

# Cloud Certificate Manager

## User Guide(SCM)

**Issue** 01  
**Date** 2023-12-15



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

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

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

---

# Contents

---

<b>1 About SCM and SSL Certificate Usage.....</b>	<b>1</b>
<b>2 Purchasing an SSL Certificate.....</b>	<b>5</b>
<b>3 Applying for an SSL Certificate.....</b>	<b>10</b>
3.1 Submitting an SSL Certificate Application to the CA.....	10
3.2 Verifying Domain Name Ownership.....	14
3.2.1 What Is Domain Name Verification.....	14
3.2.2 Manual DNS Verification.....	15
3.2.3 Verification by Email.....	19
3.3 Verifying the Organization Identity.....	20
3.4 Issuing an SSL Certificate.....	20
<b>4 Deploying SSL Certificates.....</b>	<b>22</b>
4.1 Deploying an SSL Certificate to Other Cloud Products.....	22
4.1.1 Deploying an SSL Certificate to WAF.....	22
4.1.2 Deploying an SSL Certificate to ELB.....	23
<b>5 Managing SSL Certificates.....</b>	<b>25</b>
5.1 Reissuing an SSL certificate.....	25
5.2 Unsubscribing from an SSL Certificate.....	27
5.3 Renewing an SSL Certificate.....	29
5.3.1 Performing a Manual Renewal.....	29
5.4 Revoking an SSL Certificate.....	31
5.5 Deleting an SSL Certificate from CCM.....	32
5.6 Uploading an External Certificate to SCM.....	33
5.7 Adding an Additional Domain Name.....	34
5.8 Withdrawing an SSL Certificate Application.....	36
5.9 Canceling Authorization for Privacy Information.....	37
5.10 Pushing an SSL Certificate to Other Cloud Services.....	38
5.11 Viewing Details About an SSL Certificate.....	40
5.12 Viewing the Application Progress.....	43
<b>6 Permissions Management.....</b>	<b>45</b>
6.1 Creating a User and Granting SCM Permissions.....	45
6.2 Custom Policies for SCM.....	46

---

**A Change History..... 48**

# 1 About SCM and SSL Certificate Usage

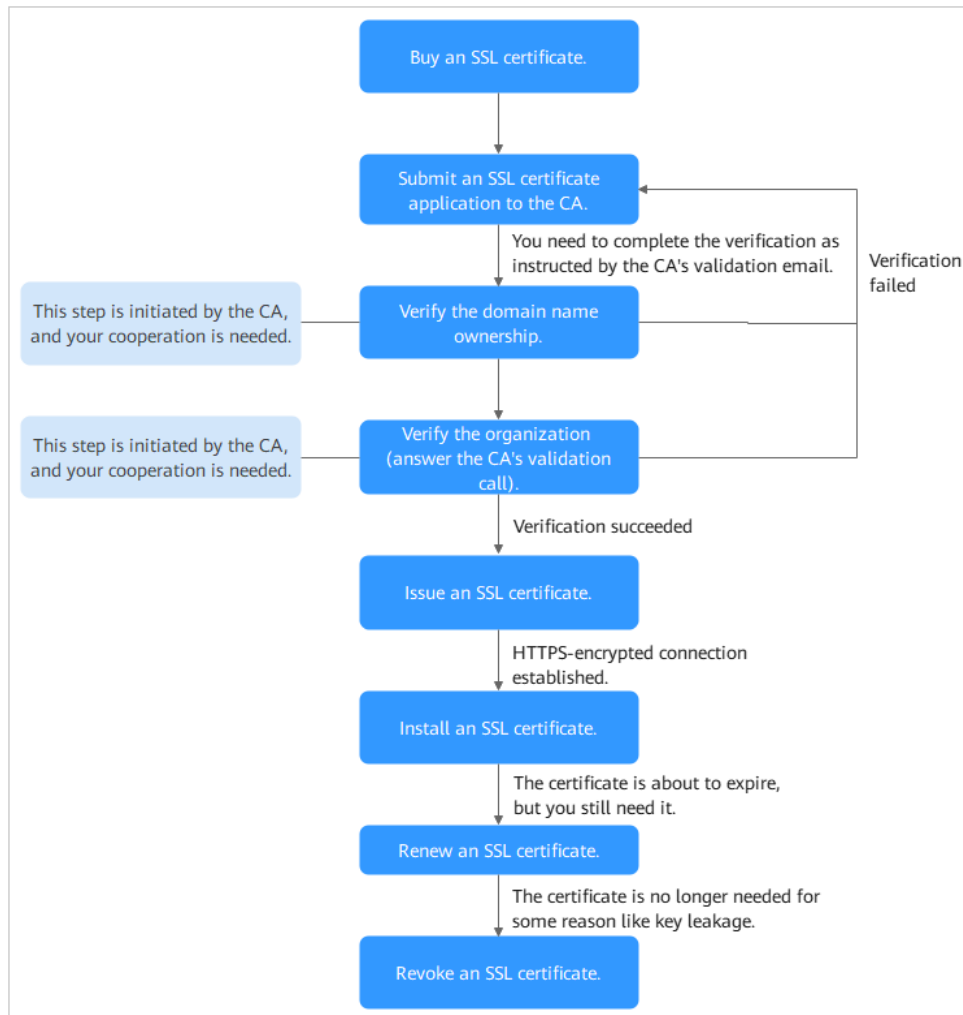
---

There are multiple SSL certificate types available from well-known CAs. For details, see [Differences Between Certificate Types](#). This section describes how to purchase and select SSL certificates.

With an SSL certificate deployed on your web server, the server uses HTTPS to establish encrypted links to the client, ensuring data transmission security.

For details, see [Figure 1-1](#) and [Table 1-1](#).

**Figure 1-1** Certificate usage process



**Table 1-1** Certificate usage process

Step	Operation	Description
1	<b>Purchasing an SSL Certificate</b>	On the SCM platform, purchase an SSL certificate for your domain name. For more details, see <a href="#">Differences Between SSL Certificate Types</a> and <a href="#">How Do I Select an SSL Certificate?</a>
2	<b>Submitting an SSL Certificate Application to the CA</b>	After you purchase a certificate, associate it with a domain name, provide additional details, and then submit the application to the CA for validation.

Step	Operation	Description
3	<a href="#">Verifying the Domain Name Ownership</a>	<p>You need to work with the CA to complete the domain name ownership verification.</p> <p>SCM provides the following domain name ownership verification methods:</p> <ul style="list-style-type: none"> <li>• Automatic DNS verification can be used for certificates that meet stated conditions.</li> <li>• Manual DNS verification: suitable for all types of certificates.</li> <li>• Email verification: suitable for OV and EV certificates only.</li> <li>• <b>File Verification:</b> This method is optional only for OV and EV certificates.</li> </ul>
4	<a href="#">Verifying the Organization (for OV and EV Certificates)</a>	<p>This operation is required only when you apply for an OV, OV Pro, EV, or EV Pro certificate.</p> <p>After the domain name ownership is verified, the CA will initiate organization verification.</p>
5	<a href="#">Issuing an SSL Certificate</a>	<p>When the verification is complete, it takes some time for the CA to approve your verification. For details about the application time, see <a href="#">How Long Does It Take for a CA to Approve an SSL Certificate?</a></p> <p>The CA will issue the certificate only after they validate your information. An SSL certificate is valid for one year from the time it is issued.</p>
6	<a href="#">Installing an SSL Certificate</a>	<p>You can download the certificate and install it on a server.</p> <ul style="list-style-type: none"> <li>• An SSL certificate cannot enable HTTPS-encrypted communication until it is installed on the web server housing the service.</li> </ul>
7	<a href="#">Renewing an SSL Certificate</a>	<p>Since September 1, 2020, global CAs issues only one-year SSL certificates. When a certificate expires, it will no longer be trusted by the browser. You are advised to manually renew the certificate 30 days before it expires to prevent your services from being affected.</p> <p>Renewing an SSL certificate is to apply for a new certificate with the exactly same configurations as the original one. The configurations include the certificate authority, certificate type, domain type, domain quantity, and primary domain name. After you renew a certificate, install the new certificate on your web server to replace the old certificate that is about to expire.</p>

Step	Operation	Description
8	<b>Revoking an SSL Certificate</b>	<p>If you no longer need an issued SSL certificate for security reasons or other reasons, for example, the certificate key is lost, you can revoke the certificate on the SCM console.</p> <p>You can revoke a certificate that has been issued by a CA. A revoked certificate is no longer trusted and can no longer be used for certificate-based encryption.</p>



# 2 Purchasing an SSL Certificate

---

In CCM, you can buy and request for many types of SSL certificates.

## Prerequisites

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

- **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project.
- **DNS Administrator**: has full permissions for DNS.


## Constraints

Special enterprises cannot apply for OV or EV certificates. For example, military units, some government agencies, and national security departments.

To apply for OV and EV certificates, organizations must verify their identity through unified social credit code published on the national official website. While, special enterprises cannot verify their organization identity because there is no related details on that website.

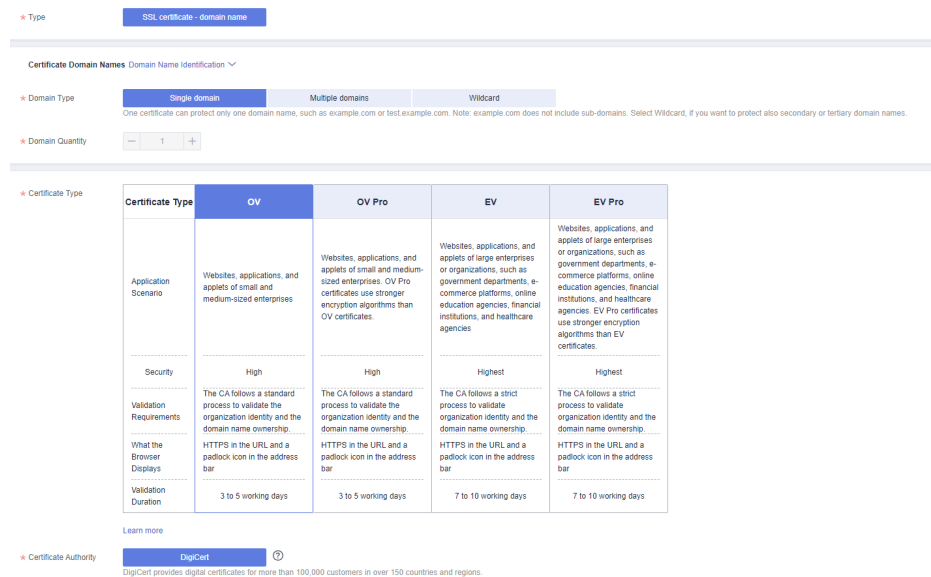
## Procedure

**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**. In the upper right corner of the page, click **Buy Certificate**.

**Step 4** On the page for purchasing a certificate, specify **Domain Type**, **Domain Quantity**, **Certificate Type**, **Certificate Authority**, **Validity Period**, and **Quantity**.



1. **Domain Type:** Select a domain name type.

Only **Single domain**, **Multiple domains**, or **Wildcard** can be selected for your certificates. For details about the parameters, see [Table 2-1](#).

**Table 2-1** Domain types

Domain Type	Description
Single domain	Only a single domain can be associated with an SSL certificate. For example, example.com.
Multiple domains	<p>Multiple domain names can be associated with an SSL certificate.</p> <ul style="list-style-type: none"> <li>You can associate a multi-domain certificate with up to 250 domain names.</li> <li>A wildcard domain name is allowed only by OV or OV pro multi-domain certificates. Other types of multi-domain certificates can only associate with multiple single domain names</li> <li>You can associate a multi-domain certificate with multiple domain names at different time points. For example, if you purchase a multi-domain certificate with three domain names, you can associate it with two domain names when applying for the certificate, and associate it with the last domain name after the certificate is issued.</li> <li>The number of domain names a multi-domain certificate can protect depends on the domain quantity you configure when you buy the certificate. If you have more domain names to protect after the purchase completes, purchase another certificate for them.</li> </ul>

Domain Type	Description
Wildcard domain	<p>Only one wildcard domain can be associated with an SSL certificate. Domain names having multiple wildcard characters, such as *.*.example.com, are not supported.</p> <p>Only one wildcard character is allowed in a wildcard domain name, for example, *.example.com, which may include domain names a.example.com, b.example.com, and more, but does not include a.a.example.com.</p>
<p>For details about how to select a domain type, see <a href="#">How Do I Select an SSL Certificate?</a></p>	

2. Set the domain quantity.
  - If the **Domain Type** value is **Single domain** or **Wildcard**, you can only associate one domain name with a certificate.
  - If you select **Multiple domains** for **Domain Type**, you can associate 2 to 250 domain names with a certificate. Set the quantity of domain names based on your needs.
3. Select a certificate type.  
For more details, see [Table 2-2](#).

**Table 2-2** Certificate types

Certificate Type	Application Scenario	Verification Requirements	Security Approval Period
EV Pro	<p>Websites, applications, and applets of large enterprises or organizations, such as government departments, e-commerce platforms, online education agencies, financial institutions, and healthcare agencies. EV Pro certificates use stronger encryption algorithms than EV certificates.</p>	<p>CAs will verify the organization identity and the domain name ownership.</p>	<p>Highest 7 to 10 working days</p>

Certificate Type	Application Scenario	Verification Requirements	Security Approval Period
EV	Websites, applications, and applets of large enterprises or organizations, such as government departments, e-commerce platforms, online education agencies, financial institutions, and healthcare agencies	CAs will verify the organization identity and the domain name ownership.	Highest 7 to 10 working days
OV Pro	Websites, applications, and applets of small and medium-sized enterprises. OV Pro certificates use stronger encryption algorithms than OV certificates.	CAs will verify the organization identity and the domain name ownership.	High 3 to 5 working days
OV	Websites, applications, and applets of small and medium-sized enterprises	The CA follows a standard process to validate the organization identity and the domain name ownership.	High 3 to 5 working days

4. Select a certificate authority.  
Currently, only **DigiCert** certificates are provided. For details about **DigiCert** certificates, see [Certificate Details](#).
5. Set **Validity Period**.  
The validity period of a certificate starts from the time the certificate is issued. After a certificate expires, a new one must be purchased.
6. Set the number of certificates you want to buy in the **Quantity** field.

**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 CCM statement by selecting **I have read and agree to the Cloud Certificate Manager Statement**. 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 Procedure

After you purchase an SSL certificate, you still need to associate a domain name with it, provide certain details, and then submit it to the corresponding CA for approval. The CA reviews your application and issues the certificate when they consider your application valid. For details, see [Submitting an SSL Certificate Application to the CA](#).

# 3 Applying for an SSL Certificate

---

## 3.1 Submitting an SSL Certificate Application to the CA

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

This topic describes how to apply for a certificate.

### Prerequisites

You have an SSL certificate in the **Pending application** status.

### Constraints

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

### 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**. In the row containing the desired certificate, click **Apply for Certificate** in the **Operation** column.
- Step 4** On the displayed page, enter the domain name, organization, and applicant information.

Figure 3-1 Domain name and other information

**Apply for Certificate**

**Domain Name Details**

\* CSR  System-generated CSR (recommended)  Upload a CSR

A system-generated CSR is recommended. If you upload a CSR you make, the certificate will not be deployed to other Huawei Cloud services directly through CCM.

\* Domain Name

Domain names cannot be modified once the certificate application is submitted. Enter correct and complete domain names. [How Do I Enter a Domain Name?](#)

Key Algorithm

\* Root Certificate Hash Algorithm  Default  SHA-256 ?

**Company Information**

\* Company Name

This information is very important. The company name provided must be the same as that on the business license.

\* Country/Region

**Applicant Details** ?

\* Name  ✓  
Enter a valid full name.

\* Phone Number  ✓  
This information is very important. We will use this number to contact you when we are reviewing the certificate application.

\* Email Address  ✓  
This information is very important. Ensure that you can receive and send emails with this email address because certificate information confirmation and change emails will be sent to this address.

**(Optional) Technical Contact Information**

Note: When your certificate is issued, Huawei Cloud will keep the preceding organization and contact details so that you can use it quickly next time you apply for a certificate. If you do not want us to keep such information, cancel the information authorization on the Application/Organization Information tab page after the certificate is issued. Once the authorization is canceled, privacy information about the certificate will be completely deleted from Huawei Cloud.

I have read, understood, and agree to the [Cloud Certificate Manager \(CCM\) Statement and Privacy Statement](#). I authorize Huawei Cloud to store and use the preceding information to generate public and private keys and CSRs for my SSL certificates. I also authorize Huawei Cloud to encrypt and store them. I also authorize Huawei Cloud to submit the preceding information to the third-party CA.

1. CSR

A certificate signing request (CSR) contains information about your server and company. When applying for a certificate, you need to submit a CSR file of your certificate to the CA for review.

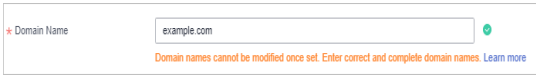

CSR file generation method:

- **System generated CSR** (recommended): 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 For details about the differences between the two types of certificate request files, see

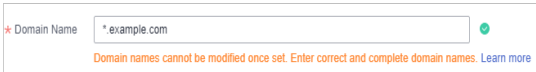
2. **Domain Name**

- If you select **Upload a CSR** for **CSR**, the domain name is auto-filled.
- If you select **System generated CSR** for **CSR**, manually enter the domain name.

**Table 3-1** Associating a certificate with a domain name

Type	Description
Single domain	<p>Enter one domain name to be associated.</p> <p>For example, if the domain name is example.com, configure the parameters as shown in the following figure.</p> 
Multiple domains	<p>The primary domain name and additional domain name must be configured.</p> <p>For example, if the domain names are example.com, a.example.com, and b.example.com, configure the parameters as shown in the following figure.</p>  <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>■ The number of additional domain names must be greater than or equal to 1. You can add one or more additional domain names at a time.</li> <li>■ One additional domain name per line.</li> <li>■ If you purchase a multi-domain certificate (single domain name + wildcard domain name), the primary domain name can be a single domain name.</li> <li>■ A primary domain and additional domains can be equally protected.</li> </ul>



Type	Description
Wildcard domain	<p>Enter the wildcard domain name to be bound. For example, if the domain name to be bound is *.example.com, set the parameters as shown in the following figure.</p> 
<p>To associate a Chinese domain name with a certificate, use encoding tool <b>Punycode</b> to encode the Chinese domain name and then enter the encoded data.</p>	

### 3. Root Certificate Hash Algorithm

If you purchase a **DigiCert OV** certificate, keep the default settings and do not select **SHA-256** unless you have to.

#### NOTICE

If **SHA-256** is used for a root certificate, there might be some compatibility issues on browsers of earlier versions.

### 4. Company Information

Enter your organization information as prompted.

#### NOTE

- This parameter is mandatory only for OV and EV certificates.
- Enter the full name of the company you registered on your business license.

### 5. Applicant Details

- The CA will contact you through the applicant email address and phone number you provide to verify information.
- Personal information used as contact details is not included in the issued certificate.

### 6. Technical Contact Information

This parameter is optional. If you set this parameter, ensure that the name, phone number, and email address of the technical support person are correct.

#### Step 5 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.

----End

## Follow-up Procedure

- The CA will handle your application within 2 to 3 working days and send a verification email to you.

Perform domain name verification as required. For more details, see [Verifying Domain Name Ownership](#).

- If you have submitted a certificate application but then discover there are incorrect details included, you can withdraw the application, modify information, and apply for a new certificate. For details, see [Withdrawing an Application](#).

## 3.2 Verifying Domain Name Ownership

### 3.2.1 What Is Domain Name Verification

After certificate application is submitted, the associated domain needs to be verified. 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 CA will issue the certificate.

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

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

**Table 3-2** Domain name verification methods

Method	Description	Application Scenario
<a href="#">Manual DNS Verification</a>	You add a record to the record set configured for the domain name for verification.	<ul style="list-style-type: none"><li>• You have the permission to modify the DNS resolution settings.</li><li>• You have selected manual DNS verification for domain name verification method when applying for the certificate.</li></ul>
<a href="#">Email Verification</a>	You log in to the email address of the domain name administrator and reply to the domain name confirmation email sent by the CA.	You have the permission to log in to the domain name administrator's mailbox. You have the domain name management permission.

Method	Description	Application Scenario
File Verification	You obtain the certificate verification file from the SCM console and create the specified file in the website root directory on the server.	<ul style="list-style-type: none"> <li>You have the permission to write content to the root directory of the server where the website is located. You have the server management permission.</li> <li>Port 80 or 443 is enabled on the server to listen to HTTP or HTTPS requests.</li> </ul> <p><b>CAUTION</b> CAs send authentication requests only to port 80 or 443. If port 80 or 443 is not enabled on your server, do not use the file verification method.</p>

### 3.2.2 Manual DNS Verification

According to the CA requirements, if you applied for an SSL certificate, you must prove that the domain name to be associated with the certificate belongs to you.

For manual DNS verification, you add a record to the record set configured for the domain name for verification. If the CA verifies that the added record can be resolved, the verification is successful.

If you select manual DNS verification when applying for a certificate, perform the operations described in this section.

#### 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.

#### Prerequisites

You have completed real-name authentication.

#### Step 1: Confirm the Verification Procedure

**When you use DNS to verify your domain ownership, the DNS records can be resolved only on the platform managing your domain name.** Perform the verification steps based on the domain name management platform.

Domain Name Management Platform	Verification Procedure
Domain names hosted on our platform	Complete all subsequent steps.
Domain names not hosted on our platform	<p>Do you want to migrate the domain name from another service provider to our DNS?</p> <ul style="list-style-type: none"> <li>• If your answer is "Yes", perform the following steps:               <ol style="list-style-type: none"> <li>1.</li> <li>2. Complete all subsequent steps.</li> </ol> </li> <li>• If your answer is "No", perform the verification on the corresponding platform.</li> </ul>

## Step 2: Obtaining Verification Information

**Step 1** Log in to the [management console](#).

**Step 2** On the **Verify Domain Name** page, view the content for **Host Record**, **Record Type**, and **Record Value**. 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.

----End

## Step 3: Performing Verification Using DNS

**Step 1** Log in to the [management console](#).

**Step 2** Choose **Networking > Domain Name Service**. In the navigation pane on the left, choose **Public Zones** to go to the **Public Zones** page.

**Step 3** In the public zone list, click the domain name you want to add a record set for. In the upper right corner of the page, click **Add Record Set**.

 **NOTE**

- Different types of record sets should be added for DNS verification of different domain name types.
  - For a single-domain certificate, if the domain name does not contain www, add a record set for the domain name. If the domain name contains www, add a record set for the corresponding higher level domain name. For example, if your certificate is used for domain name www.example.com, add a record set for example.com.
  - For a multi-domain certificate, add record sets for all domain names associated with the certificate.
  - For a wildcard-domain certificate, add a record set for the higher level domain name corresponding to the wildcard domain.  
For example, if your certificate is used for domain name \*.example.com, add a record set for example.com.
- If there is a DNS record of the corresponding type in the domain name list, click **Modify** in the **Operation** column. Modify the record in the displayed **Modify Record Set** dialog box.

**Table 3-3** Parameters for adding a record set

Parameter	Description
Name	Host record returned by the domain name service provider on the domain name verification page of the certificate.
Type	Record type returned by the domain name service provider on the domain name verification page.
Alias	Select <b>No</b> .
Line	Select <b>Default</b> .
TTL (s)	Set this parameter to <b>5 min</b> . 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. <b>NOTE</b> 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 record set 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** Check whether the DNS configuration takes effect by running the corresponding command listed in [Table 3-4](#).

**Table 3-4** Verification commands

Record Type	Verification commands
TXT	<b>nslookup -q=TXT xxx</b>
CNAME	<b>nslookup -q=CNAME xxx</b>

 **NOTE**

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 3-2](#) shows an example.

**Figure 3-2** Effective configuration of domain name ownership verification



- If the command output does not contain any records and **Non-existent domain** is displayed, the configuration does not take 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 3-5** Possible causes

Possible Cause	Procedure
A wrong domain name management platform was selected.	DNS verification can be performed only on the platform where your domain name is hosted. Check whether the platform you select is the right one.
The old record set is not deleted.	The record added can be deleted once the current certificate is issued.  If the record added for the previous certificate is not deleted, the record added for the current certificate will not take effect. Check whether the record added last time is deleted.

Possible Cause	Procedure
The record configuration is incorrect.	Check settings of <b>Host Record, Type</b> or <b>Value</b> .
It requires a long period of time for the configuration to take effect.	Check whether the effective time (TTL) is too long. It is recommended that you set the TTL to 5 minutes. This value varies depending on the DNS service provider. In our DNS platform, the default value is 5 minutes, so the configuration takes effect in 5 minutes by default. If the configured effective time does not arrive, verify after the time is right.

----End

## Step 5: Review the DNS Verification Result

### OV and EV certificates

After you complete the verification, it still takes 2 to 3 working days for the CA to validate your DNS verification. The CA will not issue the certificate until they validate your DNS verification.

If the verification fails or other problems occur, contact the CA using the information provided in the CA's validation email.

### 3.2.3 Verification by Email

According to the CA requirements, if you applied for an SSL certificate, you must prove that the domain name to be associated with the certificate belongs to you.

Email verification, you log in to the email address of the domain name administrator and reply to the domain name confirmation email sent by the CA. If the domain name administrator's replies to the verification email sent by the CA, the verification is successful.

If you select email verification when applying for a certificate, perform the operations described in this section.

#### 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

## 3.3 Verifying the Organization Identity

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

---

### NOTICE

If you purchase an OV certificate from DigiCert or GeoTrust again within 13 months and the certificate information is not changed, organization verification is not required.

---

### Prerequisites

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

### Constraints

Organization verification is required for OV, OV Pro, EV, and EV Pro certificates.

### Procedure

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

**Step 2** Open the organization verification email from the CA.

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

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

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

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

----End

## 3.4 Issuing an SSL Certificate

Your SSL certificates will be issued after the CA approves your application. The certificate approval time depends on how quickly you respond with requested information from the CA. The CA contacts you through the reserved email address



and phone number. Ensure you can be contacted through the information you leave when applying for the certificate.

- For OV and EV certificates, it takes some while for the CA to review your information after the organization verification succeeds. The certificates will be issued after being approved by the CA.

The approval period varies depending on the SSL certificate type. [Table 3-6](#) describes the approval period of each certificate type.

**Table 3-6** Certificate approval periods

Certificate	Approval Period
EV	The CA manually reviews the information. If the information is valid, the review takes 7 to 10 <b>working days</b> .
OV	The CA manually reviews the information. If the information is valid, the review takes 3 to 5 <b>working days</b> .

## Procedure

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

# 4 Deploying SSL Certificates

---

## 4.1 Deploying an SSL Certificate to Other Cloud Products

### 4.1.1 Deploying an SSL Certificate to WAF

When an SSL certificate is issued, you can deploy it to Web Application Firewall (WAF) on Huawei Cloud in just a few clicks. With SSL certificates, data access to your website protected with WAF is more secure.

#### Prerequisites

- You have enabled WAF, routed your website domain name to WAF, and configured an SSL certificate for the domain name in WAF.
- If you have not purchased WAF or the domain name you want to use the certificate for has not been added to WAF, deploying the certificate to WAF may fail.
- You have an SSL certificate that is in **Issued** or **Hosted** status.

#### Constraints

- Currently, you can use SCM to quickly deploy an SSL certificate to WAF in the **default** enterprise project only. For other enterprise projects, download the certificates first, upload them to WAF, and then deploy them in WAF.
- If you select **Upload a CSR** for **CSR** when applying for a certificate, the issued certificate **cannot** be directly deployed to other cloud products through SCM. To use a certificate in a cloud product, download the certificate to your local PC first. Then, upload it to the cloud product and complete deployment.

#### Procedure


**Step 1** Log in to the [management console](#).

**Step 2** Locate the row containing the certificate you want to deploy on other cloud product, and click **Deploy** in the **Operation** to go to the certificate deployment details page.

**Figure 4-1** Deploy

**Step 3** On the displayed page, select **WAF** in the **Deployment Details** area.

**Figure 4-2** Selecting a cloud product

**Step 4** Click  on the right of the **Region** drop-down list and select the region where you want to deploy the certificate.

**Step 5** Select the domain name you want to deploy the certificate for and click **Deploy** in the **Operation** column.

To deploy the certificate for multiple domain names, select all the domain names you want and click **Deploy** above the domain name list.

**Step 6** In the displayed confirmation dialog box, click **Confirm**.

When the certificate is deployed, the **Deployment** column for the domain name reads **Deployed**.

----End

## 4.1.2 Deploying an SSL Certificate to ELB

When an SSL certificate is issued, you can deploy it to Elastic Load Balance (ELB) in just a few clicks. With SSL certificates, data access to your website that uses ELB is more secure.

### Prerequisites

- You have enabled Elastic Load Balance (ELB) as required below, added your website domain name to ELB, and configured an SSL certificate for the website in ELB.  
If you have not purchased ELB or the domain name you want to use the certificate for has not been added to ELB, deploying the certificate to ELB may fail.
- You have an SSL certificate that is in **Issued** or **Hosted** status.

### Constraints

- You have configured the original certificate in ELB. This means the certificate that is being used for ELB and you want to update in SCM must have been configured in ELB at the very beginning. Then, you can quickly update it in SCM. For details, see
- You can use SCM to update the certificate deployed on listeners in ELB. If you update an SSL certificate in SCM, the certificate content and private keys are updated in ELB accordingly. ELB then updates the certificate content and private keys on all listeners where the certificate is deployed for.
- To update a certificate used for ELB in SCM, domain names must be associated with the certificate in ELB.

- If an ELB certificate is used for multiple domain names, ensure that the new certificate you want to update in SCM for ELB must match with those domain names. If they do not match, the domain names in the new certificate will overwrite the ones in the original certificate after the update.  
  
For example, the primary domain name and additional domain name of the new certificate are example01.com and example02.com, respectively, and the domain names associated with the original certificate in ELB are example01.com and example03.com. When you update the certificate in SCM, the domain names associated with the certificate in ELB are updated to example01.com and example02.com.
- If you select **Upload a CSR for CSR** when applying for a certificate, the issued certificate **cannot** be directly deployed to other cloud products through SCM. To use a certificate in a cloud product, download the certificate to your local PC first. Then, upload it to the cloud product and complete deployment.

## Procedure


**Step 1** Log in to the [management console](#).

**Step 2** Locate the row containing the certificate you want to deploy on other cloud product, and click **Deploy** in the **Operation** to go to the certificate deployment details page.

**Figure 4-3** Deploy

**Step 3** On the displayed page, select **ELB** in the **Deployment Details** area.

**Figure 4-4** Selecting a cloud product

**Step 4** Click  on the right of the **Region** drop-down list and select the region where you want to deploy the certificate.

**Step 5** Select the domain name you want to update the certificate for and click **Update Certificate** in the **Operation** column.

To update the certificates for multiple domain names, select all the target domain names and click **Batch Update** above the domain name list.

**Figure 4-5** Updating a certificate

**Step 6** In the displayed confirmation dialog box, click **Confirm**.

**Figure 4-6** Certificate update confirmation box

If a message indicating that the certificate is updated successfully is displayed, the SSL certificate is updated for ELB.

----End

# 5 Managing SSL Certificates

## 5.1 Reissuing an SSL certificate

If you want to change the domain name after an SSL certificate is issued, submit an application to the CA and get the certificate reissued.

### Prerequisites

- The certificate is in the **Issued** state.
- The certificate is a single-domain or wildcard-domain certificate.

### Constraints

- Free certificates and multi-domain certificates cannot be re-issued.
- An issued certificate can be reissued within a specified period. The period varies depending on domain type and CAs. The following describes the period given by some CAs:
  - DigiCert and GeoTrust: 25 days.
- There is no limit on how many times you can apply for reissues of a single-domain or wildcard-domain certificate only when the reissue is requested within the specified period. This period varies depending on CAs.

### Procedure

**Step 1** Log in to the [management console](#).

**Step 2** In the **Operation** column of the target domain name, choose **More > Reissue**.

**Figure 5-1** Reissuing an SSL certificate

Certificate Name/ID	Domain Name	Certificate Type	Description	Certificate Expires At	Status/Application Progress	Auto-renewal	Enterprise Project	Operation
ra-sc	*.com	vTrust(1 year) DV	--	Jun 27, 2024 00:00:00 GMT+08:00	CA verifying (reissue)	--	--	Confirm Operation   Add to Project
wn-sc	*.com	GeoTrust(1 year) DV	--	Jul 11, 2023 20:30:00 GMT+08:00	Issued	Expire soon	default	Renew   Download   More
wn-sc	*.com	GeoTrust(1 year) DV	--	Jun 27, 2024 00:00:00 GMT+08:00	Issued	Off	default	Download   Deploy   More
wn-sc	*.com	GeoTrust(1 year) DV	--	Jun 27, 2024 00:00:00 GMT+08:00	Issued	Off	default	Download   Reissue   More
sc	*.com	GeoTrust(1 year) DV	--	--	Pending domain name verification	Off	wild_cert	Verify   Delete   New Application   Add to Project

 NOTE

If the reissue button disappears or the reissue failed, check the following items:

- Certificate status. The certificate you want to reissue must have been **issued**. If the certificate is not issued, it cannot be reissued.
- Certificate type. Free certificates and multi-domain certificates cannot be reissued.
- Certificate CA. If your certificate was issued by GlobalSign, a reissue can only be initiated within 5 days after the certificate was issued.
- Certificate CA. If your certificate was issued by DigiCert, GeoTrust, CFCA, TrustAsia, or vTrus, a reissue can only be initiated within 25 days after the certificate was issued.

**Step 3** To change the domain name for a certificate, perform operations by referring to [Table 5-1](#). You can also modify the company contact or authorizer information.

**Table 5-1** Domain name parameters

Parameter	Description	Example Value
CSR	<p>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.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>• <b>System generated CSR:</b> 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.</li> <li>• You manually generate a CSR file and paste the content of the CSR file into the text box.</li> </ul> <p>You are advised to select <b>System generated CSR</b> to avoid approval failure caused by incorrect content.</p>	System generated CSR
Domain Name	<p>This parameter is displayed when you purchase a single-domain or wildcard-domain certificate.</p> <ul style="list-style-type: none"> <li>• If you select <b>Upload a CSR for CSR</b>, the domain name is automatically parsed based on the CSR file. You do not need to manually enter the domain name.</li> <li>• If you select <b>System generated CSR for CSR</b>, manually enter the domain name or wildcard domain to be associated with the certificate.</li> </ul> <p>Single domain: If your domain is <i>www.domain.com</i>, enter <b>www.domain.com</b> for <b>Domain Name</b>.</p>	www.domain.com

Parameter	Description	Example Value
Domain Name Verification Method	<p>In accordance with the CA specifications, after applying for a certificate, you need to work with the CA to verify ownership of the associated domain name. After your ownership of the domain name is verified by you and approved by the CA, the CA will issue the certificate.</p> <p>Options:</p> <ul style="list-style-type: none"> <li>● <b>DNS:</b> You need to verify the domain ownership by resolving a specific DNS record on the domain name management platform. <ul style="list-style-type: none"> <li>– Manual DNS verification: You need to go to the DNS service provider of the domain name to perform the verification.</li> </ul> </li> <li>● <b>File:</b> You need to create a specified file on the server to verify your ownership of the domain.</li> <li>● <b>Email:</b> You can click the link and follow the directions in the email to verify ownership of the domain.</li> </ul>	Manual DNS verification

**Step 4** Click **Submit**.

1. After you submit the reissue application, the certificate status has changed to **CA verifying (reissue)**.
2. The CA will send an email to you within one to two working days to confirm the cancellation of the issued certificate. After you confirm the email, the CA will cancel the issued certificate and the certificate will enter the reissue process.

----End

## 5.2 Unsubscribing from an SSL Certificate

For SSL certificates you purchased on SCM, you can apply for a refund on the SCM console when the refund conditions are met.

This topic describes how to unsubscribe from an SSL certificate and get the refund.

### 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 SCM 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.

**CAUTION**

Only the fees you paid for purchasing or renewing SSL certificates or related service orders can be refunded. Vouchers or discount coupons you used cannot be refunded.

## Procedure

- Step 1** Log in to the [management console](#).
- Step 2** In the row containing the desired certificate, click **Unsubscribe** in the **Operation** column. [Figure 5-2](#) shows an example.

**Figure 5-2** Unsubscribing

Certificate Name	Domain Name	Certificate Type	Description	Certificate Expires At	Status/Application Progress	Operation
com-R	Single domain	GeoTrust (1 year) DV (Basic)	--	--	Pending application Application Progress	Apply for Certificate <b>Unsubscribe</b>
com-S	Single domain	GeoTrust (1 year) DV (Basic)	123	--	Pending application Application Progress	Apply for Certificate
16-5	16.com	-- (1 year)	--	Apr 27, 2019 20:00:00 GMT+08:00	Hosted Expired	Download Push Delete

- Step 3** 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 4** 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

## 5.3 Renewing an SSL Certificate

### 5.3.1 Performing a Manual Renewal

An SSL certificate issued by a CA is valid for one year. An expired SSL certificate cannot enable HTTPS-encrypted communication. To avoid this, manually renew the certificate before it expires.

#### Manual Renewal Restrictions

- The company name cannot be changed when you renew a certificate.
- The manual renewal entry is available only for **30 calendar days** before an SSL certificate expires.
- Only paid SSL certificates that have been purchased in Huawei Cloud SCM and are about to expire can be renewed. Uploaded certificates, free certificates, and single-domain expansion packages cannot be renewed.
- Manually 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.
- The renewal certificate and the original certificate are two independent certificates. Once the renewed certificate is issued, you need to install it on the web server the original one is deployed.
- The new certificate inherits the remaining validity period of the original certificate. 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.

**NOTICE**

- 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 automatically inherit** the remaining validity period (if any) of the original certificate. So, the validity period of the new certificate is one year.

**Prerequisites**

- The paid certificate is about to expire.

**Procedure**

1. Log in to the [management console](#).
2. In the row containing the desired certificate, click **Renew** in the **Operation** column. [Figure 5-3](#) shows an example.

**Figure 5-3** Renewal

Certificate Name	Domain Name	Certificate Type	Description	Certificate Expires At	Status	Application Progress	Enterprise Project	Operation
scm-be-09	example.com Single domain	GeoTrust (1 year) DV (Basic)	--	Dec 09, 2021 14:31:38 GMT+08:00	Issued	Expire soon Application Progress: [Progress Bar]	default	Renew Download More
scm-04	example.com Single domain	DigiCert (1 year) DV (Basic)	--	--	Pending domain name verification	Application Progress: [Progress Bar]	DBSS	Verify Domain Name Withdraw Application Add to Project


3. On the certificate renewal page, confirm the certificate information and click **Buy Now**.  
If you have any questions about the pricing, click **Pricing details** in the lower left corner.
4. Confirm the order information and agree to the CCM statement by selecting **I have read and agree to the Cloud Certificate Manager Statement**. Click **Pay**.
5. On the displayed page, select a payment method.  
After the payment is complete, go back to the certificate list to view the purchased certificate.  
In this case, the certificate is in the **Pending application**. To get it issued, submit a certificate application to the CA. The CA issues the certificate only after validating your renewal application.

**Follow-up Operations**

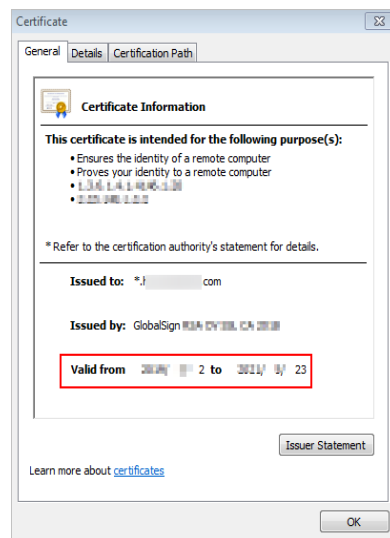
1. Submit a certificate application to the CA.  
For details, see [Submit an SSL Certificate Application to the CA](#).

**NOTICE**

When you provide the certificate application information, ensure that the company name is the same as that of the original certificate. The company name cannot be changed when you renew an SSL certificate.

2. Verify the domain name ownership.  
For more details, see [Verifying the Domain Name Ownership](#).
3. Verify the organization (required for OV and EV certificates only).  
For more details, see [Verify the Organization](#).
4. Issue the certificate.  
It will take some time for the CA to review your information. The CA will issue the certificate only after they validate your information.
5. Install the certificate.  
Install the issued certificate on your web server to replace the old certificate. If you do not install the new certificate on the web server, your server cannot use the HTTPS service after the old certificate expires.
6. Check whether the new certificate is successfully installed.  
After the new certificate is installed on the web server, check whether the certificate has been updated.
  - a. Visit your website using a web browser.
  - b. Click  in the address box of the browser to check whether the validity period of the certificate has been updated.  
If the validity period of the new certificate is displayed, the new certificate has taken effect.

**Figure 5-4** Validity Period



## 5.4 Revoking an SSL Certificate

You can revoke a certificate that has been issued by a CA. A revoked certificate is no longer trusted and can no longer be used for certificate-based encryption.

If you no longer need an issued SSL certificate for security reasons or other reasons, for example, the certificate key is lost, you can revoke the certificate on the SCM console.

After a certificate is revoked, all its records, including CA records, will be cleared and cannot be restored. Therefore, exercise caution when revoking a certificate.

## Prerequisites

The certificate is in the **Issued** state.

## Constraints

- Only issued certificates can be revoked.
- An uploaded certificate cannot be revoked.
- A certificate in the renewal period cannot be revoked. So, a certificate cannot be revoked within one month before it expires.
- After a certificate revocation application is submitted, it cannot be canceled. Certificate revocation does not affect the purchase of new certificates.

## Procedure

**Step 1** Log in to the [management console](#).

**Step 2** In the row containing the certificate you wish to revoke, in the **Operation** column, click **Revoke** or **More > Revoke**.

**Figure 5-5** Revoke

Certificate Name	Domain Name	Certificate Type	Description	Certificate Expires At	Status/Application Progress	Operation
scm-7732	www.***.com Single domain	GlobalSign (1 Year) OV	-	2031/02/07 12:40:30 GMT+08:00	Issued Application Progress	Download Push <b>Revoke</b> Delete
scm-6955	www.***.com Single domain	GeoTrust (1 Year) OV	-	2020/06/13 11:08:00 GMT+08:00	Issued Application Progress	Download Push Revoke Delete

**Step 3** (Optional) To revoke an OV or EV certificate, confirm the revocation by email.

After you submit a certificate revocation application, the CA will send a confirmation email to the email address you provide when you apply for the certificate. Check your email and confirm the certificate revocation in a timely manner.

After you confirm the revocation by email, the OV and EV certificates will be revoked.

----End

## 5.5 Deleting an SSL Certificate from CCM

Deleting an SSL certificate only removes it from . The certificate is still valid and trusted by web browsers after the deletion.

Follow the steps below to remove an SSL certificate you no longer need from CCM.

## Prerequisites

- Your paid certificate is in the **Issued**, **Revoked**, or **Expired** status.
- Your free certificate is in the **Pending application**, **Revoked**, or **Expired** status.

- Your uploaded certificate is in the **Hosted** state.

## Constraints

- Currently, free certificates in the **Issued** state cannot be deleted from the CCM console. To delete a free certificate in the **Issued** state, use the API. For details, see .
- After you delete a certificate, we will no longer keep it. You need to keep the certificate file and private key by yourself.
- A deleted certificate cannot be restored. Exercise caution when performing this operation.

## Procedure

**Step 1** Log in to the [management console](#).

**Step 2** In the row containing the certificate you wish to delete, in the **Operation** column, click **Delete** or **More > Delete**.

**Figure 5-6** Deleting a certificate

Certificate Name	Domain Name	Certificate Type	Description	Certificate Expires At	Status/Application Progress	Operation
scm7732	www.***.com Single domain	GlobalSign (1 Year) DV	-	2031/02/07 12:40:30 GMT+08:00	Issued Application Progress	Download Push Revoke <b>Delete</b>
scm6855	www.***.com Single domain	GeoTrust (1 Year) DV	-	2020/06/13 11:08:00 GMT+08:00	Issued Application Progress	Download Push Revoke Delete

**Step 3** In the dialog box that is displayed, click **Submit**. When **Certificate deleted successfully** is displayed in the upper-right corner, the certificate is deleted.

----End

## 5.6 Uploading an External Certificate to SCM

You can upload your SSL certificates (SSL certificates that have been purchased and issued on other platforms) to the CCM service for centralized management.

This topic describes how to upload a local (external) SSL certificate onto CCM.

### Prerequisites

You have prepared the following files to be uploaded:

- Certificate file in PEM encoding format (the file name extension is PEM or CRT).
- Certificate private key in PEM encoding format (the file name extension is KEY).

#### NOTE

- Currently, only certificates in PEM format can be uploaded to CCM. Certificates in other formats can be uploaded only after they are converted to certificates in the PEM format.
- The private key you want to upload cannot be protected by a password.

## Constraints

Expired certificates and certificates whose certificate chain length is 1 cannot be uploaded.

## Procedure

**Step 1** Log in to the [management console](#).

**Step 2** In the upper left corner above the certificate list, click **Upload Certificate**.

**Step 3** In the **Upload Certificate** dialog box, enter the certificate information.

**Figure 5-7** Uploading a certificate

### NOTE

- The uploaded certificate and key must correspond to each other.
- Ensure that the private key is not protected by a password.

**Step 4** Click **Submit** to upload the certificate.

When the certificate is uploaded successfully, a certificate in the **Hosted** state is added to the certificate list.

----End

## 5.7 Adding an Additional Domain Name

If you have a multi-domain SSL certificate and available quota for additional domain names, you can associate additional domain names to the certificate after it is issued.

This topic describes how to add additional domain names.

### Prerequisites

- The target certificate is in the **Issued** state.
- There is available quota for additional domain names.

### Constraints

- A certificate takes effect as of the date of the first issuance.
- You can download the certificate after you submit the new additional domain names for approval. However, the downloaded certificate does not protect these new domain names that are still being approved.
- After the approval completes and the certificates is issued, you can download the new certificate. The original certificate cannot be downloaded anymore. Keep it properly.

### Procedure

**Step 1** Log in to the [management console](#).

- Step 2** In the **Operation** column of the target certificate, click **More > Add Additional Domain Name**. The **Add Additional Domain Name** dialog box is displayed.
- Step 3** Complete the information based on site requirements. **Table 5-2** describes the required parameters. **Figure 5-8** shows an example.

**Figure 5-8** Adding an additional domain name

**Table 5-2** Parameters

Parameter	Description	Example Value
Adding an additional domain name	Additional domain names to be added	domain03.com domain04.com
Email Address	Enter a correct email address. After the certificate is submitted for review, notifications about certificate issuing will be sent to this email address. Please check it in time. <b>NOTICE</b> A CA sends confirmation emails to the email address of the domain name administrator. After submitting your application for approval, log in to the domain name administrator's mailbox, check for the confirmation email, and perform the confirmation required in the email.	-

- Step 4** Click **OK**.

After you submit the request for adding additional domain names, the SSL certificate management page is displayed, and the certificate status changes to **CA verifying (domain name addition)**.

----End

## Follow-up Procedure

After the certificate approval request is submitted, the CA sends a domain name verification email to your email address. You need to verify the domain name as required. Your certificate will remain in the **CA verifying (domain name addition)** state and will not be approved if you do not complete the domain name verification. Upon receiving your request, the CA will review your request and send a verification email. Reply to the CA immediately after receiving the verification email. If you fail to complete the verification timely, it takes longer to receive your certificates.

Domain name verification is required if you want to add an additional domain name. The certificate can be issued after the domain name is verified and approved by the CA.

## Other Operations

If you want to change the additional domain name or change the email address of the contact person after an additional domain name is submitted for approval, you can withdraw the application. Perform the following steps:

**Step 1** Log in to the [management console](#).

**Step 2** In the **Operation** column of the target certificate, click **Withdraw Application**. The **Cancel Application** dialog box is displayed.

**Step 3** Click **Submit**.

If **Request for canceling the application submitted successfully** is displayed in the upper right corner of the page, the request is canceled successfully.

At this time, the certificate is still in the **CA verifying (domain name addition)** state. After the application is canceled successfully, the certificate status changes to **Issued**.

----End

## 5.8 Withdrawing an SSL Certificate Application

This topic describes how to withdraw a certificate application.

You can withdraw the application for a certificate whose information is being approved or for which verification by DNS is in progress.

After you withdraw the application, the CA will stop approving its information. Exercise caution with the withdrawal. However, the certificate may have been approved by the CA before you withdraw a certificate application due to a procedure processing cause. In this case, application withdrawal will fail. The withdrawal result is given in the certificate list.

### Prerequisites

The certificate is in the **Pending domain name verification**, **Pending organization verification**, or **CA verifying (domain name addition)** state.



## Constraints

- After a certificate deletion or revocation application is submitted, it cannot be withdrawn.
- After a certificate is withdrawn, the certificate is in the **Pending application** status. To reissue it, apply for the certificate and complete the domain name ownership and organization verification again.

## Procedure

**Step 1** Log in to the [management console](#).

**Step 2** In the row containing the certificate you wish to withdraw your application for, in the **Operation** column, click **Withdraw Application**.

**Figure 5-9** Withdrawing an application

Certificate Name	Domain Name	Certificate Type	Description	Certificate Expires At	Status/Application Progress	Operation
scm-4229	1631.com Single domain	GlobalSign (1 Year) DV	-	-	Pending organization verification Application Progress	Verify Organization <b>Withdraw Application</b> More
1631.com	1631.com Single domain	GeoTrust (1 Year) DV	-	-	Pending organization verification Application Progress	Verify Organization More

**Step 3** 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**.

### NOTICE

After you withdraw the application, the CA will stop approving its information. Exercise caution with the withdrawal. However, the certificate may have been approved by the CA before you withdraw a certificate application due to a procedure processing cause. In this case, application withdrawal will fail. The withdrawal result is given in the certificate list.

----End

## Other Operations

After the certificate status changes to **Pending application**, you can then apply for a certificate again.

## 5.9 Canceling Authorization for Privacy Information

This topic describes how to cancel the authorization for privacy information.

After a user applies for a certificate, the user can cancel authorization for privacy information when the certificate is not being approved (that is, the certificate is not in the **Pending domain name verification**, **Pending organization verification**, **To be issued**, or **CA verifying (domain name addition)** state).

Once you revoke the authorization, will not store your information. The contact name, phone number, email address, and organization details will be deleted.

## Prerequisites

- You have applied for a certificate.
- The certificate is not being approved (that is, the certificate is not in the **Pending domain name verification**, **Pending organization verification**, **To be issued**, or **CA verifying (domain name addition)** state).

## Constraints

- Canceling authorization for privacy information is not allowed when the certificate is in any of the following statuses: **Pending domain name verification**, **Pending organization verification**, **To be issued**, or **CA verifying (domain name addition)**.
- All privacy information of the certificate cannot be restored once the authorization is canceled. Exercise caution when performing this operation.

## Procedure

**Step 1** Log in to the [management console](#).

**Step 2** Click the name of the target certificate. The certificate details page is displayed.

**Step 3** At the bottom of the certificate details page, find the configuration item **Privacy Authorization**.

**Figure 5-10** Privacy authorization



**Step 4** Disable privacy authorization.

**Step 5** In the displayed **Cancel Authorization for Privacy Information** dialog box, click **Submit**.

If the message **Authorization for privacy information canceled successfully** is displayed, the operation is successful.

In this way, your privacy information will not be displayed on the **Applicant/ Organization Information** page.

----End

## 5.10 Pushing an SSL Certificate to Other Cloud Services

### Prerequisites

The certificate is in the **Issued** or **Hosted** state.

### Constraints

- If you choose to manually generate a CSR when applying for a certificate, the issued certificate **cannot** be pushed to other cloud services.
- If you have not purchased a given 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 process may fail.

- A certificate can only be pushed to a product once in SCM. If you push a certificate that has been pushed or uploaded to a cloud product, a push failure will occur.

## Procedure


**Step 1** Log in to the [management console](#).

**Step 2** In the **Operation** column of the certificate you want to push, click **More** > **Push** to go to the certificate push details page.

**Step 3** Select the cloud service you wish to push the certificate to.

**Figure 5-11** Selecting a cloud service

**Step 4** (Optional) Perform this step if a certificate is to be pushed to WAF or ELB.


Click  on the right of the destination project and select the destination region.

**Step 5** Click **Push Certificate** at the lower right corner of the page.

If a message indicating that the certificate is successfully pushed is displayed, the SSL certificate is successfully pushed to the target service.

You need to further configure the certificate on the console of the service to enable HTTPS for it.

**Step 6** Check whether you need to immediately access the console of the target service to configure the certificate.

- If yes, click **Configure Now**. The management page of the target service is displayed. Configure the certificate:
- If no, click **Continue Pushing** or  in the upper right corner of the page. The certificate push page or SSL certificate management page is displayed. You can access the console of the target service for certificate management.

You can view the latest 10 push records on the certificate push page.

----End

## Follow-up Operation

You can manage pushed certificates on the console of the corresponding service.

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

- 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. If a certificate has been configured in WAF, you only need to update the certificate.

## 5.11 Viewing Details About an SSL Certificate

This topic describes how to view details of an SSL certificate, including an external certificate you uploaded to SCM.

You can view the certificate approval progress, modify the certificate name and description, and view the expiration date. For hosted or issued certificates, a certificate expiration reminder will be displayed in the **Status/Application** column on the console 30 days before a certificate expires.

### Prerequisites


You have purchased or uploaded a certificate.

### Procedure

**Step 1** Log in to the [management console](#).

**Step 2** View the certificate information. [Table 5-3](#) describes the certificate parameters.

#### NOTE

- The **All statuses** drop-down box enables you to specify a status so that only certificates of that status are displayed in the list.
- Enter a keyword of certificate names or associated domain names and click  or press **Enter** to search for specific certificates.
- Click the name of a certificate to view its details.
- For hosted or issued certificates, a certificate expiration reminder will be displayed in the **Status/Application** column on the console 30 days before a certificate expires.

**Table 5-3** Parameter description

Parameter	Description
Certificate Name	After you purchase a certificate or apply for a free certificate, a certificate name will be generated automatically. You can change the certificate name. For more details, see <a href="#">Changing the Name and Description of a Certificate</a> .
Domain Name	Domain name associated with the certificate
Certificate Type	Type of a certificate you specify when you purchase it
Remarks	Additional information about a certificate. You can modify the description. For more details, see <a href="#">Changing the Name and Description of a Certificate</a> .

Parameter	Description
Expiration time	Date when a certificate expires <b>NOTE</b> For issued certificates, SCM automatically notifies you of the expiration by email and SMS two months, one month, one week, three days, and one day before a certificate expires and again when the certificate actually expired.



Parameter	Description
<p>Status/ Application Progress</p>	<p>Options:</p> <ul style="list-style-type: none"> <li>● <b>Pending application</b> You need to submit information, such as domain name and user information, for a certificate. The application progress is 0%.</li> <li>● <b>Pending domain name verification</b> A certificate application request has been submitted, and domain name verification is to be completed by the CA. The application progress is 40%.</li> <li>● <b>Pending organization verification</b> 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. The application progress is 70%.</li> <li>● <b>To be issued</b> Certificate application, domain name verification, and organization verification have been completed for the purchased certificate. It is waiting for the CA to issue the purchased certificate. The application progress is 90%.</li> <li>● <b>Issued</b> Information you submitted about the certificate has been approved, and domain name and organization verification succeed. The application progress is 100%.</li> <li>● <b>Approval failed</b> Information fails to be approved.</li> <li>● <b>CA verifying (domain name addition)</b> An application for adding a domain name has been submitted for a multi-domain certificate. The CA is verifying the added domain name.</li> <li>● <b>CA verifying (application withdrawal)</b> The certificate application withdrawal has been submitted and is waiting for verification from the CA.</li> <li>● <b>CA verifying (revocation)</b> The certificate revocation application has been submitted and is waiting for verification from the CA.</li> <li>● <b>Revoked</b> The certificate has been revoked.</li> <li>● <b>Hosted</b> The uploaded certificate is in the <b>Hosted</b> state.</li> <li>● <b>Expired</b> Your certificate has expired. If a certificate expires, it cannot be renewed. You can request a new one.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>CA verifying revocation (pending domain name verification)</b> A certificate revocation request has been submitted, and domain name verification is to be completed by the CA.</li> </ul>
Operation	You can perform operations, such as apply for a certificate, verify a domain name, verify an organization, and withdraw the application, in the <b>Operation</b> column.

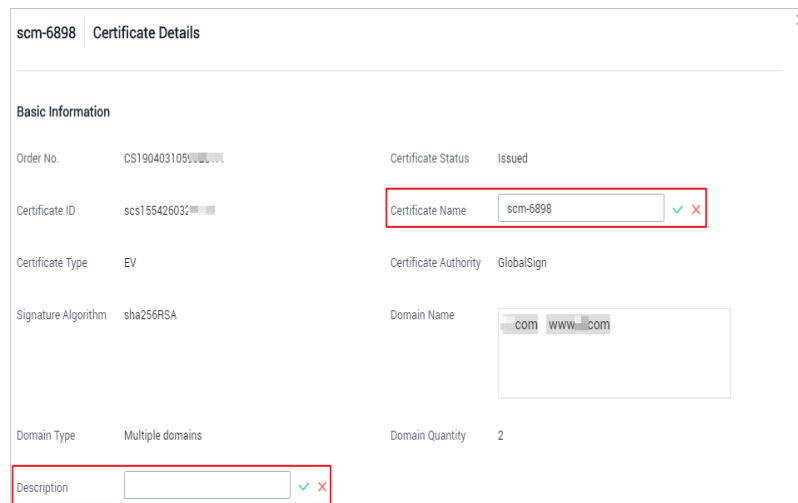
----End

## Changing the Name and Description of a Certificate

- Step 1** Log in to the [management console](#).
- Step 2** Click the name of the target certificate. The certificate details page is displayed.
- Step 3** Change the certificate name and description.

Click  on the right of **Certificate Name** (or **Description**). Enter the certificate name (or description) in the editing box and click  to save the change. When **Changed successfully** is displayed in the upper right corner, the change to the certificate name (or description) is successful.

**Figure 5-12** Changing the Name and Description of a Certificate



----End

## 5.12 Viewing the Application Progress

This topic describes how to view the approval progress of the certificate application.

You can perform operations based on the prompt in the application progress to obtain the certificate as soon as possible.

## Prerequisites

- You have purchased a certificate.
- You have submitted a certificate application to the CA.

## Procedure

**Step 1** Log in to the [management console](#).

**Step 2** View the certificate application progress in the **Status/Application Progress** column of the certificate. [Figure 5-13](#) shows an example.

**Figure 5-13** Viewing the Application Progress

Certificate Name	Domain Name	Certificate Type	Description	Certificate Expires At	Status/Application Progress	Operation
scm-75911	Single domain	GlobalSign (1 Year) DV	12	--	Pending application Application Progress 0%	Apply for Certificate
aaa	Single domain	GeoTrust (1 Year) DV	test	2020/03/05 20:00:00 GMT+08:00	Expired	Download Delete

Perform operations based on the certificate status. The following are examples of some important operations:

- **Pending application:** The domain name and user information must be submitted for the purchased certificate. The certificate application progress is 0%.
- **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. 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. 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**.

----End



# 6 Permissions Management

---

## 6.1 Creating a User and Granting SCM Permissions

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to SCM resources.
- Grant only the permissions required for users to perform a task.
- Entrust a Huawei Cloud account or cloud service to perform professional and efficient O&M to your SCM resources.

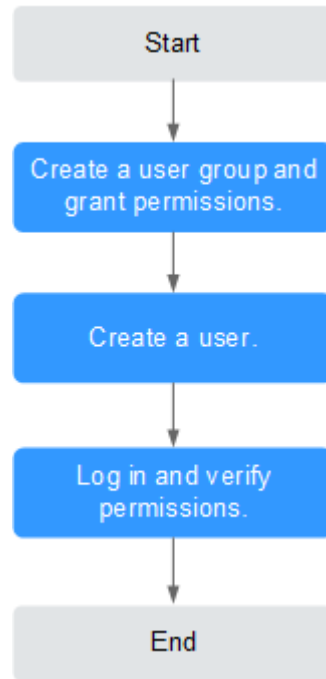
If your Huawei Cloud account does not require individual IAM users, skip this chapter.

This topic describes the procedure for granting permissions (see [Figure 6-1](#)).

## Prerequisites

### Process Flow

**Figure 6-1** Process for granting SCM permissions



1. to it.  
Create a user group on the IAM console and grant the user group the **SCM Administrator** permission for SCM.
2. Create a user on the IAM console and add the user to the group created in **1**.
3. and verify permissions.  
Log in to the CCM console by using the created user, and verify that the user only has read permissions for CCM.  
Choose **Cloud Certificate Management Service** under **Security** in the **Service List**. If no message appears indicating that you have insufficient permissions to access the service, the **SCM Administrator** policy has already taken effect.

## 6.2 Custom Policies for SCM

Custom policies can be created to supplement the system-defined policies of CCM.

### Example Custom Policies

- Example 2: denying certificate deletion  
A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

If you need to assign permissions of the **SCM Administrator** policy to a user but you want to prevent the user from deleting certificates, you can create a custom policy for denying certificate deletion, and attach both policies to the group that the user belongs to. Then, the user can perform all operations on certificates except deleting certificates. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "scm:cert:delete"
      ],
      "Effect": "Deny"
    }
  ]
}
```

- **Example 3: Defining permissions for multiple services in a policy**  
A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

# A Change History

---

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