Cloud Certificate Manager

Getting Started

Issue 06

Date 2021-05-26

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Purchasing an SSL Certificate

1.1 Certificate Selection and Purchase Process

There are multiple SSL certificate types available from well-known CAs on HUAWEI CLOUD. For details, see**Differences Between Certificate Types**. This section describes how to purchase and select SSL certificates on HUAWEI CLOUD.

How to Select a Proper SSL Certificate

We have some best recommendations for you based on different business needs. You can select the one that best fits your needs.

Your Business Need	Our Recommendation
I need a free certificate or the cheapest one.	• **Certificate Type**: Select **DV (Basic)**. • **Certificate Authority**: Select **DigiCert**. • **Domain Type**: Select **Single domain**. The default value is **Single domain**. • **Domain Quantity**: The value is fixed at **1**. When you select a DV (Basic) certificate, the number of domain names is fixed at **1** by default and cannot be changed. • **Validity Period**: The value is fixed at **1 year**. This value is the default value and cannot be changed. • **Quantity**: Retain the default value **1**. You can apply for a maximum of 20 free certificates. To reduce the waste of certificate resources, SCM allows you to apply for only one free certificate at a time.

Your Business Need	Our Recommendation
I need to use a certificate that is bound to an IP address.	• **Certificate Type**: Select **OV**. • **Certificate Authority**: Select **GlobalSign**. • **Domain Type**: Select **Single domain**. • **Domain Quantity**: The value is fixed at **1**. This value is the default value and cannot be changed. • **Validity Period**: The value is fixed at **1 year**. This value is the default value and cannot be changed. • **Domain Quantity**: Set to **1**.
I need to use a certificate to protect one domain name.	• **Certificate Type**: Not limited. • **Certificate Authority**: Not limited. • **Domain Type**: Select **Single domain**. • **Domain Quantity**: Select **1**. • **Validity Period**: The value is fixed at **1 year**. This value is the default value and cannot be changed. • **Domain Quantity**: Set to **1**.
I need to use one certificate to protect multiple non-wildcard domain names.	• **Certificate Type**: Select **OV**, **OV Pro**, or **EV Pro**. • **Certificate Authority**: Not limited. • **Domain Type**: Select **Multiple domains**. • **Domain Quantity**: Select the number of domain names to be protected. • **Validity Period**: The value is fixed at **1 year**. This value is the default value and cannot be changed. • **Quantity**: Set to **1**.
I need to use multiple certificates to protect multiple non-wildcard domain names. Each domain name needs to be protected and managed using a separate certificate.	• **Certificate Type**: Not limited. • **Certificate Authority**: Not limited. • **Domain Type**: Select **Single domain**. • **Domain Quantity**: Select the number of domain names to be protected. • **Validity Period**: The value is fixed at **1 year**. This value is the default value and cannot be changed. • **Quantity**: Select the number of certificates you need.

Your Business Need	Our Recommendation
I need to use one certificate to protect multiple wildcard domain names.	• **Certificate Type**: Select **OV** or **OV Pro**. • **Certificate Authority**: Not limited. If you select **OV Pro**, only DigiCert is available. • **Domain Type**: Select **Wildcard**. • **Domain Quantity**: Select **1**. A wildcard-domain certificate can protect only one wildcard domain name. • **Validity Period**: The value is fixed at **1 year**. This value is the default value and cannot be changed. • **Quantity**: Set to **1**.

Application and Purchase Process

Acquaint yourself with the application procedure before you apply or purchase a certificate. **Figure 1-1** shows the certificate application procedure. **Table 1-1** describes the steps required for certificate application.

Figure 1-1 Certificate application procedure

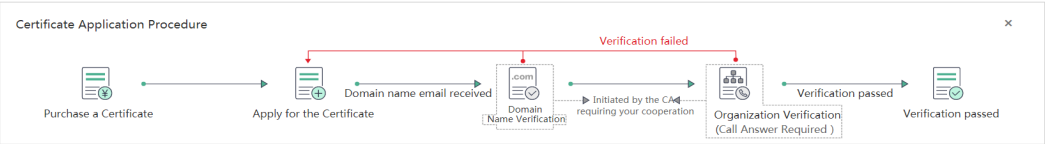


Table 1-1 Description of the certificate application procedure

Step	Operation	Description
1	**Purchasing a Certificate**	On the SCM platform, purchase a certificate for your domain. • For details about how to apply for a free certificate, see **Example 1: Applying for a Free Certificate**. • For details about how to request a certificate for a public IP address, see **Example 2: Applying for an IP Address Certificate**.
2	**Apply for a Certificate**	After you purchase a certificate, you need to associate a domain name, provide additional details, and then submit the application for approval.

Step	Operation	Description
3	**Verify the Domain Ownership**	Upon receiving your request, the CA sends a verification email to your email address for you to validate your ownership of the domain name. You can select email verification, DNS verification (manual or automatic), or file verification on HUAWEI CLOUD SCM. • Automatic DNS verification can be selected if all the following conditions are met: – Single-domain certificates – Domain names you apply for on HUAWEI CLOUD – Domain names that have been resolved by HUAWEI CLOUD DNS After you select this option, the system automatically adds the DNS record for verification. • For DV and basic DV certificates (GeoTrust entry-level SSL certificates and DigiCert free SSL certificates), DNS verification is selected by default. No configuration is required when you apply for certificates. • For IP address SSL certificates, only file verification is available.
4	**Verify the Organization**	This operation is required only when you apply for an OV, OV Pro, EV, or EV Pro certificate. The CA will send an email for you to choose a verification method. Then, the CA will contact you by the method you selected to check whether the enterprise or organization has initiated the application.
5	Issuing the Certificate	After the organization verification completes, it takes some time for CA to confirm the verification. The certificate will be issued after being approved by the CA. The certificate takes effect immediately upon issuance. You can push the certificate to other cloud products on HUAWEI CLOUD or download the certificate and deploy it on a server.

1.2 Step 1: Purchasing a Certificate

This section describes how to purchase an SSL certificate (certificate with which domain names or public IP addresses are associated).

Prerequisites

The account for purchasing a certificate has the SCM Administrator, BSS Administrator, and DNS Administrator permissions.

Constraints

- If you need to use this certificate, click **Service Tickets** > **Create Service Ticket** in the upper right corner of the management console and submit a service ticket to apply for the certificate. Currently, the CFCA certificates cannot be purchased on the SCM console.
- For OV, OV Pro, EV, or EV Pro SSL certificates, organization verification is required. If the verification cannot be completed due to certain reasons, such certificates will fail to issue. For example, special organizations, such as military units, special government agencies, and state secrecy units, cannot use those types of certificates because their unified social organization code cannot be queried on the official website.
- Currently, SSL certificates can be bound only to English domain names.
- The seven-day unconditional refund policy applies to SSL certificate. If you use a cash coupon to purchase a certificate, the amount deducted using the cash coupon cannot be refunded. To unsubscribe from the certificate within seven days after purchasing it, click **Service Tickets** > **Create Service Ticket** in the upper right corner of the management console.

  No refunds are allowed 7 days after the purchase.
- SCM supports only SSL certificates with a validity period of one year. The validity period of a certificate starts from the date when the certificate is issued. After the certificate expires, you need to purchase a new certificate and complete the certificate application process.

Application Scenarios

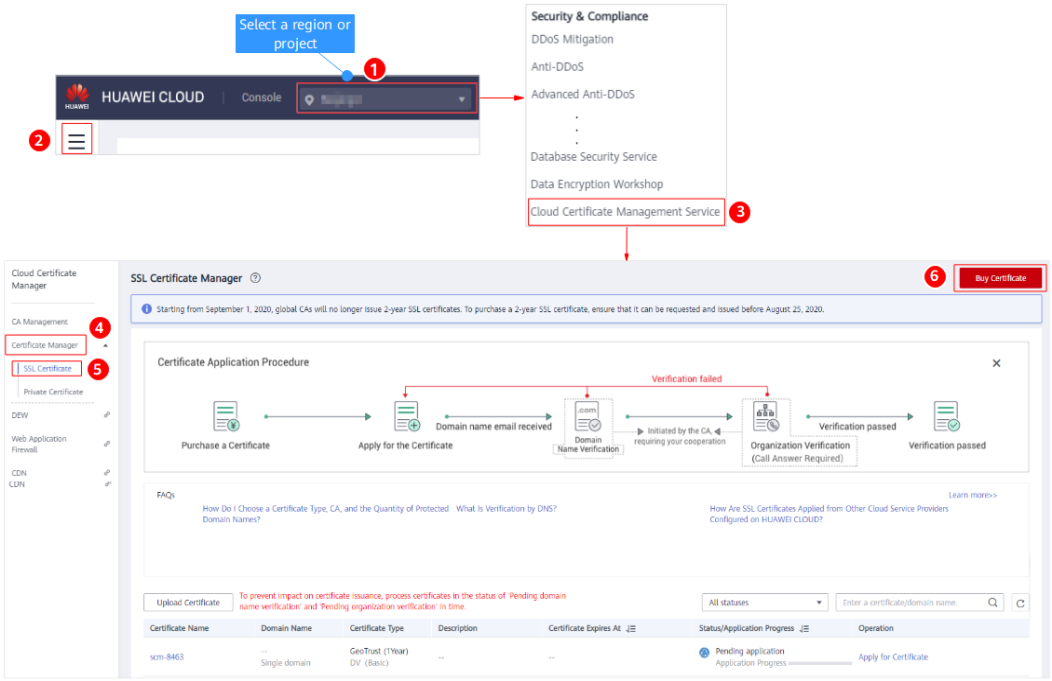
- If you need a certificate bound with an IP address, purchase a single-domain OV certificate of GlobalSign. For more about the detailed operations, see **Example 2: Applying for an IP Address Certificate**.
- If you need a free certificate for testing, purchase a DigiCert DV (Basic) certificate. For more about the detailed operations, see **Example 1: Applying for a Free Certificate**.

Procedure

Step 1 Log in to the **management console**.

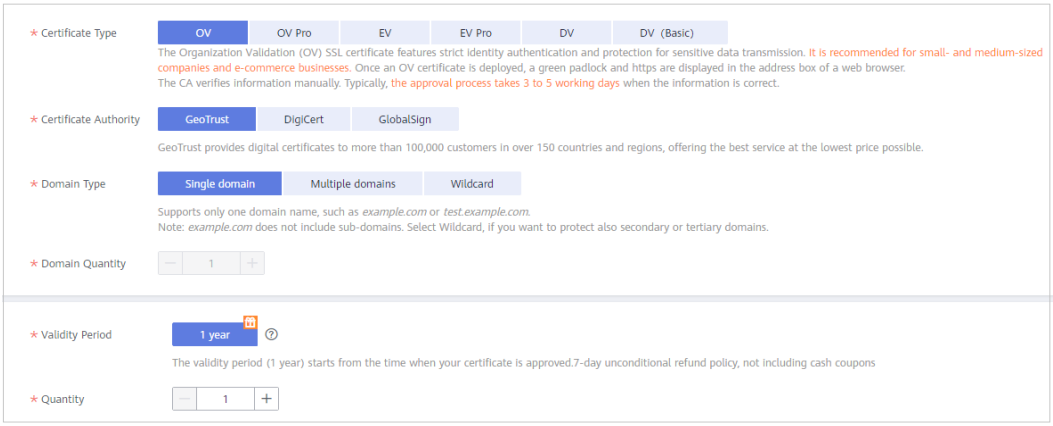
Step 2 Go to the SCM purchase page.

Figure 1-2 Navigation path for entering the SSL Certificate Manager purchase page



Step 3 Specify values for **Certificate Type**, **Certificate Authority**, **Domain Type**, **Domain Quantity**, and **Validity Period**.

Figure 1-3 Specifying details



1. Select a certificate type.

   The following certificate types are available:

   - Organization Validation (OV) SSL certificates

     OV certificates are recommended for small- and medium-sized companies and e-commerce businesses. The CA usually takes three to five working days to review the request.

   - OV Pro SSL certificates

OV Pro certificates are recommended for small- and medium-sized enterprises that have high requirements on data security. The CA usually takes three to five working days to review the request.

- EV: Extended Validation (EV) SSL certificate

  EV certificates are recommended for large enterprises with higher security requirements. The CA manually reviews the information. If the information is correct, the approval period takes seven to ten working days.

- EV Pro SSL certificates

  EV Pro certificates are recommended for institutions and organizations in the finance industry that have higher security requirements, such as insurance companies and banks, with higher security requirements than that of other industries. The CA usually takes seven to ten working days to review the request.

- DV SSL certificates

  DV certificates are recommended for personal website and enterprise tests. The CA system automatically verifies the domain owner through DNS verification. Generally, a testing DV certificate can be issued within several hours.

- DV (Basic): Basic Domain Validation (DV) SSL certificate

  Basic DV certificates include GeoTrust entry-level SSL certificates and DigiCert free SSL certificates.

  It is suitable for non-commercial scenarios, such as individual and enterprise testing purposes. The CA's certificate issuing system automatically checks authorization configuration. Generally, the system can issue the certificate within several hours.

2. Select a certificate authority.

   GeoTrust, **DigiCert**, and **GlobalSign** are available CAs in SCM.

3. Select a domain type.

   Currently, you can select **Single domain**, **Multiple domains**, or **Wildcard**. For parameters, see **Table 1-2**.

Table 1-2 Domain types

Domain Type	Description
Single domain	Only a single domain can be associated with a certificate. The domain can be a second-level domain like **domain.com** or a third-level domain like **example.domain.com**. Any subdomains of the domain cannot be protected. For example, if you associate **domain.com** with a certificate, the certificate does not protect any subdomains, such as **ssl.domain.com** or **ssl.ssl.domain.com**.

Domain Type	Description
Multiple domains	You can add multiple domains, including single domains, to one certificate. For example, if you purchase a multi-domain certificate, you can use the certificate to protect domains example.com, example.cn, and test.com. **NOTE** If the **Certificate Type** is set to **OV** or **OV Pro**, multiple single domains and multiple wildcard (*) domains can be added to one certificate. For example, if you purchase a multi-domain certificate, you can use the certificate to protect domains *.example.com, example.cn, and test.com. A maximum of 100 domains can be associated.
Wildcard domain	Only one wildcard domain can be associated with a certificate. Only one wildcard character (*) can be contained in a wildcard domain, for example, *.domain.com or *.example.domain.com. Domains like *.*.domain.com are not supported.
For details about how to select a domain type, see **How Do I Select an SSL Certificate?**	

4. Set the domain quantity.
   - If the **Domain Type** value is **Single domain** or **Wildcard**, you can only associate one domain name with a certificate.
   - If the **Domain Type** value is **Multiple domains**, you can associate 2 to 100 domain names with a certificate. Set the quantity of domains based on your needs.

     The following conditions must be met:

     - The number of primary domains is fixed at **1**.
     - The number of additional single domains must be greater than or equal to 1.

     NOTE

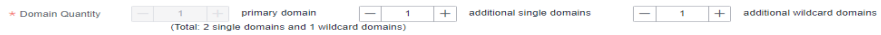
     If you are purchasing a multi-domain OV or OV Pro certificate, the number of domains must meet the following conditions:

     - The primary domain name quantity is fixed at 1, and a primary domain name must be a single domain name.
     - The number of additional single domains and additional wildcard domains must be greater than or equal to 1.

     Example: To associate *.example.com, example.cn, and test.com3 with a single SSL certificate, specify **Domain Quantity** as shown in **Figure 1-4**.

     One primary domain, one additional single domain name, and one additional wildcard domain

Figure 1-4 Domain Quantity



5. Set **Validity Period**. The default value is 1 year.

   A certificate takes effect upon issuance. The certificate issuance time refers to the time when the certificate is officially issued by the CA.

   After your old certificate expires, purchase a new certificate and complete the certificate application process.

6. Set the **Quantity**.

   You can purchase multiple certificates as needed.

Step 4 Click **Next**.

If you have any questions about the pricing, click **Pricing Details**.

Step 5 Confirm the order information and agree to the SCM disclaimer by selecting **I have read and agree to the SSL Certificate Manager Disclaimer**. Click **Pay**.

Step 6 On the displayed page, select a payment method.

After the payment is complete, go back to the certificate list to view the purchased certificate.

----End

Follow-up Procedure

After purchasing an SSL certificate, you need to apply for the certificate on the SCM console to request for approval from the CA. After being approved by the CA, the certificate will be issued.

For details about how to apply for the certificate, see **Apply for the Certificate**.

The certificate takes effect immediately upon issuance. Then you can directly push the certificate to other HUAWEI CLOUD services or download and install the certificate.

1.3 Step 2: Applying for the Certificate

After you purchase a certificate, you still need to associate a domain name with it, provide certain details, and then submit it for approval. The CA will not issue the certificate until all of the submitted details have been reviewed.

This section describes how to apply for a certificate.

Prerequisites

The certificate is in the **Pending application** state.

Constraints

- To apply for a certificate, domain ownership verification is required.
  - For IP address SSL certificates, only file verification is available.
  - For DV and basic DV certificates (GeoTrust entry-level SSL certificates and DigiCert free SSL certificates), only DNS verification is available.

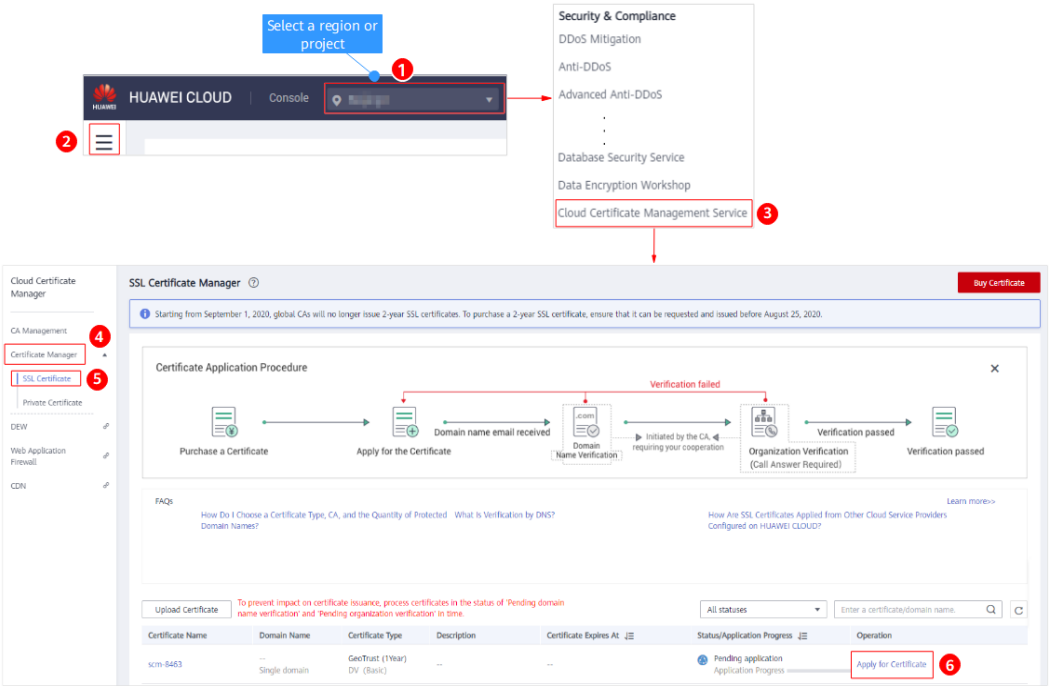
- SSL certificates can be used only for English domain names.
- If you need to protect domain names www.a.com and a.com, you can purchase one certificate for one of the domains to protect both www.a.com and a.com.

Procedure

Step 1 Log in to the **management console**.

Step 2 Go to the SCM certificate application page.

Figure 1-5 SSL certificate application page



Step 3 On the displayed page, configure required information, as shown in **Figure 1-6**. For parameters, see **Table 1-3**.

NOTICE

- SSL certificates can be bound only to English domain names.
- The www subdomains and the corresponding root domains may be considered as different domains by some CAs. Before you buy a multi-domain certificate, be sure you are familiar with the differences. The following uses the subdomain www.a.com and root domain name a.com as an example to show the differences. For more details, see **Differences Between Certificate Types**
  - For DigiCert and GeoTrust certificates, you can purchase a certificate for either the root domain or the subdomain to protect both domains at the same time. For example, if you plan to purchase a multi-domain certificate issued by DigiCert or GeoTrust and expect to use this certificate to protect www.a.com and a.com, just bind www.a.com or a.com to the certificate.
  - For GlobalSign certificates, you can purchase a certificate for the subdomain and use the certificate to protect the corresponding root domain at the same time. However, a certificate for a root domain cannot protect the corresponding subdomain. For example, if you plan to purchase a multi-domain certificate issued by GlobalSign and expect to use the certificate to protect both www.a.com and a.com, just bind domain www.a.com to the certificate.

Figure 1-6 Domain name details

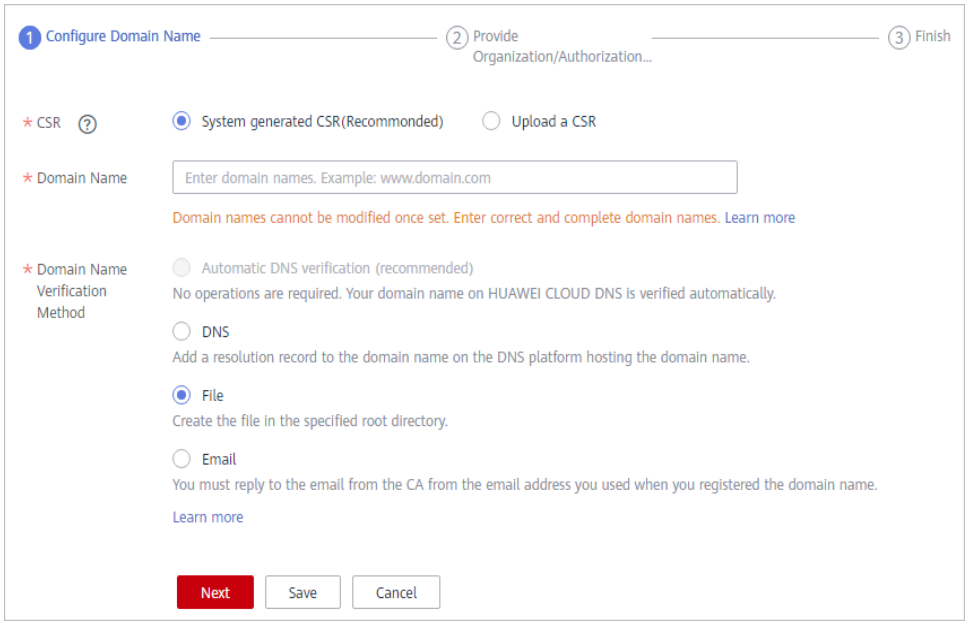


Table 1-3 Domain name parameters

Parameter	Description	Example Value
CSR	To obtain an SSL certificate, a Certificate Signing Request (CSR) file needs to be submitted to the CA for review. A CSR contains a public key and a distinguished name (DN). Typically, a CSR is generated by a web server. A pair of public and private keys are created along with the CSR. Options: • **System generated CSR**: The system automatically generates a certificate private key. Once the certificate is issued, you can download your certificate and private key on the certificate management page. • **Upload a CSR**: You manually generate a CSR file and paste the content of the CSR file into the displayed field. For more details, see **How Do I Make a CSR File?** You are advised to select **System generated CSR** to avoid approval failure caused by incorrect content. For details about the differences between the two types of certificate request files, see **What Are the Differences Between the CSR Generated by the System and the CSR Made by Yourself?**	System generated CSR

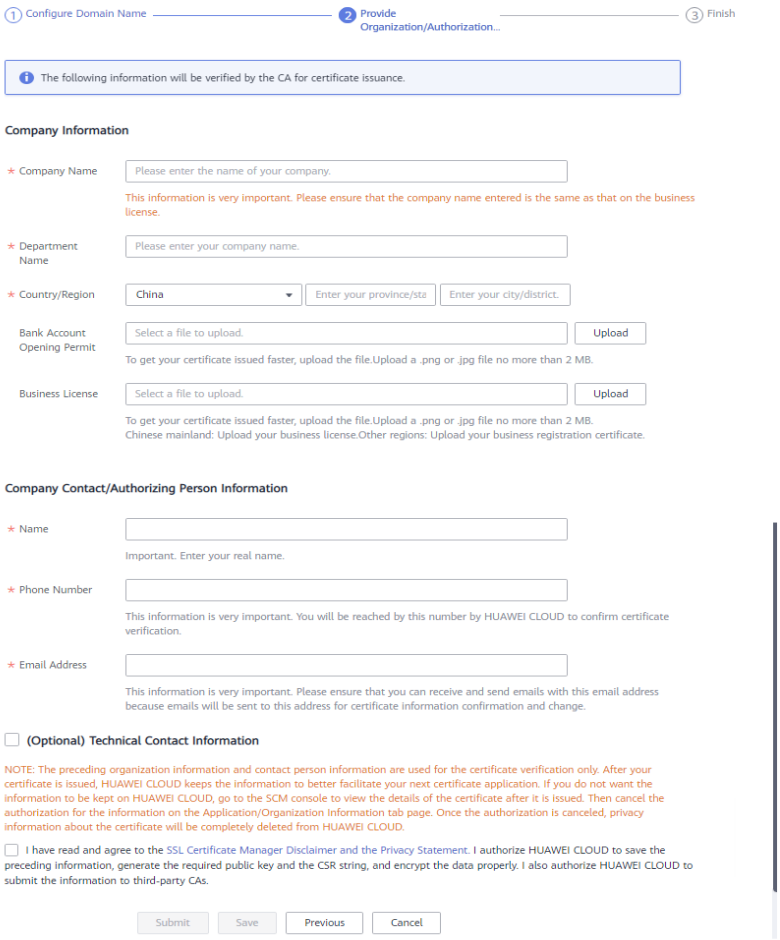
Parameter	Description	Example Value
Domain Name	This parameter is displayed when you purchase a single-domain or wildcard-domain certificate. • If you select **Upload a CSR** for **CSR**, the domain name is automatically parsed based on the CSR file. You do not need to manually enter the domain name. • If you select **System generated CSR** for **CSR**, manually enter the domain name or wildcard domain to be associated with the certificate. Single domain: If your domain is *www.domain.com*, enter ***www.domain.com*** for **Domain Name**. Wildcard domain: If you have multiple domain names that are all the same level, for instance, test.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and good.huaweicloud.com, you can use a wildcard to enter a single domain name that would include them all, in this case: ****.huaweicloud.com***.	www.domain.com

Parameter	Description	Example Value
Primary Domain Name	This parameter is displayed when you purchase a multi-domain certificate. • If you select **Upload a CSR** for **CSR**, the primary domain name is automatically parsed based on the CSR file. You do not need to manually enter the domain name. • If you select **System generated CSR** for **CSR**, manually enter the primary domain name associated with the certificate. Set one of the domain names as the primary domain and the rest as additional domains. **NOTICE** • A primary domain and additional domains can be equally protected. • If you purchase a multi-domain certificate (single domain name + wildcard domain name), the primary domain name can only be a single domain name. Example: If buy three domain names for the certificate and you have three domain names www.domain01.com, www.domain02.com, and www.domain03.com, you need to select one of them as primary domain name. If your select www.domain01.com as the primary domain name, enter www.domain01.com for **Primary Domain Name**.	www.domain01.com
Additional Domain Name	This parameter is displayed when you purchase a multi-domain certificate. Enter one or more additional domain names that need to be associated with the certificate. **NOTE** • One additional domain name per line. • You can add one or more additional domain names at a time. For more details, see **Adding an Additional Domain Name**. Example: If three domain names have been purchased, such as www.domain01.com, www.domain02.com, and www.domain03.com, and the primary domain name is www.domain01.com, enter www.domain02.com and www.domain03.com for **Additional Domain Name**.	www.domain02.com www.domain03.com

Parameter	Description	Example Value
Domain Name Verification Method	In accordance with the CA specifications, after applying for a certificate, you need to work with the CA to verify ownership of the associated domain name. After your ownership of the domain name is verified by you and approved by the CA, the status of your certificate will change. Options: ● **DNS**: You need to verify the domain ownership by resolving a specific DNS record on the domain name management platform. – Automatic DNS verification: The system automatically adds DNS records for verification. If you have purchased a single-domain certificate, and you have registered a domain name on HUAWEI CLOUD and the domain name has been resolved by HUAWEI CLOUD DNS, you can choose this verification method. – Manual DNS verification: You need to go to the DNS service provider of the domain name to perform the verification. ● **File**: You need to create a specified file on the server to verify your ownership of the domain. ● **Email**: You can click the link and follow the directions in the email to verify ownership of the domain. **NOTE** ● For DV and basic DV certificates (GeoTrust entry-level SSL certificates and DigiCert free SSL certificates), DNS verification is selected by default. ● For IP address SSL certificates, only file verification is available.	Manual DNS verification

Step 4 Click **Next** to switch to the **Provide Organization/Authorization Details** page.

Figure 1-7 Authorization information



Step 5 Configure the organization information and authorization information.

1. Set the company information based on **Table 1-4**.

   NOTE

   Company details need to be provided for OV, OV Pro, EV, and EV Pro certificates.

Table 1-4 Company information

Parameter	Description
Company Name	The full name of the company, as written on its business license
Department Name	Name of the department to which a user belongs
Country/Region	Country or region where the company resides

Parameter	Description
(Optional) Bank Account Opening Permit	Whether to upload the bank account opening permit. Click **Upload** to upload the electronic copy of the bank account opening permit. **NOTE** – Only one file can be uploaded each time. It must be in .png or .jpg format, and cannot exceed 2 MB. – If the bank account opening permit is not uploaded, the certificate issuance period will be extended. The specific extension time depends on the verification time of CA. To avoid the unnecessary time extension, upload the required business license.
(Optional) Business License	Whether to upload the enterprise business license. Click **Upload** to upload the electronic copy of the business license. – Chinese mainland: Upload your business license. – Other regions: Upload your business registration certificate. **NOTE** – Only one file can be uploaded each time. It must be in .png or .jpg format, and cannot exceed 2 MB. – If the business license is not uploaded, the certificate issuance period will be extended. The specific extension time depends on the verification time of CA. To avoid the unnecessary time extension, upload the required business license.

2. Enter the company contact or authorizer information. **Table 1-5** describes the parameters.

Table 1-5 Contact information

Parameter	Description
Name	Enter your name.
Phone Number	Enter a valid phone number so that the CA can contact you to confirm other required details. Example: 13812345678 02812345678
Email Address	Enter an email address for you to receive emails. **NOTICE** You will use this email address to receive email notifications related to certificate issuance from us. The CA will send confirmation emails to the email address. After submitting your application for approval, check for and follow the directions in the confirmation email.

NOTE

- The system automatically notifies the company contact or authorizing person by email or SMS two months, one month, and one week before a certificate expires and again when the certificate has actually expired.
- If the technical contact is required, select **(Optional) Technical Contact Information**. After selecting the check box, you can enter the technical contact information.
- Personal user information used as contact details is not included in the issued certificate.

Step 6 After confirming that the entered information is correct, read through the *SSL Certificate Manager Disclaimer*, *Privacy Statement*, and the authorization statement, and check the box to agree to the disclaimer and statements

You can revoke the privacy rule authorization if the certificate is not being approved. Once you revoke the authorization, HUAWEI CLOUD will no longer store your information. The contact name, phone number, email address, and organization details will be deleted. For more details, see **Canceling Authorization for Privacy Information**.

Step 7 Click **Submit**.

The system prompts you to perform the next operation, and the certificate status changes to **Pending domain name verification**.

The system will submit your application to the CA. During the approval process, make sure that you can be reached by phone and that you regularly check for emails from the CA.

NOTE

- You can click **Save** to save your progress.
- The CA will process your application and send you a domain name verification email within 2 to 3 working days.

----End

Follow-up Procedure

After the entered additional domain names are submitted for review, the CA will send a verification email to you. Perform domain name verification as required. Your certificate will remain in the **Pending domain name verification** state and will not be approved if you do not complete the domain name verification. Upon receiving your request, the CA will review your request and send a verification email. Reply to the CA immediately after receiving the verification email. If you fail to complete the verification timely, it takes longer to receive your certificates.

For more details, see **Step 3: Verifying the Domain Ownership**.

If you have submitted a certificate application but then discover there are incorrect details included, you can withdraw the application and apply for a new certificate. For details about how to withdraw an application, see **Withdrawing an Application**.

1.4 Step 3: Verifying the Domain Ownership

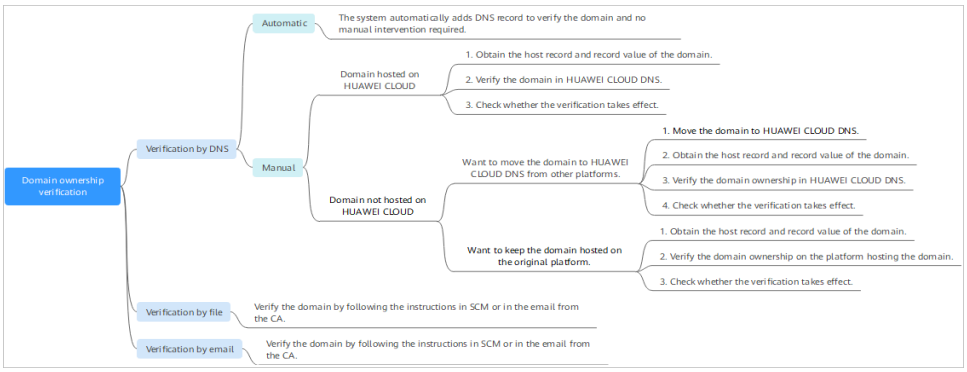
After certificate application is submitted, the associated domain needs to be verified. After you request approval from CA, you need to work with the CA to verify your ownership of the associated domain. After you complete the verification and the CA approves the verification, the status of your certificate will then change.

If you do not complete the domain ownership verification, your certificate will remain in the **Pending domain name verification** state.

You can verify your domain ownership by any of the following methods:

- **Automatic DNS Verification**
- **Manual DNS Verification**
- **Verification by File**
- **Verification by Email**

Figure 1-8 Domain ownership verification



Prerequisites

- The domain name has been licensed. Obtain the license for the domain name because the domain name verification will fail if the domain name has not been licensed.
- Verification by file: You have obtained the account and password for logging in to the server.
- Verification by email: You have obtained the account and password for logging in to the domain name administrator's mailbox. For details, see **How Do I Query and Verify the Email Address of the Domain Administrator?**
- Verification by DNS: You have obtained an account and password for the management console of your DNS provider.
- The certificate must be in the **Pending domain name verification** state.

Constraints

- For IP address SSL certificates, only file verification is available.
- For DV and basic DV certificates (GeoTrust entry-level SSL certificates and DigiCert free SSL certificates), only DNS verification is supported.

- Manual DNS verification can be performed only on your domain name management platform by following the instructions provided by the domain name service provider.

Automatic DNS Verification

You are required to verify domain ownership on the platform hosting your domain name by resolving a specific DNS record.

Automatic DNS verification: The system automatically adds DNS records for verification.

The system performs automatic DNS verification in the following scenarios:

- You have purchased an OV, OV Pro, EV, or EV Pro certificate (all of the following conditions must be met).
  - Single-domain certificates
  - Domain names you apply for on HUAWEI CLOUD
  - Domain names that have been resolved by HUAWEI CLOUD DNS
  - Automatic DNS verification selected for **Domain Name Verification Method** when you apply for a certificate
- You have purchased the DV or basic DV certificates (all of the following conditions must be met).
  - Single-domain certificates
  - Domain names you apply for on HUAWEI CLOUD
  - Domain names that have been resolved by HUAWEI CLOUD DNS

Please wait for the system to perform automatic DNS verification. After the DNS verification is complete, the CA needs to review the DNS verification information within two to three working days. After the DNS verification information is approved, the certificate enters the next state.

Manual DNS Verification

You are required to verify domain ownership on the platform hosting your domain name by resolving a specific DNS record.

This part describes how to host your domain names on HUAWEI CLOUD DNS and complete DNS verification. Refer to this part if you are managing your domain name on HUAWEI CLOUD.

NOTE

- You need to modify DNS records on your domain management platform for the DNS record to take effect.
- If your domain name is hosted on other platforms, such as www.net.cn, www.xinnet.com, and www.dnspod.cn, verify your domain name by either of the following methods:
  - Method 1: Go to the platform hosting your domain name and complete the DNS verification by following the resolution method required by the platform. For example, if the domain name is hosted on Alibaba Cloud, perform related configurations on the DNS console of Alibaba Cloud.
  - Method 2: Use HUAWEI CLOUD Domain Name Service (DNS) to host your domain name, and then perform the verification by following the instructions in this topic.

  We recommend the second method so that you can complete verification quickly and get your certificate issued faster.
- If you purchase a multi-domain certificate and select verification by DNS, you need to perform verification by DNS separately for each domain name.

(Optional) Step 1: Hosting Domain Name on HUAWEI CLOUD DNS

If your domain names are not hosted on HUAWEI CLOUD, are you willing to migrate them to HUAWEI CLOUD?

- If yes, perform the following operations:
  a. For details, see **How Do I Migrate My Domain from Another DNS Service Provider to HUAWEI CLOUD DNS?**
  b. Go to **Step 2**.
- If not, perform the verification on the corresponding platform. For example, if your domain is hosted on Alibaba Cloud, perform the verification on Alibaba Cloud.

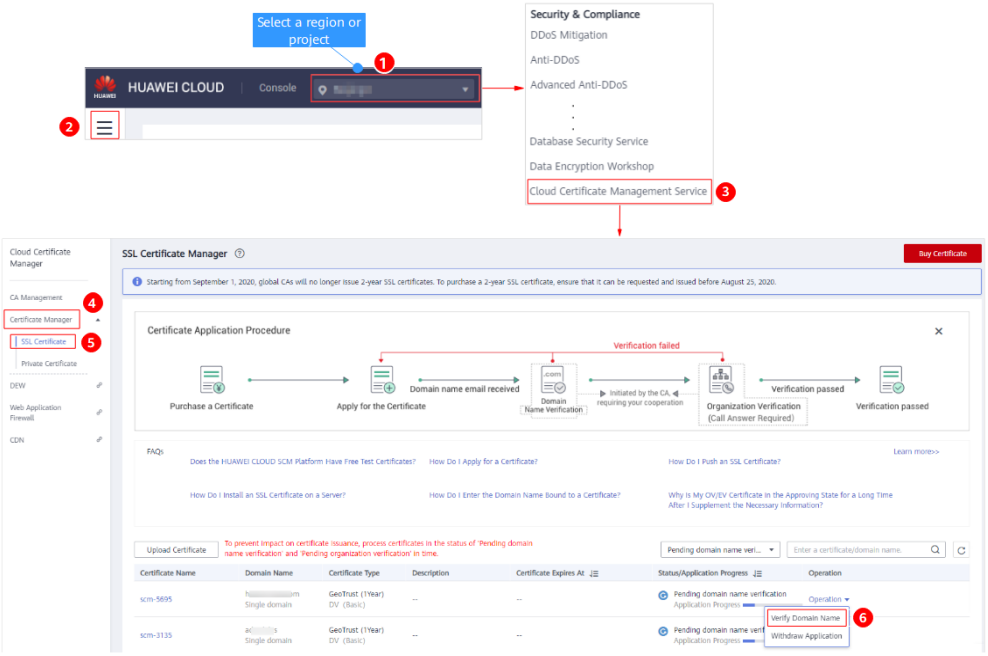
NOTE

If your domain name has been managed on HUAWEI CLOUD, skip this step.

Step 2: Obtaining the Host Record and Record Value of the Domain Name

1. Log in to the **management console**.
2. Go to the domain name verification page by following the steps in **Figure 1-9**.

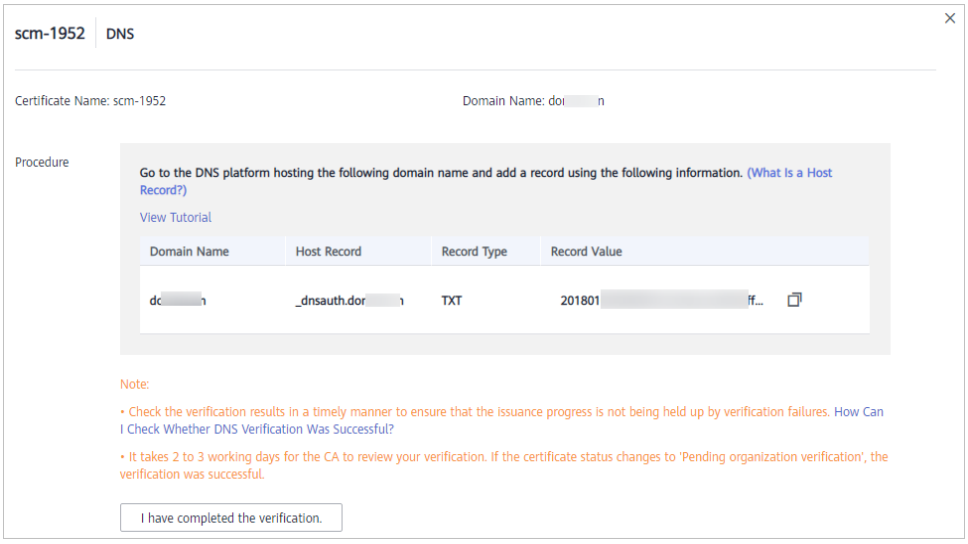
Figure 1-9 Navigation path for accessing the domain name verification page



3. On the **Verify Domain Name** page, view the content for **Host Record**, **Record Type**, and **Record Value**. **Figure 1-10** shows an example.

   If **Host Record**, **Record Type**, and **Record Value** are not displayed, log in to the mailbox to view. The mailbox is the one you provide during certificate application.

Figure 1-10 Viewing a host record



Step 3: Verifying Domain Ownership Using HUAWEI CLOUD DNS

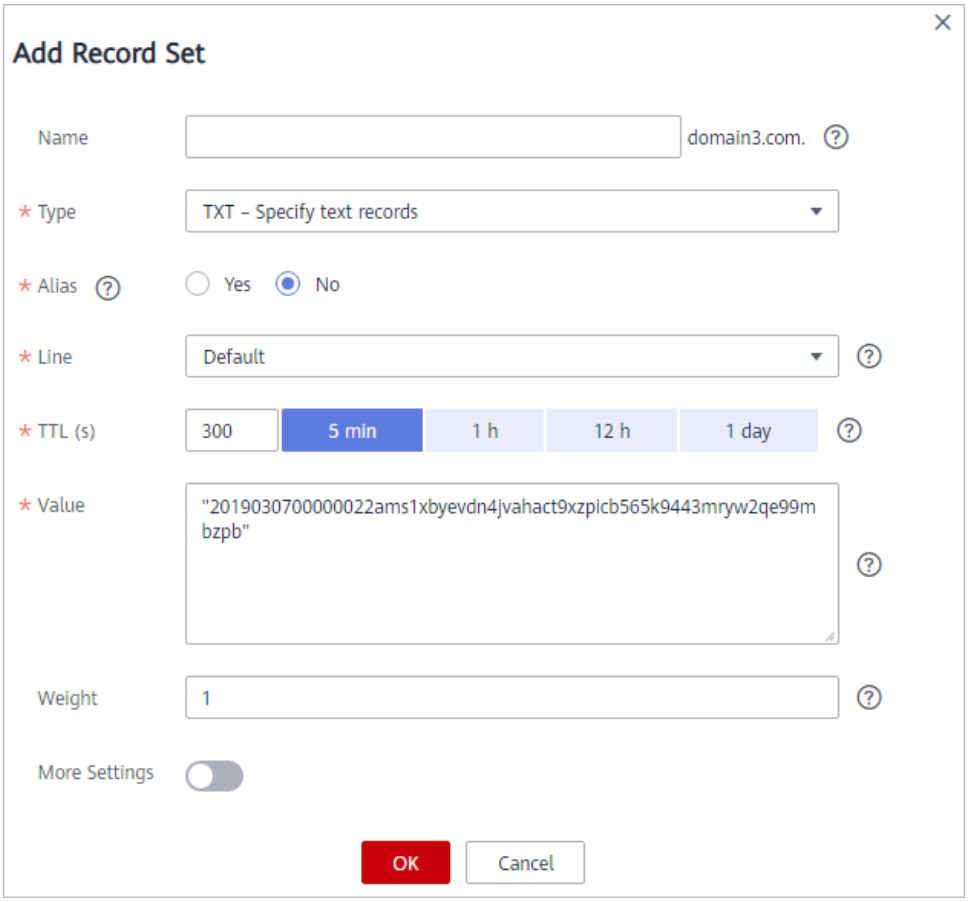
As an example, the following shows how to add a TXT record **2019030700000022ams1xbyevdn4jvahact9xzpicb565k9443mryw2qe99mbzpb** for domain name **domain3.com**. The procedure to verify domain ownership by DNS is similar.

1. Log in to the **management console**.
2. Choose **Domain Name Service** under **Network** to go to the **Domain Name Service** page.
3. In the navigation pane on the left, choose **DNS Resolution** > **Public Zones**. Then click the desired domain name in the list.
4. In the domain name list on the **Public Zones** page, click the added domain name (or the primary domain name for a multi-domain certificate) to go to the record set page.
5. In the upper right corner of the page, click **Add Record Set**. **Figure 1-11** shows an example.

   NOTE

   If there is a TXT record of domain name **domain3.com** in the domain name list, click **Modify** in the **Operation** column. Modify the record in the displayed **Modify Record Set** dialog box.

Figure 1-11 Adding a record set



- **Name**: Enter the prefix of the host record returned by the domain name service provider on the domain name verification page.

  The returned host record varies depending on the domain name service provider. The following are two examples:

  Example:

    - If the host record returned by the domain name service provider is **_dnsauth.domain3.com**, set **Name** to **_dnsauth**.
    - If the host record returned by the domain name service provider is **domain3.com**, leave **Name** empty.
  - **Type**: Select **TXT – Specify text records**.
  - **Line**: Select **Default**.
  - **TTL (s)**: The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
  - **Value**: Enter the record value returned by the domain name service provider on the domain ownership verification page.

    NOTE

    Record values must be quoted with quotation marks and then pasted in the text box.
  - Keep other settings unchanged.
6. Click **OK**.

   If the status of the record set is **Normal**, the record set is added successfully.

   NOTE

   - DNS configuration records can be deleted only after the certificate is issued or revoked.
   - Check whether the DNS record is correctly configured. If not, the certificate cannot be issued.
7. After the verification is complete, additional time is required for the CA to verify your domain name. During this period, the certificate is in the **Pending domain name verification** state.

   The certificate enters the **Pending organization verification** state only after the CA has confirmed your domain ownership.

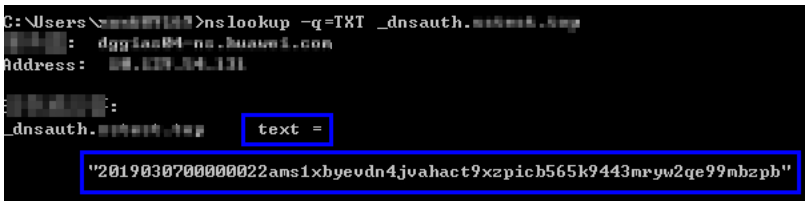
Checking Whether Domain Name Verification Takes Effect

1. On the Windows menu, click **Start** and enter **cmd** to start the command dialog box.
2. Run the following command in the cmd dialog box to check whether the configuration of domain name ownership verification takes effect:

   nslookup -q=TXT *xxx*

   xxx indicates the **Host Record** value returned by the domain name service provider.
   - If the record value in the command output (value of **text**) is the same as that returned by the domain name service provider, the configuration of domain name ownership verification has taken effect. **Figure 1-12** shows an example.

Figure 1-12 Effective configuration of domain name ownership verification



- If the command output does not contain a TXT record and **Non-existent domain** is displayed, the configuration does not take effect.

Figure 1-13 Non-effective domain name verification configuration

If the configuration of domain name ownership verification does not take effect, rectify the fault based on the following possible causes until the verification takes effect:

- It requires a long period of time for the configuration to take effect.

  Check whether the effective time (TTL) is too long. It is recommended that you set the TTL to 5 minutes. This value varies depending on the DNS service provider. In our DNS, the default value is 5 minutes, so the configuration takes effect within 5 minutes by default.

- The record configuration is incorrect.

  Check whether the **Name** or **Type** is correct.

  NOTICE

  Check whether full domain names are supported. If not, delete the suffix of the root domain name.

Verification by File

Verification by file means verifying the domain name ownership by creating a specified file on the server.

After CA approves your application, you need to verify your domain ownership as described in the order, or your certificate will remain in the **Pending domain name verification** state and will not be approved.

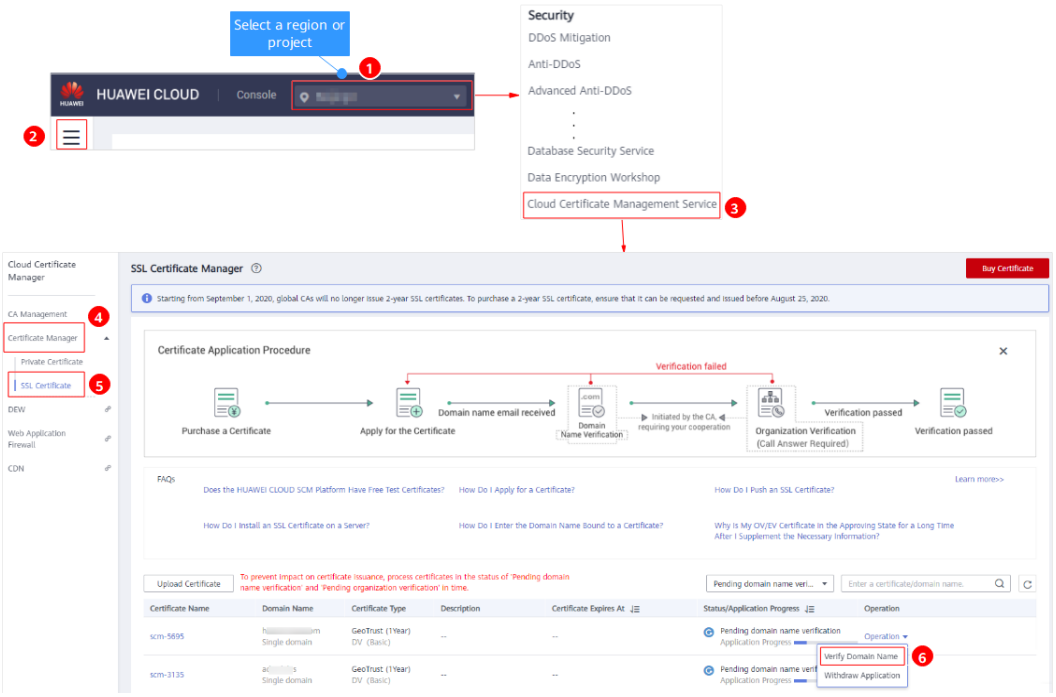
If you purchase a multi-domain certificate and select verification by file, you need to verify each domain separately by file.

Verification by file is usually performed by your server administrator. This section describes how to verify domain ownership by file.

Step 1 Log in to the **management console**.

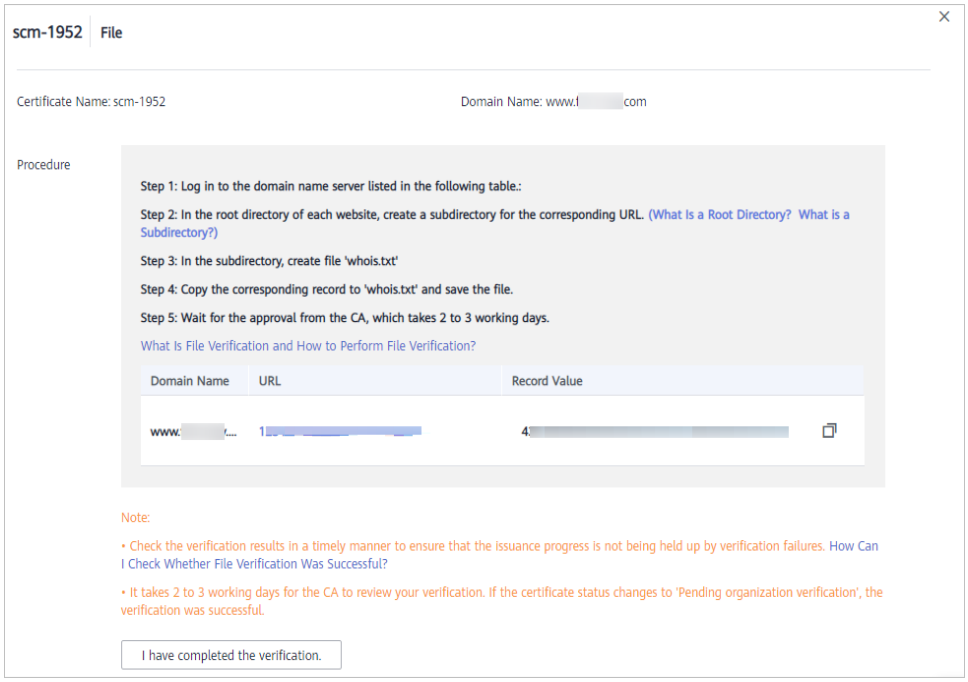
Step 2 Go to the domain name verification page.

Figure 1-14 Navigation path for accessing the domain name verification page



Step 3 View the **Record Value** on the **Verify Domain Name** page, or log in to the email you provided during certificate application, and find the **Record Value**.

Figure 1-15 Verification by file



Step 4 Log in to your server.

Step 5 Create the specified file in the root directory of the website.

NOTE

The root directory of the website refers to the folder where the website programs are stored on the server. The root directory has the following names: **wwwroot**, **htdocs**, **public_html**, **webroot**, and more. Perform operations as required.

Example:

The following uses website root directory **/www/htdocs** as an example:

1. Create the **.well-known/pki-validation** subdirectory in the root directory of the website.

   In this case, create the subdirectory in the **/www/htdocs** directory.
2. Create the **whois.txt** file in the **.well-known/pki-validation** subdirectory.
3. Place the record value obtained in **Step 3** in the **whois.txt** file.

Step 6 Check whether the configuration has taken effect.

1. Open a browser and access the URL address: **https://*your domain*/.well-known/pki-validation/whois.txt** or **http://*your domain*/.well-known/pki-validation/whois.txt**.

   Replace *your domain* in the URL address with the domain name bound during certificate application.

   - If your domain name is a common domain name, perform the following operations:

     For example, if your domain name is **example.domain.com**, the access URL address is **https://example.domain.com/.well-known/pki-validation/whois.txt** or **http://example.domain.com/.well-known/pki-validation/whois.txt**.

     NOTE

     For a domain name starting with **www**, for example, www.domain.com, perform the following operations:

     1. Perform steps **Step 1** to **Step 6** to verify domain name **www.domain.com** by file and check whether the verification configuration has taken effect.
     2. Access the URL address **https://domain.com/.well-known/pki-validation/whois.txt**, and check the value displayed.

        The value displayed must be the same as the value obtained in **Step 3**.

   - For a wildcard domain name, perform the following operations:

     For example, if your domain name is ***.domain.com**, the access URL address is **https://domain.com/.well-known/pki-validation/whois.txt** or **http://domain.com/.well-known/pki-validation/whois.txt**.
2. Check whether the verification has taken effect.

   Check whether the verification URL address can be properly accessed in the browser and if the record value displayed on the page is the same as that on the order progress page or in the email.

   - If the record value matches the one obtained in **Step 3**, the configuration of domain name verification has taken effect.
   - If they are different, the configuration of domain name verification does not take effect.

If the configuration does not take effect, check and handle the issue from the following aspects:

- Check whether the verification URL address exists in HTTPS accessible addresses. If yes, use HTTPS to re-access the URL address in the browser. If the browser displays a message indicating that the certificate is untrusted or the displayed content is incorrect, disable the HTTPS service for the domain name temporarily.
- Ensure that the verification URL address can be accessed at any place. Detection servers of some CAs are located outside China. Check whether your site has images outside China or whether the smart DNS service is used.
- Check whether the verification URL address contains 301 or 302 redirection. If such redirection exists, cancel the related settings to disable the redirection.

  You can run the **wget -S** *URL address* command to check whether the verification URL address is redirected.

Step 7 After the verification is complete, additional time is required for the CA to verify your domain name. During this period, the certificate is in the **Pending domain name verification** state.

If you have verified the domain name, the CA will take 2 to 3 working days to verify your information. The certificate enters the **Pending organization verification** state only after the CA has confirmed your domain ownership.

----End

Verification by Email

After you apply for a certificate, the CA will send a confirmation email to your domain name administrator's email address. Perform the confirmation in the email as prompted. The certificate issuing will enter the next stage after the domain name is verified.

If you purchase a multi-domain certificate and select verification by email, and different email addresses are used, you need to perform verification by email for each domain name.

This section describes how to verify domain ownership by email.

Step 1 Log in to the mailbox of the domain name administrator.

Step 2 Open the domain name confirmation email from the CA.

Step 3 Click the confirmation link in the email to complete the domain name verification.

After the verification is complete, additional time is required for the CA to verify your domain name. During this period, the certificate is in the **Pending domain name verification** state.

If you have verified the domain name, the CA will take 2 to 3 working days to verify your information. The certificate enters the **Pending organization verification** state only after the CA has confirmed your domain ownership.

----End

Follow-up Procedure

If you have applied for an OV, OV Pro, EV, or EV Pro certificate, once domain name verification is complete, the CA will send you an organization verification email. Then, the CA will contact you based on the verification mode you selected to check whether the enterprise or organization has initiated the certificate application. For details, see **Step 4: Verifying the Organization**.

1.5 Step 4: Verifying the Organization

If you apply for an OV, OV Pro, EV, or EV Pro certificate, the CA sends an email to your registered email address for organization verification after domain name verification completes. The CA contacts the enterprise or organization based on the selected verification mode to check whether the enterprise or organization has initiated the certificate application.

NOTICE

If you purchase a certificate again from the same CA within 13 months and the certificate information is not changed, organization verification is not required.

Prerequisites

The certificate is in the **Pending organization verification** state.

Constraints

In the following scenarios, the certificate can be issued only after the organization verification completes:

- Buy an OV, OV Pro, EV, or EV Pro certificate for the first time.
- More than 13 months have elapsed since the last purchase of a certificate.
- The contact information, company information, or certificate brand is different from that of the last purchase.

Procedure

Step 1 Log in to the mailbox you left when applying for a certificate.

Step 2 Open the organization verification email from the CA.

Step 3 Reply to the email from the CA to select an organization verification method.

You can select the verification by phone call or lawyer's letter. Verification by lawyer's letter requires an extra billing of ¥500. Select an organization verification method based on your needs.

If you need to change the organization verification method, reply to the email from the CA.

Step 4 Cooperate with the CA and complete the verification by the method you select.

For example, if you select verification by phone call, answer the phone when the CA contacts you through the public phone of your organization.

----End

Follow-up Procedure

After the organization verification completes, it takes some time for CA to complete the verification.

After you submit an application, the CA checks the domain ownership or organization verification status at the following frequency:

- 0 to 1 hour after the application is submitted: The CA checks the verification status every 15 minutes. Generally, if the configuration is correct, the certificate is issued within 10 to 20 minutes.
- 1 to 4 hours after the application is submitted: The CA checks the verification every 30 minutes.
- 4 to 24 hours after the application is submitted: The CA checks the verification every hour.
- 1 to 7 days after the application is submitted: The CA checks the verification every 4 hours.
- If you did not complete the required verification over 7 days after the application is submitted, the order times out and is automatically canceled. In this case, locate the causes and solve the problem by referring to **Why Does the Certificate Stay in the CA Verifying Status for a Long Time?**

After being approved by the CA, the certificate will be issued. The certificate takes effect immediately upon issuance. You can push the certificate to other cloud products on HUAWEI CLOUD or download the certificate and deploy it on a server.

For details about how to push a certificate, see **Pushing Certificates to Other Services on HUAWEI CLOUD**.

For details about how to download a certificate, see **Downloading a Certificate**.

1.6 Example 1: Applying for a Free Certificate

In HUAWEI CLOUDSCM, you can get free single-domain basic DV certificates issued by DigiCert. The validity period of such free certificates is one year.

Prerequisites

The account for purchasing a certificate has the SCM Administrator, BSS Administrator, and DNS Administrator permissions.

Constraints

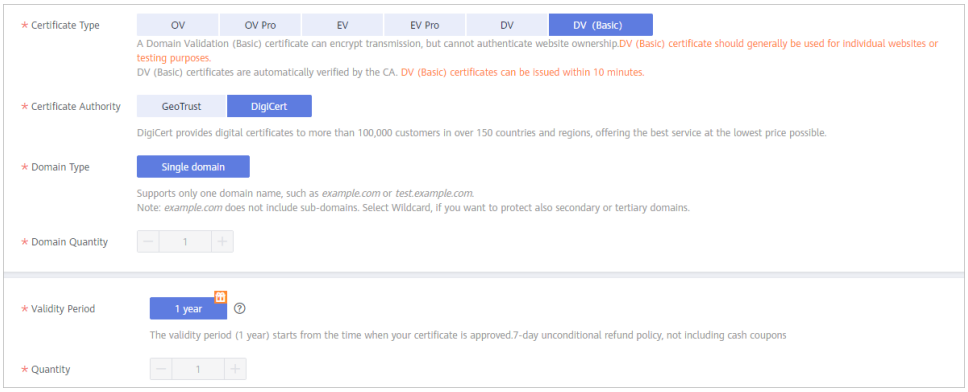
- You can apply for a maximum of 20 free SSL certificates under each account. In SCM, only one free certificate can be applied for at a time.
- One free SSL certificate can be used for only one single domain name.
- Free certificates cannot be used to protect IP addresses or wildcard domain names.

- By default, DNS verification is used to verify the domain ownership of a free certificate.
- The trust and security level of free certificates are low. They are recommended only for testing.
- For DigiCert DV (Basic) free certificates, no free technical support or installation guide is provided. To get related support services from HUAWEI CLOUD engineers, you can purchase the HTTPS service in Marketplace on HUAWEI CLOUD website.

Step 1: Buy a Certificate

1. Log in to the **management console**.
2. In the navigation pane on the left, click ☰ and choose **Cloud Certificate Management Service** under **Security & Compliance**.
3. In the navigation pane on the left, choose **Certificate Manager** > **SSL Certificate**.
4. In the upper right corner of the page, click **Buy Certificate** to go to the certificate purchase page.
5. On the certificate purchase page, set parameters.
   - **Certificate Type**: Select **DV (Basic)**.
   - **Certificate Authority**: Select **DigiCert**.
   - After you select a certificate type and CA, other parameters, such as **Domain Type**, **Domain Quantity**, **Validity Period**, and **Quantity**, are configured automatically.

   Figure 1-16 Free certificate configuration



6. Click **Next**.
7. Confirm the order information and agree to the SCM disclaimer by selecting **I have read and agree to the SSL Certificate Manager Disclaimer**. Click **Pay**.
8. On the displayed page, select a payment method.

   After the payment is complete, go back to the certificate list to view the purchased certificate.

Step 2: Apply for the Certificate from the CA

After you purchase a certificate, you need to associate a domain name, provide additional details, and then submit the application for approval.

1. Log in to the **management console**.
2. In the navigation pane on the left, click ☰ and choose **Cloud Certificate Management Service** under **Security & Compliance**.
3. In the navigation pane on the left, choose **Certificate Manager** > **SSL Certificate**.
4. In the certificate list, locate the row that contains the free certificate, and click **Apply for Certificate** in the **Operation** column.
5. On the displayed page, enter the domain name and contact information.
   a. Enter the domain name information. **Table 1-6** describes the parameters.

Figure 1-17 Domain name configuration

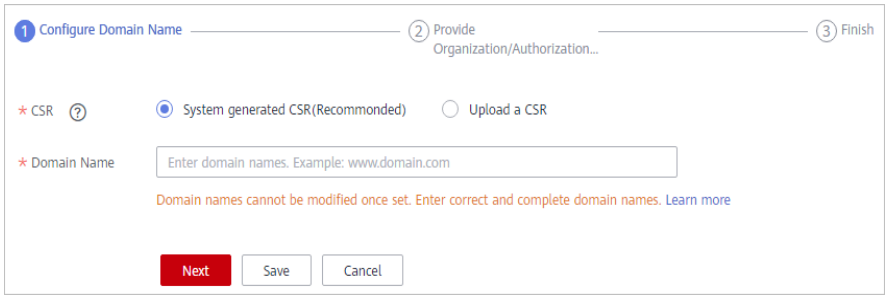


Table 1-6 Domain name parameters

Parameter	Description	Example Value
CSR	To obtain an SSL certificate, a Certificate Signing Request (CSR) file needs to be submitted to the CA for review. A CSR contains a public key and a distinguished name (DN). Typically, a CSR is generated by a web server. A pair of public and private keys are created along with the CSR. Options: • **System generated CSR**: The system automatically generates a certificate private key. Once the certificate is issued, you can download your certificate and private key on the certificate management page. • **Upload a CSR**: You need to manually generate a CSR file and paste the content of the CSR file generated into the text box. For more details, see **How Do I Make a CSR File?**	System generated CSR

Parameter	Description	Example Value
Domain Name	The domain name for which the certificate is used Example: If your domain is *www.domain.com*, enter ***www.domain.com*** for **Domain Name**.	www.domain.com

b. Click **Next**. The **Provide Organization/Authorization Details** page is displayed.

c. Enter the company contact information. **Table 1-7** describes the parameters.

Figure 1-18 Configuring authorization information

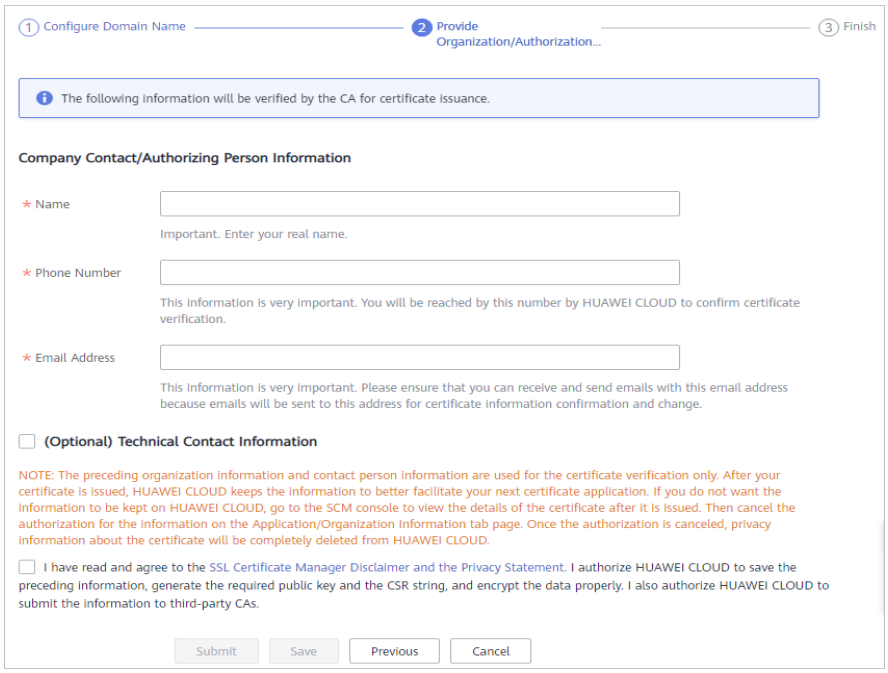


Table 1-7 Parameter description

Parameter	Description	Example Value
Company Contact/ Authorizing Person Information	You only need to enter the name, phone number, and email address of the contact. To get your certificate issued quickly, the phone number and email address entered must be valid.	None

Parameter	Description	Example Value
(Optional) Technical Contact Information	The parameter is optional. You can skip it.	None

6. After confirming that the entered information is correct, read through the *SSL Certificate Manager Disclaimer*, *Privacy Statement*, and the authorization statement, and check the box to agree to the disclaimer and statements

   You can revoke the privacy rule authorization if the certificate is not being approved. Once you revoke the authorization, HUAWEI CLOUD will no longer store your information. The contact name, phone number, email address, and organization details will be deleted. For more details, see **Canceling Authorization for Privacy Information**.

7. Click **Submit**.

   The system prompts you to perform the next operation, and the certificate status changes to **Pending domain name verification**.

   The system will submit your application to the CA. During the approval process, make sure that you can be reached by phone and that you regularly check for emails from the CA.

   NOTE

   - You can click **Save** to save your progress.
   - The CA will process your application and send you a domain name verification email within 2 to 3 working days.

Step 3: Verify Domain Ownership by DNS

Domain name ownership verification by DNS is to verify domain ownership by resolving a specific DNS record on the platform hosting the domain name. To this end, you need to add a TXT DNS record for your domain name on the platform. For example, if you purchase a domain name from company A, you need to add a TXT DNS record for your domain name on the domain name management platform of company A. For details about how to verify domain name ownership by DNS, see **Verifying Domain Ownership by Resolving the DNS TXT Record**.

- If you apply for a domain name on HUAWEI CLOUD and the domain name has been resolved by HUAWEI CLOUD DNS, the system automatically adds DNS records for verification.
- If your domain name is hosted on other platforms, such as www.net.cn, www.xinnet.com, and www.dnspod.cn, you need to go to the DNS service provider of the domain name to perform the verification.

  For more details, see **Manual DNS Verification**.

NOTE

After the certificate application succeeds, you need to complete the configuration of domain name verification based on the information displayed on the certificate list page. Otherwise, your certificate will remain in the **Pending domain name verification** state and will fail in the verification.

Step 4: Issue the Certificate

After the domain name ownership is verified using DNS, the CA will take some time to approve. The certificate will be issued after being approved by the CA.

The certificate takes effect immediately upon issuance. You can push the certificate to other cloud products on HUAWEI CLOUD or download the certificate and deploy it on a server.

NOTE

After you submit an application, the CA checks the domain ownership or organization verification status at the following frequency:

- 0 to 1 hour after the application is submitted: The CA checks the verification status every 15 minutes. Generally, if the configuration is correct, the certificate is issued within 10 to 20 minutes.
- 1 to 4 hours after the application is submitted: The CA checks the verification every 30 minutes.
- 4 to 24 hours after the application is submitted: The CA checks the verification every hour.
- 1 to 7 days after the application is submitted: The CA checks the verification every 4 hours.
- If you did not complete the required verification over 7 days after the application is submitted, the order times out and is automatically canceled. In this case, locate the causes and solve the problem by referring to **Why Does the Certificate Stay in the CA Verifying Status for a Long Time?**

1.7 Example 2: Applying for an IP Address Certificate

SSL Certificate Manager provides certificates associated with IP addresses. If you need a certificate associated with an IP address and the IP address is a public IP address, apply for a certificate associated with an IP address.

The GlobalSign authority (OV type) provides certificates associated with IP addresses. Currently, only a certificate associated with one IP address can be applied for.

The following walks you through how to apply for a certificate associated with an IP address.

Prerequisites

The account for purchasing a certificate has the SCM Administrator, BSS Administrator, and DNS Administrator permissions.

Constraints

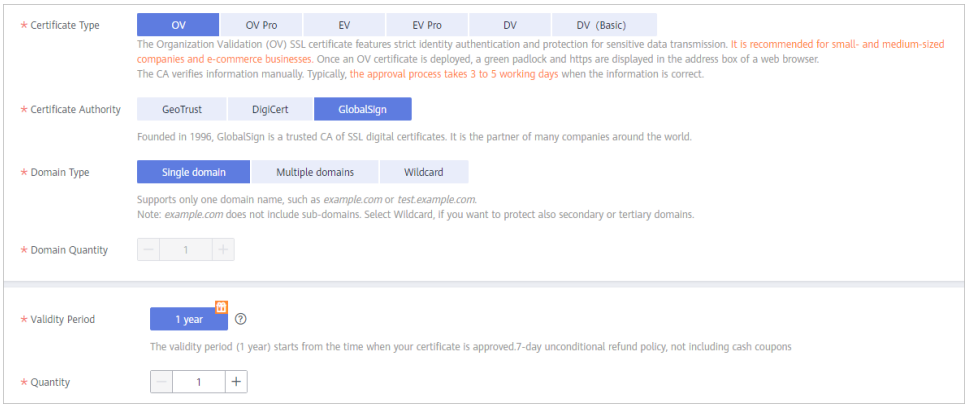
- Only GlobalSign (OV type) provides certificates associated with IP addresses.
- A single-domain OV certificate of GlobalSign can be associated with only one public IP address.
- Domain name ownership can only be verified by file.

Step 1: Buy a Certificate

A certificate associated with an IP address can be only a single-domain certificate of the GlobalSign authority and OV type. There are no IP address certificates available in other certificate authorities or types.

1. Log in to the **management console**.
2. In the navigation pane on the left, click ☰ and choose **Cloud Certificate Management Service** under **Security & Compliance**.
3. In the navigation pane on the left, choose **Certificate Manager** > **SSL Certificate**.
4. In the upper right corner of the page, click **Buy Certificate** to go to the certificate purchase page.
5. On the certificate purchase page, set parameters.
   - **Certificate Type**: Select **OV**.
   - **Certificate Authority**: Select **GlobalSign**.
   - **Domain Type**: Select **Single domain**.
   - **Quantity**: Set this parameter based on your requirements.
   - **Domain Quantity** and **Validity Period** are automatically configured.

   Figure 1-19 IP address certificate configuration



6. Click **Next**.
7. Confirm the order information and agree to the SCM disclaimer by selecting **I have read and agree to the SSL Certificate Manager Disclaimer**. Click **Pay**.
8. On the displayed page, select a payment method.

   After the payment is complete, go back to the certificate list to view the purchased certificate.

Step 2: Apply for the Certificate from the CA

After you purchase a certificate, you need to associate a domain name, provide additional details, and then submit the application for approval.

For details about how to apply for the certificate, see **Apply for the Certificate**.

NOTICE

On the **Domain Name Information** page, **Domain Name** must be set to a public IP address to be associated with, and only **File** can be selected for **Domain Name Verification Method**.

Step 3: Verify Domain Ownership by File

In this method, you are required to verify domain name ownership by creating a specified file on the server. Generally, you need to ask the server administrator to perform verification by file. For more details, see **Verification by File**.

NOTE

After CA approves your application, you need to verify your domain ownership as described in the order, or your certificate will remain in the **Pending domain name verification** state and will not be approved.

Step 4: Verify the Organization

After verification by file is complete, the CA sends an organization verification email to your mailbox. The CA contacts the enterprise or organization based on the selected verification mode to check whether the enterprise or organization has initiated the certificate application.

For more details, see **Verify the Organization**.

Step 5: Issue the Certificate

After the organization verification completes, it takes some time for CA to complete the verification. The certificate will be issued after being approved by the CA.

The certificate takes effect immediately upon issuance. You can push the certificate to other cloud products on HUAWEI CLOUD or download the certificate and deploy it on a server.

NOTE

After you submit an application, the CA checks the domain ownership or organization verification status at the following frequency:

- 0 to 1 hour after the application is submitted: The CA checks the verification status every 15 minutes. Generally, if the configuration is correct, the certificate is issued within 10 to 20 minutes.
- 1 to 4 hours after the application is submitted: The CA checks the verification every 30 minutes.
- 4 to 24 hours after the application is submitted: The CA checks the verification every hour.
- 1 to 7 days after the application is submitted: The CA checks the verification every 4 hours.
- If you did not complete the required verification over 7 days after the application is submitted, the order times out and is automatically canceled. In this case, locate the causes and solve the problem by referring to **Why Does the Certificate Stay in the CA Verifying Status for a Long Time?**

2 Applying for a Private Certificate

2.1 Step 1: Applying for a PCA

PCA is in the open beta test (OBT) phase. To use this service, apply for the OBT and obtain the approval.

This section describes how to apply for OBT for PCA.

Procedure

Step 1 Log in to the **management console**.

Step 2 In the navigation pane on the left, click  and choose **Cloud Certificate Management Service** under **Security & Compliance**. On the displayed CCM homepage, choose **CA Management** > **Private CA**.

Step 3 Click **Apply for Certificate**.

Step 4 On the **Apply to Beta Test** page, enter the application details.

After your application is approved, you can use PCA.

----End

Follow-up Procedure

After your OBT application is approved, you can use PCA.

2.2 Step 2: Creating a Private CA

This section describes how to create a private CA. The private CA can be a root CA or a subordinate CA.

A maximum of 100 CAs can be created for each user. Private CAs in the pending deletion state are also counted in the private CA quota until the private CAs are deleted.

Procedure

Step 1 Log in to the **management console**.

Step 2 In the navigation pane on the left, click ☰ and choose **Cloud Certificate Management Service** under **Security & Compliance**. On the displayed CCM homepage, choose **CA Management** > **Private CA**.

Step 3 In the upper left corner of the private CA list, click **Create CA** to switch to the **Create CA** page.

Step 4 Configure the CA information.

You need to specify the basic information, distinguished name, and certificate revocation configuration.

1. Configure the basic information. **Table 2-1** describes the parameters.

Figure 2-1 Basic information

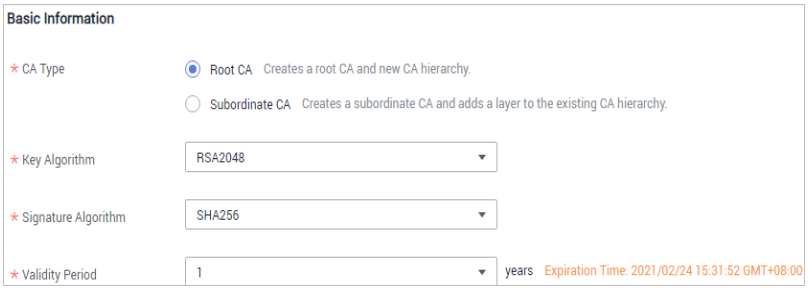


Table 2-1 Basic information parameters

Parameter	Description	Example Value
CA Type	Indicates the type of the CA to be created. The values can be: – **Root CA**: Select this option if you want to create a CA hierarchy. **NOTE** If you create a private CA for the first time, you must create a root CA. – **Subordinate CA**: Select this option if you want to add a layer to the existing CA hierarchy.	Root CA
Key Algorithm	Indicates the key algorithm. The values can be: – RSA2048 – RSA4096 – EC256 – EC384	RSA2048

Parameter	Description	Example Value
Signature Algorithm	This parameter is displayed when **CA Type** is set to **Root CA**. Indicates the signature algorithm. The values can be: – SHA256 – SHA384 – SHA512	SHA256
Validity Period	This parameter is displayed when **CA Type** is set to **Root CA**. Indicates the validity period of a private certificate issuer. The longest period is 30 years.	3 years

2. Configure the certificated distinguished name. **Table 2-2** describes the parameters.

Figure 2-2 Distinguished name

Table 2-2 Parameters

Parameter	Description	Example Value
Common Name	Indicates the CA name.	-
Country/Region	Indicates the country or region where your organization belongs. Enter the two-letter code of the country or region.	CN
State/Province	Indicates the name of the province or state where your organization is located.	ShenZhen
City	Indicates the name of the city where your company is located.	GuangZhou
Organization	Indicates the legal name of your company.	Huawei Technologies Co., Ltd.
Organizational Unit	Indicates the department to which your organization belongs.	Cloud Dept.

3. (Optional) Configure certificate revocation.

If you want to publish the certificate revocation list (CRL) for a private CA, you can configure parameters in this pane.

Otherwise, skip this step.

Table 2-3 describes the parameters.

Figure 2-3 Revoking a certificate

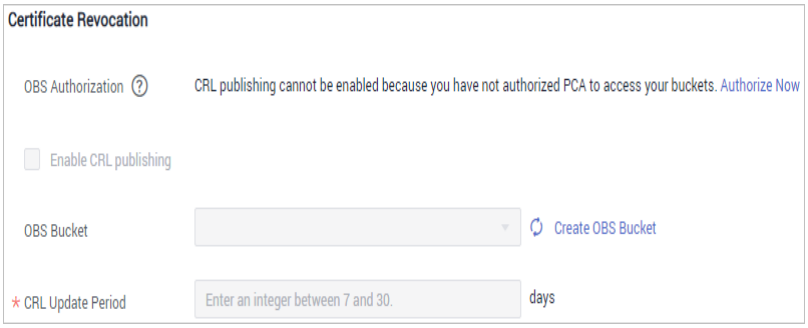


Table 2-3 Certificate revocation parameters

Parameter	Description
OBS Authorization	Indicates whether to authorize PCA to access your OBS bucket and upload the CRL file. If you want to authorize, click **Authorize Now** and complete the authorization as prompted. If you want to cancel the authorization, go to the IAM console to delete the PCAAccessPrivateOBS agency from the agency list. After the permission has been granted, follow-up operations do not require the permission to be granted again.
Enable CRL publishing	Indicates whether to enable CRL publishing.
OBS Bucket	Select an existing OBS bucket or click **Create OBS Bucket** to create an OBS bucket.
CRL Update Period	Indicates the CRL update period. PCA will generate a new CRL at the specified time. Enter an integer between 7 and 30.

Step 5 Click **Next** to enter the confirmation page.

Step 6 After confirming that the information is correct, click **Confirm and Create**.

If you create a root CA, the root CA is automatically activated after being created. If you create a subordinate CA, you need to manually activate it.

After you create a subordinate CA, click **Activate Now** or **Activate Later** to determine whether to activate the subordinate CA immediately.

----End

Follow-up Procedure

After a root CA is created, it can be used to issue private certificates. For details about how to apply for a private certificate, see **Step 4: Applying for a Private Certificate**.

After a subordinate CA is created, you need to install a certificate and activate the CA. For details, see **Step 3: Activating a Private CA**.

2.3 Step 3: Activating a Private CA

You need to active a subordinate CA after it is created.

The system provides two methods of activating private CAs: using internal private CAs or external private CAs. This section describes how to activate private CAs using internal private CAs. For details about how to activate private CAs using external private CAs, see **Activating a Private CA**.

Prerequisites

- You have created a subordinate CA.
- The subordinate CA is in the **Pending activation** state.

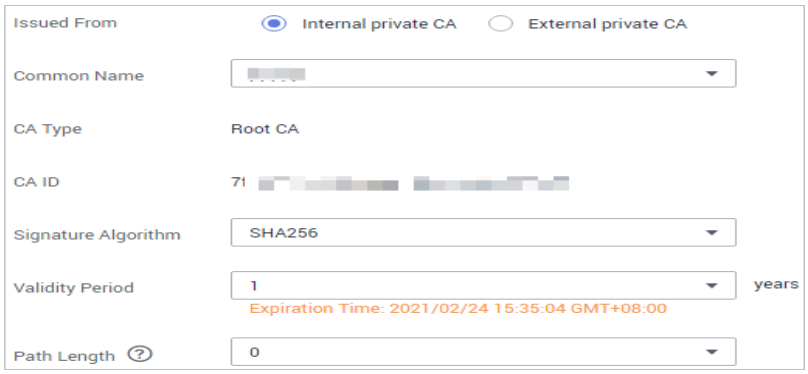
Procedure

Step 1 Log in to the **management console**.

Step 2 In the navigation pane on the left, click ☰ and choose **Cloud Certificate Management Service** under **Security & Compliance**. On the displayed CCM homepage, choose **CA Management** > **Private CA**.

Step 3 Locate the row of the subordinate CA and click **Activate** in the **Operation** column. In the **Install CA Certificate and Activate CA** page, configure the required parameters.

Figure 2-4 Internal private CA



1. Configure **Issued From**.
   Select **Internal private CA**.
2. Configure the required parameters.

Table 2-4 Parameters

Parameter	Description
Common Name	Indicates the name of the CA. The CA can be a root CA or a subordinate CA. After you select the CA, the system automatically displays the type and ID of the CA.
Signature Algorithm	Indicates the signature algorithm. The values can be: – SHA256 – SHA384 – SHA512
Validity Period	Indicates the validity period of a private CA. The longest period is 20 years.
Path Length	Indicates the path length of the subordinate CA. That is, the number of layers of CA certificates that can be issued by the current CA. This parameter can be used to control the certificate chain length.

Step 4 Confirm the configuration and click **OK**.

----End

Follow-up Procedure

After a subordinate CA is activated, it can be used to issue private certificates. For details about how to apply for a private certificate, see **Step 4: Applying for a Private Certificate**.

2.4 Step 4: Applying for a Private Certificate

This section describes how to apply for a private certificate.

Each user can apply for a maximum of 100,000 certificates.

Prerequisites

You have created a private CA and activated it.

Procedure

Step 1 Log in to the **management console**.

Step 2 In the navigation pane on the left, click ☰ and choose **Cloud Certificate Management Service** under **Security & Compliance**. On the displayed CCM homepage, choose **CA Management** > **Private CA**.

Step 3 In the left navigation pane, choose **Certificate Manager** > **Private Certificate** to switch to the **Private Certificate** page.

Step 4 In the upper left corner of the private certificate list, click **Apply for Certificate** to switch to the **Apply for Certificate** page. Configure the application details.

Figure 2-5 System generated CSR

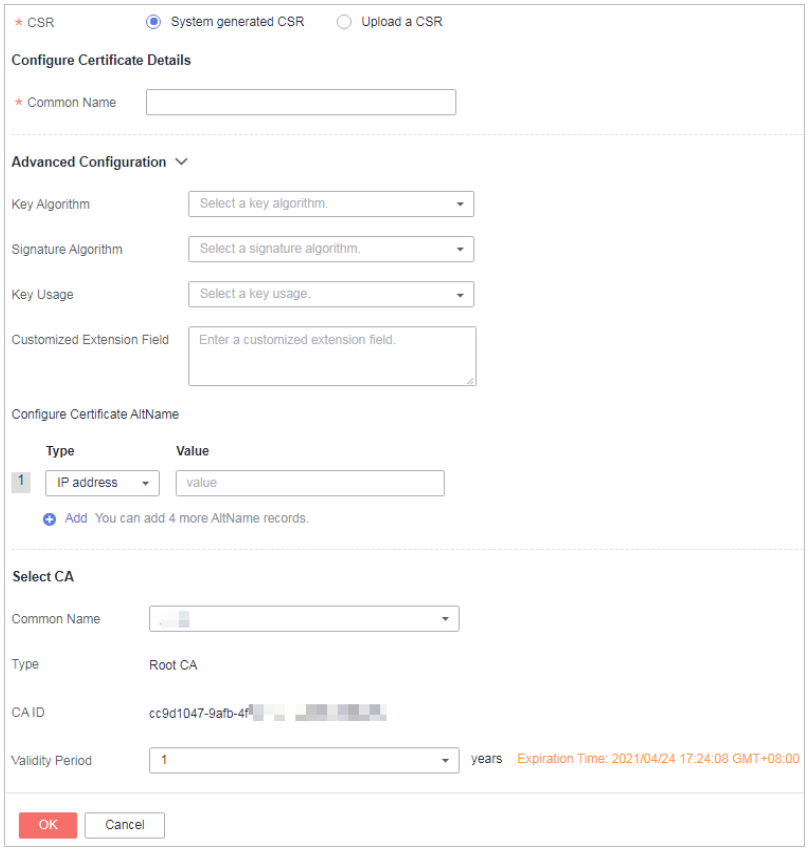
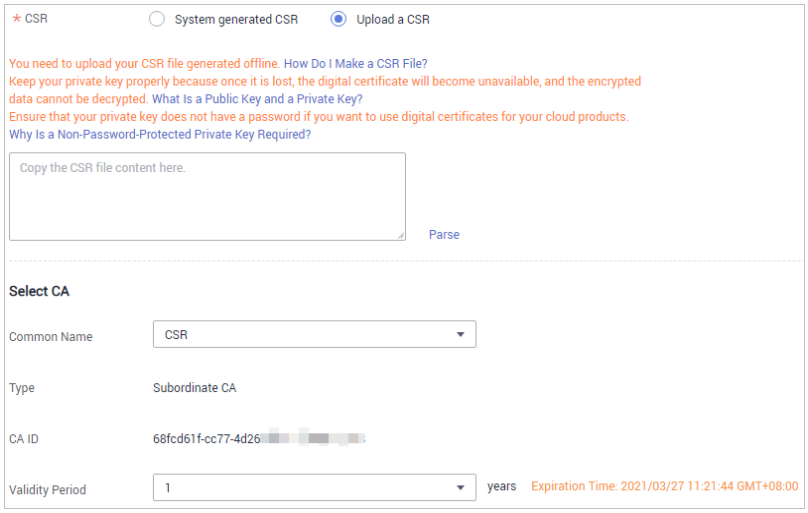


Figure 2-6 Upload a CSR



1. Select the CSR file generation method.

- **System generated CSR**: The system automatically generates a certificate private key. Once the certificate is issued, you can download your certificate and private key on the certificate management page.
- **Upload a CSR**
  i. You need to manually generate a CSR file and paste the content of the CSR file generated into the text box.
  ii. Click **Parse**.

NOTE

- To obtain a certificate, a CSR file needs to be submitted to the CA for review. A CSR contains a public key and a distinguished name (DN). Typically, a CSR is generated by a web server. A pair of public and private keys are created along with the CSR.
- You are advised to select **System generated CSR** to avoid approval failure caused by incorrect content.
- If the CSR file is generated manually, HUAWEI CLOUD is not responsible for your private key. Back up your private key and keep it secure. If a private key is lost, the corresponding certificate becomes invalid. HUAWEI CLOUD is not responsible for keeping your private key. You need to purchase a new certificate if the private key is lost.
- SCM has strict requirements on the key type and length of the CSR file. The key must be RSA and it must be 2,048 bits long.

2. Configure certificate details.

   Perform this step only when you select **System generated CSR** for **CSR**.

   Common Name: You can customize the name of the private certificate.

3. Click ^ on the right of **Advanced Configuration**.

   Perform this step only when you select **System generated CSR** for **CSR**.

   - **Key Algorithm**: Select the key algorithm and key size of the certificate. The value can be **RSA2048**, **RSA4096**, **EC256**, or **EC384**.
   - **Signature Algorithm**: Select the signature hash algorithm of the certificate. The value can be **SHA256**, **SHA384**, or **SHA512**.
   - **Key Usage**: Select the key usage of the certificate.
   - **Customized Extension Field**: Enter the customized information of the certificate.
   - (Optional) Configure the certificate AltName. You can configure **IP address** or **DNS** for certificate AltName.

     If you select **IP address**, you need to enter the corresponding IP address. If you select **DNS**, you need to enter the corresponding domain name.

     A maximum of five AltName records can be configured.

4. Select a CA.

   - **Common Name**: Select a created CA.
   - **Type**: After you select a common name, the system automatically displays the CA type.
   - **CA ID**: After you select a common name, the system automatically displays the CA ID.
   - **Validity Period**: Set the validity period of the private certificate.

Step 5 Confirm the information and click **OK**.

After you submit your application, the system will return to the private certificate list page. Message "Certificate xxx applied for successfully." is displayed in the upper right corner of the page, indicating that the private certificate application is successful.

----End

Follow-Up Procedure

After applying for a private certificate, you can download the private certificate. For details, see **Downloading a Private Certificate**.

A Change History

Released On	Description
2021-05-26	This issue is the sixth official release. Optimized **Step 3: Verifying the Domain Ownership**.
2021-04-29	This issue is the fifth official release. SCM allows you to purchase one multi-domain certificate for both single domains and wildcard domains.
2021-03-12	This issue is the fourth official release. • Updated the screenshots based on the optimized GUI page for SSL certificate application. • Added the automatic DNS verification for SSL certificate management.
2021-01-26	This issue is the third official release. Added SSL certificate management functions.
2020-04-29	This issue is the second official release. Optimized **Step 4: Applying for a Private Certificate**. Specifically, added descriptions about configuring **Key Algorithm**, **Signature Algorithm**, **Key Usage**, and **Customized Extension Field**.
2020-02-28	This issue is the first official release.

