SSL Certificate Service

Operation Guide

Product Documentation

Contents

Operation Guide
Domain Ownership Verification

Last updated : 2021-08-23 14:36:28

Overview

This document describes how to verify your ownership of a domain name after you apply for a DV certificate.

Note :

- Complete verification as soon as possible. The CA will reject your certificate application if you fail to complete or pass verification within 3 days.
- After passing verification, download the certificate from Certificate Management and install it.

Domain name ownership can be verified by using the following methods:

Verification Method	Use Case
Manual DNS verification	This method is for domain names that are hosted with any platform.
File verification	This method is for scenarios where there are limitations in using automatic DNS validation and manual DNS validation. (The process is complicated and requires a certain foundation for creating a site.)

Prerequisites

- For manual DNS verification, you need to first complete the application for a DV certificate.
- For file verification, you need to obtain the username and password for logging into the server.

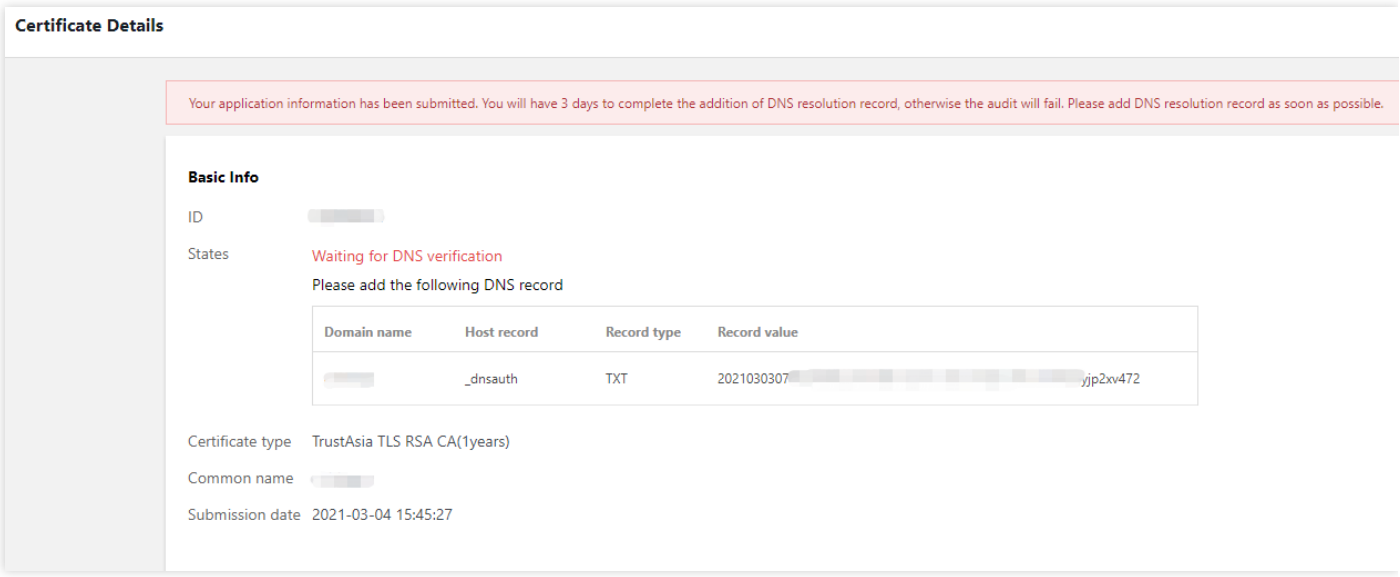
Directions

Manual DNS verification

Note：
The following operations apply only to domains hosted with Tencent Cloud DNSPod DNS. For domains hosted with other providers, please go to the corresponding **DNS hosting provider** for DNS resolution.

1. Log in to the SSL Certificates Service console.

2. On the **Certificate List** page, click the ID of the DV certificate of which you want to view the details to enter the **Certificate Details** page, as shown in the following figure.



3. Add the DNS record.

   - If your domain (for example, `www.tencent.com`) is hosted with Tencent Cloud DNSPod DNS:

     a. Go to the **Certificate Details** page to obtain the host record and record value.

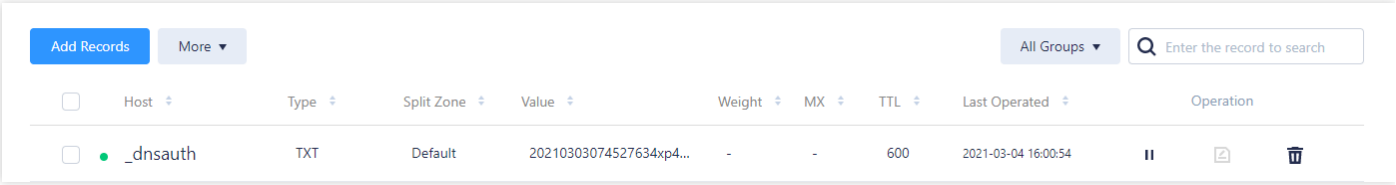
     b. Log in to the DNSPod Console to view the domain name for which a certificate has been applied, and then click **DNS** on the **Operation** column to go to the **Record Management** page.

c. Click **Add Record** and set a record type.

- If your domain is hosted with other providers, go to the **Certificate Details** page to obtain the host record and record value, and then go to the corresponding **DNS hosting provider** to add a DNS record.

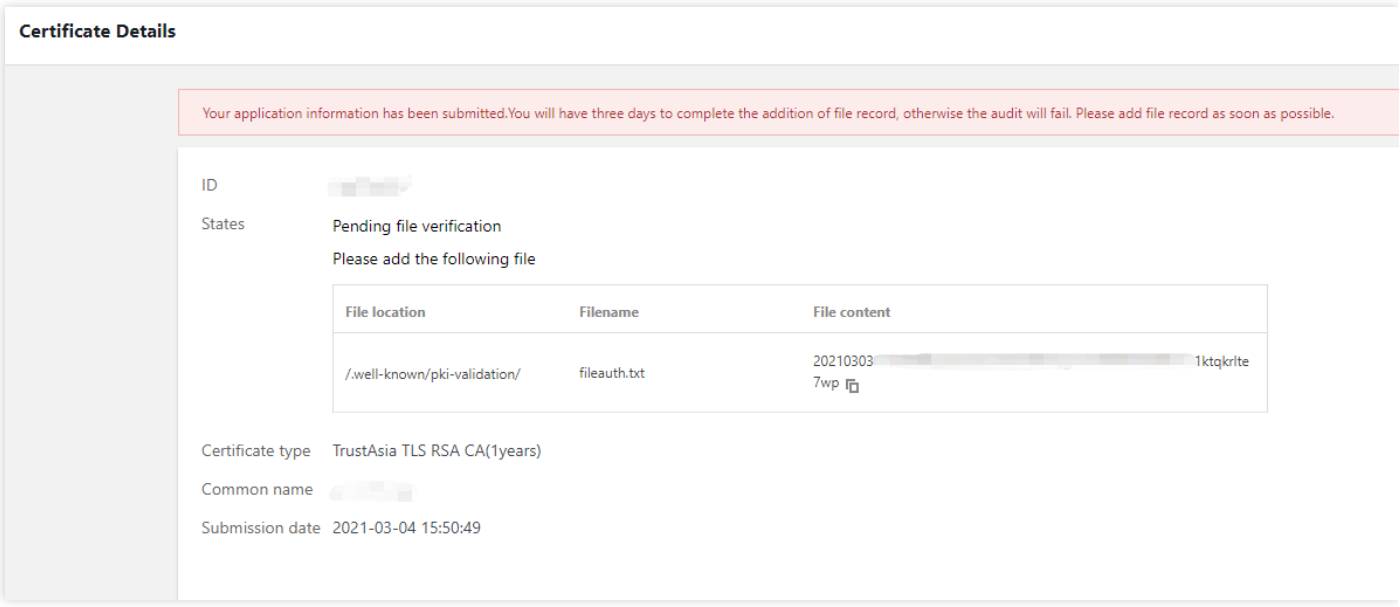
4. After the record is added, the system periodically checks for the record value. If the record value is detected and matches the specified value, the domain ownership verification will be completed, as shown in the following figure:

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



File verification

1. Log in to the SSL Certificates Service Console.
2. On the **Certificate List** page, click the ID of the DV certificate of which you want to view the details to enter the **Certificate Details** page, as shown in the following figure.



3. Log in to the server and make sure that the domain name points to the server.

> Note :
> If your domain is hosted with Tencent Cloud DNSPod DN, point the domain name to your server.

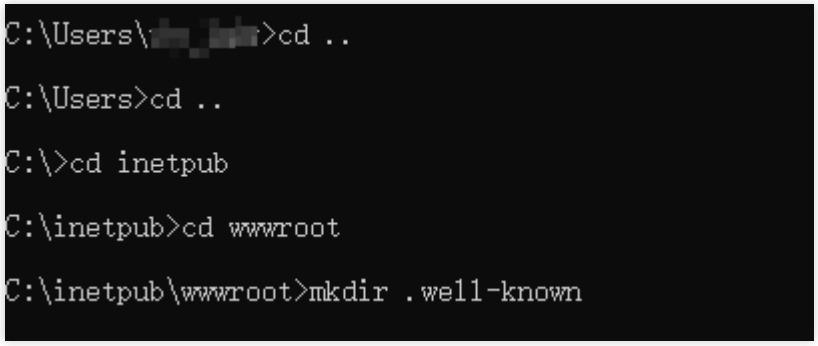
4. Create the specified file in the website root directory, including the file directory, name, and content.

> 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` .
>
> Use the filename and file content displayed on the **Certificate Details** page after the domain ownership is verified.

- **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
/.well-known/pki-validation	fileauth.txt	2019080603.....ep939jlu32alzeo

- **Note**
  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.



5. Open a browser and access the corresponding URL based on the type of the domain name to be verified.

URL format: `http://Domain name/File directory/File name` or `https://Domain name/File directory/File name`
Access the URL to obtain the file content, for example, `2019080603.....ep939jlu32alzeo`.

- If the domain name for file verification is `example.tencent.com`, access the URL `http://example.tencent.com/.well-known/pki-validation/fileauth.txt` or `https://example.tencent.com/.well-known/pki-validation/fileauth.txt` for verification.

> Note :
>
> For second-level domains prefixed with `www`, for example, `www.tencent.com`, perform the following 2 steps:
>
> - First, perform file verification for the second-level domain name.
> - Second, perform file verification for the primary domain name `tencent.com` (you do not need to reapply for a certificate). Verify the domain name according to the method specified in **URL format** and ensure that the file content is consistent.

- If the domain name for file verification is a wildcard domain name `*.tencent.com`, access the URL `http://tencent.com/.well-known/pki-validation/fileauth.txt` or `https://tencent.com/.well-`

`known/pki-validation/fileauth.txt` for verification.

Note：

- Both HTTP and HTTPS are supported, and either can be accessed.
- File verification does not support any redirect. Instead, it directly returns status code 200 and file content.

6. Wait for the CA's review. After the certificate is issued, the file and directory can be cleared.

Note：
If any problems occur during this process, please contact us.

Uploading Certificates

Last updated : 2020-12-21 17:03:08

Overview

You can upload all your SSL certificates to the SSL Certificate Service console for unified management. This document describes how to upload certificates.

Note :

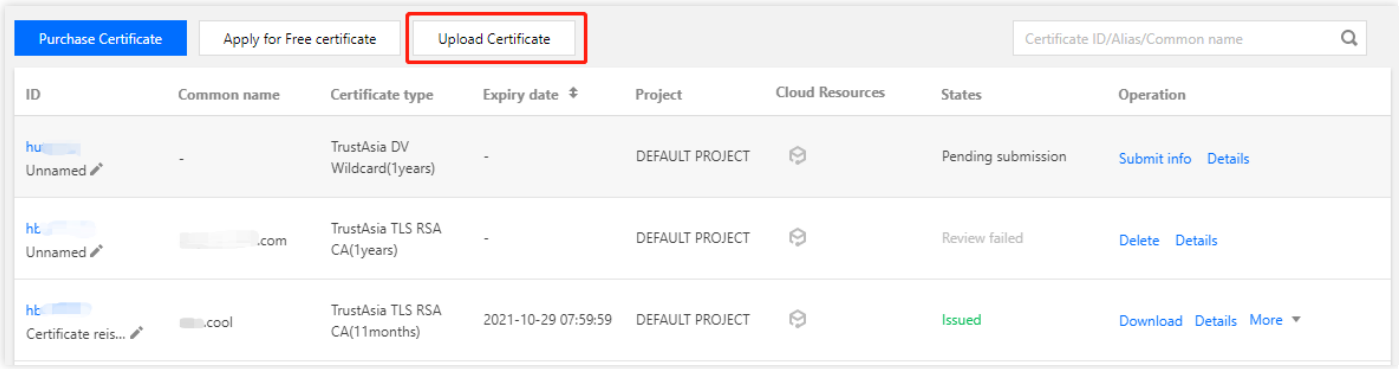
Currently, SM2 certificates cannot be uploaded.

Prerequisites

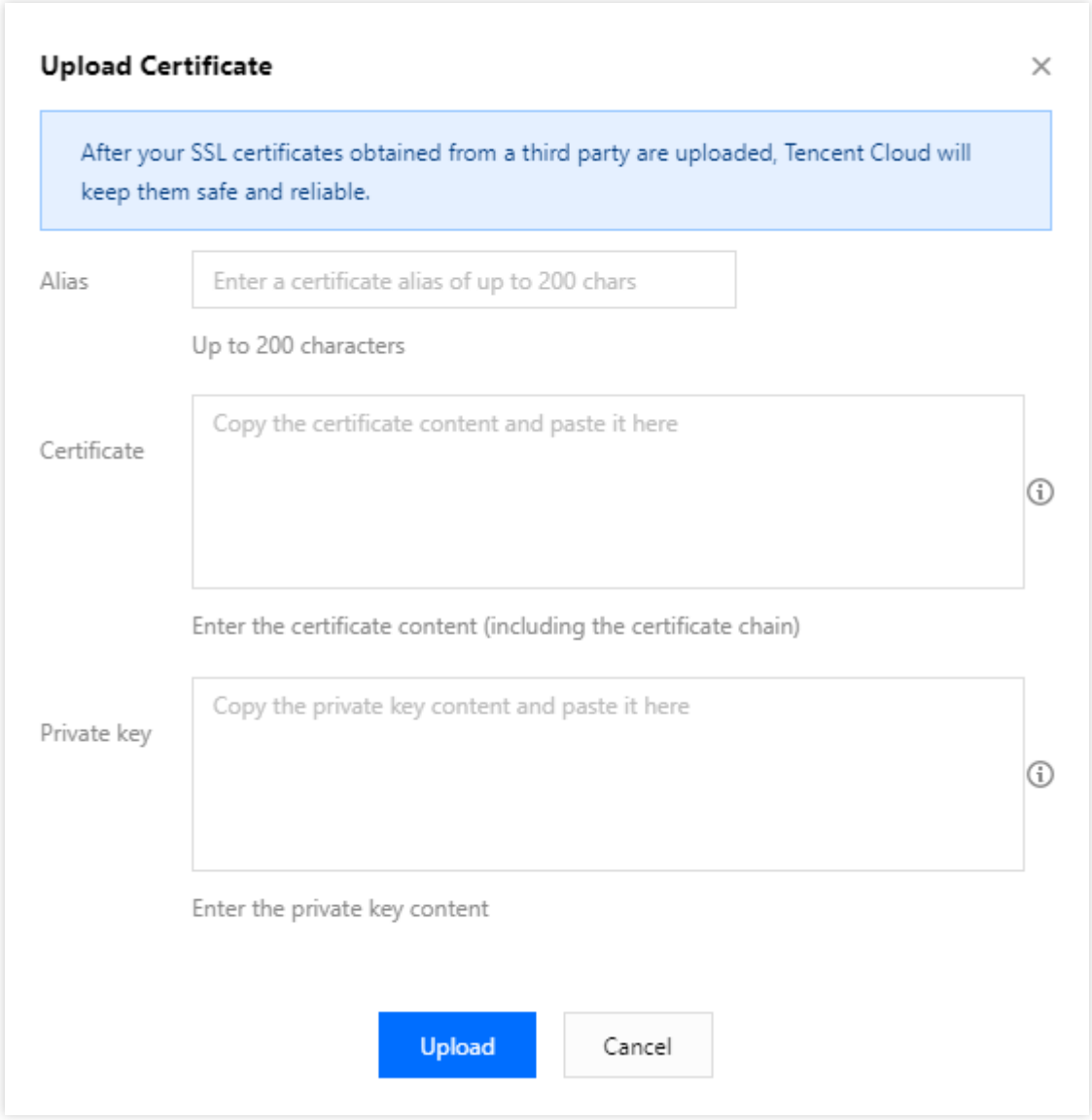
You have logged in to the SSL Certificate Service console.

Directions

1. Click **My Certificates** > **Upload Certificate**.



2. Set information as required in the **Upload Certificate** dialog box.



- **Alias**: please enter a certificate name.
- **Certificate**:
  - A certificate is usually a file with an extension such as .crt or .pem. Please use a text editor to open the certificate file and copy the certificate to the **Certificate** text box.
  - The certificate should start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----".
  - The certificate content should include the complete certificate chain.
- **Private key**:
  - A private key is usually a file with an extension such as .key and .pem. Please use a text editor to open the private key file and copy the private key to the corresponding text box.
  - The private key starts with "-----BEGIN (RSA) PRIVATE KEY-----" and ends with "-----END (RSA) PRIVATE KEY-----".

3. Click **Upload** to upload the certificate to the certificate list.

Subsequent Operations

You can deploy the uploaded certificate to a cloud service.

Secured Seal

Last updated : 2020-06-01 17:06:28

What is a Secured Seal?

Norton Secured Seal, provided by the Secure Site SSL Certificates, is the most recognized mark of trust on the internet. An individual user survey conducted by Secure Site shows that Norton Secured Seal enjoys a high reputation and high degree of trust among owners of e-commerce sites and other privacy-conscious websites. An independent survey conducted in January 2013 also shows that Norton Secured Seal makes individual users to highly trust the internet.

Reasons for Using a Secured Seal

- Norton Secured Seal shows up nearly one billion times per day in 170 countries and regions.
- Expanding online business by gaining customer recognitions: according to an international online consumer study, 90% of respondents said they were likely to continue purchasing online if they saw Norton Secured Seal during the checkout process. In situations where there are other seals or no seal, the percentage is significantly lower.
- Globally, Norton Secured Seal is displayed next to the trusted web links in search results on more than 40 million desktops with Norton Safe Web.
- Secure Site's robust PKI infrastructure, including military-grade data centers and disaster recovery features, provides users with unparalleled data protection and availability.
- This seal is visible proof of your commitment to enforcing PCI compliance when e-commerce sites must verify identity and encrypt transaction communications across its site to protect customer data.

CSR Management

Last updated : 2019-10-31 20:54:42

Use cases

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. This document describes how to generate and manage CSR files.

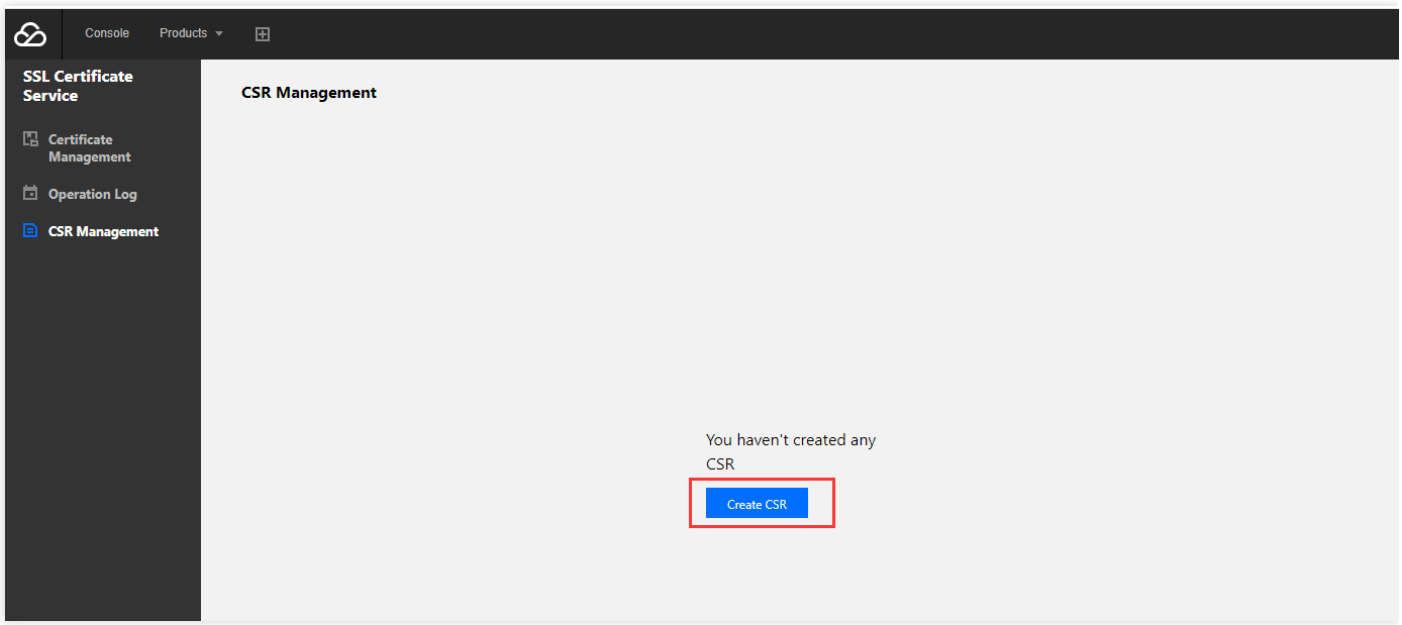
Prerequisites

You have logged in to the SSL Certificate Service Console

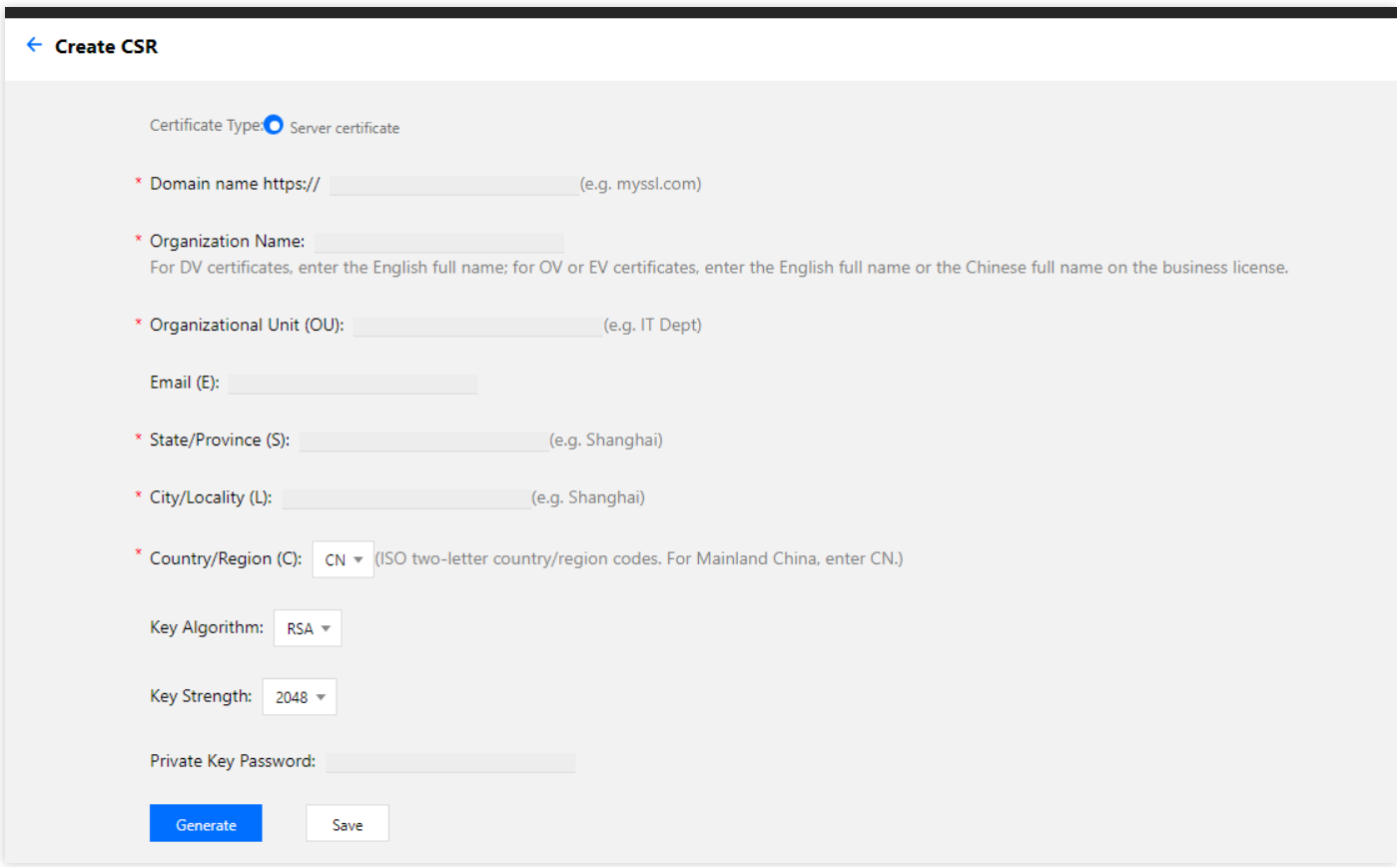
Directions

Generate a CSR

1. Select **SSL Certificate Service** > **CSR Management** and click **Create CSR**.



2. Enter the relevant information, as shown below:

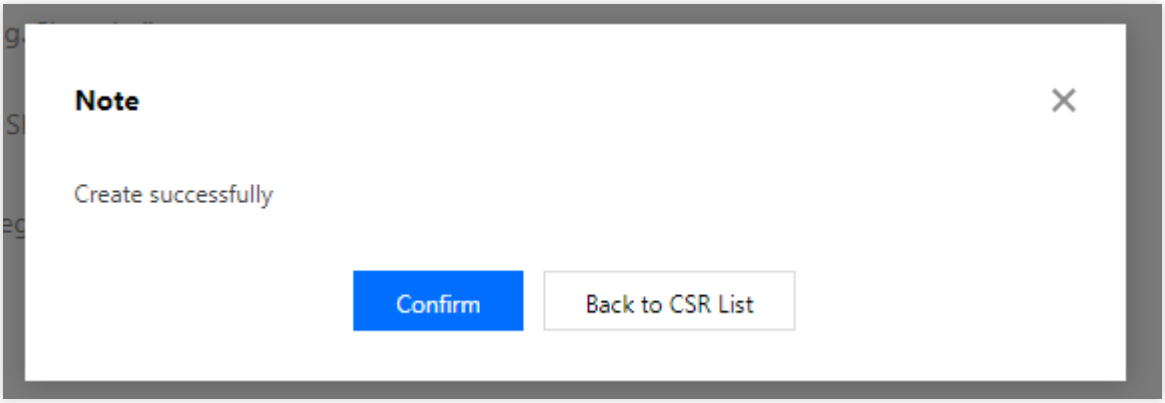


Main parameters:

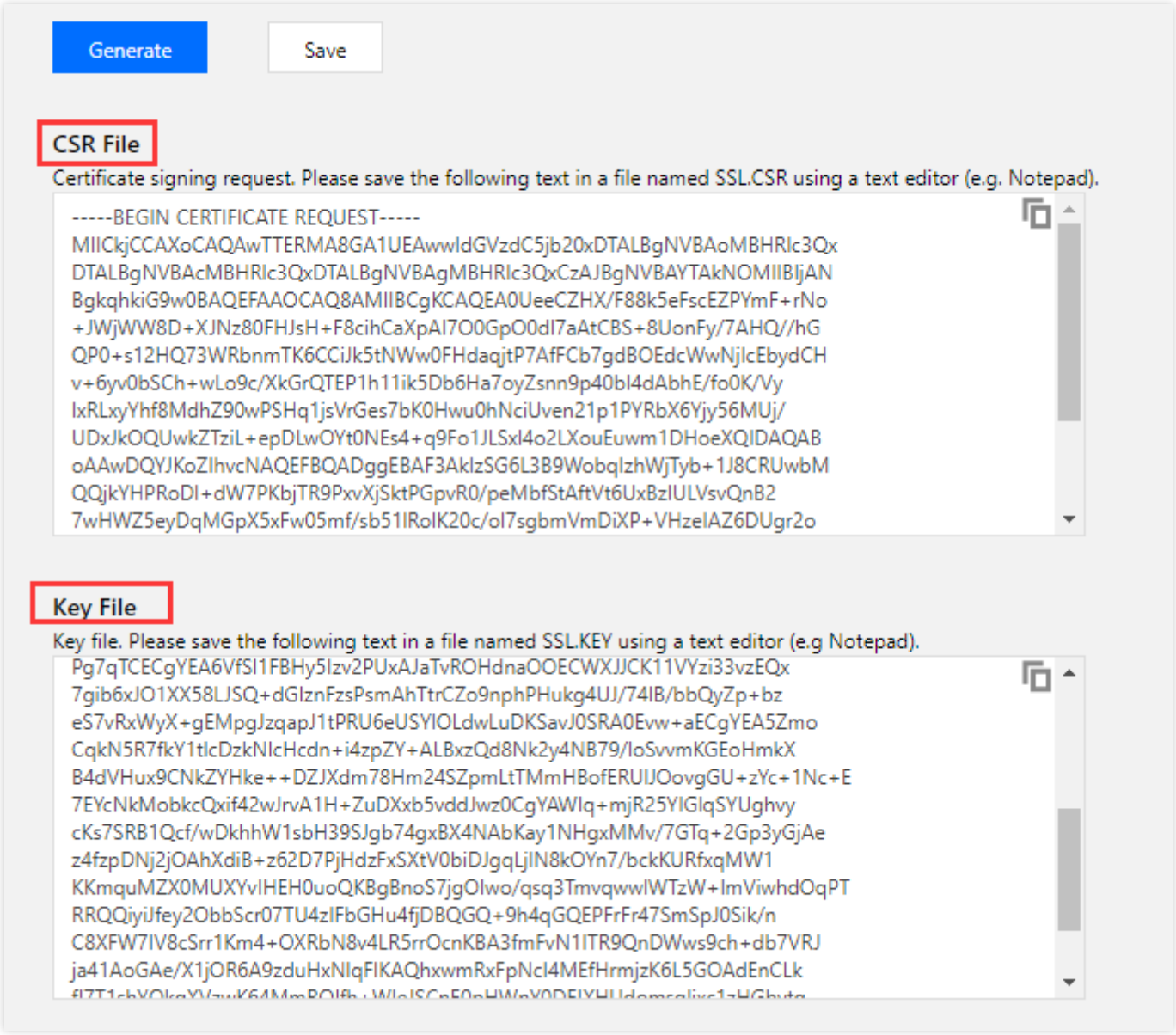
- Domain name: Enter the domain name/wildcard domain name to be bound to the certificate.
- Organization Name: The legally registered name of your organization. The complete English name must be entered for DV certificates. For OV and EV certificates, please enter the complete English or Chinese name as shown on the business license.
- Organizational Unit: This field is used to differentiate departments within an organization, such as "Engineering Department " or "Human Resources".
- Email (E): Your email address, which is optional.
- State/Province (S): The state or province where your organization is located.
- City/Locality (L): The city or locality where your organization is registered or located.

- Country/Region (C): The code of the country/region where your organization is legally registered, in the format of two letters as defined by the International Organization for Standardization (ISO).
- Key Algorithm: Optional. Value range: RSA, ECDSA.
- Key Strength: Optional. Value range: 2048, 4096
- Private Key Password: Password for the private key, which is optional.

3. Click **Generate**. The following prompt will pop up when the CSR has been successfully created.



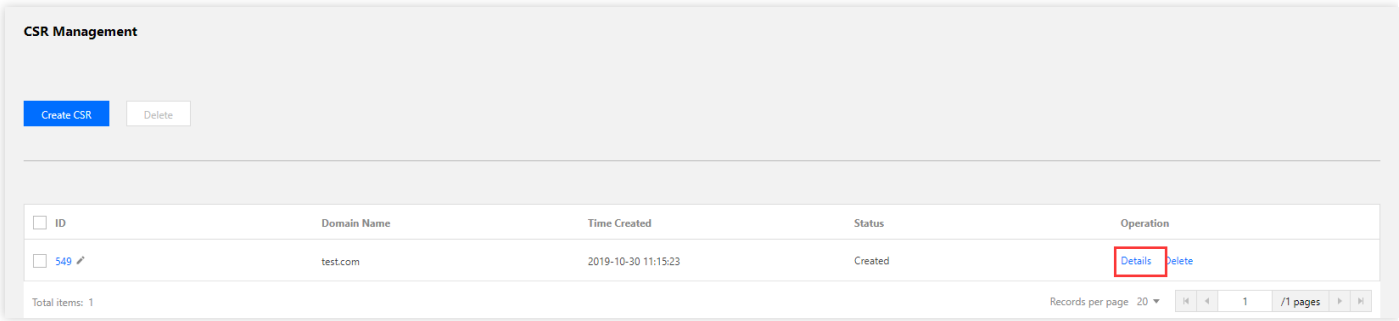
4. Click **Confirm** to view the **CSR File** and **Key File**.

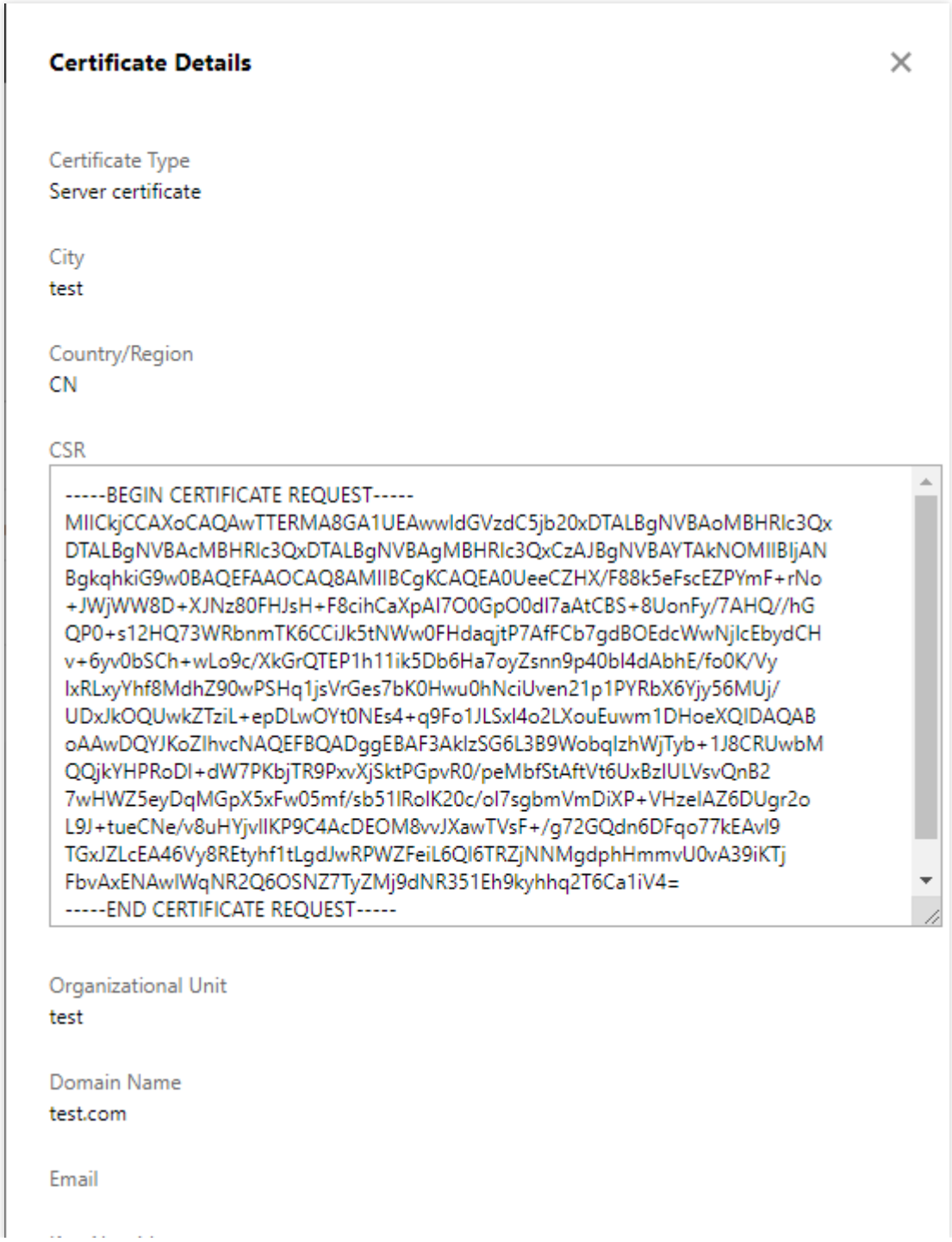


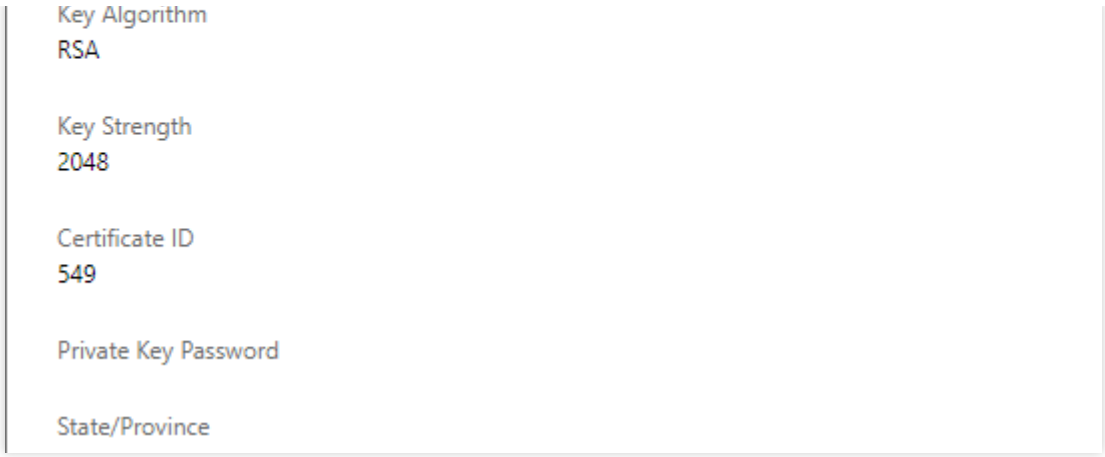
Manage a CSR

You can view, delete, or perform other operations on a CSR in CSR Management

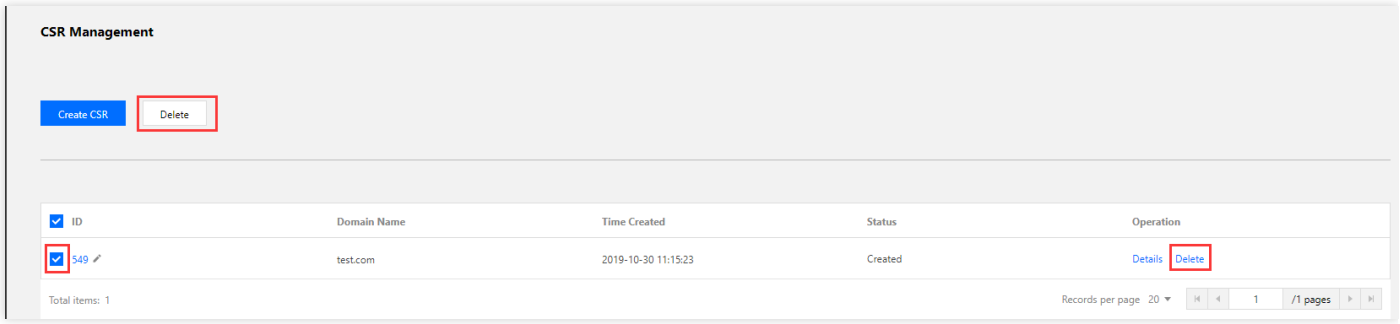
1. Click **Details** to view the CSR information.







2. Select a CSR and click **Delete** to delete it.



3. Add remarks to a CSR to distinguish the CSRs used for different projects.