and frequency of these reminders are consistent with those of subscription expiration alerts.

Is an SSL Certificate Still Available After I Renew It?

Last updated：2023-10-10 14:31:43

Can the service continue after the successful renewal of the certificate?

No. After renewing a certificate, you need to resubmit your certificate order for review, wait for the new certificate to be issued, and then re-deploy it to your Tencent Cloud service resources for use.