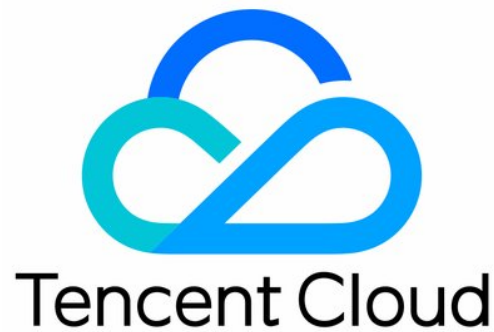


SSL Certificates

Domain Ownership Validation



Copyright Notice

©2013–2023 Tencent Cloud. All rights reserved.

The complete copyright of this document, including all text, data, images, and other content, is solely and exclusively owned by Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"); Without prior explicit written permission from Tencent Cloud, no entity shall reproduce, modify, use, plagiarize, or disseminate the entire or partial content of this document in any form. Such actions constitute an infringement of Tencent Cloud's copyright, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Trademark Notice



This trademark and its related service trademarks are owned by Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliated companies ("Tencent Cloud"). The trademarks of third parties mentioned in this document are the property of their respective owners under the applicable laws. Without the written permission of Tencent Cloud and the relevant trademark rights owners, no entity shall use, reproduce, modify, disseminate, or copy the trademarks as mentioned above in any way. Any such actions will constitute an infringement of Tencent Cloud's and the relevant owners' trademark rights, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Domain Ownership Validation

Domain Validation Method Selection

Automatic DNS Addition

File Validation

Automatic DNS Validation

Automatic file validation

Validation Result Troubleshooting Guide

FAQs

Domain Ownership Validation

Domain Validation Method Selection

Last updated: 2023-09-28 10:14:36

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:

Verification method	Use Cases	Usage Limits
Automatic DNS Addition	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.
DNS Validation	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.
File Verification	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.
Automatic DNS Validation	This method is only applicable for multi-year international standard certificates. For more details, please refer to Multi-year International Standard Certificates .	You need to have the DNS permission for the domain.
Automatic File Verification	This method is only applicable for multi-year international standard certificates. For more details, please refer to Multi-year International Standard Certificates .	This process is complex and requires a basic knowledge of website development. Wildcard domains are not supported.

Automatic DNS Addition

Last updated: 2023-09-28 10:14:51

Scenario

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.

Instructions

1. The automatic DNS addition option will be available for quickly adding a record if the following conditions are met.
 - Use Cases
 - [Adding Domain Information](#) .
 - Applying for certificates of certain brands.
 - Usage Restrictions: A domain resolved by Tencent Cloud DNSPod must be used.
2. The system will automatically add the specified DNS record for the domain name, and automatically complete domain name ownership verification.
3. After the certificate is issued or the domain name information is approved, you can manually clear the DNS record.

File Validation

Last updated: 2023-09-28 10:17:20

Scenario

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 in the SSL certificate domain validation policy, Tencent Cloud discontinued the file validation method for wildcard domain certificates on **November 21, 2021**. For more details, please refer to [SSL Certificate Domain Validation Policy Change Notice](#).
- When applying for a primary domain, additional verification for www is required. For instance, if the application domain is `tencent.com`, then `www.tencent.com` also needs to be verified.
- When applying for a domain with "www", the domain following "www" needs to be additionally validated, regardless of its level. For instance, if the applied domain is `www.a.tencent.com`, then `a.tencent.com` also needs to be validated.
- When applying for a non-primary domain without www, only the current domain needs to be validated. For example, if the applied domain is `cloud.tencent.com`, only `cloud.tencent.com` needs to be validated.

CA validation rules

- During a DNS query, it is imperative to recursively query the authoritative NS server for each domain level from the authoritative root server, and subsequently 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 disregarded.

Instructions

Step 1. View validation information

1. Log in to the [SSL Certificate Service console](#).
2. Select the certificate in **Validation in Progress**, navigate to the **Validate domain** page, and complete the validation process within the specified time frame, as shown below:

Submit certificate application > **2 Validate domain**

1 You need to go to the website root directory to create the specified file

Go to [www.0dukj.cn](#)'s website root directory to create the following file: [View instructions](#)

File location	File name	File content	Download file:
www.0dukj.cn	B.txt	085AF7... trust-provider.com	Download file Download the file and place it in the specified file directory, without changing the filename and file content.

Note:

- Within 3 days, create the file. Otherwise, the application will fail the review.
- Ensure that the website port number is set to 80 or 443, and all regions can match the validation value. If your server blocks access from outside the Chinese mainland, We recommend you allow access from outside the Chinese mainland or add the IPs for CA review to the allowlist: 91.199.212.132, 91.199.212.133, 91.199.212.148, 91.199.212.151, 91.199.212.176, and 54.189.196.217.

2 Verify domain ownership

If you have successfully completed Step 1, the following URLs can access the file content. Please click "Validate domain" to verify the domain ownership.

[Click to validate 0dukj.cn](#) [Click to validate www.0dukj.cn](#)

[Validate domain](#) [Reselect validation method](#)

Step 2. Add a file record

1. Please log in to the server and ensure that the domain name is directed to this server and the corresponding website is functioning properly.

Note

If your domain's **DNS service provider** is Tencent Cloud, refer to [A Record](#) to point your domain to your server.

2. Create the specified file in the root directory of the website. This file should include the file directory, file name, and file 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>	The file content shown on the validation page. Example: <code>A32CF**7EEtrust-provider.comTTbu6</code>	<code>201908060**alz eo</code>

Considerations

- The above is for reference only, and both the filename and content are random values. The values shown on your validation page shall prevail.
- In Windows, you need to create files and folders starting with a dot by executing commands.

For example, to create the `.well-known` folder, open the command prompt and execute the command `mkdir .well-known` . As shown below:

```

Microsoft Windows [版本 10.0.17134.590]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\>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 **Check Domain Validation Status** to verify if the configuration was successful.

 **Note**

- Both HTTP and HTTPS are supported, and either of them can be accessed.
- File verification does not support any redirect. Instead, it directly returns status code 200 and file content.
- For domain names beginning with www, such as `www.a.tencent.com` , in addition to file validation for the domain itself, file validation is also required for `a.tencent.com` .

4. Please patiently await the review by the Certificate Authority (CA). Once the certificate issuance is complete or the domain information has been approved, the files and directories can be removed.

 **Note**

Ensure that the domain is not restricted abroad. Foreign IP addresses should be able to resolve to the domain's A record and access it, otherwise, the CA organization will not be able to perform a scan review.

Automatic DNS Validation

Last updated: 2023-09-28 10:19:55

Scenario

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 only available for multi-year international standard certificates. For more information, please refer to [Multi-Year International Standard Certificates](#).

Instructions

Step 1. View validation information

1. Log in to the [SSL Certificate Service console](#), click on the **My Profile** option in the left menu to access the **My Profile** page.
2. On the **My Profile** page, click on the company name for which domain information needs to be validated to view the administrator information that has been applied for.
3. Click on the name of the administrator whose domain information needs to be validated to navigate to your "Review Information" page, as shown in the image below:

My profile Have feedback? [Join group](#) [Documentat](#)

1. Creating a profile can help you fill in the certificate review information quickly. After the relevant information is approved, you can also skip the company and domain verification operation when applying for a specific certificate. [View instructions](#)

2. [Warm reminder] Due to the large number of data review applications recently, the CA organization is busy reviewing. At present, it will prioritize the review of company information related to the submission of paid certificate applications. Please be aware of that for the majority of users. [Profile management instructions](#)

[Add organization](#)

Organization information [Edit](#) [Delete](#)

Organization name: hehe City: CNbeijingshi Address: asdq

Call: [icon] [icon] [icon] [icon]

Admins

[Add admin](#)

Name	Email	Department	Status	Creation time	Expiration time	Certificates	Domains	Operation
[icon]	[icon] [icon] [icon]	[icon]	Pending review ⓘ	2021-05-24 17:40:17	--	24	0	Edit Delete
xx	asd@qq.com	x	Pending review ⓘ	2021-08-19 14:55:47	--	0	0	Edit Delete

- Click the **Domain Information** tab, select the domain you wish to validate, and then click **View Validation**.
- On the "Domain Verification" page, please follow the prompts and add the resolution record within the specified 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.

- Please obtain the **host record** and **record value** from the **Step 1: View Verification Information (Figure for Substep 1.5)** page.
- Log in to the [DNSPod DNS Management Console](#), view the newly added domain, and click on **Resolve** in the operation column to enter the **Record Management** page.
- Click **Add Record** to incorporate a CNAME record.
 - **Host Record:** Enter the obtained host record.
 - **Record Type:** Select "CNAME".
 - **Line Type:** Select "Default" to prevent resolution issues for some users.
 - **Record Value:** Enter the obtained record value.

- **MX Priority:** No need to fill in.
- **TTL:** Represents the cache duration. The smaller the value, the quicker the record modifications take effect globally. The default is 600 seconds.

4. Click **Save** to complete the addition.

5. After successfully adding the record, please patiently wait for the CA to conduct a scan and review. If the specified value is detected and matches, the review will be deemed complete.

Note

- The DNS resolution typically takes effect within **10 minutes to 24 hours**, but the actual time depends on the refresh time of each Internet Service Provider. Please wait patiently.
- 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, please [contact us](#).

6. On the "Domain Verification" page, you can click **Verify Now** to check if the CNAME record has been added successfully.

Automatic file validation

Last updated: 2023-09-28 10:21:47

Scenario

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

The automatic file validation method only supports multi-year international standard certificates and non-wildcard domains. For more details, please refer to [Multi-Year International Standard Certificates](#).

Validation Rules

Domain 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](#).
 - When applying for a primary domain, additional validation for www is required. For instance, if the application domain is tencent.com, www.tencent.com also needs to be validated.
 - When applying for a domain with 'www', additional validation is required for the domain following 'www', regardless of the domain level. For instance, if the applied domain is www.a.tencent.com, a.tencent.com also needs to be validated.
 - When applying for a non-primary domain without 'www', only the current domain needs to be validated. For instance, if the applied domain is cloud.tencent.com, only cloud.tencent.com needs to be validated.
-
- 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](#).
 - When applying for a primary domain, additional verification for www is required. For

instance, if the application domain is `tencent.com` , then `www.tencent.com` also needs to be verified.

- When applying for a domain with "www", the domain following "www" needs to be additionally validated, regardless of its level. For instance, if the applied domain is `www.a.tencent.com` , then `a.tencent.com` also needs to be validated.
- When applying for a non-primary domain without www, only the current domain needs to be validated. For example, if the applied domain is `cloud.tencent.com` , only `cloud.tencent.com` needs to be validated.

CA validation rules

- During a DNS query, it is imperative to recursively query the authoritative NS server for each domain level from the authoritative root server, and subsequently 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 disregarded.

Instructions

Step 1. View validation information

1. Log in to the [SSL Certificate Service Console](#) , click on the left menu **My Information** to access the "My Information" management page.
2. On the "My Information" management page, click on the company name for which domain information needs to be validated to view the administrator information that has been applied for.
3. Click on the name of the administrator whose domain information needs to be validated to navigate to your "Review Information" page, as shown in the image below:

My profile Have feedback? [Join group](#) [Documentat](#)

1. Creating a profile can help you fill in the certificate review information quickly. After the relevant information is approved, you can also skip the company and domain verification operation when applying for a specific certificate. [View instructions](#)

2. [Warm reminder] Due to the large number of data review applications recently, the CA organization is busy reviewing. At present, it will prioritize the review of company information related to the submission of paid certificate applications. Please be aware of that for the majority of users. [Profile management instructions](#)

[Add organization](#)

Organization information [Edit](#) [Delete](#)

Organization name: hehe City: CNbeijingshi Address: asdq

Call: 0000 0000 0000

Admins

[Add admin](#)

Name	Email	Department	Status	Creation time	Expiration time	Certificates	Domains	Operation
*	0000000000000000	0000	Pending review	2021-05-24 17:40:17	--	24	0	Edit Delete
xx	0000000000000000	x	Pending review	2021-08-19 14:55:47	--	0	0	Edit Delete

4. Click the **Domain Information** tab, select the domain you wish to validate, and then click **View Validation**.
5. On the "Validate Domain" page, please follow the prompts on the page and complete the validation operation within the specified time

Step 2. Add file validation

1. Please log into the server and ensure that an A record has been added for your domain and that it points to this server.

! Note

If your domain's corresponding **DNS service provider** is Tencent Cloud, please refer to [A Record](#) to point your domain to your server.

2. Please start a web service on your server (or configure it on the web service where your business is running) and listen on ports 80 or 443, reverse proxy the file validation path address to the reverse proxy address provided in **Step 1: View Validation Information (Figure 1.5 in Step 1)**.

Tencent Cloud provides the following two web service configuration guides, which you can refer to according to your actual situation:

- [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.
- Support for 301/302 redirections is available, with a limit of no more than two redirections. The redirection destination and the domain being checked must be within the same primary domain. For domains beginning with www, such as `www.a.tencent.com`, file validation is required not only for the domain itself but also for its primary domain `a.tencent.com`.

3. After configuring the reverse proxy, patiently await the CA's scanning and validation process. Once the scan and validation are successful, the review will be approved.
4. On the "Validate Domain" page, you can click **Validate Now** to check if the configuration was successful.

Validation Result Troubleshooting Guide

Last updated: 2023-09-28 10:23:41

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

- **Tool Diagnosis:**
Please click on the [DNS Diagnostic Tool](#) and fill in the information as prompted.
- **Self-diagnosis method:**
 - **Check the status of the domain name.**
Ensure that the domain name can be resolved normally. For instance, the domain name may not be resolved properly if it has not been verified or if it is newly purchased.
 - **Check the DNS server.**
Make sure you have assigned the resolution process to the correct resolution provider. For example, if the DNS server is a Wanwang server, adding a TXT resolution to Tencent Cloud DNS will not work.
 - **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.

 **Note**

For more information, refer to [Resolution Effectiveness Related](#).

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

FAQs

Last updated: 2023-09-28 10:23:56

Potential issues that may be encountered during the domain verification process are detailed below.

- [How to troubleshoot when domain validation fails?](#)
- [What should I do if the free SSL certificate remains unverified?](#)
- [How do I view the domain validation result of a TrustAsia SSL certificate?](#)
- [What are the reasons for the failure of the SSL certificate application and how to address them?](#)
- [What are the reasons for the failure of the security audit?](#)
- [Can the TXT records for domain name resolution configured in the SSL certificate be deleted?](#)