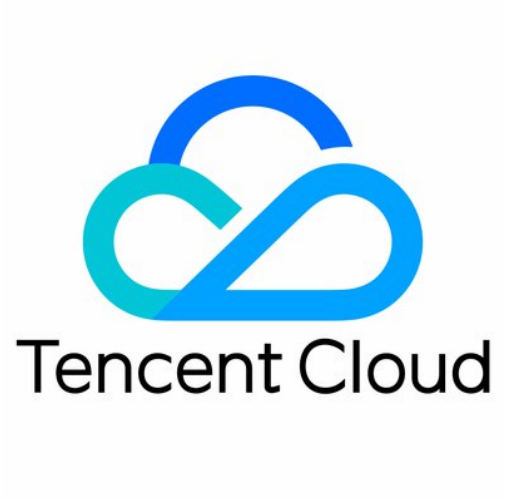
SSL Certificate Service

FAQs

Product Documentation



Contents

FAQs
SSL Certificate Selection
How Do I Choose a Certificate?

Last updated：2024-03-06 17:58:12

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：2024-03-06 17:58:12

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	EV Pro
SecureSite	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Not supported
GeoTrust	Unsupported	-	-	-	Unsupported	-
TrustAsia	Supported	-	Unsupported	-	Unsupported	-
GlobalSign	Unsupported	-	-	-	Unsupported	-

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

Last updated：2024-03-06 17:58:12

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：2024-03-06 17:58:12

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 a CAA record is not configured for the domain, any CA can issue an SSL certificate for this domain.

If your domain is hosted with DNSPod, see CAA Record.

If a CAA record for a non-Tencent Cloud CA is configured for the domain name, an SSL certificate cannot be issued for the domain properly. Before domain validation, check whether a CAA record is added for the domain and remove it if there is any.

SSL Certificate Application
Quota of Free SSL Certificates

Last updated：2024-03-06 18:00:08

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

Category	Quota
Tencent Cloud root account	20
Primary domain	20

Each Tencent Cloud root account has a quota of 20 free certificates that can be applied for at any given time.
Each primary domain has a quota of 20 free TrustAsia DV SSL certificates that can be applied for at any given time.
Note:
Both a second-level domain and its subdomains are deemed under the primary domain. For example, `tencent.com`, `ssl.tencent.com`, and `ssl.ssl.tencent.com` are under the same primary domain.
Free TrustAsia DV SSL certificates issued by other platforms for the same primary domain are also counted in the quota.

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

The quota is replenished immediately after the free certificates are revoked or expire.

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

The quota is replenished only after certificates expire; certificate revocation or deletion will not replenish the quota.

When I apply for a new free certificate, which is deducted first: the free certificate quota or the quota in a free certificate package?

The free certificate quota is deducted first. If it is used up, the quota in a free certificate package is deducted.

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

Last updated：2024-03-06 18:00:08

How to fill in the Bound Domain during the certificate application?

After purchasing the SSL certificate, you need to go to the SSL Certificate Service console to submit the materials for review. The console will prompt you the type and number of domain names based on the certificate you purchased.

Note:

Unable to bind a **.ru** domain name to an SSL certificate.

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

Some certificates can be bound with IP addresses. For details, see SSL Certificates Supporting IP Address Binding.

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:

Certificate /TypeRule	GlobalSign	TrustAsia (OV/EV)	TrustAsia (DV)	GeoTrust
If the bound domain is not prefixed with `www.`, the respective `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 be offered for free only if the general or wildcard domain is of level three or above.

Wildcard domains

A wildcard domain is one with a wildcard, such as `*.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.

Wildcard SSL Certificates

Last updated：2024-03-06 18:00:08

What domain names are supported by wildcard certificates?

Tencent Cloud SSL certificates can be wildcard certificates. A wildcard certificate can secure a single server domain name and all the sub-domain names of the same level.
A wildcard certificate covers all sub-domain names of the same level. For example, both `*.tencent.com` and `*.cloud.tencent.com` are wildcard domain names.
Currently, wildcard certificates 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, 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 can't I use file verification when applying for wildcard certificates?

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

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

Last updated：2024-03-06 18:00:08

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：2024-03-06 18:00:08

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：2024-03-06 18:00:09

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：2024-03-06 18:00:08

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:

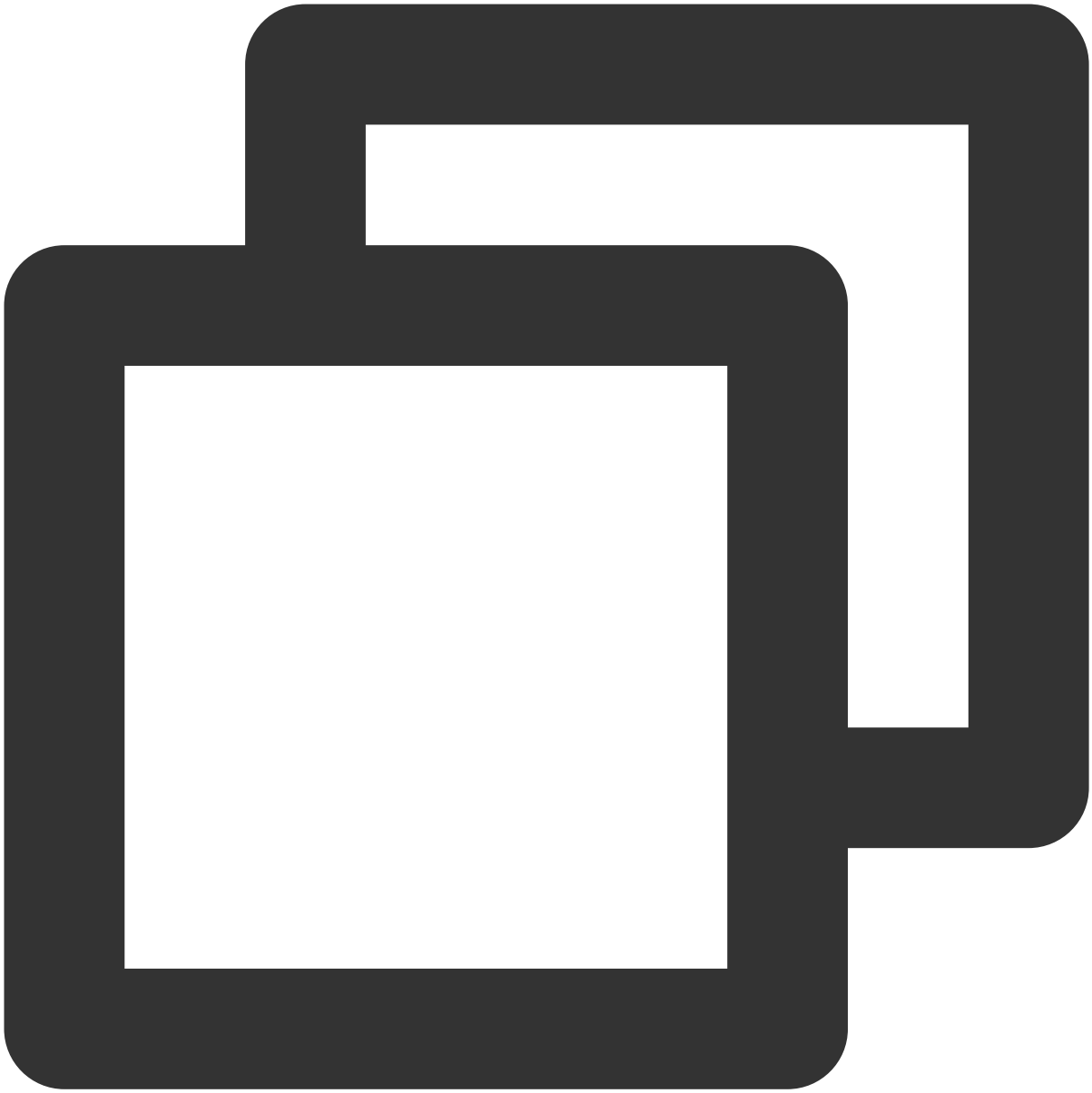
UTF-8 encoding is required for input information. Specify UTF-8 encoding when you use OpenSSL to configure the CSR.

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
```

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.

What Is Private Key Password?

Last updated：2024-03-06 18:00:08

What is the private key password for an SSL certificate?

An SSL certificate uses public key encryption and symmetric key encryption to encrypt data transmission between the client and server, so as to ensure data confidentiality and integrity as well as identity authenticity of the communicating parties. Private key disclosure for an SSL certificate will result in disclosed keys of encrypted sessions, posing the risk of website data leakage. A private key password for the SSL certificate provides an additional layer of security to the private key.

When you apply for a Tencent Cloud SSL certificate, a private key password option will be available. If you specify a private key password, the private key file in the issued SSL certificate will be protected with this password. If you do not specify a private key password, a private key password will be automatically generated, and the private key password file (e.g., `keystorePass.txt`) will be contained in the package.

When will I use a private key password?

Generally, you need to use a private key password when installing an SSL certificate to a web service. For example, when you install an SSL certificate on a Tomcat server, the field `keystorePass=` represents the private key password.

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

If you want to specify a private key password when applying for a Tencent Cloud SSL certificate, set a complex one.

Keep your private key password properly for security of your SSL certificate.

Keep your private key password confidential. Tencent Cloud will not store your private key password. For more information, see Forgot Your Private Key Password?

Forgot Your Private Key Password?

Last updated：2024-03-06 18:00:08

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.For more information, see Reissuing an SSL Certificate

Reapply for a certificate.

For more information about applying for a paid certificate, please see Purchasing Process.

Can an SSL Certificate Be Revoked?

Last updated：2024-03-06 18:00:09

Can a certificate be revoked?

Yes. For detailed directions, see Revoking an SSL Certificate.

What are the differences between RSA and ECC?

Last updated：2024-03-06 18:00:08

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

Last updated：2024-03-06 18:00:08

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

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

What’s the Difference Between Certificate Reissue and Reapplication?

Last updated：2024-03-06 18:00:08

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.

Which SSL Certificate Types Are Supported for Mini Programs?

Last updated：2024-03-06 18:00:08

Which SSL certificate types are supported for mini programs?

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

SSL Certificate Management
What Should I Do If the Quick HTTPS Plan Will Expire Soon?

Last updated：2024-03-06 18:00:37

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

If you want to continue your use of the quick HTTPS feature, go to the SSL Certificate Service console to renew and upgrade it.

If you no longer want to use the feature, we recommend that you switch the connected domain to the origin before the quick HTTPS plan expires to avoid affecting normal access after the expiration. The following are directions for DNSPod:

1. Log in to the DNSPod console.
2. Click the target **domain** to enter the **Record Management** page.
3. Search for the CNAME record type of the connected domain and change the **Record Value** to your origin address.

Note:

If your origin address is an IP, change the **Record Type** to **A record** and enter the origin IP in **Record Value**.

4. Click **OK**.

My Profile

Last updated：2024-03-06 18:00:37

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

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

How many instances can be created in my profile?

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

How long does it take to review an organization profile?

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

Note:

The CA will prioritize organization profiles of paid certificates if there are a large number of applications.

How Do I View the Certificate Information?

Last updated：2024-03-06 18:00:37

How do I view the certificate information?

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

Note:

If you use a card console, just click the certificate card.

2. On the **Certificate Details** page, view the basic certificate information such as **Certificate Type** and **Expiration Time**.

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

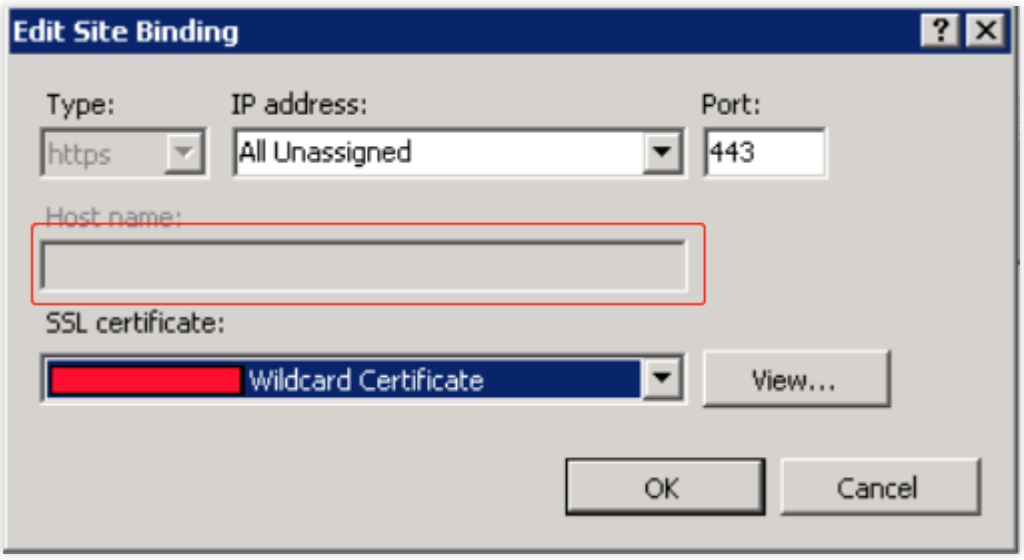
Last updated：2024-03-06 18:01:41

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

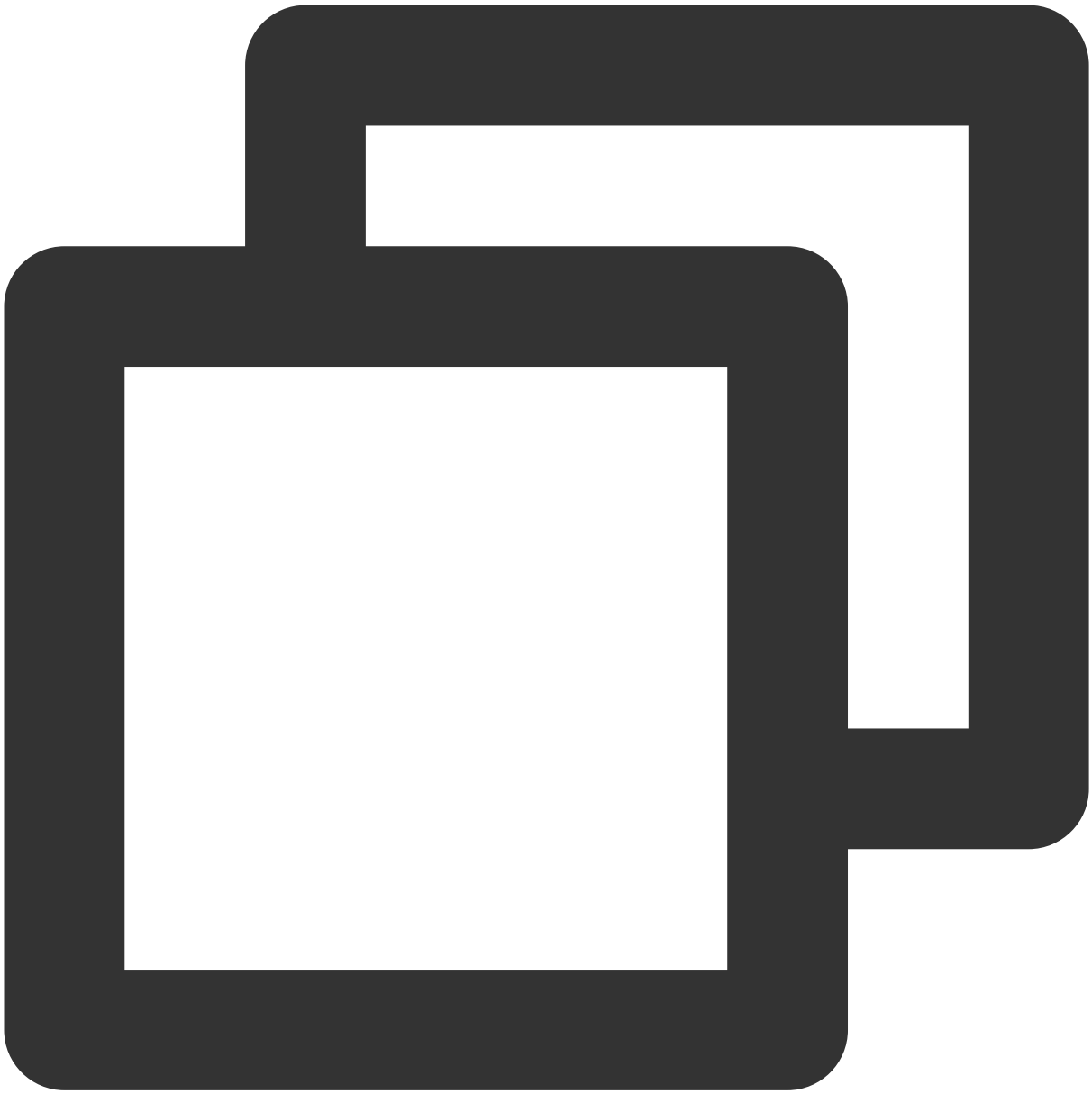
1. Open the `applicationHost.config` file in `C:\\Windows\\system32\\inetsrv\\config\\applicationHost.config`.
2. Make the following modifications:

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.
                <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 Server?

Last updated：2024-03-06 18:01:41

How Do I Enable Port 443 for a Server?

Operate based on the servers you use:

For Tencent Cloud Lighthouse servers, port 443 is enabled by default. For more information, see Managing Firewall.

For Tencent Cloud CVMs, enable port 443 as instructed in Adding Security Group Rules.

For CVMs provided by other vendors, refer to the respective documentation.

Why Does the Website Prompt “Connection Is Untrusted"?

Last updated：2024-03-06 18:01:41

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.qcloud.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：2024-03-06 18:01:41

How do I install OpenSSL?

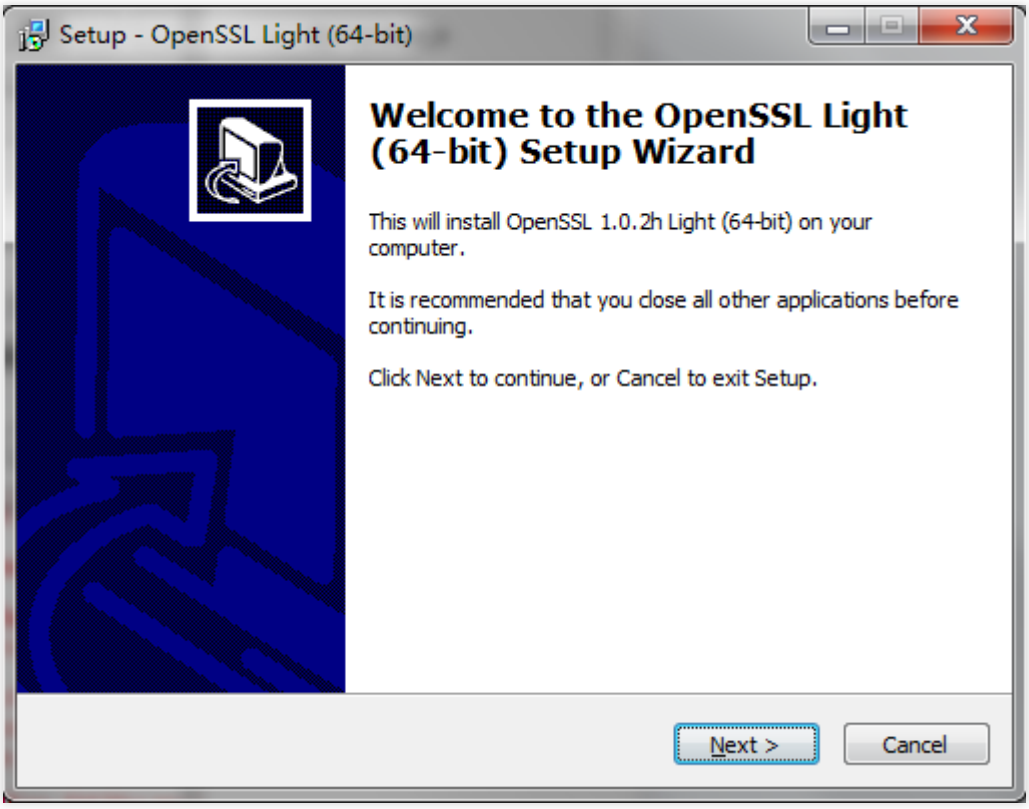
OpenSSL is a well-known open source cryptography toolkit for secure communications, featuring cryptographic algorithms, common passwords, and certificate packaging.

OpenSSL official website

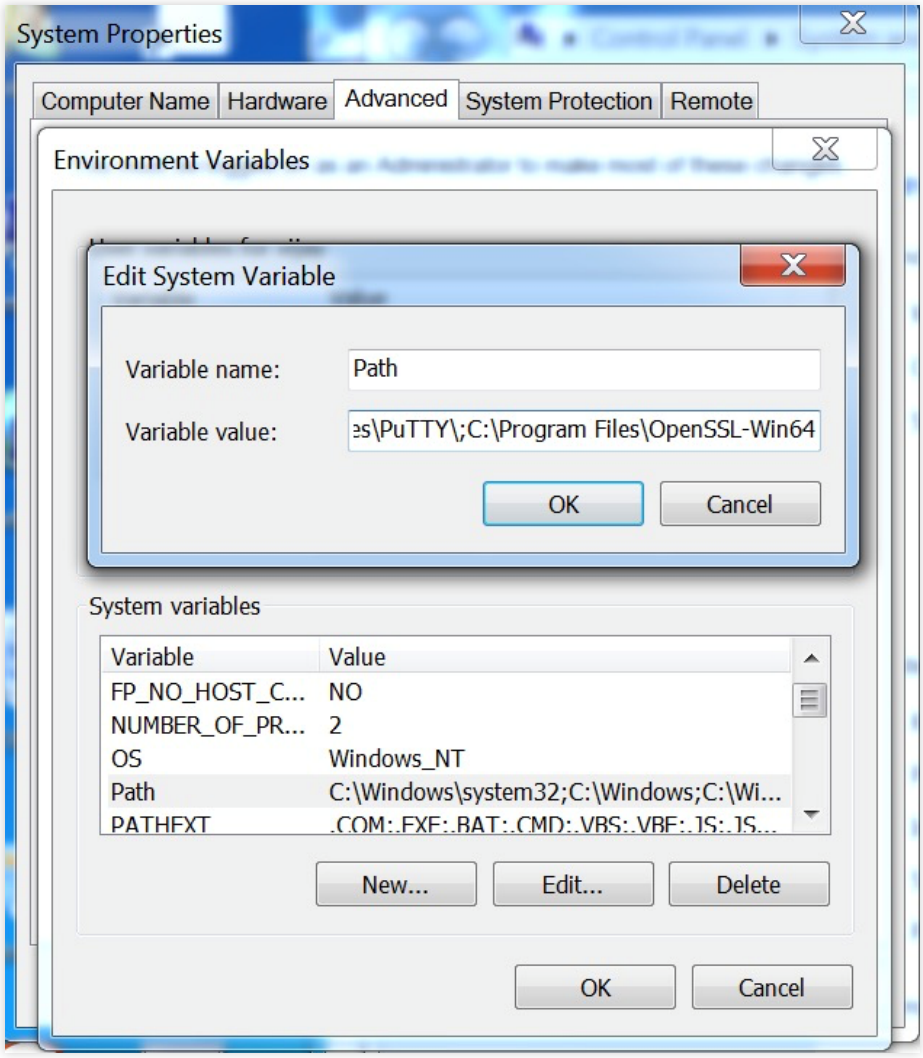
For the official download address: click here.

Installing OpenSSL on Windows

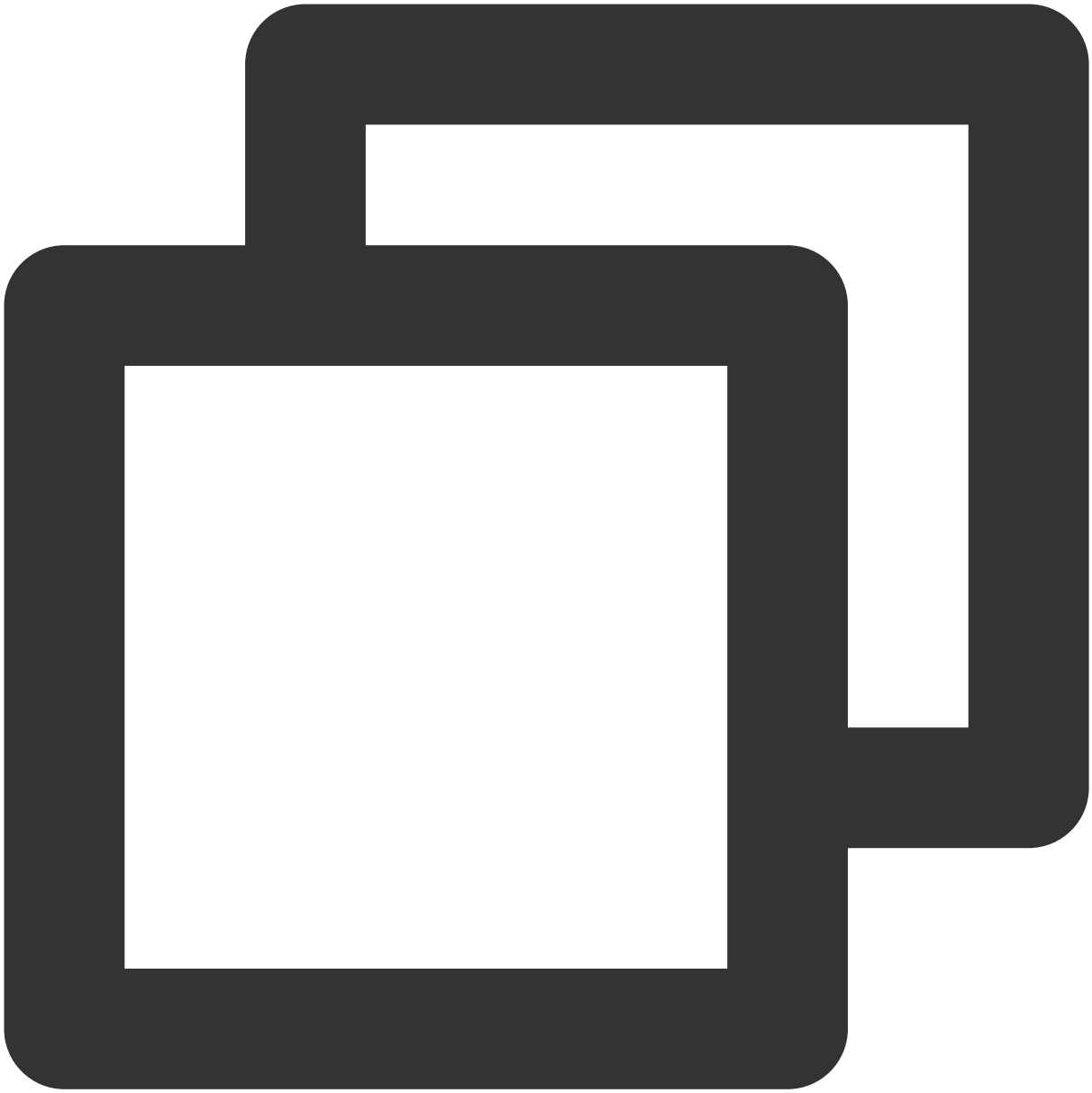
No installation package for Windows is provided on the OpenSSL official website. Instead, you can use tools provided by other open source platforms, such as, Win32/Win64 OpenSSL.
The following describes how installation and usage information Windows users.
1. Download a 32-bit or 64-bit version, for 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:\\OpenSSL-Win64` , copy `C:\\OpenSSL-Win64\\bin;` to **Path**, as shown in the following figure.

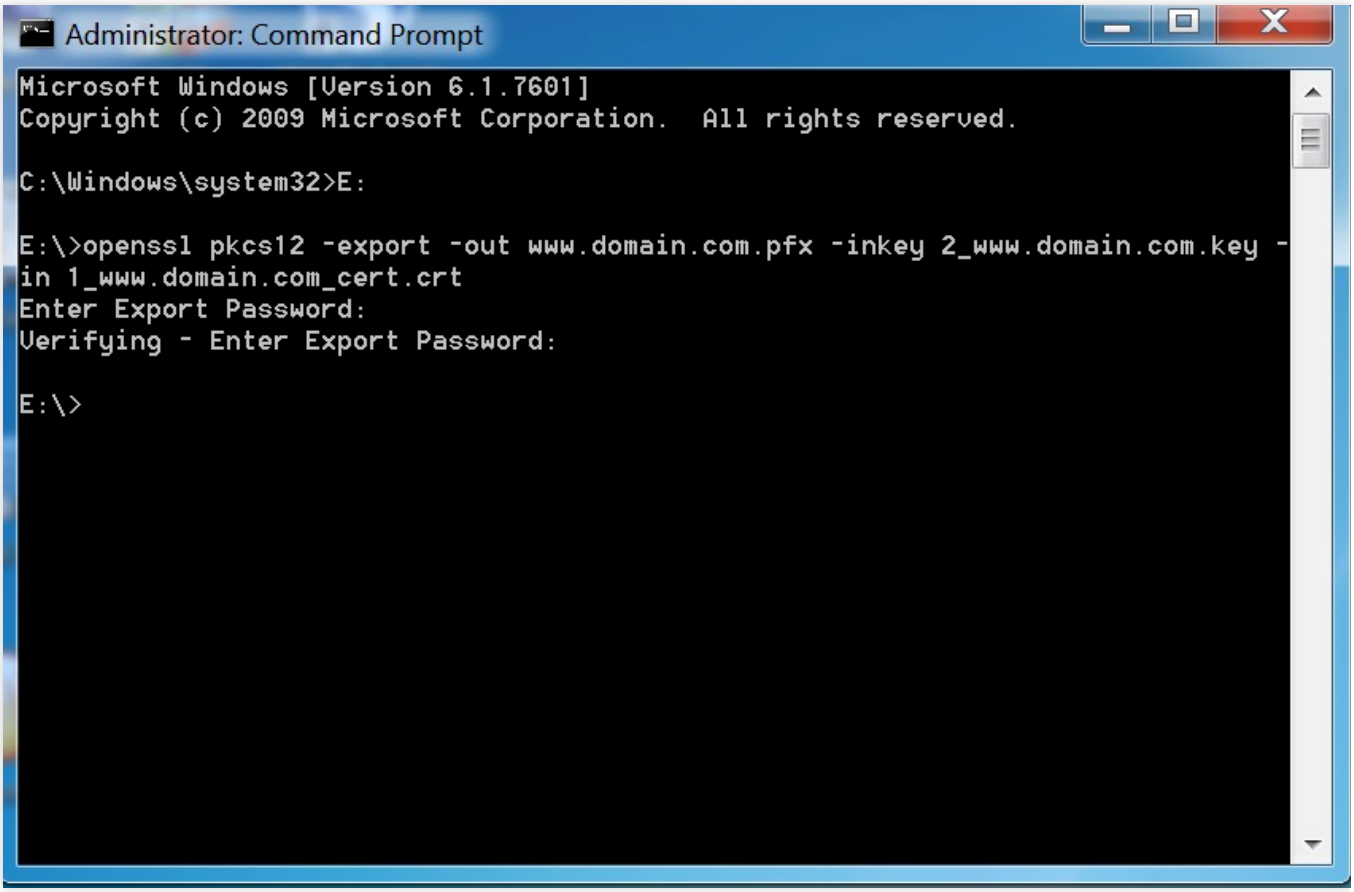


3. Open the Command Prompt (you must be logged in as the admin), go to the directory in which the files `2_www.tencent.com.key` and `1_www.tencent.com_cert.crt` are saved, and run the following command:



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

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



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：2024-03-06 18:01:41

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

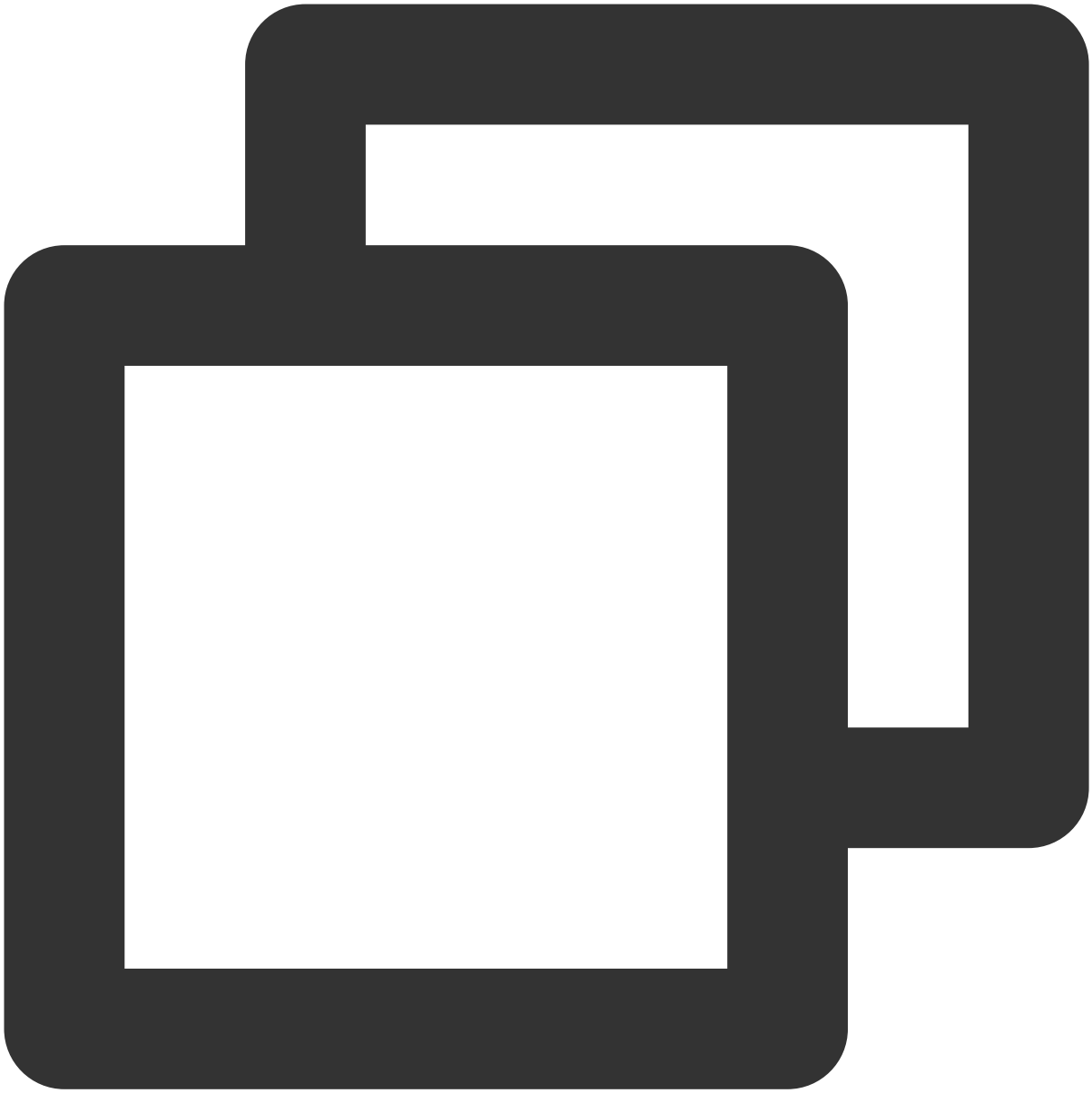
If your SSL certificates are installed in the web service on the server, find `ssl_protocols TLSv1 TLSv1.1 TLSv1.2` in the certificate configuration file of your web service and modify it as needed.
For example, if your certificate needs to support the TLSv1.1 and TLSv1.2 versions, remove `TLSv1` from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

How Can I Combine an SSL Certificate Chain?

Last updated：2024-03-06 18:01:41

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:

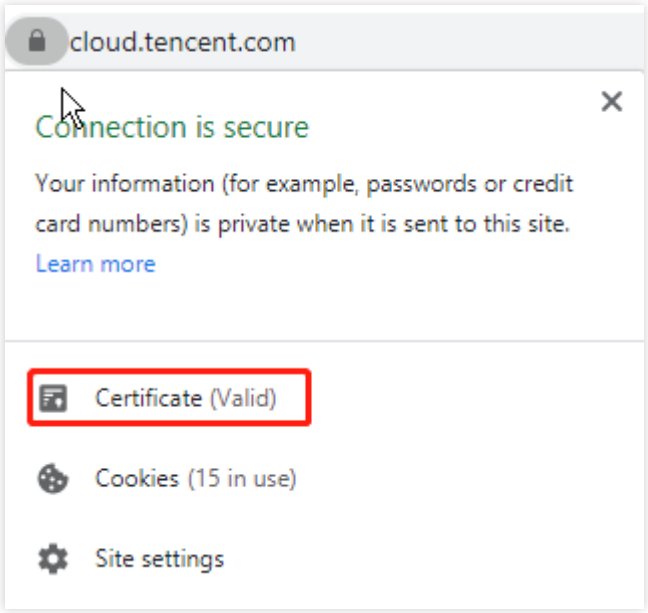
Normally, an SSL certificate chain is made up of the root CA certificate > intermediate CA certificate(s) > domain certificate. There may be multiple intermediate certificates.

International standard SSL certificates provided by Tencent Cloud are complete certificate chains, which are available without needing to be combined.

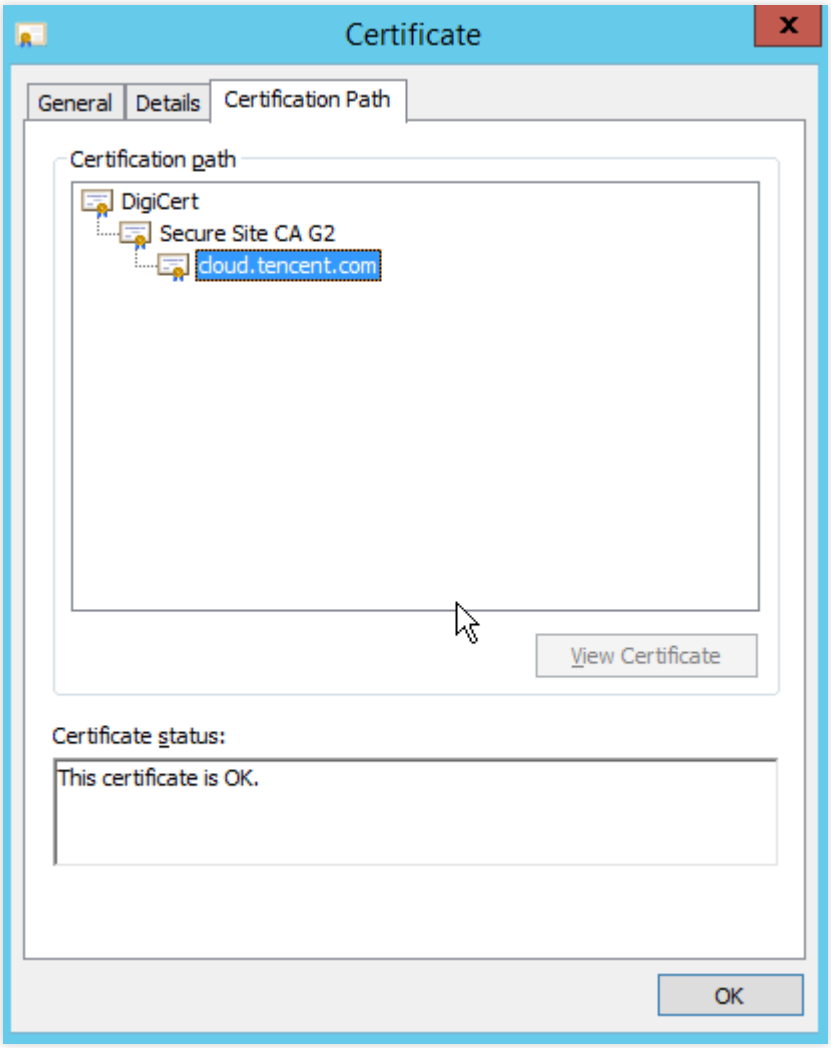
How can I view the SSL certificate chain?

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:



Can Tencent Cloud SSL Certificates Be Used for WebSocket?

Last updated：2024-03-06 18:01:41

Can Tencent Cloud SSL certificates be used for WebSocket?

Yes. You can deploy SSL certificates directly to your WebSocket service for encrypted transmission.

How Do I Enable the IIS Service?

Last updated：2024-03-06 18:01:41

How do I enable the IIS service?

1. Search for "control panel" and open the **Control Panel** window.
2. Click **Programs and Features** to enter the corresponding management page.
3. On the left sidebar, click **Turn Windows features on or off**.
4. In the **Windows Features** pop-up window, find and select all the options of **Internet Information Services**.
5. Click **OK**.

What Should I Do If I Am Prompted That HTTPS Is Not Secure After Reapplying for Deployment upon Expiration of the SSL Certificate?

Last updated：2024-03-06 18:01:41

What should I do if I am prompted that HTTPS is not secure after reapplying for deployment upon expiration of the SSL certificate?

A browser will prompt that HTTPS is not secure after SSL certificate expiration. Specifically, you will still get this prompt when accessing a website after replacing the expired certificate, as the browser caches your certificate information. We recommend that you replace a certificate before expiration to avoid any impact on your business.

Note:

In the case of redeployment after SSL certificate expiration, clear the browser cache first before access.

SSL Certificate Region
Are There Any Region Restrictions on SSL Certificate Installation?

Last updated：2024-03-06 18:03:03

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：2024-03-06 18:03:03

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：2024-03-06 18:03:04

Causes and Handling Methods for Certificate Review Failures

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

Verification file configuration error

Note:

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 verification when submitting your SSL certificate order for review, the domain 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 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 verification instead.

DNS configuration error

Causes

If you choose DNS verification as the method for domain 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 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 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 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 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.

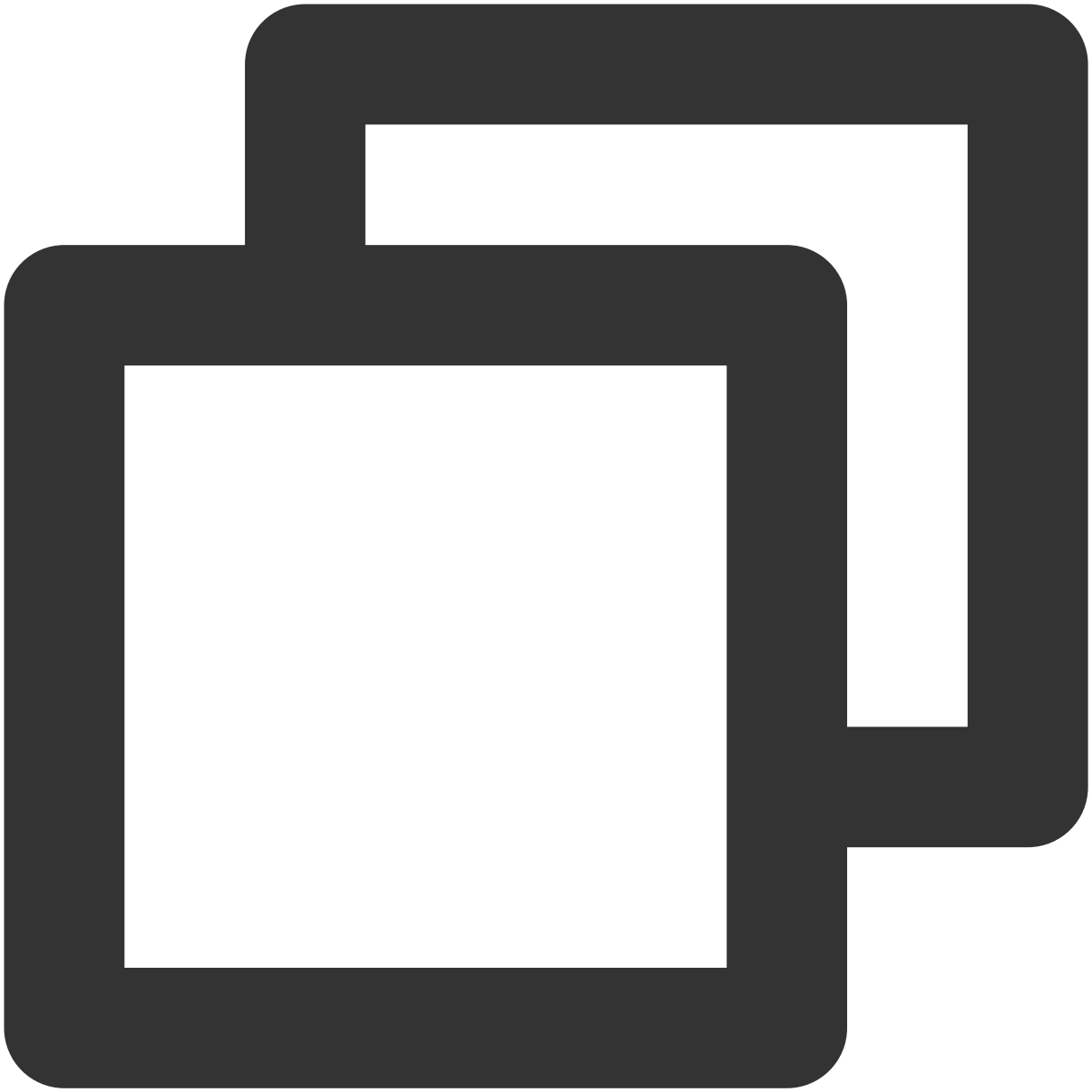
Solutions

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 a review failure message.

The message content is similar to the following:



```
The domain did not pass the CA security verification. Domain certificate applicatio
```

Causes

Due to CA's anti-phishing mechanism, sensitive words contained in domain names, such as "bank" and "pay", can cause security review failure. 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.

The following are sensitive words that may cause domain names to fail the security review. They are only examples, and the specific sensitive words are defined by CA.

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

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 quickly issued through automatic authentication without manual intervention, we use stringent sensitive words filters to set the verification standard.

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

Last updated：2024-03-06 18:03:03

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.

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

Last updated：2024-03-06 18:03:04

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

After you submit a certificate application, the CA will review your domain and submitted information and issue the certificate after approval. If your certificate has not been issued for a long time, we recommend that you check the domain validation result as follows.

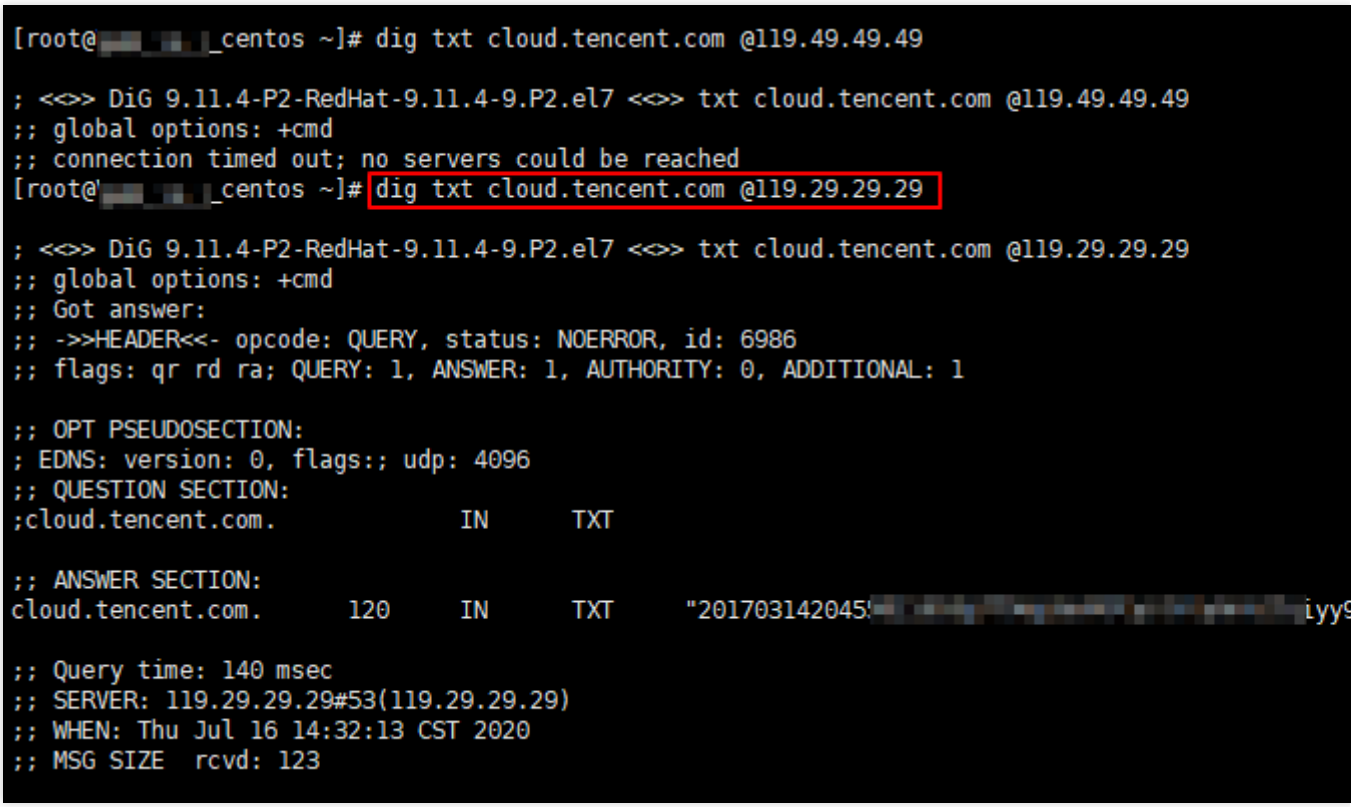
Note:

SSL Certificate Service provides hosts with fully qualified domain names (FQDNs). If your domain management system does not support them, remove the suffix of the root domain.

DNS validation type

1. Log in to your domain server and run the `dig` command to query the DNS record.
2. Run the `dig + record type + @119.29.29.29` command to specify to use the DNSPod DNS for validation.

For example, `dig txt cloud.tencent.com @119.29.29.29`



If the returned result contains a TXT record similar to that in the figure and the record value is the same as that on the **Certificate Details** page in the SSL Certificate Service console, your DNS configuration is correct and has taken

effect.

If the returned result does not contain a TXT record, it's possible that the DNS configuration is incorrect or has not taken effect.

If the DNS configuration is incorrect, go to the SSL Certificate Service console and click the **Pending validation** tab to enter the **Certificate Details** page. Copy the record value in **Certificate Details** and update the record at your DNS service provider. If the configuration has not taken effect for a long time, contact your domain hosting provider.

Note:

For detailed directions, see DNS Validation.

File validation type

1. Log in to the SSL Certificate Service console and click the **Pending validation** tab to enter the **Certificate Details** page.

2. Click to access the validation URL. If the accessed page displays the same content as the validation file content on the **Certificate Details** page, the access is normal; otherwise, check the following:

Check whether the validation URL has an address accessible over HTTPS, and if so, use the HTTPS address in the browser for another access. If the browser prompts that the certificate is untrusted or the displayed content is incorrect, disable the HTTPS service of the domain.

Check whether the validation URL can be accessed anywhere. As the servers for validating certificates of each brand are located in different regions, you should check whether your site has an image outside the Chinese mainland or whether the smart DNS service is used.

File validation requires responding to status code 200 and file content directly and does not support redirects of any kind. Check whether the validation URL has the 301 or 302 redirect, and if so, disable the redirect.

Note:

You can run the `wget -S URL` command to check whether the validation URL has a redirect.

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

Last updated：2024-03-06 18:03:04

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：2024-03-06 18:03:03

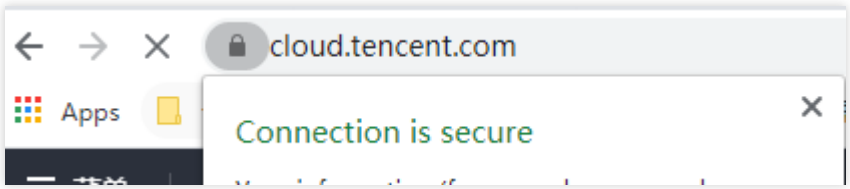
How do I check in a browser whether an SSL certificate has taken effect?

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：2024-03-06 18:03:04

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.

What Should I Do If the Issue of a Free SSL Certificate Takes Too Long or Failed?

Last updated：2024-03-06 18:03:04

This document describes how to troubleshoot a failure to issue the free SSL certificate due to domain ownership verification timeout when you apply for the certificate from Tencent Cloud.

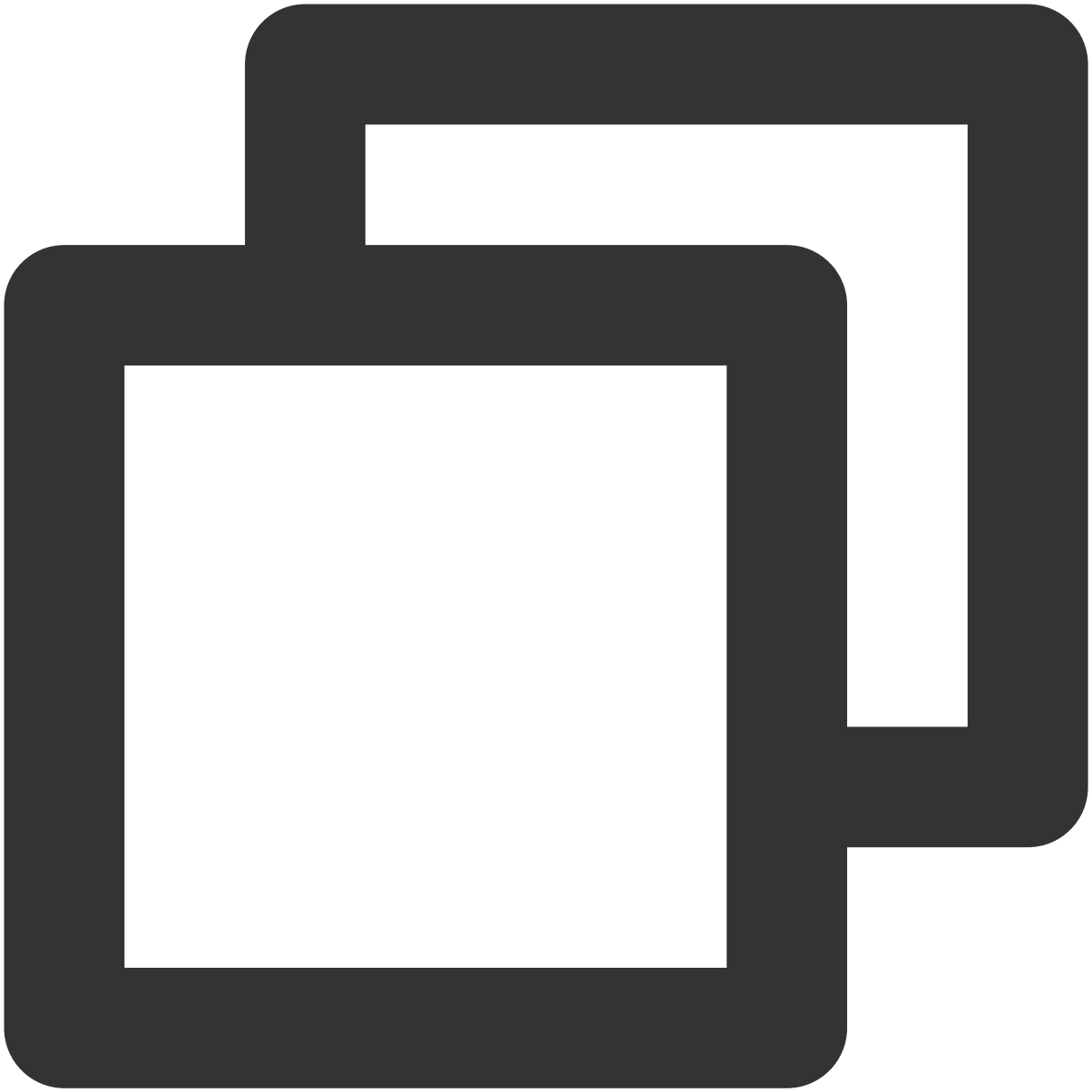
Note:

It generally takes up to 30 minutes to issue a free SSL certificate, after which you can troubleshoot the timeout as instructed in this document.

Checking the CAA Record

CAA records need to be checked for both file validation and DNS validation. If there are no CAA records or they contain `0 issuewild "sectigo.com"` and `0 issue "sectigo.com"`, the check can be passed.

`dig` command



```
dig domain name CAA
```

Everything is normal if the returned value is empty or contains `0 issuewild "sectigo.com"` and `0 issue "sectigo.com"` , as shown below:

```
rttw@Kincaid:~$ dig dnstest.cc caa

; <<>> DiG 9.18.1-1+0~20220316.73+debian11~1.gbp965910-Debian <<>> dnstest.cc c
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18535
;; flags: qr rd ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;dnstest.cc.                    IN      CAA

;; ANSWER SECTION:
dnstest.cc.             0       IN      CAA     0 issue "sectigo.com"
dnstest.cc.             0       IN      CAA     0 issuewild "sectigo.com"

;; Query time: 1270 msec
;; SERVER: 172.29.112.1#53(172.29.112.1) (UDP)
;; WHEN: Tue Mar 29 13:06:58 CST 2022
;; MSG SIZE  rcvd: 102

rttw@Kincaid:~$
```

DNS diagnosis tool

Go to the DNS diagnosis tool, enter the primary domain, select **CAA**, and click **Check**. Everything is normal if the returned value is empty or contains `0 issuewild "sectigo.com"` and `0 issue "sectigo.com"` .

Note:

If the check fails or only certain regions can be checked, check the DNS settings of the domain.

Solution

If the returned result is not empty and does not contain `0 issuewild "sectigo.com"` and `0 issue "sectigo.com"` , add the following records to the DNS settings:

Host	Record Type	Split Zone	Record Value
@	CAA	Default	0 issuewild "sectigo.com"
@	CAA	Default	0 issue "sectigo.com"

Checking the DNS Record

After checking the CAA record, check whether the validation record has been added. For self-built NS servers or those with DNS query limits outside the Chinese mainland, check whether the DNS query outside the Chinese

mainland is normal with the DNS diagnosis tool or DNSCHCKER. In general, all monitored points can return values and their returned values are the same.

1. Determine the domain to be checked.

The domain to be checked should be in the format of `host.domain` ; for example, if the certificate's host is `_26A56EBADCE479E******5D304C0D8.blog` and the domain is `dnspod.cn` , the domain to be checked should be `_26A56EBADCE479E******5D304C0D8.blog.dnspod.cn` .

2. Go to the DNS diagnosis tool, enter the target domain, select **CNAME**, and click **Check**. Everything is normal if the returned value is the record value prompted in the console.

Checking Whether the Validation IP Is Blocked by the Server

If you wait a long time for the certificate to be issued by the CA after passing the file validation, it's possible that the server or data center has blocked the CA's validation IPs (`64.78.193.238` and `216.168.247.9`). In that case, add them to the allowlist.

SSL Certificate Billing and Purchase
Are DV Certificates Permanently Free?

Last updated：2024-03-06 18:03:03

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 **1 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：2024-03-06 18:03:04

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：2024-03-06 18:03:04

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.

Viewing of SSL Certificate Expiration Time

Last updated：2024-03-06 18:03:04

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 and **SSL certificate notifications** and **Product service notifications** are not selected under **Product notifications**, you will not receive certificate expiration notifications through the Message Center, email, or SMS.
For certificates of other vendors uploaded to Tencent Cloud, if message subscriptions are configured for them, you will also receive certificate expiration notifications.
Certificate expiration notification time: the renewal channel will be opened within 30 days before certificate expiration, and the expiration reminder will be sent the next day after the renewal channel is opened.

How do I receive certificate-related system notifications?

1. Log in to the Message Center.
2. On the **Message Subscription** page, select **SSL certificate notifications** and **Product service notifications** under **Product notifications**, and then select the desired notification types.

Is an SSL Certificate Still Available After I Renew It?

Last updated：2024-03-06 18:03:04

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.