

# **SSL Certificate Service**

## **Domain Ownership Validation**

### **Product Documentation**



## Copyright Notice

©2013-2024 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

## Domain Ownership Validation

- Domain Validation Method Selection

- Automatic DNS Addition

- DNS Validation

- File Validation

- Automatic DNS Validation

- Automatic File Validation

- Validation Result Troubleshooting Guide

# Domain Ownership Validation

## Domain Validation Method Selection

Last updated : 2024-03-06 17:24:16

This document describes how to select a proper domain validation method when you apply for a certificate or add a domain in the SSL Certificate Service console.

### Domain validation method

SSL Certificate Service supports the following domain validation methods:

Validation Method	Use Cases	Use Limits
<a href="#">Automatic DNS addition</a>	You can select automatic DNS addition for the required domain ownership verification when you apply for an SSL certificate.	You must use a DNSPod domain.
<a href="#">DNS validation</a>	You can select DNS validation for the required domain ownership verification when you apply for an SSL certificate.	You need to have the DNS permission for the domain. This is applicable to domains resolved on any platform.
<a href="#">File validation</a>	You can select file validation for the required domain ownership verification when you apply for an SSL certificate.	This process is complex and requires a basic knowledge of website development.
<a href="#">Automatic DNS validation</a>	You can apply for multi-year international standard certificates only. For more information, see <a href="#">Available Multi-Year International Standard Certificates</a>	You need to have the DNS permission for the domain.
Automatic file validation	You can apply for multi-year international standard certificates only. For more information, see <a href="#">Available Multi-Year International Standard Certificates</a>	This process is complex and requires a basic knowledge of website development. Wildcard domains are not supported.

# Automatic DNS Addition

Last updated : 2024-03-06 17:24:16

## Overview

This document describes how to validate a domain through automatic DNS addition when you apply for a certificate or add a domain in the SSL Certificate Service console.

## Directions

1. The automatic DNS addition option will be available for quickly adding a record if the following conditions are met.

Use case

[Adding a domain.](#)

Applying for certificates of certain brands.

Use limits: You must use a DNSPod domain.

2. The system will automatically add the specified DNS record for the domain and complete domain ownership verification.

3. After the certificate is issued or the domain information is approved, you can manually clear the DNS record.

# DNS Validation

Last updated : 2024-03-06 17:24:16

## Overview

This document describes how to validate a domain when you apply for a certificate or add a domain in the certificate management console and the domain validation mode is DNS validation.


## Directions

### Step 1. View validation information

1. Log in to the [SSL Certificate Service console](#).
2. Select a certificate in the **Validating** state. On the **Validate Domain** page displayed, obtain the host record and record value. See the figure below.

#### Note:

Take note of the host record and record value before you go to step 2 to add a DNS record.

 **Certificate Details**

**Basic Info**

ID

uV...DR

States

**Waiting for DNS verification**  
Please add the following DNS record

Domain name	Host record	Record type	Record value
... .net	_F0D0C111B3204D DCI...B0 91A	CNAME	5B866C23EBE4EA0...9B842436C 5.TTDrPq70vb.trust-provider.com

Certificate type

TrustAsia TLS RSA CA(1years)

Common name

www.y... .net

Submission date

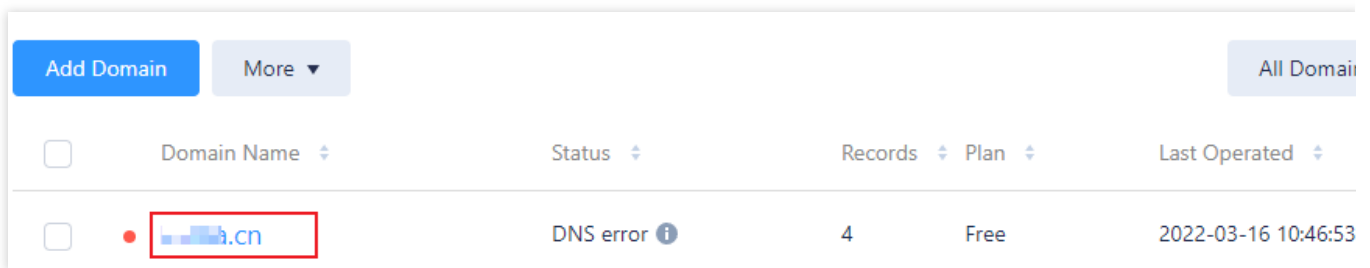
2022-03-16 10:42:26

## Step 2. Add a DNS record

### Note:

The following operations apply only to domain names hosted with Tencent Cloud. For domain names hosted with other platforms, go to the corresponding **DNS service provider** for DNS. To query DNS service providers, go to [DNS.TECH](#).

1. Obtain the host record and record value, which can be obtained on the **Validate Domain** page, as described in step 1.
2. Log in to the [DNSPod console](#) to view the domain name for which a certificate has been applied, and then click **DNS** in the **Operation** column to go to the **Record Management** page. See the figure below.



<input type="checkbox"/>	Domain Name	Status	Records	Plan	Last Operated
<input type="checkbox"/>	xx.com.cn	DNS error	4	Free	2022-03-16 10:46:53

3. Click **Add Record** and add a DNS record depending on the certificate type.

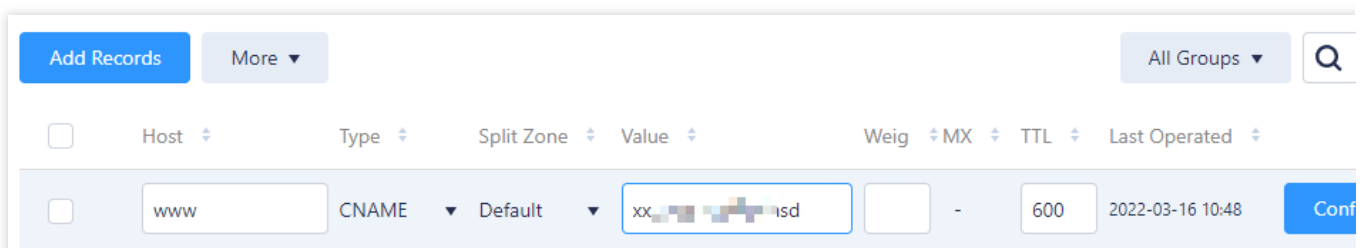
### Note:

Only the CNAME and TXT types of DNS records are supported, and they are applicable for certificates of different brands. Please select the DNS record type as needed.

TrustAsia and WoTrus Certificates

Certificates of Other Brands

For TrustAsia and WoTrus certificates, enter a DNS record of the CNAME type. See the figure below:



<input type="checkbox"/>	Host	Type	Split Zone	Value	Weight	MX	TTL	Last Operated	
<input type="checkbox"/>	www	CNAME	Default	xx.com.cn		-	600	2022-03-16 10:48	Conf

**Host:** enter the host record obtained in [step 1](#).

**Type:** select **CNAME**.

**Split Zone:** select **Default**. Otherwise, the corresponding CA will not be able to review the DNS record.

**Value:** enter the record value obtained in [step 1](#).

**MX Priority:** leave it empty.

**TTL:** it refers to the time to live. The smaller the value is, the less the time cost for record changes to take effect globally. The default value is 600 seconds.

For certificates of other brands, enter a DNS record of the TXT type. See the figure below.

The screenshot shows the 'Add Records' interface in the Tencent Cloud DNS console. At the top, there are buttons for 'Add Records' and 'More', and a dropdown for 'All Groups'. Below is a table with columns: Host, Type, Split Zone, Value, Weight, MX, TTL, and Last Operated. A new record is being added with the following details: Host is 'www', Type is 'TXT', Split Zone is 'Default', Value is a base64-encoded string, Weight is '-', MX is '-', TTL is '600', and Last Operated is '2022-03-16 10:48'.

	Host	Type	Split Zone	Value	Weight	MX	TTL	Last Operated
<input type="checkbox"/>	www	TXT	Default	[Base64 String]	-	-	600	2022-03-16 10:48

**Host:** enter the host record obtained in [step 1](#).

**Type:** select **TXT**.

**Split Zone:** select **Default**. Otherwise, the corresponding CA will not be able to review the DNS record.

**Value:** enter the record value obtained in [step 1](#).

**MX Priority:** leave it empty.

**TTL:** it refers to the time to live. The smaller the value is, the less the time cost for record changes to take effect globally. The default value is 600 seconds.

4. Click **Save**.

5. After the record is added, the system periodically checks for the record value. If the record value is detected and matches the specified value, the domain ownership verification will be completed. Please wait for the CA's review.

**Note:**

DNS usually takes effect within **10 minutes to 24 hours**. The actual time depends on the ISP refresh time.

After the certificate is issued or the domain name information is approved, you can manually clear the DNS record.



# File Validation

Last updated : 2024-03-06 17:24:16

## Overview

This document describes how to validate a domain when you apply for a certificate or add a domain in the SSL Certificate Service console and the domain validation mode is file validation.

## Validation Rules

### Domain validation rules

During file validation, pay attention to the following:

#### Note:

Due to changes of the policies for SSL certificate domain validation, Tencent Cloud discontinued the file validation mode for wildcard certificates on **November 21, 2021**. For more information, see [Domain Ownership Validation Policy Update](#).

If the domain that you apply for is a primary domain, **www** must also be validated. For example, if the domain applied for is `tencent.com`, `www.tencent.com` must also be validated.

If the domain that you apply for contains **www**, the domain name following **www** must also be validated, regardless of the domain levels. For example, if the target domain is `www.a.tencent.com`, `a.tencent.com` must also be validated.

If the domain that you apply for does not contain **www** and is not a primary domain, only the current domain needs to be validated. For example, if the target domain is `cloud.tencent.com`, only `cloud.tencent.com` needs to be validated.

### CA validation rules

During DNS query, you must recursively query the authoritative NS server of each domain on the authoritative root server, and then query the corresponding A, AAAA, or CNAME records from the NS server.

If the DNS service supports DNSSEC, you must verify the signing information of the response data.

If the queried domain is an IP address, verify the content via IP access.

The standard HTTP/HTTPS default port must be adopted for access.

Up to two 301/302 redirections are supported. The redirection destination IP and the validated domain must be in the same primary domain.

In the final validation result, the status code 200 must be returned.

For HTTPS access, certificate errors can be ignored.

# Directions

## Step 1. View validation information

1. Log in to the [SSL Certificate Service console](#).
2. Select a certificate in the **Validating** state. On the **Validate Domain** page displayed, follow instructions on the page to complete validation within a specific period of time.

## Step 2. Add a file record

1. Log in to the server and make sure that the domain name points to the server and the corresponding website is enabled.

### Note:

- If your **DNS Service Provider** is Tencent Cloud, for how to point the domain to your server, see A Record.
2. Create the specified file in the root directory of the website, including the file directory, name, and content.

### Note:

The website root directory refers to the folder where you store the website programs on the server. Its name may be `wwwroot` , `htdocs` , `public_html` , or `webroot` .

Ensure that the website port is set to 80 or 443.

### Example

The root directory of your website is `C:/inetpub/wwwroot` . You can create a file as shown in the following table in the `wwwroot` folder.

File Directory	File Name	File Content
<code>/.well-known/pki-validation</code>	<code>201908060**alzeo</code>	The file content shown on the validation page. Example: <code>A32CF****7EEtrust-provider.comTT**bu6</code>

### Note

The above is for reference only, and both the filename and content are random values. The values shown on your validation page shall prevail.

On Windows, you need to create a file and folder that begin with a dot by running commands.

For example, to create a `.well-known` folder, open a command prompt window and execute the command `mkdir .well-known` to create it. See the following figure.

```
Microsoft Windows [Version 10.0.17134.0]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\user>cd ..
C:\Users>cd ..
C:\>cd inetpub
C:\inetpub>cd wwwroot
C:\inetpub\wwwroot>mkdir .well-known
```

3. On the **Validate Domain** page, you can click **View Domain Ownership Validation Status** to check whether the configuration is successful.

**Note:**

Both HTTP and HTTPS are supported, and either can be accessed.

File verification does not support any redirection. Instead, it directly returns the status code 200 and file content.

For a domain name starting with "www", such as `www.a.tencent.com`, file validation is required for the domain name itself as well as `a.tencent.com`.

4. Wait for the CA's review. After the certificate is issued or the domain name information is approved, the file and directory can be cleared.

# Automatic DNS Validation

Last updated : 2024-03-06 17:24:16

## Overview

This document describes how to validate a domain through automatic DNS validation when you apply for a certificate or add a domain in the SSL Certificate Service console.

### Note:

Automatic DNS validation is supported for multi-year international standard certificates only. For more information, see [Available Multi-Year International Standard Certificates](#).

## Directions

### Step 1. View validation information

1. Log in to the [SSL Certificate Service console](#). In the left sidebar, click **My Profile** to go to the **My Profile** page.
2. On the **My Profile** page, click the name of the organization for which domain information is to be validated. Then you can view the information of administrators that have been applied for.
3. Click the target administrator name to enter the **Review Information** page.
4. Click the *\*Domain Information* tab, select the target domain, and click **View Validation**.
5. On the **Validate Domain** page, add a DNS record as prompted and within the specified period of time.

### Step 2. Add a DNS record

#### Note:

The following operations apply only to domains hosted with Tencent Cloud. For those hosted with other platforms, go to the corresponding DNS service provider.

1. Get the **host** and **record value** as shown in the figure in substep 5 in **Step 1. View validation information**.
2. Log in to the [DNSPod console](#) to view the target domain and click **DNS** in the **Operation** column to enter the **Record Management** page.
3. Click **Add Record** to add a CNAME record.

**Host:** Enter the obtained host.

**Record Type:** Select **CNAME**.

**Split Zone:** Make sure that it is **Default**, or resolution may fail for some users.

**Record Value:** Enter the obtained record value.

**MX Priority:** leave it empty.

**TTL:** it refers to the time to live. The smaller the value is, the less the time cost for record changes to take effect globally. The default value is 600 seconds.

4. Click **Save**.

5. After adding the record successfully, wait for the CA to scan and review it. If it can be found and matches the specified value, the review is completed.

**Note:**

DNS usually takes effect within **10 minutes to 24 hours**. The actual time depends on the ISP refresh time.

Do not delete or modify the configured CNAME record; otherwise, the proxy will not work.

Do not configure the TXT record for a domain if the CNAME record is already configured; otherwise, domain validation may fail.

If anything goes wrong during this process, [contact us](#).

6. On the **Validate Domain** page, click **Validate** to check whether the CNAME record has been added successfully.

# Automatic File Validation

Last updated : 2024-03-06 17:24:16

## Overview

This document describes how to validate a domain when you apply for a certificate or add a domain in the certificate management console and the domain validation mode is automatic file validation.

### Note:

Automatic file validation applies only to multi-year international standard certificates and non-wildcard certificates.

## Validation Rules

### Domain name validation rules

During automatic file validation, pay attention to the following:

### Note:

Due to SSL certificate domain validation policy changes, Tencent Cloud discontinued the file validation mode for wildcard certificates on **November 21, 2021**. For more information, please see [Domain Validation Policy Update](#).

If the domain that you apply for is a primary domain, **www** must also be validated. For example, if the domain applied for is `tencent.com`, `www.tencent.com` must also be validated.

If the domain that you apply for contains **www**, the domain name following **www** must also be validated, regardless of the domain levels. For example, if the domain applied for is `www.a.tencent.com`, `a.tencent.com` must also be validated.

If the domain that you apply for does not contain **www** and is not a primary domain, only the current domain needs to be validated. For example, if the domain applied for is `cloud.tencent.com`, only `cloud.tencent.com` needs to be validated.

### CA validation rules

During DNS query, you must recursively query the authoritative NS server of each domain on the authoritative root server, and then query the corresponding A, AAAA, or CNAME records from the NS server.

If the DNS service supports DNSSEC, you must verify the signing information of the response data.

If the queried domain is an IP address, verify the content via IP access.

The standard HTTP/HTTPS default port must be adopted for access.

Up to two 301/302 redirections are supported. The redirection destination IP and the validated domain must be in the same primary domain.

In the final validation result, the status code 200 must be returned.

For HTTPS access, certificate errors can be ignored.

## Directions

### Step 1. View validation information

1. Log in to the [SSL Certificate Service console](#). In the left sidebar, click **My Profile** to go to the **My Profile** page.
2. On the **My Profile** page, click the name of the organization for which domain information is to be validated. Then you can view the information of administrators that have been applied for.
3. Click the name of the administrator whose domain information is to be validated. The **Review Information** page is displayed.
4. Click the *\*Domain Information* tab, select the domain to be validated, and click **View Validation**.
5. On the **Validate Domain** page, follow the instructions on the page to complete validation within a specific period of time.

### Step 2. Add file validation

1. Log in to the server and ensure that the A record is added for your domain and the A record points to the server.

**Note:**

If your domain name is hosted with Tencent Cloud, point the domain name to your server. For more information, please see **A Record**.

2. Start a web service on the server (or use the web service where the business is running), listen on port 80 or 443, and set the reverse proxy address of the file validation path to the reverse proxy address provided in **Step 1: View validation information (as shown in the figure in substep 5 in step 1)**.

Tencent Cloud provides the following web service configuration guidelines for your reference:

NGINX reverse proxy configuration

Apache reverse proxy configuration

**Note:**

Both HTTP and HTTPS are supported, and either can be accessed.

A configured reverse proxy cannot be deleted or modified. After being deleted or modified, a reverse proxy becomes invalid.

Up to two 301/302 redirections are supported. The redirection destination IP and the validated domain must be in the same primary domain. For a domain name starting with "www", such as `www.a.tencent.com`, file validation is required for the domain name itself as well as `a.tencent.com`.

3. After configuring the reverse proxy, wait for the CA to complete the file validation. After the file validation is passed, the domain is approved.
4. On the **Validate Domain** page, you can click **Validate** to validate the domain configuration.

# Validation Result Troubleshooting Guide

Last updated : 2024-03-06 17:24:16

If you failed manual DNS validation, troubleshoot in either of the following ways:

Tool diagnosis:

Click the [DNS diagnosis tool](#) and enter the content as prompted.

Self-diagnosis:

Check the domain status.

Check whether the domain can be resolved properly. An unverified or newly purchased domain cannot be resolved properly.

Check the DNS server.

Check whether the record is added at the correct DNS service provider. For example, if the DNS server is from `www.net.cn`, it will not work to add the TXT record at DNSPod.

Check the DNS record.

If failure continues after you follow the steps above correctly, you may want to check for typos in the server name, record value, etc. Please confirm that TXT records are entered completely and correctly and wait for 24 hours.

If the DNS record is not approved in 24 hours, [contact us](#) for assistance.