Cloud Certificate Manager

SSL Certificate Manager (SCM) User Guide

Issue 23

Date 2024-09-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 About SCM and SSL Certificate Usage

SCM provides certificates of multiple types issued by different CAs. For more details, see **Differences Between SSL Certificate Types**. This document describes the process of how to purchase and use an SSL certificate.

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

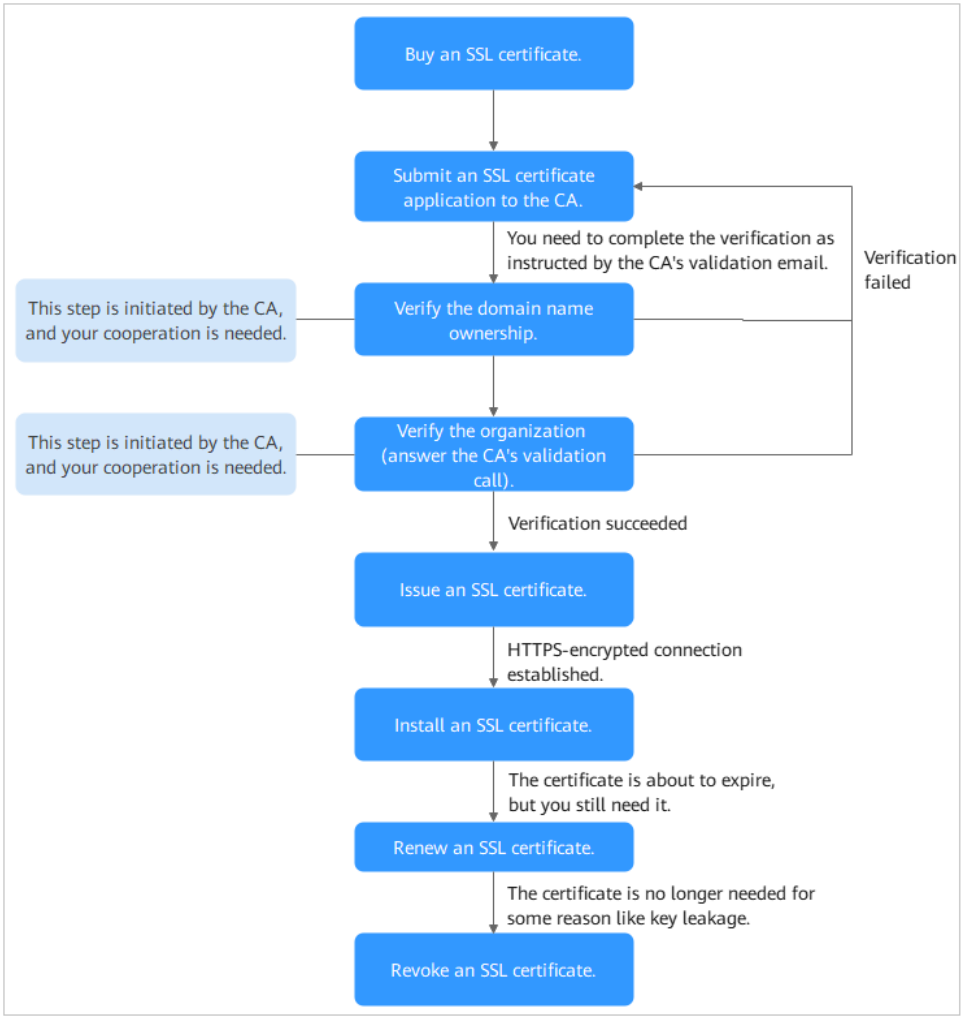


Table 1-1 Certificate usage process

Step	Operation	Description
1	**Purchasing an SSL Certificate**	On the SCM platform, purchase an SSL certificate for your domain name. For more details, see **Differences Between SSL Certificate Types** and **How Do I Select an SSL Certificate?**
2	**Submitting an SSL Certificate Application to the CA**	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	**Verifying the Domain Name Ownership**	You need to work with the CA to complete the domain name ownership verification. SCM provides the following domain name ownership verification methods: • Automatic DNS verification can be used for certificates that meet stated **conditions**. • Manual DNS verification: suitable for all types of certificates. • Email verification: suitable for OV and EV certificates only. • **File Verification**: This method is optional only for OV and EV certificates.
4	**Verifying the Organization (for OV and EV Certificates)**	This operation is required only when you apply for an OV, OV Pro, EV, or EV Pro certificate. After the domain name ownership is verified, the CA will initiate organization verification.
5	**Issuing an SSL Certificate**	When the verification is complete, it takes some time for the CA to approve your verification. For details, see **How Long Does It Take to Approve an SSL Certificate?** 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.
6	**Installing an SSL Certificate**	You can deploy the issued certificate in other Huawei Cloud services in just a few clicks or download the certificate and install it on a server. • You can use SCM to quickly deploy SSL certificates to other cloud services to improve their data access security. • An SSL certificate cannot enable HTTPS-encrypted communication until it is installed on the web server housing the service.

Step	Operation	Description
7	**Renewing an SSL Certificate**	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 enable auto-renewal or manually renew the certificate 30 days before it expires to prevent your services from being affected. 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 or deploy it on other Huawei Cloud services to replace the old certificate that is about to expire.
8	**Revoking an SSL Certificate**	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. 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.

2 Purchasing an SSL Certificate

In CCM, you can buy and request for many types of SSL certificates from multiple certificate authorities who win the trust globally.

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.

For details, see **Permissions Management**.

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

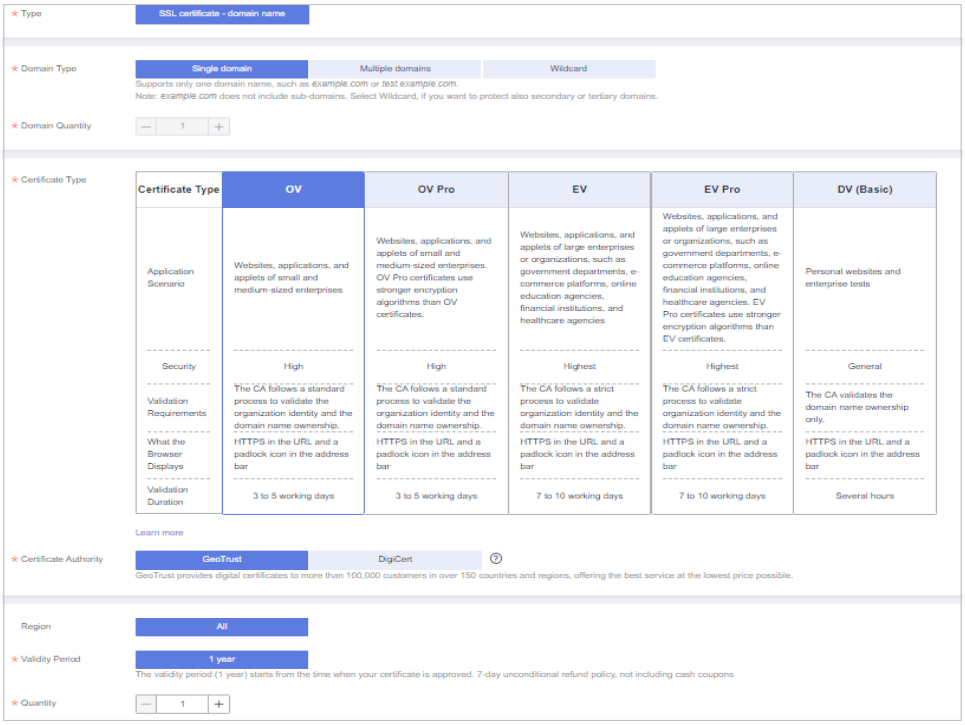
Step 1 Log in to the **management console**.

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**,, **Quantity**, and **Tags**, as shown in the following figure.

Figure 2-1 Certificate selection



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.

Domain Type	Description
Multiple domains	Multiple domain names can be associated with an SSL certificate. – You can associate a multi-domain certificate with up to 250 domain names. – 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 – 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. – 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.
Wildcard domain	Only one wildcard domain can be associated with an SSL certificate. Domain names having multiple wildcard characters, such as *.*.example.com, are not supported. 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.
For details about how to select a domain type, see **How Do I Select an SSL Certificate?**	

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	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.	CAs will verify the organization identity and the domain name ownership.	Highest	7 to 10 working days
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

Certificate Type	Application Scenario	Verification Requirements	Security	Approval Period
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
DV (Basic)	Personal websites and enterprise tests.	The CA verifies the domain name ownership only.	General	Several hours
For more details, see **Differences Between Certificate Types**				

4. Select a certificate authority.

   DigiCert and **GeoTrust** are available CAs in CCM. For more details, see **Differences Between Certificates Types**.

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

   The validity period of a certificate starts from the time the certificate is issued. After a certificate expires, a new one must be purchased.

   If you have not enabled auto-renewal, manually renew the certificate or purchase another one 3 to 10 working days before it expires. If you have enabled auto-renewal, check the validation emails from the CA and finish required verification 3 to 10 working days before it expires to ensure that the certificate is valid before the CA validates your verification and issues a new certificate.

6. Set the number of certificates you want to buy in the **Quantity** field.
7. (Optional) Tags: Add a tag to the purchased certificate. For details, see **Creating a Tag**.

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 successful, you can go to the **SSL Certificate Manager** > **SSL Certificates** page to view certificates you purchased.

- To view your paid certificates, click the **SSL Certificates** tab.
- To view your test certificates, click the **Test Certificates** tab.

----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. For details, see **Purchasing an SSL Certificate**.

Constraints

- A Chinese domain name can only be associated with a certificate when it is encoded with **Punycode**.
- If the domain name associated with your DV certificate contains special words, such as edu, gov, bank, and live, the certificate may fail to pass the security review. In this case, select an OV or EV certificate. For details about known special words, see **Immoderate Words**.
- Each CA has different promotion activities for www domain names. For details, see **Certificate Authorities**.

Procedure

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

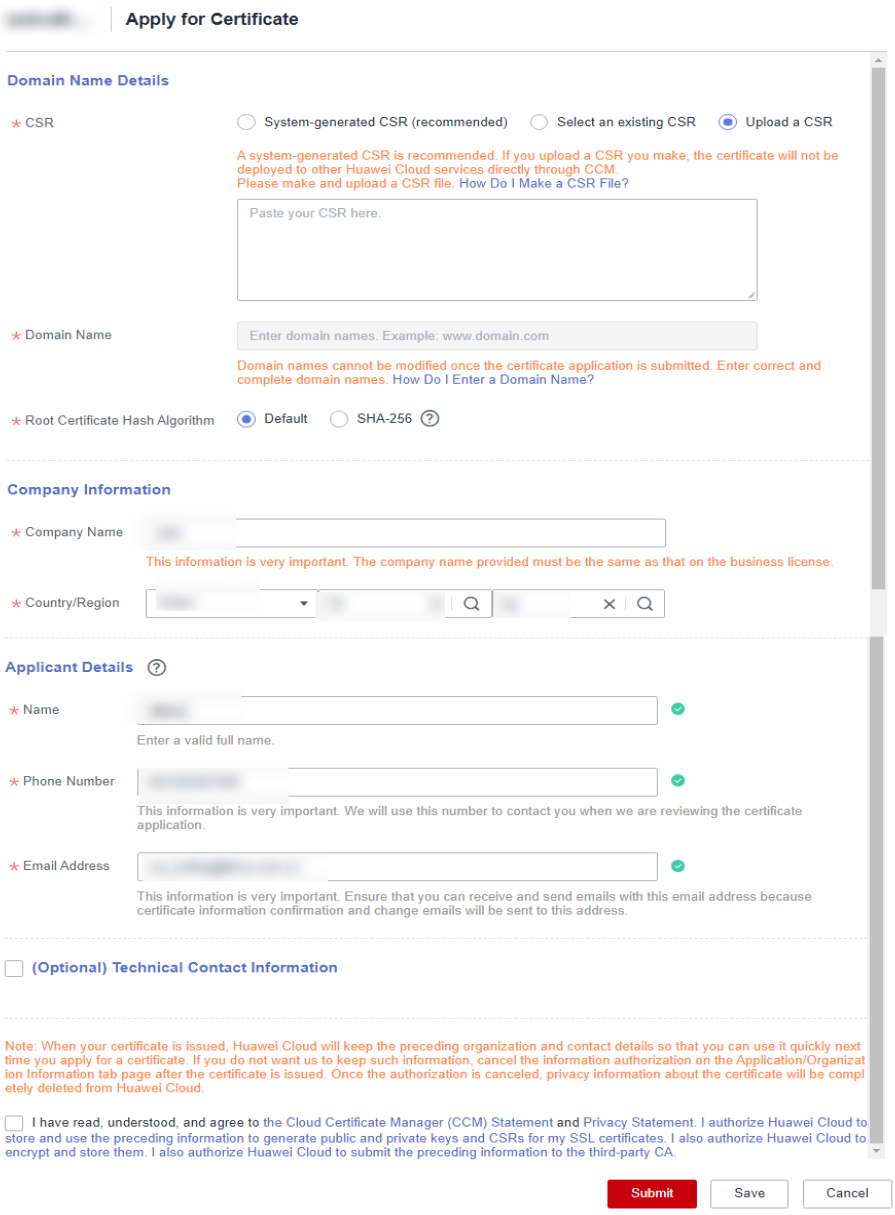
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

Step 3 In the navigation pane on the left, choose **SSL Certificate Manager** > **SSL Certificates**. In the row containing the desired certificate, click **Apply for Certificate** in the **Operation** column.

- To submit a paid certificate application, click the **SSL Certificates** tab, select the certificate and submit it.
- To submit a test certificate application, click the **Test Certificates** tab, select the certificate and submit it.

Step 4 On the displayed page, enter the domain name, organization, and applicant information.

Figure 3-1 Domain name and other information



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.

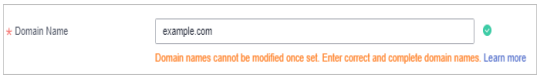
   CSR file generation method:

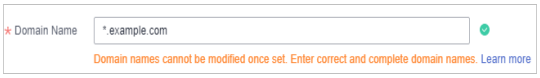
- **System generated CSR** (recommended): The system automatically generates a certificate private key. Once the certificate is issued, you can download your certificate and private key on the certificate management page.
- **Select an existing CSR**: Select a CSR file that you have created in or uploaded to the **CSRs** tab. For details, see **Creating a CSR** and **Uploading a CSR**.
- **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?**

For details about the differences between the two types of certificate request files, see **What Are the Differences Between the CSR Generated by the System and the CSR Made by Yourself?**

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	Enter one domain name to be associated. For example, if the domain name is example.com, configure the parameters as shown in the following figure. 
Multiple domains	The primary domain name and additional domain name must be configured. 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.  **NOTE** ■ 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. For more details, see **Adding an Additional Domain Name**. ■ One additional domain name per line. ■ A primary domain and additional domains can be equally protected.

Type	Description
Wildcard domain	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. 
To associate a Chinese domain name with a certificate, 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**.	

3. **Root Certificate Hash Algorithm**

   If you purchase a GeoTrust or 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. **Key Algorithm**

   Select an algorithm for the certificate. The default cryptographic algorithm is **RSA_2048**. Available cryptographic algorithms:

   - **Rivest–Shamir–Adleman (RSA)** is an asymmetric cryptographic algorithm that is widely used around the world. It has the best compatibility among the three algorithms and supports mainstream browsers and all-platform OSs. Generally, RSA uses a 2048-bit or 3072-bit key.
   - **Elliptical curve cryptography (ECC)** features faster encryption, higher efficiency, and lower server resource consumption compared with RSA. ECC is being promoted in mainstream browsers and is becoming a next-generation mainstream algorithm. Generally, ECC uses a 256-bit key.

   For details, see **cryptographic algorithms supported**.

5. **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.

6. **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.

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

Step 6 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 Domain Name Verification Overview

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
Automatic DNS Verification	With your authorization, SCM modifies the record set configured for the domain name. SCM automatically adds a record to the record set for verification.	• Your certificate is a DV (for domain name) certificate. • Your certificate is used for a domain name that you apply for on Huawei Cloud and is hosted on Huawei Cloud DNS. The system performs automatic DNS verification only when all the preceding conditions are met.
Manual DNS Verification	You add a record to the record set configured for the domain name for verification.	• You have the permission to modify the DNS resolution settings. • You have selected manual DNS verification for domain name verification method when applying for the certificate. (This is not required for DV certificates.)
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.	You have the permission to log in to the domain name administrator's mailbox. You have the domain name management permission.
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.	• 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. • Port 80 or 443 is enabled on the server to listen to HTTP or HTTPS requests. **CAUTION** 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.

3.2.2 Method 1: Automatic DNS Verification (for DV Certificates)

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.

In automatic DNS verification, you can authorize SCM to modify the record set of the domain name. In this case, a record is automatically added to the record set for verification. If the CA verifies that the added record can be resolved, the verification is successful.

This topic describes how to enable SCM to automatically verify your domain name ownership.

Constraints

The system performs automatic verification only when all the following conditions are met:

- Your certificate is a DV (for domain name) certificate.
- Your certificate is used for a domain name that you apply for on Huawei Cloud and is hosted on Huawei Cloud DNS.

Procedure

No further operations are required if you have set the verification mode to Automatic DNS verification.

Wait for the system to verify the ownership for you. After you complete the DNS verification at your side, it takes two to three working days for the CA to review the DNS information you provided. After the CA validates your DNS information, they will issue the certificate.

3.2.3 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
The domain name management platform is Huawei Cloud.	Complete all subsequent steps.
Platforms other than our platform	Are you sure you want to migrate the domain name from another service provider to Huawei Cloud DNS? • If your answer is "Yes", perform the following steps: 1. Migrate the domain name from another DNS service provider to HUAWEI CLOUD DNS. 2. Complete all subsequent steps. • If your answer is "No", perform the verification on the corresponding platform. For example, if your domain is hosted on Alibaba Cloud, perform the verification on Alibaba Cloud.

Step 2: Obtaining Verification Information

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

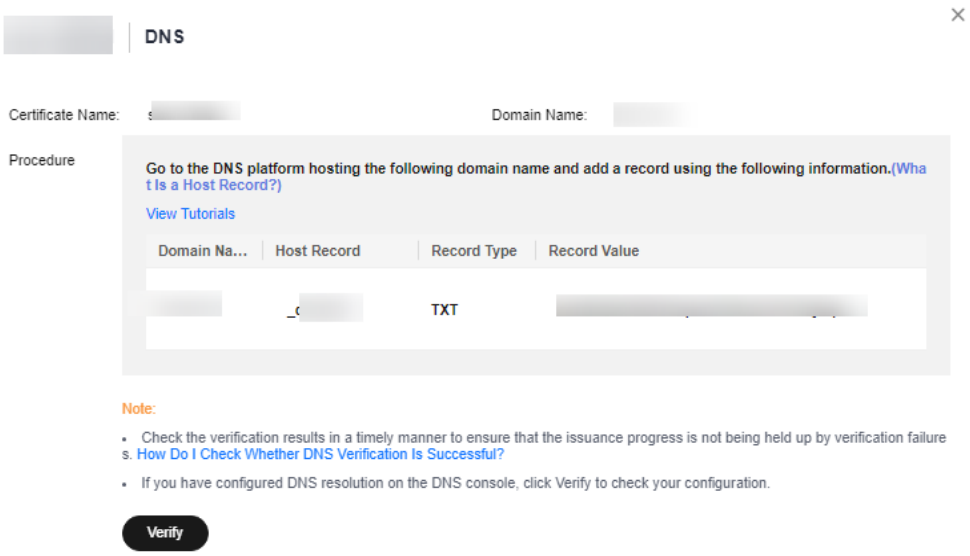
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

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 3-2** 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 3-2 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 **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.

Figure 3-3 Adding a record set

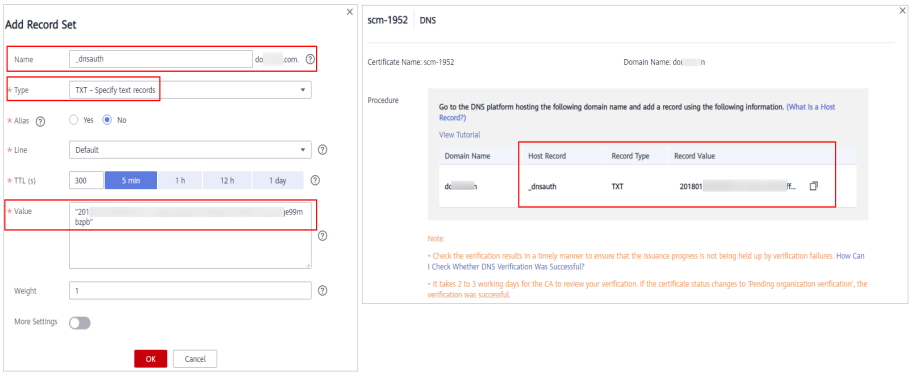


Table 3-3 Parameters for adding a record set

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 **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 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

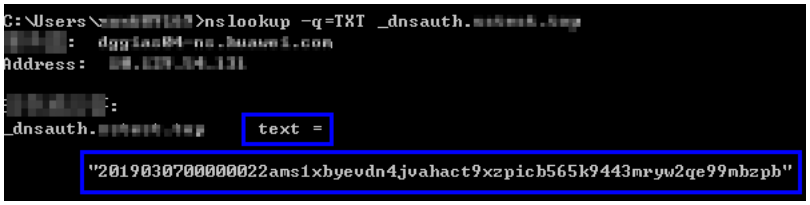
Record Type	Verification commands
TXT	**nslookup -q=TXT** *xxx*
CNAME	**nslookup -q=CNAME** *xxx*

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 3-4** shows an example.

  Figure 3-4 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.

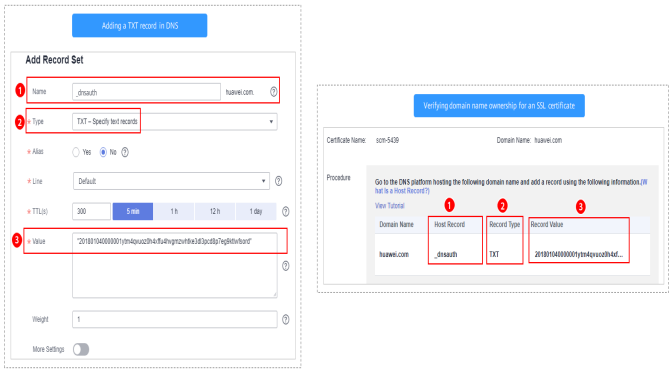
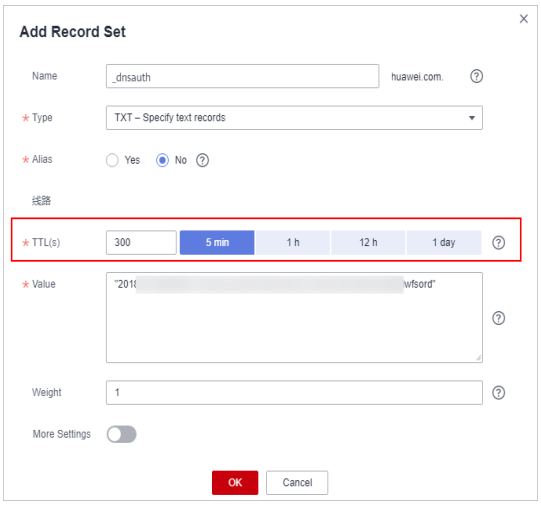
  Figure 3-5 Non-effective domain name verification configuration

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 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 **Host Record**, **Type** or **Value**. **Figure 3-6** Adding a record 
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 in 5 minutes by default. If the configured effective time does not arrive, verify after the time is right. **Figure 3-7** Setting TTL 

----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.

- **DV certificates**

  You can manually verify the result on the domain name verification page.

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

  b. 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.

  c. Click **Verify** to verify the DNS resolution configuration.

     - If the system displays "Verification succeeded. Your certificate is on the way.", the certificate will be issued within 1 minute. Refresh the page to view the certificate status then.
     - If the verification fails, fix issues by referring to **Why Did the DNS Verification for a DV Certificate Fail?** Then, perform the verification again 3 to 5 minutes later.

Why Did the DNS Verification for a DV Certificate Fail?

Failure Message	Solution
Too many verification requests. Try again later.	You may submit too many verification requests in a short time. Wait for 3 to 5 minutes and then perform the verification.
DNS records do not match.	The DNS record you configured is incorrect. Obtain the correct record by referring to **Step 2 Obtaining Verification Information** and configure the DNS record again.

Failure Message	Solution
DNS verification failed. Try again later.	Check whether the following problems exist: • Problem 1: The DNS record does not take effect. Solution: The configured DNS record does not take effect immediately, which depends on the TTL time set on your DNS server. So, wait for 3 to 5 minutes and then perform the verification again. • Problem 2: DNS records are correctly configured, but the verification still fails. Solution: The CA verification server is located outside China. There might be network errors sometimes. Try again about 1 to 2 hours later. • Problem 3: The domain name has not been licensed or passed the real-name authentication. Solution: Have the domain name licensed and complete real-name authentication first. Then, verify the domain name ownership again. • Problem 4: The domain name has a CAA record set. Solution: Delete all CAA records from the domain name resolution record sets. • Problem 5: The CA verification server does not find the DNS resolution record. Solution: The CA verification server is located outside China. So, you need to allow servers outside China to access the domain name temporarily.

3.2.4 Method 3: File 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 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. If the CA verifies that the file path can be accessed, the verification is successful.

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

Prerequisites

Port 80 or 443 is enabled on the server.

NOTE

CAs send authentication requests only to port 80 or 443.

Constraints

- Only DV single-domain free certificates support file verification.

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 3-8 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 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. Perform operations as required.

The following uses Windows servers as an example. Assume that the root directory of the website is **/www/htdocs**.

1. On the Windows menu, click **Start** and enter **cmd** to start the command dialog box.
2. Run the following command to go to the disk where the root directory of the website is located. In this example, drive **D** is such a disk.

   d:
3. Run the commands below to 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.

   ```
   cd /www/htdocs
   mkdir .well-known
   cd .well-known
   mkdir pki-validation
   cd pki-validation
   ```
4. Run the command below to create the **fileauth.txt** file in the **.well-known/pki-validation** subdirectory.

   NOTE

   The following uses the **fileauth.txt** returned by the GeoTrust as an example. Replace **fileauth.txt** with the actual file name.

   echo off>fileauth.txt
5. Run the following commands to open the **fileauth.txt** file:

   start fileauth.txt
6. Put the record you obtained in **Step 4** into the **fileauth.txt** file and choose **File** > **Save** in the upper left corner.

----End

Step 3: Checking Whether the Verification Configuration Takes Effect

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

3.2.5 Email 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.

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 ownership, 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 (OV and EV)

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.

You can perform verification by phone calls, emails, or lawyer's letters.

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 DV certificates, it takes some while for the CA to review your information after the DNS verification succeeds. The certificate will be issued after being approved by the CA.
- 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 **working days**.
OV	The CA manually reviews the information. If the information is valid, the review takes 3 to 5 **working days**.
DV	No manual review is required. The CA system automatically checks domain name ownership. The certificate can be issued within several hours if the CA validates your ownership. You need to ensure that your DNS configurations are valid.

Procedure

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

You can deploy the issued certificate in other Huawei Cloud services in just a few clicks or download the certificate and deploy it on a server.

For details about how to deploy a certificate, see **Deploying an SSL Certificate in Other Cloud Products**.

Downloading a Certificate.

4 Installing an SSL Certificate

4.1 Installing an SSL Certificate on a Web Server

4.1.1 Downloading an SSL Certificate

After an SSL certificate is issued, you need to download it. Then, you can install it on your web server and modify server configuration to let the SSL certificate work.

This topic describes how to download an SSL certificate on the SCM platform.

Prerequisites

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

Constraints

- A certificate can only be downloaded when it is in its validity period.
- If you select **System generated CSR** for **CSR**, the downloaded file package contains folders **Apache**, **IIS**, **Nginx**, and **Tomcat** and file **domain.csr**.
- If you select **Upload a CSR** for **CSR**, the downloaded file package contains only file **server.pem**. The file contains two segments of certificate code, namely, the server certificate and intermediate CA certificate. Huawei Cloud SCM does not store your private keys. Keep them properly, so keep them safe.

Procedure

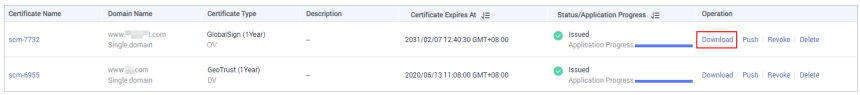
Step 1 Log in to the **management console**.

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**.

Step 3 In the navigation pane on the left, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 In the **Operation** column of the row containing the desired certificate, click **Download**.

Figure 4-1 Downloading a certificate



Step 5 In the **Operation** column, click **Download** to download the certificate you need.

Step 6 Install the certificate on the corresponding server for the SSL certificate to work.

The procedure for installing an SSL certificate varies depending on the web server. The following describes how to install an SSL certificate on mainstream web servers.

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

----End

Description of Downloaded Certificate Files

Different types of certificate files can be downloaded depending on if you select **System generated CSR** or **Upload a CSR** when you applied for the certificate.

- **System generated CSR**

  The downloaded certificate package contains **Apache**, **IIS**, **Nginx**, and **Tomcat** folders as well as the **domain.csr** file. See **Table 4-1** for details. **Figure 4-2** shows an example.

Figure 4-2 Decompressing an SSL certificate package

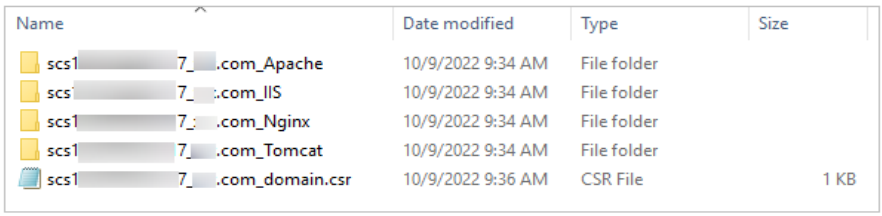


Table 4-1 Description of files/folders in the downloaded certificate

File/Folder Name	Content
Tomcat	**keystorePass.txt**: certificate password **server.jks**: certificate file
Nginx	**server.crt**: certificate file, which contains two segments of certificate code (server certificate and intermediate CA certificate respectively) **server.key**: certificate's private key file, which contains a segment of private key code of the certificate

File/Folder Name	Content
Apache	**ca.crt**: certificate chain file, which contains a segment of intermediate CA code. **server.crt**: certificate file, which contains a segment of server certificate code **server.key**: certificate's private key file, which contains a segment of private key code of the certificate
IIS	**keystorePass.txt**: certificate password **server.pfx**: certificate file
domain.csr	Certificate signing request.

- **Upload a CSR**

  The downloaded certificate package contains only the **server.pem** file. The file contains two segments of certificate code, namely, the server certificate and intermediate CA certificate.

  Huawei Cloud SCM does not store your private keys. Keep them properly, so keep them safe. When installing the certificate on a server, you will need to provide the file path to the location of your private keys.

  NOTE

  If you select **Upload a CSR** for **CSR**, the certificates cannot be directly deployed in other cloud services.

4.1.2 Downloading a Root Certificate

If your customers use browsers to access your web services, there is no need to download a root certificate because the SSL certificate you download and install on your web server already contains the corresponding root certificate.

If your customers use a client like Java to access your web services, a root certificate needs to be manually download and installed on the client to ensure that the client can validate the encrypted information on the server. For example, if a GeoTrust EV SSL certificate is installed on your web server, you need to install a GeoTrust EV root certificate on the client to ensure that your customers can access your web services through the client.

Constraints

Your customers access your web services through clients such as Java.

Download Links

Currently, only the following types of root certificates can be downloaded.

- **DigiCert-DV-TLS-CA-G1**
- **DigiCert-EV-root**
- **DigiCert-OV-DV-root**

- GeoTrust-CN-RSA-CA-G1
- GeoTrust-EV-CN-RSA-G1
- GlobalSign-R3-root

4.1.3 Installing an SSL Certificate on a Tomcat Server

This section describes how to install an SSL certificate on a Linux Tomcat 7 server. The installation process is similar for other Tomcat servers. When the certificate is installed, it secures communication between your server and the client through SSL.

NOTE

The installation procedure in this topic is for your reference only as the commands executed and configuration file modified during the installation may vary depending on OS types and server configurations.

Prerequisites

- The certificate has been issued and the certificate status is **Issued**.
- You have downloaded the SSL certificate. For details, see **Downloading a Certificate**.
- You have installed the OpenSSL tool.

  Download the latest OpenSSL installation package from **https://www.openssl.org/source/**. The OpenSSL must be 1.0.1g or later.
- You have installed Keytool.

  Keytool is typically included in the Java Development Kit (JDK) tool package.

Constraints

- Before installing the certificate, enable port 443 on the server where the SSL certificate is installed and add port 443 to the security group. Otherwise, HTTPS cannot be enabled after the installation.
- If a domain name maps to multiple servers, deploy the certificate on each server.
- 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.

Procedure

The installation process is as follows (for Tomcat 7 servers):

Step 1: Obtaining Files → **Step 2: Creating a Directory** → **Step 3: Modifying Configuration Files** → **Step 4: Restarting the Tomcat** → **Verifying the Result**

Step 1: Obtaining Files

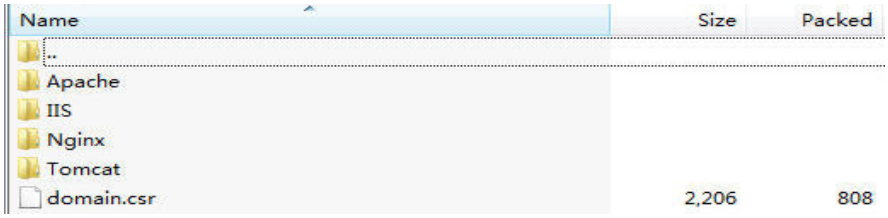
Before installing a certificate, obtain the certificate file and password file. Perform the following operations based on the value selected for **CSR** when applying for a certificate:

- 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**.

Detailed operations are as follows:

- **System generated CSR**
  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 4-3** shows an example.

     Figure 4-3 Decompressing an SSL certificate package on a local computer

  b. Obtain ***Certificate ID_Domain name bound to the certificate*_server.jks** and ***Certificate ID_Domain name bound to the certificate*_keystorePass.txt** from ***Certificate ID_Domain name bound to the certificate*_Tomcat**.
- **Upload a CSR**
  a. 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.
  b. Use OpenSSL to convert the PEM certificate into a PFX certificate and obtain the **server.pfx** file.
     i. Save the PEM certificate and the private key **server.key** generated during CSR generation to the **bin** directory in the OpenSSL installation directory.
     ii. In the **bin** directory of the OpenSSL installation directory, run the following command to convert the PEM certificate into a PFX certificate and press **Enter**:
     openssl pkcs12 -export -out server.pfx -inkey server.key -in *Certificate ID_Domain name bound to the certificate*_**server.pem**
     The command output is as follows:
     ```
     Enter Export Password:
     ```
     iii. Enter the password of the PFX certificate and press **Enter**.
     The password is user-defined. Set it as required.
     The command output is as follows:
     ```
     Verifying - Enter Export Password:
     ```


NOTE

Record the password of the PFX certificate. The password of the JKS certificate must be the same as that of the PFX certificate. Otherwise, the Tomcat service may fail to start.

To improve password security, set the password based on the following rules:

- Consists of 8 to 32 characters.
- Must contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters ~`!@#$%^&*()_+|{}:''<>?-=\[];',./

iv. Re-enter the password of the PFX certificate and press **Enter**.

If no error information is displayed, the **server.pfx** file has been generated in the OpenSSL installation directory.

c. Use Keytool to convert the PFX certificate into a JKS certificate and obtain the **server.jks** file.

i. Copy the **server.pfx** file generated in **b** to the **%JAVA_HOME%/jdk/bin** directory.

ii. In the **%JAVA_HOME%/jdk/bin** directory, run the following command and press **Enter**:

keytool -importkeystore -srckeystore server.pfx -destkeystore server.jks -srcstoretype PKCS12 -deststoretype JKS

The following message is displayed.

```
Enter the destination keystore password:
```

iii. Enter the password of the JKS certificate and press **Enter**.

NOTICE

Set the password of the JKS certificate to the same as that of the PFX certificate. Otherwise, Tomcat may fail to start.

The command output is as follows:

```
Re-enter the new password:
```

iv. Re-enter the password of the JKS certificate and press **Enter**.

The command output is as follows:

```
Enter the source keystore password:
```

v. Enter the password of the PFX certificate set in **b.iii** and press **Enter**.

If information similar to the following is displayed, the conversion is successful and the **server.jks** file has been generated in the OpenSSL installation directory.

```
Entry for alias 1 imported successfully.
Import command completed: 1 entry successfully imported, 0 entries failed or canceled
```

vi. Create a **keystorePass.txt** file in the **%JAVA_HOME%/jdk/bin** directory and save the password of the JKS certificate in the file.

d. Place the converted certificate file **server.jks** and the new password file **keystorePass.txt** in the same directory.

Step 2: Creating a Directory

Create a **cert** directory in the Tomcat installation directory, and copy the **server.jks** and **keystorePass.txt** files to the **cert** directory.

Step 3: Modifying Configuration Files

NOTICE

Before modifying the configuration file, back up the configuration file. You are advised to deploy the configuration file in the test environment and then configure it on the production environment to avoid service interruptions caused by incorrect configurations.

The installation process is as follows (for Tomcat 7 servers):

1. Find the following parameters in the **server.xml** file in the Tomcat installation directory **conf**:

```
<!--
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
              maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
              clientAuth="false" sslProtocol="TLS" />
   -->
```

2. Find the preceding parameters and delete the comment characters **<!-** and **->**.
3. Add the following parameters. Change the values of the parameters according to **Table 4-2**.

```
keystoreFile="cert/server.jks"
keystorePass="Certificate key"
```

The complete example configuration is as follows. Modify other parameters based on your needs.

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol"
              maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
     keystoreFile="cert/server.jks"
   keystorePass="Certificate key"
     clientAuth="false" sslProtocol="TLS" />
```

NOTICE

Do not directly copy all configuration. Only parameters **keystoreFile** and **keystorePass** need to be added. Set other parameters based on site requirements.

Table 4-2 Parameter description (1)

Parameter	Description
port	Port number to be used on the server. You are advised to set the value to **443**.
protocol	HTTP protocol. Retain the default value.

Parameter	Description
keystoreFile	Path for storing the **server.jks** file. The value can be an absolute path or a relative path. Example: **cert/server.jks**
keystorePass	Password of **server.jks**. Set this parameter to the password provided in the **keystorePass.txt** file. **NOTICE** If the password contains **&**, replace it with **&** to avoid configuration failure. An example command is provided as follows: If the password is **keystorePass="lx6&APWgcHf72DMu"**, change it to **keystorePass="lx6&APWgcHf72DMu"**.
clientAuth	Whether to require all customers to show the security certificate and authenticate their identity. Retain the default value.

4. Find the following parameters in the **server.xml** file in the Tomcat installation directory **conf**:

```
<Host name="localhost"  appBase="webapps"
    unpackWARs="true" autoDeploy="true">
```

5. Change the value of **Host name** to the domain name bound to the certificate.

   The complete configuration is as follows (**www.domain.com** is used as an example):

```
<Host name="www.domain.com"  appBase="webapps"
    unpackWARs="true" autoDeploy="true">
```

6. Save the configuration file.

Step 4: Restarting the Tomcat

Run the **./shutdown.sh** command in the **bin** directory of Tomcat to stop the Tomcat service.

After 10 seconds, run the **./startup.sh** command to start the Tomcat service. If the process is automatically started by the daemon process, you do not need to manually start the process.

Verifying the Result

After the deployment succeeds, in the address bar of the browser, enter **https://** *Domain name* and press **Enter**.

If a security padlock is displayed in the address bar of the browser, the certificate has been installed successfully.

- If the website still returns the warning tip, fix it by referring to **Why Does the Browser Still Consider the Website Insecure While the Website Has an SSL Certificate Deployed?**
- If the website cannot be accessed using the domain name, see **Why Is My Website Inaccessible by Domain Name After an SSL Certificate Is Installed?**

4.1.4 Installing an SSL Certificate on an Nginx Server

This section describes how to install an SSL certificate on an Nginx 1.7.8 server running CentOS 7. The installation process is similar for other Nginx servers. When the certificate is installed, it secures communication between your server and the client through SSL.

NOTE

The installation procedure in this topic is for your reference only as the commands executed and configuration file modified during the installation may vary depending on OS types and server configurations.

Prerequisites

- The certificate is in the **Issued** status.
- You have downloaded the SSL certificate. For details, see **Downloading a Certificate**.

Constraints

- Before installing the certificate, enable port 443 on the server where the SSL certificate is installed and add port 443 to the security group. Otherwise, HTTPS cannot be enabled after the installation.
- If a domain name maps to multiple servers, deploy the certificate on each server.
- 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.

Procedure

The installation process is as follows (for Nginx 1.7.8 servers running CentOS 7):

Step 1: Obtaining Files → **Step 2: Creating a Directory** → **Step 3: Uploading the Certificate File** → **Step 4: Modifying Configuration Files** → **Step 5: Verifying the Configuration** → **Step 6: Restarting Nginx** → **Step 7: Verifying the Result**

Step 1: Obtaining Files

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**.

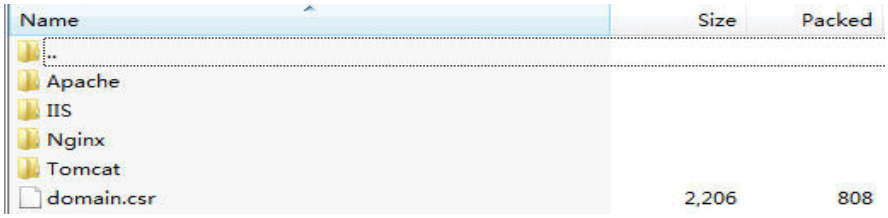
Detailed operations are as follows:

- **System generated CSR**

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, as shown in **Figure 4-4**.

Figure 4-4 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-----**.

- **Upload a CSR**

a. 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.

b. Change the suffix of ***Certificate ID_Domain name bound to the certificate*_server.pem** to **crt**, that is, **server.crt**.

c. Place **server.crt** and the **server.key** private key generated during CSR generation in the same folder.

Step 2: Creating a Directory

Create the **cert** directory in the Nginx installation directory **conf** for storing certificate files.

1. Run the following command to go to the directory **conf** in the Nginx installation directory:

   The default Nginx configuration file directory **/usr/local/nginx/conf** is used as an example. Replace it with the actual directory.

   cd /usr/local/nginx/conf

2. Run the following command to create a **cert** directory.

mkdir cert

Step 3: Uploading the Certificate File

Upload the local **server.key** and **server.crt** certificate files obtained in step 1 to the certificate directory (**cert** directory created in step 2) on the Nginx server.

NOTE

If you use an ECS, see **Uploading a File to the ECS** to learn how to upload files. You can also use the local file upload function provided by a remote login tool (such as PuTTY or Xshell) to upload files.

Step 4: Modifying Configuration Files

NOTICE

Before modifying the configuration file, back up the configuration file. You are advised to deploy the configuration file in the test environment and then configure it on the production environment to avoid service interruptions caused by incorrect configurations.

Configure the **nginx.conf** file in the **conf** directory of Nginx.

1. Find the following configuration:

```
#server {
#    listen       443 ssl;
#    server_name  localhost;
#    ssl_certificate      cert.pem;
#    ssl_certificate_key  cert.key;
#    ssl_session_cache    shared:SSL:1m;
#    ssl_session_timeout  5m;
#    ssl_ciphers  HIGH:!aNULL:!MD5;
#    ssl_prefer_server_ciphers  on;
#    location / {
#        root   html;
#        index  index.html index.htm;
#    }
#}
```

2. Delete comment tags (#) at the beginning of the lines.

```
server {
            listen              443 ssl;
            server_name         localhost;
            ssl_certificate     cert.pem;
            ssl_certificate_key cert.key;
            ssl_session_cache   shared:SSL:1m;
            ssl_session_timeout 5m;
            ssl_ciphers         HIGH:!aNULL:!MD5;
            ssl_prefer_server_ciphers  on;
            location / {
                    root     html;
                    index    index.html index.htm;
                     }
}
```

3. Modify the following parameters according to **Table 4-3**.

```
ssl_certificate         cert/server.crt;
ssl_certificate_key     cert/server.key;
```

The complete configuration is as follows. Modify other parameters based on your needs.


```
server {
    listen       443 ssl; # Set the default HTTPS port to 443. If the default HTTPS port is not configured, Nginx may fail to start.
    server_name  www.domain.com; #Replace www.domain.com with the domain name associated with your certificate.
    ssl_certificate      cert/server.crt; #Replace cert/server.crt with the path of the certificate file.
    ssl_certificate_key  cert/server.key; #Replace cert/server.key with the path of the private key.
    ssl_session_cache    shared:SSL:1m;
    ssl_session_timeout  5m;
    ssl_ciphers  HIGH:!aNULL:!MD5; #Encryption suite
    ssl_prefer_server_ciphers  on;
    location / {
        root   html; #Site directory
        index  index.html index.htm; #Add attributes.
            }
}
```

NOTICE

Do not directly copy all configuration. Only attributes starting with **ssl** are directly related to the certificate configuration. Modify other parameters based on site requirements.

Table 4-3 Parameters

Parameter	Description
listen	SSL access port number. Set the value to **443**. Set the default HTTPS port to 443. If the default HTTPS port is not configured, Nginx may fail to start.
server_name	Domain name which the certificate is used for. Example: www.domain.com
ssl_certificate	Certificate file **server.crt** Set the value to the path of the **server.crt** file. The path cannot contain Chinese characters. An example of the path is **cert/server.crt**.
ssl_certificate_key	Private key file **server.key** Set the value to the path of the **server.key** file. The path cannot contain Chinese characters. An example of the path is **cert/server.key**.

4. Save the configuration file.

Step 5: Verifying the Configuration

Go to the execution directory of Nginx and run the following command:

sbin/nginx -t

If the following information is displayed, the configuration is correct.

```
nginx.conf syntax is ok
nginx.conf test is successful
```


Step 6: Restarting Nginx

Run the following command to restart Nginx to make the configuration take effect:

cd /usr/local/nginx/sbin

./nginx -s reload

Verifying the Result

After the deployment succeeds, in the address bar of the browser, enter **https://** *Domain name* and press **Enter**.

If a security padlock is displayed in the address bar of the browser, the certificate has been installed successfully.

- If the browser still displays a message indicating that the website is insecure, fix the issue by referring to **Why Does the Website Still Display a Message Indicating that the Website Is Insecure After an SSL Certificate Is Deployed?**
- If the website cannot be accessed using a domain name, fix the issue by referring to **Why Is My Website Inaccessible by Domain Name After an SSL Certificate Is Installed?**

4.1.5 Installing an SSL Certificate on an Apache Server

This section describes how to install an SSL certificate on an Apache 2.4.6 server running CentOS 7. The installation process is similar for other Apache servers. When the certificate is installed, it secures communication between your web server and the client through SSL.

NOTE

The installation procedure in this topic is for your reference only as the commands executed and configuration file modified during the installation may vary depending on OS types and server configurations.

Prerequisites

- The certificate is in the **Issued** status.
- You have downloaded the SSL certificate. For details, see **Downloading a Certificate**.
- You have installed the **mod_ssl.so** module (for enabling SSL) on the Apache server.

Constraints

- Before installing the certificate, enable port 443 on the server where the SSL certificate is installed and add port 443 to the security group. Otherwise, HTTPS cannot be enabled after the installation.
- If a domain name maps to multiple servers, deploy the certificate on each server.

- 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.

Procedure

The installation process is as follows (for Apache 2.4.6 servers running CentOS 7):

Step 1: Obtaining Files → **Step 2: Creating a Directory** → **Step 3: Modifying Configuration Files** → **Step 4: Restarting Apache** → **Step 5: Verifying the Result**

Step 1: Obtaining Files

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:

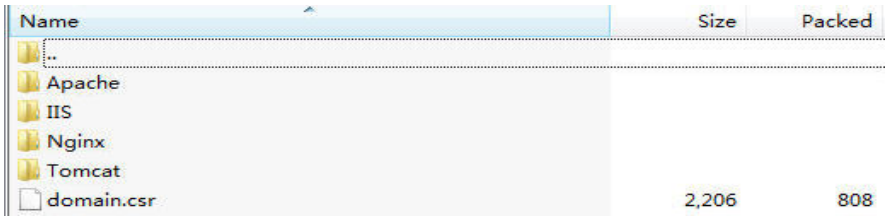
- If you select **System generated CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in **System generated CSR**.
- If you select **Upload a CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in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

Detailed operations are as follows:

- **System generated CSR**
  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, as shown in **Figure 4-5**.

     Figure 4-5 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-----**.

- **Upload a CSR**

  a. 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.

  b. Copy the first segment of certificate code (server certificate) in the ***Certificate ID_Domain name bound to the certificate*_server.pem** file and save it as the **server.crt** file.

  c. Copy the second segment of certificate code (intermediate CA certificate) in the ***Certificate ID_Domain name bound to the certificate*_server.pem** file and save it as the **ca.crt** file.

  d. Place **ca.crt**, **server.crt**, and the **server.key** private key generated during CSR generation in any folder.

Step 2: Creating a Directory

Create a **cert** directory in the Apache installation directory, and copy the **server.key**, **server.crt**, and **ca.crt** files to the **cert** directory.

Step 3: Modifying Configuration Files

NOTICE

Before modifying the configuration file, back up the configuration file. You are advised to deploy the configuration file in the test environment and then configure it on the production environment to avoid service interruptions caused by incorrect configurations.

1. Open the **conf.d/ssl.conf** file in the Apache root directory.
2. Configure the domain name associated with the certificate.

   Find and modify the following parameter:

   ```
   ServerName www.example.com:443
   ```

   The complete configuration is as follows (**www.domain.com** is used as an example):

   ```
   ServerName www.domain.com:443 #Replace www.domain.com with the domain name of your server.
   ```

3. Configure the public key for the certificate.

   Find and modify the following parameter:

   ```
   SSLCertificateFile "${SRVROOT}/conf/server.crt"
   ```

   Set the value to the path of the **server.crt** file. The path cannot contain Chinese characters. An example of the path is **cert/server.crt**.

   The complete configuration is as follows:


```
SSLCertificateFile "cert/server.crt"
```

4. Configure the private key for the certificate.

   Find and modify the following parameter:

   ```
   SSLCertificateKeyFile "${SRVROOT}/conf/server.key"
   ```

   Set the value to the path of the **server.key** file. The path cannot contain Chinese characters. An example of the path is **cert/server.key**.

   The complete configuration is as follows:

   ```
   SSLCertificateKeyFile "cert/server.key"
   ```

5. Configure the certificate chain.

   Find and modify the following parameter:

   ```
   #SSLCertificateChainFile "${SRVROOT}/conf/server-ca.crt"
   ```

   Delete the comment tag **#** at the beginning of the line. Set this parameter to the path of the **ca.crt** file. The path cannot contain Chinese characters. An example of the path is **cert/ca.crt**.

   The complete configuration is as follows:

   ```
   SSLCertificateChainFile "cert/ca.crt"
   ```

6. Save the **ssl.conf** file and exit.

Step 4: Restarting Apache

Restart the Apache service for the configuration to take effect:

1. Run the **service named stop** command to stop the Apache server.
2. Run the **service httpd start** command to start the Apache server.

Step 5: Verifying the Result

After the deployment succeeds, in the address bar of the browser, enter **https://** *Domain name* and press **Enter**.

If a security padlock is displayed in the address bar of the browser, the certificate has been installed successfully.

- If the browser still displays a message indicating that the website is insecure, fix the issue by referring to **Why Does the Website Still Display a Message Indicating that the Website Is Insecure After an SSL Certificate Is Deployed?**
- If the website cannot be accessed using a domain name, fix the issue by referring to **Why Is My Website Inaccessible by Domain Name After an SSL Certificate Is Installed?**

4.1.6 Installing an SSL Certificate on an IIS Server

This topic describes how to install an SSL certificate on an IIS server. When the certificate is installed, it secures communication between your server and the client through SSL.

NOTE

The installation procedure in this topic is for your reference only as the commands executed and configuration file modified during the installation may vary depending on OS types and server configurations.

Prerequisites

- The certificate is in the **Issued** status.
- You have downloaded the SSL certificate. For details, see **Downloading a Certificate**.

Constraints

- Before installing the certificate, enable port 443 on the server where the SSL certificate is installed and add port 443 to the security group. Otherwise, HTTPS cannot be enabled after the installation.
- If a domain name maps to multiple servers, deploy the certificate on each server.
- 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.

Procedure

To install an SSL certificate on an IIS server, perform the following steps:

Step 1: Obtaining Files → **Step 2: Configuring IIS** → **Verifying the Result**

Step 1: Obtaining Files

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:

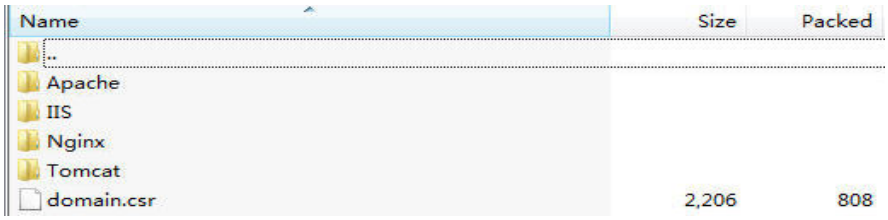
- If you select **System generated CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in **System generated CSR**.
- If you select **Upload a CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in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

Detailed operations are as follows:

- **System generated CSR**
  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 4-6** shows an example.

     Figure 4-6 Decompressing an SSL certificate package on a local computer

  b. Obtain the SSL certificate file ***Certificate ID_Domain name bound to the certificate*_server.pfx** and password file ***Certificate ID_Domain***

***name bound to the certificate*_keystorePass.txt** from ***Certificate ID_Domain name bound to the certificate*_IIS**.

- **Upload a CSR**

  a. 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.

  b. Use OpenSSL to convert the PEM certificate into a PFX certificate and obtain the **server.pfx** file.

  i. Save the PEM certificate and the private key **server.key** generated during CSR generation to the **bin** directory in the OpenSSL installation directory.

  ii. In the **bin** directory of the OpenSSL installation directory, run the following command to convert the PEM certificate into a PFX certificate and press **Enter**:

  openssl pkcs12 -export -out server.pfx -inkey server.key -in *Certificate ID_Domain name bound to the certificate*_**server.pem**

  Information similar to the following is displayed.

  ```
  Enter Export Password:
  ```

  iii. Enter the password of the PFX certificate and press **Enter**.

  The password is user-defined. Set it as required.

  Information similar to the following is displayed.

  ```
  Verifying - Enter Export Password:
  ```

  NOTE

  Record the password of the PFX certificate. The password of the JKS certificate must be the same as that of the PFX certificate. Otherwise, the IIS service may fail to start.

  To improve password security, a password must:

  - Consist of 8 to 32 characters.
  - Contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters ~`!@#$%^&*()_+|{}:"<>?-=\[];',./

  iv. Re-enter the password of the PFX certificate and press **Enter**.

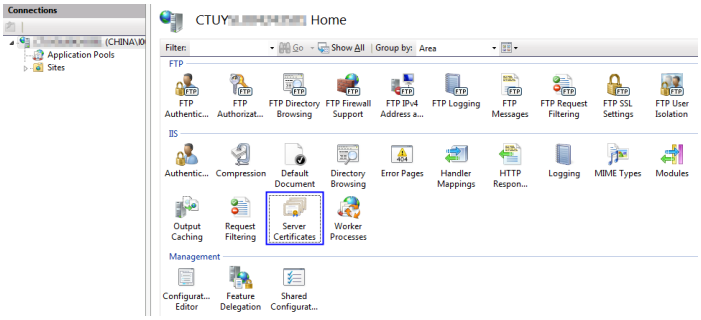
  If no error information is displayed, the **server.pfx** file has been generated in the OpenSSL installation directory.

  v. Create a **keystorePass.txt** file in the OpenSSL installation directory and save the password of the PFX certificate in the file.

Step 2: Configuring IIS

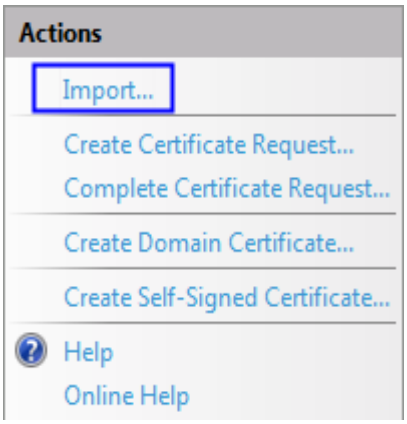
1. Install IIS as instructed by IIS guides.
2. Open the IIS management console, double-click **Server Certificates**.

Figure 4-7 Double-clicking Server Certificates



3. In the displayed dialog box, click **Import**.

Figure 4-8 Import

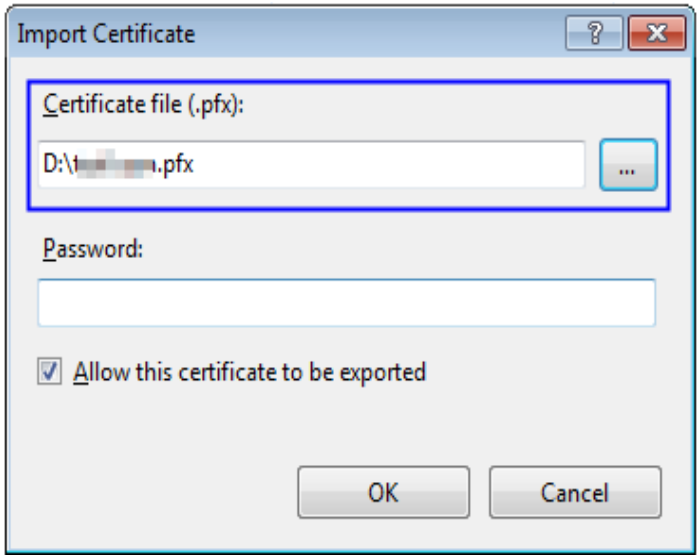


4. Import the **server.pfx** certificate file. Then click **OK**.

   NOTE

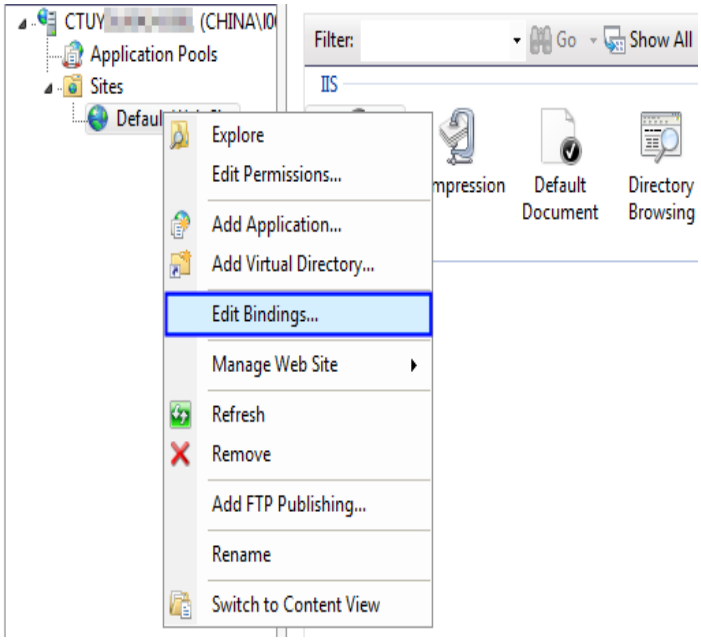
   In the **Password** box, enter the password provided in the **keystorePass.txt** file.

Figure 4-9 Importing a PFX certificate file



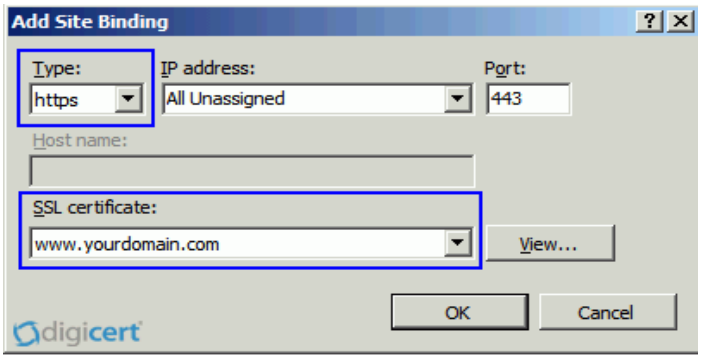
5. Right-click the target site (the default site is used as an example). Choose **Edit Bindings** from the shortcut menu.

Figure 4-10 Choosing Edit Bindings



6. In the dialog box that is displayed, click **Add**. Then enter the following information.

Figure 4-11 Binding a website



   - **Type**: Select **https**.
   - **Port**: Retain the default port **443**.
   - **SSL certificate**: Select the certificate imported in **4**.
7. Click **OK**.

Verifying the Result

After the deployment succeeds, in the address bar of the browser, enter **https://***Domain name* and press **Enter**.

If a security padlock is displayed in the address bar of the browser, the certificate has been installed successfully.

- If the website still returns the warning tip, fix it by referring to **Why Does the Browser Still Consider the Website Insecure While the Website Has an SSL Certificate Deployed?**

- If the website cannot be accessed using the domain name, see **Why Is My Website Inaccessible by Domain Name After an SSL Certificate Is Installed?**

4.1.7 Installing an SSL Certificate on a WebLogic Server

WebLogic is a Java EE application server, used to develop, integrate, deploy, and manage large-scale distributed Web apps, network apps, and database apps. It applies dynamic functions of Java and security of the Java Enterprise standard to the development, integration, deployment, and management of large-scale network applications.

Currently, WebLogic 10.3.1 and later versions support SSL certificates of all mainstream brands. Versions earlier than WebLogic 10.3.1 do not support SSL certificates of brands.

This topic describes how to install an SSL certificate on a WebLogic server. When the certificate is installed, it secures communication between your server and the client through SSL.

NOTE

The installation procedure in this topic is for your reference only as the commands executed and configuration file modified during the installation may vary depending on OS types and server configurations.

Prerequisites

- The certificate is in the **Issued** status.
- You have downloaded the SSL certificate. For details, see **Downloading a Certificate**.
- The JDK has been installed.

  The JDK has been installed after WebLogic installation is complete. If the JDK has not been installed, install the **Java SE Development Kit (JDK)**.

Constraints

- Before installing the certificate, enable port 443 on the server where the SSL certificate is installed and add port 443 to the security group. Otherwise, HTTPS cannot be enabled after the installation.
- If a domain name maps to multiple servers, deploy the certificate on each server.
- 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.

Procedure

To install an SSL certificate on a WebLogic server, perform the following steps:

Step 1: Obtaining Files → **Step 2: Configuring WebLogic** → **Verifying the Result**

Step 1: Obtaining Files

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:

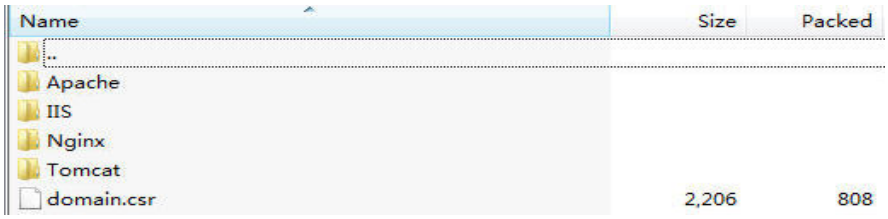
- If you select **System generated CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in **System generated CSR**.
- If you select **Upload a CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in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

Detailed operations are as follows:

- **System generated CSR**
  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 4-12** shows an example.

     Figure 4-12 Decompressing an SSL certificate package on a local computer

  b. Obtain ***Certificate ID_Domain name bound to the certificate*_server.jks** and ***Certificate ID_Domain name bound to the certificate*_keystorePass.txt** from ***Certificate ID_Domain name bound to the certificate*_Tomcat**.
- **Upload a CSR**
  a. 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.

  b. Use OpenSSL to convert the PEM certificate into a PFX certificate and obtain the **server.pfx** file.

     i. Save the PEM certificate and the private key **server.key** generated during CSR generation to the **bin** directory in the OpenSSL installation directory.

     ii. In the **bin** directory of the OpenSSL installation directory, run the following command to convert the PEM certificate into a PFX certificate and press **Enter**:

     openssl pkcs12 -export -out server.pfx -inkey server.key -in *Certificate ID_Domain name bound to the certificate*_**server.pem**

     Information similar to the following is displayed.

```
Enter Export Password:
```

iii. Enter the password of the PFX certificate and press **Enter**.

The password is user-defined. Set it as required.

The following message is displayed.

```
Verifying - Enter Export Password:
```

NOTE

Record the password of the PFX certificate. The password of the JKS certificate must be the same as that of the PFX certificate. Otherwise, the WebLogic service may fail to start.

To improve password security, a password must:

- Consist of 8 to 32 characters.
- Contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters ~`!@#$%^&*()_+|{}:"<>?-=\[];',./

iv. Re-enter the password of the PFX certificate and press **Enter**.

If no error information is displayed, the **server.pfx** file has been generated in the OpenSSL installation directory.

c. Use Keytool to convert the PFX certificate into a JKS certificate and obtain the **server.jks** file.

i. Copy the **server.pfx** file generated in **b** to the **%JAVA_HOME%/jdk/bin** directory.

ii. In the **%JAVA_HOME%/jdk/bin** directory, run the following command and press **Enter**:

keytool -importkeystore -srckeystore server.pfx -destkeystore server.jks -srcstoretype PKCS12 -deststoretype JKS

Information similar to the following is displayed.

```
Enter the destination keystore password:
```

iii. Enter the password of the JKS certificate and press **Enter**.

NOTICE

Set the password of the JKS certificate to the same as that of the PFX certificate. Otherwise, the WebLogic service may fail to start.

Information similar to the following is displayed.

```
Re-enter the new password:
```

iv. Re-enter the password of the JKS certificate and press **Enter**.

Information similar to the following is displayed.

```
Enter the source keystore password:
```

v. Enter the password of the PFX certificate set in **2.c** and press **Enter**.

If information similar to the following is displayed, the conversion is successful and the **server.jks** file has been generated in the OpenSSL installation directory.

```
Entry for alias 1 imported successfully.
Import command completed: 1 entry successfully imported, 0 entries failed or canceled
```

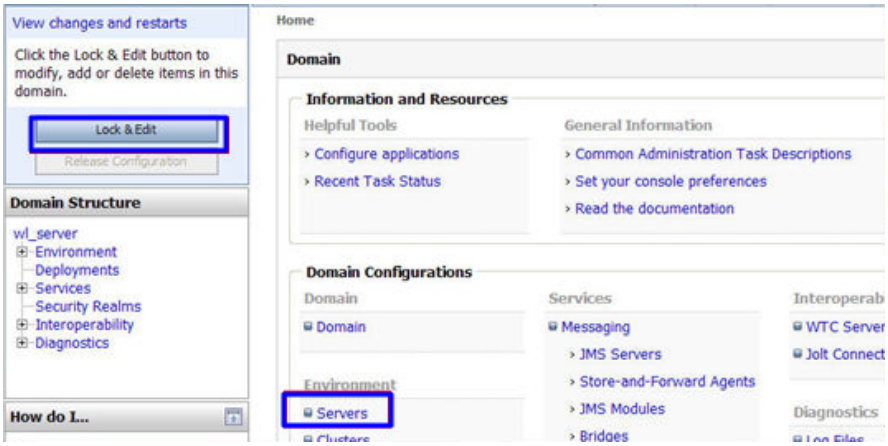

vi. Create a **keystorePass.txt** file in the **%JAVA_HOME%/jdk/bin** directory and save the password of the JKS certificate in the file.

d. Place the converted certificate file **server.jks** and the new password file **keystorePass.txt** in the same directory.

Step 2: Configuring WebLogic

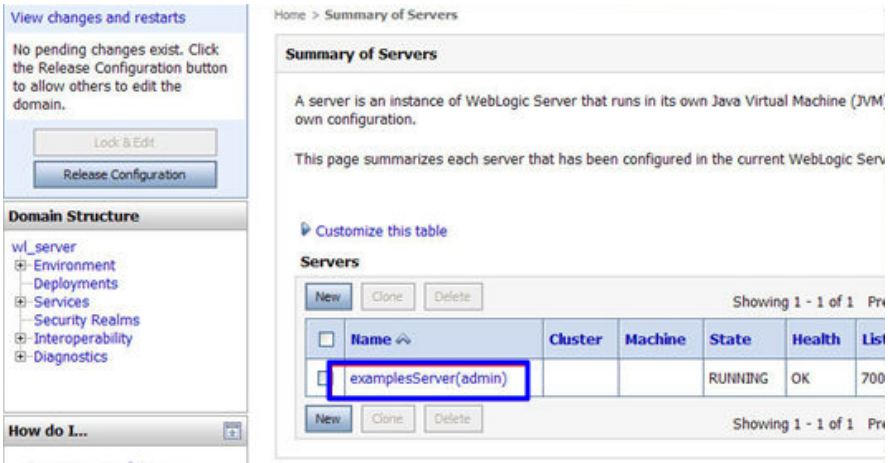
1. Log in to the management console of the WebLogic server.
2. Click **Lock & Edit** in the upper left corner of the page to unlock the configuration.
3. Click **Servers** in **Domain Configurations**.

Figure 4-13 Server



4. In the server list, select the server for which you want to configure the server certificate. The server configuration page is displayed.

Figure 4-14 Target server

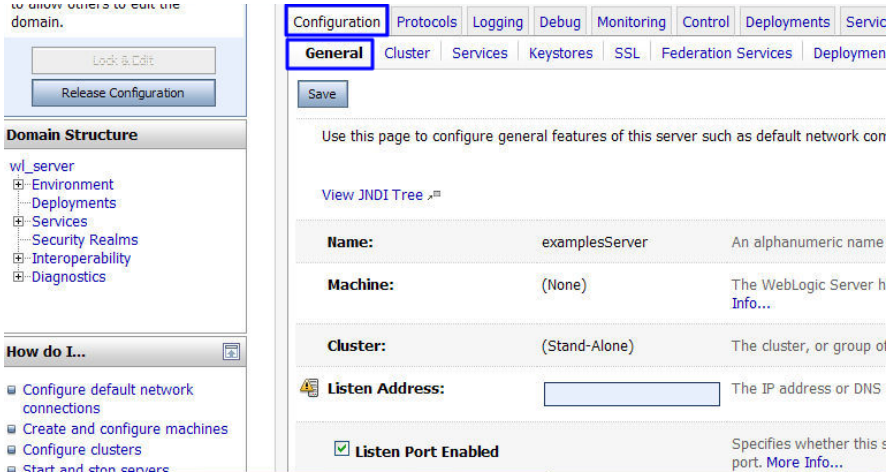


5. Modify the HTTPS port.

   On the server configuration page, click the **General** tab and configure whether to enable HTTP and HTTPS and the access port number.

   Select **Listen SSL Port Enabled** and change the port number to **443**.

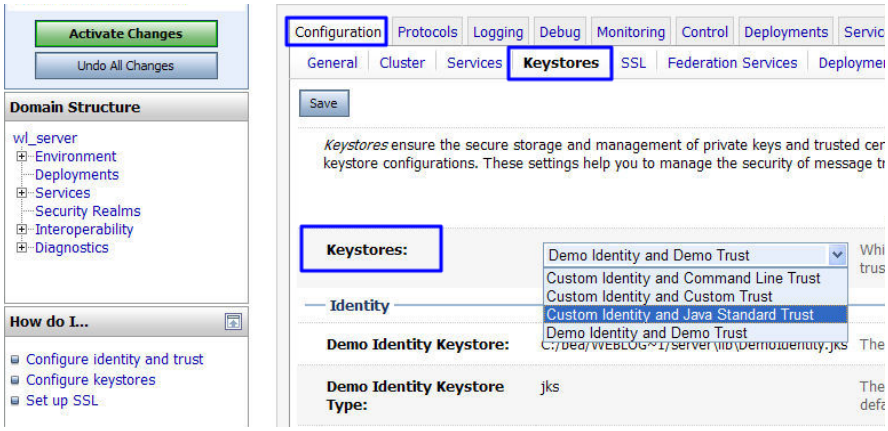
Figure 4-15 port



6. Configure an authentication mode and a key.

   a. On the server configuration page, click the **Keystores** tab and configure an authentication mode.

      Figure 4-16 Authentication mode

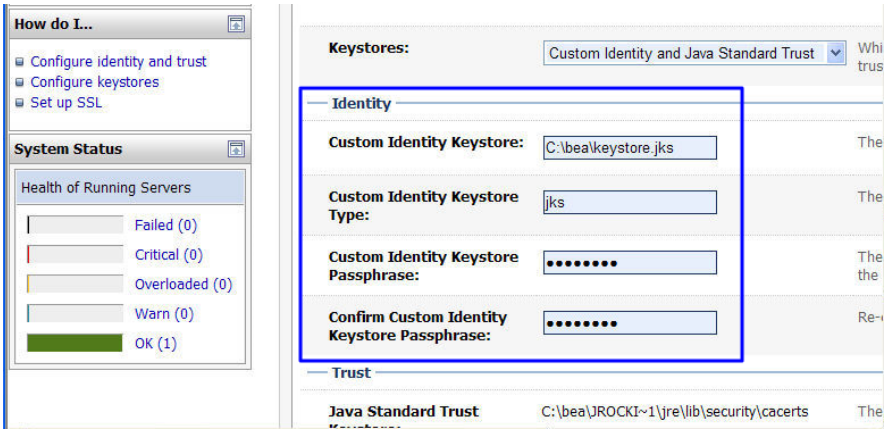


      - Select **Custom Identity and Java Standard Trust** for server authentication.
      - Select **Custom Identity and Custom Trust** for bidirectional authentication.

   b. Configure a key in the **Identity** area.

      Configure the path for storing the keystore file **server.jks** on the server and enter the password of the keystore file.

Figure 4-17 Key

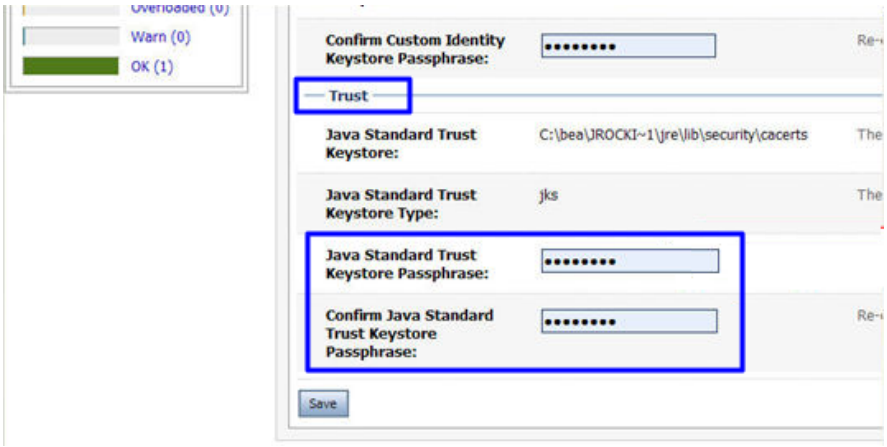


- **Custom Identity Keystore**: Enter the path for storing the .jks file. Example: C:\bea\server.jks
- **Custom Identity Keystore Type**: Set the file format to **jks**.
- **Custom Identity Keystore Passphrase**: Enter the certificate password, that is, the password in **keystorePass.txt**.
- **Confirm Custom Identity Keystore Passphrase**: Re-enter the certificate password.

c. In unidirectional authentication, configure the default trust store file **cacerts** of the JRE.

The default password of **cacerts** is **changeit**.

Figure 4-18 Trust store file

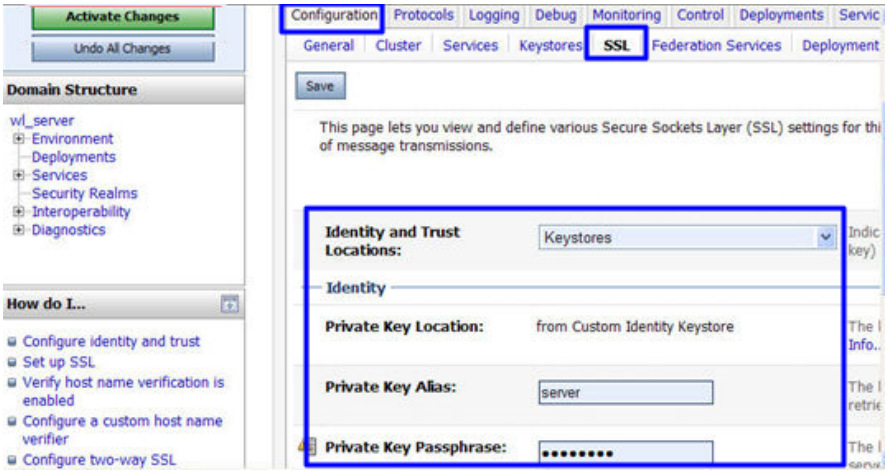


- **Java Standard Trust Keystore Passphrase**: Enter the default password **changeit**.
- **Confirm Java Standard Trust Keystore Passphrase**: Re-enter the default password.

7. Configure the private key alias of the server certificate.

On the server configuration page, click the **SSL** tab and set the following parameters:

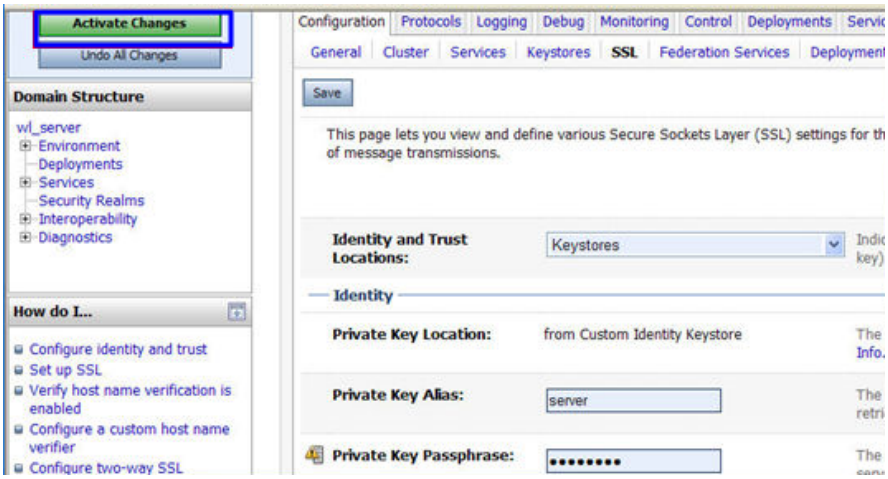
Figure 4-19 Private key



- **Identity and Trust Locations**: Select **Keystores**.
- **Private Key Alias**: Configure a private key alias in the private key library. You can run the **keystool -list** command to view the private key alias.
- **Private Key Passphrase**: Enter the private key protection password. Generally, the private key protection password is the same as the keystore file protection password.
- **Confirm Private Key Passphrase**: Enter the private key protection password again.

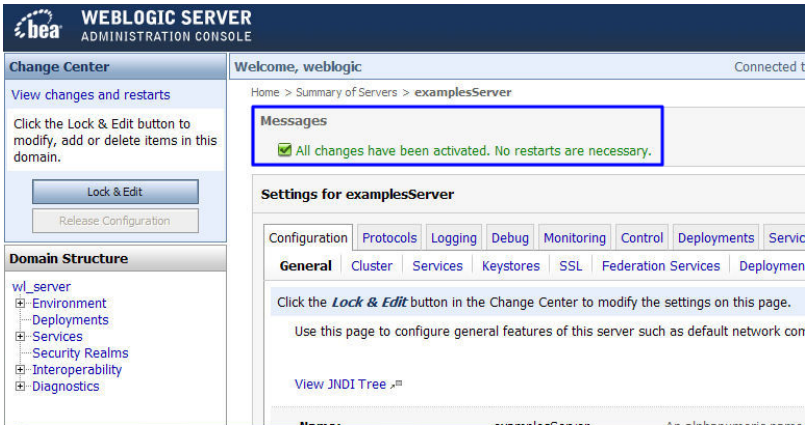
8. Click **Active Changes** to save the settings.

Figure 4-20 Saving the settings



9. (Optional) If the system prompts you to restart the WebLogic server, restart the WebLogic server for the settings to take effect. As shown in **Figure 4-21**, you do not need to restart the WebLogic server.

Figure 4-21 Message displayed



Verifying the Result

After the deployment succeeds, in the address bar of the browser, enter **https://***Domain name* and press **Enter**.

If a security padlock is displayed in the address bar of the browser, the certificate has been installed successfully.

- If the website still returns the warning tip, fix it by referring to **Why Does the Browser Still Consider the Website Insecure While the Website Has an SSL Certificate Deployed?**
- If the website cannot be accessed using the domain name, see **Why Is My Website Inaccessible by Domain Name After an SSL Certificate Is Installed?**

4.1.8 Installing an SSL Certificate on a Resin Server

This topic describes how to install an SSL certificate on a Resin server. When the certificate is installed, it secures communication between your server and the client through SSL.

NOTE

The installation procedure in this topic is for your reference only as the commands executed and configuration file modified during the installation may vary depending on OS types and server configurations.

Prerequisites

- The certificate is in the **Issued** status.
- You have downloaded the SSL certificate. For details, see **Downloading a Certificate**.

Constraints

- Before installing the certificate, enable port 443 on the server where the SSL certificate is installed and add port 443 to the security group. Otherwise, HTTPS cannot be enabled after the installation.
- If a domain name maps to multiple servers, deploy the certificate on each server.

- 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.

Procedure

To install an SSL certificate on a Resin server, perform the following steps:

Step 1: Obtaining Files → **Step 2: Configuring Resin** → **Verifying the Result**

Step 1: Obtaining Files

Before installing a certificate, obtain the certificate file and key file. Perform the following operations based on the method you select for **CSR**:

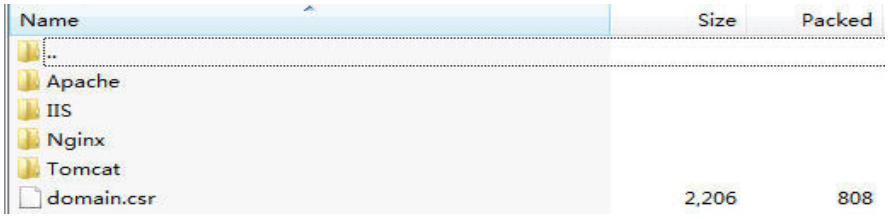
- If you select **System generated CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in **System generated CSR**.
- If you select **Upload a CSR** for **CSR** when applying for a certificate, perform the operations according to the instructions in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

Detailed operations are as follows:

- **System generated CSR**
  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 4-22** shows an example.

     Figure 4-22 Decompressing an SSL certificate package on a local computer

  b. Obtain ***Certificate ID_Domain name bound to the certificate*_server.jks** and ***Certificate ID_Domain name bound to the certificate*_keystorePass.txt** from ***Certificate ID_Domain name bound to the certificate*_Tomcat**.
- **Upload a CSR**
  a. 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.
  b. Use OpenSSL to convert the PEM certificate into a PFX certificate and obtain the **server.pfx** file.

i. Save the PEM certificate and the private key **server.key** generated during CSR generation to the **bin** directory in the OpenSSL installation directory.

ii. In the **bin** directory of the OpenSSL installation directory, run the following command to convert the PEM certificate into a PFX certificate and press **Enter**:

openssl pkcs12 -export -out server.pfx -inkey server.key -in *Certificate ID_Domain name bound to the certificate*_**server.pem**

Information similar to the following is displayed.

```
Enter Export Password:
```

iii. Enter the password of the PFX certificate and press **Enter**.

The password is user-defined. Set it as required.

Information similar to the following is displayed.

```
Verifying - Enter Export Password:
```

NOTE

Record the password of the PFX certificate. The password of the JKS certificate must be the same as that of the PFX certificate. Otherwise, the Resin service may fail to start.

To improve password security, a password must:

- Consist of 8 to 32 characters.
- Contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters ~`!@#$%^&*()_+|{}:"<>?-=\[];',./

iv. Re-enter the password of the PFX certificate and press **Enter**.

If no error information is displayed, the **server.pfx** file has been generated in the OpenSSL installation directory.

c. Use Keytool to convert the PFX certificate into a JKS certificate and obtain the **server.jks** file.

i. Copy the **server.pfx** file generated in **b** to the **%JAVA_HOME%/jdk/bin** directory.

ii. In the **%JAVA_HOME%/jdk/bin** directory, run the following command and press **Enter**:

keytool -importkeystore -srckeystore server.pfx -destkeystore server.jks -srcstoretype PKCS12 -deststoretype JKS

Information similar to the following is displayed.

```
Enter the destination keystore password:
```

iii. Enter the password of the JKS certificate and press **Enter**.

NOTICE

Set the password of the JKS certificate to the same as that of the PFX certificate. Otherwise, the Resin service may fail to start.

Information similar to the following is displayed.

```
Re-enter the new password:
```


iv. Re-enter the password of the JKS certificate and press **Enter**.

Information similar to the following is displayed.

```
Enter the source keystore password:
```

v. Enter the password of the PFX certificate set in **2.c** and press **Enter**.

If information similar to the following is displayed, the conversion is successful and the **server.jks** file has been generated in the OpenSSL installation directory.

```
Entry for alias 1 imported successfully.
Import command completed: 1 entry successfully imported, 0 entries failed or canceled
```

vi. Create a **keystorePass.txt** file in the **%JAVA_HOME%/jdk/bin** directory and save the password of the JKS certificate in the file.

d. Place the converted certificate file **server.jks** and the new password file **keystorePass.txt** in the same directory.

Step 2: Configuring Resin

NOTICE

Before modifying the configuration file, back up the configuration file. You are advised to deploy the configuration file in the test environment and then configure it on the production environment to avoid service interruptions caused by incorrect configurations.

1. (Optional) Install Resin.

   If you have installed Resin, skip this step.

   a. Log in to the **Resin** official website and download the appropriate application packages for your operating system.

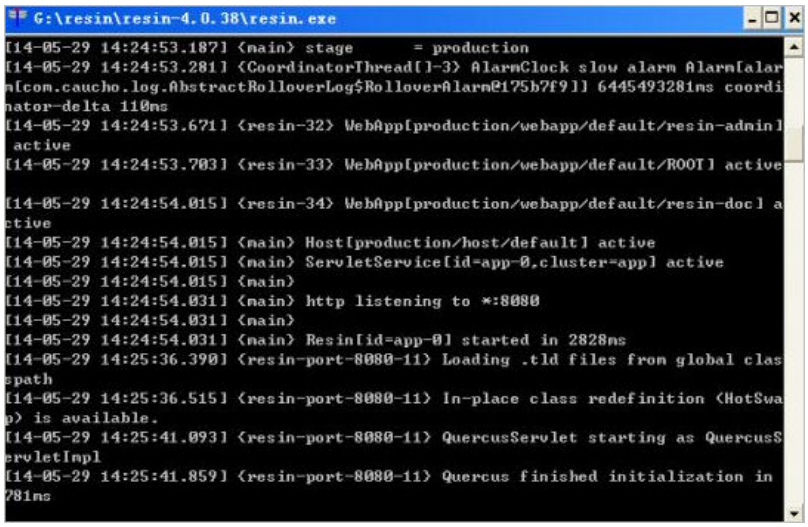
      The following uses **Resin-4.0.38** for Windows as an example.

   b. Decompress the downloaded Resin software package.

   c. Access the root directory of Resin-4.0.38 and find the **resin.exe** file.

   d. Run the **resin.exe** file. During the execution, the command prompt window **Figure 4-23** will display.

Figure 4-23 Information dialog box



e. After the resin.exe file is executed. Start the Microsoft Internet Explorer, enter the default address **http://127.0.0.1:8080** of Resin in the address bar, and then press **Enter**.

   If the information similar to **Figure 4-24** is displayed, Resin is installed successfully.

Figure 4-24 Logging In to Resin

2. Modify the configuration file.

   a. Find the following parameters in the **Resin.properties** configuration file in the Resin installation directory (the configuration file may be **resin.xml** for different Resin versions):

```
# specifies the --server in the config file
# home_server : app-0

# Set HTTP and HTTPS bind address
# http_address : *

# Set HTTP and HTTPS ports.
# Use overrides for individual server control, for example: app-0.http : 8081
app.http          : 8080
# app.https         : 8443

web.http          : 8080
# web.https         : 8443
```


b. Delete the comment symbol (#) before **app.https** and **web.https**. Then modify port **8443** to **443**. After the modification:

app.https and **web.https**: Port to be used on the server. You are advised to set the value to **443**.

```
# specifies the --server in the config file
# home_server : app-0

# Set HTTP and HTTPS bind address
# http_address : *

# Set HTTP and HTTPS ports.
# Use overrides for individual server control, for example: app-0.http : 8081
app.http          : 8080
app.https          : 443

web.http          : 8080
web.https          : 443
```

c. Find the following parameters and delete the comment symbol (#) before **jsse_keystore_type**, **jsse_keystore_file**, and **jsse_keystore_password**.

```
# JSSE certificate configuration
# Keys are typically stored in the resin configuration directory.
jsse_keystore_tye : jks
jsse_keystore_file : cert/server.jks
jsse_keystore_password: certificate password
```

d. Modify certificate-related parameters. For details, see **Table 4-4**.

```
# JSSE certificate configuration
# Keys are typically stored in the resin configuration directory.
jsse_keystore_tye : jks
jsse_keystore_file : cert/server.jks
jsse_keystore_password: certificate password
```

Table 4-4 Description

Parameter	Description
jsse_keystore_tye	Type of the Keystore file. Generally, this parameter is set to **jks**.
jsse_keystore_file	Path for storing the **server.jks** file. The value can be an absolute path or a relative path. Example: **cert/server.jks**
jsse_keystore_password	Password of **server.jks**. Set this parameter to the password provided in the **keystorePass.txt** file. **NOTICE** If the password contains **&**, replace it with **&** to avoid configuration failure. An example command is provided as follows: If the password is **keystorePass="Ix6&APWgcHf72DMu"**, change it to **keystorePass="Ix6&APWgcHf72DMu"**.

e. Save the configuration file.

3. Restart Resin.

Verifying the Result

After the deployment succeeds, in the address bar of the browser, enter **https://***Domain name* and press **Enter**.

If a security padlock is displayed in the address bar of the browser, the certificate has been installed successfully.

- If the website still returns the warning tip, fix it by referring to **Why Does the Browser Still Consider the Website Insecure While the Website Has an SSL Certificate Deployed?**
- If the website cannot be accessed using the domain name, see **Why Is My Website Inaccessible by Domain Name After an SSL Certificate Is Installed?**

4.2 Deploying an SSL Certificate to Other Huawei Cloud Products

4.2.1 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

- 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 because no private key of the certificate is available on the cloud.. To use a certificate in a cloud product, download the certificate to your local PC first. Then, upload the certificate and private key to the cloud product and complete deployment.

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.

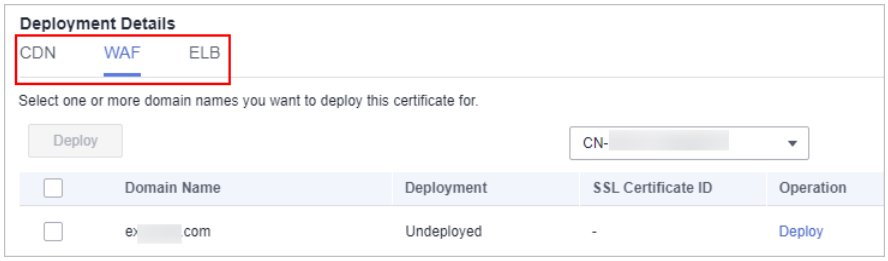
Step 3 In the navigation pane on the left, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 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 4-25 Deploy

Step 5 On the displayed page, select **WAF** in the **Deployment Details** area.

Figure 4-26 Selecting a cloud product



Step 6 Click on the right of the **Region** drop-down list and select the region where you want to deploy the certificate.

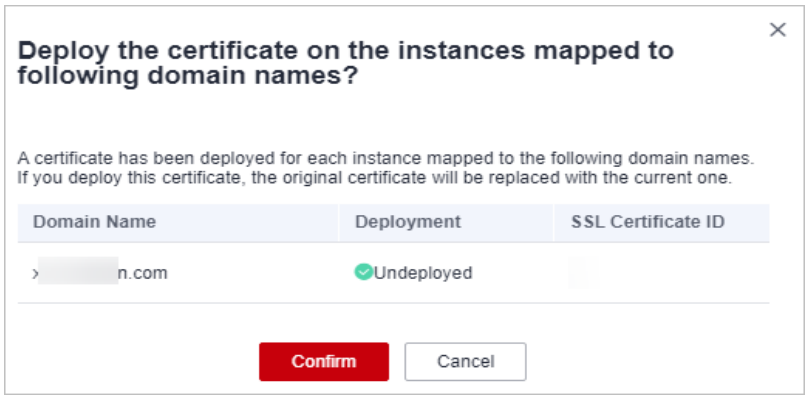
Step 7 Select the domain name you want to deploy the certificate for and click **Deploy** in the **Operation** column.

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

Figure 4-27 Deploy

Step 8 In the displayed confirmation dialog box, click **Confirm**.

Figure 4-28 Certificate deployment confirmation box



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

----End

4.2.2 Deploying an SSL Certificate to ELB

When an SSL certificate is issued, you can deploy it to Huawei Cloud 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 need to create a listener and configure **HTTPS** for the listener so that you can use CCM to deploy SSL certificates in just a few clicks.
- If an ELB certificate is used for multiple domain names, ensure that the new certificate you want to update in CCM 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.
- 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 because no private key of the certificate is available on the cloud.. To use a certificate in a cloud product, download the certificate to your local PC first. Then, upload the certificate and private key to the cloud product and complete deployment.

NOTE

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.

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.

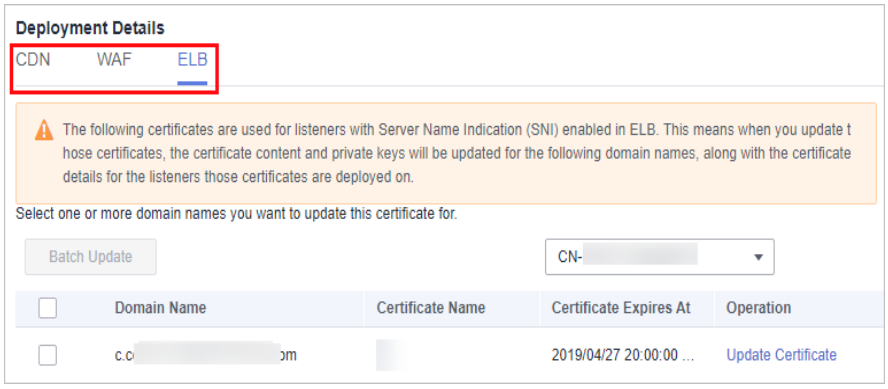
Step 3 In the navigation pane on the left, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 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 4-29 Deploying a certificate

Step 5 On the displayed page, select **ELB** in the **Deployment Details** area.

Figure 4-30 Selecting a cloud product

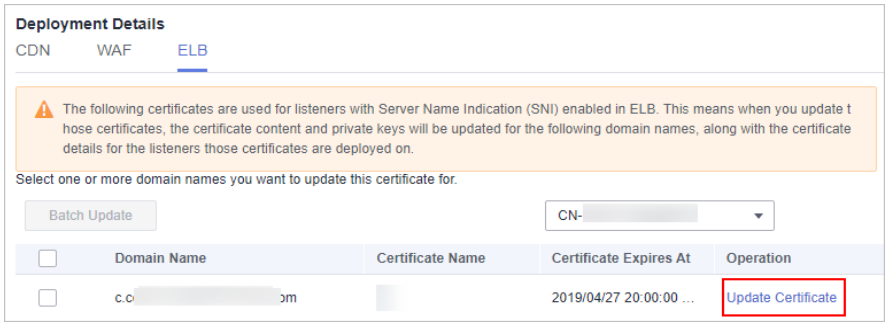


Step 6 Click ▼ on the right of the **Region** drop-down list and select the region where you want to deploy the certificate.

Step 7 Select the domain name you want to update the certificate for and click **Update Certificate** in the **Operation** column.

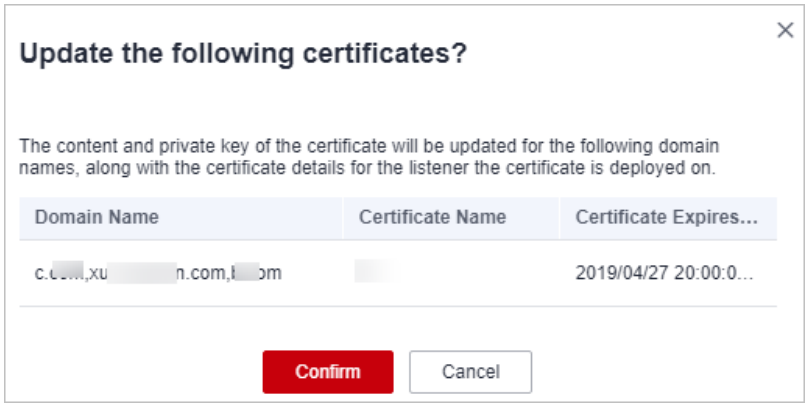
To update the certificates for multiple domain names, select all the target domain names and click **Batch Update** above the domain name list.

Figure 4-31 Updating a certificate



Step 8 In the displayed confirmation dialog box, click **Confirm**.

Figure 4-32 Certificate update confirmation box



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

----End

4.2.3 Deploying an SSL Certificate to CDN

When an SSL certificate is issued, you can deploy it to Huawei Cloud Content Delivery Network (CDN) in just a few clicks. With SSL certificates, data access to your website that uses CDN is more secure.

Prerequisites

- You have enabled CDN, added your website to CDN, and configured an SSL certificate for the website in CDN.

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

Constraints

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 because no private key of the certificate is available on the cloud.. To use a

certificate in a cloud product, download the certificate to your local PC first. Then, upload the certificate and private key to the cloud product and complete deployment.

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** > **SSL Certificates**.

Step 4 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 4-33 Deploying a certificate

Step 5 On the displayed page, select **CDN** in the **Deployment Details** area.

Figure 4-34 Selecting a cloud product

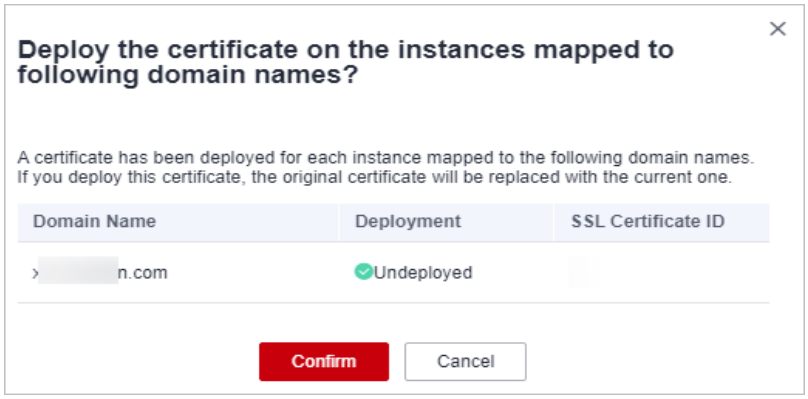
Step 6 Select the domain name you want to deploy the certificate for and click **Deploy** in the **Operation** column.

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

Figure 4-35 Deploy

Step 7 In the displayed confirmation dialog box, click **Confirm**.

Figure 4-36 Certificate deployment confirmation box



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

----End

4.2.4 Viewing Associated Cloud Resources

This topic walks you through how to view cloud services where your SSL certificates are deployed.

Prerequisites

Certificates have been deployed on Huawei Cloud services.

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.

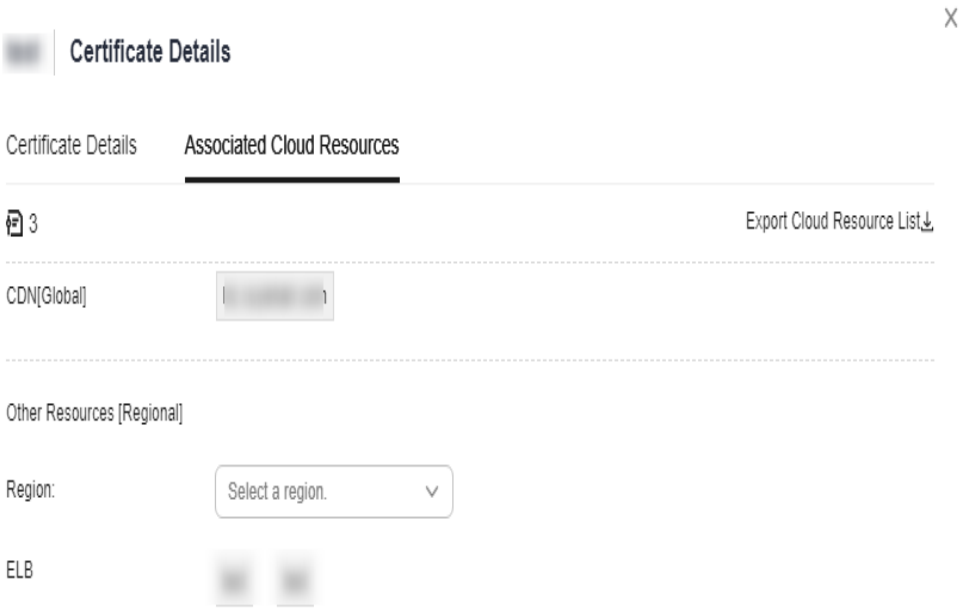
Step 3 In the navigation pane on the left, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 Select a deployed SSL certificate, hover over the **Associated Resources** column, and click **View Details**. The certificate details panel is displayed on the right.

Step 5 Click the **Associated Cloud Resources** tab to view the cloud resources that the certificate has been deployed for. For parameters, see **Table 4-5**.

To view more details, click **Export Cloud Resource List** in the upper right corner of the page.

Figure 4-37 Associated cloud resource details



NOTE

For an expired certificate, click **More** to view the deployment records of the certificate in other cloud services.

Table 4-5 Parameters for associated cloud resources

Parameter		Description
Global	CDN	Acceleration domain names the certificate is associated with in the CDN service
Regional	Region	The region where ELB or WAF associated with the certificate has been deployed.
	Load balancer certificates	Certificates that have been associated with the certificate for ELB in the selected region.

Parameter		Description
	Domain names protected by WAF	Protected domain names in the default enterprise project in WAF in the selected region. **NOTE** Only cloud resources in the default enterprise project associated with the certificates are displayed for WAF as certificates in CCM support only resources in the default enterprise project for WAF.

----End

5 Managing SSL Certificates

5.1 Reissuing an SSL Certificate

Reissuing an SSL certificate is a process in which a user needs to obtain a new certificate to replace the original certificate when the SSL certificate is still valid. Generally, you need to re-issue the SSL certificate in the following scenarios:

- Key leakage or loss: If the key of a website is disclosed or lost, you are advised to issue a new SSL certificate to ensure website security.
- Changing the domain name: If the domain name of a website is changed, the original SSL certificate is no longer applicable. You need to issue a new SSL certificate to match the new domain name.
- Incorrect certificate configuration: If the configuration information (for example, the domain name or organization information) is incorrect when you apply for an SSL certificate, you need to re-issue the SSL certificate.

Prerequisites

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

Constraints

- Free certificates, multi-domain certificates, and revoked certificates cannot be reissued.
- 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

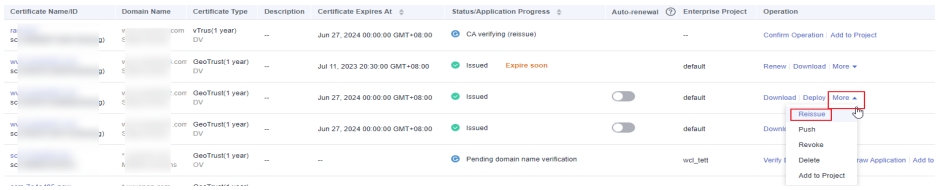
Step 1 Log in to the **management console**.

Step 2 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** > **SSL Certificates**.

Step 4 In the **Operation** column of the target domain name, choose **More** > **Reissue**.

Figure 5-1 Reissuing an SSL certificate



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 5 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.

Figure 5-2 Reissuing a certificate

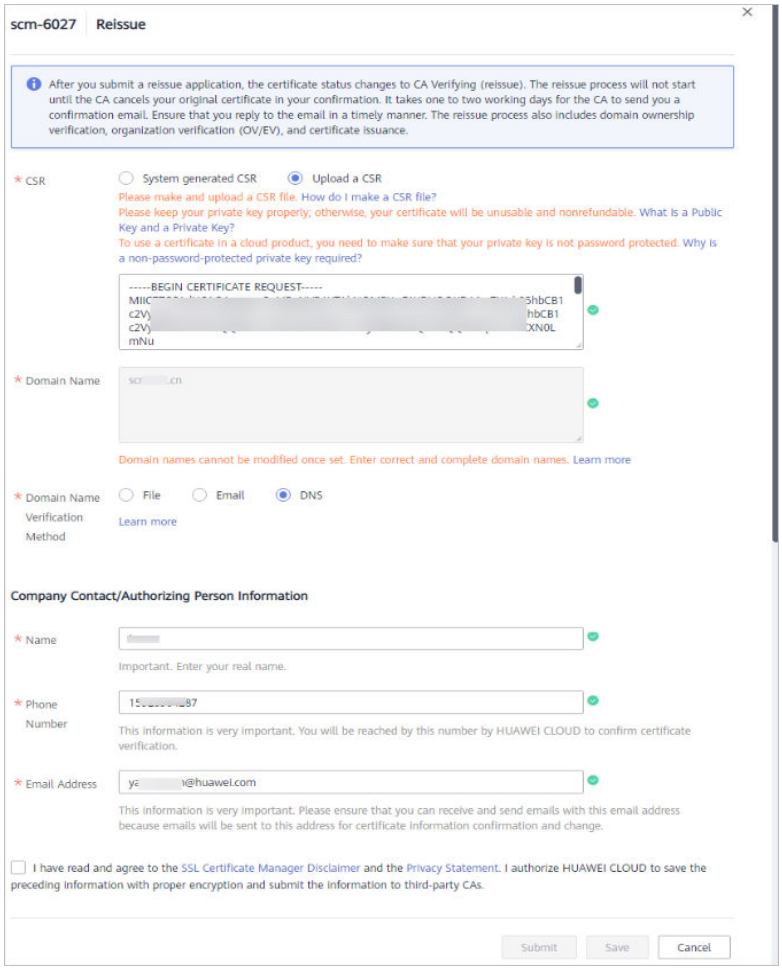


Table 5-1 Domain name parameters

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. • You manually generate a CSR file and paste the content of the CSR file into the text box. For more details, see **How Do I Make a CSR File?** You are advised to select **System generated CSR** to avoid approval failure caused by incorrect content. For details about the differences between the two types of certificate request files, see **What Are the Differences Between the CSR Generated by the System and the CSR Made by Yourself?**	System generated CSR

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

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

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

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

Step 7 Click **Submit**.

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.

   If you have modified the domain name or information about the company contact or authorizer, the certificate is in the **Pending domain name verification** status after the original certificate is canceled. The certificate can be reissued only when you complete **Verifying Domain Name Ownership** and **Verifying the Organization (OV and EV)** (required only for OV, OV Pro, EV, and EV Pro certificates).

----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

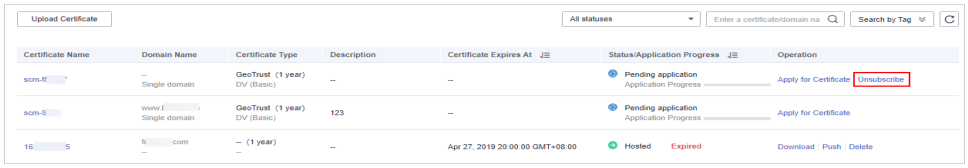
Step 1 Log in to the **management console**.

Step 2 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, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 In the row containing the desired certificate, click **Unsubscribe** in the **Operation** column. **Figure 5-3** shows an example.

Figure 5-3 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

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 exactly 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 or deploy it on the Huawei Cloud product 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

- The entry for renewing a DigiCert DV (basic) wildcard-domain certificate is available only within **15 calendar days** before the certificate expires.
- A DigiCert DV (basic) wildcard-domain certificate you obtain through renewal cannot inherit the remaining validity of the old 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 automatically inherit** the remaining validity period (if any) of the original certificate. So, the validity period of the new certificate is one year.

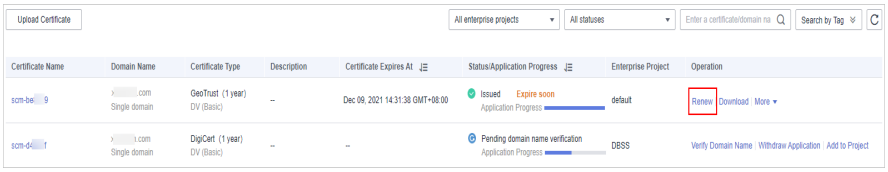
Prerequisites

- The paid certificate is about to expire.
- Auto-renewal is not enabled for the certificate.

Procedure

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, choose **SSL Certificate Manager** > **SSL Certificates**.
4. In the row containing the desired certificate, click **Renew** in the **Operation** column. **Figure 5-4** shows an example.

   Figure 5-4 Renewal

5. 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.
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**.
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.

   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.

   The procedure for installing an SSL certificate varies depending on the web server. The following describes how to install an SSL certificate on mainstream web servers.

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

6. Check whether the new certificate is successfully installed.

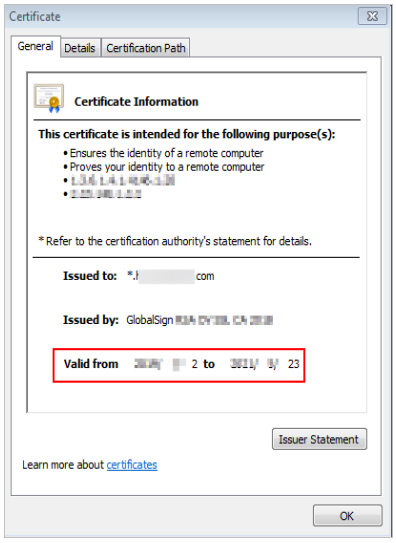
   After the new certificate is installed on the web server, check whether the certificate has been updated.

   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 5-5 Validity Period



5.3.2 Performing an Auto-Renewal

You can enable auto-renewal to let the system renew your certificate before it expires. The system automatically renews a certificate within 30 days before it expires.

CAUTION

To ensure automatic application of certificates, do not cancel privacy authorization.

Auto-Renewal Restrictions

- 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.
- If auto-renewal is enabled for a certificate, the system automatically purchases a new certificate that has the same specifications with the original one 30 days before the original one expires and submits a certificate application using the application information of the original certificate. You still need to cooperate with the CA to complete domain name ownership and/or organization verification. The CA will not issue the certificate until they validate your domain name ownership and identity.
- 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 or deploy it on the Huawei Cloud product 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

- CCM starts a renewal of a DigiCert DV (basic) wildcard-domain certificate **15 calendar days** before the certificate expires.
- A DigiCert DV (basic) wildcard-domain certificate you obtain through renewal cannot inherit the remaining validity of the old certificate.

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, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 In the row containing the certificate you want to renew, click  in the **Auto-renewal** column to enable auto-renewal.

----End

Follow-up Operations

1. Verify the domain name ownership.

   You must complete domain name verification to prove your ownership of the associated domain name. For details, see **Verifying the Domain Name Ownership**.

2. Verify the organization (required for OV and EV certificates only).

   The CA validates the organization used to submit the certificate application. For details, see **Verifying the Organization**.

3. 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.

4. Install the certificate.

   Install the renewed certificate on your web server or deploy it on Huawei Cloud products to replace the old certificate that is about to expire. For details, see **Installing an SSL Certificate**.

5. Check whether the new certificate is successfully installed.

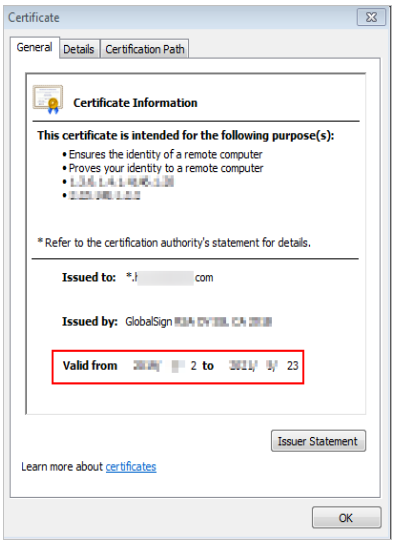
   After the new certificate is installed on the web server, check whether the certificate has been updated.

   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 5-6 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. In addition, the certificate cannot be reissued. A revoked certificate cannot be reissued. For details, see **Reissuing an SSL Certificate**. 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

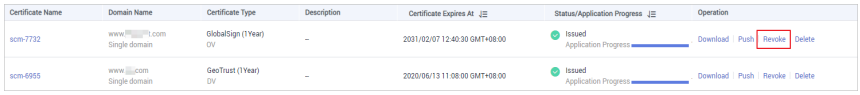
Step 1 Log in to the **management console**.

Step 2 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** > **SSL Certificates**.

Step 4 In the row containing the certificate you wish to revoke, in the **Operation** column, click **Revoke** or **More** > **Revoke**.

Figure 5-7 Revoke



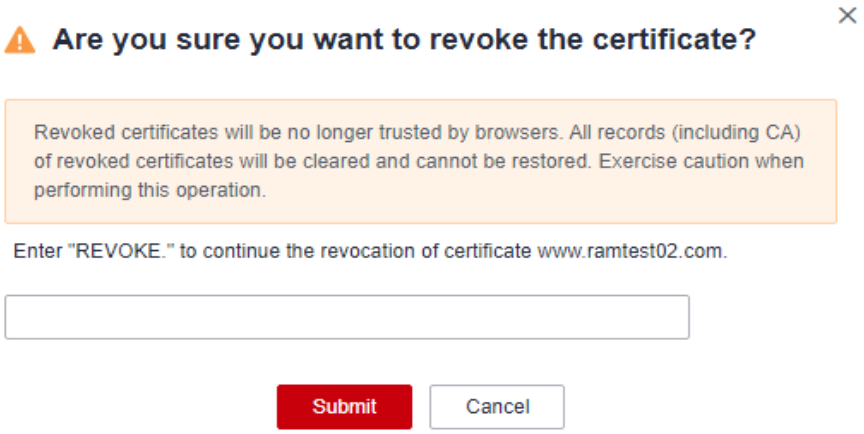
Step 5 In the dialog box displayed, enter "REVOKE" and click **Submit**.

If the **Certificate revoked successfully** message is displayed in the upper right corner, the certificate revocation application has been submitted, and the certificate will be revoked after the application is approved by the CA.

NOTICE

After a certificate revocation application is submitted, it cannot be withdrawn. Exercise caution with a certificate revocation application.

Figure 5-8 Revoke Certificate



Step 6 (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 Huawei Cloud. 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 **Deleting a Certificate**.
- After you delete a certificate, Huawei Cloud 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 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

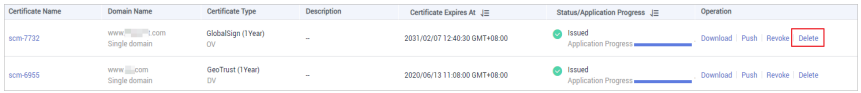
Step 3 In the navigation pane, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 In the row containing the certificate you wish to delete, in the **Operation** column, click **Delete** or **More** > **Delete**.

NOTE

To delete certificates in batches, select the certificates you want to delete and click **Delete** in the upper left corner.

Figure 5-9 Deleting a certificate



Step 5 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. After an SSL certificate is uploaded, you can install the certificate on other Huawei Cloud services and set a reminder before the certificate expires.

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. For more details, see **How Do I Convert a Certificate to PEM Format?**

  For details about how to configure a certificate chain, see **How Do I Configure a Certificate Chain?**
- The private key you want to upload cannot be protected by a password. For more details, see **Why Is a Non-Password-Protected Private Key Required?**
- For uploaded certificates, SCM reminds you of certificate expiration 30 days before the certificates expire. In addition, you can configure notifications, and then SCM sends emails and SMS messages to notify you of certificate expiration two months, one month, one week, three days, and one day before a certificate expires and again when the certificate actually expired. For details, see **How Do I Configure a Certificate Expiration Notification?**

Constraints

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

Procedure

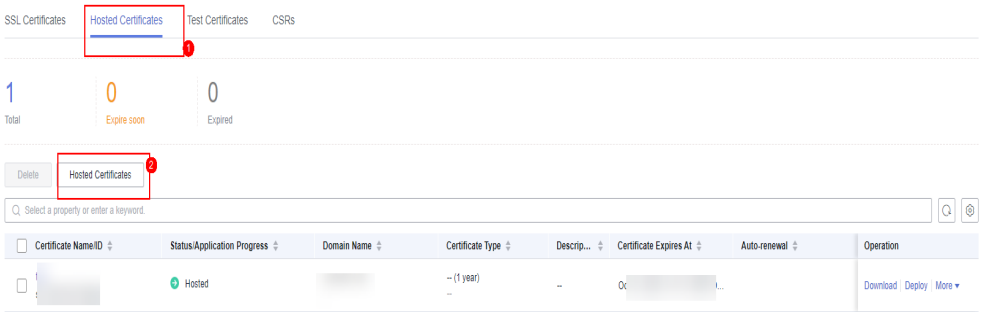
Step 1 Log in to the **management console**.

Step 2 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** > **SSL Certificates**.

Step 4 Click the **Hosted Certificates** tab. In the upper left corner of the displayed tab, click **Hosted Certificates**. The **Hosted Certificates** dialog box is displayed

Figure 5-10 Hosted Certificates



Step 5 In the **Hosted Certificates** dialog box, enter the certificate information. For details, see **Table 5-2**.

Figure 5-11 Uploading a certificate

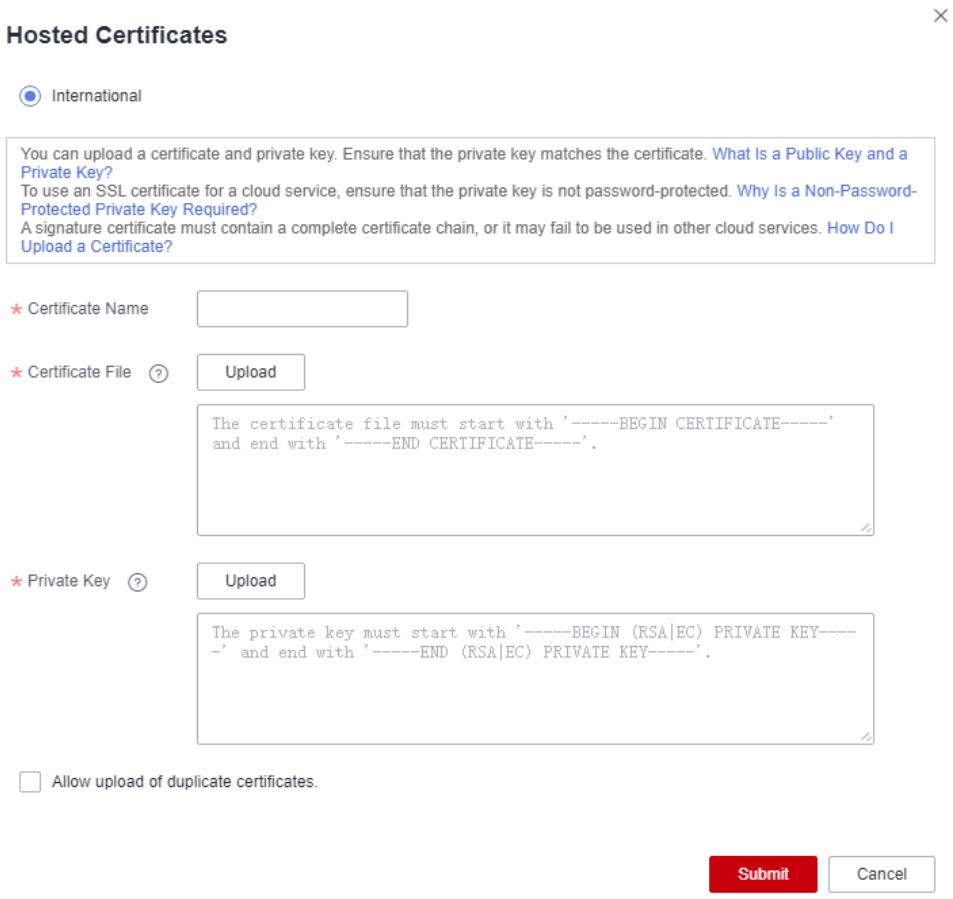


Table 5-2 Parameters for uploading a certificate

Parameter	Description
Certificate Name	A certificate name you specify.
Certificate File	Open the PEM file in the certificate to be uploaded as a text file and copy the certificate content in the file to this text box. Note that you need to upload a combined certificate file that contains both the server certificate content and certificate chain content into this field. The content of the certificate chain should be pasted right below the content of the server certificate. For more details, see **How Do I Upload a Certificate File?**
Private Key	Open the KEY file in the certificate to be uploaded as a text file and copy the private key content to this text box.

NOTE

- The uploaded certificate and key must correspond to each other.
- Ensure that the private key is not protected by a password. For more details, see **Why Is a Non-Password-Protected Private Key Required?**
- If an error message is displayed when you upload a certificate, see **What Can I Do If Errors Are Reported When I Upload an SSL Certificate?**

Step 6 Click **Submit** to upload the certificate.

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

Uploaded certificates can be deployed to other Huawei Cloud products.

----End

Other Operations

Deploy the uploaded certification other cloud products. For more details, see **Deploying an SSL Certificate to Other Huawei Cloud Products**.

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 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, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 In the **Operation** column of the target certificate, click **More** > **Add Additional Domain Name**. The **Add Additional Domain Name** dialog box is displayed.

Step 5 Complete the information based on site requirements. **Table 5-3** describes the required parameters. **Figure 5-12** shows an example.

Figure 5-12 Adding an additional domain name

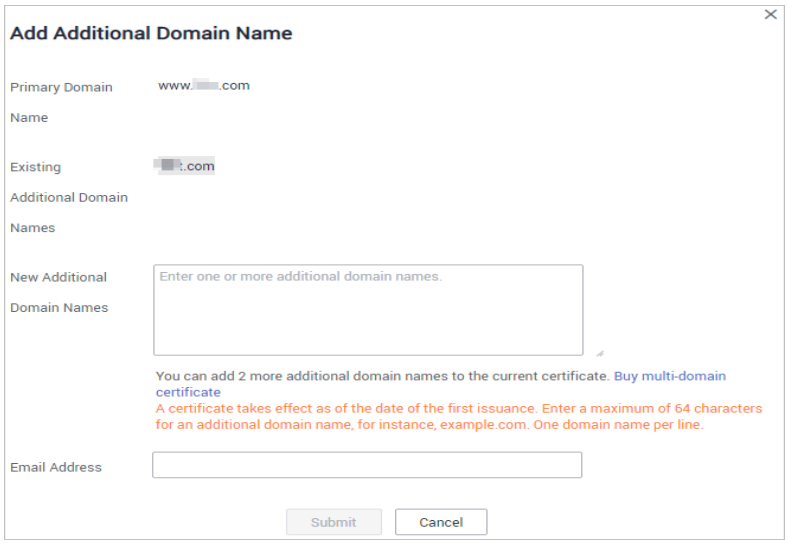


Table 5-3 Parameters

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, HUAWEI CLOUD sends notifications (about certificate issuing) to this email address. Please check it in time. **NOTICE** 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 6 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.

For details, see **Verifying Domain Name Ownership**.

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 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, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 In the **Operation** column of the target certificate, click **Withdraw Application**. The **Cancel Application** dialog box is displayed.

Step 5 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

- You can withdraw a certificate application to modify the domain name or other information as long as the certificate is not issued. Once a certificate is issued, only single-domain and multi-domain certificates can be reissued within the specified period. For more details, see **Reissuing an SSL Certificate**.
- 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

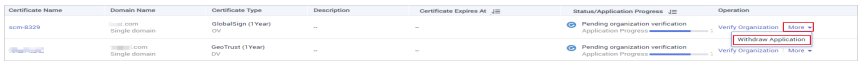
Step 1 Log in to the **management console**.

Step 2 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, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 In the row containing the certificate you wish to withdraw your application for, in the **Operation** column, click **Withdraw Application**.

Figure 5-13 Withdrawing an application



Step 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**.

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. For details, see **Submitting an SSL Certificate Application to the CA**.

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, Huawei Cloud 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 ☰ 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, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 Click the name of the target certificate. The certificate details page is displayed.

Step 5 At the bottom of the certificate details page, find the configuration item **Privacy Authorization**.

Figure 5-14 Privacy authorization

Step 6 Disable privacy authorization.

Step 7 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

After an SSL certificate is issued, you can push it to other Huawei Cloud services, such as Web Application Firewall (WAF), Content Delivery Network (CDN), and Elastic Load Balance (ELB) in just few clicks. In this manner, data access through the cloud services is more secure.

Prerequisites

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

Constraints

- For CDN, SSL certificate names cannot be the same as those of existing SSL certificates. Otherwise, they will fail to be pushed.
- 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**.

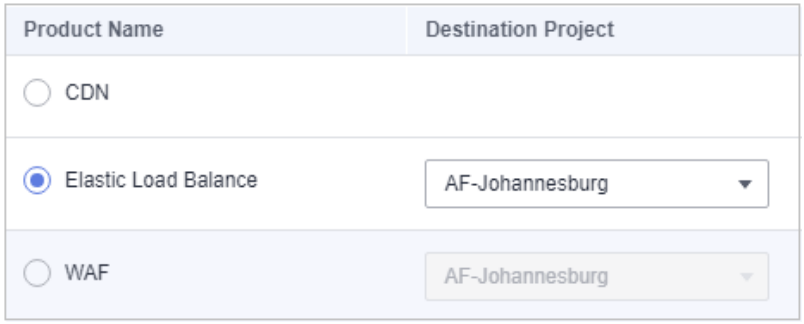
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

Step 3 In the navigation pane on the left, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 In the **Operation** column of the certificate you want to push, click **More** > **Push** to go to the certificate push details page.

Step 5 Select the cloud service you wish to push the certificate to.

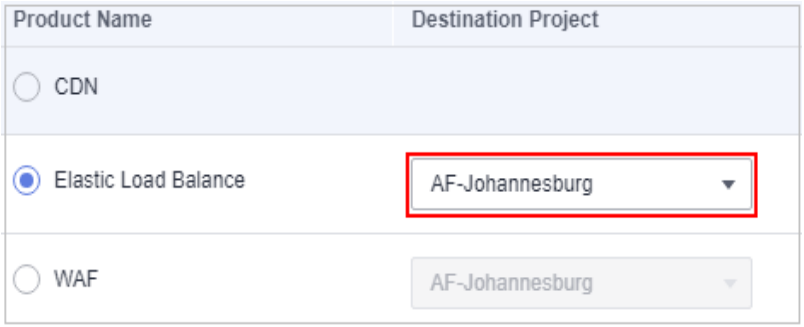
Figure 5-15 Selecting a cloud service



Step 6 (Optional) Perform this step if a certificate is to be pushed to WAF or ELB.

Click ▼ on the right of the target project and select the target region. You can select up to 10 regions.

Figure 5-16 Selecting the destination region



Step 7 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 8 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 Operations

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.

- 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** in ELB.

  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**.

5.11 Viewing Details About an SSL Certificate

This topic walks you through how to view details about your SSL certificates, including paid certificates, test certificates, and hosted certificates. Hosted certificates are the ones you purchase from other platforms and upload to CCM for management.

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

Prerequisites

You have purchased or uploaded a certificate.

Procedure

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

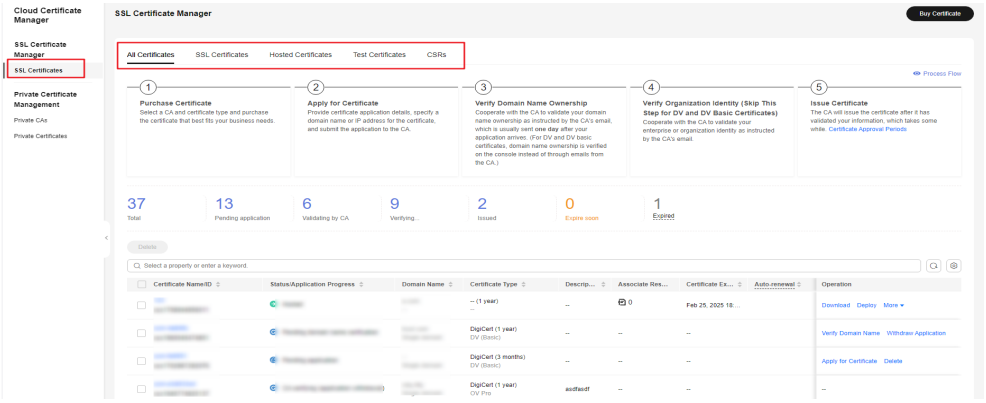
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**. The service console is displayed.

Step 3 In the navigation pane on the left, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 View the certificate details, as shown in the **Certificate list**. **Table 5-4** describes the certificate parameters.

- To view details about all certificates, click the **All Certificates** tab.
- To view details about paid certificates, click the **SSL Certificates** tab.
- To view details about certificates you upload to CCM, click the **Hosted Certificates** tab.
- To view details about test certificates, click the **Test Certificates** tab.

Figure 5-17 Certificate list



NOTE

- To search for a specific certificate, select a filter and enter a keyword in the search box, and click the displayed search criteria or press **Enter**.
- To view details about a certificate, click its name.
- For a hosted or issued certificate, a certificate expiration reminder will be displayed in the **Status/Application** column on the console 30 days before the certificate expires.
- If a certificate has expired for more than 30 days, it will be collapsed in the SSL certificate list automatically. To view details about the certificate, you need to manually search for it.
- In CCM, only certificates that have expired for less than three years are stored.

Table 5-4 Certificate parameters

Parameter	Description
Certificate Name/ID	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 **Changing the Name and Description of a Certificate**.

Parameter	Description
Status/ Application Progress	Options: – **Pending application** You need to submit information, such as domain name and user information, for a certificate. For more details, see **Submitting an SSL Certificate Application to the CA**. The application progress is 0%. – **Pending domain name verification** A certificate application request has been submitted, and domain name verification is to be completed by the CA. For more details, see **Verifying Domain Name Ownership**. The 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 more details, see **Verifying the Organization (OV and EV)**. The application progress is 70%. – **To be issued** 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%. – **Issued** Information you submitted about the certificate has been approved, and domain name and organization verification succeed. The application progress is 100%. – **Approval failed** Information fails to be approved. – **CA verifying (reissue)** An application for a reissue is submitted for an issued certificate and the application is waiting for the approval of the CA. – **CA verifying (domain name addition)** An application for adding a domain name has been submitted for a multi-domain certificate. The CA is verification the added domain name. For details, see **Adding an Additional Domain Name**. – **CA verifying (application withdrawal)** The certificate application withdrawal has been submitted and is waiting for verification from the CA. For

Parameter	Description
	details, see **Withdrawing an SSL Certificate Application**. – **CA verifying (revocation)** The certificate revocation application has been submitted and is waiting for verification from the CA. – **Revoked** The certificate has been revoked. – **Hosted** The uploaded certificate is in the **Hosted** state. – **Expired** Your certificate has expired. If a certificate expires, it cannot be renewed. You can request a new one. – **CA verifying revocation (pending domain name verification)** A certificate revocation request has been submitted, and domain name verification is to be completed by the CA.
Domain Name	Domain name the certificate is used for.
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 **Changing the Name and Description of a Certificate**.
Associated Resources	All cloud resources associated with the current certificate are displayed. You can view their details by referring to **Viewing Associated Cloud Resources**.
Certificate Expires At	Date when a certificate expires **NOTE** For issued certificates, CCM 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.
Auto-renewal	You can enable ( ) or disable ( ) auto-renewal. For details about auto-renewal, see **Performing an Auto-Renewal**.
Operation	You can perform operations, such as apply for a certificate, verify a domain name, verify an organization, and withdraw the application, in the **Operation** column.

----End

Changing the Name and Description of a Certificate

NOTE

The name and description of a shared certificate cannot be modified.

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** > **SSL Certificates**.

Step 4 Click the name of the target certificate. The certificate details page is displayed.

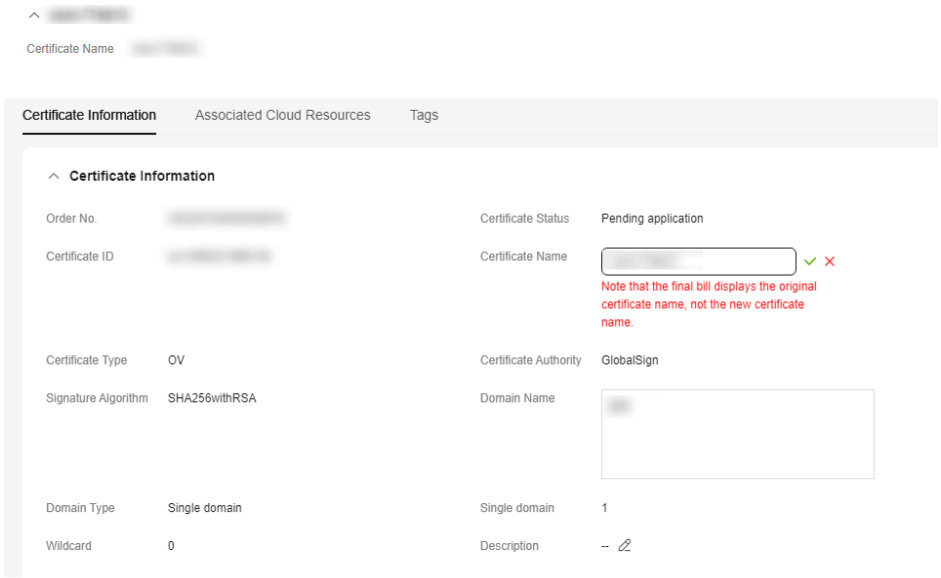
Step 5 Change the certificate name and description.

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.

CAUTION

Note that the final bill displays the original certificate name, not the new certificate name.

Figure 5-18 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

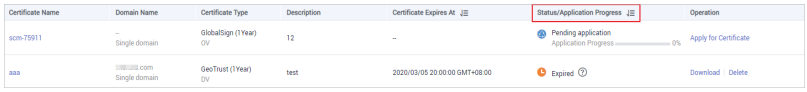
Step 1 Log in to the **management console**.

Step 2 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, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 View the certificate application progress in the **Status/Application Progress** column of the certificate. **Figure 5-19** shows an example.

Figure 5-19 Viewing the Application Progress



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

- **Pending application**: You have not submitted the certificate application to the corresponding CA. You need to submit it manually. For details, see **Submitting an SSL Certificate Application to the CA**.
- **Pending domain name verification**: You have submitted the certificate application to the CA but have not completed domain name ownership verification. You need to validate domain name ownership as instructed by the CA. For details, see **Verifying Domain Name Ownership**.
- **Pending organization verification**: For an OV or EV certificate, the CA will further validate your organization identity after domain name ownership verification. For more details, see **Verifying the Organization (OV and EV)**.
- **To be issued**: You have completed operations, such as domain name ownership verification and organization verification. The CA will issue the certificate after it has validated your verification, which takes some while.

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

----End

5.13 CSRs

You can refer to this section to create CSRs and private keys, upload existing CSRs, and manage them centrally based on RSA, ECC, and SM2.

5.13.1 Create CSR

Procedure

Step 1 Log in to the management console.

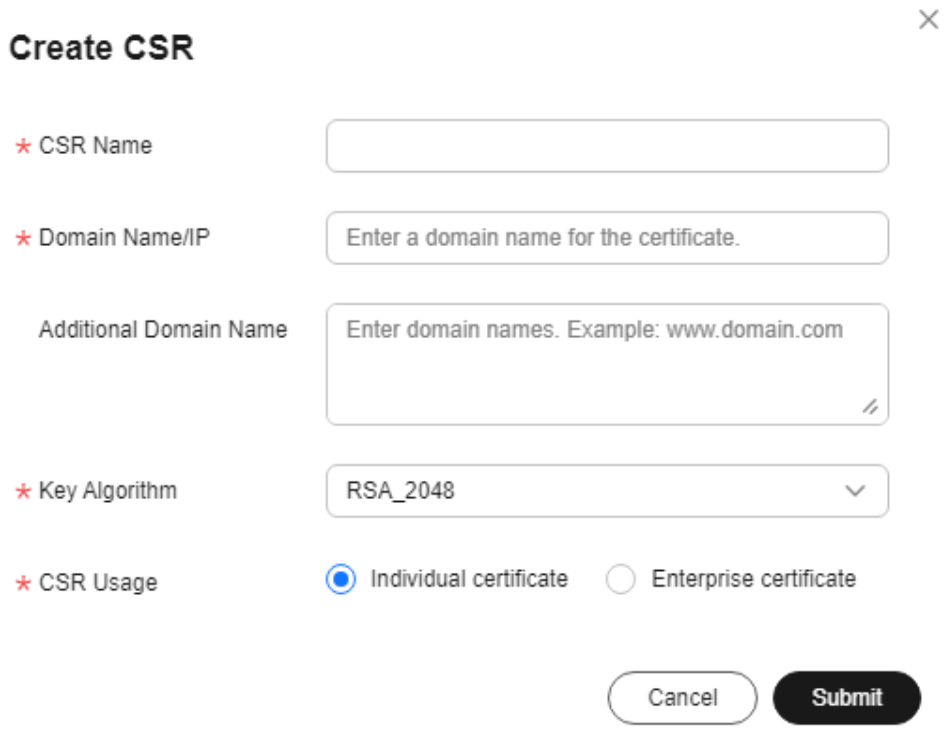
Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Cloud Certificate Management Service**.

Step 3 In the navigation pane, choose **SSL Certificate Manager** > **SSL Certificates** > **CSRs**. The CSRs page is displayed.

Step 4 Click **Create CSR**.

Step 5 In the displayed dialog box, set the parameters, as shown in the following figure Create CSR.

Figure 5-20 Create CSR



The table below describes the parameters.

Table 5-5 Description

Parameter	Description
CSR Name	Customize a name for the created CSR. The value can contain uppercase letters, lowercase letters, numbers, underscores (_), and hyphens (-). The value is a string of a maximum of 50 characters.
Domain Name/IP	Configure the domain name of the certificate to be requested. If you want to use the CSR, ensure the domain name bound to a certificate contains the domain name set here. Example: If you set the domain name to **huaweiyun.com**, a CSR can be matched only if its domain name is bound to a certificate containing **huaweiyun.com**.
Additional Domain Name	Enter another domain name that shares the same certificate with the configured domain name. You can enter multiple domain names and separate them with commas (,).
Key Algorithm	Types of the key algorithm are as follows. Value: ● RSA_2048 ● RSA_3072 ● RSA_4096 ● EC_P256 ● EC_P384 ● SM2
CSR Usage	Select the usages of the CSR. Values: ● Individual certificate ● Enterprise certificate If you select enterprise certificate for the CSR usage, enter the company name and country/region.

Step 6 Click **OK** to create a CSR.

----End

Follow-up Operations

- After the CSR is created, you can view its details in the CSR list.
- You can set **Select an existing CSR** and select a target CSR from the matched CSRs.

  NOTE

  You can also click **Edit** or **Delete** in the **Operation** column of a CSR.
  - Only the CSR name can be edited.
  - Deleted CSRs cannot be restored. Exercise caution when performing this operation.

5.13.2 Upload CSR

If you need to use a CSR that is not created on the cloud service management console when applying for a certificate, you can refer to this section.

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**.

Step 3 In the navigation pane, choose **SSL Certificate Manager** > **SSL Certificates** > **CSRs**.

Step 4 Click **Upload CSR**.

Step 5 On the displayed page, upload the **Certificate File** and **Private Key**, as shown in **Upload CSR**.

Figure 5-21 Upload CSR

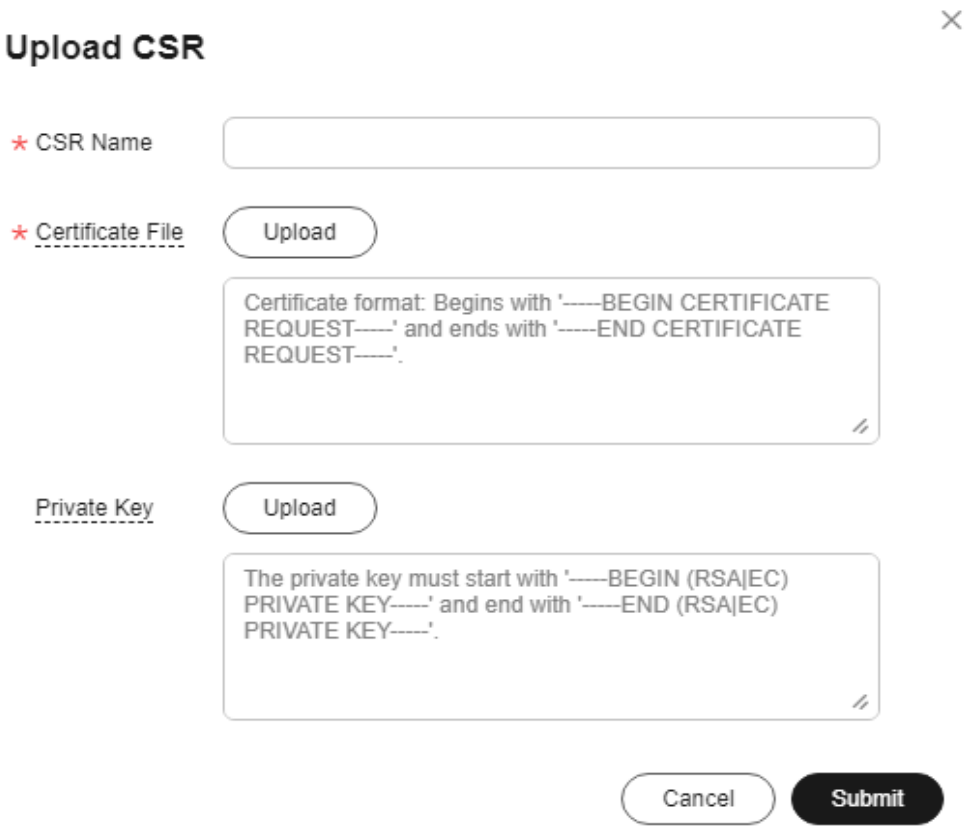


Table 5-6 Description

Parameter	Description
CSR Name	Enter a name for the created CSR. The value can contain uppercase letters, lowercase letters, numbers, underscores (_), and hyphens (-). The value is a string of a maximum of 50 characters.
Certificate File	Upload the target CSR file. Click **Upload** under the text box, select the CSR file stored on the local computer, and upload the file to the text box.
Private Key	Upload the certificate private key. Click **Upload** under the text box, select the certificate private key stored on the local computer, and upload the file to the text box.

Step 6 Click **Submit**.

----End

Follow-up Operations

- After the CSR is uploaded, you can view the details of the uploaded CSR in the CSR list.
- You can set **Select an existing CSR** and select a target CSR from the matched CSRs.

  NOTE

  You can also click **Edit** or **Delete** in the **Operation** column of a CSR.
  - Only the CSR name can be edited.
  - Deleted CSRs cannot be restored. Exercise caution when performing this operation.

6 Sharing

6.1 Overview

Introduction

SCM allows you to share an SSL certificate of account A with all member accounts, such as accounts B and C, in the same organization unit. These accounts can deploy the shared certificate on services such as ELB, WAF, and CDN to enable HTTPS.

- Account A is the SSL certificate owner (owner for short).
- Accounts B and C are SSL certificate recipients (recipient for short).

SSL Certificate Owner and Recipient Permissions

Owners can perform all operations on SSL certificates, while recipients can only perform certain operations. For details, see **Table 6-1**.

Table 6-1 Operations supported for SSL certificate recipients

Role	Operation Supported	Description
Recipient	scm:cert:get	Access through the console or API
	scm:cert:getApplicationInfo	Access through the console or API
	scm:cert:getDomainValidation	Access through the console or API
	scm:cert:listDeployedResources	Access through the console or API
	scm:cert:listCertificatesByTag	Access through the console or API

Role	Operation Supported	Description
	scm:cert:listTagsByCertificate	Access through the console or API
	scm:cert:listAllTags	Access through the console or API
	scm:cert:push	Access through the console or API
	scm:cert:listPushHistory	Access through the console or API
	scm:cert:enableAutoDeploy	Access through the console or API
	scm:cert:listAutoDeployedResources	Access through the console or API
	scm:cert:deployResources	Access through the console or API
	scm:cert:listDeployResourcesHistory	Access through the console or API
	scm:cert:getDeployQuota	Access through the console or API

Supported Resource Types and Regions

Table 6-2 lists the resource types and regions can be shared in SCM.

Table 6-2 Resources and regions supported by SCM

Cloud Service	Resource Type	Supported Region
SCM	cert: SSL certificate	ALL

Billing Description

For details about SCM billing, see **Billing Items**.

The certificate owner pays for the shared certificates. So, only the resource owner will be charged for shared resources.

6.2 Creating a Resource Share

Scenario

To share resources with other accounts, you need to create a resource share first. During the creation, you need to specify resources to be shared, configure permissions, specify users to be shared with, and confirm the configuration.

Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner, choose **Management & Governance** > **Resource Access Manager**, and go to the resource access management page.

Step 3 Choose **Shared by Me** > **Resource Shares**.

Step 4 Click **Create Resource Share** in the upper right corner.

Step 5 Set resource type to **scm:cert**, choose the corresponding region, and select SSL certificates to be shared. Click **Next: Associate Permissions**.

Step 6 Associate a RAM managed permission with each resource type on the displayed page. Then, click **Next: Grant Access to Principals** in the lower right corner.

Step 7 Specify the principals that you want to have access to the resources on the displayed page. Then, click **Next: Confirm** in the lower right corner.

Table 6-3 Description

Parameter	Description
Principal Type	• Organization For details about how to create an organization, see **Creating an Organization**. **NOTE** If you haven't enabled resource sharing with organizations, this parameter cannot be set to **Organization**. For details, see **Enabling Sharing with Organizations**. • Huawei Cloud account ID

Step 8 Check the configurations and click **OK**.

NOTE

After a resource share is created, RAM initiates a resource sharing invitation to the specified principals. If the principal type is **Huawei Cloud account ID**, the principals can access and use the shared resources only after they accept the invitation. If the principal type is **Organization**, the principals in that organization are automatically granted access to the shared resources without the use of invitations.

----End

6.3 Updating a Resource Share

You can update a resource share at any time, including updating its name, description, tags, shared resources, RAM managed permissions, and principals.

Procedure

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

Step 2 Click ☰ in the upper left corner, choose **Management & Governance** > **Resource Access Manager**, and go to the resource access management page.

Step 3 Choose**Shared by Me** > **Resource Shares**.

Step 4 Select the resource share to be updated and click **Edit** in the **Operation** column.

Step 5 Update the resource share on the displayed page. You can modify its name, description, tags, and add or delete shared resources.

Step 6 After the update is complete, click **Next: Associate Permissions** in the lower right corner.

Step 7 Add or delete the permissions supported by **scm:cert**. Wait until the update is complete, click **Next: Grant Access to Principals**.

Step 8 On the displayed page, add or delete principals based on your needs. Then, click **Next: Confirm** in the lower right corner.

Step 9 Confirm the configurations and click **OK** in the lower right corner.

----End

6.4 Viewing a Resource Share

You can check the details of the created resource share, as well as search for, edit, and delete a resource share. Moreover, you can check the shared resources and resource principals.

Procedure

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

Step 2 Click ☰ in the upper left corner, choose **Management & Governance** > **Resource Access Manager**, and go to the resource access management page.

Step 3 Choose**Shared by Me** > **Resource Shares**.

Step 4 Click the target resource share, go to the details page, and check the configurations.

NOTE

You can query shared SSL certificate and resource principals. For details, see **Viewing Your Shared Resources** and **Viewing Principals You Share With**.

----End

6.5 Responding to a Resource Sharing Invitation

You can check the resource sharing invitation and confirm whether you will accept the invitation.

Constraints

- If you are in the same organization with the resource owner, and sharing resources with organization has been enabled, you do not need to accept the invitation to access the shared resources.
- If you are in a different organization from the resource owner, or sharing resources with organization has not been enabled, you will receive a resource sharing invitation.
- The invitation exists for seven days by default. If the invitation is not accepted after seven days, it is rejected by system. To use the shared resources, the owner should create a resource share to generate a new invitation.

  NOTE

  For details about enabling resource sharing with organizations, see **Enabling Sharing with Organizations**.

Procedure

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

Step 2 Click ☰ in the upper left corner, choose **Management & Governance** > **Resource Access Manager**, and go to the resource access management page.

Step 3 Choose **Share with Me** > **Resource Shares** and access the resource share management page.

Step 4 Click **Resource Shares To Be Accepted**, select target resource shares, and click **Accept** or **Reject** in the **Operation** column.

Step 5 Click **OK** in the displayed dialog box.

Step 6 After accepting the invitation, you can check the accepted resource shares on the displayed page.

NOTE

After accepting the invitation, you can view the shared resources in use and the resource owner. For details, see **Viewing Your Shared Resources** and **Viewing Principals You Share With**.

----End

6.6 Leaving a Resource Share

If you no longer need to access shared SSL certificates, you can leave a share at any time. After you leave the share, you will lose access to the shared SSL certificate.

Procedure

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

Step 2 Click  in the upper left corner, choose **Management & Governance** > **Resource Access Manager**, and go to the resource access management page.

Step 3 Choose **Share with Me** > **Resource Shares** and access the resource share management page.

Step 4 Click **Accepted Resource Shares**, select target instances, and click **Leave**.

Step 5 Click **Leave** in the displayed dialog box.

----End

7 Managing Tags

7.1 Overview

Scenario

Tags can be used to identify SSL certificates. You can use tags to group certificates by usage, owner, or environment and manage them centrally.

You can add a tag when purchasing a certificate or add a tag on the certificate details page after the purchase.

Tag Naming Rules

- Each tag consists of a key-value pair.
- A maximum of 20 tags can be added for an SSL certificate.
- For each certificate, a tag key must be unique and can have only one tag value.
- A tag consists of a tag key and a tag value. The naming rules are listed in **Table 7-1**.

  NOTE

  If your organization has configured a tag policy for the CCM service, you need to add tags to resources based on the tag policy. If a tag does not comply with the policies, the tag may fail to be added for a certificate. Contact your organization administrator to learn more about tag policies.

Table 7-1 Tag parameters

Parameter	Rule	Example
Tag key	• This parameter is mandatory. • An SSL certificate can have only one tag key. • The value can contain a maximum of 128 characters. • The value cannot start or end with a space. • The value cannot start with _**sys**_. • The following character types are allowed: – Chinese – English – Digit – Space – Special characters: _.:/=+	cost
Tag value	• This tag value can be left blank. • The value can contain a maximum of 255 characters. • The value cannot start or end with a space. • The following character types are allowed: – Chinese – English – Digit – Space – Special characters: _.:/=+-@	100

7.2 Creating a Tag Policy

Introduction

Tag policies are a type of policy that can help you standardize tags across resources in your organization's accounts. A tag policy is only applied to tagged resources and tags that are defined in that policy.

For example, a tag policy can specify that a tag attached to a resource must use the case treatment and tag values defined in the tag policy. If the case and value of the tag do not comply with the tag policy, the resource will be marked as non-compliant.

You can use tag policies as detective or preventive guardrails:

1. Detective guardrails: If a resource tag violates a tag policy, the resource will appear as noncompliant in the compliance result.

2. Preventive guardrails: If enforcement is enabled for a tag policy, non-compliant tagging operations will be prevented from being performed on specified resource types.

Constraints

Only organization administrators can create a tag policy.

NOTE

Before you create a tag policy and add it to the organization unit and account, a tag policy must be enabled by the administrator account. For details, see **Enabling or Disabling the Tag Policy Type**.

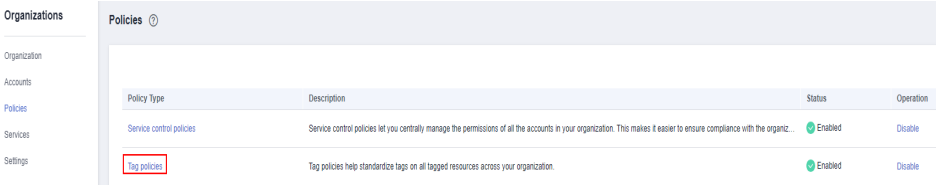
Procedure

Step 1 Log in to Huawei Cloud as an organization administrator or an administrator account.

Step 2 Click ☰ on the left, choose **Management & Governance** > **Organizations**. The organization management page is displayed.

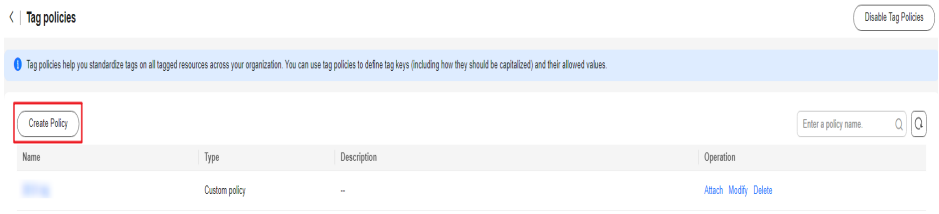
Step 3 Click **Policies** on the left to go to the policy management page and click **Tag policies**.

Figure 7-1 Accessing the **Tag policies** page



Step 4 Click **Create Policy**.

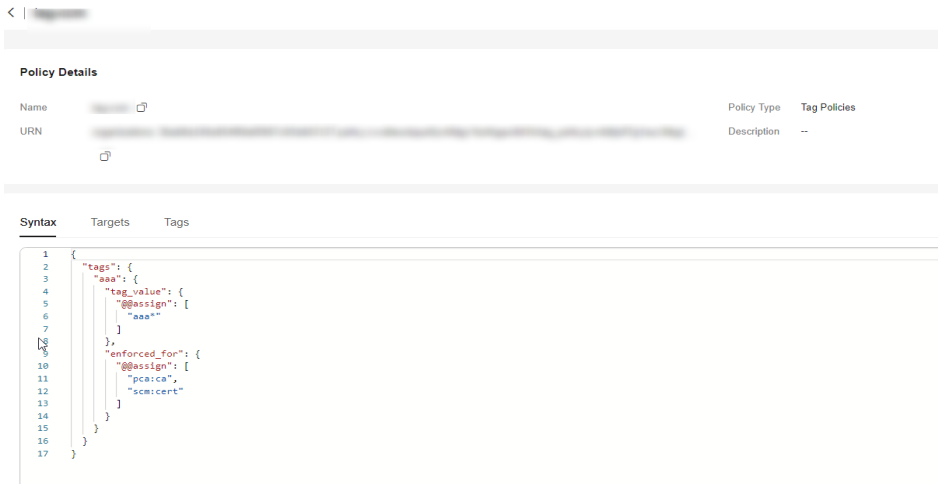
Figure 7-2 Creating a policy



Step 5 Enter a policy name. Note that the policy name you enter cannot be the same as that of other policies.

Step 6 Set a policy according to **Tag Policy Syntax**. The system automatically verifies the syntax. If the syntax is incorrect, modify it as prompted.

Figure 7-3 Setting a policy tag



Step 7 (Optional) Add one or more tags to the policy. Enter a tag key and a tag value, and click **Add**.

Step 8 Click **Save** in the lower right corner. If the tag policy is created successfully, it will be added to the list.

NOTE

To update or delete a tag policy, see **Updating or Deleting a Tag Policy**.

To attach or detach a tag policy, see **Attaching or Detaching a Tag Policy**.

----End

7.3 Creating a Tag

This topic describes how to add a tag to an SSL certificate.

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.

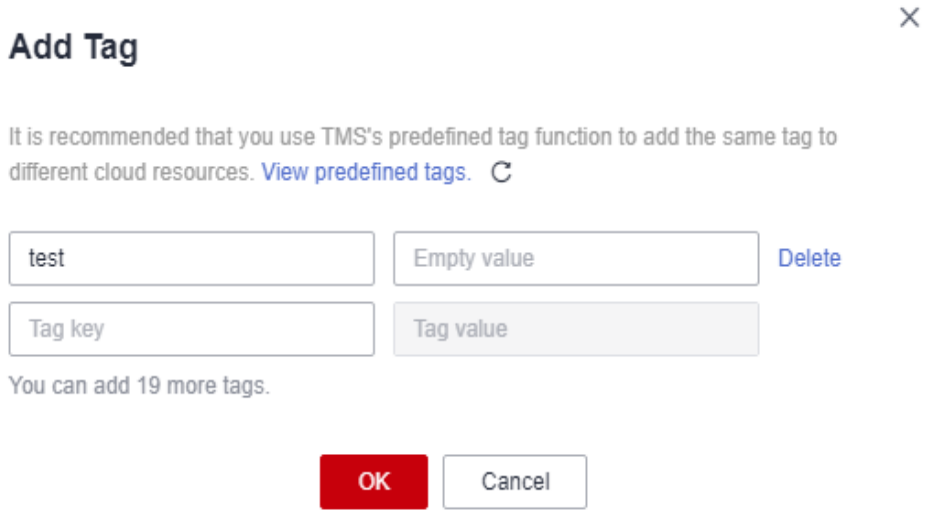
Step 3 In the navigation pane on the left, choose **SSL Certificate Manager** > **SSL Certificates**.

Step 4 Click the name of the target SSL certificate to go to its details page.

Step 5 Click the **Tags** tab to go to the tag management page.

Step 6 Click **Add Tag**. In the displayed dialog box, set **Tag key** and **Tag value**.

Figure 7-4 Add Tag



NOTE

To delete a tag, click **Delete** next to it.

- If you want to use the same tag to identify multiple cloud resources, you can create predefined tags in TMS. In this way, the same tag can be selected for all services. For more information about predefined tags, see the *Tag Management Service User Guide*.
- To delete a tag, click **Delete** next to it.

Step 7 Click **OK** to complete.

----End

7.4 Searching for SSL Certificates by Tag

This section describes how to search for an SSL certificate by tag in a project on the SCM console.

Prerequisites

A tag has been added.

Constraints

- At most 20 tags can be added for one search. If multiple tags are added, SSL certificates that meet all search criteria will be displayed.

- If you want to delete an added tag from the search criteria, click next to the tag.

Procedure

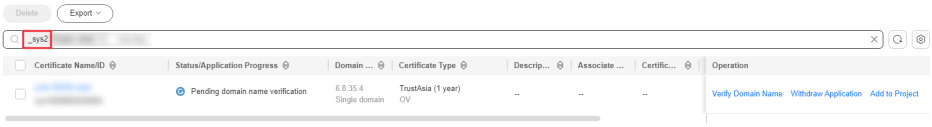
Step 1 Log in to the **management console**.

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** > **SSL Certificates**.

Step 4 Click the search box and enter the tag key and tag value to search for the resource. SSL certificates that meet the search criteria are displayed.

Figure 7-5 Search result



NOTE

- At most 20 tags can be added for one search. If multiple tags are added, SSL certificates that meet all search criteria will be displayed.
- If you want to delete an added tag from the search criteria, click next to the tag.

----End

7.5 Editing a Tag Value

This section describes how to edit an SSL certificate tag.

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** > **SSL Certificates**.

Step 4 Click the name of the target SSL certificate to go to its details page.

Step 5 Click the **Tags** tab to go to the tag management page.

Step 6 Click **Edit**. The **Edit Tag** dialog box is displayed. Edit the tag value and click **OK**.

----End

7.6 Deleting a Tag

This section describes how to delete an SSL certificate tag.

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** > **SSL Certificates**.

Step 4 Click the name of the target SSL certificate to go to its details page.

Step 5 Click the **Tags** tab to go to the tag management page.

Step 6 Click **Edit Tag**. In the displayed dialog box, locate the row that contains the target tag, click **Delete**, and then click **OK**.

----End

8 Permissions Management

8.1 Creating a User and Granting SCM Permissions

This topic describes how to use **IAM** to implement fine-grained permissions control for your SCM resources. With IAM, you can:

- 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 on your HSS resources.

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

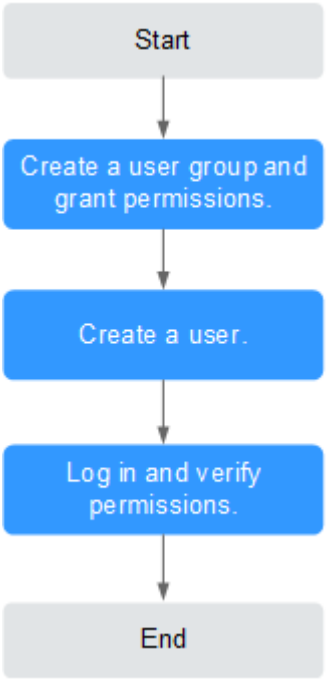
This topic describes the procedure for granting permissions (see **Figure 8-1**).

Prerequisites

Learn about the permissions (see **Permissions Management**) supported by SCM and choose policies or roles based on your requirements.

Process Flow

Figure 8-1 Process for granting SCM permissions



1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console and grant the user group the **SCM Administrator** permission for SCM.

2. **Create an IAM user.**

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** 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.

8.2 Custom Policies for SCM

Custom policies can be created to supplement the system-defined policies of CCM. For actions you can add to custom policies, see **Permissions and Supported Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common SCM custom policies.

Example Custom Policies

- Example 1: Allowing users to query the certificate list

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "scm:cert:list"
            ],
            "Effect": "Allow"
        }
    ]
}
```

- 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:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "scm:cert:upload",
                "scm:cert:push",
                "cdn:configuration:queryHttpsConf"
            ],
            "Effect": "Allow"
        }
    ]
}
```

