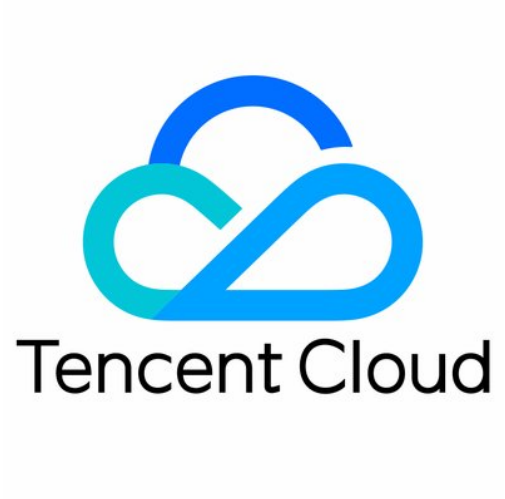
SSL Certificate Service

Purchase Guide

Product Documentation



Contents

Purchase Guide
Pricing

Last updated : 2020-07-09 14:36:17

Notes:

- **Single-domain SSL certificate**: only one domain name can be bound. This can be a second-level domain name like example.domain.com, a third-level domain name like example.example.domain.com, or a first-level domain name like domain.com. But all sub-domains under the first-level domain name are not supported. Up to 100 levels of domain name can be supported.
- **Multi-domain SSL certificate**: one 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 SSL certificate**: only one wildcard domain name with only one wildcard can be bound, such as *.domain.com and *.example.domain.com (up to 100 levels). Multi-wildcard domain names like *.*.domain.com are not supported.
- **Multi-domain wildcard SSL certificate**: multiple wildcard domain names with only 1 wildcard can be bound, such as *.domain.com and *.example.domain.com (up to 100 levels). Multi-wildcard domain names like *.*.domain.com are not supported.

The following prices are unit prices based on 1 year of purchase.

Certificate Brand	Number of Supported Domain Names	Certificate Model	Unit Price (only for the first year of purchase and subject to any discounts for subsequent years as stated on Tencent Cloud's official website)	Remarks
SecureSite	Single domain name	OV SSL certificate	809 USD/year	-
	Single domain name	OV Pro SSL certificate	1,294 USD/year	-

	Single domain name	EV SSL certificate	1,294 USD/year	-
	Single domain name	EV Pro SSL certificate	2,071 USD/year	-
	Multiple domain names	OV SSL certificate for multiple domain names	809 USD/year	The total price is calculated by multiplying the unit price by the number of domain names.
	Multiple domain names	OV Pro SSL certificate for multiple domain names	1,294 USD/year	The total price is calculated by multiplying the unit price by the number of domain names.
	Multiple domain names	EV SSL certificate for multiple domain names	1,294 USD/year	The total price is calculated by multiplying the unit price by the number of domain names.
	Multiple domain names	EV Pro SSL certificate for multiple domain names	2,071 USD/year	The total price is calculated by multiplying the unit price by the number of domain names.
	Wildcard domain name	OV wildcard SSL certificate	6,471 USD/year	-
GeoTrust	Single domain name	OV SSL certificate	461 USD/year	-

	Single domain name	EV SSL certificate	785 USD/year	-
	Wildcard domain name	OV wildcard SSL certificate	1,108 USD/year	-
	Multiple domain names	OV SSL certificate for multiple domain names	903 USD/year, and 105 USD/year for 1 extra domain name	By default, 5 domain names are supported. One extra domain name is priced at 105 USD/year.
	Multiple domain names	EV SSL certificate for multiple domain names	1,561 USD/year, and 235 USD/year for 1 extra domain name	By default, 5 domain names are supported. One extra domain name is priced at 235 USD/year.
TrustAsia	Single domain name	DV SSL certificate	Free	-
	Single domain name	OV SSL certificate	728 USD/year	-
	Single domain name	EV SSL certificate	1,537 USD/year	-
	Multiple domain names	DV SSL certificate for multiple domain names	794 USD/year	By default, 5 domain names are supported. One extra domain name is priced at 154 USD/year.
	Multiple domain names	OV SSL certificate for multiple	1,051 USD/year	By default, 2 domain names are supported. One extra domain name

		domain names		is priced at 324 USD/year.
	Multiple domain names	EV SSL certificate for multiple domain names	2,103 USD/year	By default, 2 domain names are supported. One extra domain name is priced at 566 USD/year.
	Wildcard domain name	DV wildcard SSL certificate	323 USD/year	-
	Wildcard domain name	OV wildcard SSL certificate	2,184 USD/year	-
	Multiple domain names with wildcard	OV wildcard SSL certificate for multiple domain names	4,368 USD/year	By default, 2 domain names are supported. One extra domain name is priced at 2,184 USD/year.
GlobalSign	Single domain name	OV SSL certificate	603 USD/year	-
	Single domain name	EV SSL certificate	1,598 USD/year	-
	Multiple domain names	OV SSL certificate for multiple domain names	923 USD/year	By default, 2 domain names are supported. One extra domain name is priced at 320 USD/year.
	Multiple domain names	EV SSL certificate for	2,080 USD/year	By default, 2 domain names are supported. One

		multiple domain names		extra domain name is priced at 482 USD/year.
	Wildcard domain name	OV wildcard SSL certificate	2,111 USD/year	-
	Multiple domain names with wildcard	OV wildcard SSL certificate for multiple domain names	4,221 USD/year	By default, 2 domain names are supported. One extra domain name is priced at 2,111 USD/year.

Purchasing Process

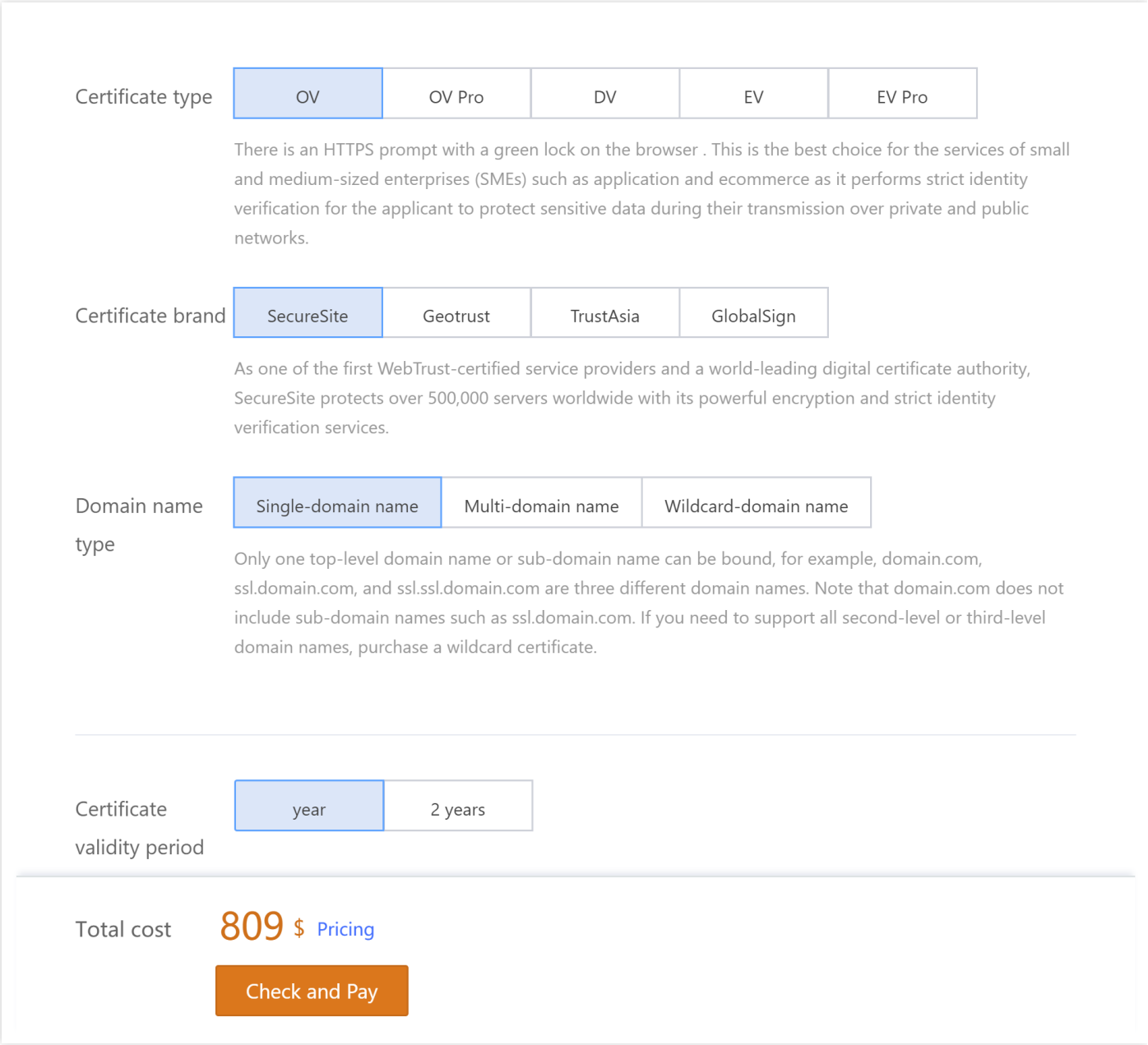
Last updated : 2021-03-25 10:48:25

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 to the SSL Certificate Service console.
2. On the **Certificate Management** page, click **Purchase Certificate** to go to the SSL certificate purchase page.

3. Read the information on the SSL certificate purchase page, as shown in the following figure:



Step 2. Select the certificate type and brand

1. Select a certificate type that best fits your industry and actual needs. For more information about certificate types, please see Selecting Certificate Types.
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	Description	Notes

Name Type		
Single-domain name	Only 1 domain name can be bound. The domain name can be a second-level domain name such as `tencent.com` or a third-level domain name such as `example.tencent.com`.	• However, binding all sub-domain names under a second-level domain name is not supported. • Up to 100 levels of domain names are supported. • An SSL certificate bound to the domain name `www.tencent.com` (`www` as the sub-domain name) supports the second-level domain name `tencent.com`.
Multi-domain name	A single certificate can be bound to multiple domain names, subject to the maximum number of supported domain names displayed in the console.	• The prices of SecureSite multi-domain name certificates are calculated based on the number of domain names. • For the GeoTrust, TrustAsia, GlobalSign, Wotrus, and DNSPod multi-domain name certificates, there are additional charges for the domain names that exceed the default maximum number of domain names supported.
Wildcard domain name	Only 1 wildcard domain name with only 1 wildcard can be bound.	• For example, `\*.tencent.com` and `\*.example.tencent.com` support up to 100 levels. • Multi-wildcard domain names such as `\*.\*.tencent.com` are not supported. • An SSL certificate bound to the domain name `\*.tencent.com` (which must be a second-level wildcard domain name) supports the second-level domain name `tencent.com`.
Multi-wildcard domain name	Multiple wildcard domain names can be bound.	For example, `\*.tencent.com`, `\*.ssl.tencent.com`, and `\*.another.com` are counted as a total of 3 wildcard domain names, including all the sub-domain names at the same level, subject to the maximum number of supported domain names displayed in the console.

Step 4. Select the certificate validity period

Due to changes in Apple and Google root store policies, as of September 1, 2020, newly issued SSL/TLS certificates with a validity period greater than 13 months (397 days) will be prohibited and will not be trusted. Starting from September 1, 2020, global CAs will no longer issue 2-year SSL certificates, and **only 1-year SSL certificates will be available for purchase by default.** For

more information, see the Notice on Stopping the Issuance of 2-Year SSL Certificates by CAs Starting from September 1, 2020.

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.

> **Note :**
>
> If you need an invoice, please see Self-Service Invoice Feature.

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 click **Submit info** to go to the **Certificate Information Submission** page. Then, enter the relevant 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 click **Submit info** to go to the **Certificate Information Submission** page. Then, enter the relevant information to pre-apply for the certificate. After your pre-application is successfully reviewed, the domain ownership will need to be verified.
2. After the domain ownership is verified, it will be reviewed. After the review is successfully completed, the certificate will be issued.

Other OV and EV SSL certificates

1. After purchasing the certificate, log in to the SSL Certificate Service console and click **Submit info** to go to the **Certificate Information Submission** page. Then, enter the relevant 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.

DV SSL certificates

After purchasing the certificate, log in to the SSL Certificate Service console and click **Submit info** to go to the **Certificate Information Submission** page. Then, enter the relevant 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.

Paid SSL Certificates Renewal

Last updated : 2020-08-12 17:46:57

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.

- 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 3 months 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.

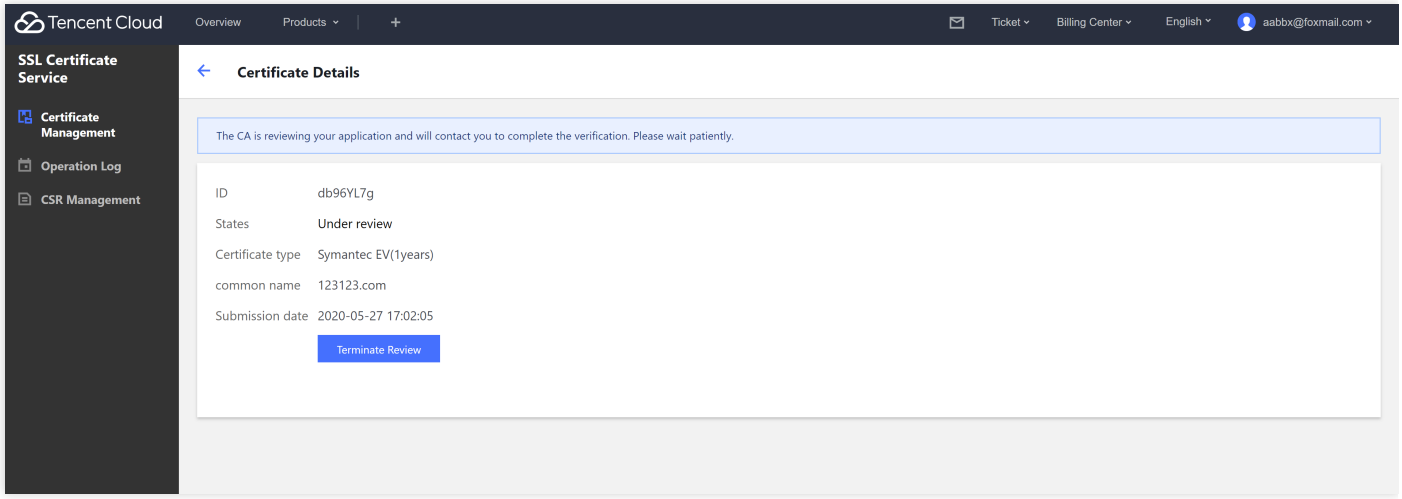
2. Confirming the renewal information and make the payment.

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.



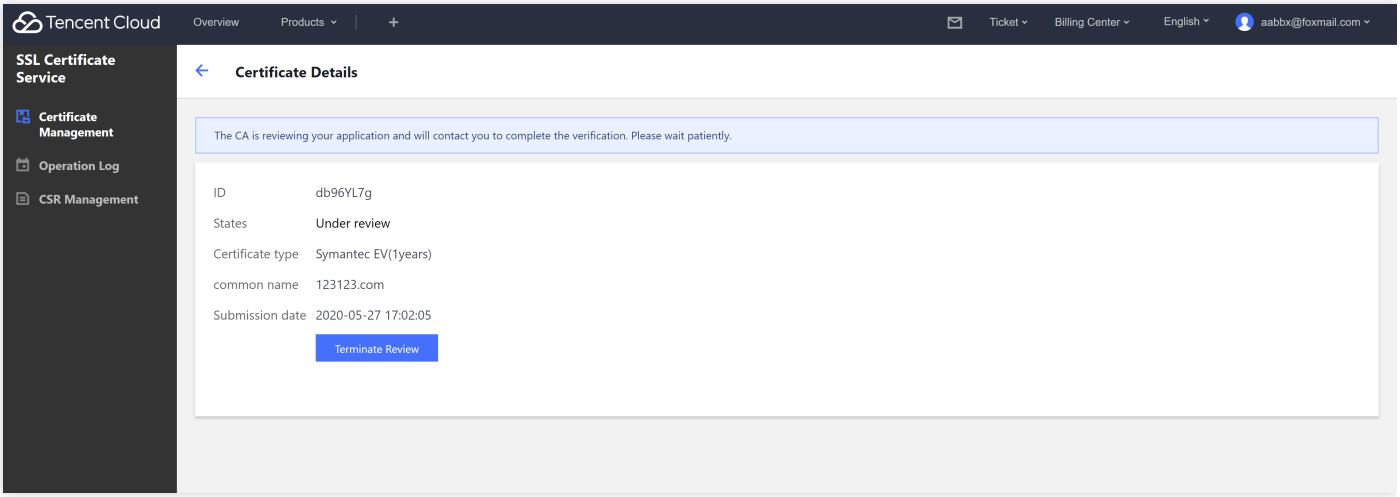
3. After you submit the confirmation letter, the certificate status changes to **Pending verification**. Wait for the reviewer to verify your information by phone and confirm the domain information email.

> 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.

> 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

> 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.

Refund

Last updated : 2020-09-17 12:01:05

Refund conditions

- No refund for free DV SSL certificates.
- No refund for SSL certificates that have been successfully issued by CAs.
- Refund can be applied for SSL certificates that are in a terminated verification process after the payments complete.

Refund method

Submit a ticket to apply for refund, and we will help you complete the refund process.