# Cloud Certificate Manager

# FAQ

**Issue** 01

**Date** 2023-12-15

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

## Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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 FAQs

## 1.1 Certificate Consulting

### 1.1.1 What Are the Differences Between SSL Certificate Manager and Private Certificate Authority?

#### Concepts

SCM is a platform to centrally manage your Secure Sockets Layer (SSL) certificates. Working with trusted Certificate Authorities (CAs) around the world, SCM enables one-stop SSL certificate lifecycle management and helps you improve trust and secure data transmission for your websites.

Private Certificate Authority (PCA) is a private CA and certificate management platform. You can use CCM to set up a complete CA hierarchy and use it to issue and manage private certificates for your organization. It is used to authenticate application identities and encrypt and decrypt data within an organization.

#### Differences Between SCM and PCA

**Table 1-1** describes the differences between SCM and PCA.

**Table 1-1** Differences between SCM and PCA

| Service Name | Function | Application Scenario | Security Level | Apply to Internal Network |
| --- | --- | --- | --- | --- |
| SSL Certificate Manager (SCM) | After an SSL certificate is deployed on a server, HTTPS is enabled on the server. The server uses HTTPS to establish encrypted links to the client, ensuring data transmission security.<br>• Authenticate websites and ensure that data is sent to the correct clients and servers.<br>• Set up encrypted connections between clients and servers, preventing data from being stolen or tampered with during transmission. | • Authenticating websites<br>An SSL certificate validates the identity of a website on the Internet. If a website is not installed with an SSL certificate, the browser considers the website as insecure so that the website is hardly trusted by users and have few visitors. Visitors are more likely to explore a website secured with an SSL certificate because they believe the website is secure enough. Especially the websites that use OV or EV certificates, the CA validates the domain name ownership and enterprise identity before issuing a certificate, which effectively improves the website credibility.<br>• Website data encryption<br>The data transmitted over HTTP always faces high risks of being disclosed, eavesdropped, or tampered with as | High | Not supported. SSL certificates can be used only for public domain names. |

| Service Name | Function | Application Scenario | Security Level | Apply to Internal Network |
| --- | --- | --- | --- | --- |
| | | HTTP cannot encrypt data in transit. SSL certificates covert your HTTP website to an HTTPS one. An HTTPS-secured website enables encrypted communication and effectively improves data transmission security.<br>• Website loading speed acceleration SSL certificates are compatible with HTTP/2 and can be used to quickly and dynamically load web page content. | | |

| Service Name | Function | Application Scenario | Security Level | Apply to Internal Network |
| --- | --- | --- | --- | --- |
| PCA | • Allows you to set up a complete CA hierarchy, including root CAs and multi-level intermediate CAs.<br>• Provides high-availability and high-security private CA hosting capabilities.<br>• Allow you to create and manage private certificates. These private certificates are used to identify and protect the resources of your organization, including applications, services, devices, and users. | • Internal application data security control You can use PCA to establish an internal certificate management system for your enterprise and issue and manage self-signed private certificates to authenticate identities, encrypt and decrypt data, and secure data transmission within the enterprise.<br>• IoV applications Telematics Service Providers (TSPs) can use PCA to issue a certificate to each vehicle terminal, thereby providing security capabilities such as authentication and encryption during vehicle-vehicle, vehicle-cloud, and vehicle-road interaction.<br>• IoT applications The Internet of Things (IoT) platform can use PCA to issue a certificate to each IoT device to implement IoT device identity verification and authentication, ensuring device access security in IoT scenarios. | Low | Supported. Private certificates can be deployed on the intranet. |

## 1.1.2 Which Websites Require HTTPS?

HTTPS is adopted by more and more websites in today's world where information security is increasingly important. Currently, HTTPS is strongly recommended for the following websites:

- E-commerce platforms and their payment systems
- Banking systems and high-privacy websites of financial institutions
- Websites of governments, universities, research institutes
- Websites whose visitors are mostly brought by search engines
- Enterprises' email-based internal communication platforms

In the long run, HTTPS is an inevitable trend. Enabling HTTPS encryption is a key point of today's website construction. In addition to the websites listed earlier, users are advised to enable HTTPS for other types of websites to prepare their companies for development.

## 1.1.3 What Are the Differences Between HTTPS and HTTP?

### Differences Between HTTPS and HTTP

Hypertext Transfer Protocol (HTTP) was commonly used for a long time. HTTP does not encrypt the data that it transmits, which means that confidential information, such as passwords, accounts, and transaction records, is plaintext and may be leaked, stolen, or tampered with anytime. Therefore, HTTP is regarded as an insecure protocol for private information.

Based on the Secure Sockets Layer (SSL) protocol, Hypertext Transfer Protocol Secure (HTTPS) activates an SSL encrypted channel between a web browser and a website server for a user to visit the website where an SSL certificate has been installed. The channel allows high-strength bidirectional encrypted transmission to prevent leakage or tampering of the data being transmitted. Simply put, HTTPS is HTTP plus SSL or a secure version of HTTP.

### How Do I Change the Website Protocol from HTTP to HTTPS?

If you want to implement HTTPS for a website, you can purchase an SSL certificate and deploy it on the server corresponding to the website.

After an SSL certificate is deployed on a server, HTTPS is enabled on the server. The server uses HTTPS to establish encrypted links to the client, ensuring data transmission security.

## 1.1.4 What Is a Public Key and a Private Key?

A pair of public and private keys are used in the encryption method commonly known as the asymmetric encryption method. The key pair, consisting of a public key and a private key, is generated based on an algorithm. The public key is open while the private key is not. The public key is usually used to encrypt session keys, verify digital signatures, or encrypt data that can be decrypted using the corresponding private key.

The public and private key pair is unique across the whole world. If one key is used to encrypt a piece of data, the other key must be used to decrypt the data. If you use either key to encrypt a piece of data, the encrypted data can only be decrypted using the other key or the decryption fails.

**NOTE**

Due to the privacy of a private key, you are advised to generate and keep it properly by yourself. Loss of the private key may cause website information leakage. If the private key is lost, revoke the certificate immediately and apply for a new SSL certificate for the domain name.

## Working Principles of a Digital Certificate

A digital certificate uses the public key system which consists of a pair of matched keys to encrypt and decrypt data. Each user sets a specific private key that is known only to himself or herself and uses it for decryption and signature. At the same time, the user sets a public key and shares it with a group of other users for encryption and signature verification.

Because only the owner has the key, the owner can use it to generate a digital signature that no other users can generate.

A digital certificate is a file digitally signed by a CA and contains information about the owner of a public key and the public key. The simplest certificate contains a public key, name, and digital signature of the CA. Another important feature of a digital certificate is that it is valid only within a specific period of time.

## Creating a Private Key

SCM has the following requirements on the encryption algorithm and length of your private key:

- RSA
- At least 2048 bits

  **NOTE**

  The 2048-bit SHA256 digest algorithm is recommended.

You can use either of the following methods to create your private key:

- Using OpenSSL

  OpenSSL is a powerful and widely used security library tool. You can download the latest OpenSSL installation package from **http://www.openssl.org/source/**.

  **NOTE**

  The OpenSSL version must be 1.0.1g or later.

  After installing OpenSSL, run the **openssl genrsa -out** *myprivate.pem* **2048** command in the command-line interface (CLI).

  - *myprivate.pem* indicates your private key.
  - **2048** indicates the encryption length.
- Using Keytool

Keytool is a key management tool coming with JDK. You can use it to create a KEYSTORE (JKS) certificate file. Obtain Keytool by downloading a JDK package from **http://www.oracle.com/technetwork/java/javase/downloads/index.html**.

By default, the public key and private key created using Keytool cannot be exported. You need to export the private key from the created KEYSTORE file.

In the exported file, the following part is the private key:

```
-----BEGIN RSA PRIVATE KEY-----
......
-----END RSA PRIVATE KEY-----
```

or

```
-----BEGIN PRIVATE KEY-----
......
-----END PRIVATE KEY-----
```

**NOTICE**

No matter which method you use to generate a private key, you need to keep it properly because once it is lost or damaged the corresponding public key and digital certificate will be unusable.

## 1.1.5 What Are the Relationships Between a Public Key, Private Key, and Digital Certificate?

According to the principle of asymmetric cryptography, each certificate holder has a pair of public and private keys, which can be used to encrypt and decrypt each other.

The public key is public and does not need to be kept confidential. The private key is unique to the certificate holder and must be properly kept and kept confidential. A digital certificate is a digital file generated after the CA verifies the identity of a certificate applicant and signs the basic information and public key of the applicant with the root certificate of the CA (equivalent to stamping the official seal of the CA).

A digital certificate is a public key authenticated by the CA. Therefore, a digital certificate and a public key are both public.

A digital certificate is a public key authenticated by the CA. A private key is generated by the certificate holder locally or by a trusted third party. The certificate holder or a trusted third party can keep the private key.

If you select **System generated CSR** for **CSR** when applying for a certificate, the private key and certificate file are stored in the certificate folder after the certificate is issued. You can download the certificate to obtain the private key and certificate file.

If you select **Upload a CSR** for **CSR** when applying for a certificate, the downloaded certificate contains only one file named **server.pem** after the certificate is issued successfully. The file **server.pem** contains two segments of certificate code, that is, the server certificate and CA intermediate certificate. SCM does not store your private keys. Keep them safe.

# 1.1.6 Why Is a Non-Password-Protected Private Key Required?

When using your certificate, other services will require its private key from you. If the key is password-protected, the services will fail to use the certificate, which will cause certificate decryption failure and HTTPS failure. Therefore, you need to provide a private key that is not password protected.

When you generate a private key, remove its password protection before uploading the certificate.

## How Do I Remove Password Protection for a Private Key?

You can run the following command using OpenSSL to remove password protection for a protected private key:

**openssl rsa -in encryedprivate.key -out unencryed.key**

**encryedprivate.key** indicates the private key with password protection. **unencryed.key** indicates the private key with password protection removed. The extension name can be **.key** or **.pem**.

If your certificate uses a private key that is not password protected, the system checks the format of the certificate file when you deploy it on CDN. CDN requires that a certificate file must be encrypted using RSA. That is, the private key of the certificate starts with **-----BEGIN RSA PRIVATE KEY-----** and ends with **-----END RSA PRIVATE KEY-----**. If the certificate is not in this format, use a tool to convert the certificate format. For details, see **What Are Mainstream Formats of Digital Certificates?**

## How Do I Determine Whether a Private Key Is Password Protected?

Use the text editor to open a private key file. If the private key file is in the following format, then it is password protected:

- Password-protected private keys in PKCS#8 format
  ```
  -----BEGIN ENCRYPTED PRIVATE KEY-----
  ......BASE64 Private key content.....
  -----END ENCRYPTED PRIVATE KEY-----
  ```
- Password-protected private keys in OpenSSL ASN format
  ```
  -----BEGIN RSA PRIVATE KEY-----
  Proc-Type: 4,ENCRYPTED
  DEK-Info:DES-EDE3-CBC,4D5D1AF13367D726
  ......BASE64 Private key content.....
  -----END RSA PRIVATE KEY-----
  ```

**NOTE**

All keys generated using Keytool are protected by passwords. You can convert them into key files that are not password protected. For details, see **What Are Mainstream Formats of Digital Certificates?**

# 1.1.7 What Are Mainstream Formats of Digital Certificates?

Mainstream web service software uses a basic password library provided by OpenSSL or Java.

- Tomcat, WebLogic, and JBoss use the password library provided by Java. Java Keystore (JKS) certificate files are generated with the Keytool tool in the Java Development Kit (JDK) tool package.
- Apache and Nginx use the password library provided by OpenSSL to generate PEM, KEY, or CRT certificate files.
- IBM web service products, such as WebSphere and IBM HTTP Server (IHS), use the built-in iKeyman tool to generate KDB certificate files.
- The Internet Information Services (IIS) service of Microsoft Windows Server uses the built-in certificate library to generate PFX certificate files.

## Checking the Format of a Certificate File

- You can determine whether a certificate file is text or binary based on its name extension:
  - A DER or CER file is binary and contains only the certificate information.
  - A CRT file can be either binary or text. Most CRT files are text and have the same function as DER or CER files.
  - A PEM file is text typically and contains a certificate or private key or both. If a PEM file contains only a private key, it is usually replaced by a KEY file.
  - A PFX or P12 file is binary. Containing both a certificate and a private key, it is password protected typically.
- You can also use Notepad to open the certificate file. If strings of digits and letters are displayed in the file, the certificate file is in text format.

  Examples:

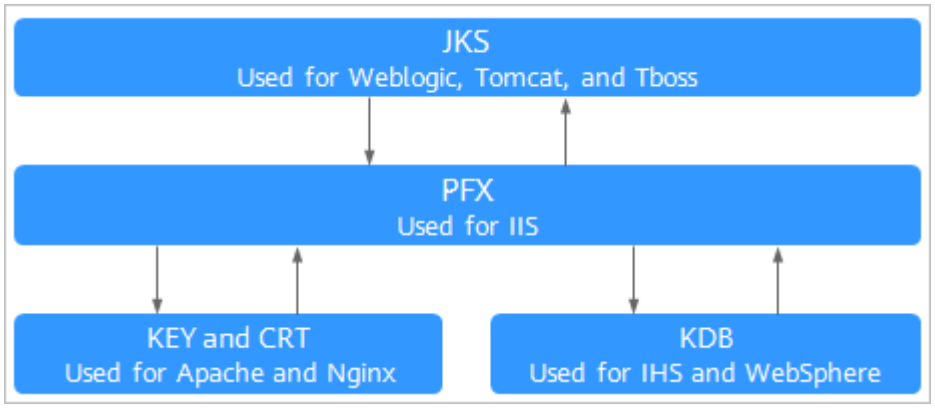
  ```
  —–BEGIN CERTIFICATE—–
  MIIE5zCCA8+gAwIBAgIQN+whYc2BgzAogau0dc3PtzANBgkqh.....
  —–END CERTIFICATE—–
  ```

  - If **--BEGIN CERTIFICATE--** is displayed, the file contains a certificate.
  - If **--BEGIN RSA PRIVATE KEY--** is displayed, the file contains a private key.

## Certificate Format Conversion

Certificate formats as listed in **Figure 1-1** can be converted mutually.

**Figure 1-1** Certificate Format Conversion



You can use the following methods to convert certificate formats:

- Converting from JKS into PFX

  You can use the built-in Keytool of JDK to convert a JKS certificate file into PFX.

  For example, you can run the following command to convert **server.jks** into **server.pfx**:

  **keytool -importkeystore -srckeystore D:\server.jks -destkeystore D:\server.pfx -srcstoretype JKS -deststoretype PKCS12**

- Converting from PFX into JKS

  You can use the built-in Keytool of JDK to convert a PFX certificate file into JKS.

  For example, you can run the following command to convert **server.pfx** into **server.jks**:

  **keytool -importkeystore -srckeystore D:\server.pfx -destkeystore D:\server.jks -srcstoretype PKCS12 -deststoretype JKS**

- Converting from PEM/KEY/CRT into PFX

  You can use the **OpenSSL** tool to convert a KEY key file and CRT public key file into a PFX certificate file.

  For example, copy the **server.key** key file and **server.crt** public key file to the OpenSSL tool installation directory and run the following command to convert the certificate into the **server.pfx** certificate file:

  **openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt**

- Converting from PFX into PEM/KEY/CRT

  You can use the **OpenSSL** tool to convert a PFX certificate file into a PEM certificate file, KEY key file, and CRT public key file.

  For example, copy your PFX certificate file to the OpenSSL tool installation directory, and use the OpenSSL tool to run the following command to convert it into the **server.pem** certificate file, **server.key** key file, and **server.crt** public key file:

  **openssl pkcs12 -in server.pfx -nodes -out server.pem**

  **openssl rsa -in server.pem -out server.key**

  **openssl x509 -in server.pem -out server.crt**

**NOTICE**

This conversion method is used only for scenarios where OpenSSL is used to generate private keys and CSRs for applying for certificate files. Using this method, you can separate the private keys when you have obtained PEM public keys. When deploying a digital certificate, use the private key separated with this method to match the public key certificate issued to you.

## 1.1.8 What Information Does an SSL Certificate Contain?

A certificate contains the following information after it is successfully issued and deployed:

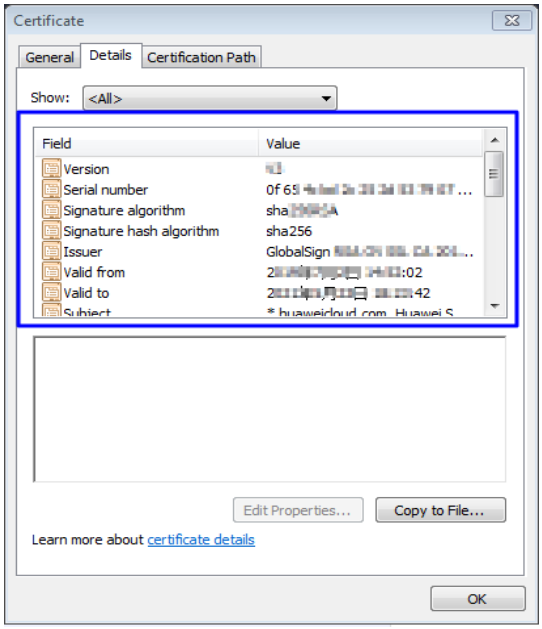
  

1. Address bar: security padlock, HTTPS flag, and enterprise name (only for EV certificates)
2. General: user, issuer, and validity period of a certificate
3. Details: certificate version, serial number, signature algorithm, encryption algorithm, public key, validity period, and user information (such as the province, city, enterprise name, and department)

NOTE

When applying for a certificate, enter the company contact or authorizing person information (contact name and mobile phone number). The information that involves personal information is not included in the certificate after the certificate is issued.

**Figure 1-2** Certificate details example




# 1.1.9 Can I Use SSL Certificates for Other Regions, Accounts, or Platforms?

## Can I Use an SSL Certificate for Other Regions?

Yes.

SCM is a global service. You can use your SSL certificates in all regions after you purchase them in a certain region.

## Can I Use an SSL Certificate for Different Accounts?

Yes.

After an SSL certificate is issued, it can be used under different account regardless whether it is purchased under the account.

- Example 1:

  The SSL certificate purchased under account A can be used on the servers under account B.

SSL certificates are associated with domain names. Therefore, the domain name you want to protect must be the same as the domain name bound to the certificate. Otherwise, a message will be reported indicating that the request is insecure.

### Can I Use an SSL Certificate for Other Platforms?

Yes.

SSL certificates purchased in SCM can be used on any platforms.

After an SSL certificate is issued, you can download the certificate file in SCM.

After you obtain the certificate file, deploy it on a server corresponding to your websites.

## 1.1.10 Can I Use an Unused SSL Certificate Anytime I Want?

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

If an additional domain name is added for a multi-domain certificate, the certificate validity period starts from the date when the certificate is issued for the first time.

Check whether the certificate is available.

- If you have purchased a certificate but have not applied for the certificate and the certificate has not been issued:

  The certificate can be used.

  The validity period of a certificate starts from the date when the certificate is issued. Therefore, you can use the certificate after applying for it.
- If you have purchased a certificate that has been issued and is still within the validity period:

  The certificate can be used within the validity period.
- If you have purchased a certificate and the certificate is issued, but it expires:

  The certificate cannot be used.

## 1.1.11 Can SSL Certificates Be Upgraded?

No.

After a certificate is issued, it cannot be upgraded. The certificate information, such as the domain name associated with the certificate, certificate validity period, and certificate authority, cannot be modified.

To associate a certificate with another domain name, change the certificate authority, or change the certificate validity period, apply for a new certificate.

## 1.1.12 Does the SSL Certificate Have Restrictions on the Server Port?

There is no limit. An SSL certificate is associated with a domain name and has nothing to do with the server port.

### 1.1.13 Why Is the Service Displayed as Inaccessible or the Button Displayed in Gray When I Access the SCM Service on the Console?

When you access SCM on the console and the service is displayed as inaccessible or the button displayed is in gray, perform the following operations:

In SCM, the system displays a message indicating that you do not have the permission to perform this operation regardless of whether your account has insufficient permissions or is in arrears.

- If you do not have the permission to perform this operation, contact the administrator to grant the permission. After the permission is granted, perform the corresponding operations.
- If your account is in arrears, top up your account. After your account is topped up, perform the corresponding operations.

## 1.2 SSL Certificate Application and Purchase

## 1.2.1 SSL Certificate Selection

### 1.2.1.1 Does SCM Provide Free Certificates?

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

### Notes on Using Free Certificates

- 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.

  **NOTICE**

  - Deleted certificates and revoked certificates are all counted towards the free certificate quota.
  - Your account and the IAM users created under your account share the quota of the 20 free certificates. For example, if an account has applied for 20 free certificates, no free certificate can be applied for by the account and the IAM users created using this account.
  - If your account has used up the quota of 20 free SSL certificates but you still want to apply for more free SSL certificates, purchase the DigiCert DV (basic) single-domain certificate package to increase your free certificate quota. For details, see **What Can I Do If My Free Certificate Quota Is Used Up?**

- 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.

- 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.
- A free certificate is valid for one year and cannot be renewed. After a free certificate expires, it cannot be used anymore. If you still need an SSL certificate, create one in CCM.

## 1.2.1.2 How Do I Select an SSL Certificate?

This topic describes all you want to know about how to select an SSL certificate that meets your business needs.

## Which Certificate Type Is Suitable for Me?

When you purchase SSL certificates, you can select **OV**, **OV Pro**, **EV**, **EV Pro**, or **DV (Basic)** for **Certificate Type**.

- EV certificates are recommended for finance and payment service businesses. For other enterprises, OV or higher-level certificates are recommended.
- For use on mobile devices or in interface invocation, OV or higher-level certificates are recommended.
- If you do not have a business license, you can apply for only basic DV certificates.

## Which Certificate Authorities Are Available?

The following table lists the CAs supported by SCM and the certificate types each CA provides.

**Promotion activities**

- Single domain names (using domain name www.a.com and root domain name a.com as an example)
- Wildcard domain name (using domain names *.a.com and *.a.b.com as an example)

## Which Domain Type Should I Select?

You need to confirm how many domains you want to protect. In SCM, options for **Domain Type** can be **Single domain**, **Multiple domains**, or **Wildcard**.

**Table 1-2** Domain Type

| Parameter | Description |
| --- | --- |
| Single domain | Only one common domain name can be associated.<br>If you have only one domain name, select **Single domain**. |

| Parameter | Description |
| --- | --- |
| Multiple domains | • Multiple domains can be added to a certificate. Multiple single domains can be set for domains. For example, you can use one multi-domain certificate to protect domains example.com, example.cn, and test.com.<br>• You need to configure the domain quantity based on the number of domains you need to protect with a single multi-domain certificate.<br>• The number of domain names ranges from 2 to 250. A maximum of 250 domain names can be protected with a certificate.<br>If you have multiple domain names, select **Multiple domains**. Purchase domain names of the required quantity on the purchase page. |
| Wildcard domain | • Only one wildcard domain name can be associated.<br>If all of your domain names are at the same level, select **Wildcard**. |

To purchase a wildcard-domain certificate, you need to pay attention to the domain name matching rules. **Table 1-3** are some examples.

**Table 1-3** Examples of wildcard-domain matching rules

| Domain name | Matched Domain Name | Unmatched Domain Name |
| --- | --- | --- |

**NOTICE**

- For wildcard-domain certificates, only those associated with root domain names support the domain names. For example:
- If the www subdomain is associated with a certificate, the certificate also protects the root domain. For example:
- Once your digital certificate is issued, the associated domain cannot be changed.

**Table 1-4** provides domain type selection examples.

**Table 1-4** Domain type selection examples

| Example Scenario | Example Domain Name | Domain Type Selection | Quantity Selected |
| --- | --- | --- | --- |
| You have only one domain. | | Single domain | Single-domain type. The value of **Quantity** is fixed at **1**. |
| | | Single domain | |
| | | Single domain | |
| You have multiple domains. | Two domains | Multiple domains | 2 |
| | Three domains | Multiple domains | 3 |
| | Four domains | Multiple domains | 4 |
| You have multiple domains at the same level. | | Wildcard domain | Wildcard domain type. The value of **Quantity** is fixed at **1**. |

## 1.2.1.3 How Can I Apply for a Free SSL Certificate?

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

## 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.

  **NOTICE**

  - Deleted certificates and revoked certificates are all counted towards the free certificate quota.
  - Your account and the IAM users created under your account share the quota of the 20 free certificates. For example, if an account has applied for 20 free certificates, no free certificate can be applied for by the account and the IAM users created using this account.
  - If your account has used up the quota of 20 free SSL certificates but you still want to apply for more free SSL certificates, purchase the DigiCert DV (basic) single-domain certificate package to increase your free certificate quota. For details, see **What Can I Do If My Free Certificate Quota Is Used Up?**

- 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.
- A free certificate is valid for one year and cannot be renewed. After a free certificate expires, it cannot be used anymore. If you still need an SSL certificate, create one in CCM.

## Step 1: Creating a Free Certificate (Method 1)

1. Log in to the **management console**.
2. In the upper left corner of the certificate list, click **Create Test Certificate**.

   The numbers displayed next to the **Create Test Certificate** button indicate the remaining quota and total quota of test certificates you can create. For example, if **13/20** is displayed, you can create 13 more test certificates and can create up to 20 test certificates.
3. Read and select **I have read and agree to the Cloud Certificate Manager Statement**. Then, click **OK**.
4. You can view the created free test certificate in the SSL certificate list.

   NOTE

   If the test certificate is not displayed in the certificate list, refresh the page.

## Step 1: Creating a Free Certificate (Method 2)

1. Log in to the **management console**.
2. In the upper right corner of the page, click **Buy Certificate** to go to the certificate purchase page.
3. On the certificate purchase page, set parameters.
   - **Domain Type**: Select **Single domain**.
   - **Certificate Type**: Select **DV (Basic)**.
   - **Certificate Authority**: Select **DigiCert**.
   - After you select a certificate type and CA, other parameters, such as **Domain Quantity**, **Validity Period**, and **Quantity**, are configured automatically.

   **Figure 1-3** Free certificate configuration
4. Click **Next**.
5. Confirm the order information and agree to the CCM statement by selecting **I have read and agree to the Cloud Certificate Manager Statement**. Click **Pay**.
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.

## Step 2: Submit a Certificate Application to the CA

After you create a test certificate, associate a domain name with the certificate, provide additional details, and then submit the application for approval.

1. Log in to the **management console**.
2. In the certificate list, locate the row that contains the free certificate, and click **Apply for Certificate** in the **Operation** column.
3. On the displayed page, enter the domain name and contact information.
   a. Enter the domain name information.

      **Table 1-5** 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.<br>Options:<br>• **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.<br>• **Upload a CSR**: You need to manually generate a CSR file and paste the content of the CSR file generated into the text box. | System generated CSR |
| Domain Name | The domain name for which the certificate is used<br>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 1-6** describes the parameters.

**Figure 1-4** Configuring authorization information

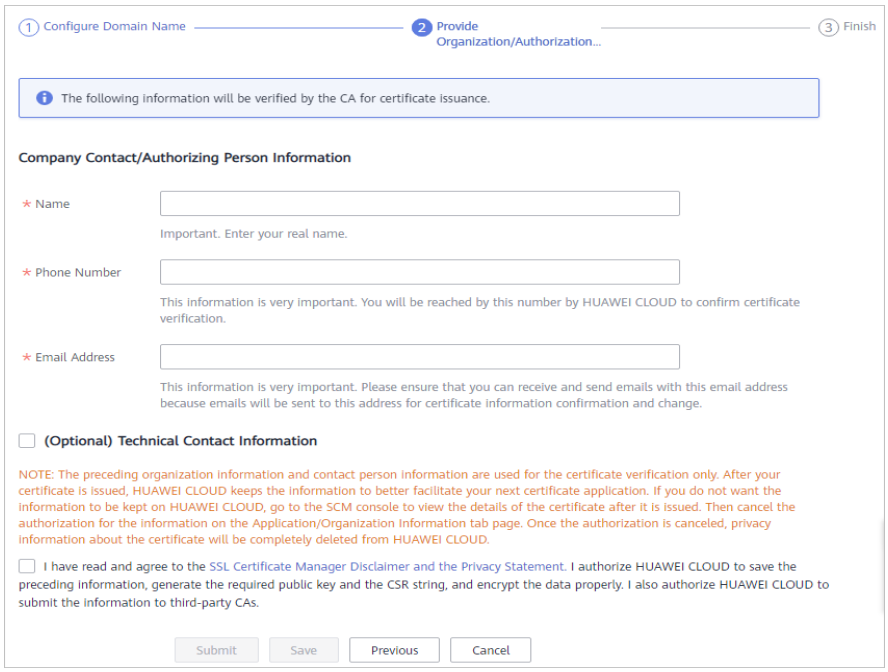



**Table 1-6** Parameter description

| Parameter | Description | Example Value |
| --- | --- | --- |
| Company Contact/ Authorizing Person Information | You only need to enter the name, phone number, and email address of the contact.<br>To get your certificate issued quickly, the phone number and email address entered must be valid. | None |
| (Optional) Technical Contact Information | The parameter is optional. You can skip it. | None |

4. Click **Submit**.

   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.

## 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 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.

- If you apply for a domain name on and the domain name has been resolved by 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.

NOTE

- After you submit the certificate application to a CA, complete the configuration of domain name verification based on the information displayed on the certificate list page, or your certificate will remain in the **Pending domain name verification** state and will fail the verification.
- After you complete the DNS verification on your side, it still takes a while for the CA to review your DNS verification results.

## Step 4: Issue the Certificate

After the domain name ownership is verified using DNS, it takes some time for the CA to approve your application. The CA will issue the certificate only after they validate your information.

The certificate takes effect immediately upon issuance. You can deploy the certificate to other cloud products 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.

## 1.2.1.4 What Can I Do If My Free Certificate Quota Is Used Up?

The following provides some methods to handle issues you may encounter when you apply for a free certificate:

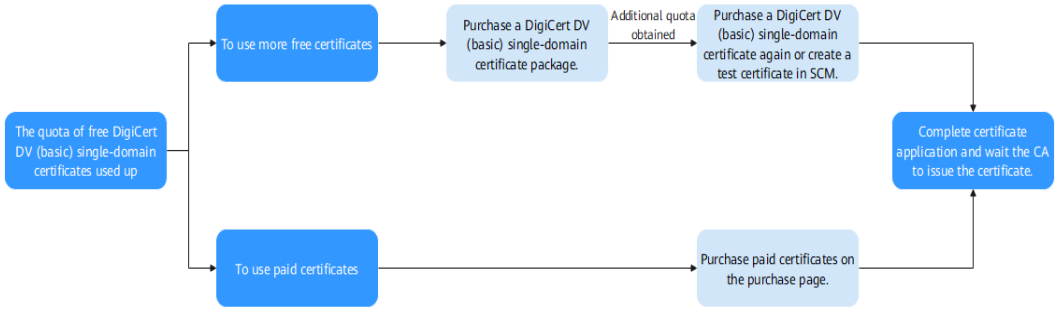
- The **Create Test Certificate** button on the CCM console is grayed out, and you cannot create a free DigiCert DV (Basic) certificate.
- When you purchase a DigiCert DV (Basic) single-domain certificate (free certificate) on the CCM console, a message is displayed indicating that the number of free certificates has reached the maximum and no more free certificates can be added.

## Free Certificate Quota

Each account has a quota of 20 free SSL certificates. If this quota is used up, follow the procedure shown in **Figure 1-5**. You can make your choice to meet your needs.

**Figure 1-5** Quota description




- If you still want to use more free certificates, you can purchase a DigiCert DV (basic) single-domain certificate package to increase the quota of DigiCert DV (basic) single-domain certificates.

  **Follow the procedure below to increase the quota.**
- If you want to use a paid certificate, buy one on the purchase page.

## Restrictions on Purchasing and Using a Single-domain Certificate Package

- The DigiCert DV (basic) single-domain certificate package is billed at an additional cost. This means if you have applied for the quota of 20 free certificates under your account for free, you will be billed for this package.
- You will receive the invoice with the amount equal to how much you pay when you purchase a DigiCert DV (basic) single-domain certificate package. No separate invoice will be issued for the free certificates you apply for using the DigiCert DV (basic) single-domain certificate package.
- Once purchased, the DigiCert DV (basic) single-domain certificate package cannot be refunded, returned, or replaced.

## Procedure

This procedure is intended for free certificates. For paid certificates, see .

**Step 1** Purchase a single-domain certificate package.

1. Log in to the **management console**.
2. On the certificate purchase page, specify parameters.
   - **Certificate Type**: Select **DV (Basic)**.
   - **Certificate Authority**: Select **DigiCert**.
   - **Domain Type**: Select **Single-domain certificate package**

   After you specify **Certificate Type**, **Certificate Authority**, and **Domain Type**, **Validity Period** and **Quantity** are automatically configured.

   **Figure 1-6** Certificate package

3. Click **Next**.
4. Confirm the order information and agree to the CCM statement by selecting **I have read and agree to the Cloud Certificate Manager Statement**. Click **Pay**.
5. On the displayed page, select a payment method.

**Step 2** Apply for a free certificate.

For details, see **How Can I Apply for a Free SSL Certificate?**

**----End**

## 1.2.1.5 How Do I Query the Remaining Quota for Free SSL Certificates?

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.

**NOTICE**

- Deleted certificates and revoked certificates are all counted towards the free certificate quota.
- Your account and the IAM users created under your account share the quota of the 20 free certificates. For example, if an account has applied for 20 free certificates, no free certificate can be applied for by the account and the IAM users created using this account.
- If your account has used up the quota of 20 free SSL certificates but you still want to apply for more free SSL certificates, purchase the DigiCert DV (basic) single-domain certificate package to increase your free certificate quota. For details, see **What Can I Do If My Free Certificate Quota Is Used Up?**

You can query the free SSL certificate quota usage in either of the following ways:

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

**Step 2** Hover the cursor over the **Create Test Certificate** button above the SSL certificate list and view your available free SSL certificate quota.

If the quota of 20 free certificates has been used up, click the **buy expansion package** link to purchase an expansion package. The package includes another 20 free certificates.

**----End**

## 1.2.1.6 How Do I Apply for an Entry-Level SSL Certificate?

This topic describes how to apply for an entry-level DV certificate.

In SCM, GeoTrust provides entry-level SSL certificates.

## Prerequisites

The account for purchasing a certificate has the SCM Administrator/SCM FullAccess and BSS Administrator permissions.

## Step 1: Buy a Certificate

1. Log in to the **management console**.
2. On the **Buy Certificate** page, set parameters as required. **Table 1-7** describes the parameters.

**Table 1-7** Parameters for purchasing a certificate

| Parameter | Description |
| --- | --- |
| Certificate Type | Certificate type<br>Select **DV (Basic)**. |
| Certificate Authority | Certificate authorities<br>Select **GeoTrust**. |
| Domain Type | Domain name type. You can select **Single domain** or **Wildcard** as needed.<br>• **Single domain**: You can associate only one domain with a certificate.<br>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**.<br>• **Wildcard**: You can associate only one wildcard domain with a certificate.<br>Only one wildcard character (*) can be contained in the wildcard domain, for example, ***.domain.com** or ***.example.domain.com**. ***.*.domain.com** is not supported.<br>For details about the domain names supported by wildcard-domain certificates, see **What Domains Can Wildcard-Domain Certificates Support?** |
| Domain Quantity | Quantity of selected domain quantity selected<br>You do not need to set this parameter. It is fixed at **1**. |
| Period of validity | Certificate validity period<br>Currently, the validity period of a certificate can be set to **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. You need to buy a new one after the certificate expires. |
| Quantity | Set the number of certificates. You can set the quantity as required. |

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

4. Confirm the order information and agree to the CCM statement by selecting **I have read and agree to the Cloud Certificate Manager Statement**. Click **Pay**.
5. 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: Submit a Certificate Application to the CA

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

**NOTICE**

In the **Domain Name Information** dialog box, select **DNS** for **Domain Name Verification Method**.

## Step 3: Verify Domain Ownership by DNS

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

After you submit the certificate application to a CA, 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 the verification.

## Step 4: Issue the Certificate

After the domain name ownership is verified using DNS, it takes some time for the CA to approve your application.

The CA will issue the certificate only after they validate your information. The certificate takes effect immediately upon issuance. You can deploy the certificate to other products or download the certificate and deploy it on a server.

## 1.2.1.7 What Are Differences Between Free and Paid SSL Certificates?

All SSL certificates can be used to create an encrypted channel for visitors to access websites through HTTPS. If a website is secured with an SSL certificate, a security padlock will be displayed on the browser when visitors access the website.

This topic describes the differences between free and paid SSL certificates.

**Table 1-8** Differences between free and paid SSL certificates

| Item | Free Certificate | Paid Certificate |
| --- | --- | --- |
| Security Level | General | High |

| Item | Free Certificate | Paid Certificate |
| --- | --- | --- |
| Compatibility with the certificate running environment | General | High |
| SSL certificate warranties from CAs | Not supported | Supported |
| Restrictions on certificate quantity | 20 free certificates for each account, including its IAM users | Unlimited |
| Types of website domain names that can be associated with | One single domain | Single domain, multiple domains, and wildcard domains |
| Supported certificate types | DV | DV, OV, and EV |
| Technical support | Not supported | Supported |
| Online Certificate Status Protocol (OCSP) | There is no local OCSP. So there might be network delay or timeout. | All paid certificates except DV (Basic) support OCSP acceleration access. |

Generally, free certificates are used only for personal websites or testing purposes. It is not recommended that you use free certificates for enterprise websites with mature services.

For enterprise websites, paid certificates are recommended. For governments, financial institutions, e-commerce platforms, and healthcare agencies, OV or EV certificates are recommended. These certificates make your website more trust while better protecting website data and identity authentication. For more details about paid certificate selection, see **How Do I Select an SSL Certificate?**

## 1.2.1.8 How Do I Apply for a Combination Certificate?

If you want to use a single certificate to protect multiple wildcard domains and common domains, buy a combination certificate by referring to the following operations.

For details about domain types, see **Domain-related Concepts**.

Before purchasing this certificate, you need to:

Confirm how many wildcard domains and common domains you will need to protect. You need to associate at least two domains to the certificate.

For details about the mapping between a domain name and a wildcard domain name, see **What Domains Can Wildcard-Domain Certificates Support?**

## Follow-up Operations

### 1.2.1.9 Can I Change the Certificate Authority, Type, or Bound Domain After A Certificate Is Purchased?

After you purchase a certificate in SCM, you cannot modify information such as the certificate authority, certificate type, bound domains, or validity period.

If you want to change the certificate authority or type, you need to purchase a new certificate.

### 1.2.1.10 Problems Related to Certificate Purchases

### What Are the Requirements for Enterprises to Purchase SSL Certificates?

Any enterprises can purchase SSL certificates on Huawei Cloud. You are allowed to purchase SSL certificates in the name of your branches.

### Does SCM Support Loading of DTLS Certificates?

Currently, SCM supports only SSL certificates.

### What Operations Should I Do After I Purchase a Certificate?

After you pay for the certificate order, submit a certificate application to the CA and complete domain name verification and organization verification. For details, see .

The basic process for applying for a certificate is as follows: Purchase a certificate > Submit a certificate application to the CA> Verify the domain ownership > Verify the organization > Issue the certificate. The CA will not issue the certificate until all of the submitted details have been reviewed.

### Why a Not Secure Warning Is Displayed in the Address Bar of My Browser?

If your website is not bound with an SSL certificate, a **Not Secure** warning will be displayed in the address bar, indicating that your connection with that page is insecure.

If you want to implement HTTPS for a website, you can purchase an SSL certificate and deploy it on the server corresponding to the website.

After an SSL certificate is deployed on a server, HTTPS is enabled on the server. The server uses HTTPS to establish encrypted links to the client, ensuring data transmission security.

After an SSL certificate is deployed, when a user accesses a website using HTTPS, the encryption lock icon is displayed in the address bar or on the right of the address bar, indicating that the website is encrypted. If the EV certificate is used, the company name can be directly displayed in the address bar.

## 1.2.1.11 How Do I Apply for an SSL Certificate That Uses SM Series Cryptographic Algorithms?

SCM provides OV SM2 SSL certificates issued by CFCA, TrustAsia, or vTrus.

## Prerequisites

The account for purchasing a certificate has the SCM Administrator/SCM FullAccess and BSS Administrator permissions.

## Procedure

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

**Step 2** On the certificate purchase page, set the parameters for purchasing an SM2 SSL certificate. **Table 1-9** describes the parameters.

**Table 1-9** Purchasing an SM2 SSL Certificate

| Parameter | Description |
| --- | --- |
| Service Type | Select **SSL certificate - domain name**. |
| Domain Type | Type of the domain name to be associated with the SSL certificate. The options are as follows:<br>• **Single domain**: An SSL certificate can be used for only one domain name, such as example.com.<br>• **Multi-domain**: An SSL certificate can be used for a maximum of 250 domain names.<br>• **Wildcard**: An SSL certificate can be used for only one wildcard domain name. For example, *.example.com (including a.example.com, b.example.com, ..., but excluding a.a.example.com). |
| Domain Quantity | If the **Domain Type** value is **Single domain** or **Wildcard**, you can only associate one domain name with a certificate. |
| Certificate Type | Select the **OV** certificate. |

| Parameter | Description |
| --- | --- |
| Certificate Authority | CAs that support the SM2 algorithm vary depending on the selected domain name type.<br>• CAs supported for single-domain certificates:<br>– CFCA<br>– TrustAsia<br>– vTrus<br>• CAs supported for multi-domain certificates:<br>– CFCA<br>– vTrus<br>• CAs supported for wildcard-domain certificates:<br>– CFCA<br>– TrustAsia<br>– vTrus |
| Validity Period | Select the certificate validity.<br>• **1 year**: A one-year SSL certificate.<br>• **2 years**: Two one-year SSL certificates. CCM uses the certificate information of the first certificate to automatically apply the second certificate 30 days before the first one expires.<br>• **3 years**: Three one-year SSL certificates. CCM will apply for the next certificate thirty days before the previous one expires using the information you provide when you apply for your first certificate. |
| Quantity | Select the number of certificates you want to purchase. You can purchase up to 100 certificate once. |

**Step 3** Confirm the product details and click **Next**.

If you have any questions about the pricing, click **Pricing details** in the lower left corner.

**Step 4** Confirm the order information and agree to the CCM statement by selecting **I have read and agree to the Cloud Certificate Manager Statement**. Click **Pay**.

**Step 5** 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 6** Submit the certificate application. For details, see .

NOTICE

The key algorithm must be set to **SM2**.

**Step 7** Verify the domain name ownership. For details, see .

**Step 8** Verify an organization. For details, see .

**Step 9** Issue the certificate.

It will take some time for the CA to review your information. The CA will issue the certificate only after they validate your information.

**----End**

## 1.2.2 About Required Domain Name Details

### 1.2.2.1 How Do I Enter a Domain Name for a Certificate When Applying for an SSL Certificate?

SSL certificates are associated with domains. When you purchase the certificate, you need to select a domain type based on site requirements.

To learn more about domain name, see **Domain-related Concepts**.

After you purchase a certificate, provide certificate details for approval on the SCM console to bind the domain name to the certificate. The first step for applying for a certificate is to enter a domain name and associate the domain name with the purchased certificate.

Enter the domain type as prompted by the SCM console based on the purchased certificate.

If the domain name associated with your DV certificate contains special words, such as edu, gov, bank, and live, the certificate may fail to pass the security review. In this case, select an OV or EV certificate. For details about known special words, see

**Table 1-10** describes the domain types. For more information, see the examples.

**Table 1-10** Domain Name

| Parameter | Description |
| --- | --- |
| Single domain | Only one common domain name can be associated.<br>When associating a domain name, you only need to associate a common domain name with a certificate. |

| Parameter | Description |
| --- | --- |
| Multiple domains | • You can associate multiple domain names with a certificate. The number of domain names that can be associated depends on how many domain names you purchase under a multi-domain certificate.<br>• When applying for a certificate, set one of the domain names to the primary domain name and configure the rest as additional domain names. Configure the settings based on site requirements.<br>For example, if you purchase three domain names, set one domain name as the primary domain name and the other two as additional domain names.<br>**NOTICE**<br>• A primary domain and additional domains can be equally protected. |
| Wildcard domain | Only one wildcard domain name can be associated.<br>When associating a domain name, you can associate a wildcard domain name, which includes an asterisk (*). |

Examples:

- Single-domain certificate

  If you purchase a single-domain certificate, only one common domain name can be associated.

  Example:

  Enter in the text box next to **Domain Name** when applying for a certificate.
- Multi-domain certificate

  If you purchase a multi-domain certificate, you can associate multiple domain names with the certificate. The number of domain names you can associate depends on the domain quantity you selected when purchasing the certificate.

  When applying for a certificate, set one of the domain names to the primary domain name and configure the rest as additional domain names. Configure the settings based on site requirements. You can add additional domain names in batches.

  **NOTICE**

  • A primary domain and additional domains can be equally protected.
- Wildcard-domain certificate

  If you purchase a wildcard-domain certificate, only one wildcard domain name can be associated.

## 1.2.2.2 What Are the Differences Between a Single-Domain Name, Multi-Domain Name, and Wildcard-Domain Name in SCM?

In SCM, options for **Domain Type** can be **Single domain**, **Multiple domains**, or **Wildcard**.

**Table 1-11** Domain Type

| Parameter | Description |
| --- | --- |
| Single domain | Only one common domain name can be associated.<br>If you have only one domain name, select **Single domain**. |
| Multiple domains | • Multiple domains can be added to a certificate. Multiple single domains can be set for domains. For example, you can use one multi-domain certificate to protect domains example.com, example.cn, and test.com.<br>• You need to configure the domain quantity based on the number of domains you need to protect with a single multi-domain certificate.<br>• The number of domain names ranges from 2 to 250. A maximum of 250 domain names can be protected with a certificate.<br>If you have multiple domain names, select **Multiple domains**. Purchase domain names of the required quantity on the purchase page. |
| Wildcard domain | • Only one wildcard domain name can be associated.<br>If all of your domain names are at the same level, select **Wildcard**. |

Before you purchase a wildcard-domain certificate, pay attention to the domain name matching rules. **Table 1-12** are some examples.

**Table 1-12** Examples of wildcard-domain matching rules

| Domain name | Matched Domain Name | Unmatched Domain Name |
| --- | --- | --- |

**NOTICE**

- For wildcard-domain certificates, only those associated with root domain names support the domain names. For example:
- If the www subdomain is associated with a certificate, the certificate also protects the root domain. For example:
- Once your digital certificate is issued, the associated domain cannot be changed.

Table 1-13 is given here for your reference.

**Table 1-13** Domain type selection examples

| Example Scenario | Example Domain Name | Domain Type Selection | Quantity Selected |
| --- | --- | --- | --- |
| You have only one domain. | | Single domain | Single-domain type. The value of **Quantity** is fixed at **1**. |
| | | Single domain | |
| | | Single domain | |
| You have multiple domains. | Two domains | Multiple domains | 2 |
| | Three domains | Multiple domains | 3 |
| | Four domains | Multiple domains | 4 |
| You have multiple domains at the same level. | | Wildcard domain | Wildcard domain type. The value of **Quantity** is fixed at **1**. |

## 1.2.2.3 What Is the Relationship Between a Domain Name and an SSL Certificate?

An SSL certificate is used to protect a website. To make an SSL certificate work, bind it to the domain name of the website you want to protect. To that end, you need to confirm the certificate type, certificate authority, domain name type, and domain name when you make a purchase.

## How Many Domain Names Can Be Protected with an SSL Certificate?

When you purchase a certificate, you will select domain type according to your business needs. The number of domain names that can be protected with a certificate varies depending on domain name type. For more details, see Table 1-14.

**Table 1-14** Number of domain names that can be protected with a certificate

| Certificate Types | Supported Domain Name Type | Number of Domain Names that Can Be Protected |
| --- | --- | --- |
| OV and OV Pro | Single domain | One |

| Certificate Types | Supported Domain Name Type | Number of Domain Names that Can Be Protected |
| --- | --- | --- |
| | Multiple domains | The number of domain names ranges from 2 to 250. A maximum of 250 domain names can be protected with a certificate. |
| | Wildcard domain | One<br>For details about the domain names supported by wildcard-domain certificates, see **What Domains Can Wildcard-Domain Certificates Support?** |
| EV and EV Pro | Single domain | One |
| | Multiple domains | The number of domain names ranges from 2 to 250. A maximum of 250 domain names can be protected with a certificate. |
| DV (Basic) - GeoTrust entry-level SSL certificates | Single domain | One |
| | Wildcard domain | One<br>For details about the domain names supported by wildcard-domain certificates, see **What Domains Can Wildcard-Domain Certificates Support?** |
| DV (Basic) - DigiCert free SSL certificate | Single domain | One |

## How Many SSL Certificates Can Be Used for a Domain Name?

There is no restriction. You can purchase multiple certificates for the same domain name. The certificates will take effect when you use them to applications or install them on servers.

A certificate is a one-off product. If the current certificate cannot meet your requirements or is about to expire, you can purchase a new certificate that matches the domain name type and use the new certificate to the target domain name.

## 1.2.2.4 What Domains Can Wildcard-Domain Certificates Support?

You can purchase wildcard-domain certificates in SCM to protect a single domain name of the server and all its subdomains of the same level. Wildcard domains are supported by OV, OV Pro, and Geo Trust entry-level DV (Basic) certificates.

If you have multiple subdomain names at the same level, you do not need to purchase and install certificates for each subdomain name when using a wildcard-domain certificate.

**NOTICE**

- For wildcard-domain certificates, only those associated with root domain names support the domain names. For example:
- Once your digital certificate is issued, the associated domain cannot be changed.

To purchase a wildcard-domain certificate, you need to pay attention to the domain name matching rules. Only subdomain names of the same level can be matched. For details about the domain name levels, see **Domain-related Concepts**.

**Table 1-15** provides matching examples.

**Table 1-15** Examples of wildcard-domain matching rules

| Domain name | Matched Domain Name | Unmatched Domain Name |
| --- | --- | --- |
| *.example.com | Domain names, such as abc.example.com, sport.example.com, and good.example.com | Domain names, such as mycard.good.example.com and mycalc.good.example.com |
| *.good.example.com | Domain names, such as mycard.good.example.com and mycalc.good.example.com | Domain names, such as abc.example.com, sport.example.com, and good.example.com |

## 1.2.2.5 What Domain Name Should I Use to Apply for an SSL Certificate?

This topic uses examples to describe what domain names should be used during certificate application.

Assume the following: your website is **www.domain.com**; it has a user login page, which is **http://www.domain.com/login.asp**; you want to apply for an SSL certificate to ensure the username and password security for your users against theft during data transmission; it has a user login information management page, which is **http://www.domain.com/oa/manage.asp**; you want to apply for an SSL certificate to ensure the security of confidential information on that page. In this case, you can use **www.domain.com** to apply for an SSL digital certificate to protect those pages.

If your website has large access traffic, you are advised to set an independent web server (HTTP server) for the pages that require SSL digital certificates and use an independent domain name to apply for an SSL certificate, for example, secure.domain.com or ssl.domain.com.

NOTICE

The domain name used together with **https://** must be the same as that used for applying for an SSL digital certificate; otherwise, the browser may display a warning indicating that the name on the certificate is invalid or inconsistent with the site name. Use a proper domain name to apply for an SSL certificate for your website based on your conditions.

## 1.2.2.6 Can I Change the Primary Domain Name Associated with a Certificate?

That depends on the situation.

- If the certificate has not been issued:

  Yes.

  Revoke the certificate application, associate a new primary domain name with the certificate, and submit the certificate application again.
- If the certificate has been issued:

  No.

  The primary domain name associated with the certificate cannot be changed. To change the primary domain name, purchase a new certificate.

## 1.2.2.7 Does the Relationship Between the Primary Domain Name and Additional Domain Name Have Any Impact on Domain Names?

If **Domain Type** is set to **Multiple domains**, you can associate one primary domain name and at least one additional domain names with the certificate when applying for a certificate. One additional domain name per line.

For example, if you purchase three domain names, set one domain name as the primary domain name and the other two as additional domain names.

NOTICE

- A primary domain and additional domains can be equally protected.

For more details, see **How Do I Enter a Domain Name for a Certificate When Applying for an SSL Certificate?**

## 1.2.2.8 How Do I Make a CSR File?

Before applying for a digital certificate, you must generate a private key and a certificate signing request (CSR). The CSR file is the source file for your public key certificate. It contains your server and company details and needs to be submitted to the CA for review.

> **NOTE**
>
> Select the **System generated CSR** option because manually generated certificates often include errors. For details about how to handle the failure in getting approved, see What Can I Do When a Message Indicating Approval Failure Due to Blank Main Domain Name Is Displayed?

A private key file will be generated when the CSR file is generated manually. Keep your private key stored safely.

The following describes how to generate a CSR file. You can select whichever method you prefer.

- **Generating a CSR File Using OpenSSL**

  If you need to enter Chinese characters, use Keytool to generate a CSR file.
- **Generating a CSR File Using Keytool**

> **NOTE**
>
> 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.

## Generating a CSR File Using OpenSSL

**Step 1** Install the **OpenSSL** tool.

**Step 2** Run the following command to generate a CSR file:

**openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout *myprivate.key* -out *mydomain.csr***

- **-new** specifies that a new CSR is generated.
- **-nodes** specifies that the private key file is not encrypted.
- **-sha256** specifies the digest algorithm.
- **-newkey rsa:2048** specifies the type and length of the private key.
- **-keyout** specifies that a private key file is generated. The file name can be customized.
- **-out** specifies that the name of the CSR file is generated. The name can be customized.

**Step 3** Generate a CSR file named **mydomain.csr**.

**Figure 1-7** Generating a CSR file

```
Generating a 2048 bit RSA private key
....+++
.....................................................................+++
writing new private key to 'myprivate.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:CN
State or Province Name (full name) []:ZheJiang
Locality Name (eg, city) [Default City]:HangZhou
Organization Name (eg, company) [Default Company Ltd]:HangZhou xxx Technologies,Inc.
Organizational Unit Name (eg, section) []:IT Dept.
Common Name (eg, your name or your server's hostname) []:www.example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

The information to be entered is as follows:

| Field | Description | Example Value |
| --- | --- | --- |
| Country Name | Two-letter code of the country where your company is located. For example, enter **CN** for China. | CN |
| State or Province Name | The name of the province or state where your company is located. | ZheJiang |
| Locality Name | The name of the city where your company is located. | HangZhou |
| Organization Name | The legal name of your company. | HangZhou xxx Technologies, Inc. |
| Organizational Unit Name | The department of your company that the applicant belongs to | IT Dept. |
| Common Name | The website domain name you are applying for an SSL certificate for.<br>**NOTE**<br>• For a certificate with multiple domain names, enter the primary domain name to be associated with the certificate.<br>• For a wildcard-domain certificate, enter the wildcard domain name. Example: *.example.com | www.example.com |

| Field | Description | Example Value |
| --- | --- | --- |
| Email Address | Email of an applicant.<br>The CSR file password does not need to be entered. Just press **Enter**. | - |
| A challenge password | CSR file password.<br>The CSR file password does not need to be entered. Just press **Enter**. | - |

NOTE

- Make sure that UTF8 encoding format is used for a Chinese character–based certificate with OpenSSL. In addition, enable the UTF8 support during OpenSSL compilation.
- 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.

After you enter information as prompted, the **myprivate.key** (private key file) and **mydomain.csr** (CSR) files are generated in the current directory.

**----End**

## Generating a CSR File Using Keytool

**Step 1** Install Keytool, which is typically included in the Java Development Kit (JDK) tool package.

**Step 2** Use Keytool to generate a Keystore certificate file.

NOTE

The Keystore file contains a key. For details about how to export the key, see **What Are Mainstream Formats of Digital Certificates?**

1. Run the following command to generate the **keystore** certificate file:

   **keytool -genkey -alias mycert -keyalg RSA -keysize 2048 -keystore ./mydomain.jks**

   - **-keyalg** specifies the key type, which must be **RSA**.
   - **-keysize** specifies the key length, which must be 2,048.
   - **-alias** specifies the certificate alias, which can be customized.
   - **-keystore** specifies the path for saving the certificate file. The certificate file name can be customized.

**Figure 1-8** Generating the **keystore** certificate file

```
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  www.example.com
What is the name of your organizational unit?
  [Unknown]:  IT Dept.
What is the name of your organization?
  [Unknown]:  HangZhou xxx Technologies,Inc.
What is the name of your City or Locality?
  [Unknown]:  HangZhou
What is the name of your State or Province?
  [Unknown]:  ZheJiang
What is the two-letter country code for this unit?
  [Unknown]:  CN
Is CN=www.example.com, OU=IT Dept., O="HangZhou xxx Technologies,Inc.", L=HangZhou, ST=Zhe
Jiang, C=CN correct?
  [no]:  Y

Enter key password for <mycert>
        (RETURN if same as keystore password):
```

2. Enter the certificate password and enter information described in the following table:

| Question | Description | Example Value |
| --- | --- | --- |
| What is your first and last name? | Domain name for which you are applying for a certificate.<br>**NOTE**<br>– For a certificate with multiple domain names, enter the primary domain name to be associated with the certificate.<br>– For a wildcard-domain certificate, enter the wildcard domain name. Example: *.example.com | www.example.com |
| What is the name of your organizational unit? | Name of the department that the applicant belongs to. | IT Dept |
| What is the name of your organization? | The name of the company to which the applicant belongs. | HangZhou xxx Technologies,Ltd |
| What is the name of your City or Locality? | The city where an applicant is located. | HangZhou |
| What is the name of your State or Province? | The state or province where an applicant is located. | ZheJiang |

| Question | Description | Example Value |
| --- | --- | --- |
| What is the two-letter country code for this unit? | The country where the applicant belongs. Use a two-character ISO country code. | CN |

After you enter the information, review the entered content for errors. If there are no errors, press **Y**.

3. Enter the key password as prompted. The password can be the same as the certificate password. If they are the same, press **Enter**.

**Step 3** Use the certificate file to generate a CSR.

1. Run the following command to generate a CSR file:

   **keytool -certreq -sigalg SHA256withRSA -alias mycert -keystore ./mydomain.jks -file ./mydomain.csr**

   - **-sigalg** specifies the digest algorithm, which is **SHA256withRSA**.
   - **alias** specifies the alias, which must be the same as the certificate alias in the keystore file in **-alias**.
   - **-keystore** specifies the certificate file.
   - **-file** specify the CSR file. The file name can be customized.

2. Enter the certificate password as prompted to generate the **mydomain.csr** file.

**----End**

## 1.2.2.9 What Are the Differences Between the CSR Generated by the System and the CSR Made by Yourself?

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.

When you apply for a certificate, you can set **CSR** to **System generated CSR** or **Upload a CSR**. If you select the latter, copy the file content to the text box. **Table 1-16** describes the differences between two methods to provide the CSR file.

**Table 1-16** Comparisons on CSR files generated by the system or made by yourself

| CSR | Description | Differences |
| --- | --- | --- |
| 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. | • If **System generated CSR** is selected, there are multiple formats available for download.<br>• After you download the certificate, you can directly install and deploy certificate because certificate file **server.jks** and password file **keystorePass.txt** are automatically generated for you. |
| **Upload a CSR** | You need to manually generate a CSR file and paste the content of the CSR file generated into the text box.<br>For details, see **How Do I Make a CSR File?** | • 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. Then you will need to purchase a new certificate.<br>• After you download the certificate, use the OpenSSL tool to convert certificate format from PEM to PFX to obtain the **server.pfx** file. Then use the Keytool tool to convert the certificate format from PFX to JKS to obtain certificate file **server.jks** and password file **keystorePass.txt**. Then you can install and deploy your certificate. |

**System generated CSR** is recommended, which can avoid certificate approval failures caused by incorrect CSR content.

## 1.2.2.10 Domain-related Concepts

- Wildcard domain

  A wildcard domain is a domain name that contains only one * and starts with *.

  For example, ***.a.com** is a correct wildcard domain name, but ***.*.a.com** is not.

NOTE

A wildcard domain name counts as one domain name. For details about the mapping between a domain name and a wildcard domain name, see **What Domains Can Wildcard-Domain Certificates Support?**

- Common domain name

  A common domain name is a specific domain name or a non-wildcard domain name.

  For example, **www.a.com** or **a.com** is a common domain name.

  The number of common domain names that can be associated depends on the number of domain names selected in your order.

  NOTE

  For example, **buy.example.com** counts as one domain name and **next.buy.example.com** would count as a separate domain name.

- Domain levels

  A domain name is composed of one or more domain levels separated by periods (.), for example, . The hierarchy of domains descends from the right to the left label in the name.

  A top-level domain is the highest level in the domain name hierarchy. A second-level domain is directly below a top-level domain. **Table 1-17** details the domain levels.

**Table 1-17** Domain Level

| Parameter | Description |
| --- | --- |
| Top-level domain | The highest level in the domain name hierarchy. All domain names include a top-level domain suffix. Top-level domains include generic top-level domains (such as .com, .net, and .org), international/regional top-level domains (such as .us, .cn, and .tk), and new generic top-level domains (such as .info and .biz). |
| Second-level domain | A second-level domain is directly below a top-level domain. For example, in **example.com**, **example** is the second-level domain. |
| Third-level domain | A third-level domain is directly below a second-level domain. For example, in **www.example.com**, **www** is the third-level domain. |
| You can add a new domain level to the left of the last level. | |

## 1.2.2.11 Problems Related to Domains

## Can I Associate a Chinese Domain with an SSL Certificate?

A Chinese domain name can only be associated with a certificate when it is encoded with **Punycode**.

## Does the Domain Name Need to Be Registered Before Being Associated with an SSL Certificate?

- During the certificate application, the domain name associated with the SSL certificate can be unlicensed. However, the domain name that is not licensed will be blocked. As a result, the domain name cannot be accessed. Therefore, you are advised to license the domain name immediately after the website is set up.
- An SSL certificate can be bound to a domain name that is registered by an individual (the website is owned by an individual and does not contain any information of enterprises and institutions) or enterprise (the website is owned by enterprise or company).

## Does SCM Provide Wildcard-Domain Certificates?

Yes.

SCM provides single-domain, multi-domain, and wildcard-domain certificates.

You can buy wildcard certificates, or wildcard-domain certificates, on SCM.

## What Are the Rules for a Wildcard Certificate to Match a Domain Name? Can a Wildcard Certificate Match Domain Names Across Domain Levels?

You can purchase wildcard certificates on SCM.

A wildcard domain is a domain name that contains only one * and starts with *.

For example, ***.a.com** is a correct wildcard domain name, but ***.*.a.com** is not.

To purchase a wildcard-domain certificate, you need to pay attention to the domain name matching rules. Only the subdomain names of the same level can be matched. **Table 1-18** provides the examples.

**Table 1-18** Examples of wildcard-domain matching rules

| Domain name | Matched Domain Name | Unmatched Domain Name |
| --- | --- | --- |

## Which Domain Names Can Be Associated with A Single-Domain Certificate?

In SCM, options for **Domain Type** can be **Single domain**, **Multiple domains**, or **Wildcard**.

A single-domain certificate can be associated with only one common domain name, for example, example.com and test.example.com.

Note that example.com does not contain subdomain names such as test.example.com. If all level-2 and level-3 domain names need to be supported, purchase a wildcard-domain certificate.

### Which Domain Names Can Be Protected with A Multi-Domain Certificate?

In SCM, options for **Domain Type** can be **Single domain**, **Multiple domains**, or **Wildcard**.

If you buy a multi-domain certificate, you can add multiple different domains, including multiple single domains. For example, you can use one multi-domain certificate to protect domains example.com, example.cn, and test.com.

You need to configure the domain quantity based on the number of domains you need to protect with a single multi-domain certificate.

The number of domain names ranges from 2 to 250. A maximum of 250 domain names can be protected with a certificate.

### Which Domain Names Can Be Protected with A Wildcard-Domain Certificate?

In SCM, options for **Domain Type** can be **Single domain**, **Multiple domains**, or **Wildcard**.

A wildcard-domain certificate can protect only one wildcard domain name.

- 

To purchase a wildcard-domain certificate, you need to pay attention to the domain name matching rules. Only the subdomain names of the same level can be matched. **Table 1-19** provides the examples.

**Table 1-19** Examples of wildcard-domain matching rules

| Domain name | Matched Domain Name | Unmatched Domain Name |
| --- | --- | --- |

**NOTICE**

- For wildcard-domain certificates, only those associated with root domain names support the domain names. For example:
- If the www subdomain is associated with a certificate, the certificate also protects the root domain. For example:
- Once your digital certificate is issued, the associated domain cannot be changed.

# 1.3 SSL Certificate Approval

## 1.3.1 How Long Does It Take to Approve an SSL Certificate?

The certificate approval time depends on how quickly you respond with requested information from the CA. Once you submit the certificate, the CA will contact you

through the email address and phone number. Please monitor the approval email inbox and make sure to click the link contained in the email sent from the Certificate Authority.

The approval period varies according to certificate types. The CA needs to confirm the submitted information before issuing a certificate. A certificate takes effect immediately upon issuance.

For approval period of different certificate types, see **Table 1-20**.

**Table 1-20** Certificate approval period

| Certificate Type | Approval Period |
| --- | --- |
| Extended Validation (EV) and EV Pro | The CA usually takes seven to ten **working days** to review your information |
| Organization Validation (OV) and OV Pro | The CA usually takes three to five **working days** to review your information. |
| DV (Basic) | Generally, a basic DV certificate can be issued within several hours. Domains of basic DV certificates are verified by the CA automatically.<br>Free certificates are included in certificates of this type. Generally, a basic DV certificate can be issued within several hours. Domains of basic DV certificates are verified by the CA automatically. |

It will take less time to issue the certificate if you respond with the requested information from the CA correctly and quickly. To shorten the certificate issuance time, ensure that:

- The submitted information is correct to avoid repeated modification.
- Answer calls from the CA or confirm emails from the CA in a timely manner.

**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.

## Related Questions

- Why Does the SSL Certificate Remain in the Pending Domain Name Verification State (Application Progress Is 40%) After Domain Name Verification Is Complete?
- How Do I Check Whether Domain Name Verification Takes Effect?
- What Can I Do If Domain Ownership Verification Does Not Take Effect?
- Why Does the Certificate Stay in the CA Verifying Status for a Long Time?

# 1.4 SSL Certificate Download, Installation, and Use

## 1.4.1 SSL Certificate Use

### 1.4.1.1 Which Region Will a Certificate Be Deployed to When I Deploy an SSL Certificate in CCM to Other Cloud Product?

Digital certificates purchased through SCM can be deployed to Web Application Firewall (WAF), Elastic Load Balance (ELB), and Content Delivery Network (CDN) in just a few clicks.

The certificate deployment regions vary depending on cloud products you select.

- When you deploy or update a certificate for ELB or WAF, you can select a region, and the certificate will be deployed to the region you select.
- If you deploy a certificate in CCM for CDN, there is no need to select a region, and the certificate is deployed to CDN.

If you have not purchased a given cloud product or the domain name associated with a certificate has not been added to the product, do not deploy the certificate on the product because the process may fail.

### 1.4.1.2 Is HTTPS Automatically Enabled After an SSL Certificate Is Deployed to a Cloud Product?

Yes.

After you use SCM to deploy the certificate to other cloud products, HTTPS encryption is automatically enabled. You do not need to configure other parameters.

### 1.4.1.3 Why Is a Message Indicating that the Certificate Chain Is Incomplete Displayed When I Configure HTTPS on CDN?

When an SSL certificate is used for HTTPS configuration on Content Delivery Network (CDN), if the HTTPS certificate fails to be configured and a message is displayed indicating that the certificate chain is incomplete, perform the following operations to locate and rectify the fault:

Check whether the certificate chain is complete, whether the certificate is added in the format as required, whether all certificates are typed, and whether the certificate sequence is correct.

Ensure that the content of the certificate chain is pasted right below the content of the server certificate.

If the certificate chain is incomplete, complete the certificate chain by referring to How Do I Fix an Incomplete SSL Certificate Chain?

If your SSL certificates were purchased through SCM, you can deploy them to CDN in just a few clicks. You do not have to make the certificate chain manually, and

you can stop worrying about such errors. Therefore, you are advised to purchase certificates in SCM.

# 1.5 Certificate Validity Period

## 1.5.1 What Can I Do If My SSL Certificate Expired?

SSL certificates have a validity period. Once a certificate expires, it cannot be used. Renewals are allowed only for valid certificates.

You can renew only paid SSL certificates you have purchased in SCM before they are about to expire.

To replace the certificate that is about to expire, manually install the new certificate on your server. A certificate application must be submitted to the CA when you purchase a new certificate or renew a certificate.

You can replace the old certificate with the new one once it is issued. The replacement does not affect services.

**NOTE**

- You are advised to purchase or renew an SSL certificate at least **3 to 10 working days** before the current one expires.
- After a certificate is renewed, the validity periods of the old and new certificates are described as follows:
  - Details of new certificate not changed

    If the certificate details remain unchanged, the actual validity period of the new certificate equals to the remaining validity period of the original one plus the requested validity period of the new one. A maximum of 30 days can be counted towards the validity period of the new certificate.

    For example, assume that your current certificate expires on October 1, 2019, and you request a new one-year SSL certificate with the same details from the same CA on August 31, 2019. If the new certificate is issued on Sept. 1, 2019, it will be valid from Sept. 1, 2019 to Sept. 30, 2020.

    This rule is formulated, interpreted, and clarified by the CA. If you have any questions, we will work with you to communicate and negotiate with the CA.
  - Information about the new certificate is modified during manual renewal. For example, the domain name, certificate type, or company name is different from that of the old certificate.

    The validity periods of the current and new certificates are calculated separately.

    The use of the new certificate does not affect the current certificate. The current certificate can continue to be used until it expires.

## 1.5.2 How Long Is an SSL Certificate Valid?

### When Does the Certificate Validity Period Start?

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

If an additional domain name is added for a multi-domain certificate, the certificate validity period starts from the date when the certificate is issued for the first time.

# 1.5.3 What Can I Do If an SSL Certificate Is About to Expire?

You can replace the old certificate with the new one once it is issued. The replacement does not affect services.

# 1.5.4 How Long Does an SSL Certificate Take Effect After Being Purchased?

After an SSL certificate is purchased, you need to apply for the certificate. The CA reviews the application submitted by the user and issues the certificate only after the application is approved.

A certificate takes effect immediately upon issuance.

An SSL certificate is valid for one year. Once an SSL certificate expires, it cannot be used. You need to manually renew the certificate or purchase another one 3 to 10 working days before it expires. Otherwise, the certificate may expire before the CA validates your verification and issues new certificate.

If an additional domain name is added for a multi-domain certificate, the certificate validity period starts from the date when the certificate is issued for the first time.

# 1.5.5 Validity Periods and Replacement of the Current and New SSL Certificates

## Validity Periods of Current and New SSL Certificates

After the certificate is renewed, the current certificate is still valid. The validity period and usage of the new certificate depend on whether certificate details have changed:

- Certificate details not changed

  If the certificate details remain unchanged, the actual validity period of the new certificate equals to the remaining validity period of the original one plus the requested validity period of the new one. A maximum of 30 days can be added to the validity period of the new certificate.

  For example, assume that your current certificate expires on October 1, 2019, and you request a new one-year SSL certificate with the same details from the same CA on August 31, 2019. If the new certificate is issued on Sept. 1, 2019, it will be valid from Sept. 1, 2019 to Sept. 30, 2020.

  This rule is formulated, interpreted, and clarified by the CAs. If you have any questions, we will work with you to communicate and negotiate with the CAs.

  In this case, the two certificates are considered as the same certificate and in use concurrently.

- Information about the new certificate is modified during manual renewal. For example, the domain name, certificate type, or company name is different from that of the old certificate.

  The validity periods of the current and new certificates are calculated separately.

  The use of the new certificate does not affect the current certificate. The current certificate can continue to be used until it expires.

### Does the Replacement of Old Certificates with New Ones Affect Services?

You can replace the old certificate with the new one once it is issued. The replacement does not affect services.

## 1.5.6 How Can I Renew an SSL Certificate?

After a new certificate is issued, you need to install it on the server to replace the current certificate that is about to expire or replace the certificate in the corresponding cloud product. For more details about certificate installation, see the following FAQs:

- For details about how to install an SSL certificate, see **Table 1-21**.

**Table 1-21** Example for installing an SSL certificate

| Server Type | Operation |
| --- | --- |
| Tomcat | |
| Nginx | |
| Apache | |
| IIS | |
| Weblogic | |
| Resin | |

## 1.5.7 Will Services Be Affected If an SSL Certificate Is Not Updated After It Expires?

If an SSL certificate expires and will not be used anymore, you do not need to purchase it again, and services are not affected.

In addition, if the SSL certificate expires and is not updated in a timely manner, an alarm indicating that the security certificate of the website has expired is displayed when a user accesses the website. Unauthorized users, such as hackers, can use expired SSL certificates to tamper with or steal information and data transmitted between the browser and server, affecting user data security.

If a browser user finds that the website server certificate expires, the user does not trust the website, which brings negative impact on the brand image of the enterprise. After the website server expires, users may choose to stop accessing the website to avoid personal loss.

## 1.5.8 Validity Periods of Private Certificates

### How Long Is the Validity Period of a Private Certificate?

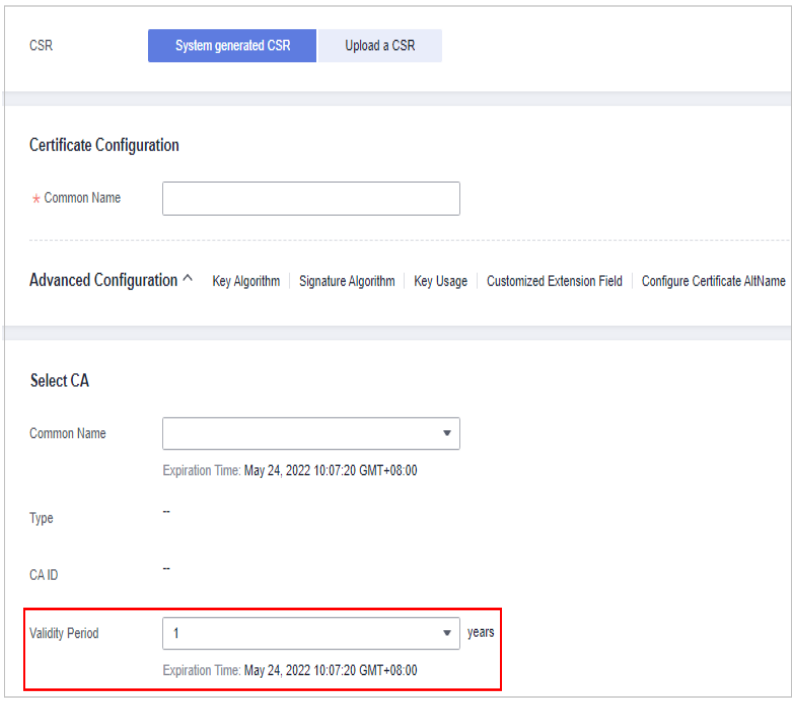
The validity period of a private certificate is set when it is applied for.

**NOTE**

A private certificate is issued by an activated private CA. Therefore, the validity period of a private certificate must be shorter than or equal to that of the private CA that issued it.

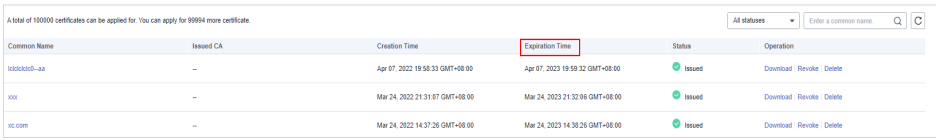
**Figure 1-9** Setting the validity period




A private certificate is issued by an activated CA.

After you applied for a private certificate, you can view its expiration time on the private certificate list page. If a private certificate expires, you need to apply for a new one.

**Figure 1-10** Viewing expiration time




## How Do I Prevent Service Interruptions When My Private Certificate Is About to Expire?

Rotate the certificate before it actually expires. Before the old certificate expires, replace it with the newly issued certificate.

# 1.5.9 How Long Will an Order Become Invalid If I Do Not Apply for a Certificate After Purchasing It?

Your order for SSL certificates never expires. You can apply for certificates in your orders anytime you want.

# 1.6 Certificate Management

## 1.6.1 Can I Discontinue a Private CA After It Issues A Private Certificate?

You can use either of the following methods to disable some functions of a private CA or discontinue a private CA:

- If you do not need to use a private CA to issue certificates but need to use it to revoke certificates or sign CRLs, you can disable the private CA. After a private CA is disabled, using of all certificates subordinated to the CA is not affected. For details, see Disabling a Private CA.

  **CAUTION**

  Disabled private CAs will also be billed.

- If you no longer need a private CA, delete it. When a private CA is deleted, the billing stops. The exported certificates (not revoked) can still be used. However, all certificates subordinated to the private CA cannot be revoked, and the CRL cannot be updated. All private certificates issued by the private CA or its subordinate CAs cannot be exported. For details, see Deleting a Private CA.

# A Change History

| Released On | Description |
| --- | --- |
| 2023-12-15 | This issue is the first official release. |