

SSL Certificate Service

FAQs

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

FAQs

SSL Certificate Selection

How Do I Choose a Certificate?

What SSL Certificates Support IP Address Binding?

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

CAA Record

SSL Certificate Application

How to Fill In the Domains Bound to an SSL Certificate During the Application?

Questions Related to Wildcard Certificates

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

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

What Is CSR?

How Do I Make a CSR File?

Forgot Your Private Key Password?

Can a Certificate Be Revoked?

What are the differences between RSA and ECC?

What's the Difference Between Certificate Reissue and Reapplication?

SSL Certificate Installation

What Should I Do If the Host Name Field Is Uneditable in the IIS Manager?

How Do I Enable Port 443 for a VM?

Why Does the Website Prompt "Connection Is Untrusted"?

How Do I Install OpenSSL?

How Can I Set TLS Versions for SSL Certificates?

How Can I Combine an SSL Certificate Chain?

SSL Certificate Region

Are There Any Region Restrictions on SSL Certificate Installation?

SSL Certificate Review

How Long Will the Certificate Review Takes?

Causes and Handling Methods for Certificate Review Failures

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

SSL Certificate Taking Effect

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

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

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

SSL Certificate Billing and Purchase

Are DV Certificates Permanently Free?

SSL Certificate Validity Period

What Should I Do If an SSL Certificate Is About to Expire?

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

Questions Related to the Viewing of SSL Certificate Expiration Time

Is an SSL Certificate Still Available After I Renew It?

FAQs

SSL Certificate Selection

How Do I Choose a Certificate?

Last updated : 2020-09-16 15:11:25

Which certificate should I choose?

- If the website owner is an individual (without a business license), you can only apply for DV SSL certificates.
- 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 do I choose 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 4 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, binding all sub-domain names under a second-level domain name is not supported.** Up to 100 levels of domain name are supported.
- **Multi-domain name:** 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 name:** only 1 wildcard domain name with only 1 wildcard can be bound, such as `*.tencent.com` and `*.example.tencent.com` (up to 100 levels). A wildcard domain name with multiple wildcards like `*.*.tencent.com` is not supported.
- **Multi-wildcard domain name:** multiple wildcard domain names with each containing only 1 wildcard can be bound, such as `*.tencent.com` and `*.example.tencent.com` (up to 100 levels). A wildcard domain name with multiple wildcards like `*.*.tencent.com` is not supported.

What SSL Certificates Support IP Address Binding?

Last updated : 2021-04-13 17:18:07

What Certificate Brands and Types are Supported to be Bound to IP Addresses?

SSL certificates that are supported by Tencent Cloud to be bound to IP addresses are as follows:

Certificate Brand	OV	OV Pro	DV	Free DV	EV	E
SecureSite	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	N S
GeoTrust	Unsupported	-	-	-	Unsupported	-
TrustAsia	Supported	-	Unsupported	-	Unsupported	-
GlobalSign	Unsupported	-	-	-	Unsupported	-

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

Last updated : 2020-08-26 11:37:32

Can I apply for an SSL certificate before activating 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 have not purchased any Tencent Cloud service resources when you apply for an SSL certificate, the file verification method will not be supported during certificate verification.

CAA Record

Last updated : 2021-09-09 12:41:41

What is CAA?

Certification Authority Authorization (CAA) is designed to avoid SSL certificates from being issued wrongly, which was approved by the Internet Engineering Task Force (IETF) as [RFC 6844](#). In March 2017, the CA/Browser Forum passed Ballot 187, which requires mandatory CAA checking 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 the domain name holder did not set a CAA record for the domain name, any CA can issue an SSL certificate for this domain name.
- If your domain name is hosted with DNSPod, see [CAA Record](#).

SSL Certificate Application

How to Fill In the Domains Bound to an SSL Certificate During the Application?

Last updated : 2021-06-02 10:11:12

How to fill in the domains bound to an SSL certificate during the application?

After purchasing the SSL certificate, you need to go to the [SSL Certificate Service console](#) to submit the materials for review. The SSL Certificate Service console will prompt you the type and number of domain names based on the certificate you purchased, as shown in the following figure:

Basic Info

Common name *

Email address for application * ⓘ
Email address is required

Certificate alias

Private key password
In order to protect the security of the private key, the private key retrieval function is currently not supported. Please keep your private key safe.
 If you need to deploy CLB, CDN and other services on Tencent Cloud, do not fill in the private key.

Project

[Next](#)

Note :

To ensure that your SSL certificate can be issued and HTTPS can be used properly, please fill in information about the bound domains correctly.

Based on the brand of your certificate and the domains bound, SSL Certificate Service will offer the corresponding parent domain for free. Details are described as follows:

Type Rule	Certificate			
		GlobalSign	TrustAsia (OV/EV)	TrustAsia (DV)

Certificate Type Rule	GlobalSign	TrustAsia (OV/EV)	TrustAsia (DV)	GeoTrust
If the bound domain is not prefixed with `www.`, the `www.` sub-domain is offered for free.	No	If the bound domain is a primary domain, the `www.` sub-domain is offered for free.	If the bound domain is a primary domain, the `www.` sub-domain is offered for free.	If the bound domain is a primary domain, the `www.` sub-domain is offered for free.
If the bound domain is a general or wildcard domain, the parent domain is offered for free.	Yes	Yes	Yes	Yes

Note :

- If the bound domain is a primary domain, some brands will offer the `www.` sub-domain for free. For example, if the bound domain is `tencent.com`, the `www.tencent.com` sub-domain will be offered for free.
- If the bound domain is a general or wildcard domain, some brands will offer the corresponding parent domain for free. For example, if the bound domain is `*.tencent.com`, `tencent.com` will be offered for free.
- A parent domain will only be offered for free if the general or wildcard domain is of level three or above.

Wildcard domains

A wildcard domain is one with a wildcard, for example, `*.tencent.com` and `*.cloud.tencent.com`. It includes all sub-domains at the same level.

Note :

Cross-level domains are not supported. For example, `*.tencent.com` does not include the `*.cloud.tencent.com` child domains.

Questions Related to Wildcard Certificates

Last updated : 2020-11-30 09:47:31

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. Both OV certificates and DV certificates can be wildcard certificates.

If you have a server with multiple sub-domain names of the same level, you can use a wildcard certificate instead of purchasing and installing a certificate for each sub-domain name.

- Wildcard SSL certificates support second-level domain names.
- A wildcard certificate supports only 1 wildcard domain name, and does not support multiple domain names.
- Currently, wildcard certificates support only wildcard domain names, and do not support ordinary domain names (non-wildcard domain names). If you require a certificate that covers multiple wildcard domain names and 1 or more ordinary domain names, we recommend purchasing a multi-domain wildcard SSL certificate.

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

A wildcard certificate can match only sub-domain names of the same level, and cannot match sub-domain names of different levels. For example, a third-level wildcard domain name such as

`*.tencent.com` does not support a fourth-level domain name such as `www.ssl.tencent.com`.

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

Last updated : 2020-08-26 11:37:32

Why does the order status not change after a notification email is received from a CA?

While reviewing your materials in the process of issuing your certificate, the CA may send an email to notify you of the progress of your certificate application. If the order status does not change in the Tencent Cloud SSL Certificate Service Console after you have received that email, it may be due to a delay in the CA pushing the order status to Tencent Cloud. Just be patient and the status will be updated in time.

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

Last updated : 2020-08-26 11:37:33

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 : 2020-09-03 11:18:00

What is CSR?

CSR is short for Certificate Signing Request. To obtain an SSL certificate, you need to first generate a CSR file and submit it to the certificate authority (CA). A CSR file contains a public key and a distinguished name and is usually generated from a web server. A pair of public and private keys for encryption and decryption will be created at the same time.

Relevant organization information is required to create a CSR. The web server creates a distinguished name based on the information provided to identify the certificate. The organization information includes the following items:

Country or region code

The code of the country/region where your organization is legally registered, in the 2-letter format defined by the International Organization for Standardization (ISO).

Province, city, or autonomous region

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

City/region

The city/region where your organization is registered.

Organization

The legal registered name of your business.

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 CSR common name field must be the Fully Qualified Domain Name (FQDN) of the website to which you apply the certificate, such as "www.domainnamegoeshere".

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

How Do I Make a CSR File?

Last updated : 2020-07-27 14:41:04

How do I make a CSR file?

This topic describes how to generate a Certificate Signing Request (CSR) file.

Prerequisites

Before applying for an SSL certificate, you need to generate a key file and a CSR file for generating the certificate. The CSR file is the source file of your public key certificate. It contains your server and company information and needs to be submitted to a certificate authority (CA) for review. You are advised to use the CSR file generated by the system to avoid approval failures caused by information input errors. If you choose to manually generate a CSR file, ensure that you properly keep and back up your private key file. Pay attention to the following when manually generating a CSR file:

- UTF-8 encoding is required for input information. Specify UTF-8 encoding when you use OpenSSL to configure the CSR.
- The SSL certificate service system has strict requirements regarding the key length of the CSR file. The key length must be 2,048 bits and the key type must be RSA.
- For a multi-domain SSL certificate or wildcard SSL certificate, you only need to enter a domain name for `Common Name` or `What is your first and last name?` .

Generating a CSR file using OpenSSL

1. Log in to a local computer or server running Linux.
2. Install OpenSSL. For installation details, see [How to Install OpenSSL?](#).
3. Run the following command to generate a CSR file:

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

Note :

- **new**: generate a new CSR file.
- **nodes**: do not encrypt the key file.
- **sha256**: digest algorithm.
- **newkey rsa:2048**: key type and length.
- **[\$Key_File]**: key file name.
- **[\$OpenSSL_CSR]**: storage path of the encrypted file.

4. Enter information required for CSR file generation as prompted. The necessary fields are described as follows:

- **Organization Name:** company or organization name.
- **Organizational Unit Name:** department or section name.
- **Country Code:** two-letter country code of the country where your company is located. For example, enter `CN` for China.
- **State or Province Name:** name of the province or state where your company is located.
- **Locality Name:** name of the city where your company is located.
- **Common Name:** website domain name for which you are applying for an SSL certificate.
- **Email Address:** this field is optional.
- **Challenge Password:** this field is optional.

After you enter the information as prompted, the key file and CSR file are generated in the current directory.

Forgot Your Private Key Password?

Last updated : 2021-05-07 09:52:02

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 the certificate.

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.
 - For more information about applying for a paid certificate, please see [Purchasing Process](#).

Can a Certificate Be Revoked?

Last updated : 2020-12-16 12:23:47

Can I revoke certificates?

Currently, Tencent Cloud only supports offline certificate revocations. Please submit a ticket to contact Tencent Cloud engineers for certificate revocation.

What are the differences between RSA and ECC?

Last updated : 2021-05-06 10:38:50

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

- RSA (international standard algorithm): one of the earliest-introduced algorithms that is used commonly. It applies to a wider range and offers higher compatibility compared with ECC. However, it is normally 2,048 bits in length, which makes it consume more server resources.
- 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
Key length	256 bits	2,048 bits
CPU usage	Less	Higher
Memory usage	Less	Higher
Network usage	Less	Higher
Efficiency	High	Normal
Anti-attack	High	Normal
Compatibility	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 : 2021-09-09 12:41:41

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 change the certificate information. If the certificate was free, the reapplication uses another free tier. If the certificate was a paid one, you will have to pay for it again.

SSL Certificate Installation

What Should I Do If the Host Name Field Is Uneditable in the IIS Manager?

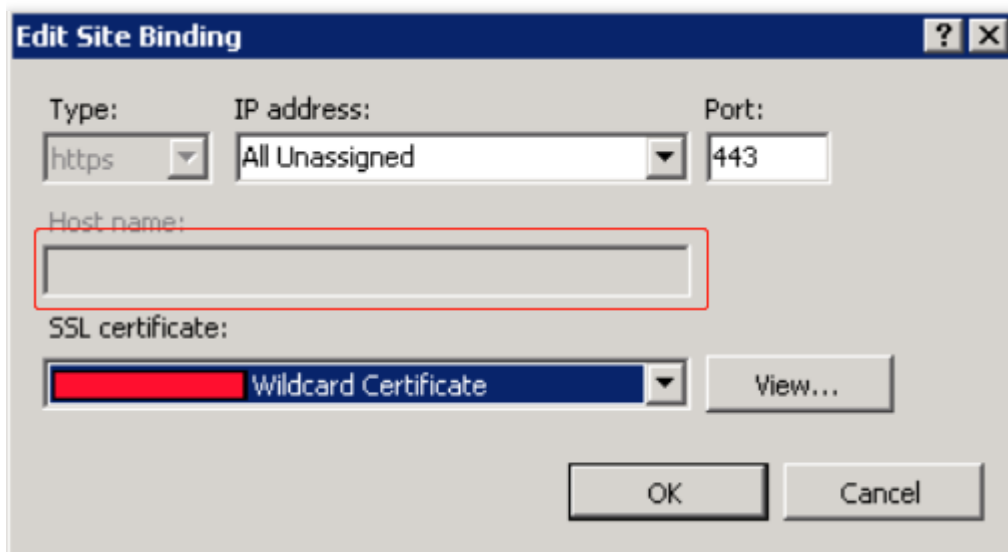
Last updated : 2020-09-01 09:58:07

What should I do if the host name field is uneditable in IIS Manager?

When installing a certificate in IIS Manager, after you import a PFX certificate file and set **Type** to **https** during website binding, the **Host name** field becomes uneditable. You can use the following method to address this problem.

Scenario

If **Type** is set to **https** during certificate installation in IIS Manager, the **Host name** field becomes uneditable after the SSL certificate is selected, as shown in the following example.



Solution

1. Open the `applicationHost.config` file in `C:\Windows\system32\inetsrv\config\applicationHost.config`.
2. Make the following modifications:

Note :

- `tencent.com` is used as the domain name in the following example.

- Replace `<binding protocol="https" bindingInformation="*:443:" />` in the following sample code with `<binding protocol="https" bindingInformation="*:443:tencent.com" />` .
- If you cannot modify the file directly, try modifying it as an admin, or copy and paste it to your desktop, modify it, and then replace the original file with the modified one.

```
<site name="example.tencent.com" id="8">
<application path="/">
<virtualDirectory path="/" physicalPath="D:¥web¥tencent" />
</application>
<bindings>
<binding protocol="http" bindingInformation="*:80:example.tencent.com" />
<binding protocol="http" bindingInformation="*:80:www.tencent.com" />
<binding protocol="https" bindingInformation="*:443:" />
</bindings>
</site>
```

3. After saving the modified file, bind the website again.

How Do I Enable Port 443 for a VM?

Last updated : 2020-12-14 09:34:33

How do I enable port 443 for a VM?

- For Tencent Cloud CVMs, see [Adding Security Group Rules](#).
- For other cloud providers' VMs, see the corresponding cloud provider's documentation.

Why Does the Website Prompt "Connection Is Untrusted"?

Last updated : 2020-07-01 10:21:16

The accessed site prompts "connection is not secure" after SSL certificate deployment. Has the certificate deployment failed?

The certificate has been successfully deployed. This problem occurs because the browser considers the access to sites using HTTPS protocol unsafe when the pages contain unencrypted HTTP contents. In this case, code needs to be modified.

For frontend modification, here are some guidelines:

- Use the relative path to reference resources.
- When referencing the absolute path, use `//` to reference resources. For example, `//img.qqcloud.com/example.png` indicates compliance with the protocol of the current page, and the browser will automatically complete it.

How Do I Install OpenSSL?

Last updated : 2020-09-01 09:58:07

How do I install OpenSSL?

OpenSSL is a well-known open source cryptography toolkit for secure communications, featuring cryptographic algorithms, common passwords, and certificate packaging.

OpenSSL official website

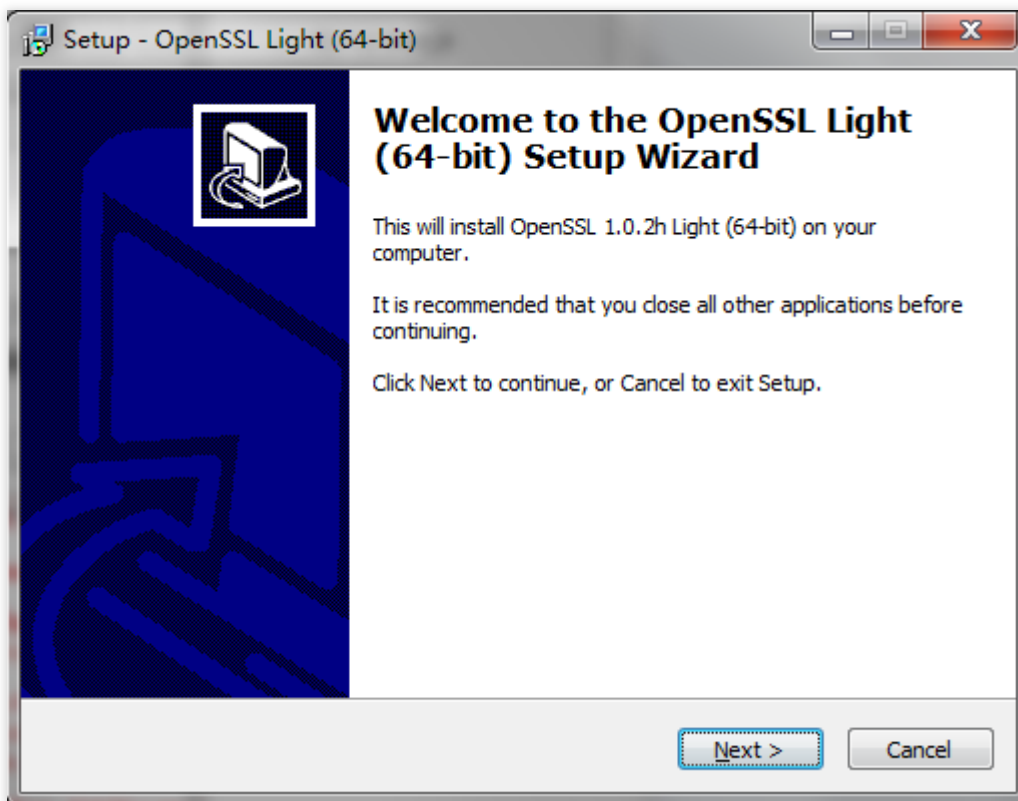
For the official download address: click [here](#).

Installing OpenSSL on Windows

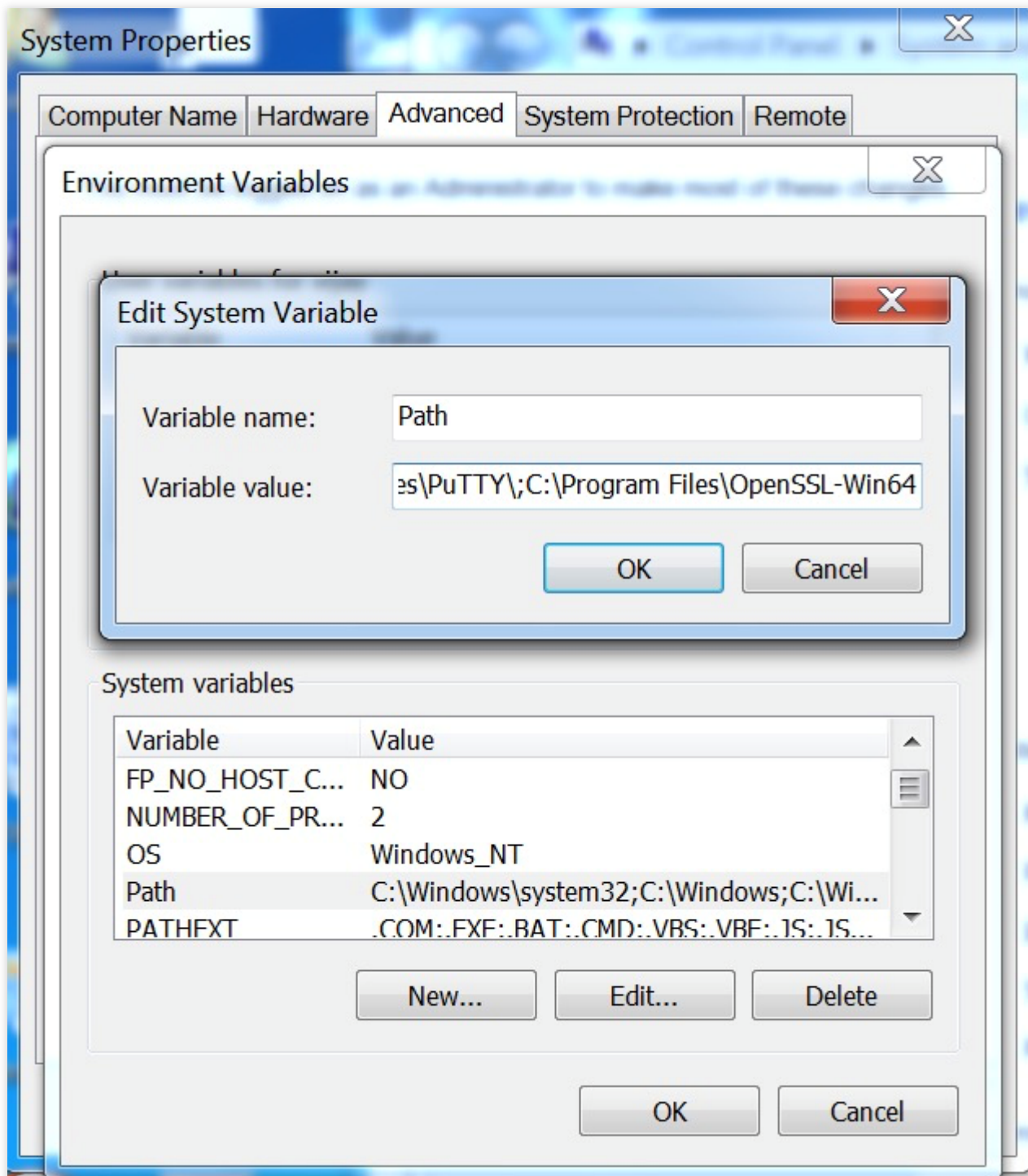
No installation package for Windows is provided on the OpenSSL official website. Instead, you can use tools provided by other open source platforms, such as, [Win32/Win64 OpenSSL](#).

The following describes how installation and usage information Windows users.

1. Download a 32-bit or 64-bit version, for example, `Win64openssl_Light-1_0_2h.exe` , as shown in the following figure.



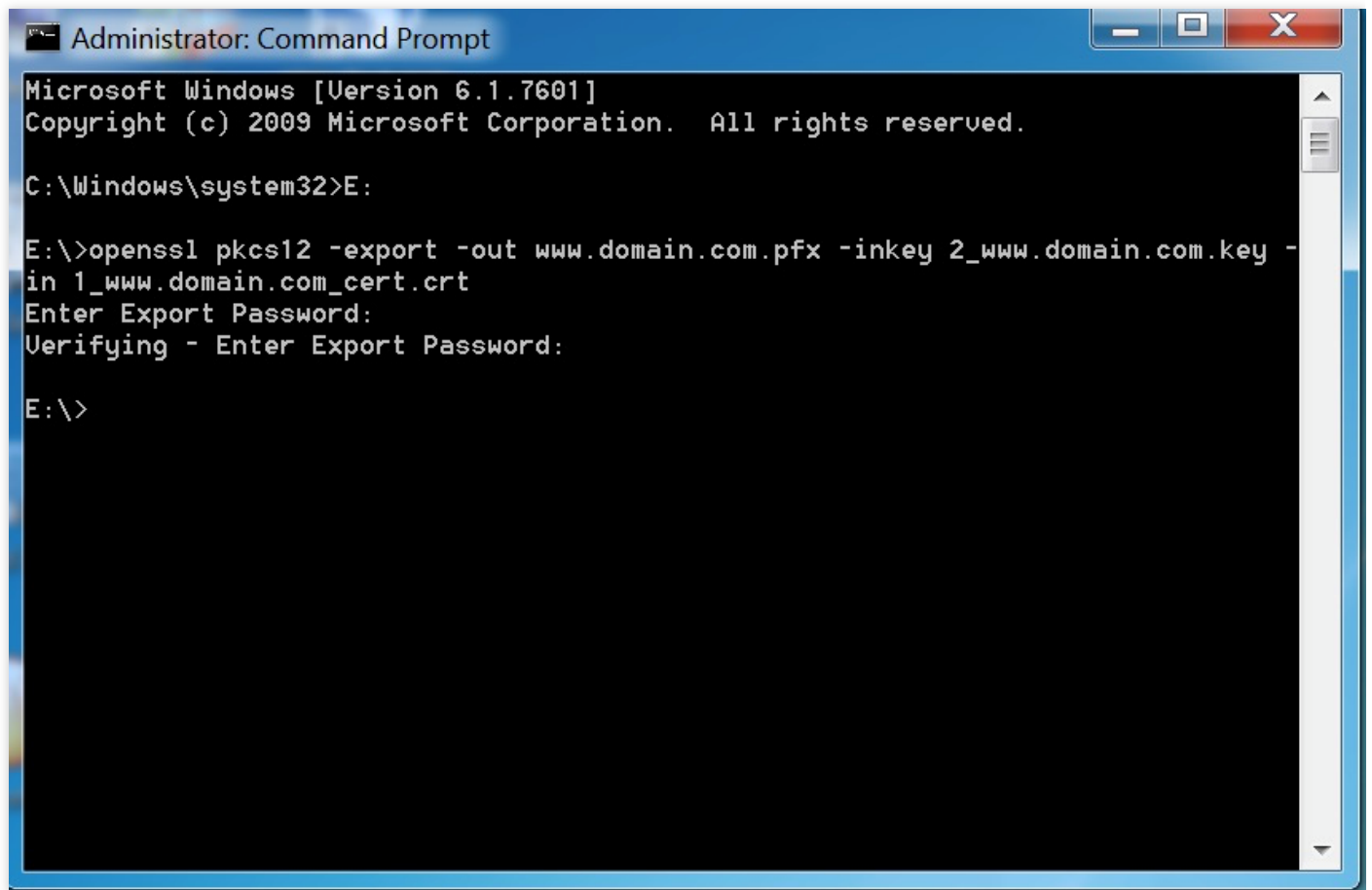
2. Set the environment variables. If the tool is installed in `C:\%0penSSL-Win64` , copy `C:\%0penSSL-Win64\bin;` to **Path**, as shown in the following figure.



3. Open the Command Prompt (you must be logged in as the admin), go to the directory in which the files `2_www.tencent.com.key` and `1_www.tencent.com_cert.crt` are saved, and run the following command:

```
openssl pkcs12 -export -out www.tencent.com.pfx -inkey 2_www.tencent.com.key -in 1_www.tencent.com_cert.crt
```

If the .key and .cert files are stored in `D:¥` , the running status will be as follows:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>E:

E:\>openssl pkcs12 -export -out www.domain.com.pfx -inkey 2_www.domain.com.key -
in 1_www.domain.com_cert.crt
Enter Export Password:
Verifying - Enter Export Password:

E:\>
```

Note :

If Export Password is not required, press **Enter** directly.

4. After the file `www.tencent.com.pfx` is generated in `D:¥` , continue to complete the certificate installation in IIS Manager.

How Can I Set TLS Versions for SSL Certificates?

Last updated : 2021-02-25 16:42:51

Versions of the TLS protocol include TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3, and more. You can set the TLS version for your SSL certificates in the Tencent Cloud service console or web service on the server as needed.

Tencent Cloud services

If your SSL certificates are deployed to the following Tencent Cloud services, you can configure by referring to the following documentations:

- CLB: [HTTPS Forwarding Configurations](#)
- CDN: [TLS Version Configuration](#)

Server web services

If your SSL certificates are installed in the web service on the server, find `ssl_protocols TLSv1 TLSv1.1 TLSv1.2` in the certificate configuration file of your web service and modify it as needed. For example, if your certificate needs to support the TLSv1.1 and TLSv1.2 versions, remove `TLSv1` from `ssl_protocols TLSv1 TLSv1.1 TLSv1.2`.

How Can I Combine an SSL Certificate Chain?

Last updated : 2021-02-26 14:26:55

In most cases, browsers for PCs can obtain the intermediate certificate from the URL of Authority Information Access (AIA). However, on browsers of some Android systems, the certificate may appear to be untrusted or cannot be accessed.

This main reason is that browsers for those Android systems do not support obtaining the intermediate certificate from the URL of AIA. In this case, you need to combine the certificate chain files into one according to the SSL certificate chain structure and deploy it on the server again. When the browser connects with the server, it downloads the user certificate as well as the intermediate certificate so that the certificate will appear to be trusted for your browser's access. The SSL certificate chain structure is as follows:

```
-----BEGIN CERTIFICATE-----  
Domain certificate  
-----END CERTIFICATE-----  
  
-----BEGIN CERTIFICATE-----  
Root CA certificate  
-----END CERTIFICATE-----  
  
-----BEGIN CERTIFICATE-----  
Intermediate CA certificate  
-----END CERTIFICATE-----
```

Note :

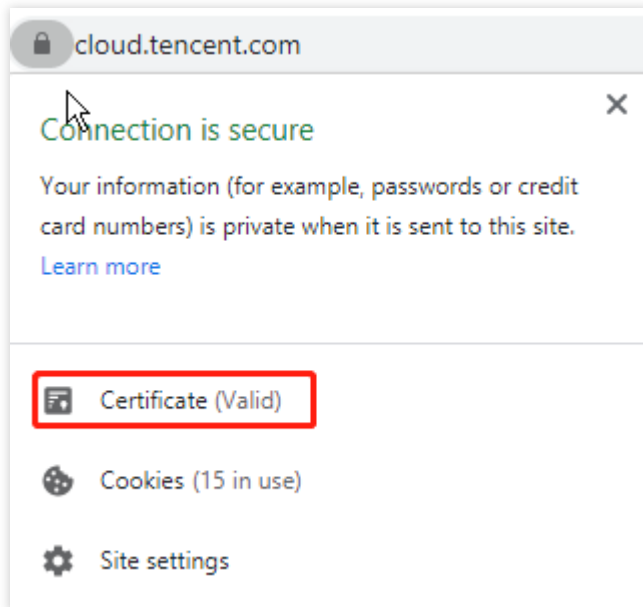
- Normally, an SSL certificate chain is made up of the root CA certificate > intermediate CA certificate(s) > domain certificate. There may be multiple intermediate certificates.
- International standard SSL certificates provided by Tencent Cloud are complete certificate chains, which are available without needing to be combined.

How can I view the SSL certificate chain?

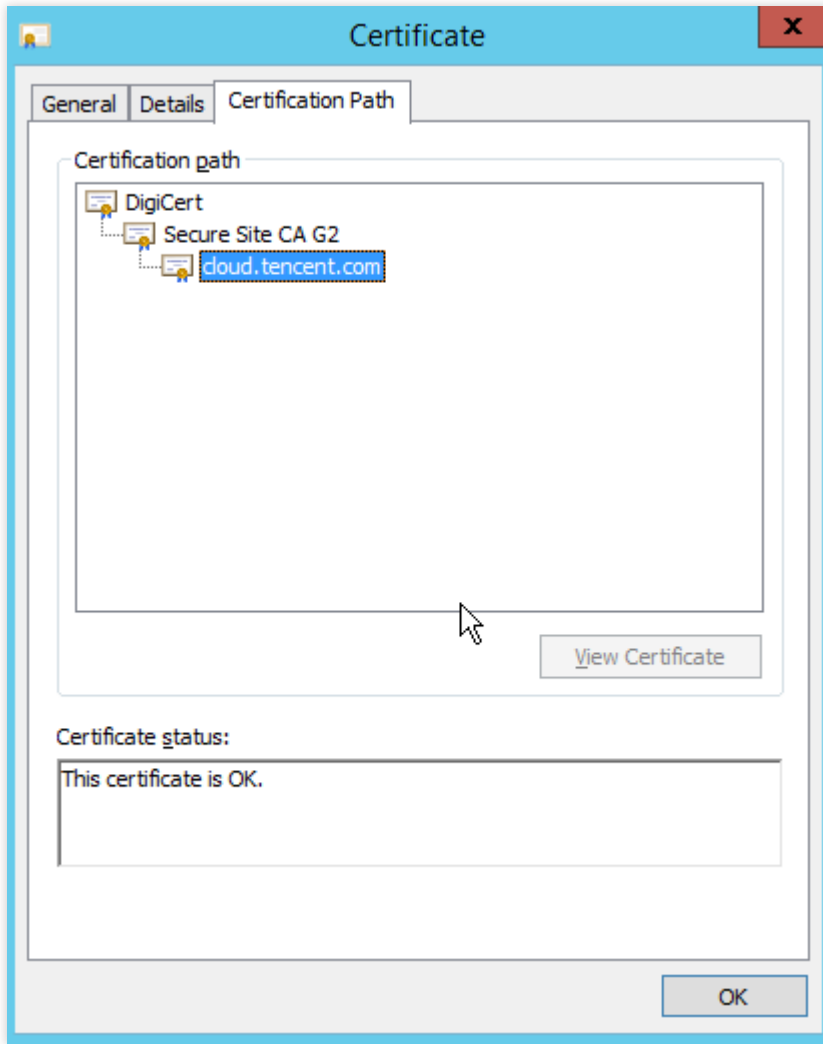
1. Open a browser to access the website that has successfully installed and deployed the SSL certificate. Chrome is used as an example herein.



2. Click  in the browser address box, and click **Certificate** on the page that is displayed, as shown in the following figure:



3. On the **Certificate** page, click **Certificate Path** to view the SSL certificate chain, as shown in the following figure:



SSL Certificate Region

Are There Any Region Restrictions on SSL Certificate Installation?

Last updated : 2020-08-26 11:37:33

Are there any region restrictions on SSL certificate installation?

No. After an SSL certificate is purchased and issued, there are no region restrictions for certificate installation and deployment.

SSL Certificate Review

How Long Will the Certificate Review Takes?

Last updated : 2021-06-02 10:11:12

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 :

DV certificates do not involve human review. Therefore, when CA detects that your domain has been verified, the certificate can be issued.

SSL Certificate Type	Time Needed
DV certificate	-
OV certificate	3–5 business days
EV certificate	5–7 business days

Causes and Handling Methods for Certificate Review Failures

Last updated : 2020-08-26 11:37:33

Troubleshooting certificate review failure

This section describes the possible causes of and outlines solutions for certificate review failure.

Verification file configuration error

Note :

We recommend running the `curl -k -v` or `wget -S` command to verify whether the file URL is valid for both HTTPS and HTTP.

• Causes

If you chose file verification as the method for domain name verification when submitting your SSL certificate order for review, the domain name may fail the verification due to the following possible causes:

- HTTPS access is enabled for some pages of the site. However, the verification file is deployed only under the HTTP service path, not under the HTTPS service path. As a result, the verification file will not be found when requested through HTTPS.
- When the verification file is accessed, the site returns an error code.
- CDN is enabled, but the verification file is not synchronized to CDN servers outside the Chinese mainland.

• Solutions

- Deploy the verification file under the HTTP and HTTPS service paths, and confirm that it can be accessed through HTTPS. Alternatively, temporarily disable HTTPS for all of the website pages.
- Confirm that the correct verification file content can be directly accessed through the verification file URL specified by the CA, instead of through redirection or other methods.

Note :

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

- Synchronize the verification file to CDN servers outside of the Chinese mainland, or temporarily disable CDN acceleration outside the Chinese mainland.

Note :

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

DNS configuration error**• Causes**

If you choose DNS verification as the method for domain name verification when submitting your SSL certificate order for review, the review may fail due to the following possible causes:

- The DNS resolution record value is configured incorrectly.
- For non-existent host records, the domain name resolution services of certain service providers provide query return values that are not as expected. As a result, the CA determines that the return values are incorrect.
- The DNS resolution record has timed out. After you submit your certificate order for review, you will have 3 calendar days to add the DNS resolution records, otherwise the review will fail.
- The dynamic domain name resolution service is enabled. However, the corresponding TXT resolution record value has not been synchronized to the DNS servers outside of the Chinese mainland in time.

• Solutions

- Configure the correct DNS host records and record values.
- Ignore the error prompts related to domain name resolution configuration, configure DNS resolution records as required, and complete the domain name verification.
- Resubmit the certificate order for review and add the DNS resolution records within 3 calendar days.
- Confirm that the dynamic resolution service works properly and ensure that it can resolve newly added TXT resolution records properly outside of the Chinese mainland.

Note :

If you change an existing TXT record value, the time when the changed value takes effect is determined by the TTL value. However, if you add a new TXT record value, the new value takes effect in seconds. Therefore, we recommend completing the domain name verification by adding a TXT record value and deleting the TXT resolution record after the domain name passes verification.

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.

- **Causes**

For OV and EV SSL certificates, the company phone number field is required. If it is left empty or set to an invalid value, you need to reset it.

- **Solutions**

Enter the correct company phone number by which you can be contacted for verification by the CA.

CSR file already used in other orders

- **Causes**

To ensure certificate key security, CSR information that has been used in earlier orders cannot be reused in new orders.

- **Solutions**

If you have used a CSR file in a successfully submitted order before, generate a new CSR file for each subsequent order. This ensures that each SSL certificate has a unique key pair, ensuring the security of your SSL certificates.

Incorrect format of the domain name bound with the certificate

- **Causes**

A valid domain name can be up to 64 characters in length and contain only letters, digits, and hyphens (-).

- **Solutions**

Check that the domain name information in the CSR file and order is correct.

Empty or incorrect primary domain name

- **Causes**

The `Common Name` field is empty or not correctly set when the CSR file is created.

 **Note :**

The `Common Name` field must be set to one of the bound domain names.

- **Solutions**

We recommend using the online CSR file generation feature provided by the system.

Domain name security review failure

When you apply for an SSL certificate, you may receive review results as shown in the following figure.

- **Causes**

Due to CA's anti-phishing mechanism, sensitive words contained in domain names, such as "bank" and "pay", can cause security review failure. Specific sensitive words are defined by the CA. Some less commonly used root domain names may also result in review failure. For example, root domain names suffixed with .pw, such as `www.qq.pw` and `www.qcloud.pw`, will not pass the review.

- **Solutions**

We recommend changing the host name in the domain name and trying to submit the order again. If the problem persists after you change the host name several times, we recommend that you choose a paid certificate product or use a different primary domain name to apply for a certificate.

Note :

Because DV SSL certificates are issued quickly 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 : 2020-12-17 15:36:49

What should I do after submitting the order for the review of a purchased certificate?

After purchasing an SSL certificate, you need to apply for the certificate and submit the application information for review. After the information passes review, you can use the certificate and deploy it for your Tencent Cloud service resources.

For a paid certificate, after you submit the certificate order for review, the CA will contact you to confirm certificate information. Make sure that you can be reached by phone and check your email in time to avoid missing the confirmation notice sent by the CA during the review (the phone and email here refer to those you specify when submitting the certificate order for review).

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:

- **Pending verification:** if your certificate order is in this state, click **Details** to view the domain name verification mode and complete verification. After the certificate status changes to **Issued**, the certificate is available for use.
- **Failed to pass review:** if your certificate order is in this state, click **Details** to check the cause of review failure, modify the certificate information accordingly, and submit the modified information for review.

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 certificates will be issued in several hours or 1 calendar day after application, depending on the time required by the review processes of different CAs.

SSL Certificate Taking Effect

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

Last updated : 2020-08-26 11:37:33

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

If the SSL certificate is bound to a domain name, it is not affected by the change of the server IP address.

As long as the domain name bound with the SSL certificate remains unchanged, it can be resolved to the new IP address, and the original SSL certificate is still valid.

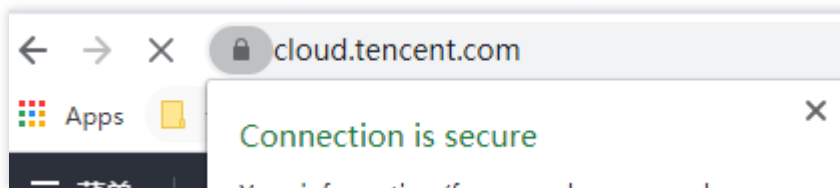
How Do I Check in a Browser Whether an SSL Certificate Has Taken Effect?

Last updated : 2020-08-26 11:37:33

How do I check in a browser whether an SSL certificate has taken effect?

After an SSL certificate is successfully installed and your domain name is resolved to a server IP address, perform the following steps to check whether the SSL certificate has taken effect:

1. Open a browser (Chrome is used as an example), and enter the domain name address bound to the SSL certificate in the https format in the address box.
2. Press **Enter** to access the domain name address. Check whether the following conditions are met:
 - You can successfully access the website using the domain name address.
 - 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 : 2021-06-21 10:18:21

Background

As of May 27, 2019, GlobalSign officially started using a new intermediate CA to sign SSL certificates. Because there is no new root certificate support for Windows 7, websites whose GlobalSign certificates were issued (including updated or reissued certificates) after May 27, 2020 are not trusted when being accessed using Windows 7. For details, see [GlobalSign SSL Products Intermediate and Root Migration](#).

Solution

Use a text editor to open the CRT file in the Nginx directory of the downloaded certificate, and copy and paste the cross certificate to the end of the certificate chain. Then, restart the Nginx service for the certificate to work properly.

To download the cross certificate, [click here](#).

SSL Certificate Billing and Purchase

Are DV Certificates Permanently Free?

Last updated : 2020-06-01 17:06:29

Are DV certificates permanently free?

Regardless of whether the SSL certificates are free DV certificates or paid OV certificates, CAs set a validity period for security reasons. It is possible that a website becomes a phishing website, so CAs conduct a regular review instead of issuing permanently valid certificates.

Additionally, you can apply for certificate revocation if you lose your private key. The CA then adds the revoked certificate to a certificate revocation list (CRL). Whenever an HTTPS website is accessed, the browser retrieves the CRL from the CA to determine whether to trust the certificate. Because issuing permanently valid certificates leads to an increasing CRL, it will increase the request traffic for browsers. Therefore, CAs specify validity periods for certificates.

At present, Tencent Cloud provides a free DV certificate with the model of **TrustAsia DV SSL CA - G5** and a valid period of **1 year**. You can apply a new certificate **3 months** before the certificate expires. DV certificates can be issued within 1 business day, so you have sufficient time to switch the certificates for the website.

SSL Certificate Validity Period

What Should I Do If an SSL Certificate Is About to Expire?

Last updated : 2021-08-16 12:15:04

What should I do if an SSL certificate is expired?

A paid SSL certificate becomes invalid once it expires. Before the expiration, you need to renew it, bind to the domain name again, and submit an application for approval.

Once your application is approved, you will obtain a new SSL certificate. Install it on the server to replace the original one before it expires.

Note :

- If you are using a free domain-validated (DV) certificate, you need to apply for a new one before the current one expires.
- You are advised to renew the certificate 3 to 10 business days before expiration to avoid impacting your business.

For more information, see [Paid SSL Certificates Renewal](#).

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

Last updated : 2020-08-26 11:37:34

What will happen if I do not renew my SSL certificate in time after it expires?

If an SSL certificate expires and is not renewed in time, the following may occur:

- When a user visits your website, the user's browser displays a warning message indicating that the website's security certificate has expired. After receiving such a warning message, the user may lose trust in the website or choose to stop visiting the website, which has an adverse impact on the company's brand image and subscriber base.
- Hackers and other cyber-criminals may take advantage of the expired SSL certificate to tamper with or steal information transmitted between the browser and server, affecting user data security.
- Certificate expiration will cause unexpected business interruption, leading to operating problems and capital loss.
- Certificate expiration will affect the website's SEO ranking.

Questions Related to the Viewing of SSL Certificate Expiration Time

Last updated : 2020-10-12 17:03:55

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

Before a certificate expires, log in to the [Tencent Cloud SSL Certificate Service Console](#) and check the certificate expiration information in the **Expiry date** column on the Certificate Management page. Alternatively, you can configure message subscriptions to receive certificate related system notifications.

Note :

If message subscriptions are not configured, you will not receive certificate expiration notifications through the Message Center, email, or SMS.

Certificate expiration notification time: 30 days before certificate expiration

How do I receive certificate related system notifications?

1. Log in to the [Message Center](#).
2. On the **Message Subscription** page, under **Product notifications**, select **SSL Certificate Notifications**, and then select the desired notification types.

Is an SSL Certificate Still Available After I Renew It?

Last updated : 2020-08-26 11:37:34

Is an SSL certificate still available after I renew it?

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.