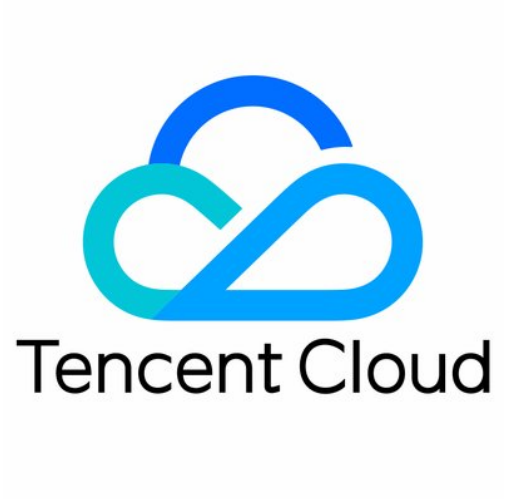
# SSL Certificate Service

# Purchase Guide

## Product Documentation



# Contents

# Purchase Guide
# Pricing

Last updated：2024-03-06 16:57:28

## SSL Certificate Service

Before using SSL Certificate Service, note the following:

**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`. But sub-domains are not supported. The domain name can go down to 100 levels at most.

**Multi-domain SSL certificate**: Multiple domain names can be bound, subject to the maximum number of supported domain names stated on Tencent Cloud website.

**Wildcard SSL certificate**: Only one single-wildcard domain name can be bound, such as `*.tencent.com` or `*.example.tencent.com` (up to 100 levels). Multi-wildcard domain names like `*.*.tencent.com` are not supported.

**Multi-domain wildcard SSL certificate**: Multiple single-wildcard domain names can be bound, such as `*.tencent.com` and `*.example.tencent.com` (up to 100 levels). Multi-wildcard domain names like `*.*.tencent.com` are not supported.

**Note**

The SSL Certificate Service currently does not support binding a **.ru** domain name.

You must provide all the domain names when applying for a multi-domain SSL certificate. For example, if you want to purchase a multi-domain certificate for three domain names, provide all the three domain names in the application.

The following prices are unit prices for 1-year certificate use.

| Brand | Supported Domains | Certificate Model | Unit Price (This is only for 1-year use after purchase. For prices and discounts for subsequent years, visit the Tencent Cloud website.) | Remarks |
|---|---|---|---|---|
| SecureSite | Single domain name | OV SSL certificate | 836 USD/year | - |
| | Single domain name | OV Pro SSL certificate | 1,342 USD/year | - |
| | Single domain name | EV SSL certificate | 1,342 USD/year | - |

| | | | | |
|---|---|---|---|---|
| | Single domain name | EV Pro SSL certificate | 2,507 USD/year | - |
| | Multiple domain names | OV SSL certificate for multiple domain names | 1,672 USD/year | This is the price for two domain names, and each additional domain name costs 836 USD. |
| | Multiple domain names | OV Pro SSL certificate for multiple domain names | 2,684 USD/year | This is the price for two domain names, and each additional domain name costs 1,342 USD. |
| | Multiple domain names | EV SSL certificate for multiple domain names | 2,684 USD/year | This is the price for two domain names, and each additional domain name costs 1,342 USD. |
| | Multiple domain names | EV Pro SSL certificate for multiple domain names | 5,014 USD/year | This is the price for two domain names, and each additional domain name costs 2,507 USD. |
| | One single-wildcard domain name | OV wildcard SSL certificate | 5,968 USD/year | - |
| GeoTrust | Single domain name | OV SSL certificate | 415 USD/year | - |
| | Single domain name | EV SSL certificate | 896 USD/year | - |
| | One single-wildcard domain name | OV wildcard SSL certificate | 1,086 USD/year | - |
| | Multiple domain | EV SSL certificate for multiple domain names | 2,686 USD/year | This is the price for five domain |

| | | | | |
|---|---|---|---|---|
| | names | | | names, and each additional domain name costs 448 USD. |
| TrustAsia | Single domain name | DV SSL certificate | Free | - |
| | Single domain name | OV SSL certificate | 672 USD/year | - |
| | Single domain name | EV SSL certificate | 1,418 USD/year | - |
| | Multiple domain names | DV SSL certificate for multiple domain names | 732 USD/year | This is the price for five domain names, and each additional domain name costs 142 USD. |
| | Multiple domain names | OV SSL certificate for multiple domain names | 970 USD/year | This is the price for two domain names, and each additional domain name costs 299 USD. |
| | Multiple domain names | EV SSL certificate for multiple domain names | 1,940 USD/year | This is the price for two domain names, and each additional domain name costs 523 USD. |
| | One single-wildcard domain name | DV wildcard SSL certificate | 299 USD/year | - |
| | One single-wildcard domain name | OV wildcard SSL certificate | 2,015 USD/year | - |
| | Multiple single-wildcard | DV wildcard SSL certificate for multiple domain names | 1,194 USD/year | This is the price for two domain names, and each additional domain |

| | | | | |
|---|---|---|---|---|
| | domain names | | | name costs 299 USD. |
| | Multiple single-wildcard domain names | OV wildcard SSL certificate for multiple domain names | 4,029 USD/year | This is the price for two domain names, and each additional domain name costs 2,015 USD. |
| GlobalSign | Single domain name | OV SSL certificate | 557 USD/year | - |
| | Single domain name | EV SSL certificate | 1,475 USD/year | - |
| | Multiple domain names | OV SSL certificate for multiple domain names | 852 USD/year | This is the price for two domain names, and each additional domain name costs 296 USD. |
| | Multiple domain names | EV SSL certificate for multiple domain names | 1,919 USD/year | This is the price for two domain names, and each additional domain name costs 445 USD. |
| | One single-wildcard domain name | OV wildcard SSL certificate | 1,947 USD/year | - |
| | Multiple single-wildcard domain names | OV wildcard SSL certificate for multiple domain names | 3,894 USD/year | This is the price for two domain names, and each additional domain name costs 1,947 USD. |

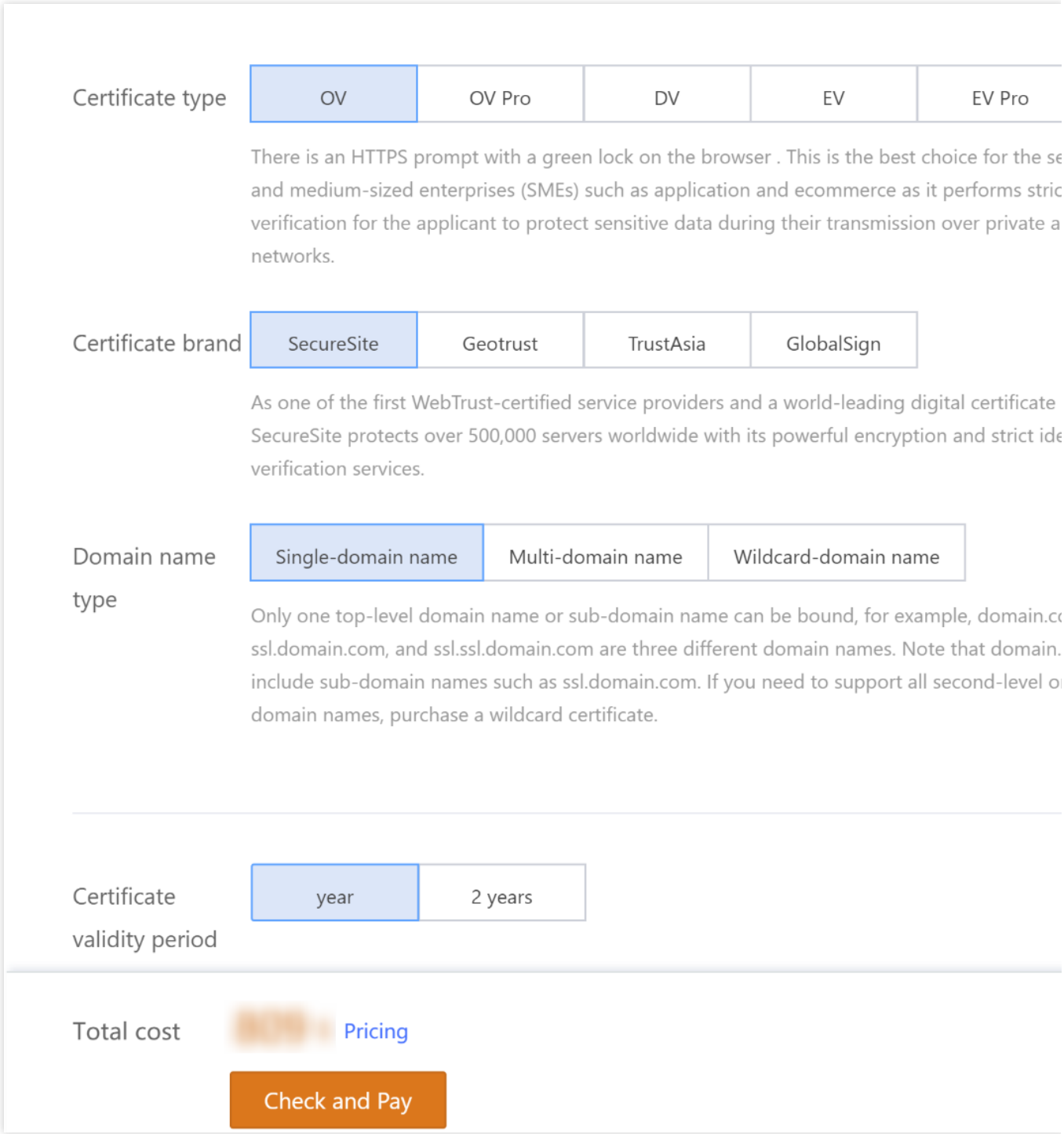
# SSL Certificate Purchase Process

Last updated：2024-03-06 16:57:28

We recommend that you take the time to understand the differences between the different certificate types and domain name types so that you can purchase the appropriate certificate for your actual needs. The following details the process of purchasing a certificate.

### Step 1. Go to the SSL certificate purchase page

1. Log in at the SSL certificate purchase page.
2. Click **Purchase Certificate** to view the detailed certificate configuration and pricing information, as shown in the following image:




**Note:**

If you are not familiar with certificate types and brands, click **Quick Configuration** to quickly purchase a certificate recommended by the system.

Click **Advanced Settings** and set **Project** and **Tag** to better manage existing Tencent Cloud resources by category. For detailed directions on how to add a tag, see Querying Resources by Tag.

### Step 2. Select the certificate type and brand

1. Select a certificate type that best fits your industry and actual needs. For more information, see Certificate Type Selection Cases.
2. Select a certificate brand. For more information, please see Certificate Brands.

### Step 3. Select the domain name type and the number of domain names supported

| Domain Type | Description | Notes |
| --- | --- | --- |
| Single-domain | Only one domain can be bound. The domain can be a second-level domain such as `tencent.com` or a third-level domain such as `example.tencent.com` . | Binding all subdomains under a second-level domain is not supported.Up to 100 levels of domains are supported.An SSL certificate bound to the domain `www.tencent.com` ( `www` as the subdomain) supports the second-level domain `tencent.com`. |
| Multi-domain | A certificate can be bound to multiple domains, subject to the maximum number of domains displayed in the console. | The prices of SecureSite multi-domain certificates are calculated based on the number of domains.For the GeoTrust, TrustAsia, GlobalSign, WoTrus, and DNSPod multi-domain certificates, there are additional charges for the domains that exceed the default maximum number of domains supported. |
| Wildcard domain | One and only one wildcard domain can be bound, and only one wildcard can be added. | For example, `\\*.tencent.com` and `\\*.example.tencent.com` support up to 100 levels.<br>Multi-wildcard domains such as `\\*.\\*.tencent.com` are not supported.An SSL certificate bound to the domain `\\*.tencent.com` (which must be a second-level wildcard domain) supports the second-level domain `tencent.com` . |
| Multiple wildcard domains | Multiple wildcard domains can be bound. | For example, `\\*.tencent.com` , `\\*.ssl.tencent.com` , and `\\*.another.com` are counted as a total of three wildcard domains, including all the subdomains at the same level, subject to the maximum number of domains displayed in the console. |

### Step 4. Select the certificate validity period

Due to changes in Apple and Google root store policies, newly issued SSL/TLS certificates with a validity period greater than 13 months (397 days) have been prohibited by policy since September 1, 2020. Therefore, global CAs have ceased issuing such certificates since September 1, 2020.

**Currently, only certain multi-year SSL certificates are available from Tencent Cloud (others available are all SSL certificates with a validity period of 13 months). Within 30 days before expiration of your current multi-year certificate, Tencent Cloud will automatically apply for a new one for you, which will be automatically issued upon CA approval.**

**Note:**

Available multi-year SSL certificate brands and types are as displayed on the purchase page.

If the original certificate is installed at the server website, you need to replace it with a newly issued one as instructed in Selecting an Installation Type for an SSL Certificate.

## Step 5. Pay for your order

After selecting the brand, model, supported domain name, and certificate validity period, you can submit your order and complete the payment process.

## Step 6. Submit an application

**DNSPod (SM2) OV and EV SSL certificates:**

1. After purchasing the certificate, log in to the SSL Certificate Service console and select **Pending Submission** to enter the management page. Then, submit the information, upload the confirmation letter, and complete the domain ownership verification.
2. After your application is submitted, it will be reviewed. After the review is successfully completed, the certificate will be issued.

**WoTrus OV and EV SSL certificates**

1. After purchasing the certificate, log in to the SSL Certificate Service console and select **Pending Submission** to enter the management page. Then, submit the information to pre-apply for the certificate. After your pre-application is approved, the domain ownership needs to be verified.
2. After your domain is validated, manual approval is needed, upon which the certificate will be issued. For more information, see Information Submission Process for Wotrus OV and EV SSL Certificates.

**Other OV and EV SSL certificates**

1. After purchasing the certificate, log in to the SSL Certificate Service console and select **Pending Submission** to enter the management page. Then, submit the information and upload the confirmation letter to apply for the certificate.
2. After your application is submitted, it will be reviewed. After the review is successfully completed, the certificate will be issued. For more information, please see The Process of Submitting Materials for OV/EV SSL Certificates.

**Note:**

If you use the approved organization and administrator information in **My Profile**, the confirmation letter is not required.
For GlobalSign certificates, the confirmation letter still needs to be uploaded when you submit the information.

### DV SSL certificates

After purchasing the certificate, log in to the SSL Certificate Service console and select **Pending Submission** to enter the management page. Then, submit the information and complete the domain ownership verification, after which the CA will issue the certificate.

### Free DV SSL certificates

After applying for the certificate, complete the domain ownership verification. The CA will then issue the certificate.

# SSL Certificate Selection
# SSL Certificates Supporting IP Address Binding

Last updated：2024-03-06 16:57:28

The following table describes the support for IP address binding by different SSL certificates:

**Note:**

You can apply for free certificates only for single domains, but not for wildcard domains and multi-domains.

Single-domain or multi-domain refers to the domain type you selected on the SSL Certificate Service buy page.

– indicates that this type of certificate is not available for sale in Tencent Cloud.

A private CA certificate can be bound with a private IP, but both a free certificate and a standard paid certificate cannot be bound with a private IP.

| Certificate Brand | OV | OV Pro | DV | Free DV | EV | EV Pr |
|---|---|---|---|---|---|---|
| SecureSite | **Supported by single-domain/multi-domain SSL certificates** Not supported by other domain types | **Supported by single-domain/multi-domain SSL certificates** Not supported by other domain types | Not supported | - | Not supported | Not suppo |
| GeoTrust | **Supported by single-domain/multi-domain SSL certificates** Not supported by other domain types | - | - | - | Not supported | - |
| TrustAsia | **Supported by single-domain/multi-domain SSL certificates** Not supported | - | Not supported | Not supported | Not supported | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| | by other domain types | | | | | |
| GlobalSign | **Supported by single-domain/multi-domain SSL certificates** Not supported by other domain types | - | - | - | Not supported | - |
| Wotrus | Not supported | - | Not supported | - | Not supported | - |
| DNSPod (SM) | **Supported by single-domain/multi-domain SSL certificates** Not supported by other domain types | - | - | - | **Supported by single-domain/multi-domain SSL certificates** Not supported by other domain types | - |
| DNSPod (Standard) | **Supported by single-domain/multi-domain SSL certificates** Not supported by other domain types | - | **Supported by single-domain/multi-domain SSL certificates** Not supported by other domain types | - | **Unsupported** | - |

# SSL Certificate Brands

Last updated：2024-03-06 16:57:28

## Certificate Brands and Models

Tencent Cloud provides the following brands of SSL certificates for sale:

| Certificate Brand | Description |
| --- | --- |
| SecureSite | SecureSite is the world's largest information security service provider and most reputable certificate authority. It provides a wide spectrum of content and network security solutions to individuals, businesses, and service providers.<br>93% of Fortune Global 500 companies choose VeriSign SSL digital certificates.<br>SecureSite acquired VeriSign in August 2010, changed VeriSign's product name and brand logo in April 2012, and since then has been providing the VeriSign verification service. |
| GeoTrust | GeoTrust, the world's second-largest digital certificate authority (CA) and a leader in identity verification and trust certification, provides state-of-the-art technologies that enable organizations and companies of all sizes to deploy SSL digital certificates securely and cost-effectively and to implement a wide range of identity verifications.<br>GeoTrust was founded in 2001, and by 2006, it accounted for 25% of the global market.<br>VeriSign acquired GeoTrust for 125 million USD in May-September 2006, and is now another cost-effective SSL certificate brand under SecureSite. |
| TrustAsia | TrustAsia, a brand under Yashu Information Technology (Shanghai) Co., Ltd in the field of information security, is a SecureSite platinum partner. TrustAsia specializes in providing businesses with complete network security services including digital certificates. TrustAsia SSL certificates are issued using Sectigo root certificates. |
| GlobalSign | Founded in 1996, GlobalSign is a reputable and trusted CA and provider of SSL certificates with more than 20 million SSL certificates issued worldwide.<br>A great number of server providers, domain name registrars, and system service providers in the Chinese market prefer GlobalSign and partner with it for digital certification services. |
| WoTrus | WoTrus, operated by WoTrus CA Limited, is an internationally verified CA that has also obtained the electronic certification service license (issued by the MIIT) of China. It provides third-party digital identity verification for organizations and issues globally trusted digital certificates. |
| DNSPod GM (SM2) | Tencent Cloud’s DNSPod certificate adopts the GM standards and is completely China-developed. Supported by well-reputed CAs in China, it is highly convenient and efficient and complies with regulatory requirements of China. |

| | |
|---|---|
| DNSPod International (SM2) | Tencent Cloud's DNSPod provides the international standard certificates on the basis of the SM certificates, balancing SM algorithm compliance and universal application. |

## Brand Differences

The certificates of different brands vary depending on the browser address bar, encryption level, and the level guaranteed compensation. The most important difference lies in their root certificates as follows:
A TrustAsia wildcard certificate is issued using a Sectigo root certificate. Serving more than 150 countries/regions, Sectigo is a world-leading CA with a long history. It also supports OCSP nodes in the Chinese mainland with faster response.
A GeoTrust wildcard certificate is issued using a GeoTrust root certificate, a SecureSite wildcard certificate using a SecureSite root certificate, and a DigiCert wildcard certificate using a DigiCert root certificate.
A GlobalSign wildcard certificate is issued using a GlobalSign root certificate, a DNSPod certificate using a WoTrus root certificate, and a WoTrus wildcard certificate using a Sectigo root certificate.
From a technical point of view, the differences between SecureSite (former VeriSign) and GeoTrust are as follows:
Compatibility: SecureSite outperforms GeoTrust. SecureSite is compatible with all browsers commercially available and many mobile devices.
OCSP response speed: SecureSite outperforms GeoTrust.
CA security: SecureSite outperforms GeoTrust. As an internationally renowned security vendor, SecureSite provides the best CA security in the world.
Data security: In addition to encrypted data transmission, SecureSite certificates provide malware scanning and vulnerability assessment.
Commercial insurance compensation for certificate: SecureSite (up to 1.75 million USD) outperforms GeoTrust (up to 1.5 million USD).

# Certificate Type Selection Cases

Last updated：2024-03-06 16:57:28

This topic lists certificate type selection cases for certain industries to help you determine which certificate type for which to apply or purchase.

| Industry | Recommended Certificate Type | Case | Industry Requirement |
| --- | --- | --- | --- |
| Finance and banking | EV certificate | Bank of China | Enterprise identity information must be displayed in the website address bar.<br>Data transmission must be highly secure. |
| Education, government, and internet | OV wildcard certificate | Ministry of Foreign Affairs of the People's Republic of China<br>JD.com<br>Tencent News<br>Shanghai Gold Exchange<br>State Grid Corporation of China<br>Yonyou Network Technology Co. Ltd.<br>Langchao<br>Tencent Cloud | New sites will be added in the later stage of the website project.<br>The government or company name does not need to be displayed in the website address bar. |
| Individual business | DV certificate | Personal blog | No data transmission.<br>The website displays pure information or content. |

# Paid SSL Certificates Renewal

Last updated：2024-03-06 16:57:28

Renewing an SSL certificate is equivalent to applying for a new certificate in the console, so you need to install and deploy the new certificate to your server. The new certificate does not affect the usage of the existing one.

**Note:**

If you want to modify the certificate information, apply for a new one.

After renewal, a new certificate will be issued. Replace the website certificate with the new certificate. For information about how to install a certificate, see Certificate Installation.

## Advantages of Renewal

Renewing the existing certificate holds the following advantages over purchasing a new one:

### Simplifying renewal procedure

Instead of entering the application information again, you only need to confirm the original certificate application data pulled automatically by the system and proceed to the payment process. After making the payment, upload the confirmation letter and wait for review.

### Prolonging certificate validity after renewal

After renewal, the remaining available time of the original certificate and an extra 1 to 90 days roll to the validity time of the new certificate for free. You will not experience any loss in certificate validity period due to renewal.

## Certificate Renewal Procedure

### 1. Going to the certificate renewal page

1. A quick renewal feature will be **enabled 30 days before your certificate expires**. On the **Certificate Management** page of the SSL Certificate Service console, click **Quick Renewal** in the **Operation** column of the certificate you want to renew.

2. On the pop-up window, confirm the information and click **Renew Now** to enter the renewal page.

### 2. Confirming the renewal information and make the payment.

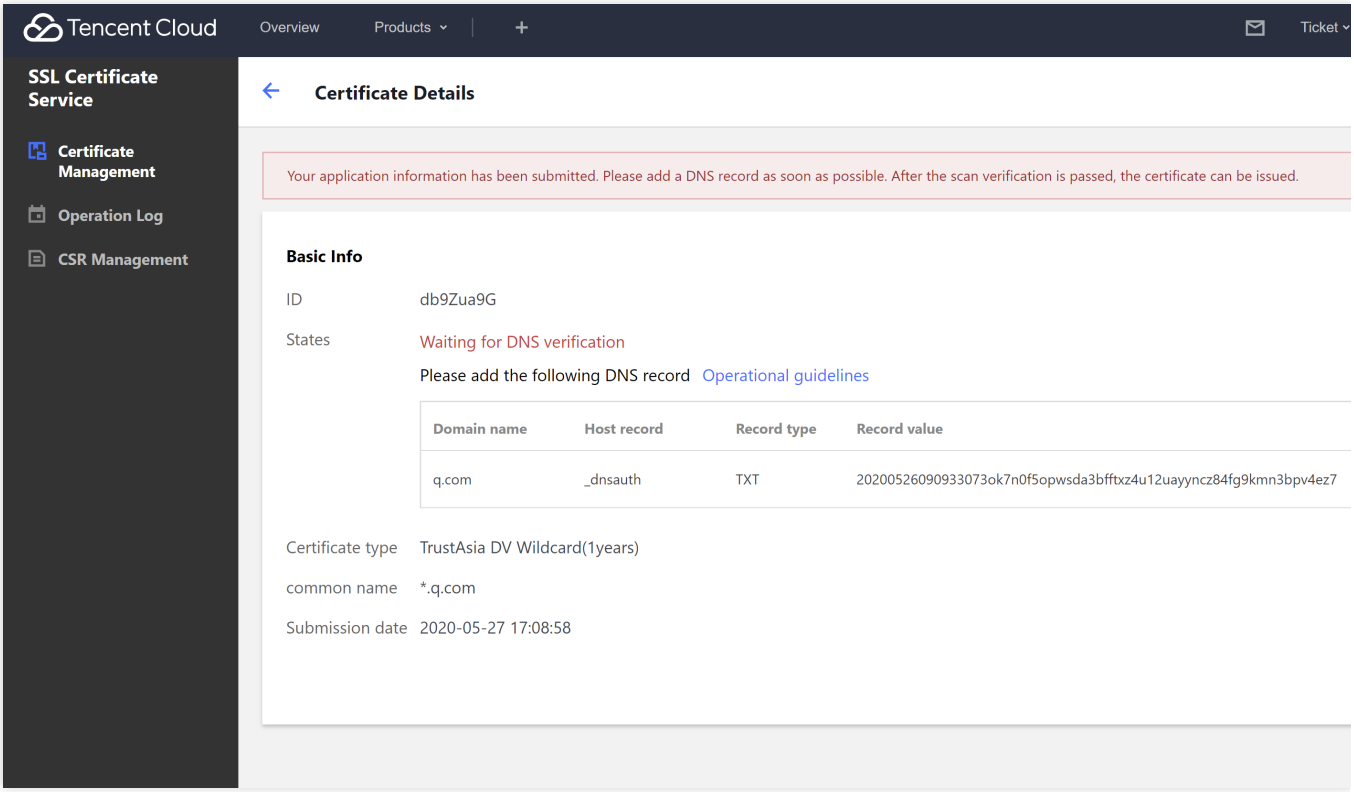
1. When renewing a certificate, you do not need to enter the certificate information again. A new certificate will be generated after renewal, so you need to create a CSR file for the new certificate.

You can automatically generate a CSR file through the system (**this option is recommended, and the CSR and private key can be generated**).
Or, upload a CSR file (**no private key can be generated with this option**).
2. After confirming the information, select the renewal period, and click **Quick Payment** to go to the payment page.
3. Confirm the certificate information and click **Purchase** for payment.

## 3. Confirming the certificate application

**For an OV/EV paid certificate, upload the confirmation letter and wait for review.**

1. After you complete payment, on the **Certificate Management** page in the SSL Certificate Service console, you can find a new certificate with the status of **Pending confirmation letter upload** in the certificate list. Click **Upload confirmation letter** to go to the confirmation letter details page.
2. Click **Download Confirmation Letter** as prompted, fill in the information, and seal the letter. Scan the confirmation letter to a file and click **Upload for Review**, as shown in the following figure.



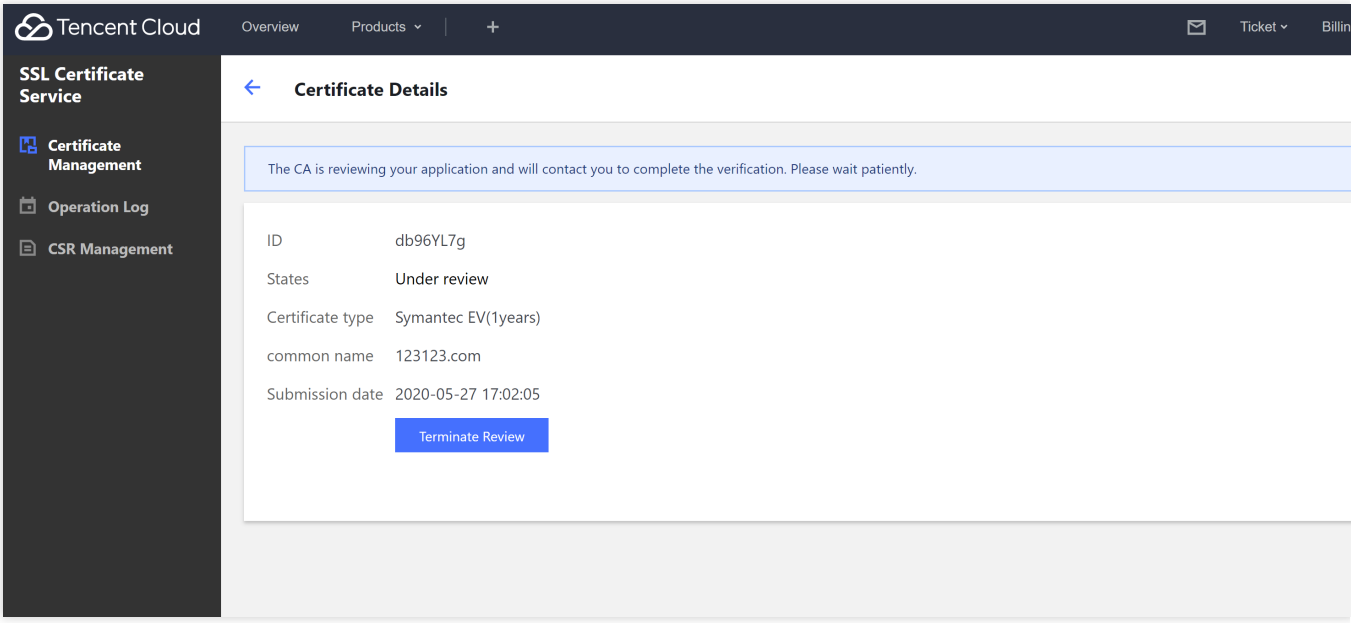

3. After you submit the confirmation letter, the certificate status changes to **Pending verification**. Wait for the reviewer to verify your information by phone and confirm the domain information email.
**Note:**
For OV certificates, certificate issuance takes **3 to 5 business days**. For EV certificates, certificate issuance takes **5 to 7 business days.**

**For paid DV certificates, verify the domain name.**

1. After you complete payment, on the **Certificate Management** page of the SSL Certificate Service console, you can find a new certificate with the status of **Pending verification** in the certificate list. Click **Details** to go to the **Certificate Details** page.
2. The DNS verification value is displayed on the **Certificate Details** page. Add this DNS record and wait for scan and verification by the CA. The certificate will be issued after approval.

**Note:**

Issuance of DV certificates takes **10 minutes to 24 hours**.




# Certificate Installation

After the certificate is issued, install the certificate based on your server type. For more information about certificate installation, see the following:

Installing a Certificate on Apache servers

Installing a Certificate on Nginx servers

Installing a Certificate on IIS servers

Installing a Certificate on Tomcat servers

**Note:**

If there is no certificate installation tutorial for the sever you use, go to the Tencent Cloud MARKET, search for certificate installation services, and select a vendor for certificate installation service.

# SSL Certificate Renewal Process
# Renewal Process for Paid SSL Certificates

Last updated：2024-03-06 16:57:28

Renewing an SSL certificate is equivalent to applying for a new one in the console, and you need to install and deploy it on the server. The new certificate does not affect the use of the existing one.

**Note:**

If you need to modify the certificate information, apply for a new one.

Renewing a certificate is equivalent to issuing a new one, and you need to replace the existing one with the new one.

Renewing a free certificate is free of charge. Specifically, you can reapply for a certificate as instructed in Renewal Process for Free DV SSL Certificates.

## Advantages of Renewal

Renewing the existing certificate holds the following advantages over purchasing a new one:

### Simplified renewal procedure

Instead of entering application information again, you only need to confirm the original certificate's application data pulled automatically by the system and proceed with the payment. After making the payment, upload the confirmation letter and wait for certificate review.

**Note:**

After renewing a WoTrus international standard certificate or DNSPod Chinese SM (SM2) certificate, you can directly enter the domain identity verification process without uploading the confirmation letter again.

### Extra-prolonged certificate validity after renewal

After renewal, the remaining validity period of the original certificate will roll to the validity period of the new certificate.

**Note:**

The quick renewal option will become available **within 30 calendar days before** a paid certificate expires, and the validity period of a renewed certificate **cannot exceed 398 days**.

The expiration reminder will be sent on the second calendar day after the quick renewal option becomes available. Renew your certificate as soon as possible upon receiving the reminder.

## Renewal Process for Paid Certificates

### Step 1. Enter the certificate renewal entry

1. For a paid certificate, the quick renewal option will become available **one month before its expiration date**. You can open the **Quick Renewal** window by clicking **Quick Renewal** in the **Status** column of the certificate in **My Certificates** in the SSL Certificate Service console.
2. In the SSL certificate renewal pop-up window, confirm the information and click **Renew** to enter the renewal page.

### Step 2. Confirm the renewal information and make the payment

1. When renewing a certificate, you do not need to enter the certificate information again. A new certificate will be generated after the renewal, so you need to configure a CSR file for the new certificate.
You can automatically generate a CSR file through the system (**this option is recommended, and the CSR and private key can be generated**).
You can also upload a CSR file (**no private key can be generated with this option**).
2. After confirming the information, select the renewal period and click **Quick Payment** to enter the payment process.
3. Confirm the certificate information, click **Purchase**, and make the payment.

### Step 3. Submit the certificate for review

**Note:**
It is estimated to take **3–5 business days** to issue an OV certificate and **5–7 business days** to issue an EV one.
It is estimated to take **10 minutes to 24 hours** to issue a DV certificate.

#### Renewing a paid WoTrus OV/EV certificate

A renewed WoTrus OV/EV certificate will be issued only after manual approval and domain validation.
**Note:**
After you applied, there will be a manual review, during which you will receive a call from the US to your organization's business registration number.

#### Renewing a DNSPod Chinese SM (SM2) OV/EV certificate

A renewed DNSPod Chinese SM (SM2) OV/EV certificate will be issued only after manual approval and domain validation.
**Note:**
The first domain validation will remain valid for 13 months from approval, during which no domain validation will be performed if you apply for a DNSPod Chinese SM (SM2) OV/EV SSL certificate with the same organization name for the domain.
The certificate will be issued only after manual approval and domain validation.
Manual approval will not be required if you apply for a certificate with the same information after having successfully applied for a certificate of the same type.

#### Renewing a paid OV/EV certificate of another brand

1. After purchasing a certificate successfully, a new certificate in **Pending confirmation letter upload** status will be generated in the certificate list in the SSL Certificate Service console. Then, click **Upload Confirmation Letter** to enter the confirmation letter details page.
2. Click to **download the confirmation letter template**, enter the required information, print it out, and affix the official seal.
3. Click **Upload**.
4. After the confirmation letter is uploaded, the **Certificate Status** will change to **Pending validation**, and you need to wait for the verification call from the reviewer as well as the domain confirmation email.

**Renewing a paid DV certificate**

1. After purchasing a certificate successfully, a new certificate in **Pending validation** status will be generated in the certificate list in the SSL Certificate Service console. Then, click **Details** to enter the **Certificate Details** page.
2. Add a DNS record based on the validation value on the **Certificate Details** page.
3. Wait for scan and validation by the CA. The certificate will be issued immediately after approval.

# Certificate Installation Documentation

After the certificate is issued successfully, you need to reinstall it based on its encryption standard type and server type.

**Note:**

The quick HTTPS feature helps you upgrade from HTTP to HTTPS without tedious SSL certificate deployment.

International standard certificates:

Linux system:

Installing an SSL Certificate on an Apache Server (Linux)

Installing an SSL Certificate on an Nginx Server

Installing an SSL Certificate (JKS Format) on a Tomcat Server

Installing an SSL Certificate (PFX Format) on a Tomcat Server

Installing an SSL Certificate on a GlassFish Server

Installing an SSL Certificate on a JBoss Server

Installing an SSL Certificate on a Jetty Server

Windows system:

Install a certificate on an IIS server

Installing a Certificate on WebLogic Servers

Installing an SSL Certificate on an Apache Server (Windows)

Installing an SSL Certificate (JKS Format) on a Tomcat Server

# Renewal Process for Free DV SSL Certificates

Last updated：2024-07-31 09:51:59

Due to changes in Apple and Google root store policies, global CAs have ceased issuing SSL certificates with a validity period greater than two years since September 1, 2020. Therefore, renewing an SSL certificate is equivalent to applying for a new one in the console, and the old certificate will not have a longer validity period. After the new certificate is issued, you need to reinstall it on the server, which takes effect upon deployment.
For detailed directions on how to install a certificate, see Installing Certificate. If the old certificate is within the validity period, its use will not be affected.

**Note:**

Renewing a free certificate is free of charge.

## Renewal Process for Free Certificates

### Step 1. Quickly apply for a new free certificate

1. For a free certificate, the quick renewal option will become available **one month before its expiration date**. You can open the **Quick Certification Reapplication** page by clicking **Quick Renewal** in the **Status** column of the certificate in **My Certificates** in the SSL Certificate Service console.
2. On the **Submit Information** page, confirm your application and click **Next** to enter the **Select Validation Method** page.

### Step 2. Validate the domain

1. On the **Select Validation Method** page, select the validation method.

**Adds DNS validation automatically**: For more information, see Details.

**Note:**

If the domain applied for has been successfully hosted in the
DNSPod console
, DNS validation can be added automatically.

**DNS validation**: For more information, see DNS Validation.

**File validation**: For more information, see File Validation.

2. Complete the domain identity verification as prompted by **Validation Instruction**.

**Note:**

Click **View Domain Validation Status** to view the current status of the domain validation.

Validating: The system is validating the domain.

Pending validation: The domain validation operation is to be added.
Validation timeout: The system validation failed after more than 30 seconds.
Passed: The domain validation has been passed.
Failed: The domain validation is not completed within the validation period.
3. After the domain validation is passed, the CA will issue the certificate within 24 hours.

## Download and Deployment

After the domain validation is completed, log in to the SSL Certificate Service console, select the issued certificate, and click **Download** to download and install it. For detailed directions, see Installing Certificate.
You can directly deploy a certificate on a Tencent Cloud service as instructed in Selecting an Installation Type for an SSL Certificate.

## Certificate Installation Documentation

After the certificate is issued successfully, you need to reinstall it based on the server type.
**Note:**
The quick HTTPS feature helps you upgrade from HTTP to HTTPS without tedious SSL certificate deployment.
International standard certificates:
Linux system:
Installing an SSL Certificate on an Apache Server (Linux)
Installing an SSL Certificate on an Nginx Server
Installing an SSL Certificate (JKS Format) on a Tomcat Server
Installing an SSL Certificate (PFX Format) on a Tomcat Server
Installing an SSL Certificate on a GlassFish Server
Installing an SSL Certificate on a JBoss Server
Installing an SSL Certificate on a Jetty Server
Windows system:
Install a certificate on an IIS server
Installing a Certificate on WebLogic Servers
Installing an SSL Certificate on an Apache Server (Windows)
Installing an SSL Certificate (JKS Format) on a Tomcat Server

## FAQs

# SSL Certificate Refund Process

Last updated：2024-03-06 16:57:28

If you have paid for an SSL certificate order, but the application failed, the approval process was suspended, and the certificate was not issued, you can request a refund. This document describes how to do so.

**Note:**

If you use a discount or voucher for purchase, the discount amount and voucher will not be refunded.

A completed refund application cannot be canceled. Proceed with caution.

## 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 order and click **Refund**.

**Note:**

If **Refund** is not displayed in your certificate list and the **Pending Submission** status is displayed in the **Operation** column, click the target **Certificate ID** to enter the **Certificate Details** page and click **Cancel Application**. Then, **Refund** will be displayed in the certificate list.

3. In the pop-up window, indicate your consent to the refund policy and click **Next**.
4. Click **OK**.

**Note:**

For a normal certificate purchase, the payment will be returned to your Tencent Cloud account by the proportion of the cash and gift cards paid for the purchase.

If you use benefit points for the certificate purchase, they will be returned to the corresponding benefit package.