

Cloud Certificate Manager

Getting Started

Issue 01
Date 2026-03-31



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

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 Quickly Applying for and Using an OV SSL Certificate.....	1
2 Getting Started Through Common Practices.....	12

1 Quickly Applying for and Using an OV 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.

Scenarios

- Cloud Certificate & Manager provides domain SSL certificates. You can purchase them as required. There are three types of domain name certificates: DV, OV, and EV. OV wildcard-domain SSL certificates are widely used to provide encryption protection for all subdomain names and are widely used by the Ministry of Foreign Affairs, State Grid, and Huawei Cloud.
- This topic walks you through on how to quickly apply for and use an SSL certificate in CCM. Let's apply for a wildcard-domain OV SSL certificate from GlobalSign.
- A wildcard-domain certificate can protect only subdomains of the same level. For example, a level-2 wildcard domain name *.example.com can protect test.example.com, but cannot protect a level-3 subdomain name such as test.test.example.com.

Procedure

Step	Description
Preparations	After registering a Huawei Cloud and enabling Huawei Cloud services, complete real-name authentication, top up your account, and grant permissions to IAM users.
Step 1: Purchase an SSL Certificate	Configure the parameters for purchasing an OV SSL certificate.
Step 2: Apply for an SSL Certificate	After you purchase a certificate, associate a domain name, provide additional details, and then submit the application for approval.


Step	Description
Step 3: Verify the Domain Ownership	After you submit a certificate application, configure domain name verification information to verify your ownership of the domain name.
Step 4: Verify the Organization	After the domain name ownership is verified, the CA will initiate organization verification.
Step 5: Issue an SSL Certificate	After the organization verification is complete, the CA manually reviews the certificate information. After the information is approved, the CA issues the certificate.
Step 6: Using an OV SSL Certificate	After applying for a certificate, you can deploy the certificate to other Huawei Cloud services in one-click mode or download the certificate and deploy it on a server.

Preparations

1. Sign up with Huawei Cloud and complete real-name authentication.
Before purchasing a certificate, [Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services](#) and [Real-name authentication](#).
2. Ensure that your account has sufficient balance or has a valid payment method configured.
3. 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](#).

Step 1: Purchase an SSL Certificate

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

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance > Cloud Certificate & Manager**. The SSL certificate manager page is displayed.

Step 3 In the upper right corner of the page, click **Buy Certificate** to go to the certificate purchase page.

Step 4 On the **Buy CCM** page, set the following parameters, as shown in [Figure 1-1](#).

Table 1-1 Parameters for purchasing an OV SSL certificate

Parameter	Example	Description
Billing Mode	One-time	SSL certificates are a single-time product.
Type	SSL certificate - domain name	-
Domain Type	Wildcard	You can associate Single domain , Multiple domain , or Wildcard with a certificate as required. For more information, see Domain Name Types Supported in SCM .
Domain Quantity	1	<ul style="list-style-type: none"> If the Domain Type value is Single domain or Wildcard, you can only associate one domain name with a certificate. If the Domain Type value is Multiple domains. The number of domain names ranges from 2 to 250. Set the number of domain names as required.
Certificate Type	OV	CCM provides three types of SSL certificates: OV, DV, and EV. Different types of certificates apply to different application scenarios, trust levels, and security levels. For details, see Certificate Types .
Certificate Authority	GlobalSign	CCM supports the following certificate authorities: GeoTrust , DigiCert , GlobalSign , CFCA (Chinese) , TrustAsia (Chinese) , and vTrus (Chinese) . CCM supports the following certificate authorities: DigiCert , GeoTrust , and GlobalSign . For details about the types of certificates that can be issued by each CA, see Certificate Authority .
Region	All	-
Subscription Period	1 year	Select the subscription period as required. The longer the subscription period, the higher the discount.
Enterprise Project	default	This parameter is displayed only when you use an enterprise account to purchase an SSL certificate. It enables unified management of cloud resources by project.
Quantity	1	Set the value as required.
Tags	Not added	Tags are used to identify SSL certificates, facilitating cloud resource classification and management.

Figure 1-1 Parameters for purchasing an OV SSL certificate

Certificate Type	OV	OV Pro	DV	DV (Basic)
Application Scenario	Websites, applications, and applets of small and medium-sized enterprises	Websites, applications, and applets of small and medium-sized enterprises. OV Pro certificates use stronger encryption algorithms than OV certificates.	Personal websites and enterprise tests. This type of certificate cannot be issued for special top-level domain names such as edu.cn, edu, and gov.	Personal websites and enterprise tests. This type of certificate cannot be issued for special top-level domain names such as edu.cn, edu, and gov.
Supported Cryptographic Algorithms	RSA_2048, RSA_3072, RSA_4096, EC_P256, EC_P384			
Security	High	High	General	General
Validation Requirements	The CA follows a standard process to validate the organization identity and the domain name ownership.	The CA follows a standard process to validate the organization identity and the domain name ownership.	The CA validates the domain name ownership only.	The CA validates the domain name ownership only.
What the Browser Displays	HTTPS in the URL and a padlock icon in the address bar	HTTPS in the URL and a padlock icon in the address bar	HTTPS in the URL and a padlock icon in the address bar	HTTPS in the URL and a padlock icon in the address bar
Validation Duration	3 to 5 working days	3 to 5 working days	Several hours	Several hours

Step 5 Click **Next**.

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.

----End

Step 2: Apply for an SSL Certificate

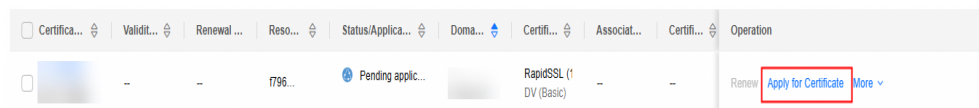
After you purchase a certificate, you still need to associate a domain name with it, provide certain details, and then submit it for approval. The CA will not issue the certificate until all of the submitted details have been reviewed.

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

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance > Cloud Certificate & Manager**. The SSL certificate manager page is displayed.

Step 3 In the **Operation** column that contains the certificate to be applied for, click **Apply for Certificate**.

Figure 1-2 Applying for a Certificate



Step 4 On the displayed page, set parameters such as domain name, enterprise, and applicant. For details, see [Submitting an SSL Certificate Application](#).

Figure 1-3 Certificate application details page

Apply for Certificate

✕

Domain Name Details

★ CSR System-generated CSR (recommended) Select an existing CSR Upload a CSR

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

★ Domain Name/IP

Domain names cannot be modified once the certificate application is submitted. Enter correct and complete domain names. [How Do I Enter a Domain Name?](#)
(For example, if you enter `www.cloud.com`, the certificate protects `www.cloud.com`. If you enter `cloud.com`, the certificate protects `cloud.com`, instead of `www.cloud.com`.)

Key Algorithm

RSA_2048

Company Information

★ Company Name

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

★ Country/Region

▼

Applicant Details

★ Name

[Name]

✔

Enter a valid full name.

★ Phone Number

[Phone]

✔

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

Submit

Save

Cancel

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

Step 3: Verify the Domain Ownership

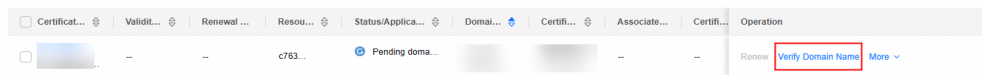
The CA will handle your application within 2 to 3 working days and send a verification email to you. You need to verify the domain name as required to prove the domain name ownership. This section uses DNS verification as an example.

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

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance > Cloud Certificate & Manager**. The SSL certificate manager page is displayed.

Step 3 In the SSL certificate list, locate the row that contains the certificate to be applied for, and click **Verify Domain Name** in the **Operation** column.

Figure 1-4 Domain ownership verification



Step 4 On the **Verify Domain Name** page, view the content for **Host Record**, **Record Type**, and **Record Value**. [Figure 1-5](#) shows an example.

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

Figure 1-5 Viewing a host record

DNS

Basic Information

Certificate Name: scm-8b519e
Domain Name: [Redacted]

Procedure

- 1 Go to the DNS of the domain name and log in to the domain name management platform (your domain name hosting platform).
- 2 Add DNS resolution records on the domain name management platform.
Go to the DNS platform hosting the following domain name and add a record using the following information. [\(What Is a Host Record?\)](#)
[View Tutorials](#)

Domain Name	Host Record	Record Type	Record Value
[Redacted]	_dnsauth	TXT	[Redacted]

- 3 Check whether the DNS verification was successful.

Info: If they are different, the configuration of domain name verification does not take effect. [How Do I Check Whether File Verification Is Successful?](#)

If you have configured DNS resolution on the DNS console, click Verify to check your configuration.

Step 5 Go to the DNS service provider of your domain name and add a record. For details, see [Manual DNS Verification](#).

Step 6 Check whether the domain name verification takes effect. For details, see [Manual DNS Verification](#).

Step 7 Review the DNS verification result.

If you have verified the domain name ownership, the CA will take 2 to 3 working days to verify your information. You can proceed to the organization verification step only after the application is approved.

----End

Step 4: Verify the Organization

If you apply for an OV SSL certificate, the CA sends an organization verification email after domain name ownership is verified. The CA validates your organization identity by contacting you through the method you select.

- If you purchase a certificate again from the same CA within 13 months and the certificate information is not changed, organization verification is not required.
- After the organization verification completes, it takes some time for CA to complete the verification.

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.

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

----End

Step 5: Issue 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.

Generally, the CA manually reviews the information about an OV SSL certificate after the organization verification is complete. If the information is correct, the review takes three to five working days. After the CA approves the certificate, it issues the certificate. The certificate takes effect upon issuance. The OV SSL certificate application is complete.

Step 6: Using an OV SSL Certificate

After applying for a certificate, you can deploy the certificate to other Huawei Cloud services in one-click mode or download the certificate and deploy it on a server. [Downloading a Certificate](#). The following describes how to deploy a certificate:

Scenario 1: Deploying an SSL Certificate to WAF

If traffic passes through WAF and needs to be encrypted using HTTPS, you need to deploy the SSL certificate on WAF, especially when the multi-node architecture such as **CDN** → **WAF** → **Origin Server** is used. This prevents attackers from tampering with data on intermediate nodes and decrypts, detects, and allows incoming traffic, improving overall security and data transmission security.

- Prerequisites
 - You have enabled WAF, routed your website domain name to WAF, and configured an SSL certificate for the domain name in WAF.
 - You have an SSL certificate that is in **Issued** or **Hosted** status.
- Constraints
 - 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.
 - 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 Huawei 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.
- Step
 - a. Log in to the [CCM console](#).
 - b. In the navigation pane on the left, choose **SSL Certificate Manager** > **SSL Certificates**.
 - c. Locate the row containing the certificate you want to deploy on other cloud product, and click **More** > **Deploy** in the **Operation** to go to the certificate deployment details page.

- d. On the displayed page, select **WAF** in the **Deployment Details** area.
- e. Select the domain name you want to deploy the certificate for and click **Deploy** in the **Operation** column.
To deploy the certificates for multiple domain names, select all the target domain names and click **Batch Update** above the domain name list.
- f. In the displayed confirmation dialog box, click **Confirm**.
After the deployment is successful, a message is displayed, indicating that the deployment is successful. Go to the deployment record page to view the result.

Scenario 2: Deploying an SSL Certificate to ELB

To enable secure connections for website traffic distributed through ELB, you need to deploy SSL certificates on ELB. This applies to all websites that need to protect user data privacy and security, prevent **insecure** browser warnings, and protect customer information, such as online transactions and sensitive data.

- 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. This means the certificate that is being used for ELB and you want to update in CCM must have been configured in ELB at the very beginning. Then, you can quickly update it in CCM.
 - 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 Huawei 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.

CAUTION

- 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.
-

- Step
 - a. Log in to the [CCM console](#).
 - b. In the navigation pane on the left, choose **SSL Certificate Manager > SSL Certificates**.
 - c. Locate the row containing the certificate you want to deploy on other cloud product, and click **More > Deploy** in the **Operation** to go to the certificate deployment details page.
 - d. On the displayed page, select **ELB** in the **Deployment Details** area.
 - e. Select the domain name you want to deploy the certificate for and click **Deploy** in the **Operation** column.

To deploy the certificates for multiple domain names, select all the target domain names and click **Batch Update** above the domain name list.
 - f. In the displayed confirmation dialog box, click **Confirm**.

After the deployment is successful, a message is displayed, indicating that the deployment is successful. Go to the deployment record page to view the result.

Scenario 3: Deploying an SSL Certificate to CDN

When traffic passes through intermediate nodes such as CDN and the connection between the client and these nodes needs to be encrypted, you need to deploy the SSL certificate to CDN. This method can protect communication security between users and the CDN and prevent data from being intercepted or tampered during transmission, especially when the website access traffic is heavy or sensitive information needs to be transmitted.

- 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 Huawei 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.
- Step
 - a. Log in to the [CCM console](#).
 - b. In the navigation pane on the left, choose **SSL Certificate Manager > SSL Certificates**.
 - c. Locate the row containing the certificate you want to deploy on other cloud product, and click **More > Deploy** in the **Operation** to go to the certificate deployment details page.

- d. On the displayed page, select **CDN** in the **Deployment Details** area.
- e. Select the domain name you want to deploy the certificate for and click **Deploy** in the **Operation** column.
To deploy the certificates for multiple domain names, select all the target domain names and click **Batch Update** above the domain name list.
- f. In the displayed confirmation dialog box, click **Confirm**.
After the deployment is successful, a message is displayed, indicating that the deployment is successful. Go to the deployment record page to view the result.

Scenario 4: Deploying an SSL Certificate to VOD

To ensure the security of playback data and transmission information, such as playback records and data transmission in live streams, you need to enable HTTPS encryption in VOD. In HTTPS, key user information is encrypted to prevent session IDs or cookies from being captured by attackers, which may cause sensitive information leakage.

- Prerequisites
 - You have subscribed to VOD and configured a website domain name that matches the SSL certificate in VOD.
 - If you have not subscribed to VOD or the domain name you want to use the certificate for has not been added to VOD, deploying the certificate to VOD 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. To use a certificate for a cloud product, download the certificate to your local PC first. Then, upload it to the cloud product and complete deployment.
- Step
 - a. Log in to the [CCM console](#).
 - b. In the navigation pane on the left, choose **SSL Certificate Manager > SSL Certificates**.
 - c. Locate the row containing the certificate you want to deploy on other cloud product, and click **More > Deploy** in the **Operation** to go to the certificate deployment details page.
 - d. On the displayed page, select **VOD** in the **Deployment Details** area.
 - e. Select the domain name you want to deploy the certificate for and click **Deploy** in the **Operation** column.
To deploy the certificates for multiple domain names, select all the target domain names and click **Batch Update** above the domain name list.
 - f. In the displayed confirmation dialog box, click **Confirm**.
After the deployment is successful, a message is displayed, indicating that the deployment is successful. Go to the deployment record page to view the result.

2 Getting Started Through Common Practices

This topic introduces some common practices along with explicit operation guidelines to help you quickly start with Cloud Certificate & Manager (CCM).

Best Practices for SSL Certificate Manager

Best Practice	Description
Resolving a DNS Record on Huawei Cloud or Alibaba Cloud	After an SSL certificate application is submitted to the CA, domain name verification is required. This section walks you through how to verify domain name ownership on Huawei Cloud and Alibaba Cloud.
Enabling HTTPS Encryption for Websites	This section describes the process of purchasing and installing an SSL certificate on a server, helping you convert an HTTP website into an HTTPS-encrypted one with ease.
Deploying SSL Certificates to Huawei Cloud Products	This section walks you through how to use CCM to quickly deploy SSL certificates you obtain through CCM or a third party platform on your Huawei Cloud CDN, WAF, or ELB instances, converting your services from HTTP to HTTPS and improving data access security.
Using FunctionGraph to Automatically Obtain and Update ECS Server Certificates	This section describes how to use FunctionGraph to automatically obtain and update an ECS server certificate. With this method, there is no need to manually update ECS server certificates after certificate renewals.

Best Practices for Private Certificate Management

Best Practice	Description
Best Practices for Private Certificate Management	This section provides guidelines for private certificate lifecycle management and rotation and describes private certificate statuses.
Best Practices for Private CA Management	This section describes how to design the hierarchy of private CAs and how to manage private CAs throughout their lifecycle, including management of certificate revocation lists (CRLs) and rotation of private CAs. This section also describes different states of private CAs.
Example PCA Code	This section describes the example code of private CA management, including creating, deleting, disabling, and enabling a CA. This section also provides example code of private certificate management, including applying for, deleting, exporting, and revoking a certificate.
Building an Internal Identity Authentication System	This section walks you through how to use CCM to establish a CA hierarchy for your organization so that you can issue and manage self-signed private certificates internally.