Cloud Certificate Manager

FAQs

Issue 16

Date 2021-12-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 FAQs on SCM

We sort out the most frequently asked questions on SSL certificate. The following lists related links for you to make a quick reference.

SSL certificate process: **SSL Certificate Purchase** > **SSL Certificate Application** > **Domain Ownership Verification** > **Organization Verification** > **SSL Certificate Issuance** > **SSL Certificate Installation and Usage**

SSL Certificate Purchase

- **Differences Between Certificate Types**
- **Certificate Selection and Application Process**
- **How Do I Apply for a Free Certificate?**
- **How Do I Apply for an Entry-Level SSL Certificate?**
- **Purchase a Certificate**

SSL Certificate Application

- **Apply for the Certificate**
- **How Do I Enter a Domain Name Associated with a Certificate When Applying for a Certificate?**
- **What Domain Name Should I Use to Apply for an SSL Certificate?**
- **How Do I Apply for a Combination Certificate?**
- **How Can I Provide the Organization Information as an Individual User During Certification Application?**
- **Do I Need to Upload the Bank Account Opening Permit and Business License When Applying for a Certificate?**
- **What Is the Relationship Between a Domain Name and a Certificate?**

Domain Ownership Verification

- **Verify the Domain Ownership**
- **How Do I Verify Domain Ownership by DNS?**
- **How Do I Verify Domain Ownership by File?**
- **How Do I Verify Domain Ownership by Email?**

- **How Do I Check Whether Domain Ownership Verification Takes Effect?**
- **What Can I Do If Domain Ownership Verification Does Not Take Effect?**

Organization Verification

- **Verify the Organization**
- **Why Does the Certificate Stay in the CA Verifying Status for a Long Time?**
- **How Do I Handle the Email or Phone Call from the CA?**
- **Do I Need to Get a Newly Purchased Certificate Approved?**

NOTE

- Organization verification is not required for DV and basic DV certificates. These certificates are issued upon the completion of domain ownership verification.
- 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.

SSL Certificate Issuance

After the organization verification completes, it takes some time for CA to complete the verification. For details about the review time, see **How Long Does It Take to Approve an SSL Certificate?**.

After the CA approves the certificate, it issues the certificate. The certificate takes effect upon issuance.

SSL Certificate Installation and Usage

- Using SSL certificates to other HUAWEI CLOUD services
  - **How Do I Configure a Non-HUAWEI CLOUD SSL Certificate for a HUAWEI CLOUD Service?**
  - **How Do I Apply an SSL Certificate to Other HUAWEI CLOUD Services?**
  - **Pushing Certificates to Other Services on HUAWEI CLOUD**
- Deploying SSL certificates on servers
  - **Download a Certificate**
  - **How Do I Install an SSL Certificate on a Server?**
  - **On Which Servers Can an SSL Certificate Be Deployed?**
  - **In Which Geographical Locations Can an SSL Certificate Be Used?**
  - **How Do I Add an SSL Certificate to the Background of a Website Built by BaoTa?**
  - **Will Consulting Services for Installing and Configuring SSL Certificates Be Provided?**
- Troubleshooting after SSL certificates are deployed
  - **Why Does the Website Still Display a Message Indicating that the Website Is Insecure After an SSL Certificate Is Deployed?**
  - **Why Cannot I Access a Website Using the Associated Domain Name After an SSL Certificate Is Deployed?**
  - **Why Does the HTTPS Access Speed Become Slower After an SSL Certificate Is Installed?**

2 Consulting

2.1 What Are the Differences Between SSL Certificate Management and Private Certificate Authority?

Definition

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

Private Certificate Authority (PCA) is a private certificate and CA management platform. It allows you 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 your organization.

Differences Between SCM and PCA

Table 2-1 describes the differences between SCM and PCA.

Table 2-1 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. • Authenticate websites and ensure that data is sent to the correct clients and servers. • Set up encrypted connections between clients and servers, preventing data from being stolen or tampered with during transmission.	• Authenticating websites Websites can be authenticated with SSL certificates. This effectively prevents the websites from being forged. • Authenticating applications Cloud and mobile applications can be authenticated with SSL certificates. For example, a wide range of cloud applications, such as CRM, OA, and ERP, can be authenticated to prevent unauthorized access. • Encrypting transmission of application data Data transmitted between websites/ applications and clients can be encrypted with SSL certificates. This effectively ensures data integrity and prevents data from being stolen or tampered with.	High	Not supported. SSL certificates can be used only for public domain names.

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. • Provides high-availability and high-security private CA hosting capabilities. • 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.	• Enterprise information digitalization A unified certificate management system is established to implement full-lifecycle certificate management. The system integrates with continuous monitoring and automation to prevent risks caused by improper certificate management. • IoV 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. • IoT 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	Low	Supported. Private certificates can be deployed on the intranet.

Service Name	Function	Application Scenario	Security Level	Apply to Internal Network
		access security in IoT scenarios.		

2.2 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.

2.3 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.

An SSL certificate is an SSL-compliant digital certificate issued by a trusted CA. 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.

For more details, see **Purchasing a Certificate**.

2.4 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

HUAWEI CLOUD 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.

2.5 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 in HUAWEI CLOUD SCM, 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. HUAWEI CLOUD SCM does not store your private keys. Keep them safe.

2.6 Why Is a Non-Password-Protected Private Key Required?

When using your certificate, other HUAWEI CLOUD products will require its private key from you. If the key is password-protected, the products 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 push it to 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?**

2.7 What Are Regions and AZs?

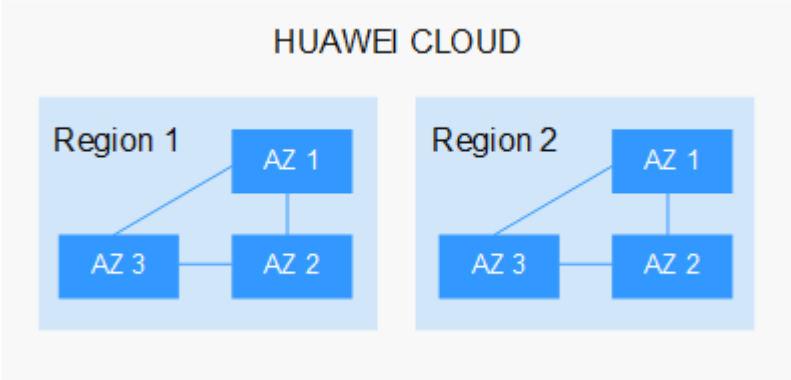
Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

Figure 2-1 shows the relationship between the regions and AZs.

Figure 2-1 Region and AZ



HUAWEI CLOUD provides services in many regions around the world. You can select a region and AZ as needed.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  You are advised to select a region close to you or your target users. This reduces network latency and improves access rate. However, Chinese mainland regions provide basically the same infrastructure, BGP network quality, as well as operations and configurations on resources. Therefore, if you or your target users are in the Chinese mainland, you do not need to consider the network latency differences when selecting a region.

  - If you or your target users are in the Asia Pacific region, except the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your target users are in Africa, select the **AF-Johannesburg** region.
  - If you or your target users are in Europe, select the **EU-Paris** region.
- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

2.8 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:

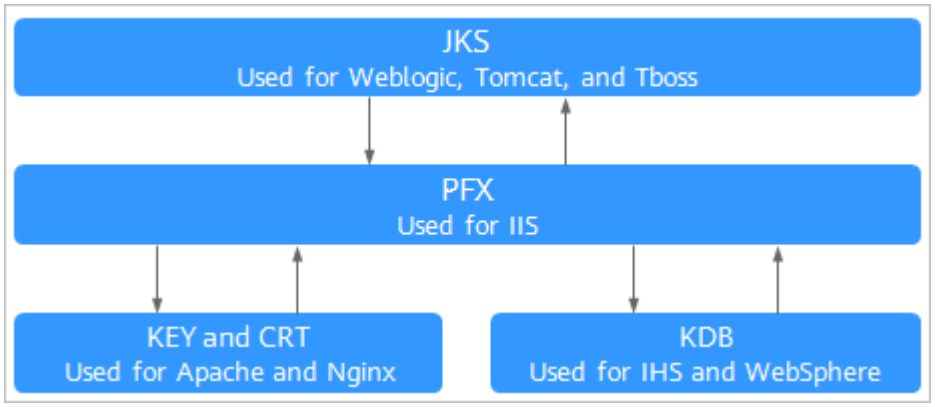
  ```
  —–BEGIN CERTIFICATE—–
  MIIE5zCCA8+gAwIBAgIQN+whYc2BgzAogau0dc3PtzANBgkqh.....
  —–END CERTIFICATE—–
  ```

  - 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 2-2** can be converted mutually.

Figure 2-2 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.

2.9 In Which Regions Are SCM Available?

SCM is a global service and is available in all regions.

SSL certificates are not issued by HUAWEI CLOUD. They are issued by trusted certificate authorities (CAs). Therefore, the use of an SSL certificate is not restricted by the region where it is purchased. After a certificate is purchased, it can be used globally.

2.10 What Information Does an SSL Certificate Contain?

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

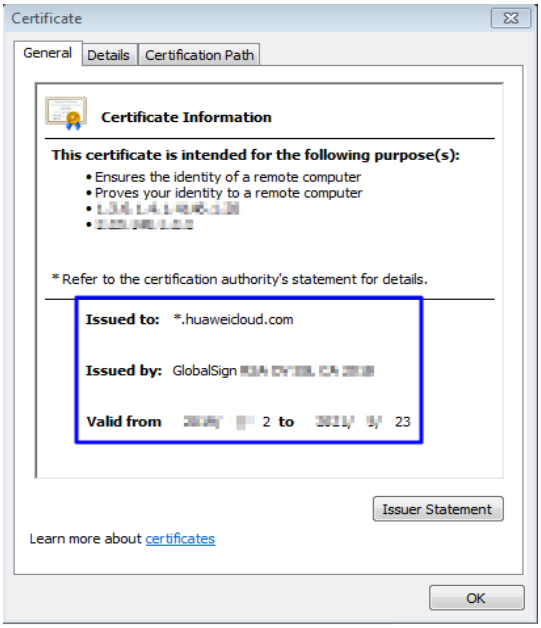
1. Address bar: security padlock, HTTPS flag, and enterprise name (only for EV certificates)

   Example: Display effect of an EV certificate on the Google Chrome browser

2. General: user, issuer, and validity period of a certificate

   Figure 2-3 Certificate general information example

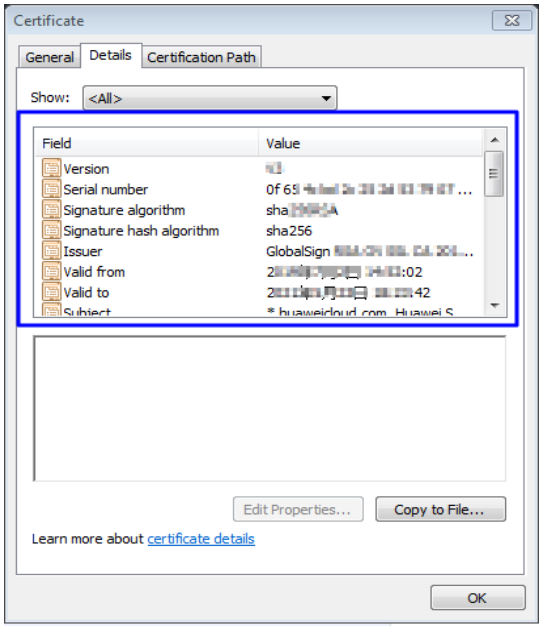
   

3. Details: certificate version, serial number, signature algorithm, encryption algorithm, public key, validity period, and user information (such as the province, city, enterprise name, and department)

   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 2-4 Certificate details example



2.11 Can SSL Certificates Be Used for Other Regions, Accounts, or Platforms?

Can SSL Certificates Be Used 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 SSL Certificates Be Used 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.

- Example 2:

  An SSL certificate under account A can be directly pushed to other cloud products, such as WAF, ELB, and CDN under account A.

  To use an SSL certificate under account A to the products under account B, download the certificate first.

  Then deploy it for products under account B.

Can SSL Certificates Be Used 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 or cloud products based on your needs.

The server can be a HUAWEI CLOUD server or a non-HUAWEI CLOUD server.

2.12 Can I Use a Purchased SSL Certificate That Has Not Been Used?

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. For details, see **Apply for an SSL Certificate**.
- 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.

2.13 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 another domain name, change the certificate authority, or extend the certificate validity period, apply for a new certificate.

2.14 Does the SSL Certificate Have Restrictions on the Server Port?

There is no limit. An SSL certificate is bound to a domain name or a pure IP address and has nothing to do with the server port.

2.15 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.

3 SSL Certificate Application and Purchase

3.1 SSL Certificate Selection

3.1.1 Does SCM Provide Free Certificates?

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

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

NOTICE

- 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.
  - Deleted certificates, revoked certificates, certificates that failed to be purchased due to overdue bills, and purchased certificates that are deleted without being applied for from CA 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.
- 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. To get technical support, you can purchase the HTTPS service in Marketplace on HUAWEI CLOUD website.

3.1.2 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.

For more details, see **Differences Between Certificate Types**

Which Certificate Type Is Suitable for Me?

When you purchase SSL certificates, you can select **OV**, **OV Pro**, **EV**, **EV Pro**, **DV**, 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?

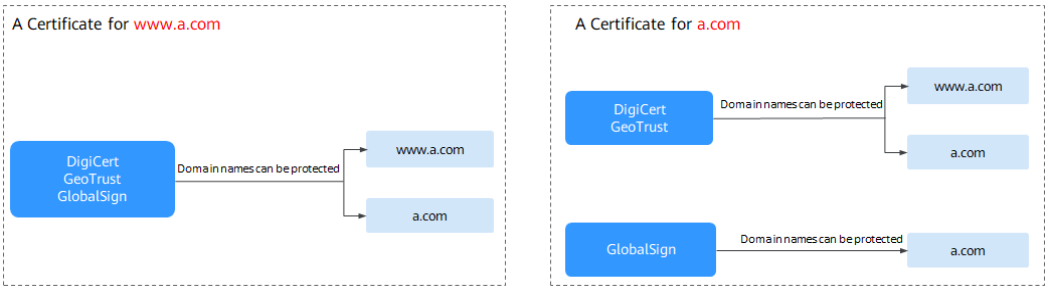
For details about CAs supported in SCM, see the following table.

Table 3-1 Certificate authorities

Certificate Authority	Description
DigiCert	DigiCert, formerly Symantec, is the world's largest CA. It provides services for more than 100,000 customers in over 150 countries and regions. Advantages: High security, stability, and compatibility. Suitable for digital transactions with high security requirements and widely used by financial institutions.
GeoTrust	GeoTrust, the world's second largest CA, is an industry-leading provider of identity and trust validation. It is committed to offering the best service at the lowest price possible to enterprises of all sizes. Advantages: Powered by DigiCert. High security, stability, and compatibility, cost-effective, and less know-how required for HTTPS protection
GlobalSign	Founded in 1996, GlobalSign is one of the world's earliest CAs. A trusted CA of SSL digital certificates, they have partnered with many companies around the word. Advantages: Fast issuance and verification Widely used by large e-commerce enterprises (including HUAWEI CLOUD), supported standard RSA+ECC algorithms, less resource required for installation

Promotion activities (using domain name www.a.com and root domain name a.com as an example)

Figure 3-1 Promotion activities



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 3-2 Domain Type

Parameter	Description
Single domain	Only one common domain name can be associated. 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. If the **Certificate Type** is set to **OV** or **OV Pro**, multiple single domains and multiple wildcard (*) domains can be added to one certificate. For example, if you purchase a multi-domain certificate (the number of domain names is three), you can use the 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. • Different promotion activities are offered by CAs for subdomain names, or www domain names. For details, see **Which Certificate Authorities Are Available?**. The following uses subdomain name www.a.com and root domain name a.com as an example to show the differences. – For DigiCert and GeoTrust certificates, you can purchase a certificate for either the root domain or the subdomain to protect both domains at the same time. For example, if you plan to purchase a multi-domain certificate issued by DigiCert or GeoTrust and expect to use this certificate to protect www.a.com and a.com, just bind www.a.com or a.com to the certificate. – For GlobalSign certificates, you can purchase a certificate for the subdomain and use the certificate to protect the corresponding root domain at the same time. However, a certificate for a root domain cannot protect the corresponding subdomain. For example, if you plan to purchase a multi-domain certificate issued by GlobalSign and expect to use the certificate to protect both www.a.com and a.com, just bind domain www.a.com to the certificate. • The number of domain names ranges from 2 to 250. A maximum of 250 domain names can be protected with a certificate. The following conditions must be met: – The number of primary domains is fixed at **1**. – The number of additional single domain names cannot be smaller than 1. If you select an OV or OV Pro certificate, the number of additional single domain names plus the number of additional wildcard domain names must be greater than or equal to 1. If you have multiple domain names, select **Multiple domains**. Purchase domain names of the required quantity on the purchase page.

Parameter	Description
Wildcard domain	• Only one wildcard domain name can be associated. • A wildcard domain name is the one that starts with a wildcard (*), for example, *.huaweicloud.com or *.example.huaweicloud.com. • Only the same-level domain matching is supported. For example, a certificate associated with *.huaweicloud.com can protect p1.huaweicloud.com but not p2.p1.huaweicloud.com. If you need to protect p2.p1.huaweicloud.com, purchase a wildcard-domain certificate associated with *.p1.huaweicloud.com. For details about more level matching rules, see **Table 3-3**. If all of your domain names are at the same level, select **Wildcard**.

NOTE

If you want to use one SSL certificate to protect more than one wildcard domain name and more than one common domain name, you can purchase a multi-domain OV or OV Pro certificate. For more details, see **How Do I Apply for a Combination Certificate?**.

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

Table 3-3 Examples of wildcard-domain matching rules

Domain name	Matched Domain Name	Unmatched Domain Name
*.huaweicloud.com	test.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names	abc.test.huaweicloud.com, yun.test.huaweicloud.com, example.test.huaweicloud.com, and other domain names
*.test.huaweicloud.com	abc.test.huaweicloud.com, yun.test.huaweicloud.com, example.test.huaweicloud.com, and other domain names	abc.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names

NOTICE

- For wildcard-domain certificates, only those associated with root domain names support the domain names. For example:
  - A certificate associated with the wildcard domain *.huaweicloud.com (a root domain) protects huaweicloud.com and other domain names of the same level. No additional certificate needs to be purchased for this.
  - A certificate associated with the wildcard domain *.p1.huaweicloud.com (not a root domain) will not protect p1.huaweicloud.com (a different level domain). It can only protect domain names of the same level. To protect p1.huaweicloud.com, you would need to purchase a new certificate.
- If the www subdomain is associated with a certificate, the certificate also protects the root domain. For example:

  A certificate purchased for domain www.huaweicloud.com can also protect huaweicloud.com. There is no need to purchase another certificate.
- Once your digital certificate is issued, the associated domain cannot be changed.

Table 3-4 provides domain type selection examples.

Table 3-4 Domain type selection examples

Example Scenario	Example Domain Name	Domain Type Selection	Quantity Selected
You have only one domain.	huaweicloud.com	Single domain	Single-domain type. The value of **Quantity** is fixed at **1**.
	test.huaweicloud.com	Single domain	
	p1.test.huaweicloud.com	Single domain	
You have multiple domains.	Two domains huaweicloud.com and p1.huawei.com	Multiple domains	2
	Three domains huaweicloud.com, p1.huawei.com, and p1.test.huaweicloud.cn	Multiple domains	3
	Four domains huaweicloud.com, test.huaweicloud.cn, p1.test.huaweicloud.cn, and p1.test.yun.huaweicloud.com	Multiple domains	4

Example Scenario	Example Domain Name	Domain Type Selection	Quantity Selected
You have multiple domains at the same level.	test.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names are the same level and are part of *.huaweicloud.com.	Wildcard domain	Wildcard domain type. The value of **Quantity** is fixed at **1**.

3.1.3 How Can I Apply for a Free SSL Certificate?

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

Prerequisites

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

Constraints

- You can apply for a maximum of 20 free SSL certificates under each account. In SCM, only one free certificate can be applied for at a time.

  NOTICE

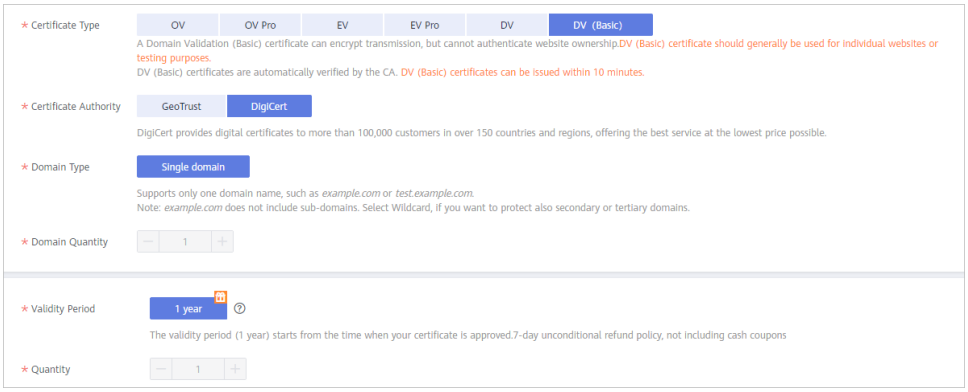
  - Deleted certificates, revoked certificates, certificates that failed to be purchased due to overdue bills, and purchased certificates that are deleted without being applied for from CA are all counted towards the free certificate quota.
  - Your account and the IAM users created under your account 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.

- One free SSL certificate can be used for only one single domain name.
- Free certificates cannot be used to protect IP addresses or wildcard domain names.
- By default, DNS verification is used to verify the domain ownership of a free certificate.
- The trust and security level of free certificates are low. They are recommended only for testing.
- For DigiCert DV (Basic) free certificates, no free technical support or installation guide is provided. To get technical support, you can purchase the HTTPS service in Marketplace on HUAWEI CLOUD website.

Step 1: Buy a Certificate

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

   Figure 3-2 Free certificate configuration



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

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

Step 2: Apply for the Certificate from the CA

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

1. Log in to the **management console**.
2. Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.
3. In the navigation pane on the left, choose **SSL Certificate Manager**. The **SSL Certificate Manager** page is displayed.

4. In the certificate list, locate the row that contains the free certificate, and click **Apply for Certificate** in the **Operation** column.
5. On the displayed page, enter the domain name and contact information.
   a. Enter the domain name information. **Table 3-5** describes the parameters.

Figure 3-3 Domain name configuration

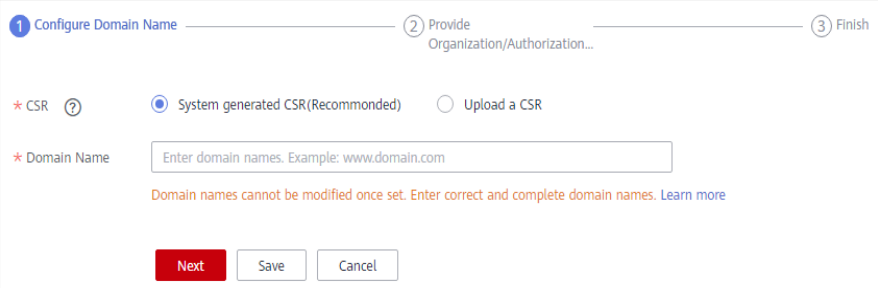


Table 3-5 Domain name parameters

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. Options: • **System generated CSR**: The system automatically generates a certificate private key. Once the certificate is issued, you can download your certificate and private key on the certificate management page. • **Upload a CSR**: You need to manually generate a CSR file and paste the content of the CSR file generated into the text box. For more details, see **How Do I Make a CSR File?**	System generated CSR

Parameter	Description	Example Value
Domain Name	The domain name for which the certificate is used Example: If your domain is *www.domain.com*, enter ***www.domain.com*** for **Domain Name**. If you need to bind a Chinese domain name, use encoding tool **Punycode** to encode the Chinese domain name and then enter the encoded data. For example, if the encoded data is **xn--siq1ht8k.com**, set this parameter to **xn--siq1ht8k.com**.	www.domain.com

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

c. Enter the company contact information. **Table 3-6** describes the parameters.

Figure 3-4 Configuring authorization information

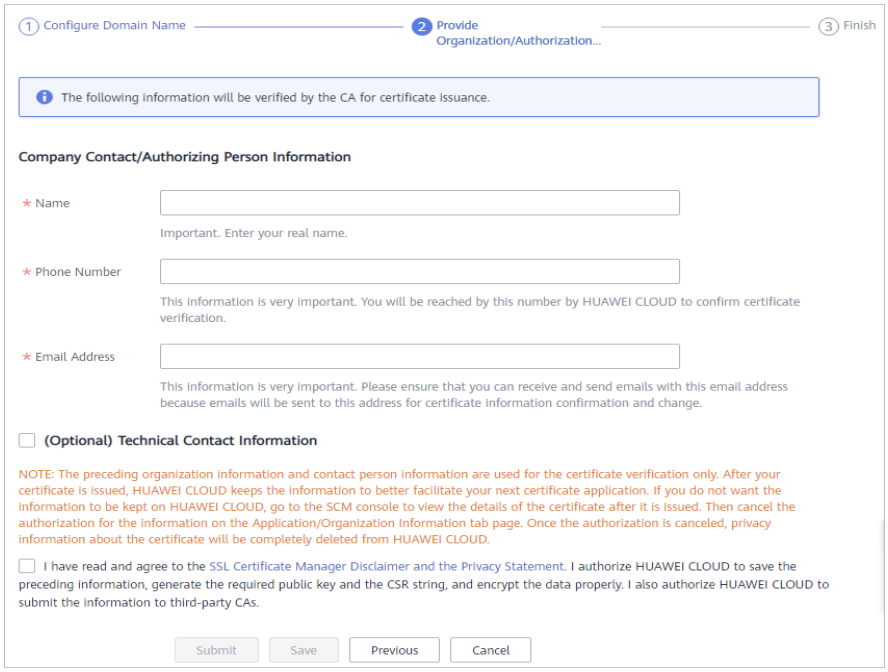


Table 3-6 Parameter description

Parameter	Description	Example Value
Company Contact/ Authorizing Person Information	You only need to enter the name, phone number, and email address of the contact. 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

6. After confirming that the entered information is correct, read through the *SSL Certificate Manager Disclaimer*, *Privacy Statement*, and the authorization statement, and check the box to agree to the disclaimer and statements
7. 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 TXT DNS record for your domain name on the platform. For example, if you purchase a domain name from company A, you need to add a TXT DNS record for your domain name on the domain name management platform of company A. For details about how to verify domain name ownership by DNS, see **Verifying Domain Ownership by Resolving the DNS TXT Record**.

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

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

NOTE

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

Step 4: Issue the Certificate

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

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

NOTE

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

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

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

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

In HUAWEI CLOUD SCM, GeoTrust provides entry-level SSL certificates.

Prerequisites

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

Step 1: Buy a Certificate

1. Log in to the **management console**.
2. Click  in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.
3. In the navigation pane on the left, choose **SSL Certificate Manager**. In the upper right corner of the page, click **Buy Certificate**.
4. On the **Buy Certificate** page, set parameters as required. **Table 3-7** describes the parameters.

Table 3-7 Parameters for purchasing a certificate

Parameter	Description
Certificate Type	Certificate type Select **DV (Basic)**.
Certificate Authority	Certificate authorities Select **GeoTrust**.
Domain Type	Domain name type. You can select **Single domain** or **Wildcard** as needed. • **Single domain**: You can associate only one domain with a certificate. The domain can be a second-level domain like **domain.com** or a third-level domain like **example.domain.com**. Any subdomains of the domain cannot be protected. For example, if you associate **domain.com** with a certificate, the certificate does not protect any subdomains, such as **ssl.domain.com** or **ssl.ssl.domain.com**. • **Wildcard**: You can associate only one wildcard domain with a certificate. Only one wildcard character (*) can be contained in the wildcard domain, for example, ***.domain.com** or ***.example.domain.com**. ***.*.domain.com** is not supported. 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 You do not need to set this parameter. It is fixed at **1**.
Period of validity	Certificate validity period 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.

5. Click **Next**.

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

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

7. On the displayed page, select a payment method.

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

Step 2: Apply for the Certificate from the CA

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

For details, see **Applying for a Certificate**.

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

For more details, see **How Do I Verify Domain Ownership by DNS?**

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

3.1.5 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 3-8 Differences between free and paid SSL certificates

Item	Free Certificate	Paid Certificate
Security Level	General	High
Compatibility with the certificate running environment	General	High

Item	Free Certificate	Paid Certificate
SSL certificate warranties from CAs	Not supported	Supported
Restrictions on certificate quantity	A maximum of 20 certificates for each calendar year	Unlimited
Types of website domain names that can be associated with	One single domain	Single domain, multiple domains, and wildcard domains
Associating a certificate with an IP address	Not supported	Supported by OV certificates issued by GlobalSign
Supported certificate types	DV	DV, OV, and EV
Technical support	Not supported	Supported

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?**

3.1.6 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.

Only multi-domain OV and OV Pro SSL certificates allow you to associate single domains and wildcard domain names.

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?**

Procedure

As an example, the following procedure shows how to associate two common domains and two wildcard domains to a certificate.

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

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

Step 3 In the navigation pane on the left, choose **SSL Certificate Manager**. In the upper right corner of the page, click **Buy Certificate**.

Step 4 Specify **Certificate Type**, **Certificate Authority**, **Domain Type**, **Domain Quantity**, and **Validity Period**.

Figure 3-5 Specifying details

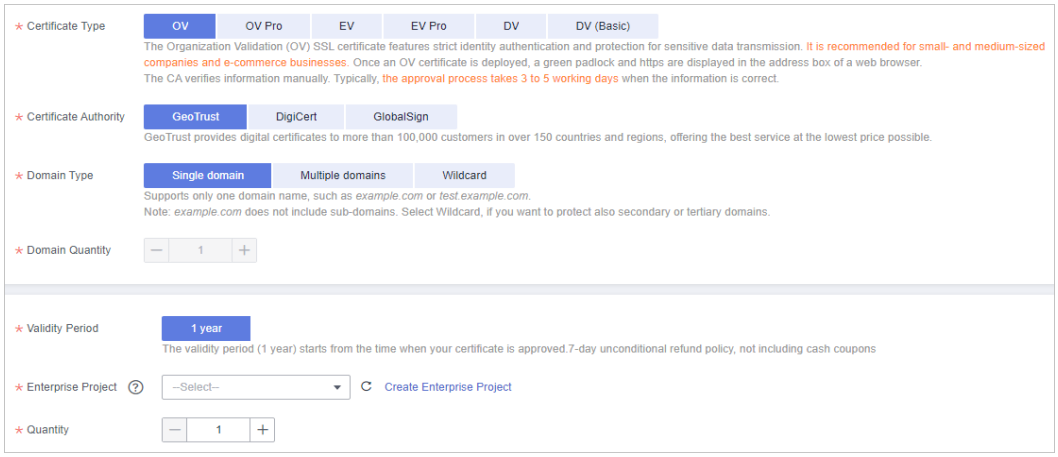


Table 3-9 Purchasing SSL certificates

Parameter	Description
Certificate	OV and OV Pro SSL certificates can be bound to mixed domain names. Select the required certificate type: • **OV**: Suitable for small- and medium-sized companies and e-commerce businesses • **OV Pro**: Suitable for small- and medium-sized enterprises that have high requirements on data security
Certificate Authority	You can only select a CA that can issue the certificate you need. • OV certificates can be issued by **DigiCert**, **GlobalSign**, or **GeoTrust**. • OV Pro certificates can be issued only by **DigiCert**.
Domain Type	Type of the domain name to be bound to the SSL certificate. Select **Multiple domains**.
Domain Quantity	Quantity of domain names based on your needs. By default, there is only one primary domain. You need to configure the numbers of additional single domains and additional wildcard domains.

Parameter	Description
Validity Period	Currently, the validity period of a certificate can be set to **1 year**.
Quantity	Number of required certificates contained in this order

Step 5 Click **Next**.

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

Step 6 Confirm the order information and agree to the SCM disclaimer by selecting **I have read and agree to the SSL Certificate Manager Disclaimer**. Click **Pay**.

Step 7 On the displayed page, select a payment method.

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

----End

Follow-up Operations

After you buy a certificate, get it issued. To do so, **apply for the certificate**, **verify the domain ownership**, and **verify the organization**.

3.1.7 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. For more details, see **Purchasing a Certificate**.

3.1.8 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 CFCA Certificates?

If you need to use this certificate, click **Service Tickets** > **Create Service Ticket** in the upper right corner of the management console and submit a service ticket to apply for the certificate. Currently, the CFCA certificates cannot be purchased on the SCM console.

Is Real-Name Verification Required to Purchase an SSL Certificate?

Yes.

If your real-name has not been verified, you cannot complete the payment when purchasing a certificate on HUAWEI CLOUD.

Is There a Location or Region Restriction When I Purchase an SSL Certificate?

There are no location or region restrictions on SSL certificate purchases.

SCM is a global service. You can use your SSL certificates in any regions. The region they were purchased in is not relevant.

The server region you selected during the purchase has no impact on the use of your SSL certificate.

Are SSL Certificates Necessary for My Website or Must I Purchase Them on HUAWEI CLOUD?

If you need to access websites through HTTPS or manage your certificates using HUAWEI CLOUD SCM, you need to purchase certificates on HUAWEI CLOUD.

You can also purchase certificates from other vendors, but we recommend HUAWEI CLOUD SCM for improved services.

If you already have a certificate, you can upload it to HUAWEI CLOUD SCM so that you can manage your certificates on one platform.

Does SCM Support Loading of DTLS Certificates?

Currently, SCM supports only SSL certificates.

What Are Special Rewards for Purchasing Certificates on SCM?

There are different discounts available depending on how long you need the certificated for. You can view the pricing on the **SCM** homepage or on the **Pricing Details** page.

What Operations Should I Do After I Purchase a Certificate?

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

The basic process for applying for a certificate is as follows: Purchase a certificate > Apply for the certificate > 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.

For details, see **Certificate Purchase and Application Procedure**.

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.

An SSL certificate is an SSL-compliant digital certificate issued by a trusted CA. 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.

For more details, see **Purchasing a Certificate**.

Why Does the Number of Certificates Reach the Upper Limit?

If the number of certificates you can purchase has reached the upper limit, you cannot add more certificates. This means the free certificate quota for your account has been used up. In this situation, we recommended paid SSL certificates.

NOTICE

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.

- Deleted certificates, revoked certificates, certificates that failed to be purchased due to overdue bills, and purchased certificates that are deleted without being applied for from CA 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.

3.2 Domain Name Filling - SCM

3.2.1 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.

If you purchase an IP address SSL certificate, provide only the IP address for the **Domain Name** field.

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.

Table 3-10 describes the domain types. For more information, see the examples.

Table 3-10 Domain Name

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

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.
	• 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.
	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.
	  • If you purchase a multi-domain certificate (single domain name + wildcard domain name), the primary domain name can only be associated with a single domain name.

Wildcard domain	Only one wildcard domain name can be associated. When associating a domain name, you can associate a wildcard domain name, which includes an asterisk (*).

Examples:

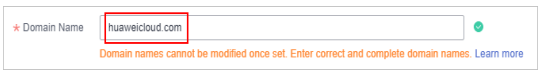
- Single-domain certificate

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

  Example: huaweicloud.com

  Enter **huaweicloud.com** in the text box next to **Domain Name** when applying for a certificate.

  Figure 3-6 Associating a single domain name

- 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 one or more additional domain names at a time. For more details, see **Adding an Additional Domain Name**.

NOTICE

- A primary domain and additional domains can be equally protected.
- If you purchase a multi-domain certificate (single domain name + wildcard domain name), the primary domain name can only be associated with a single domain name.

Example: If you plan to buy a multi-domain certificate for three domains, huaweicloud.com, test.huaweicloud.com, and *.huaweicloud.cn:

Set **Primary Domain Name** to **huaweicloud.com**, and **Additional Domain Name** to **test.huaweicloud.com** and ***.huaweicloud.cn** when applying for a certificate. Enter one additional domain name per line.

Figure 3-7 Associating multiple domain names

- Wildcard-domain certificate

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

  Example: Your domain names are test.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and good.huaweicloud.com, which are at the same level.

  Enter ***.huaweicloud.com** in the text box next to **Domain Name** when applying for a certificate.

  Figure 3-8 Associating a wildcard domain name

3.2.2 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 3-11 Domain Type

Parameter	Description
Single domain	Only one common domain name can be associated. 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. If the **Certificate Type** is set to **OV** or **OV Pro**, multiple single domains and multiple wildcard (*) domains can be added to one certificate. For example, if you purchase a multi-domain certificate (the number of domain names is three), you can use the 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. • Different promotion activities are offered by CAs for subdomain names, or www domain names. For details, see **Which Certificate Authorities Are Available?**. The following uses subdomain name www.a.com and root domain name a.com as an example to show the differences. – For DigiCert and GeoTrust certificates, you can purchase a certificate for either the root domain or the subdomain to protect both domains at the same time. For example, if you plan to purchase a multi-domain certificate issued by DigiCert or GeoTrust and expect to use this certificate to protect www.a.com and a.com, just bind www.a.com or a.com to the certificate. – For GlobalSign certificates, you can purchase a certificate for the subdomain and use the certificate to protect the corresponding root domain at the same time. However, a certificate for a root domain cannot protect the corresponding subdomain. For example, if you plan to purchase a multi-domain certificate issued by GlobalSign and expect to use the certificate to protect both www.a.com and a.com, just bind domain www.a.com to the certificate. • The number of domain names ranges from 2 to 250. A maximum of 250 domain names can be protected with a certificate. The following conditions must be met: – The number of primary domains is fixed at **1**. – The number of additional single domain names cannot be smaller than 1. If you select an OV or OV Pro certificate, the number of additional single domain names plus the number of additional wildcard domain names must be greater than or equal to 1. If you have multiple domain names, select **Multiple domains**. Purchase domain names of the required quantity on the purchase page.

Parameter	Description
Wildcard domain	• Only one wildcard domain name can be associated. • A wildcard domain name is the one that starts with a wildcard (*), for example, *.huaweicloud.com or *.example.huaweicloud.com. • Only the same-level domain matching is supported. For example, a certificate associated with *.huaweicloud.com can protect p1.huaweicloud.com but not p2.p1.huaweicloud.com. If you need to protect p2.p1.huaweicloud.com, purchase a wildcard-domain certificate associated with *.p1.huaweicloud.com. For details about more level matching rules, see **Table 3-12**. 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 3-12** are some examples.

Table 3-12 Examples of wildcard-domain matching rules

Domain name	Matched Domain Name	Unmatched Domain Name
*.huaweicloud.com	test.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names	abc.test.huaweicloud.com, yun.test.huaweicloud.com, example.test.huaweicloud.com, and other domain names
*.test.huaweicloud.com	abc.test.huaweicloud.com, yun.test.huaweicloud.com, example.test.huaweicloud.com, and other domain names	abc.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names

NOTICE

- For wildcard-domain certificates, only those associated with root domain names support the domain names. For example:
  - A certificate associated with the wildcard domain *.huaweicloud.com (a root domain) protects huaweicloud.com and other domain names of the same level. No additional certificate needs to be purchased for this.
  - A certificate associated with the wildcard domain *.p1.huaweicloud.com (not a root domain) will not protect p1.huaweicloud.com (a different level domain). It can only protect domain names of the same level. To protect p1.huaweicloud.com, you would need to purchase a new certificate.
- If the www subdomain is associated with a certificate, the certificate also protects the root domain. For example:

  A certificate purchased for domain www.huaweicloud.com can also protect huaweicloud.com. There is no need to purchase another certificate.
- Once your digital certificate is issued, the associated domain cannot be changed.

Table 3-13 is given here for your reference.

Table 3-13 Domain type selection examples

Example Scenario	Example Domain Name	Domain Type Selection	Quantity Selected
You have only one domain.	huaweicloud.com	Single domain	Single-domain type. The value of **Quantity** is fixed at **1**.
	test.huaweicloud.com	Single domain	
	p1.test.huaweicloud.com	Single domain	
You have multiple domains.	Two domains huaweicloud.com and p1.huawei.com	Multiple domains	2
	Three domains huaweicloud.com, p1.huawei.com, and p1.test.huaweicloud.cn	Multiple domains	3
	Four domains huaweicloud.com, test.huaweicloud.cn, p1.test.huaweicloud.cn, and p1.test.yun.huaweicloud.com	Multiple domains	4

Example Scenario	Example Domain Name	Domain Type Selection	Quantity Selected
You have multiple domains at the same level.	test.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names are the same level and are part of *.huaweicloud.com.	Wildcard domain	Wildcard domain type. The value of **Quantity** is fixed at **1**.

3.2.3 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 3-14**.

Table 3-14 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
	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 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.

Certificate Types	Supported Domain Name Type	Number of Domain Names that Can Be Protected
DV	Single domain	One
DV (Basic) - GeoTrust entry-level SSL certificates	Single domain	One
	Wildcard domain	One 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.

Other Operations

- **How Do I Apply an SSL Certificate to Other HUAWEI CLOUD Services?**
- **How Do I Install an SSL Certificate on a Server?**

3.2.4 What Domains Can Wildcard-Domain Certificates Support?

You can purchase wildcard-domain certificates in HUAWEI CLOUD 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:
  - A certificate associated with the wildcard domain *.huaweicloud.com (a root domain) protects huaweicloud.com and other domain names of the same level. No additional certificate needs to be purchased for this.
  - A certificate associated with the wildcard domain *.p1.huaweicloud.com (not a root domain) will not protect p1.huaweicloud.com (a different level domain). It can only protect domain names of the same level. To protect p1.huaweicloud.com, you would need to purchase a new certificate.
- 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 3-15 provides matching examples.

Table 3-15 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

3.2.5 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.

3.2.6 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, bind a new primary domain name, and apply for the certificate again.

- If your certificate has been issued and is within the allowable reissue period (GlobalSign allows you to apply for a reissue within five days after the certificate is issued. DigiCert and GeoTrust allow you to apply for a reissue within 25 days after the certificate is issued.):

  Yes.

  Apply for a reissue for the certificate. For more details, see **Reissuing an SSL Certificate**.

- If your certificate has been issued and is out of the allowable reissue period (GlobalSign allows you to apply for a reissue within five days after the certificate is issued. DigiCert and GeoTrust allow you to apply for a reissue within 25 days after the certificate is issued.):

  No.

  The primary domain name cannot be changed in this situation. To change the primary domain name, purchase a new certificate. For more details, see **Purchase an SSL Certificate**.

3.2.7 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.
- If you purchase a multi-domain certificate (single domain name + wildcard domain name), the primary domain name can only be associated with a single domain name.

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

3.2.8 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 3-9 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.

Field	Description	Example Value
Common Name	The website domain name you are applying for an SSL certificate for. **NOTE** • For a certificate with multiple domain names, enter the primary domain name to be associated with the certificate. • For a wildcard-domain certificate, enter the wildcard domain name. Example: *.example.com	www.example.com
Email Address	Email of an applicant. The CSR file password does not need to be entered. Just press **Enter**.	-
A challenge password	CSR file password. 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 3-10 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. **NOTE** – For a certificate with multiple domain names, enter the primary domain name to be associated with the certificate. – 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

Question	Description	Example Value
What is the name of your State or Province?	The state or province where an applicant is located.	ZheJiang
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

3.2.9 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 3-16** describes the differences between two methods to provide the CSR file.

Table 3-16 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. • 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. For details, see **How Do I Make a CSR File?**	• Certificates with CSR manually generated **cannot** be pushed to other HUAWEI CLOUD services. • If the CSR file is generated manually, HUAWEI CLOUD is not responsible for your private key. Back up your private key and keep it secure. If a private key is lost, the corresponding certificate becomes invalid. HUAWEI CLOUD is not responsible for keeping your private key. You need to buy a new certificate if the private key is lost. • 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.

3.2.10 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, www.huaweicloud.com. 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 3-17** details the domain levels.

Table 3-17 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.	

The following uses **abc.huaweicloud.com** as an example to describe the domain name hierarchy:

.com is only a top-level domain.

huaweicloud.com is a domain name containing two domain levels.

abc.huaweicloud.com is a domain name containing three domain levels.

3.2.11 Problems Related to Domains

Can I Associate a Chinese Domain with an SSL Certificate?

If you need to bind a Chinese domain name, use encoding tool **Punycode** to encode the Chinese domain name and then associate the encoded name.

Example: A Punycode-encoded Chinese domain name is **xn--siq1ht8k.com**.

When you apply for a certificate, associate **xn--siq1ht8k.com** with the certificate.

Figure 3-11 Associating a Chinese domain name

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

- During certificate purchase, the domain name bound to 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 HUAWEI CLOUD SCM Provide Wildcard-Domain Certificates?

Yes.

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

You can buy wildcard certificates, or wildcard-domain certificates, on HUAWEI CLOUD 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 3-18** provides the examples.

Table 3-18 Examples of wildcard-domain matching rules

Domain name	Matched Domain Name	Unmatched Domain Name
*.huaweicloud.com	test.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names	abc.test.huaweicloud.com, yun.test.huaweicloud.com, example.test.huaweicloud.com, and other domain names
*.test.huaweicloud.com	abc.test.huaweicloud.com, yun.test.huaweicloud.com, example.test.huaweicloud.com, and other domain names	abc.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names

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 following conditions must be met:

- The number of primary domains is fixed at **1**.
- The number of additional single domain names cannot be smaller than 1. If you select an OV or OV Pro certificate, the number of additional single domain names plus the number of additional wildcard domain names must be greater than or equal to 1.

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.

- A wildcard domain must start with an asterisk symbol and a dot (***.**) and contain only one asterisk symbol (*), for example, *.huaweicloud.com and *.example.huaweicloud.com.
- Only the same-level domain matching is supported. For example, a certificate associated with *.huaweicloud.com can protect p1.huaweicloud.com but not p2.p1.huaweicloud.com. If you need to protect p2.p1.huaweicloud.com, purchase a wildcard-domain certificate associated with *.p1.huaweicloud.com. For details about more level matching rules, see **Table 3-19**.

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 3-19** provides the examples.

Table 3-19 Examples of wildcard-domain matching rules

Domain name	Matched Domain Name	Unmatched Domain Name
*.huaweicloud.com	test.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names	abc.test.huaweicloud.com, yun.test.huaweicloud.com, example.test.huaweicloud.com, and other domain names

Domain name	Matched Domain Name	Unmatched Domain Name
*.test.huaweicloud.com	abc.test.huaweicloud.com, yun.test.huaweicloud.com, example.test.huaweicloud.com, and other domain names	abc.huaweicloud.com, yun.huaweicloud.com, example.huaweicloud.com, and other domain names

NOTICE

- For wildcard-domain certificates, only those associated with root domain names support the domain names. For example:
  - A certificate associated with the wildcard domain *.huaweicloud.com (a root domain) protects huaweicloud.com and other domain names of the same level. No additional certificate needs to be purchased for this.
  - A certificate associated with the wildcard domain *.p1.huaweicloud.com (not a root domain) will not protect p1.huaweicloud.com (a different level domain). It can only protect domain names of the same level. To protect p1.huaweicloud.com, you would need to purchase a new certificate.
- If the www subdomain is associated with a certificate, the certificate also protects the root domain. For example:

  A certificate purchased for domain www.huaweicloud.com can also protect huaweicloud.com. There is no need to purchase another certificate.
- Once your digital certificate is issued, the associated domain cannot be changed.

3.3 Information Input in SCM

3.3.1 How Can I Provide the Organization Information as an Individual User During SSL Certification Application?

Organization details are required when you apply for an OV, OV Pro, EV, or EV Pro certificates on HUAWEI CLOUD. An individual user who does not belong to an organization cannot complete this type of application.

The organization details are not required if you purchase a DV or basic DV certificate.

You can apply free certificates from some CAs. For details, see **How Can I Apply for a Free SSL Certificate?**

3.3.2 Do I Need to Upload the Bank Account Opening Permit and Business License When Applying for an SSL Certificate?

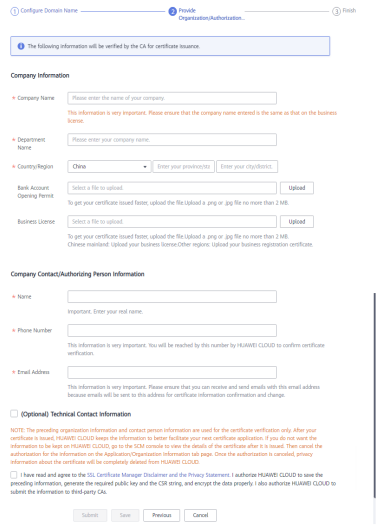
No.

Bank Account Opening Permit and **Business License** are optional. You can set them based on your needs

If you do not upload the bank account opening permit or business license, it may take longer to issue your certificate. The length of the delay depends on the CA.

When applying for an OV or EV certificate, you need to complete **Company Information**. You can complete **Bank Account Opening Permit** and **Business License** if you want.

Figure 3-12 Authorization information



Both **Bank Account Opening Permit** and **Business License** are optional. You can set them based on your needs.

- Bank Account Opening Permit

  Click **Upload** to upload the electronic copy of the bank account opening permit.

  NOTE

  - Only one file can be uploaded each time. It must be in .png or .jpg format, and cannot exceed 2 MB.
  - If the bank account opening permit is not uploaded, the certificate issuance period will be extended. The specific extension time depends on the verification time of CA.

    To avoid the unnecessary time extension, upload the required permit.

- Business License

  Click **Upload** to upload the electronic copy of the business license.

  – Chinese mainland: Upload your business license.
  – Other regions: Upload your business registration certificate.

NOTE

- Only one file can be uploaded each time. It must be in .png or .jpg format, and cannot exceed 2 MB.
- If the business license is not uploaded, the certificate issuance period will be extended. The specific extension time depends on the verification time of CA.

  To avoid the unnecessary time extension, upload the required business license.

3.4 Troubleshooting

3.4.1 What Can I Do If I Encounter a Problem When Purchasing, Applying for, Installing, or Using a Free SSL Certificate?

A free certificate is issued automatically. You can obtain the certificate after completing the configuration as required. In addition, free certificates are recommended only for testing. If you want to establish more secure data transmission between your server and client, you are advised to purchase other types of certificates.

For more details, see the following topics:

- **How Can I Apply for a Free SSL Certificate?**
- **How Do I Verify the Domain Ownership Manually by DNS?**
- **How Do I Install an SSL Certificate on a Server?**
- **How Do I Apply an SSL Certificate to Other HUAWEI CLOUD Services?**

We provide consulting service about certificate configuration at additional cost for free certificates. The consulting service about SSL certificate configuration optimization is available in the Marketplace on HUAWEI CLOUD website. However, if you buy other certificates, free consulting services are available.

3.4.2 What Can I Do If the Submit Button Is Unavailable?

Problem Description

When you apply for a certificate, the **Submit** button is unavailable.

Possible Causes

- Possible cause 1: arrears
- Possible cause 2: insufficient permission

Solution

Perform the following operations based on the possible cause:

- **Possible cause 1: arrears**

  Solution: Top up your account and then apply for a certificate.

- **Possible cause 2: insufficient permission**

  Solution: Contact your administrator to grant the permission to apply for a certificate. Perform operations after the permission is granted.

3.4.3 Can I Change Certificate Information After I Submit a Certificate Application?

What Information Changes or Incorrect Information Will Affect the Certificate Approval?

The certificate approval will be affected if all information except the contact name is incorrect.

Which of the Following Information Changes or Incorrect Information Will Affect the Certificate Use?

Table 3-20 Whether the certificate use will be affected by the information changes or incorrect information

Item	SSL Certificate Affected
Domain name	Yes
Contact name	No **NOTE** When you apply for a certificate, the company contact or authorizing person information entered in **Company Contact/Authorizing Person Information** is used for verification only and not included in the certificate after the certificate is issued. If the information is changed, the certificate use is not affected and no action is required.
Contact mobile number	
Address of the company	Yes
Business scope of the company	Yes

Can I Change Certificate Information After I Submit a Certificate Application?

1. Check whether the incorrect information affects the approval or use of the certificate.
   - If yes, go to 2.
   - If no, performed the corresponding operations based on the actual situation.
     - If the certificate is not issued, perform the subsequent operations and wait for the certificate to be approved.

- If the certificate is issued, no actions are required, and you can use the certificate.

2. Check whether the certificate is issued.
   - If the certificate has not been issued:

     If you have submitted a certificate application but then discover there are incorrect details included, you can withdraw the application.

     For details, see **Withdrawing an SSL Certificate Application**.
   - If the certificate has been issued:
     - If your certificate has been issued and is within the allowable reissue period, you can apply for a reissue to change the certificate information if there is incorrect information in the certificate or the certificate information needs to be changed. The allowable reissue period varies depending on CAs. GlobalSign allows you to apply for a reissue within five days after the certificate is issued. DigiCert and GeoTrust allow you to apply for a reissue within 25 days after the certificate is issued. For more details, see **Reissuing an SSL Certificate**.
     - If your certificate has been issued and is out of the allowable reissue period, you need to purchase a new certificate if there is incorrect information in the certificate or the certificate information needs to be changed. The allowable reissue period varies depending on CAs. GlobalSign allows you to apply for a reissue within five days after the certificate is issued. DigiCert and GeoTrust allow you to apply for a reissue within 25 days after the certificate is issued.

3.4.4 What Can I Do If I Encounter a Problem During SSL Certificate Application?

You may encounter the following problems when applying for a certificate:

May I Enter My Own Name in Company Contact When Applying for a Certificate?

Yes.

The contact details are used for communications purposes only. They are not officially reviewed.

Can I Delete the TXT Records Added During DNS Verification?

The DNS resolution records are configured to verify the domain names. The TXT records can be deleted only after the certificate domain name is verified. The approval and use of the certificate will not be affected after the TXT records are deleted.

Do I Need to Use Quotation Marks When Adding TXT Records to a Record Set for Domain Name Resolution on HUAWEI CLOUD DNS?

After the SSL certificate application is submitted, domain name ownership verification is required.

When you use HUAWEI CLOUD DNS to resolve a domain name and add a record set, you need to enter the TXT host record of the domain name. Use quotation marks when entering the record value

An example command is provided as follows:

"201807040000001v0p73k28ruec3am17s0wl6z7angvqlesyipf65k7347knjm7h"

For more details, see **Step 3: Performing Verification Using HUAWEI CLOUD DNS**.

How Do I Select a CSR When Applying for a Certificate?

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 select **System generated CSR** or **Upload a CSR** for **CSR**.

- **System generated CSR**: The system automatically generates a certificate private key. Once the certificate is issued, you can download your certificate and private key on the certificate management page.
- **Upload a CSR**: Manually make a CSR file. For details, see **How Do I Make a CSR File?**

NOTE

You are advised to select **System generated CSR** to avoid approval failure caused by incorrect content. For details about the differences between the two types of certificate, see **What Are the Differences Between the CSR Generated by the System and the CSR Made by Yourself?**

Which of the Enterprise Business Licenses Needs To Be Uploaded for Applying for A Certificate?

When applying for a certificate, you can determine whether to upload the enterprise business license based on site requirements.

If you need to upload the business license, upload the business license of the enterprise that uses the certificate. Be sure not to upload the business license of the organization who developed your system.

If you do not upload the business license, it may take longer to issue your certificate.

3.4.5 About IP Address Application for SSL Certificates

Does an SSL Certificate Associated with an IP Address Needs to Be Approved?

Yes.

The application process is the same regardless of whether an SSL certificate is associated with a domain name or an IP address. The SSL certificate must be applied for and approved by the CA before it can be used.

The application process is as follows: Purchase a certificate → Apply for a certificate → Verify the domain name → Verify the organization (required only for OV, OV Pro, EV, and EV Pro certificates) → Issue a certificate.

The difference is that the domain name verification of an SSL certificate associated with an IP address supports only verification by file.

What Is the Domain Name Verification Method for an SSL Certificate Associated with an IP address?

The domain name of an SSL certificate associated with an IP address can be verified only by file. Therefore, when applying for a certificate, select **File** for **Domain Name Verification Method** for SSL certificates associated with IP addresses.

For details about how to verify files, see **How Do I Perform Verification by File?**

4 Verification of the Domain Name Ownership - SCM

4.1 How Do I Verify Domain Ownership?

You need to work with the CA to complete the domain name ownership verification for your SSL certificate.

After your ownership of the domain name is verified by you and approved by the CA, the status of your certificate will change.

Table 4-1 describes available methods to verify domain name ownership on SCM. Perform operations based on the verification method you selected.

Table 4-1 Domain ownership verification

Parameter	Description
Automatic DNS Verification	You are required to verify domain ownership on the platform hosting your domain name by resolving a specific DNS record. Automatic DNS verification: The system automatically adds DNS records for verification. The system performs automatic DNS verification only when all the following conditions are met: • The certificate you bought is a single-domain certificate. • Your certificate is used for a domain name that you apply for on HUAWEI CLOUD and is hosted on HUAWEI CLOUD DNS. • When you apply for the certificate, you select automatic DNS verification for domain name verification method. (This is not required for DV certificates.)

Parameter	Description
Manual DNS Verification	In this method, you need to verify the domain ownership by resolving a specific DNS record on the domain name management platform. Manual DNS verification: You need to go to the DNS service provider of the domain name to perform the verification. For more details, see **How Do I Verify the Domain Ownership Manually by DNS?**
File	In this method, you are required to verify domain name ownership by creating a specified file on the server. For more details, see **How Do I Perform Verification by File?**
Email	In the method, you need to reply an email from the CA to complete the domain ownership verification. For more details, see **How Do I Perform Verification by Email?**

NOTE
• IP address SSL certificates can only be verified by file.
• DV and basic DV certificates (GeoTrust entry-level SSL certificates and DigiCert free SSL certificates) can be verified by DNS by default.
  • If you apply for a domain name on HUAWEI CLOUD and the domain name has been resolved by HUAWEI CLOUD DNS, the system automatically verifies the domain.
  • If your domain name is hosted on other platforms, such as www.net.cn, www.xinnet.com, and www.dnspod.cn, you need to manually verify your domain name.	

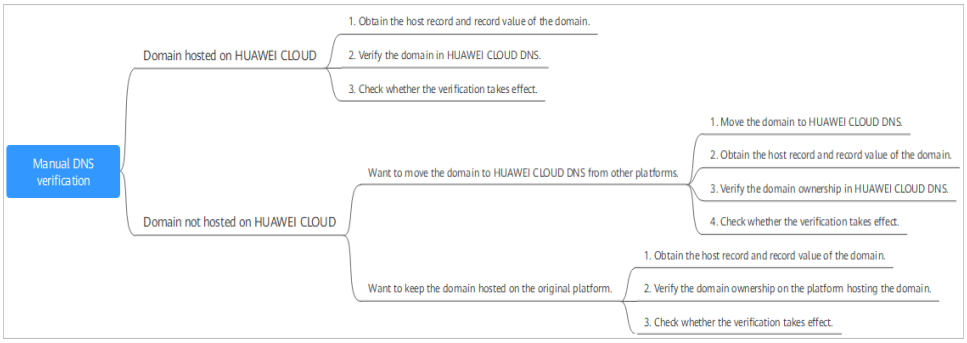
4.2 How Do I Verify the Domain Ownership Manually by DNS?

Domain name ownership verification by DNS is to verify domain ownership by resolving a specific DNS record on the platform hosting the domain name. SCM supports automatic and manual DNS verification.

This topic uses our platform as an example to describe how to verify domain name ownership manually by DNS.

Manual DNS verification: You need to go to the DNS service provider of the domain name to perform the verification.

Figure 4-1 Manual DNS verification



Constraints

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

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

When you use DNS to verify your domain ownership, the DNS records can be resolved only on the platform managing your domain name. If your domain names are not hosted on HUAWEI CLOUD, are you willing to migrate them to HUAWEI CLOUD?

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

NOTE

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

Step 2: Obtaining Verification Information

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

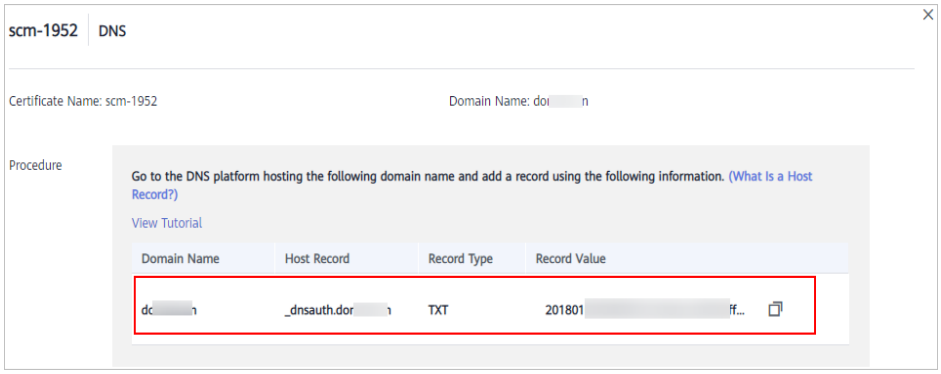
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

Step 3 In the navigation pane on the left, choose **SSL Certificate Manager**. In the row containing the desired certificate, click **Verify Domain Name** in the **Operation** column. The **Verify Domain Name** page is displayed.

Step 4 On the **Verify Domain Name** page, view the content for **Host Record**, **Record Type**, and **Record Value**. **Figure 4-2** shows an example.

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

Figure 4-2 Viewing a host record



----End

Step 3: Performing Verification Using HUAWEI CLOUD DNS

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

Step 2 Choose **Networking** > **Domain Name Service**. In the navigation pane on the left, choose **DNS Resolution** > **Public Zones**. The **Public Zones** page is displayed.

Step 3 In the public zone list, click the domain name to be resolved. In the upper right corner of the page, click **Add Record Set**. The **Add Record Set** dialog page is displayed.

NOTE

If there is already a TXT record in the record set, click **Modify** in the **Operation** column. Modify the record in the displayed **Modify Record Set** dialog box.

Figure 4-3 Adding a record set

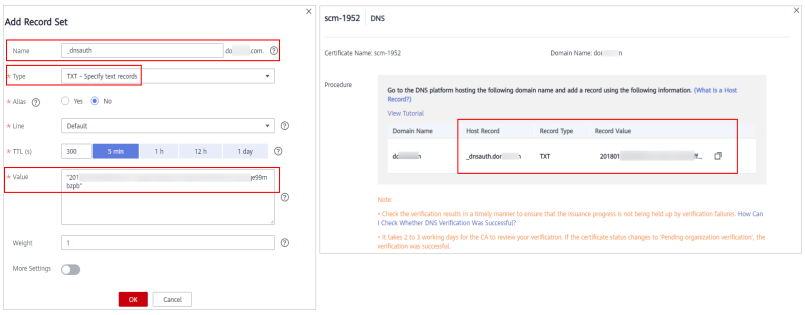


Table 4-2 Record set parameters

Parameter	Description
Name	Host record returned by the domain name service provider on the domain name verification page of the certificate. Note that host records returned by domain name service providers are different. Ensure that the host record is correct. **Examples** • If the host record returned by the domain name service provider is **_dnsauth.example.com**, set **Name** to **_dnsauth**. • If the host record returned by the domain name service provider is **example.com**, leave **Name** empty.
Type	Select **TXT – Specify text records**.
Alias	Select **No**.
Line	Select **Default**.
TTL (s)	Set this parameter to **5 min**. A larger TTL value indicates less frequency of DNS record synchronization and update.
Value	Record value returned by the domain name service provider on the domain name verification page of the certificate. **NOTE** Record values must be quoted with quotation marks and then pasted in the text box.
Keep other settings unchanged.	

Step 4 Click **OK**.

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

NOTE

The TXT record can be deleted only after the certificate is issued.

----End

Step 4: Checking Whether Domain Ownership Verification Takes Effect

Step 1 On the Windows menu, click **Start** and enter **cmd** to start the command dialog box.

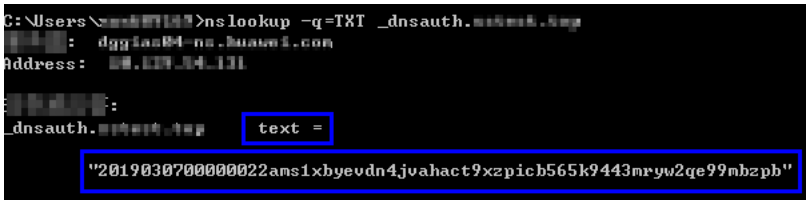
Step 2 Run the following command in the cmd dialog box to check whether the configuration of DNS verification takes effect:

nslookup -q=TXT *xxx*

xxx indicates the **Host Record** value returned by the domain name service provider.

- If the record value in the command output (value of **text**) is the same as that returned by the domain name service provider, the configuration of domain name ownership verification has taken effect. **Figure 4-4** shows an example.

Figure 4-4 Effective configuration of domain name ownership verification

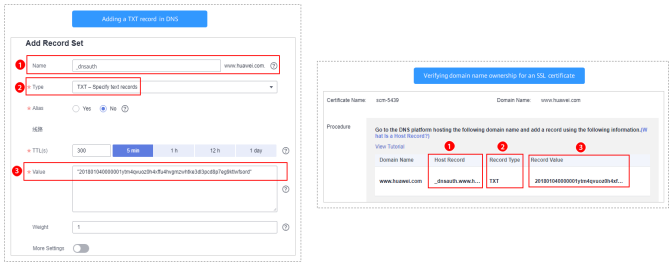


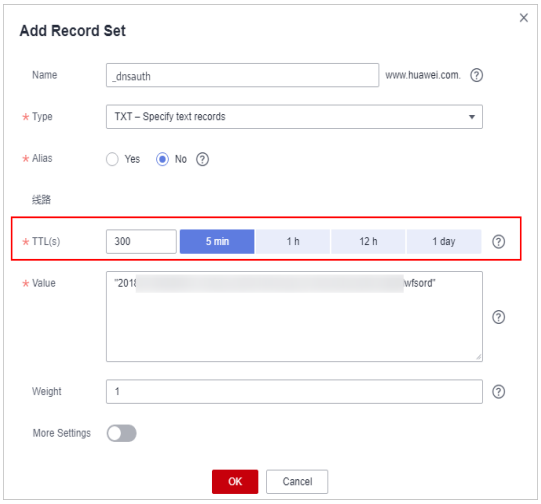
- If the command output does not contain a TXT record and **Non-existent domain** is displayed, the configuration does not take effect.

Figure 4-5 Non-effective domain name verification configuration

Step 3 If the configuration of DNS verification does not take effect, rectify the fault based on the following possible causes until the verification takes effect:

Table 4-3 Possible causes

Possible Cause	Procedure
The record configuration is incorrect.	Check whether the **Name** or **Type** is correct. The following uses the DNS configuration on HUAWEI CLOUD as an example: **Figure 4-6** Adding a record  The returned host record varies depending on the domain name service provider. The following are two examples: Example: • If the host record returned by the domain name service provider is **_dnsauth.www.huawei.com**, set **Name** to **_dnsauth**. • If the host record returned by the domain name service provider is **www.huawei.com**, leave **Name** empty. **NOTICE** Check whether full domain names are supported. If not, delete the suffix of the root domain name.

Possible Cause	Procedure
It requires a long period of time for the configuration to take effect.	Check whether the effective time (TTL) is too long. It is recommended that you set the TTL to 5 minutes. This value varies depending on the DNS service provider. In HUAWEI CLOUD DNS, the default value is 5 minutes, so the configuration takes effect within 5 minutes by default. If the configured effective time does not arrive, verify after the time is right. **Figure 4-7** Setting TTL 

----End

4.3 How Do I Perform Verification by File?

In this method, you are required to verify domain name ownership by creating a specified file on the server.

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

Verification by file is usually performed by your server administrator. This topic describes how to perform verification by file.

NOTE

The verification file can be deleted only after the certificate is issued or revoked.

Constraints

- If the associated domain name contains **www**, you need to verify both the domain name with www and without www. For example, if the domain name

is **www.example.com**, you need to verify the ownership of both **example.com** and **www.example.com**.

- If the associated domain name is a wildcard domain name, only the domain name without the asterisk (*) needs to be verified. For example, if the domain name is ***.example.com**, only **example.com** needs to be verified.

Step 1: Obtaining Verification Information

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

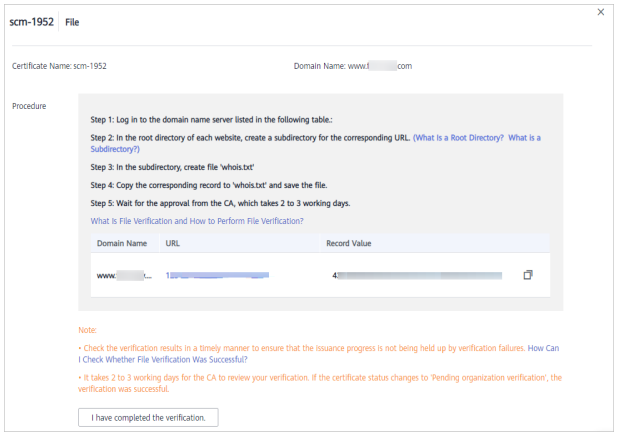
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

Step 3 In the navigation pane on the left, choose **SSL Certificate Manager**. In the row containing the desired certificate, click **Verify Domain Name** in the **Operation** column. The **Verify Domain Name** page is displayed.

Step 4 On the **Verify Domain Name** page, view the **Record Value**.

If the page is not displayed, log in to your email (the one specified during certificate application) to view the recorded value.

Figure 4-8 File verification



----End

Step 2: Creating the Required File

Step 1 Log in to your server and ensure that the domain name points to the server and the website is enabled.

Step 2 Create a specified file in the root directory of the website. You need to specify the file directory, file name, and content.

NOTE

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

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

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

   In this case, create the subdirectory in the **/www/htdocs** directory.
2. Create the **whois.txt** file in the **.well-known/pki-validation** subdirectory.
3. Add the record value obtained in **Step 1: Obtaining Verification Information** to the **whois.txt** file.

----End

Step 3: Checking Whether the Verification Configuration Takes Effect

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

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

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

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

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

Step 2 Check whether the verification URL address can be properly accessed in the browser and whether the record value displayed on the page is the same as that on the order progress page.

- If the record value displayed on the page is the same as that displayed on the domain name verification page of the SCM console, the configuration of domain name verification has taken effect.
- If they are different, the configuration of domain name verification does not take effect.

Step 3 If the configuration does not take effect, check and handle the issue from the following aspects:

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

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

----End

4.4 How Do I Perform Verification by Email?

Verification by email indicates that the domain name ownership is verified by replying to an email.

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

Procedure

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

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

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

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

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

----End

4.5 How Do I Check Whether Domain Name Verification Takes Effect?

You can check whether the domain name verification takes effect if you have configured for domain name ownership verification. This part describes how to check whether the domain name verification takes effect.

Procedure

- **Checking Verification by DNS**: If **Domain Name Verification Method** is **DNS**, perform the operations described in this section.
- **Checking Verification by File**: If **Domain Name Verification Method** is **File**, perform the operations described in this section.

Prerequisites

- Domain name verification has been configured. For details, see **Verify the Domain Ownership**.
- The domain name has been licensed. Obtain the license for the domain name because the domain name verification will fail if the domain name has not been licensed.

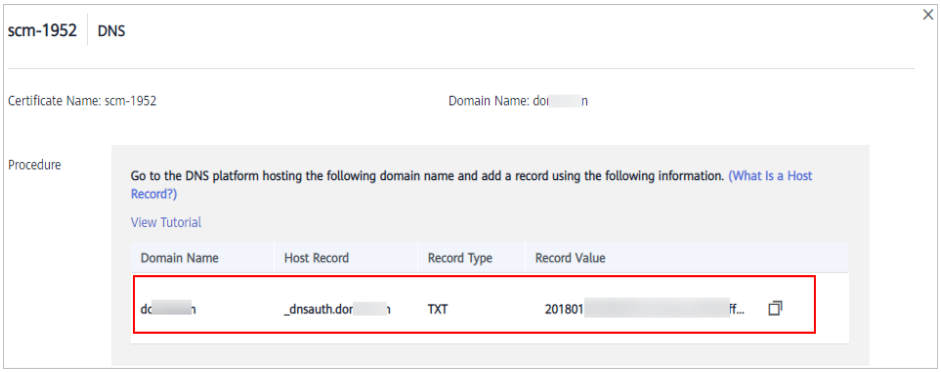
Checking Verification by DNS

Step 1 Obtain the host record and record value.

1. Log in to the **management console**.
2. Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.
3. In the navigation pane on the left, choose **SSL Certificate Manager**. The **SSL Certificate Manager** page is displayed.
4. In the **Operation** column of the certificate for which domain name verification is to be performed, click **Verify Domain Name**.
5. On the **Verify Domain Name** page, view the content for **Host Record**, **Record Type**, and **Record Value**. **Figure 4-9** shows an example.

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

Figure 4-9 Viewing a host record



Step 2 Select a command based on your operating system and check whether the DNS configuration takes effect.

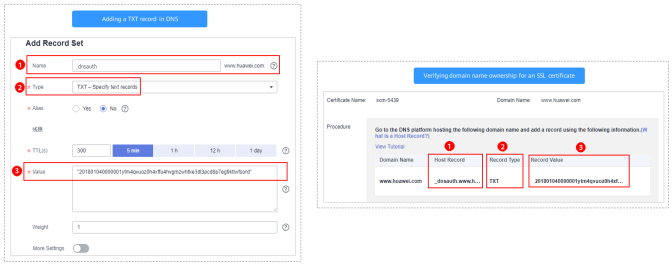
Use TXT record **_dnsauth.domain.com** as an example.

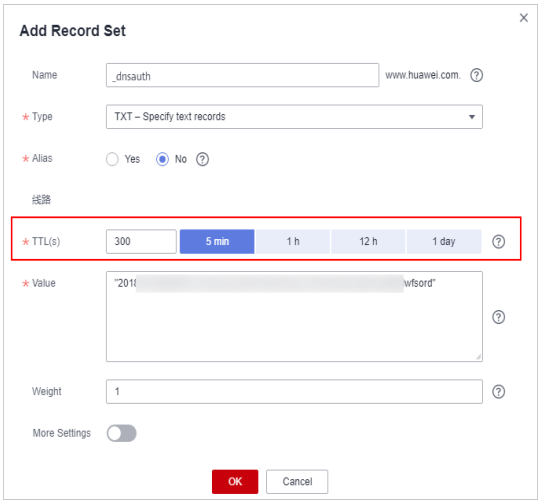
- For Windows OSs:
  ```
  nslookup -q=TXT _dnsauth.domain.com
  ```
- For Linux OSs:
  ```
  dig TXT _dnsauth.domain.com
  ```
- For macOS OSs:
  ```
  dig TXT _dnsauth.domain.com
  ```

If the record value in the command output (value of **text**) is the same as that returned by the domain name service provider, the configuration of domain ownership verification has taken effect.

Step 3 If the configuration of DNS verification does not take effect, rectify the fault based on the following possible causes until the verification takes effect:

Table 4-4 Possible causes

Possible Cause	Procedure
The record configuration is incorrect.	Check whether the **Name** or **Type** is correct. The following uses the DNS configuration on HUAWEI CLOUD as an example: **Figure 4-10** Adding a record  The returned host record varies depending on the domain name service provider. The following are two examples: Example: • If the host record returned by the domain name service provider is **_dnsauth.www.huawei.com**, set **Name** to **_dnsauth**. • If the host record returned by the domain name service provider is **www.huawei.com**, leave **Name** empty. **NOTICE** Check whether full domain names are supported. If not, delete the suffix of the root domain name.

Possible Cause	Procedure
It requires a long period of time for the configuration to take effect.	Check whether the effective time (TTL) is too long. It is recommended that you set the TTL to 5 minutes. This value varies depending on the DNS service provider. In HUAWEI CLOUD DNS, the default value is 5 minutes, so the configuration takes effect within 5 minutes by default. If the configured effective time does not arrive, verify after the time is right. **Figure 4-11** Setting TTL 

----End

Checking Verification by File

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

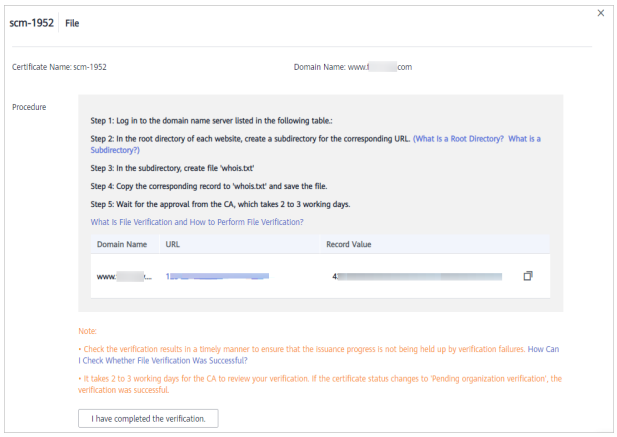
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

Step 3 In the navigation pane on the left, choose **SSL Certificate Manager**. In the row containing the desired certificate, click **Verify Domain Name** in the **Operation** column. The **Verify Domain Name** page is displayed.

Step 4 On the **Verify Domain Name** page, view the **Record Value**.

If the page is not displayed, log in to your email (the one specified during certificate application) to view the recorded value.

Figure 4-12 File verification



Step 5 Open a browser and access the URL address: **https://*your domain*/.well-known/pki-validation/whois.txt** or **http://*your domain*/.well-known/pki-validation/whois.txt**.

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

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

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

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

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

Step 6 Check whether the verification URL address can be properly accessed in the browser and whether the record value displayed on the page is the same as that on the order progress page.

- If the record value displayed on the page is the same as that displayed on the domain name verification page of the SCM console, the configuration of domain name verification has taken effect.
- If they are different, the configuration of domain name verification does not take effect.

Step 7 If the configuration does not take effect, check and handle the issue from the following aspects:

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

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

----End

4.6 How Can I Check Whether DNS Verification Takes Effect for Windows OSs?

This topic describes how to check whether domain ownership DNS verification takes effect on Windows OSs.

After you apply for a certificate, complete the domain ownership verification by DNS.

Step 1 On the Windows menu, click **Start** and enter **cmd** to start the command dialog box.

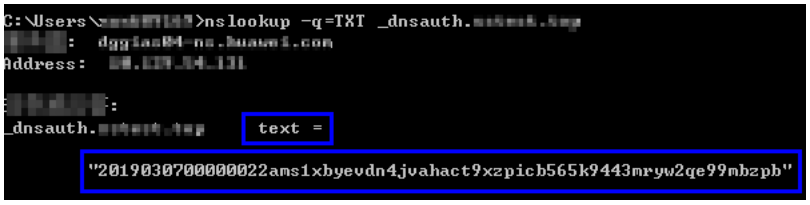
Step 2 Run the following command in the cmd dialog box to check whether the configuration of DNS verification takes effect:

nslookup -q=TXT *xxx*

xxx indicates the **Host Record** value returned by the domain name service provider.

- If the record value in the command output (value of **text**) is the same as that returned by the domain name service provider, the configuration of domain name ownership verification has taken effect. **Figure 4-13** shows an example.

  Figure 4-13 Effective configuration of domain name ownership verification

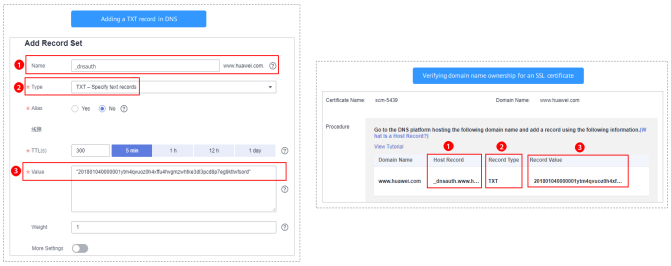
- If the command output does not contain a TXT record and **Non-existent domain** is displayed, the configuration does not take effect.

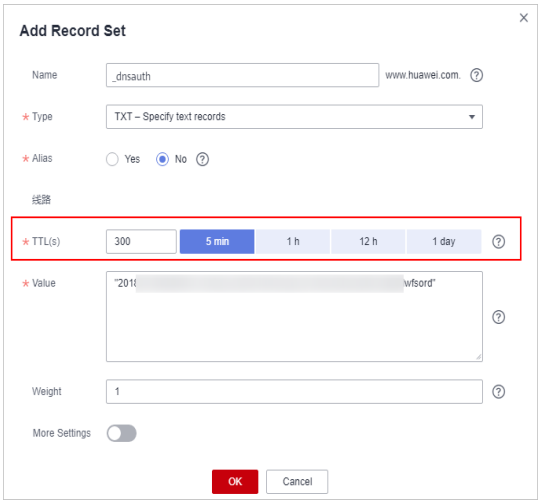
  Figure 4-14 Non-effective domain name verification configuration

Step 3 If the configuration of DNS verification does not take effect, rectify the fault based on the following possible causes until the verification takes effect:

Table 4-5 Possible causes

Possible Cause	Procedure
The record configuration is incorrect.	Check whether the **Name** or **Type** is correct. The following uses the DNS configuration on HUAWEI CLOUD as an example: **Figure 4-15** Adding a record  The returned host record varies depending on the domain name service provider. The following are two examples: Example: • If the host record returned by the domain name service provider is **_dnsauth.www.huawei.com**, set **Name** to **_dnsauth**. • If the host record returned by the domain name service provider is **www.huawei.com**, leave **Name** empty. **NOTICE** Check whether full domain names are supported. If not, delete the suffix of the root domain name.

Possible Cause	Procedure
It requires a long period of time for the configuration to take effect.	Check whether the effective time (TTL) is too long. It is recommended that you set the TTL to 5 minutes. This value varies depending on the DNS service provider. In HUAWEI CLOUD DNS, the default value is 5 minutes, so the configuration takes effect within 5 minutes by default. If the configured effective time does not arrive, verify after the time is right. **Figure 4-16** Setting TTL 

----End

4.7 What Can I Do If Domain Ownership Verification Does Not Take Effect?

If you have completed domain name verification but the configuration does not take effect, perform the operations described in this section.

Procedure

- If **Domain Name Verification Method** is set to **DNS**, perform the operations described in **Configuration Does Not Take Effect After DNS Verification**.
- If **Domain Name Verification Method** is set to **File**, perform the operations described in **Configuration Does Not Take Effect After File Verification**.

Prerequisites

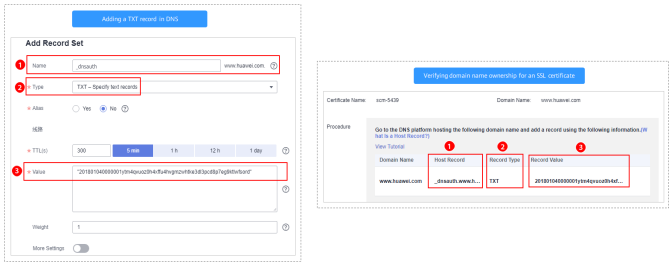
- The domain name has been licensed. Obtain the license for the domain name because the domain name verification will fail if the domain name has not been licensed.

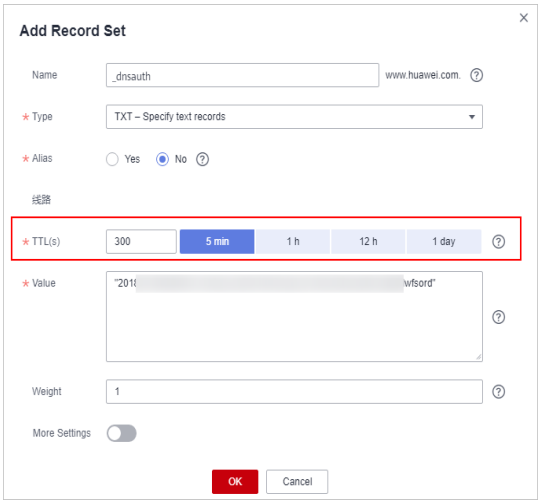
- Domain name verification has been configured. For details, see **Verify the Domain Ownership**.
- Check whether the domain name verification takes effect. For more details, see **How Do I Check Whether Domain Name Verification Takes Effect?**

Configuration Does Not Take Effect After DNS Verification

Locate the failure cause and fix the issue by referring to the following table.

Table 4-6 Possible causes

Possible Cause	Procedure
The record configuration is incorrect.	Check whether the **Name** or **Type** is correct. The following uses the DNS configuration on HUAWEI CLOUD as an example: **Figure 4-17** Adding a record  The returned host record varies depending on the domain name service provider. The following are two examples: Example: • If the host record returned by the domain name service provider is **_dnsauth.www.huawei.com**, set **Name** to **_dnsauth**. • If the host record returned by the domain name service provider is **www.huawei.com**, leave **Name** empty. **NOTICE** Check whether full domain names are supported. If not, delete the suffix of the root domain name.

Possible Cause	Procedure
It requires a long period of time for the configuration to take effect.	Check whether the effective time (TTL) is too long. It is recommended that you set the TTL to 5 minutes. This value varies depending on the DNS service provider. In HUAWEI CLOUD DNS, the default value is 5 minutes, so the configuration takes effect within 5 minutes by default. If the configured effective time does not arrive, verify after the time is right. **Figure 4-18** Setting TTL 

If your problem persists, HUAWEI CLOUD provides one-to-one professional consulting services to help you deploy SSL certificates on the cloud. Our professional SSL certificate service will help you complete installation and configuration of HTTPS SSL certificates for your website. You can buy SSL certificate configuration service at additional cost. Then we will help you install and configure SSL certificates for your websites.

Configuration Does Not Take Effect After File Verification

If the DNS verification configuration does not take effect, perform the following checks:

- If the record value displayed on the page is the same as that displayed on the domain name verification page of the SCM console or in the email, the configuration of domain name verification has taken effect.
- If they are different, the configuration of domain name verification does not take effect.

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

  – Check whether the verification URL address exists in HTTPS accessible addresses. If yes, use HTTPS to re-access the URL address in the browser.

If the browser displays a message indicating that the certificate is untrusted or the displayed content is incorrect, disable the HTTPS service for the domain name temporarily.

- Ensure that the verification URL address can be accessed at any place. Detection servers of some CAs are located outside China. Check whether your site has images outside China or whether the smart DNS service is used.
- Check whether the verification URL address contains 301 or 302 redirection. If such redirection exists, cancel the related settings to disable the redirection.

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

If your problem persists, HUAWEI CLOUD provides one-to-one professional consulting services to help you deploy SSL certificates on the cloud. Our professional SSL certificate service will help you complete installation and configuration of HTTPS SSL certificates for your website. You can buy SSL certificate configuration service in marketplace at additional cost.

4.8 How Do I Query a Domain Name Provider?

By querying domain registration information, you can confirm the information about the DNS servers of a domain name and then perform authentication by DNS based on the DNS server information.

Procedure

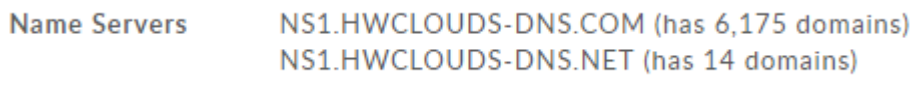
Step 1 Open a browser and visit **https://whois.domaintools.com/**.

Step 2 Enter the domain name to be queried and click **Search**. The domain name registration details page is displayed.

Step 3 In the displayed information, check **Name Servers** to determine the DNS servers of the domain name.

If the value of **Name Servers** similar to **Figure 4-19** is displayed, the DNS servers of the domain name are provided by HUAWEI CLOUD.

Figure 4-19 Name Servers



Perform the verification based on the DNS servers of the domain name as follows:

- If the domain name is hosted on a HUAWEI CLOUD DNS server, perform the verification on HUAWEI CLOUD by referring to **How Do I Verify Domain Ownership by DNS?**
- If the domain name is not hosted on HUAWEI CLOUD, think about whether you want to migrate it to HUAWEI CLOUD DNS.
  - If yes, perform the following operations:

i. For details, see **How Do I Migrate My Domain from Another DNS Service Provider to HUAWEI CLOUD DNS?**

ii. Perform the verification on HUAWEI CLOUD by referring to **How Do I Verify the Domain Ownership Manually by DNS?**

– If not, perform the verification on the corresponding platform. For example, if your domain is hosted on Alibaba Cloud, perform the verification on Alibaba Cloud.

----End

4.9 How Do I Query and Verify the Email Address of the Domain Administrator?

This topic describes how to query the email address of the domain administrator during certificate approval and perform confirmation as prompted.

Procedure

Step 1 Visit **http://whois.domaintools.com/** and enter the domain name whose administrator email address you want to query.

Step 2 In the query result, view the email address of the domain administrator.

Step 3 If the email address is correct, the CA will send a confirmation email to the email address after you apply for a certificate. Click the confirmation link in the email received and perform the confirmation as prompted.

----End

4.10 How Do I Use DNS to Verify Domains Not Hosted on HUAWEI CLOUD?

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

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

4.11 Why Does the SSL Certificate Remain in the Pending Domain Name Verification State After Domain Name Verification Completes?

If domain name verification is complete but the certificate remains in the **Pending domain name verification** state, perform the following steps:

1. Check whether the ownership of the domain name for which the certificate is used is verified.
   - If domain ownership is verified, go to **2**.
   - If domain ownership has not been verified, go to your domain name service provider to complete the verification.
2. Check whether the domain name verification has been completed.
   - If you have completed domain name verification, go to **3**.
   - If you have not completed domain ownership verification and organization verification, perform operations as prompted.

     For details, see **Verify the Domain Ownership**.
3. Check whether the domain name verification takes effect.

   For details, see **How Do I Check Whether Domain Name Verification Takes Effect?**.
   - If domain name verification takes effect, go to **4**.
   - If the verification still does not take effect, perform the required operations in **What Can I Do If Domain Ownership Verification Does Not Take Effect?**

   For details about how to make the verification take effect, see **DNS Verification Configuration Does Not Take Effect**.
4. The review may take a while.

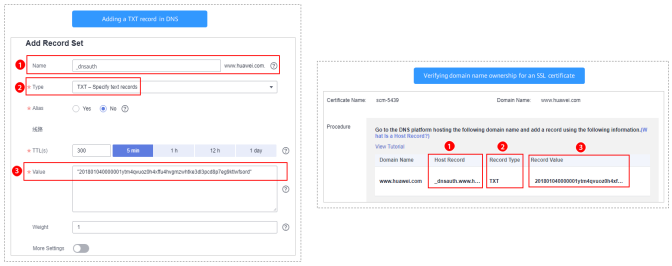
   After the verification is complete, additional time is required for the CA to verify your domain name. During this period, the certificate is in the **Pending domain name verification** state.

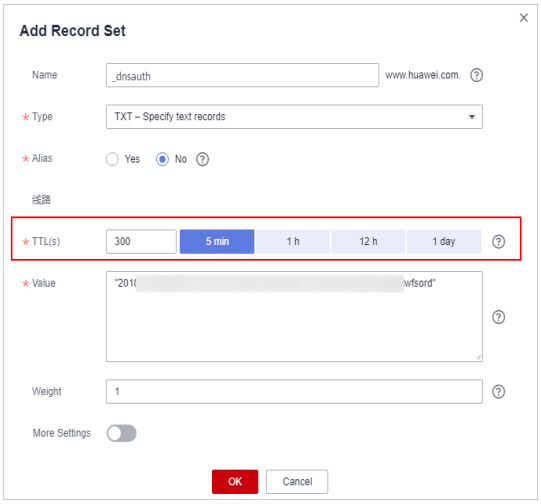
   If you have verified the domain name, the CA will take 2 to 3 working days to verify your information. The certificate state changes only after the CA verifies the certificate.

DNS Verification Configuration Does Not Take Effect

Locate the failure cause and fix the issue by referring to the following table.

Table 4-7 Possible causes

Possible Cause	Procedure
The record configuration is incorrect.	Check whether the **Name** or **Type** is correct. The following uses the DNS configuration on HUAWEI CLOUD as an example: **Figure 4-20** Adding a record  The returned host record varies depending on the domain name service provider. The following are two examples: Example: • If the host record returned by the domain name service provider is **_dnsauth.www.huawei.com**, set **Name** to **_dnsauth**. • If the host record returned by the domain name service provider is **www.huawei.com**, leave **Name** empty. **NOTICE** Check whether full domain names are supported. If not, delete the suffix of the root domain name.

Possible Cause	Procedure
It requires a long period of time for the configuration to take effect.	Check whether the effective time (TTL) is too long. It is recommended that you set the TTL to 5 minutes. This value varies depending on the DNS service provider. In HUAWEI CLOUD DNS, the default value is 5 minutes, so the configuration takes effect within 5 minutes by default. If the configured effective time does not arrive, verify after the time is right. **Figure 4-21** Setting TTL 

4.12 How Do I Change the Domain Name Verification Mode When the SSL Certificate Status Is Pending domain name verification?

If your SSL certificate is in the **Pending domain name verification** state, the domain name is to be verified based on the verification mode selected during certificate application.

If you need to change the domain name verification mode during this stage, withdraw the certificate application, change the domain name verification mode, and submit the application again.

NOTE

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

Step 1 Withdraw the certificate application.

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

2. Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.
3. In the navigation pane on the left, choose **SSL Certificate Manager**. The **SSL Certificate Manager** page is displayed.
4. In the row containing the desired certificate, click **Withdraw Application** in the **Operation** column.

   Figure 4-22 Withdrawing an application

5. In the **Cancel Application** dialog box that is displayed, click **Submit**. When "Request for canceling the application submitted successfully" is displayed in the upper right corner, the request has been submitted.

   At this time, the certificate is in the **CA verifying (application withdrawal)** state. After the application is withdrawn successfully, the certificate status changes to **Pending application**.

Step 2 Apply for the certificate.

If the withdrawal is successful, the certificate is in the **Pending application** state and you need to submit the application again. Change the domain name verification mode when submitting the application.

For more details, see **Apply for a Certificate**.

Step 3 Complete the certificate application procedure.

Apply for the certificate as prompted.

----End

5 SSL Certificate Approval

5.1 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 5-1**.

Table 5-1 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.
Domain Validation (DV) and DV (Basic)	Generally, a basic DV certificate can be issued within several hours. Domains of basic DV certificates are verified by the CA automatically. 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 After Domain Name Verification Completes?**
- **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?**

5.2 Why Does the Certificate Stay in the CA Verifying Status for a Long Time?

Upon completion of the certificate information, the Certificate Authority (CA) will review your domain name and the submitted certificate information. To ensure that your certificate can be issued as soon as possible, perform the following operations.

NOTE

The approval time may vary depending on certificate authorities. For details about approval time, see **How Long Does It Take to Approve an SSL Certificate?**

Procedure

Step 1 Check whether the ownership of the domain name for which the certificate is used is verified.

- If domain ownership is verified, go to **Step 2**.
- If domain ownership has not been verified, go to your domain name service provider to complete the verification.

Step 2 Check whether you have correctly filled in and submitted the certificate application.

- If yes, go to **Step 3**.
- If the entered information is incorrect, you can withdraw the application. After the withdrawal is successful, modify the information and then submit it for approval. After the modification, go to **Step 3**.

  For details, see **Withdrawing a Certificate Application**.

For details, see **Apply for a Certificate**.

Step 3 Ensure that you have completed domain name verification and organization verification according to the certificate status/application progress on the SCM console.

- If you have completed domain ownership verification and organization verification, go to **4**.
- If you have not completed domain ownership verification and organization verification, perform operations as prompted.

  For details, see **Verify the Domain Ownership**. After the verification completes, check whether the verification takes effect.

  For details, see **Verify the Organization**. Organization information check is required only for OV, OV Pro, EV, and EV Pro certificates.

Step 4 Check whether the domain name verification takes effect.

For details, see **How Do I Check Whether Domain Name Verification Takes Effect?**.

- If domain name verification takes effect, go to **Step 5**.
- If the verification still does not take effect, perform the required operations in **What Can I Do If Domain Ownership Verification Does Not Take Effect?**

Step 5 Check whether Certification Authority Authorization (CAA) restricts the CA from issuing certificates.

- If the CA is restricted by CAA, you can cancel the restriction or add a CAA resolution record by referring to **Setting CAA Records to Prevent Unauthorized HTTPS Certificate Issuing**.
- If the CA is not restricted by CAA, go to **Step 6**.

Step 6 The review may take a while.

After you apply for a certificate, the CA will review your information. The review may take a while.

The CA will contact you by the phone number you provided to guide you through necessary operations. Make sure that you can be reached by phone during the validation. If the CA cannot contact you in time, the order validation progress may be delayed.

- Validation duration for OV and EV certificates

  For OV or EV certificates, it takes three to seven **working days** for the CA to review your certificate order.

  During the validation, the CA will contact you using the phone number you provided to guide you through necessary operations. Make sure that you can be reached by phone. If the CA cannot contact you in time, the order validation progress may be delayed. Your timely response will effectively shorten the SSL certificate validation progress.

- Validation duration for DV certificates or free certificates

  After the domain ownership is verified, the CA will issue the certificate within one to two working days.

If your domain name contains some sensitive words, such as bank, pay, or live, the manual review mechanism may be triggered, which takes a long time to issue the certificate.

NOTE

A free certificate will be issued within one to two working days after you apply for it. Your certificate may be issued within several hours or two working days, depending on the validation process of the CA.

----End

5.3 What Can I Do After I Submit an SSL Certificate Application?

After purchasing an SSL certificate, you need to apply for the certificate and submit it for approval. The certificate can be used only after it is approved.

After the certificate order is submitted for approval, you can view the next step in **Status/Application Progress** of the certificate in the certificate management list on the SCM console. The following are examples of some important operations:

- **Pending domain name verification**: Domain name verification needs to be completed for a certificate based on the requirements of the CA after a certificate application request is submitted. For details, see **Verifying the Domain Ownership**. The certificate application progress is 40%.
- **Pending organization verification**: If you apply for an OV or EV certificate, the CA checks whether the organization has initiated the certificate application after domain name verification is complete. For details, see **Verify the Organization**. The certificate application progress is 70%.
- **To be issued**: Operations, such as domain name verification and organization verification, have been completed. It is waiting for the CA to approve the certificate. Please wait. The certificate application progress is 90%.

After all information is verified, the certificate status changes to **Issued**.

OV, OV Pro, EV, and EV Pro Certificates

If you have purchased an OV, OV Pro, EV, or EV Pro certificate, you need to apply for the certificate, verify a domain name, and verify the organization as prompted in **Status/Application Progress** of the certificate on the SCM console.

After the preceding operations are complete, you need to wait patiently. The CA (the issuer of the certificate) may need a period of time to approve the certificate. Your digital certificate will be issued after it is approved by the CA.

During the validation, the CA will contact you using the phone number you provided to guide you through necessary operations. Make sure that you can be reached by phone.

DV or DV (Basic) Certificates

If you have purchased a DV or basic DV certificate, you need to apply for the certificate, verify a domain name, and verify the organization as prompted in **Status/Application Progress** of the certificate on the SCM console.

After the domain name verification is complete, your SSL certificate will be issued within one to two working days.

If your domain name contains some sensitive words, such as bank, pay, or live, the manual review mechanism may be triggered, which takes a long time to issue the certificate.

5.4 How Do I Handle the Email or Phone Call from the CA?

If you receive a certificate-related email or call during SSL certificate application, perform the processing according to the call or the instructions in the email as soon as possible after confirming that the certificate-related email or call is from the CA. This is to prevent the certificate approval progress from being affected.

The CA may send an email or make a call to you in the following cases:

- Verifying the domain name ownership
  - Cause: According to the specifications of the CA, you must complete domain name ownership verification to prove that you have the ownership of the bound domain name during SSL certificate application.
  - Solution: Verify the domain name ownership based on the email content. For details, see **Verify the Domain Ownership**.
- Organization Verification
  - Cause: The CA will contact you using the public phone number of the organization to check whether the organization initiates the certificate application, when you apply for an OV or EV certificate.
  - Solution: The CA will contact you using the public phone number of the organization. Please pay attention to and handle it in time.

5.5 Do I Need to Get a Newly Purchased SSL Certificate Approved?

Yes.

No matter whether you have applied for a certificate or not, you need to get a new certificate approved after purchasing it. The certificate application process is the same for each certificate. All certificates must be applied for and approved by the CA.

After purchasing or renewing an SSL certificate, you need to submit an application to the CA for approval. You will obtain the new certificate after the CA approves your application. For the new certificate to take over the job, install it on your server to replace the old one, or replace the old one in the cloud service with the new one.

The certificate can be replaced immediately after a new certificate is issued. The replacement does not affect services.

5.6 What Can I Do When I Fail to Pass the Security Approval?

Problem Description

You may receive the following message if your application for a free DV certificate fails to pass the order approval:

This domain name has not passed the security approval by the CA and you cannot apply for the free testing DV certificate. Please use another domain name or apply for a paid certificate.

Possible Causes

Your domain name contains sensitive words.

Known sensitive words that lead to approval failure are:

- live (excluding top-level domain names ending with **.live**)
- bank
- banc
- ban.c
- alpha
- test
- example
- credit
- Intranet and Internet IP addresses
- Host name
- pw (including top-level domain names ending with **.pw**)
- apple
- ebay
- trust
- root
- amazon
- android
- visa
- google
- discover
- financial
- wordpress
- pal
- hp
- lv

- free
- SCP

CAs do not reveal more details about the validation failure to HUAWEI CLOUD.

Solution

Based on the suggestions from the CA, you can:

- Purchase a paid certificate for the domain name.
- Use a domain name that does not contain the sensitive words described earlier to apply for a testing certificate.

5.7 What Can I Do When a Message Indicating Approval Failure Due to Blank Main Domain Name Is Displayed?

Problem Description

A message indicating approval failure due to blank main domain name is displayed when I choose to upload my own CSR to apply for a certificate.

Possible Causes

You did not set the **Common Name** value properly when you created the CSR file.

Solution

Create and upload a CSR again. Ensure that the **Common Name** field is set correctly.

NOTICE

The **Common Name** value must be the primary domain name associated with the certificate.

To ensure that the CSR content is correct, you are advised to use the system-generated CSR file. The system-generated CSR file supports download of the issued certificate in different formats.

6 SSL Certificate Download, Installation, and Use

6.1 SSL Certificate Download

6.1.1 Can I Download and Use an Issued SSL Certificate for Multiple Times?

You can download and use the certificate repeatedly within its validity period. Upon downloading, you can install and deploy the certificate on your server on any platforms.

NOTE

The domain name to be run on the target server must be the same as the one associated with the certificate. Otherwise, the web browser will display a message indicating that the domain name is insecure.

If a certificate is re-downloaded and installed on another server, the original server is not affected. Your web browser should react normally when you access the associated domain name.

6.1.2 How Do I Obtain the SSL Certificate Private Key File server.key?

The methods for obtaining the certificate private key file **server.key** vary with CSR generation methods (system generated CSR or self-generated CSR) selected when applying for a certificate.

- System generated CSR

  If the CSR is generated by the system, download the certificate file again. For details, see **Downloading an SSL Certificate**.

- **Upload a CSR**

  If the CSR is generated by a user, **server.key** is kept by the user and cannot be downloaded or obtained from SCM.

6.1.3 What Can I Do If My SSL Certificate Fails to be Downloaded?

Problem Description

An issued SSL certificate cannot be downloaded in SCM.

Possible Causes

- Possible cause 1: The certificate is the uploaded certificate.
- Possible cause 2: The account is in arrears or has insufficient permission.
- Possible cause 3: The browser cache is large.

Solution

Perform the following operations based on the possible cause:

- **Possible cause 1: The certificate is the uploaded certificate.**

  SCM does not support the download of uploaded certificates.
- **Possible cause 2: The account is in arrears or has insufficient permission.**

  Solution: If your account is in arrears, top up your account; If your permission is insufficient, contact your administrator to grant required permissions to you.
- **Possible cause 3: The browser cache is large.**

  Solution: Clear the browser cache or use another browser.

  If the fault still persists, submit a service ticket to contact us and describe it in the service ticket (for example, you cannot download a certificate that is not uploaded to SCM but has been issued, or you cannot download a certificate when your account is not in arrears and has the download permission).

6.2 SSL Certificate Installation

6.2.1 On Which Servers Can an SSL Certificate Be Deployed?

There are no restrictions on servers for deploying SSL certificates. You can deploy your SSL certificates on servers on any cloud platforms or on-premises servers.

After obtaining the certificate file, you can deploy it on the server hosting your website or use it in a HUAWEI CLOUD service, such as WAF, ELB, and CDN. For details about how to deploy, see the following topics:

- **How Do I Install an SSL Certificate on a Server?**
- **How Do I Apply an SSL Certificate to Other HUAWEI CLOUD Services?**

6.2.2 How Do I Install an SSL Certificate on a Server?

Installation

After an SSL certificate is issued, you can download and install it on a Tomcat, Nginx, Apache, or IIS server. For more details, see the following topics:

- **Installing an SSL Certificate on a Tomcat Server**
- **Installing an SSL Certificate on an Nginx Server**
- **Installing an SSL Certificate on an Apache Server**
- **Installing an SSL Certificate on an IIS Server**
- **Installing an SSL Certificate on a WebLogic Server**
- **Installing an SSL Certificate on a Resin Server**

We will provide one-to-one professional consulting services to help you deploy SSL certificates on the cloud if you have any problems during certificate installation. Our professional SSL certificate service will help you complete installation and configuration of HTTPS SSL certificates for your website.

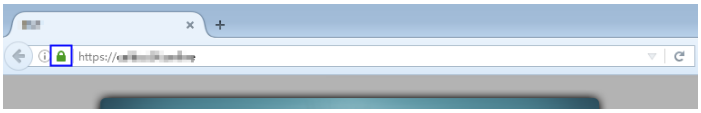
Additionally, we will help you install and configure HTTPS SSL certificates for your websites.

Verifying the Result

Verify that the certificate is installed correctly.

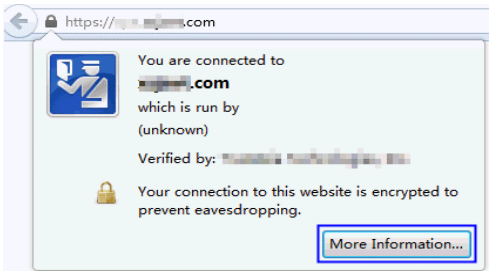
1. In the address box of the browser, enter **https://***Domain name* and press **Enter**.
2. Click  to view the certificate.

   Figure 6-1 Viewing a certificate

3. Click **More Information**.

   Figure 6-2 Clicking More Information

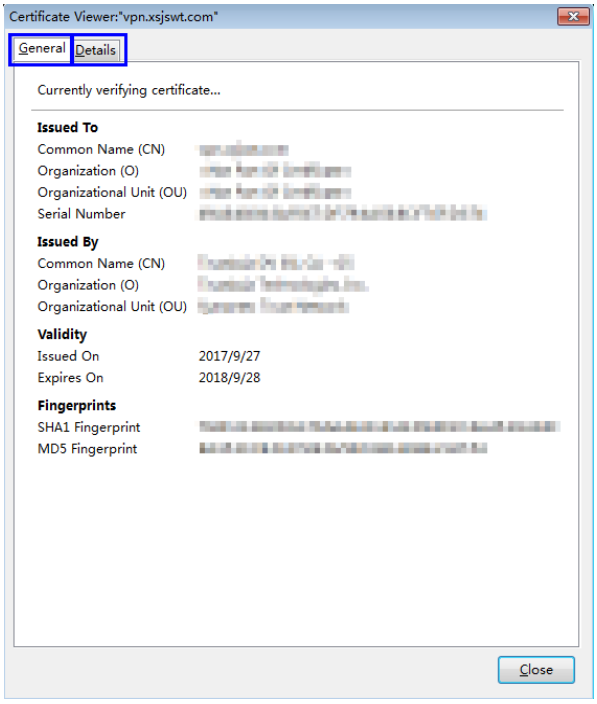
   

4. In the **Page Info** window, choose **Security** > **View Certificate**.

Figure 6-3 Viewing Certificate Information

5. In the displayed **Certificate Viewer** dialog box, click **General** or **Details** to view the general information or details about the certificate. Check whether the certificate is successfully installed based on the information.

Figure 6-4 Certificate information



If the preceding certificate information is correct, the certificate is correctly installed.

6.2.3 How Do I Check Whether the Deployed SSL Certificate Takes Effect?

An SSL certificate is not issued until the CA of the trusted root certificate in web browsers authenticates the server. Therefore, an SSL certificate has two functions: website authentication and transmission encryption.

If you can use **https://** to visit your website after you configure your SSL certificate, the certificate is working properly.

Procedure

In the address bar of the browser, enter **https://***domain name associated with your digital certificate* (for example, https://www.huaweicloud.com) to access your website through HTTPS.

If the website can be accessed and the security lock icon is displayed in the address bar of the browser, the SSL certificate is working properly.

Figure 6-5 SSL certificate working properly

6.2.4 Is the Original SSL Certificate Still Available After a Server IP Address Is Changed?

Yes.

SSL certificates are associated with domain names and are irrelevant to the IP address changes of the server.

They can be used as long as the domain names remain unchanged and can be resolved to the new IP address.

6.2.5 In Which Geographical Locations Can an SSL Certificate Be Used?

There are no restrictions on geographical locations for deploying SSL certificates. SSL certificates can be used for servers in anywhere.

After obtaining the certificate file, you can deploy it on the server hosting your website or use it in a HUAWEI CLOUD service, such as WAF, ELB, and CDN. For details about how to deploy, see the following topics:

- **How Do I Install an SSL Certificate on a Server?**
- **How Do I Apply an SSL Certificate to Other HUAWEI CLOUD Services?**

6.2.6 How Do I Add an SSL Certificate to the Background of a Website Built by Baota?

Before installing a certificate, obtain the certificate file and password file. Perform the following operations based on the value selected for **CSR** when applying for a certificate:

- If you select **System generated CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in **System generated CSR**.
- If you select **Upload a CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in **Upload a CSR**.

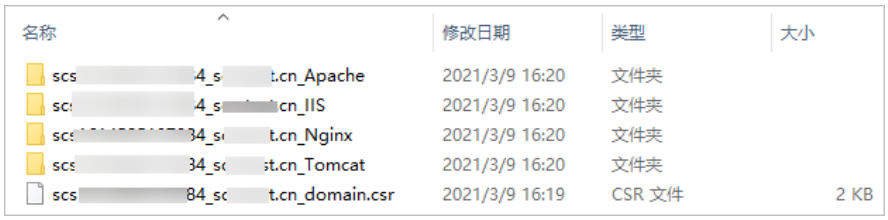
System generated CSR

The Pagoda panel contains the Apache environment and Nginx environment.

- Configuring the SSL Certificate in the Nginx Environment
  a. Decompress the downloaded certificate file on your local PC.

     The downloaded file contains the **Apache**, **IIS**, **Nginx**, and **Tomcat** folders as well as the **domain.csr** file.

     Figure 6-6 Decompressing an SSL certificate package on a local computer

  b. Obtain the certificate file ***Certificate ID_Domain name bound to the certificate*_server.crt** and private key file ***Certificate ID_Domain name bound to the certificate*_server.key** from ***Certificate ID_Domain name bound to the certificate*_Nginx**.

     - The ***Certificate ID_Domain name bound to the certificate*_server.crt** file contains two segments of certificate codes **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----**, which are the server certificate and intermediate CA certificate respectively.
     - The ***Certificate ID_Domain name bound to the certificate*_server.key** file contains a segment of private key code **-----BEGIN RSA PRIVATE KEY-----** and **-----END RSA PRIVATE KEY-----**.

  c. Open the SSL page of BaoTa.

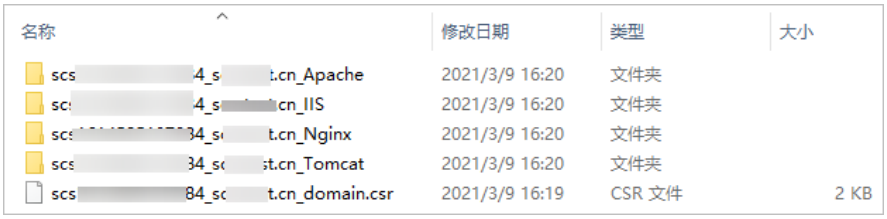
     - Copy the content in ***Certificate ID_Domain name bound to the certificate*_server.key** to the **KEY** text box.
     - Copy the content in ***Certificate ID_Domain name bound to the certificate*_server.crt** to the configuration box of the certificate (in PEM format).

- Configuring the SSL Certificate in the Apache Environment

  a. Decompress the downloaded certificate file on your local PC.

  The downloaded file contains the **Apache**, **IIS**, **Nginx**, and **Tomcat** folders as well as the **domain.csr** file.

  Figure 6-7 Decompressing an SSL certificate package on a local computer

  b. Obtain the certificate files ***Certificate ID_Domain name bound to the certificate*_ca.crt** and ***Certificate ID_Domain name bound to the certificate*_server.crt**, and private key file ***Certificate ID_Domain name bound to the certificate*_server.key** from ***Certificate ID_Domain name bound to the certificate*_Apache**.

  - The ***Certificate ID_Domain name bound to the certificate*_ca.crt** file contains a segment of intermediate CA certificate code **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----**.
  - The ***Certificate ID_Domain name bound to the certificate*_server.crt** file contains a segment of server certificate code **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----**.
  - The ***Certificate ID_Domain name bound to the certificate*_server.key** file contains a segment of private key code **-----BEGIN RSA PRIVATE KEY-----** and **-----END RSA PRIVATE KEY-----**.

  c. Open the SSL page of BaoTa.

  - Copy the content in ***Certificate ID_Domain name bound to the certificate*_server.key** to the **KEY** text box.
  - Combine ***Certificate ID_Domain name bound to the certificate*_server.crt** and ***Certificate ID_Domain name bound to the certificate*_ca.crt** and enter the combined content in the configuration box of the certificate (in PEM format).

CAUTION

- When the **server.crt** and **ca.crt** files are combined, the content of the **server.crt** file must be placed before that of the **ca.crt** file. If the sequence is incorrect, the Apache cannot be started properly.
- If your certificate is not purchased on SCM, the names of the downloaded .crt files are _**public.crt** and _chain.crt. The mappings with the certificate files issued by SCM are as follows:
  - The _**public.crt** file maps to the **server.crt** file.
  - The _**chain.crt** file maps to the **ca.crt** file.

  During the combination, the content of the _**public.crt** file is placed before that of the _**chain.crt** file.

Upload a CSR

In this case, perform the following steps in both the Apache and Nginx environments.

1. Decompress the downloaded certificate package to obtain the ***Certificate ID_Domain name bound to the certificate*_server.pem** file.

   The ***Certificate ID_Domain name bound to the certificate*_server.pem** file contains two segments of certificate codes **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----**, which are the server certificate and intermediate CA certificate respectively.
2. Open the SSL page of the Pagoda website.
   - Copy the content of the private key server.key generated during CSR generation to the **KEY** text box.
   - Copy the content in ***Certificate ID_Domain name bound to the certificate*_server.pem** to the configuration box of the certificate (in PEM format).

6.2.7 How Do I Solve Problems Related to SSL Certificate Installation or Use?

Can Multiple SSL Certificates Be Configured on a Server?

Yes. You can configure multiple certificates on a server.

Can an SSL Certificate Be Deployed on Multiple Servers?

Certificates are bound to domain names or IP addresses, and there is no limit on the number of servers. If the domain name bound to the purchased certificate is used on multiple servers, the purchased certificate takes effect only after being deployed on each server.

Must an SSL Certificate Be Installed on a HUAWEI CLOUD Server?

No.

An SSL certificate you bought on SCM can be used for your server on HUAWEI CLOUD or other platforms.

You can download and use the certificate repeatedly within its validity period. Upon downloading, you can install and deploy the certificate on your server on any platforms.

Can I Use an SSL Certificate on a Cloud Host or Website in Hong Kong (China)?

Yes.

The use of an SSL certificate is not restricted by geographical locations.

Why Cannot I Find the Newly Issued or Uploaded SSL Certificates in Cloud Services Such as WAF, ELB, and CDN?

After an SSL certificate is issued or uploaded, it can be used in other HUAWEI CLOUD services, such as WAF, ELB, and CDN.

Currently, you can push certificates to WAF, ELB, and CDN on HUAWEI CLOUD by one click and complete required configuration in the specific service for the certificate to take effect. If a certificate needs to be pushed to another HUAWEI CLOUD service, you need to download the certificate, upload the certificate to the corresponding service console, and deploy the certificate.

Applying Certificates in WAF, ELB, and CDN

SCM supports the push of certificates to WAF, ELB, and CDN. After the push, the certificates can be configured in the corresponding HUAWEI CLOUD services. After the configuration succeeds, data access through the HUAWEI CLOUD services is more secure.

You need to use SCM to push a certificate to the corresponding HUAWEI CLOUD service, and then configure the certificate in the corresponding HUAWEI CLOUD service to enable the HTTPS service. Perform the following steps to complete the check.

Step 1 Use SCM to push a certificate to other HUAWEI CLOUD services.

For details, see **Pushing an SSL Certificate to Other Cloud Services**.

Step 2 Configure the certificate in the corresponding HUAWEI CLOUD service.

- ELB: If HTTPS data transmission encryption is required, you need to associate a certificate when creating an HTTPS listener. If you choose to push the certificate to ELB in one click, you can select the pushed certificate in ELB. Otherwise, you need to manually upload the certificate. For details about how to set ELB parameters, see **Creating a Certificate**.

  Generally, only server certificates need to be configured to authenticate servers for HTTPS-based business. For some key businesses, such as bank payment, two-way authentication is required for enhanced business security. For details about how to deploy certificates for two-way authentication, see **Mutual Authentication**.
- CDN: To implement HTTPS security acceleration, you need to configure an HTTPS certificate for the acceleration domain name and deploy the certificate

on CDN nodes on the entire network. If you choose to push the certificate to CDN in one click, you can select the pushed certificate in CDN. Otherwise, you need to manually upload the certificate. For details about how to set CDN parameters, see **HTTPS Certificate Requirements**.

- WAF: You need to configure a certificate when adding a domain to WAF if HTTPS is used for communications between the client and WAF. If you choose to push the certificate to WAF in one click, you can select the pushed certificate in WAF. Otherwise, you need to manually upload the certificate. For details, see **Adding a Domain Name**.

  If a certificate has been configured in WAF, you only need to update the certificate. For details, see **Updating a Certificate**.

If you have any questions during the configuration, refer to the corresponding service documentation or consult the corresponding service personnel.

----End

How Do I Export the Certificate Key to WAF After I Purchase an SSL Certificate and WAF on HUAWEI CLOUD?

When configuring WAF, you need to use the key in the SSL certificate. For more details, see **Configuring WAF Certificates**.

If you have any questions during the configuration, refer to the corresponding service documentation or consult the corresponding service personnel.

6.2.8 Will Consulting Services for Installing and Configuring SSL Certificates Be Provided?

HUAWEI CLOUD provides one-to-one professional consulting services to help users deploy SSL certificates on the cloud. Our professional SSL certificate service will help you complete installation and configuration of HTTPS SSL certificates for your website. In addition, the installation and configuration consulting service is charged. You can select the service based on your needs.

Click **Consult Now** in the **One-to-One Consultation** area on the right of the certificate download page if required. After purchasing the service, you can contact technical support.

Additionally, we will help you install and configure HTTPS SSL certificates for your websites.

6.3 SSL Certificate Use

6.3.1 How Do I Configure a Non-HUAWEI CLOUD SSL Certificate for a HUAWEI CLOUD Service?

A non-HUAWEI CLOUD certificate refers to an SSL certificate that is applied for from non-HUAWEI CLOUD and is issued by a CA, for example, an SSL certificate that is applied for from another cloud service provider or an offline certificate provider and issued by a CA.

All SSL certificates are issued by the CA, regardless of platforms on which SSL certificates are applied for.

Any SSL certificates you requested from any platforms can be used in HUAWEI CLOUD after the certificate is issued by a trusted CA. However, the one-click push function cannot be used to push these certificates to HUAWEI CLOUD services, such as WAF, ELB, and CDN. Therefore, you are advised to use an SSL certificate applied for on HUAWEI CLOUD so that you can push the certificate to the corresponding HUAWEI CLOUD service in one-click mode. After the certificate is pushed, you can directly select the pushed certificate from the corresponding HUAWEI CLOUD service, and you do not need to import the certificate separately. For example, after a certificate is issued, you can push the certificate to WAF with just one click. When you add a domain name to WAF, you can directly select the pushed certificate.

To configure a non-HUAWEI CLOUD SSL certificate for a HUAWEI CLOUD service, perform the following operations as required:

Table 6-1 Scenario description

Scenario	Procedure
Managing all you certificates on HUAWEI CLOUD SCM	Upload SSL certificates to SCM. For details, see **Uploading an External Certificate**.

Scenario	Procedure
Using certificates in WAF, ELB, and CDN	If you have any problem during the configuration, see the corresponding service documentation to solve the problem. • ELB: If HTTPS data transmission encryption is required, you need to associate a certificate when creating an HTTPS listener. If you choose to push the certificate to ELB in one click, you can select the pushed certificate in ELB. Otherwise, you need to manually upload the certificate. For details about how to set ELB parameters, see **Creating a Certificate**. Generally, only server certificates need to be configured to authenticate servers for HTTPS-based business. For some key businesses, such as bank payment, two-way authentication is required for enhanced business security. For details about how to deploy certificates for two-way authentication, see **Mutual Authentication**. • CDN: To implement HTTPS security acceleration, you need to configure an HTTPS certificate for the acceleration domain name and deploy the certificate on CDN nodes on the entire network. If you choose to push the certificate to CDN in one click, you can select the pushed certificate in CDN. Otherwise, you need to manually upload the certificate. For details about how to set CDN parameters, see **HTTPS Certificate Requirements**. • WAF: You need to configure a certificate when adding a domain to WAF if HTTPS is used for communications between the client and WAF. If you choose to push the certificate to WAF in one click, you can select the pushed certificate in WAF. Otherwise, you need to manually upload the certificate. For details, see **Adding a Domain Name**. If a certificate has been configured in WAF, you only need to update the certificate. For details, see **Updating a Certificate**.
Using a certificate in other HUAWEI CLOUD products	Download the certificate, upload the certificate to the corresponding service console, and deploy the certificate. If you have any questions during the configuration, refer to the corresponding service documentation or contact the corresponding service personnel.

If you need to install an SSL certificate on a server, configure the certificate based on the server type. For details, see **How Do I Install an SSL Certificate on a Server?**

6.3.2 How Do I Apply an SSL Certificate to Other HUAWEI CLOUD Services?

After an SSL certificate is issued or uploaded, it can be used in other HUAWEI CLOUD services, such as WAF, ELB, and CDN.

Currently, you can push certificates to WAF, ELB, and CDN on HUAWEI CLOUD by one click and complete required configuration in the specific service for the certificate to take effect. If a certificate needs to be pushed to another HUAWEI CLOUD service, you need to download the certificate, upload the certificate to the corresponding service console, and deploy the certificate.

Applying Certificates in WAF, ELB, and CDN

SCM supports the push of certificates to WAF, ELB, and CDN. After the push, the certificates can be configured in the corresponding HUAWEI CLOUD services. After the configuration succeeds, data access through the HUAWEI CLOUD services is more secure.

You need to use SCM to push a certificate to the corresponding HUAWEI CLOUD service, and then configure the certificate in the corresponding HUAWEI CLOUD service to enable the HTTPS service. Perform the following steps to complete the check.

Step 1 Use SCM to push a certificate to other HUAWEI CLOUD services.

For details, see **Pushing an SSL Certificate to Other Cloud Services**.

Step 2 Configure the certificate in the corresponding HUAWEI CLOUD service.

- ELB: If HTTPS data transmission encryption is required, you need to associate a certificate when creating an HTTPS listener. If you choose to push the certificate to ELB in one click, you can select the pushed certificate in ELB. Otherwise, you need to manually upload the certificate. For details about how to set ELB parameters, see **Creating a Certificate**.

  Generally, only server certificates need to be configured to authenticate servers for HTTPS-based business. For some key businesses, such as bank payment, two-way authentication is required for enhanced business security. For details about how to deploy certificates for two-way authentication, see **Mutual Authentication**.
- CDN: To implement HTTPS security acceleration, you need to configure an HTTPS certificate for the acceleration domain name and deploy the certificate on CDN nodes on the entire network. If you choose to push the certificate to CDN in one click, you can select the pushed certificate in CDN. Otherwise, you need to manually upload the certificate. For details about how to set CDN parameters, see **HTTPS Certificate Requirements**.
- WAF: You need to configure a certificate when adding a domain to WAF if HTTPS is used for communications between the client and WAF. If you choose to push the certificate to WAF in one click, you can select the pushed certificate in WAF. Otherwise, you need to manually upload the certificate. For details, see **Adding a Domain Name**.

If a certificate has been configured in WAF, you only need to update the certificate. For details, see **Updating a Certificate**.

If you have any questions during the configuration, refer to the corresponding service documentation or consult the corresponding service personnel.

----End

Applying Certificates in Other Cloud Products

If you want to deploy your certificate to other HUAWEI CLOUD services than the previously mentioned ones, download the certificate to your local PC and then upload and deploy it on the management console of the desired cloud service.

6.3.3 Which Region Will a Certificate Be Pushed to When I Push the SSL Certificate to Another HUAWEI CLOUD Service in One Click?

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

The regions to which certificates are to be pushed vary depending on services.

- When a certificate is to be pushed to ELB and WAF, you can select a target region. After the region is selected and **Push** is clicked, SCM pushes the certificate to the selected region.
- If a certificate is to be pushed to CDN, there is no need to select a region, and SCM directly pushes the certificate to CDN.

If you have not purchased the cloud service or the service is not available for the domain name associated with your certificate, do not push the certificate to it because the pushing will fail.

6.3.4 Is the HTTPS Service Automatically Enabled After an SSL Certificate Is Pushed to a HUAWEI CLOUD Service in One Click?

No.

After using SCM to push a certificate to a HUAWEI CLOUD service, you need to set parameters on the management console of the corresponding HUAWEI CLOUD service. In addition, you need to confirm that your website is ready for HTTPS.

- ELB: If HTTPS data transmission encryption is required, you need to associate a certificate when creating an HTTPS listener. If you choose to push the certificate to ELB in one click, you can select the pushed certificate in ELB. Otherwise, you need to manually upload the certificate. For details about how to set ELB parameters, see **Creating a Certificate**.

  Generally, only server certificates need to be configured to authenticate servers for HTTPS-based business. For some key businesses, such as bank payment, two-way authentication is required for enhanced business security. For details about how to deploy certificates for two-way authentication, see **Mutual Authentication**.

- CDN: To implement HTTPS security acceleration, you need to configure an HTTPS certificate for the acceleration domain name and deploy the certificate on CDN nodes on the entire network. If you choose to push the certificate to CDN in one click, you can select the pushed certificate in CDN. Otherwise, you need to manually upload the certificate. For details about how to set CDN parameters, see **HTTPS Certificate Requirements**.
- WAF: You need to configure a certificate when adding a domain to WAF if HTTPS is used for communications between the client and WAF. If you choose to push the certificate to WAF in one click, you can select the pushed certificate in WAF. Otherwise, you need to manually upload the certificate. For details, see **Adding a Domain Name**.

  If a certificate has been configured in WAF, you only need to update the certificate. For details, see **Updating a Certificate**.

If you have any questions during the configuration, refer to the corresponding service documentation or contact the service personnel.

6.3.5 How Do I Solve the Problem That Occurs When I Use Certificates in WAF, ELB, or CDN?

If you encounter any problems when using certificates in WAF, ELB, and CDN, submit a service ticket to the involved service for consultation.

SCM supports one-click push of issued certificates to the WAF, ELB, or CDN service. After the push, you need to configure information in the corresponding service.

If you have any questions during the push or configuration process, refer to the WAF, ELB, or CDN documentation or submit a service ticket to the involved service for help.

If the problem persists, submit a service ticket to WAF, ELB, or CDN for help.

Follow-up Procedure

Push the certificate to WAF, ELB, and CDN with just a few clicks. For details, see **Pushing an SSL Certificate to Other Cloud Services**.

After the push, you need to complete required configuration in the corresponding service.

If you have any questions during the configuration, refer to the corresponding service documentation or contact the service personnel.

- ELB: If HTTPS data transmission encryption is required, you need to associate a certificate when creating an HTTPS listener. If you choose to push the certificate to ELB in one click, you can select the pushed certificate in ELB. Otherwise, you need to manually upload the certificate. For details about how to set ELB parameters, see **Creating a Certificate**.

  Generally, only server certificates need to be configured to authenticate servers for HTTPS-based business. For some key businesses, such as bank payment, two-way authentication is required for enhanced business security. For details about how to deploy certificates for two-way authentication, see **Mutual Authentication**.
- CDN: To implement HTTPS security acceleration, you need to configure an HTTPS certificate for the acceleration domain name and deploy the certificate

on CDN nodes on the entire network. If you choose to push the certificate to CDN in one click, you can select the pushed certificate in CDN. Otherwise, you need to manually upload the certificate. For details about how to set CDN parameters, see **HTTPS Certificate Requirements**.

- WAF: You need to configure a certificate when adding a domain to WAF if HTTPS is used for communications between the client and WAF. If you choose to push the certificate to WAF in one click, you can select the pushed certificate in WAF. Otherwise, you need to manually upload the certificate. For details, see **Adding a Domain Name**.

  If a certificate has been configured in WAF, you only need to update the certificate. For details, see **Updating a Certificate**.

6.3.6 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?**

Digital certificates purchased through HUAWEI CLOUD SCM can be pushed to CDN with just a few clicks. After the push, you can select the corresponding certificate in the CDN configuration and do not need to manually import the certificate, avoiding the reporting of the error. Therefore, you are advised to purchase certificates in HUAWEI CLOUD SCM.

6.3.7 What Can I Do If an Error Occurs When an SSL Certificate Applied By Uploading a CSR Is Pushed to WAF, ELB, or CDN?

If you select **Upload a CSR** for **CSR** when applying for a certificate, the certificate file does not contain the certificate private key file after the certificate is issued. As a result, an error is reported when you push the certificate to WAF, ELB, or CDN.

When you manually generate a CSR file, a private key file is also generated. Although you do not need to upload the private key file when uploading the CSR file, you need to keep the private key file properly.

SCM makes it easier for you to quickly deploy such certificates in WAF, ELB, and CDN. Alternatively, you can directly deploy such certificates in those services. The detailed operations are as follows:

- Using SCM

a. Download a certificate.

   Download an issued certificate to the local PC. For details, see **Downloading an SSL Certificate**.

b. Upload the certificate.

   Upload the certificate downloaded in **a** and the local private key file to SCM. For details, see **Uploading an External Certificate**.

c. Push the certificate to WAF, ELB, or CDN.

   Push the uploaded certificate to WAF, ELB, and CDN with just few clicks. For details, see **Pushing an SSL Certificate to Other Cloud Services**.

   After the push, you need to complete required configuration in the corresponding service.

   - ELB: If HTTPS data transmission encryption is required, you need to associate a certificate when creating an HTTPS listener. If you choose to push the certificate to ELB in one click, you can select the pushed certificate in ELB. Otherwise, you need to manually upload the certificate. For details about how to set ELB parameters, see **Creating a Certificate**.

     Generally, only server certificates need to be configured to authenticate servers for HTTPS-based business. For some key businesses, such as bank payment, two-way authentication is required for enhanced business security. For details about how to deploy certificates for two-way authentication, see **Mutual Authentication**.

   - CDN: To implement HTTPS security acceleration, you need to configure an HTTPS certificate for the acceleration domain name and deploy the certificate on CDN nodes on the entire network. If you choose to push the certificate to CDN in one click, you can select the pushed certificate in CDN. Otherwise, you need to manually upload the certificate. For details about how to set CDN parameters, see **HTTPS Certificate Requirements**.

   - WAF: You need to configure a certificate when adding a domain to WAF if HTTPS is used for communications between the client and WAF. If you choose to push the certificate to WAF in one click, you can select the pushed certificate in WAF. Otherwise, you need to manually upload the certificate. For details, see **Adding a Domain Name**.

     If a certificate has been configured in WAF, you only need to update the certificate. For details, see **Updating a Certificate**.

- Not using SCM

  a. Download a certificate.

     Download an issued certificate to the local PC. For details, see **Downloading an SSL Certificate**.

  b. Upload the certificate to WAF, ELB, and CDN.

     Upload the certificate downloaded in **a** to a specific service, such as WAF, ELB, and CDN. For details, see the corresponding service documentation.

6.3.8 How Do I Use an SSL Certificate After It Is Issued?

The certificate will be issued after being approved by the CA. The certificate can be used upon issuance.

- Certificates requested through SCM on HUAWEI CLOUD
  - SCM allows you to use those certificates to HUAWEI CLOUD WAF, ELB, and CDN with just a few clicks. For more details, see **Pushing an SSL Certificate to Other Cloud Services**.
  - You can also use those certificates to other cloud services. Download the certificate, upload the certificate to the service on the corresponding console, and deploy the certificate.
  - SCM also allows you to deploy those certificates on servers. You need to download the certificate to the local PC and deploy the certificate on the corresponding server by referring to **How Do I Install an SSL Certificate on a Server?**
- Certificates requested through other platforms
  - To deploy those certificates on a cloud service, you need to download the certificate, upload the certificate to the service on the corresponding console, and then deploy the certificate.
  - SCM also allows you to deploy those certificates on servers. You need to download the certificate to the local PC and deploy the certificate on the corresponding server by referring to **How Do I Install an SSL Certificate on a Server?**

6.3.9 What Can I Do If My SSL Certificate Cannot Be Pushed?

With SCM, you can push SSL certificates to other HUAWEI CLOUD services, such as Web Application Firewall (WAF), Elastic Load Balance (ELB), and Content Delivery Network (CDN) with just a few clicks. However, the certificate will fail to be pushed in the following scenarios:

- Currently, SSL certificates can be pushed only to the **default** enterprise projects of WAF, ELB, and CDN. If you are using other projects, you cannot directly push certificates to them.

  Solution

  Download the certificate, upload the certificate to the corresponding service console, and deploy the certificate.
- For CDN, SSL certificate names cannot be the same as those of existing SSL certificates. Otherwise, they will fail to be pushed.

  Solution

  Change the SSL certificate name and push the certificate again.
- If you choose to manually generate a CSR when applying for a certificate, the issued certificate **cannot** be pushed to other cloud services.

  Solution

  Download the certificate, upload the certificate to the corresponding service console, and deploy the certificate.
- If you have not purchased the desired cloud product or the domain name associated with the digital certificate is not enabled in the cloud product, the push may fail.

Solution

Purchase the cloud service, or enabled the domain name in the cloud product.

- A certificate can only be pushed to a product once in SCM. Any certificate that has been pushed or uploaded to a cloud product cannot be pushed again.

  Solution

  Check whether the SSL certificate has been pushed before. If it has, you do not need to push it again.

6.3.10 How Do I Solve Problems Related to SSL Certificate Uploading?

If you encounter problems related to certificate uploading, use a specific solution based on your situation.

Which Format Is Required of a Certificate to Be Uploaded to SCM?

Currently, only certificates in the PEM format can be uploaded to SCM.

Certificates in other formats can be uploaded only after being converted into those in the PEM format. For details, see **How Do I Convert a Certificate to PEM Format?**

Can I Download an Uploaded Certificate?

Your uploaded digital certificate and private key will be encrypted and stored on HUAWEI CLOUD. You cannot download the certificate and private key again. Therefore, back up and store your private key.

Is the Use of Certificate on the Original Platform Affected After Uploading?

No. Uploading a certificate does not affect the use of it on the original platform.

Certificate uploading can be regarded as copying a local certificate to HUAWEI CLOUD. The copy operation does not affect the use of the certificate.

Why Is a Message Indicating Insecurity Displayed When I Access the Domain Name After the Certificate Is Uploaded?

After a certificate is uploaded, you need to push the certificate to the corresponding cloud product and complete required configuration.

SCM supports the push of certificates to WAF, ELB, and CDN. After the push, the certificates can be configured in the corresponding HUAWEI CLOUD services. After the configuration succeeds, data access through the HUAWEI CLOUD services is more secure.

You need to use SCM to push a certificate to the corresponding HUAWEI CLOUD service, and then configure the certificate in the corresponding HUAWEI CLOUD service to enable the HTTPS service. Perform the following steps to complete the check.

Step 1 Use SCM to push a certificate to other HUAWEI CLOUD services.

For details, see **Pushing an SSL Certificate to Other Cloud Services**.

Step 2 Configure the certificate in the corresponding HUAWEI CLOUD service.

- ELB: If HTTPS data transmission encryption is required, you need to associate a certificate when creating an HTTPS listener. If you choose to push the certificate to ELB in one click, you can select the pushed certificate in ELB. Otherwise, you need to manually upload the certificate. For details about how to set ELB parameters, see **Creating a Certificate**.

  Generally, only server certificates need to be configured to authenticate servers for HTTPS-based business. For some key businesses, such as bank payment, two-way authentication is required for enhanced business security. For details about how to deploy certificates for two-way authentication, see **Mutual Authentication**.
- CDN: To implement HTTPS security acceleration, you need to configure an HTTPS certificate for the acceleration domain name and deploy the certificate on CDN nodes on the entire network. If you choose to push the certificate to CDN in one click, you can select the pushed certificate in CDN. Otherwise, you need to manually upload the certificate. For details about how to set CDN parameters, see **HTTPS Certificate Requirements**.
- WAF: You need to configure a certificate when adding a domain to WAF if HTTPS is used for communications between the client and WAF. If you choose to push the certificate to WAF in one click, you can select the pushed certificate in WAF. Otherwise, you need to manually upload the certificate. For details, see **Adding a Domain Name**.

  If a certificate has been configured in WAF, you only need to update the certificate. For details, see **Updating a Certificate**.

If you have any questions during the configuration, refer to the corresponding service documentation or contact the corresponding service personnel.

----End

6.4 Troubleshooting

6.4.1 What Can I Do If the Browser Displays a Message Indicating that the SSL Certificate Is Untrusted?

Check the brand (CA) of your certificate and the type of the terminal you are using.

Certificates issued by some CAs are not supported by some terminals. For details, see the certificate introduction of the CA on the official website.

Currently, DigiCert, GlobalSign, and GeoTrust certificates are supported by mainstream devices in the market.

NOTE

Google Chrome 53 is incompatible with DigiCert and GeoTrust certificates due to known issues.

- Chrome 53 Bug Affecting DigiCert SSL/TLS Certificates
- Warning | Certificate Transparency error with Chrome 53

Troubleshooting Procedure

After you rule out the possibility of incompatibility between the certificate and the terminal, locate the cause in the following procedure:

1. Perform a check using the **GlobalSign SSL Server Test** tool.
   - If the certificate authority, certificate type, or domain name in the check result is inconsistent with that in your order, check the certificate configuration on your server.
   - If the check result shows that the certificate chain is incomplete, check whether the certificate configuration is correct.

   NOTICE

   A PEM certificate provided by SCM contains two parts and neither can be lost. If there is a blank line between the two parts, delete the blank line. After the configuration modification is complete, restart the web service and check the configuration again.
2. Ensure that insecure protocols, such as SSLv3, have been disabled in your digital certificate configuration.
3. Check whether some HTTP resources are referenced on your web page. Some browsers regard the reference of HTTP resources by HTTPS sites as insecure.
4. If a domain name has multiple servers, check whether the certificate is correctly deployed on each server.

6.4.2 Why Does the Website Still Display a Message Indicating that the Website Is Insecure After an SSL Certificate Is Deployed?

Problem Description

After HTTPS is configured, the access to the website is still blocked, and a message is displayed indicating that the website is insecure.

Possible Causes

- **Possible cause 1**: The accessed domain name is not the same as the one associated with the purchased certificate.
- **Possible cause 2**: Non-HTTPS items, including images, CSS files, and JavaScript files, are incorrectly referenced to the website.
- **Possible cause 3**: The certificate has expired.
- **Possible cause 4**: The browser cache is large.
- **Possible cause 5**: Unknown

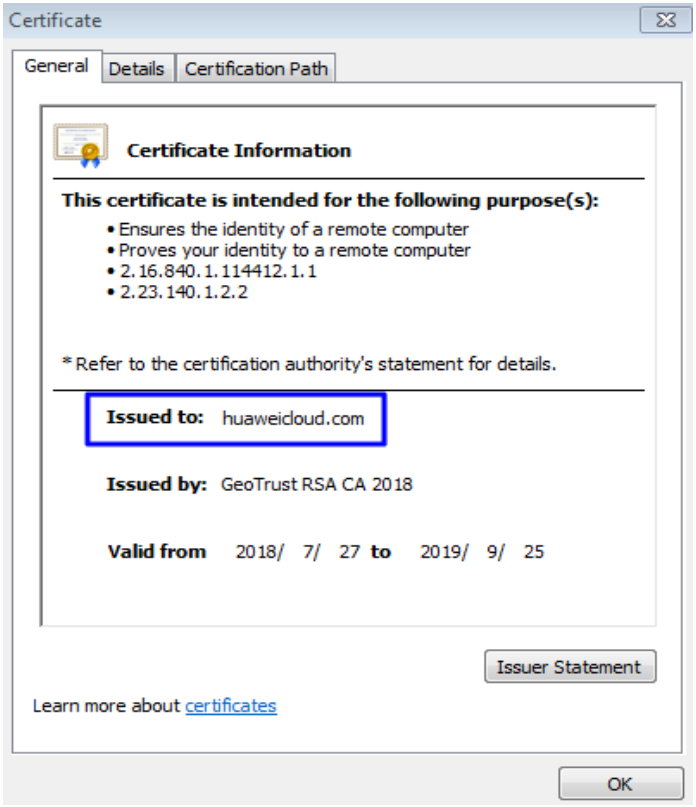
Solution

Perform the following operations based on the possible cause:

- **Possible cause 1**: The accessed domain name is not the same as the one associated with the purchased certificate.

  For example, the associated domain name is **huaweicloud.com**, but you are accessing **https://yun.huaweicloud.com/**. The certificate information is shown in **Figure 6-8**.

  Figure 6-8 Certificate information

  The purchased certificate is associated with **huaweicloud.com** and therefore it does not protect **yun.huaweicloud.com**. Either **huaweicloud.com** or **yun.huaweicloud.com** counts as a domain name. A single-domain certificate protects only the associated domain name.

  Solution:

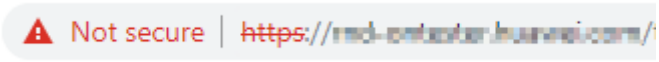
  You are advised to request a certificate and associate it with the domain name you want to protect. For example, you can purchase a certificate and associate it with **yun.huaweicloud.com**. Then you can access **https://yun.huaweicloud.com/**.

  If you have multiple domain names at the same level to be associated, for example, **yun.huaweicloud.com**, **test.huaweicloud.com**, and **example.huaweicloud.com**, which are all under ***.huaweicloud.com**, select **Wildcard** for the domain type when purchasing a certificate and associate the certificate with the wildcard domain name ***.huaweicloud.com**.

- **Possible cause 2**: Non-HTTPS items, including images, CSS files, and JavaScript files, are incorrectly referenced to the website.

  When insecure HTTP items are referenced to an HTTPS web page, such as images, JavaScript files, CSS files, audio files, video files, and flash files, HTTP

images referenced in CSS files, and insecure items written in JavaScript scripts are blocked by the browser by default. If you forcibly load the web page, a message is displayed indicating insecurity.

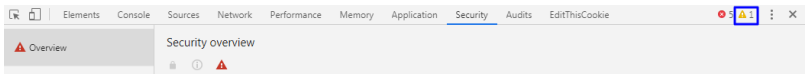


Solution:

a. Open a web browser (Google Chrome 74 is used as an example) and access the web page to be checked.

b. Press **F12** to access **Developer Tools**. In the upper right corner, you can see which insecure web links affect the website.

Figure 6-9 Checking insecure links



c. Find the reported insecure link and make sure it is an HTTP link.

Figure 6-10 Checking insecure items

- If the web link is useless, delete it. Then check whether the insecure link is cleared successfully.
- If the web link is important and cannot be deleted, change the HTTP path to an HTTPS path.

NOTICE

If your website involves data like APIs, you are advised to contact the vendor that provides the invoked data. This is because APIs are important and cannot be modified randomly. If the vendor does not perform HTTPS authentication, you are advised not to perform authentication to prevent any errors in invoked data. For details, contact your vendor.

d. After the processing is complete, clear the browser cache and access the website again.

- **Possible cause 3**: The certificate has expired.

  If your SSL certificate has expired, a message will be displayed indicating insecurity when you access the associated domain name.

  Solution:

  Purchase a new certificate. For details, see **What Can I Do If My SSL Certificate Expired?**

- **Possible cause 4**: The browser cache is large.

  Solution: Clear the browser cache or use another browser.

- **Possible cause 5**: Unknown

  Solution:

  HUAWEI CLOUD provides one-to-one professional consulting services to help you deploy SSL certificates on the cloud. You can buy the service in marketplace if needed.

6.4.3 Why Is My Website Inaccessible by Domain Name After an SSL Certificate Is Installed?

Problem Description

After an SSL certificate is deployed on a server, you enter **https://***Associated domain name* in the address bar of a web browser but the website fails to be opened.

Possible Causes

- **Possible cause 1**: Port 443 is disabled.
- **Possible cause 2**: The configuration file is not correct.

Solution

Perform the following operations based on the possible cause:

- **Possible cause 1**: Port 443 is disabled.

  Solution:

  Enable port 443 on the server where the SSL certificate is installed and add port 443 to the security group to ensure that HTTPS can be enabled after the installation.

- **Possible cause 2**: The configuration file is not correct.

  Solution: On the right of the certificate download page on the SCM console, click **Consult Now** in the **One-to-One Consultation** area. After purchasing the service, you can contact technical support.

  Additionally, we will help you install and configure HTTPS SSL certificates for your websites.

6.4.4 Why Does the HTTPS Access Speed Become Slower After an SSL Certificate Is Installed?

After an SSL certificate is installed, HTTPS requires several more handshakes than HTTP during website access. The handshake phase of HTTPS is time-consuming, and RSA verification is required. Therefore, the access speed of HTTPS is slower than that of HTTP after SSL certificates are used.

In addition, processing workload of the CPU of your server is increased slightly because each SSL connection needs to be encrypted and decrypted.

To reduce the pressure on the server, do the following:

1. Use SSL only for pages that need to be encrypted, for example, **https://www.domain.com/login.asp**. Do not use **https://** for all pages, especially home pages with the largest number of visits.

2. Avoid using large-sized image files or other files on pages that use SSL. Use concise pages with few images instead.

6.4.5 Why Does the Browser Prompt a Not Secure Warning to Visitors After I Configure an SSL Certificate for the Website?

Symptom

An SSL certificate has been configured in ELB. When some visitors access the domain name, a message is displayed indicating that the domain name is untrusted, and some computers on the same office network report that "Windows does not have enough information to verify the certificate."

Cause

The root certificate fails to be identified by the computer because the browser version on the computer is not updated in a timely manner.

Solution

Update the browser to the latest version. To access your server more stably, mainstream browsers, such as Google Chrome and Internet Explorer, are recommended.

6.4.6 What Can I Do If the Browser Displays "Your Connection Is Not a Private Connection"?

Symptom

In November 2016, some users reported that the **NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED** error occurred when they accessed the HTTPS website using Chrome 53 or QQ 9.5.1 (based on Chromium 53). As a result, the HTTPS website was abnormal.

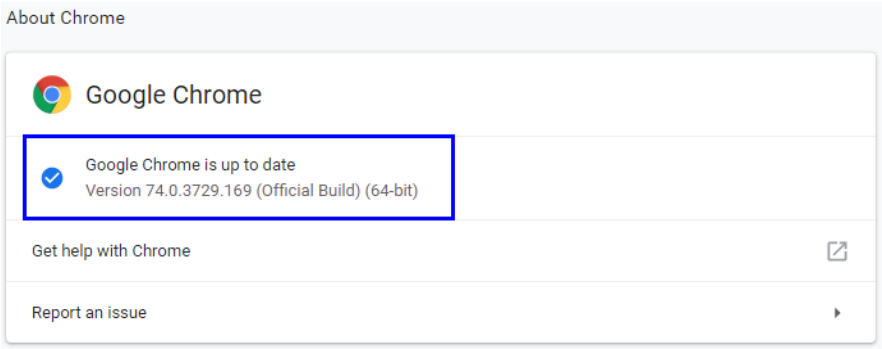
Solution

- For Google Chrome 53 users, Use other versions of Google Chrome browsers to access the HTTPS website.

  To check the version of Google Chrome, perform the following steps:

  a. Open Google Chrome, click  in the upper right corner of the window, and choose **Help** > **About Chrome**.
  b. On the page that is displayed, view the version of Google Chrome.

Figure 6-11 Version of Google Chrome



- For QQ browser version 9.5.1 (based on Chromium 53) users, update the QQ browser to the latest version. This issue has been resolved in the latest version.

  To check the version of QQ browser, perform the following steps:

  a. Open the QQ browser, click ☰ in the upper right corner of the browser, and choose **Help** > **About**.
  b. In the displayed dialog box, check the version of the QQ browser.

This problem is not reported for other browsers.

6.4.7 Will the Browser Prompt A Warning Indicating the Deployed SSL Certificate Is Not Secure?

No.

Free testing certificates are used only to verify the domain names of the websites and secure the transmission. The browser will not prompt a Not Secure warning when the certificate is correctly installed and within the validity period.

The paid certificates will perform strict identity authentication on the applicant and provides strong communication link encryption function to protect sensitive data transmission on internal and external networks. The browser will not prompt a Not Secure warning when the certificate is correctly installed and within the validity period.

7 Certificate Validity Period

7.1 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.

The renewal entry will be available for 30 calendar days before an SSL certificate expires. For details, see **Renewing an SSL Certificate**.

SCM will notify you of certificate expiration 30 days before the certificate expires.

- For certificates you purchase through SCM, SCM automatically notifies you of the expiration by email and SMS two months, one month, and one week before a certificate expires and again when the certificate actually expired.
- You need to configure an expiration reminder for uploaded certificate so that the system can send emails and SMS messages to notify you of the certificate expiration. For details, see **How Do I Configure a Certificate Expiration Notification?**

After purchasing or renewing an SSL certificate, you need to submit an application to the CA for approval. You will obtain the new certificate after the CA approves your application. For the new certificate to take over the job, install it on your server to replace the old one, or replace the old one in the cloud service with the new one.

The certificate can be replaced immediately after a new certificate is issued. The replacement does not affect services.

NOTE

- You are advised to purchase or renew an SSL certificate at least three to ten working days before the current one expires.
- DigiCert, GlobalSign, and GeoTrust are available CAs in HUAWEI CLOUD SCM. You can request a new certificate 90 days before the current one expires.

  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. You are advised to apply for a certificate 30 days before the original one expires.

  For example, if your current certificate expires on October 1, 2019. 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, HUAWEI CLOUD will work with you to communicate and negotiate with the CA.

- To install the certificate, refer to the corresponding FAQ.
  - **Installing an SSL Certificate on a Tomcat Server**
  - **Installing an SSL Certificate on an Nginx Server**
  - **Installing an SSL Certificate on an Apache Server**
  - **Installing an SSL Certificate on an IIS Server**
  - **Installing an SSL Certificate on a WebLogic Server**
  - **Installing an SSL Certificate on a Resin Server**
- For details about how to use certificates in other HUAWEI CLOUD services, see **How Do I Apply an SSL Certificate to Other HUAWEI CLOUD Services?**

7.2 How Long Is the Validity Period of an SSL Certificate?

An SSL certificate is valid for one year. Once an SSL certificate expires, it cannot be used.

You can renew an SSL certificate before it expires. For details, see **Renewing an SSL Certificate**.

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.

When Will a Notification Be Sent Before a Certificate Expires?

SCM will notify you of certificate expiration 30 days before the certificate expires.

- For certificates you purchase through SCM, SCM automatically notifies you of the expiration by email and SMS two months, one month, and one week before a certificate expires and again when the certificate actually expired.
- You need to configure an expiration reminder for uploaded certificate so that the system can send emails and SMS messages to notify you of the certificate expiration. For details, see **How Do I Configure a Certificate Expiration Notification?**

The renewal entry will be available for 30 calendar days before an SSL certificate expires. For details, see **Renewing an SSL Certificate**.

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

SSL certificates have a validity period. Expired SSL certificates cannot secure your website communication connections. If your SSL certificate expires, a message indicating that your website is insecure or cannot be accessed will be displayed to visitors. This will deteriorate your website services and trustfulness.

You can renew an SSL certificate on the console before it expires. The renewal entry will be available for 30 calendar days before an SSL certificate expires.

SCM will notify you of certificate expiration 30 days before the certificate expires.

- For certificates you purchase through SCM, SCM automatically notifies you of the expiration by email and SMS two months, one month, and one week before a certificate expires and again when the certificate actually expired.
- You need to configure an expiration reminder for uploaded certificate so that the system can send emails and SMS messages to notify you of the certificate expiration. For details, see **How Do I Configure a Certificate Expiration Notification?**

After purchasing or renewing an SSL certificate, you need to submit an application to the CA for approval. You will obtain the new certificate after the CA approves your application. For the new certificate to take over the job, install it on your server to replace the old one, or replace the old one in the cloud service with the new one.

The certificate can be replaced immediately after a new certificate is issued. The replacement does not affect services.

NOTE

- You are advised to purchase or renew an SSL certificate at least three to ten working days before the current one expires.
- DigiCert, GlobalSign, and GeoTrust are available CAs in HUAWEI CLOUD SCM. You can request a new certificate 90 days before the current one expires.

  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. You are advised to apply for a certificate 30 days before the original one expires.

  For example, if your current certificate expires on October 1, 2019. 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, HUAWEI CLOUD will work with you to communicate and negotiate with the CA.

7.4 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.

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.

7.5 Validity Periods and Replacement of the Current and New SSL Certificates

Validity Periods of Current and New SSL Certificates

DigiCert, GlobalSign, and GeoTrust are available CAs in HUAWEI CLOUD SCM. You can request a new certificate 90 days before the current one expires.

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

- Certificate details have 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. You are advised to apply for a certificate 30 days before the original one expires.

For example, if your current certificate expires on October 1, 2019. 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, HUAWEI CLOUD will work with you to communicate and negotiate with the CA.

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

- The certificate details, such as the domain name, certificate type, or company name, is changed.

  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?

After purchasing or renewing an SSL certificate, you need to submit an application to the CA for approval. You will obtain the new certificate after the CA approves your application. For the new certificate to take over the job, install it on your server to replace the old one, or replace the old one in the cloud service with the new one.

The certificate can be replaced immediately after a new certificate is issued. The replacement does not affect services.

7.6 How Can I Renew an SSL Certificate?

An SSL certificate is a one-time product and has a validity period. An expired certificate is invalid. You can renew a certificate before it expires. For details, see **Renewing an SSL Certificate**.

SCM will notify you of certificate expiration 30 days before the certificate expires.

- For certificates you purchase through SCM, SCM automatically notifies you of the expiration by email and SMS two months, one month, and one week before a certificate expires and again when the certificate actually expired.
- You need to configure an expiration reminder for uploaded certificate so that the system can send emails and SMS messages to notify you of the certificate expiration. For details, see **How Do I Configure a Certificate Expiration Notification?**

After purchasing or renewing an SSL certificate, you need to submit an application to the CA for approval. You will obtain the new certificate after the CA approves your application. For the new certificate to take over the job, install it on your server to replace the old one, or replace the old one in the cloud service with the new one.

The certificate can be replaced immediately after a new certificate is issued. The replacement does not affect services.

NOTE

- You are advised to purchase or renew an SSL certificate at least three to ten working days before the current one expires.
- DigiCert, GlobalSign, and GeoTrust are available CAs in HUAWEI CLOUD SCM. You can request a new certificate 90 days before the current one expires.

  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. You are advised to apply for a certificate 30 days before the original one expires.

  For example, if your current certificate expires on October 1, 2019. 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, HUAWEI CLOUD will work with you to communicate and negotiate with the CA.

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:

- To install the certificate, refer to the corresponding FAQ.
  - **Installing an SSL Certificate on a Tomcat Server**
  - **Installing an SSL Certificate on an Nginx Server**
  - **Installing an SSL Certificate on an Apache Server**
  - **Installing an SSL Certificate on an IIS Server**
  - **Installing an SSL Certificate on a WebLogic Server**
  - **Installing an SSL Certificate on a Resin Server**
- For details about how to use certificates in other HUAWEI CLOUD services, see **How Do I Apply an SSL Certificate to Other HUAWEI CLOUD Services?**

7.7 How Do I Configure a Certificate Expiration Notification?

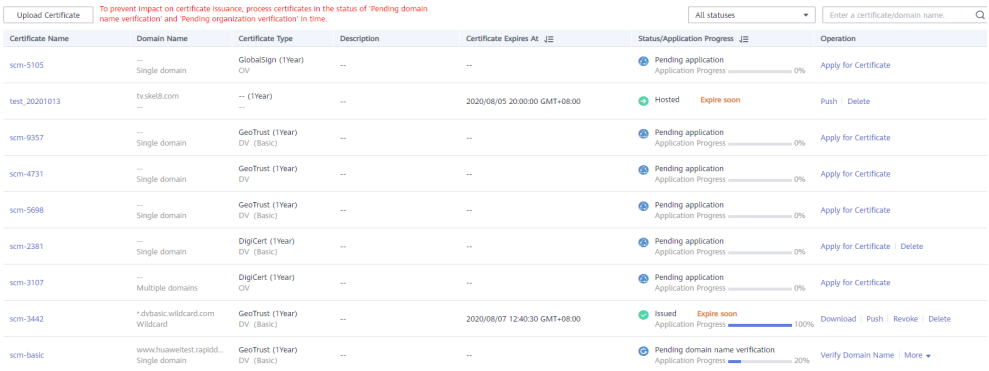
Scenario

Expired SSL certificates cannot be renewed so it is recommended that you should purchase a new SSL certificate at least three to ten working days before the current one expires.

To prevent risks caused by certificate expiration, we provide the following methods to notify you of certificate expiration:

- Reminder on the SCM console: For hosted or issued certificate, a certificate expiration reminder will be displayed on the SCM console 30 days before a certificate expires. **Figure 7-1** shows an example.

Figure 7-1 Certificate list



- Message notification: For issued and uploaded certificates, SCM automatically notifies the certificate applicants or configured message recipients of the expiration two months, one month, or one week before the certificate expires and again on the day when the certificate actually expired. For details about how to add or modify a notification recipient, see **Adding a Message Recipient**.

If your certificate is about to expire and you receive a notification from the system, address the issue by following **What Can I Do If an SSL Certificate Is About to Expire?**

Adding a Message Recipient

Step 1 Log in to the management console.

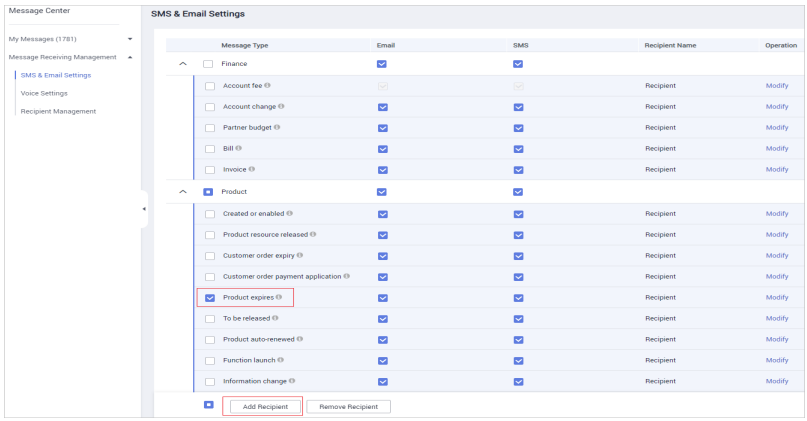
Step 2 Click  in the upper right corner of the page.

Step 3 Click **More** to go to the **Message Center** page.

Step 4 In the navigation pane on the left, choose **Message Receiving Management** > **SMS & Email Settings**.

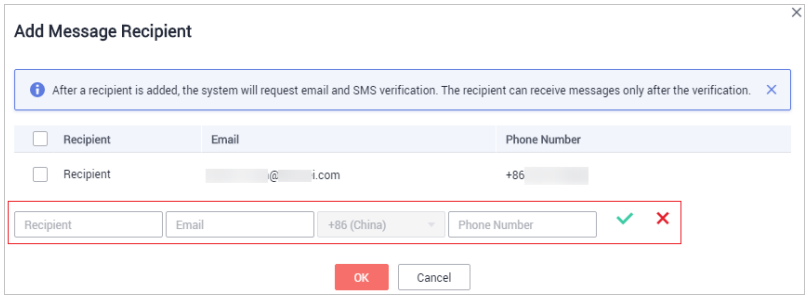
Step 5 In the **Product** area, select **Product expires** and click **Add Recipient** in the lower part of the page.

Figure 7-2 Add Recipient



Step 6 In the displayed **Add Message Recipient** dialog box, select an existing contact or click **Add Recipient**, enter the name, email address, and mobile number of the recipient, and click  to save entered information.

Figure 7-3 Add Message Recipient



Step 7 Click **OK**.

After a recipient is added, the system automatically sends a verification message to the entered mobile number and email address. The newly added recipient can receive messages only after the verification.

----End

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

If an SSL certificate expires and will not be used any more, 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.

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

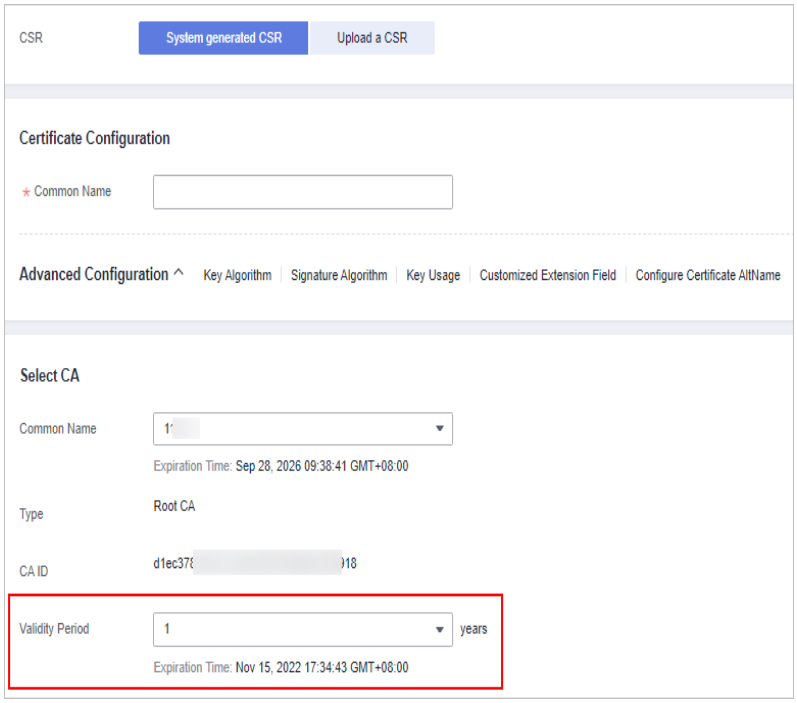
The validity period of a private certificate is set when it is applied for.

NOTE

The validity period of the private certificate can be 1, 2, 3, 4, 5, 10, 15, or 20 years. Private certificates are issued by a private CA. The validity period of a private certificate must be less than or equal to that of the private CA.

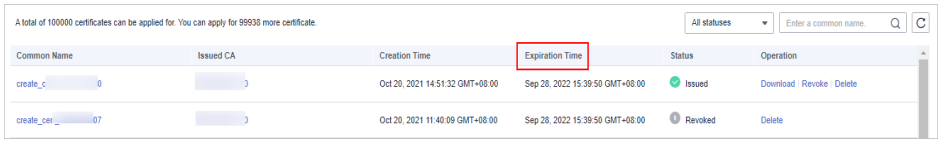
For details about how to apply for a private certificate, see **Applying for a Private Certificate**.

Figure 7-4 Setting the validity period



After you applied for a private certificate, you can view its expiration time on the private certificate list page, as shown in **Figure 7-5**. After a private certificate expires, you need to apply for a new one.

Figure 7-5 Viewing expiration time



8 Billing

8.1 How Is an SSL Certificate Billed?

SCM provides you with free single-domain DV (basic) certificates issued by DigiCert. The process for applying for a free certificate is similar to that for paid certificate. For more details, see **How Can I Apply for a Free SSL Certificate?**

If you choose other SSL certificates, you will be billed based on the certificate type, certificate brand, domain name type, domain name quantity, and required duration.

For price details, see **Product Pricing Details**.

You can upload external SSL certificates to SCM to manage all of your certificate in one place for free.

8.2 Can I Renew an SSL Certificate?

Yes.

The default validity period of an SSL certificate issued by a CA is one year. You need to renew the certificate before it expires.

The renewal entry will be available for 30 calendar days before an SSL certificate expires. For details, see **Renewing an SSL Certificate**.

NOTICE

- External certificates you upload to SCM and free certificates you apply for in SCM cannot be renewed in SCM.
- You can renew only paid SSL certificates that have been purchased in SCM and are about to expire.
- The renewal entry is available for 30 calendar days before an SSL certificate expires.
- Renewing an SSL certificate is to purchase a new certificate with the exact same configurations as the original one. The configurations include the certificate authority, certificate type, domain type, domain quantity, and primary domain name.

  If there is any configuration that is different from the original one, renewal is not supported, and you need to apply for a new certificate.
- Validity period of a renewed certificate
  - The new certificate will inherit the remaining validity period of the original certificate. However, the remaining validity period cannot exceed 30 days.

    For example, your one-year certificate will expire on November 30, 2022. If you renew the certificate and the CA issues it on November 25, 2022, the new certificate will expire on November 30, 2023. The validity period of the new certificate is one year plus the remaining validity period (five days in this case) of the original certificate.
  - If you renew an SSL certificate on the certificate renewal page, and the certificate authority, certificate type, domain type, domain quantity, and/or primary domain name of the new certificate are different from those of the original certificate, the new certificate cannot inherit the remaining validity period (if any) of the original certificate. So, the validity period of the new certificate is one year.
  - If you purchase a new certificate on the purchase page, the validity period of the new certificate is one year as the new certificate cannot inherit the remaining validity period (if any) of the original certificate.

8.3 Can I Unsubscribe from an SSL Certificate?

The 7-day unconditional refund policy applies to SCM.

Constraints

- You can request a refund for an SSL certificate order that meets all of the following conditions:
  - You have purchased an SSL certificate on the CCM console.
  - Your refund request cannot be later than 7 natural days (or 7x24 hours) after your pay for the order.

    For example, if you pay for an SSL certificate at 12:00 on December 1, you can unsubscribe from it before 11:59 on December 8. After 11:59 on December 8, you cannot unsubscribe from it.

CAUTION

No refunds are allowed 7 days after the purchase.

  - The purchased SSL certificate must meet one of the following conditions:
    - The certificate application is not submitted. The certificate status is **Pending application**.
    - The certificate application has been submitted but has been canceled before it is issued. The certificate status is **Pending application**.
    - The certificate has been issued, and the certificate revocation process has been completed within seven days after the order is placed. The certificate status is **Revoked**.
- The full refund indicates the fees you paid for the SSL certificate. If a cash coupon is used when you purchase a certificate, the used cash coupon will be refunded.

Procedure

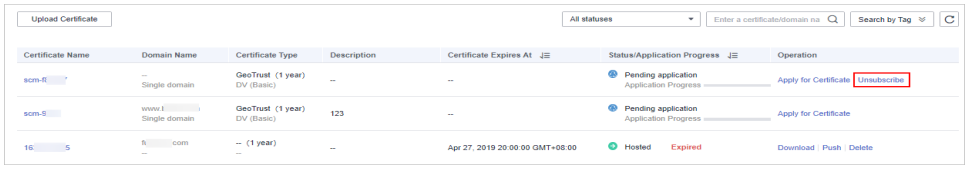
Step 1 Log in to the **management console**.

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

Step 3 In the navigation pane on the left, choose **SSL Certificate Manager**. The **SSL Certificate Manager** page is displayed.

Step 4 In the row containing the desired certificate, click **Unsubscribe** in the **Operation** column. **Figure 8-1** shows an example.

Figure 8-1 Unsubscribing



Step 5 On the **Confirm Unsubscription** page, confirm the certificate information. If the information is correct, select **I acknowledge that the certificate will be deleted and cannot be restored after the unsubscription**.

Step 6 In the lower right corner of the page, click **Unsubscribe**.

NOTICE

- Unsubscribed certificates will be deleted and cannot be recovered. Exercise caution when performing this operation.
- The system will review your unsubscription. After the unsubscription is approved, the certificate will not be displayed in the certificate list. During the review period, do not perform any operation on the SSL certificate. Otherwise, the approval fails.

Certificate unsubscribed. is displayed in the upper right corner of the page. The refund will be credited to the original payment account.

You can choose **Billing Center** > **Orders** > **My Orders** to view the unsubscription record.

----End

8.4 How Will I Be Charged for Using PCA?

You will be billed based on how many private CAs and private certificates you use. The pricing details are displayed on the purchase page.

How Do I Stop the Billing of a Private CA or Certificate?

You can delete your private CAs and private certificates to stop the billing.

For details, see **Deleting a Private CA** and **Revoking a Private Certificate**.

CAUTION

If you delete a private CA, it takes a few days for the deletion to take effect. It takes at least 7 days for a scheduled deletion to take effect (depending on the delay time you configured). During the scheduled deletion period, you will be billed in accordance with the following rules:

- If you have not canceled the scheduled deletion and the private CA is deleted, the private CA is not billed for this period.
- If you cancel the scheduled deletion but the private CA is not deleted during this period, the private CA is still billed for this period.

For example, if you delete a private CA at 00:00 on January 1, 2022 and the private CA is deleted seven days later as scheduled, you will not be billed for the seven days. If you cancel the scheduled deletion at 00:00 on January 4, 2022 and the private CA is not deleted, you will still be billed for the CA for the period from 00:00 on January 1, 2022 to 00:00 on January 4, 2022.

9 Others

9.1 SSL Certificate Management

9.1.1 What Are the Differences Between Revoking a Certificate and Deleting a Certificate?

You can revoke or delete certificates in HUAWEI CLOUD SCM.

The revocation or deletion of a certificate has no impact on repurchase of the certificate.

The differences are as follows:

- Description
  - Revoking a certificate: indicates invalidating an issued certificate at the CA. A revoked certificate is no longer trusted and can no longer be used for certificate-based encryption.
  - Deleting a certificate: indicates deleting a certificate from HUAWEI CLOUD. The certificate will still be valid and trusted by web browsers.
- Constraints
  - Revoking a certificate:

    If you no longer need a certificate, the private key of the certificate is lost, or you have certain security concerns, you can revoke an issued certificate on the SCM console.
  - Deleting a certificate:

    If your certificate is in the **Expired**, **Hosted**, or **Issued** state, you can delete it on the SCM console.

9.1.2 Can I Withdraw a Certificate Revocation or Deletion Application?

No.

After a certificate revocation or deletion application is submitted, it cannot be withdrawn. Exercise caution with certificate revocation or deletion.

- Certificate revocation indicates invalidating an issued certificate at the CA. A revoked certificate is no longer trusted and can no longer be used for certificate-based encryption.

  After a certificate revocation application is submitted, the CA reviews the application. The revocation is complete only after the application is approved.

  No operation is required during the revocation process, and the approval process of the CA takes little time. Therefore, the revocation application cannot be withdrawn after being submitted. Exercise caution with certificate revocation.
- Deleting a certificate indicates deleting a certificate from HUAWEI CLOUD. The certificate will still be valid and trusted by web browsers.

  After the certificate deletion application is submitted, HUAWEI CLOUD directly deletes the certificate without requiring the approval by the CA. Therefore, the certificate deletion operation cannot be withdrawn after being performed. Exercise caution with certificate deletion.

9.1.3 How Do I Convert a Certificate to PEM Format?

Certificate formats can be converted mutually.

It is recommended that **OpenSSL** be used to convert certificates in other formats into the **PEM** format. The following examples illustrate some popular conversion methods.

Converting the Certificate Format to PEM

Table 9-1 Certificate format conversion commands

Format	Conversion Method (Using OpenSSL)
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	• Obtain a private key. As an example, run the following command to convert **cert.pfx** into **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem** • Obtain a certificate. As an example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Convert a certificate. As an example, run the following command to convert **cert.p7b** into **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Rename obtained certificate file **cert.cer** to **cert.pem**.

Format	Conversion Method (Using OpenSSL)
DER	• Obtain a private key. As an example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** • Obtain a certificate. As an example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

PKCS8 Certificate Encoding Format

Currently, HUAWEI CLOUD WAF, ELB, and CDN do not support the PKCS8 format. An error will occur if you upload a certificate in PKCS8 format to SCM and then push the certificate to WAF, ELB, and CDN.

NOTE

- If the private key file of a certificate starts with **-----BEGIN PRIVATE KEY-----**, the certificate is in PKCS8 format.
- If the private key file of a certificate starts with **-----BEGIN RSA PRIVATE KEY-----**, the certificate is in PKCS1 format.

If your public or private key is in PKCS8 format, perform the following operations to use the PKCS8 certificate to WAF, ELB, and CDN services:

Step 1 Check whether the certificate is in PEM format.

- If yes, go to **Step 2**.
- If no, convert the certificate format to PEM by referring to **Converting the Certificate Format to PEM** and then go to **2**.

Step 2 Run the following commands to convert format from PKCS8 to PKCS1:

- Converting the private key format from PKCS8 to PKCS1:

  openssl rsa -in pkcs8.pem -out pkcs1.pem

- Converting the public key format from PKCS8 into PKCS1:

  openssl rsa -pubin -in public.pem -RSAPublicKey_out

Step 3 Upload the converted certificate to SCM. For more details, see **Uploading an External Certificate**.

Step 4 Push the uploaded certificate to other HUAWEI CLOUD service. For more details, see **Pushing an SSL Certificate to Other Cloud Services**.

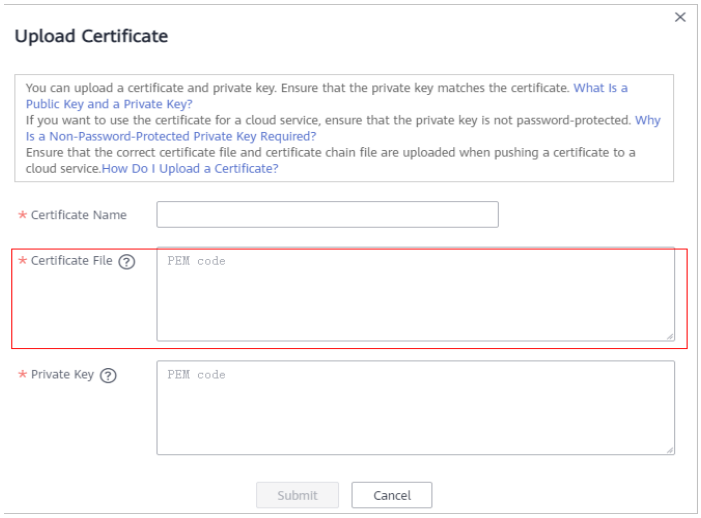
----End

9.1.4 How Do I Complete the Certificate File When Uploading a Certificate?

You can upload your external certificates to SCM so that you can centrally manage all your certificates.

When uploading an existing certificate to SCM, you need to upload a certificate file.

Figure 9-1 Certificate



Currently, only certificate files in the PEM format can be uploaded to SCM.

When uploading a certificate file, open the .PEM file to be uploaded with Notepad and copy the content to the **Certificate File** text box.

If the system displays a message indicating that the certificate chain is incomplete during the upload, perform the following operations:

Generally, a certificate file issued by an intermediate agency contains multiple certificates, for example, a server certificate and a certificate chain in *.PEM format. A certificate chain is an ordered list of certificates, containing an SSL certificate and Certificate Authority (CA) certificates, that enable the receiver to verify that the sender and all CA's are trustworthy. You need to combine all certificates into a single, complete certificate file before upload. For more information about the certificate chain, see **How Do I Configure a Certificate Chain?**

A server certificate must be placed before the certificate chain in a certificate file. Perform the following steps to make a certificate file:

1. Use Notepad to open all ***.PEM** certificate files.
2. Paste the server certificate before the certificate chain.

   Generally, an instruction will be issued by the intermediate agency together with the certificate. Be aware of the rules in the instruction. The general rules are as follows:

   - There are no empty lines between certificates.
   - The format of the certificate chain is as follows:

     -----BEGIN CERTIFICATE-----

     -----END CERTIFICATE-----

     -----BEGIN CERTIFICATE-----

     -----END CERTIFICATE-----

Figure 9-2 shows a complete certificate file.

Figure 9-2 A complete PEM certificate file

```
-----BEGIN CERTIFICATE-----
MIIE/DCCA+SgAwIBAgIUOWwvEj4lj5OamNabjVbGY42BBcQwDQYJKoZIhvcNAQEL
BQAwgYIxCzAJBgNVBAYTAmNuMRIwEAYDVQQIDAlHdWFuZ0RvbmcxETAPBgNVBAcM
CFNoZW56aGVuMQ8wDQYDVQQKDAZIdWF3ZWkxCzAJBgNVBAsMAklUMS4wLAYDVQQD
DCVIdWF3ZWkgV2ViIFNlY3VyZSBJbnRlcm5ldCBHYXRld2F5IENBMB4XDTE3MTAx
ODAwNDA0NloXDTE4MTAxODAwNDA0NlowgZoxCzAJBgNVBAYTAkNOMRAwDgYDVQQI
DAdqaWFuZ3N1MRAwDgYDVQQHDAduYW5qaW5nMS4wLAYDVQQKDCVIdWF3ZWkgU29m
dHdhcmUgVGVjaG5vbG9naWVzIENvLiwgTHRkMRkwFwYDVQQLDBBDbG91ZGJ1IFNS
RSBEZXB0MRwwGgYDVQQDDBN3d3cuaHVhd2VpY2xvdWQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3f5hC6J2OXSF/Y7Wb8o6l30yzgaUYWGLEX8t
1dQ1JAus93xMC2Jr6UOXmXR6WaRu5lZxpPfLT/IV6UnvMLnxJQBavqauykCSkadW
stYA9ttTI/FYq+MR1XKbNrqK/ADhRfmR4owS/3w1wxvdpwy5TRZ+V/D6TjxHZCjc
+8lSmUuLxsgoUe79B/ruccY1ufuqr3v0TToaNn4c37kwjJeKf+b2F/IqO/KF+9zF
[redacted]
AgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMEIGA1UdEQQ7MDmCE3d3dy5odWF3ZWlj
bG91ZC5jb22CESouaHVhd2VpY2xvdWQuY29tgg9odWF3ZWljbG91ZC5jb20wDQYJ
KoZIhvcNAQELBQADggEBACsLP7Hj+4KY1ES38OnOWuwQ3st8axvhDD9jZGoninzW
JSGpdmO4NEshlvwSFdEHpjy/xKSLCIqg5Ue8tTI8zOFl3U0ROnMeHSKSxJG6zc8X
h/3N217oBygPgvpmc6YX66kvwXmbA7KRniiYS0nmCi2KUyng5Bv4dsx21djlqQ3b
HI+i026Q9odLsmhsKOsFUC0vDKoMIJz0Socy7Cq1+tFWF9S79MI4QjxaXVEvpIEg
QLEze3BXSsoiWRkdfsdDB9s+UtdWeJy0HMh/otwUQQtB6areV2+CPthfmDENA+A8
IK6GzHyp/mgrwKdDh97aQ42ARreAv4KVFAiJGZ02LOY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID2TCCAsGgAwIBAgIJALQPO9XxFFZmMA0GCSqGSIb3DQEBCwUAMIGCMQswCQYD
VQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25nMREwDwYDVQQHDAhTaGVuemhlbjEP
MA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJVDEuMCwGA1UEAwwlSHVhd2VpIFdl
YiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBDQTAeFw0xNjA1MTAwOTAyMjdaFw0y
NjA1MDgwOTAyMjdaMIGCMQswCQYDVQQGEwJjbjESMBAGA1UECAwJR3VhbmdEb25n
MREwDwYDVQQHDAhTaGVuemhlbjEPMA0GA1UECgwGSHVhd2VpMQswCQYDVQQLDAJJ
VDEuMCwGA1UEAwwlSHVhd2VpIFdlYiBTZWN1cmUgSW50ZXJuZXQgR2F0ZXdheSBD
[redacted]
rG0CAwEAAaNQME4wHQYDVR0OBBYEFDB6DZZX4Am+isCoa48e4ZdrAXpsMB8GA1Ud
IwQYMBaAFDB6DZZX4Am+isCoa48e4ZdrAXpsMAwGA1UdEwQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAKN9kSjRX56yw2Ku5Mm3gZu/kQQw+mLkIuJEeDwS6LWjW0Hv
3l3xlv/Uxw4hQmo6OXqQ2OM4dfIJoVYKqiLlBCpXvO/X600rq3UPediEMaXkmM+F
tuJnoPCXmew7QvvQQvwis+0xmhpRPg0N6xIK01vIbAV69TkpwJW3dujlFuRJgSvn
rRab4gVi14x+bUgTb6HCvDH99PhADvXOuI1mk6Kb/JhCNbhRAHezyfLrvimxI0Ky
2KZWitN+M1UWvSYG8jmtDm+/FuA93V1yErRjKj92egCgM1u67lliddt7zzzzqW+U
QLU0ewUmUHQsV5mk62v1e8sRViHBlB2HJ3DU5gE=
-----END CERTIFICATE-----
```

9.1.5 How Do I Configure a Certificate Chain?

When you upload an SSL certificate to SCM for unified management, import the certificate, certificate chain, and private key separately and encode them in PEM format.

The following examples describe the PEM format.

NOTICE

If you incorrectly edit any character in a PEM file, for example, adding one or more spaces at the end of any line, the certificate, certificate chain, or private key will be invalid. Exercise caution when editing a PEM file.

- Example 1: PEM-encoded certificate

  Figure 9-3 PEM-encoded certificate

  ```
  -----BEGIN CERTIFICATE-----
  Base64-encoded certificate
  -----END CERTIFICATE-----
  ```

- Example 2: PEM-encoded certificate chain

  A certificate chain contains one or more certificates. You can use a text editor to add your certificate files into a chain. Certificates must be linked in sequence so that each certificate can prove the previous one.

  The following example contains three certificates. Your certificate chain may contain more or fewer certificates.

  Figure 9-4 PEM-encoded certificate chain

  ```
  -----BEGIN CERTIFICATE-----
  Base64-encoded certificate
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  Base64-encoded certificate
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  Base64-encoded certificate
  -----END CERTIFICATE-----
  ```

- Example 3: PEM-encoded private key (private certificates only)

  A public key algorithm is used for X.509 version 3 certificates. When you create an X.509 certificate or request a certificate, you need to specify the algorithm and key bit size required to create the private-public key pair, and add the public key in the certificate or request.

  In addition, you need to keep the private key password. An unencrypted private key is required when you import a certificate. For details, see **Why Is a Non-Password-Protected Private Key Required?**

  The following is an example of the RSA private key encoded in PEM format:

  ```
  -----BEGIN RSA PRIVATE KEY-----
  Base64-encoded private key
  -----END RSA PRIVATE KEY-----
  ```


The following example shows an elliptic curve private key encoded in PEM format. Depending on how you create the secret, your private key may not contain a parameter block. If the private key contains a parameter block, delete it (before using the private key) from the file to be imported to SCM.

```
-----BEGIN EC PARAMETERS-----
Base64-encoded parameters
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
Base64-encoded private key
-----END EC PRIVATE KEY-----
```

9.1.6 Why Is the SSL Certificate Not Displayed in the Certificate List?

The following two types of certificates are displayed in the certificate list on the SCM console:

- Certificates purchased on the CCM console
- Certificates uploaded to the SCM platform

In addition, certificates purchased from other platforms (including the marketplace) must be uploaded to the SCM console so that SCM can manage them. For details, see **Uploading an External Certificate**.

9.2 Troubleshooting

9.2.1 How Do I Add, Unbind, Replace, or Change the Domain Name for an SSL Certificate?

Select a processing method based on your requirements.

Adding a Domain Name Bound for an SSL Certificate

- If you have purchased an SSL certificate with a single domain name:

  A new certificate needs to be purchased.
- If you have purchased an SSL certificate with multiple domain names:
  - If the certificate has a quota for adding additional domain names, you can add additional domain names for the certificate. For more details, see **Adding an Additional Domain Name**.
  - If the certificate does not have a quota for additional domain names, you need to purchase a new certificate.
- If you have purchased an SSL certificate with a wildcard domain name:
  - If the domain name to be added is at the same level as the domain name associated with the certificate, you can directly use the existing certificate without adding the domain name.

    For example, if the domain name associated with the certificate is ***.huaweicloud.com** and you want to associate **test.huaweicloud.com**

with the certificate, you do not need to add the domain name **test.huaweicloud.com**, and you can directly use the existing certificate.

- If the domain name to be added is not at the same level as the domain name associated with the certificate, you need to purchase a new certificate.

  For example, if the domain name associated with the certificate is ***.huaweicloud.com** and you want to associate the domain name **abc.test.huaweicloud.com** with the certificate, you need to purchase a new certificate and associate the domain name with the certificate.

Unbinding a Domain Name from an SSL Certificate

- If the certificate has not been issued, and you need to unbind the domain name from the current certificate and bind a new domain name:

  You can withdraw the certificate application. For details, see **Withdrawing an SSL Certificate Application**.

- If the certificate has been issued, and you need to unbind the domain name from the current certificate and bind a new domain name:

  Reissue the certificate.

  An issued certificate can be reissued within a specified period. The period varies depending on CAs. The following describes the period given by some CAs:

  - GlobalSign: 5 days.
  - DigiCert and GeoTrust: 25 days.

  There is no limit on the number of certificate reissues only when the reissue is within the specified period, which varies depending on CAs. A certificate cannot be reissued if it exceeds the specified period.

  For details about how to re-issue a certificate, see **Re-issuing a Certificate**.

Replacing or Changing the Domain Name Bound to an SSL Certificate

- If the certificate has not been issued, and you need to replace or change the domain name bound to the current certificate:

  You can withdraw the certificate application. For details, see **Withdrawing an SSL Certificate Application**.

- If the certificate has been issued, and you need to replace or change the domain name bound to the current certificate:

  Reissue the certificate.

  An issued certificate can be reissued within a specified period. The period varies depending on CAs. The following describes the period given by some CAs:

  - GlobalSign: 5 days.
  - DigiCert and GeoTrust: 25 days.

  There is no limit on the number of certificate reissues only when the reissue is within the specified period, which varies depending on CAs. A certificate cannot be reissued if it exceeds the specified period.

  For details about how to re-issue a certificate, see **Re-issuing a Certificate**.

9.2.2 How Do I Configure an SSL Certificate on the Internal Network?

An SSL certificate cannot be deployed on internal networks.

To deploy a certificate on an internal network, apply for a private certificate. For more details, see **Applying for a Private Certificate**.

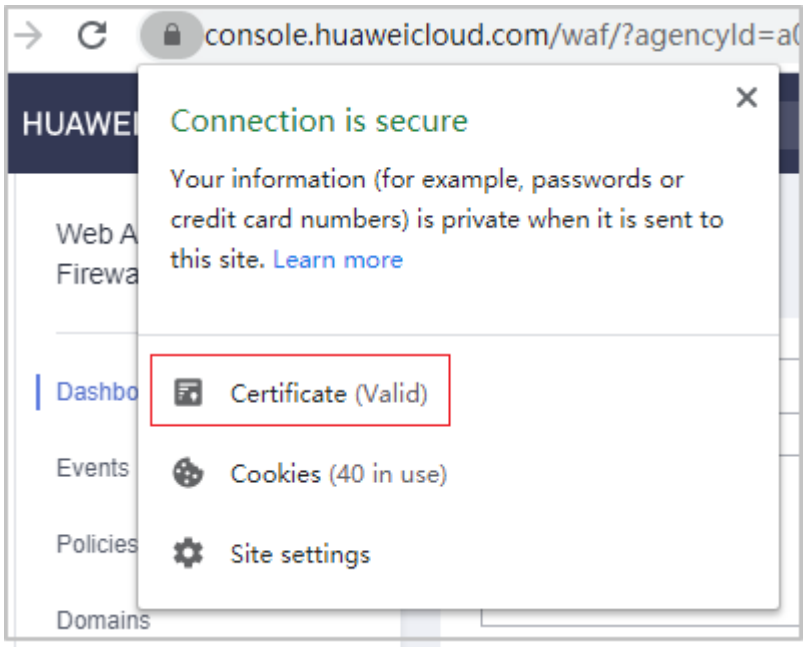
9.2.3 How Do I Fix an Incomplete SSL Certificate Chain?

If the certificate provided by the certificate authority is not found in the built-in trust store on your platform and the certificate chain does not have a certificate authority, the certificate is incomplete. If you use the incomplete certificate to access the website corresponding to the protected domain name, the access will fail.

You can manually create a complete certificate chain to solve this problem. The latest Google Chrome version supports automatic verification of the trust chain. The following describes how to manually create a complete certificate chain (using a HUAWEI CLOUD certificate as an example):

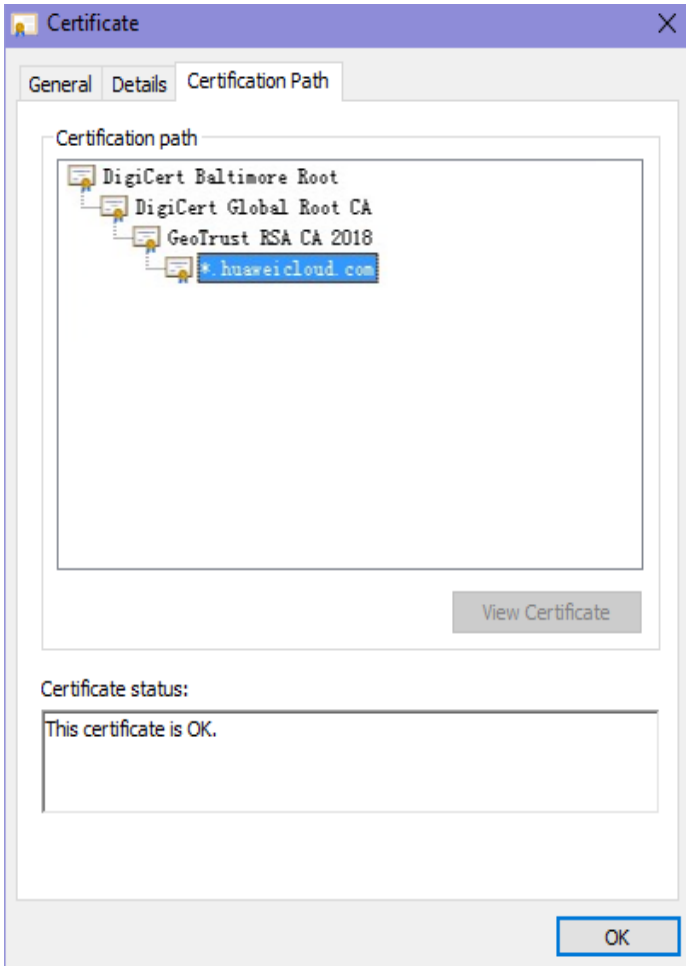
Step 1 **Viewing the certificate.** Click the padlock in the address bar to view the certificate status (see **Figure 9-5**).

Figure 9-5 Viewing the certificate



Step 2 **Check the certificate chain.** Click **Certificate**. Select the **Certificate Path** tab and then click the certificate name to view the certificate status. **Figure 9-6** shows an example.

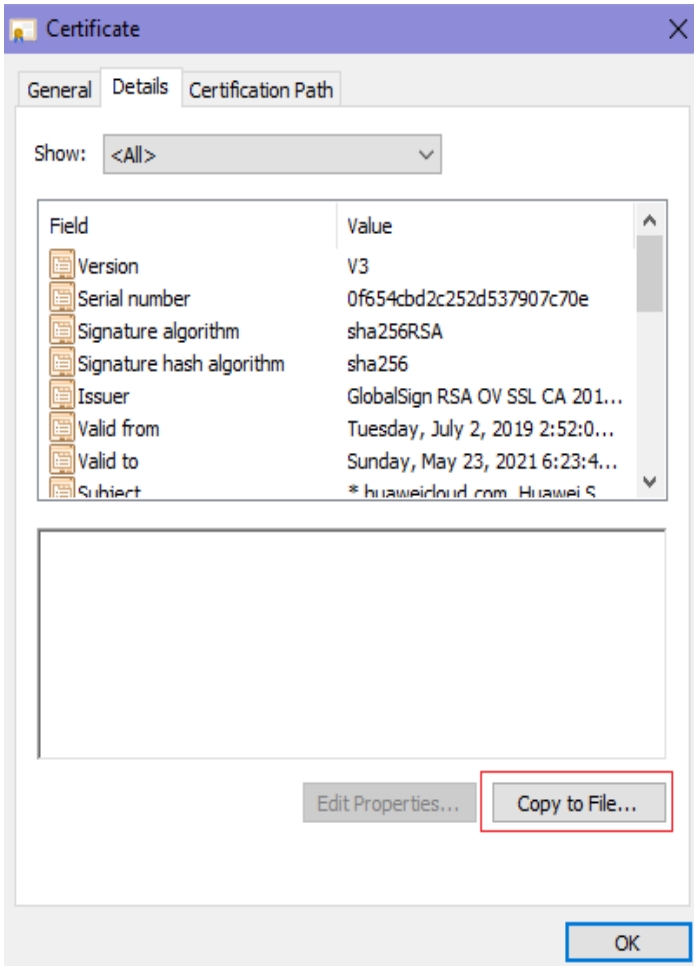
Figure 9-6 Viewing the certificate chain



Step 3 Save the certificates to the local PC one by one.

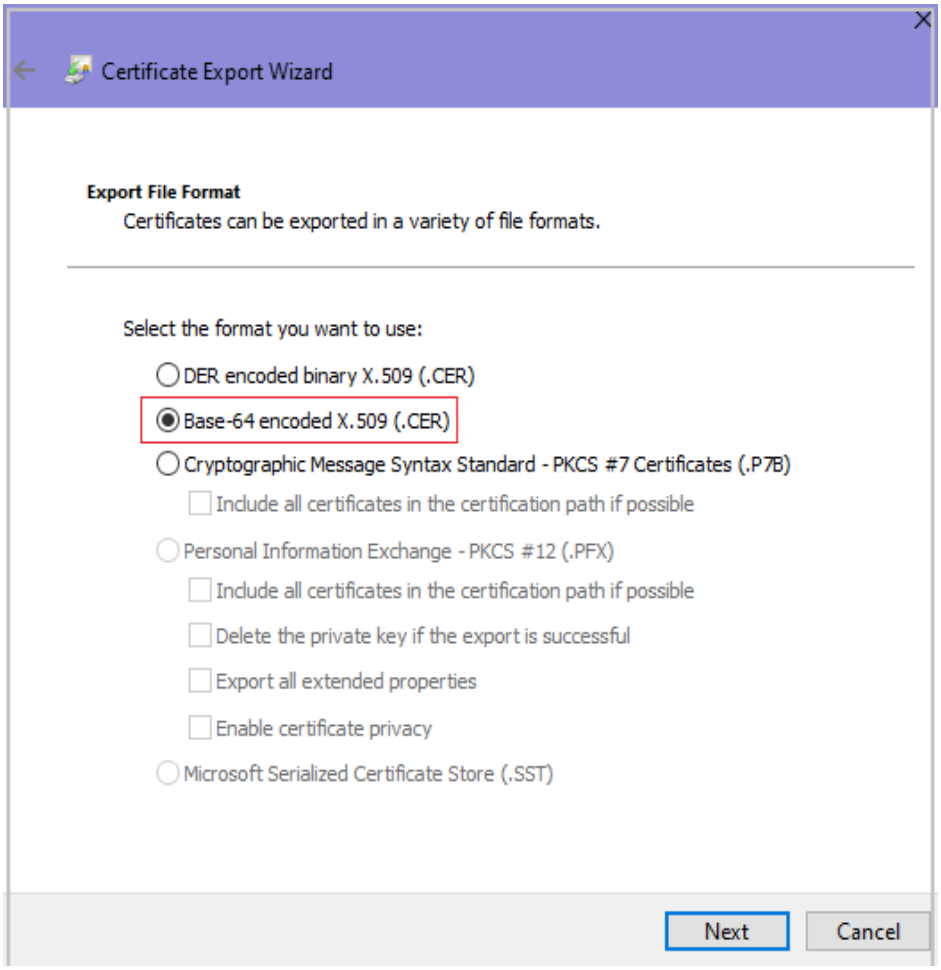
1. Select the certificate name and click the **Details** tab. **Figure 9-7** shows an example.

Figure 9-7 Details



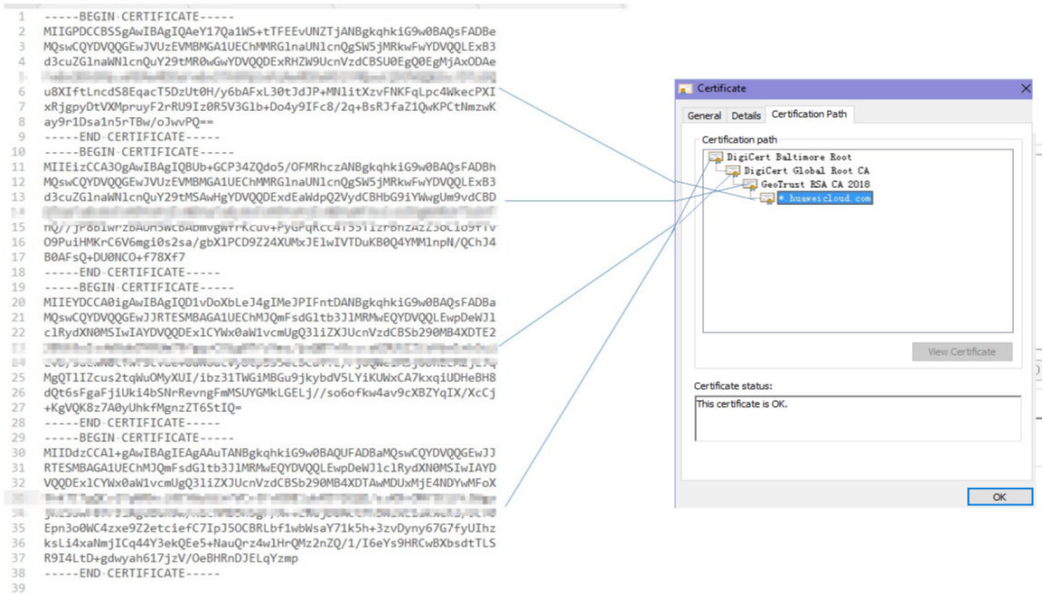
2. Click **Copy to File**, and then click **Next** as prompted.
3. Select **Base-64 encoded X.509 (.CER)** and click **Next**. **Figure 9-8** shows an example.

Figure 9-8 Certificate export wizard



Step 4 **Rebuild the certificate.** After all certificates are exported to the local PC, open the certificate file in Notepad and rebuild the certificate according to the sequence shown in **Figure 9-9**.

Figure 9-9 Certificate rebuilding



Step 5 Upload the certificate again.

----End

A Change History

Released On	Description
2021-12-15	This issue is the sixteenth official release. • Optimized descriptions in **Can I Unsubscribe from an SSL Certificate?** • Optimized descriptions in **Why Does the Website Still Display a Message Indicating that the Website Is Insecure After an SSL Certificate Is Deployed?**. • Optimized descriptions in **How Can I Apply for a Free SSL Certificate?** • Optimized descriptions in **Does SCM Provide Free Certificates?**
2021-11-26	This issue is the fifteenth official release. Added a renewal entry on the console for SSL certificates and updated **What Can I Do If My SSL Certificate Expired?** and **Can I Renew an SSL Certificate?**
2021-11-01	This is the fourteenth official release. • Updated the document based on the console optimization. • Adjusted the document structure. • Added **How Can I Apply for a Free SSL Certificate?** and **How Do I Configure a Certificate Chain?**
2021-10-18	This is the thirteen official release. Optimized **Does SCM Provide Free Certificates?** and **Problems Related to Domains**.

Released On	Description
2021-09-30	This issue is the twelfth official release. • Added **How Long Is the Validity Period of a Private Certificate?**. • Optimized **How Do I Verify the Domain Ownership Manually by DNS?** and **How Long Does It Take to Approve an SSL Certificate?** • Supported canceling SSL certificate subscriptions on the SCM console and optimized **Can I Unsubscribe from an SSL Certificate?**
2021-08-16	This issue the eleventh official release. • Updated sections related to the new commercial version of the private certificate management service. • Optimized **How Do I Check Whether Domain Name Verification Takes Effect?**, **What Can I Do If Domain Ownership Verification Does Not Take Effect?**, and **Why Does the SSL Certificate Remain in the Pending Domain Name Verification State After Domain Name Verification Completes?**
2021-06-15	This issue is the tenth official release. Optimized **What Are Differences Between Free and Paid SSL Certificates**, **How Do I Install an SSL Certificate on a Server?**, and **How Do I Configure a Non-HUAWEI CLOUD SSL Certificate for a HUAWEI CLOUD Service?**
2021-05-26	This issue is the ninth official release. Optimized **How Do I Verify Domain Ownership?**, **How Do I Verify the Domain Ownership Manually by DNS?**, and **Why Does the Certificate Stay in the CA Verifying Status for a Long Time?**
2021-04-29	This issue is the eighth official release. Updated **How Do I Select an SSL Certificate?**, **How Do I Apply for a Combination Certificate?**, **What Are the Differences Between a Single-Domain Name, Multi-Domain Name, and Wildcard-Domain Name in SCM?**, and **Problems Related to Domains** and added the description of purchasing multi-domain certificates.
2021-04-14	This issue is the seventh official release. Added **What Are Differences Between Free and Paid SSL Certificates**

Released On	Description
2021-03-19	This issue is the sixth official release. • Updated **What Can I Do If My SSL Certificate Expired?** and **How Do I Configure a Certificate Expiration Notification?** SCM automatically sends email and SMS messages to notify of the certificate expiration. • Updated the description of the validity period of old and new certificates.
2021-03-12	This issue is the fifth official release. • Updated the screenshots based on the optimized GUI page for SSL certificate application. • Added the automatic DNS verification for SSL certificate management.
2021-01-26	This issue is the fourth official release. • Added SSL certificate management functions. • Added **How Do I Add, Unbind, Replace, or Change the Domain Name for an SSL Certificate?**
2020-08-31	This issue is the third official release. Updated "What Is PCA?" Added the description of the PCA validity period.
2020-02-27	This issue is the second official release. Added the following FAQs: • How Do I Make a CSR File? • What Is a Public Key and a Private Key? • Why Is a Non-Password-Protected Private Key Required? • What Are Mainstream Formats of Digital Certificates?
2020-01-17	This issue is the first official release.