Cloud Certificate Manager

Billing

Issue	01
Date	2023-08-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

Contents

1 Overview

In this document, you will learn about how CCM certificates are billed, how you can renew subscriptions and manage costs, and what happens if your account goes into arrears.

- **Billing modes**

  CCM provides two billing modes: one-time billing and pay-per-use billing for you to meet your needs. SSL certificates are one-off billing products. You will need to pay a one-time fee based on the certificate type, certificate authority, domain type, domain quantity, and purchased duration. You will be billed based on how many private CAs and private certificates you use. For details about billing modes, see **Billing Modes**.

- **Billing items**

  In CCM, the billing items for SCM include SSL certificates and free certificate expansion packages The billing items of private certificate management consist of the private CA fee and private certificate fee. For details about the billing factors and formulas of each billing item, see **Billing Items**.

  For details about billing examples and how the fee is calculated for each billing item in different billing modes, see **Billing Examples**.

- **Renewing subscriptions**

  An expired SSL certificate cannot protect your service. If you want to continue using the SSL certificate, you need to renew the SSL certificate within a specified period. You can enable auto-renewal for it or manually renew it on the console. For more information about renewal, see **Renewal Overview**.

- **Bills**

  To learn about your expenditures, go to **Billing Center** > **Billing**, and view the transactions and billing details related to CCM. For details, see **Viewing Bills**.

- **Arrears**

  If there is not a sufficient account balance to pay for your bill and there is no other payment method configured, your account will go into arrears. If your account is in arrears, the service cannot work. You need to top up your account in a timely manner. For details, see **About Arrears**.

- **Billing termination**

If you no longer need a cloud service resource, you can unsubscribe from or delete it to stop the billing. For details, see **Billing Termination**.

- **Cost management**

  You can manage costs from cost composition, allocation, analysis, and optimization. For details, see **Cost Management**.

2 Billing Modes

2.1 Overview

CCM provides two billing modes: one-time billing and pay-per-use billing for you to meet your needs.

- One-time billing applies only to SSL certificates. When purchasing an SSL certificate, a one-time fee is charged based on the certificate type, certificate authority, domain type, number of domain names, and required duration you select.
- Pay-per-use billing is a postpaid mode in which you pay for what you use. This mode applies only to private CAs and certificates. Private CAs and certificates are billed by the second and settled by the hour. With the pay-per-use billing mode, you can easily adapt to resource requirement changes, reducing the risk of over-provisioning of resources or lacking capacity. In this mode, there are no upfront commitments required.

  Table 2-1 describes the differences between the billing modes.

Table 2-1 Billing modes

Billing Mode	One-time payment	Pay-per-Use Billing
Payment Method	Prepaid Calculated based on the specifications of the purchased certificate.	Postpaid Billed for what you use.
Billing period	One-time payment based on specifications of purchased certificates.	Billed by the second and settled by the hour.
Billing items	● SSL certificates ● SSL certificate expansion package	● Private certificate ● Private CAs

Billing Mode	One-time payment	Pay-per-Use Billing
Changing billing mode	The billing mode for SSL certificates cannot be changed as SSL certificates are one-time billing products.	Switching to one-time billing is not supported. To terminate the billing, delete the corresponding private CA or private certificate.
Application scenario	This billing mode applies to SSL certificates only.	This billing mode applies to private CAs and certificates only.

2.2 One-time Payment

One-time billing is a prepaid mode in which you pay for SSL certificates before using them. This mode applies only to SSL certificates.

Billing Item Details

The following table lists billing items of SSL certificates.

NOTE

For the final prices of different billing items, see the purchase page.

Table 2-2 SSL certificate billing items

Service	Description
SSL certificates	A certificate can be valid for 1 year, 2 years, or 3 years. **NOTE** The longer the certificate, the more discount you get.
DV (Basic) single-domain free certificate package	Each account has 20 free certificates. If your free certificate quota is used up and you want to continue using some free certificates, you need to purchase an expansion package. Each expansion package includes up to 20 free certificates.

Billing Examples

Assume that you purchased a one-year single-domain OV SSL certificate for one domain name from GeoTrust at 14:25:30 on May 25, 2023, and the certificate was issued at 15:30:30 on May 28, 2023. The price includes:

- Total one-time fee of the certificate = Unit price x 1
- The certificate expires at 15:30:30 on May 28, 2024.

Table 2-3 Billing formulas

Resource Type	Billing Formula
SSL certificates	Unit price of the corresponding certificate specifications x Quantity

2.3 Pay-per-Use Billing

Pay-per-use billing is a postpaid mode in which you pay for what you use. This billing mode requires no upfront or long-term commitments. In CCM, this billing mode is used only for **private CAs and private certificates**. This topic describes the billing rules for private CAs and certificates.

📖 NOTE

A root CA is billed from the moment it is created. Subordinate CAs are not billed until they are activated.

Application Scenarios

Pay-per-use billing is good for short-term, burst, or unpredictable workloads that cannot tolerate any interruption

Billing Items

You are billed for the following resources on a pay-per-use basis.

Table 2-4 Billing items

Billing Item	Description
Private root CA	Root CAs you create are billed on a pay-per-use basis.
Private subordinate CA	Subordinate CAs you create are billed on a pay-per-use basis.
Private certificate	Private certificates you apply for from existing private CAs are billed on a pay-per-use basis.

Table 2-5 Private CA billing details

Private CA Status	Billed or Not	Description
Pending activation	No	A private certificate can be used only after being activated.
Activated	Yes	An activated CA can issue certificates, revoke certificates, and sign CRLs. **NOTICE** How an activated CA works depends on what type of key it owns.
Disabled	Yes	A disabled CA cannot be used to issue certificates, but it can still revoke certificates and sign CRLs. **NOTICE** How an activated CA works depends on what type of key it owns.

Private CA Status	Billed or Not	Description
Pending deletion	● If a private CA in the **Pending deletion** status is finally deleted as scheduled, no additional fee is incurred for the pending deletion period. ● If the deletion is canceled for a private CA in the **Pending deletion** status, the pending period for the private CA will be billed. For example, if you delete a private CA at 00:00 on January 1, 2022 and the private CA is deleted seven days later as scheduled, you will not be billed for the seven days. If you cancel the scheduled deletion at 00:00 on January 4, 2022 and the private CA is not deleted, you will still be billed for the CA for the period from 00:00 on January 1, 2022 to 00:00 on January 4, 2022. **NOTICE** Only **Disabled** or **Expired** private CAs can enter into the **Pending deletion** status when they are deleted. This means when you delete a disabled or expired certificate, it cannot be deleted immediately. It takes at least 7 days for a scheduled deletion to take effect (depending on the delay time you configured).	Only the deletion cancellation is provided.

Private CA Status	Billed or Not	Description
Expired	Yes	An expired private CA is no longer trusted and cannot issue or revoke certificates or sign CRLs, but it still uses the CA quota and can be exported. **CAUTION** If you no longer need a certificate, delete it as soon as possible to prevent unnecessary fees incurred.
Revoked	No	Only subordinate CAs can be revoked. If the CRL function is enabled for their parent CA, the revocation information will be published in the CRL of subordinate CAs. Revoked private CA will no longer be trusted.

3 Billing Items

Billing Description

The billing items of CCM consist of the SSL certificate management fee and private certificate management fee. For details, see **CCM billing items**.

Table 3-1 CCM billing items

Billing Item	Description	Billing Mode	Billing Formula
SSL certificates	Fees are calculated on the certificate type, CA, certificate validity, and how many certificates are purchased.	One-time payment	One-time payment: Unit price of certificates x certificate quantity
DV (Basic) single-domain free certificate package	Each account has 20 free certificates. When the free certificates are used up, you need to purchase a free certificate package. Each package can contain up to 20 certificates.	One-time payment	One-time payment: Unit price of the expansion package x Quantity
Private CA	If this is your first time creating a private CA, you must create a root CA.	Pay-per-use billing	Private CA unit price x Required duration
Private certificate	Only activated CAs can be used to issue private certificates.	Pay-per-use billing	Private certificate unit price x Required duration

4 Billing Examples

Example 1:

Scenarios

A customer purchased an SSL certificate at 9:00:00 on May 30, 2023, and the certificate was issued at 17:00:00 on June10, 2023. The certificate specifications are as follows:

- Certificate type: OV (organization validated)
- Certificate authority: DigiCert
- Domain type: Single domain
- Validity period: 1 year

The total fee = Certificate unit price x 1

The validity period starts when the certificate is issued. In this example, the certificate expires at 17:00:00 June 10, 2024.

5 Renewing Your Subscription

5.1 Overview

Renewal Introduction

An SSL certificate is a one-time payment product. An expired SSL certificate cannot encrypt communications over HTTPS. This will put your service at risk. If you want to continue using an SSL certificate, you need to renew the certificate before it expires.

Only SSL certificates can be renewed. Private CAs and certificates are billed on a pay-per-use basis, so you only need to ensure that your account has a valid payment method configured or your account balance is sufficient.

How to Renew Subscriptions

The following table describes how to renew SSL certificates.

Table 5-1 Renewal methods

Method	Description
Manually Renewing an SSL Certificate	The manual renewal entry is available only for **30 calendar days** before an SSL certificate expires.

Method	Description
Auto-renewing an SSL Certificate	If auto-renewal is enabled for a certificate, the system automatically purchases a new certificate that has the same specifications as 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 new certificate until they validate your domain name ownership and identity.

5.2 Manually Renewing an SSL Certificate

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.
- Manually renewing an SSL certificate is to purchase a new certificate with the exact same configurations as the original one. The configurations include the certificate authority, certificate type, domain type, domain quantity, and primary domain name.
- 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.
- 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.

  For more details, see **Manual Renewal Restrictions**.

NOTICE

- 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.

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**.

Step 4 In the **Operation** column of the certificate you want to renew, click **Renew**.

Step 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.

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 you complete the payment, 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.

----End

5.3 Auto-renewing an SSL Certificate

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.

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 as 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 new 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.

  For restrictions on auto-renewals, see **Auto-Renewal Restrictions**.

NOTICE

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**.

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

6 Bills

You can view bills in the **Billing Center** to learn about the usage and billing details of the resource in a certain period.

Bill Reporting Period

After a one-time charge is paid, a bill is reported to the billing system in real time for settlement.

The usage of pay-per-use resources is reported to the billing system at a fixed interval for settlement. A pay-per-use resource is billed by the hour, day, or month, depending on the resource's usage type. In CCM, the bills for private certificate management are settled by the hour.

You are not charged immediately after a billing record is generated. For example, if a private certificate (which is billed on an hourly basis) is disabled at 08:30, your expenditures for the hour from 08:00 to 09:00 will not likely be billed until about 10:00. On the **Billing Center** > **Billing** > **Transactions and Detailed Bills** > **Transaction Bills** page, **Expenditure Time** indicates the time when a pay-per-use product is used.

Viewing Bills of a Specific Resource

Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, choose **Billing & Costs** > **Bills**.

Step 3 In the navigation tree on the left, choose **Billing** > **Expenditure Details**.

Step 4 In the **Settings** area, click ⚙, select **Resource Type**. Then, select **Cloud Certificate Manager Service (CCM)** in the **Service Type** column or select **Private CA Quantity** in the **Resource Type** column. The system displays the bills of the service.

By default, expenditure details are displayed by usage and the statistical period is a billing cycle. You can also set other statistical dimensions and periods.

----End

7 About Arrears

If there is not a sufficient account balance to pay for your bill and there is no other payment method configured, your account will go into arrears. If your account is in arrears, the service cannot work. You need to top up your account in a timely manner.

Arrears Reason

You have purchased a private CA or certificate, but your account balance cannot cover the fees for them.

Impact of Arrears

- One-time payment

  There is no impact on the SSL certificates you have purchased as you have paid for a one-time fee for them. However, you will not be able to perform other operations that may incur fees, such as auto-renewal.

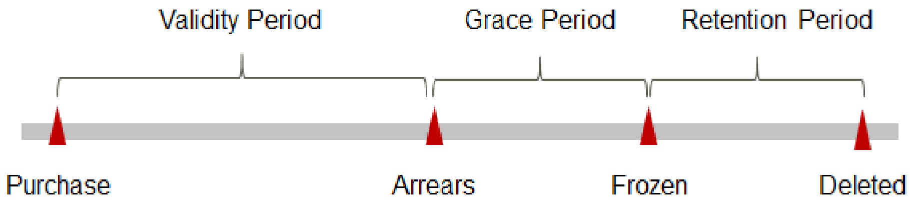
- Pay-per-use billing

  If your account is insufficient to pay your amount due, your account goes into arrears. However, your pay-per-use resources will not be stopped immediately. There will be a grace period. You need to pay the pay-per-use resource fees incurred during the grace period. To view the fees, go to the **Billing Center** > **Overview** page. The system will charge the fees after you top up your account.

  If your account is still in arrears after the grace period ends, the resources enter the retention period and their status turns to **Frozen**. You cannot perform any operations on pay-per-use resources in the retention period.

  If your account is still in arrears after the retention period ends, the created private CAs and private certificates will be deleted and cannot be restored.

Figure 7-1 Lifecycle of a pay-per-use private CA or certificate



NOTE

Huawei Cloud offers a 15-day grace period and a 15-day retention period.

Avoiding and Handling Arrears

You need to top up your account once it is in arrears.

You can delete private CAs and certificates that are no longer used to avoid unexpected expenditures.

Configure the **Balance Alert** function on the **Billing Center** > **Overview** page. When the total amount of the available quota, general cash coupons, and cash coupons is lower than the threshold, the system automatically notifies you by SMS or email.

If your account is in arrears, top up your account in a timely manner.

8 Billing Termination

To prevent resource waste and unnecessary fees, you can stop billing for unused resources.

One-time Payment Resources

SSL certificates are one-time payment resources. You need to pay for them at a time when purchasing them. After an SSL certificate expires, it cannot be trusted anymore.

- The 7-day unconditional refund policy applies to SSL Certificates. So you can unsubscribe an SSL certificate if you no longer need it within 7 days after the purchase.

  However, if a refund application is required, the application must be submitted no later than 7 calendar days (24 x 7 hours) after you place the order.

  For more restrictions on unsubscription, see **Unsubscribing from an SSL Certificate**.
- If you have enabled **auto-renewal** but no longer wish to automatically renew the subscription, disable it before the auto-renewal date (30 days before the certificate expiration date by default) to avoid unexpected expenditures.

Pay-per-Use Resources

In CCM, private CAs and certificates are billed on a pay-per-use basis. To terminate the billing of a private CA or certificate, just delete it. The billing stops upon the deletion. To delete them, go to the CCM console and choose **Private CAs** or **Private Certificates** under **Private Certificate Management**. Then, locate the target CA or certificate and click **Delete** in the **Operation** column.

For more details about private CAs, see **Deleting a Private CA**

For more details about private certificates, see **Deleting a Private Certificate**.

9 Cost Management

As you migrate more of your services to the cloud, managing cloud costs becomes more important. For example, you may be more concerned with cost management when using CCM. The following describes how to manage costs in terms of cost composition, allocation, analysis, and optimization. Optimizing costs cn help you maximize return on investment.

Cost Composition

The costs of using CCM depend on the service edition and resource packages you use. Billing items are different for each edition. For details, see **Billing Items**.

Huawei Cloud **Cost Center** helps you manage resource costs with ease. However, you need to identify, manage, and optimize O&M costs by yourself.

Cost Allocation

A good cost accountability system is the basis of cloud financial management. It ensures that departments, business teams, and owners are accountable for their respective cloud costs. Allocate costs to different teams or projects so that organizations have a clear picture of their respective costs.

Huawei Cloud **Cost Center** provides multiple tools for cost collection and reallocation.

- **Allocate costs by linked account.**

  The enterprise master account can categorize the costs of its member accounts by linked account to manage the accounting of those member accounts. For details, see **Viewing Costs by Linked Account**.

- **Allocate costs by enterprise project.**

  Before allocating costs, enable Enterprise Project Management Service (EPS) and plan your enterprise projects based on your organizational structure or businesses. Select an enterprise project for a newly purchased cloud resource so that the costs of that resource will be allocated to the selected enterprise project. For details, see **Viewing Costs by Enterprise Project**.

Figure 9-1 Enterprise Project

* Enterprise Project: --Select--

Cost Analysis

To accurately control and optimize your costs, you need a clear understanding of what parts of your enterprise incurred different costs. Cost Center visualizes your original costs or amortized costs using various dimensions and display filters for cost analysis so that you can analyze the trends and drivers of your service usage and costs from a variety of perspectives or within different defined scopes.

You can also use **Cost Anomaly Detection** in Cost Center to detect unexpected expenses in a timely manner. In this way, costs can be monitored, analyzed, and traced.

For details, see **Performing Cost Analysis to Explore Costs and Usage** and **Enabling Cost Anomaly Detection to Identify Anomalies**.

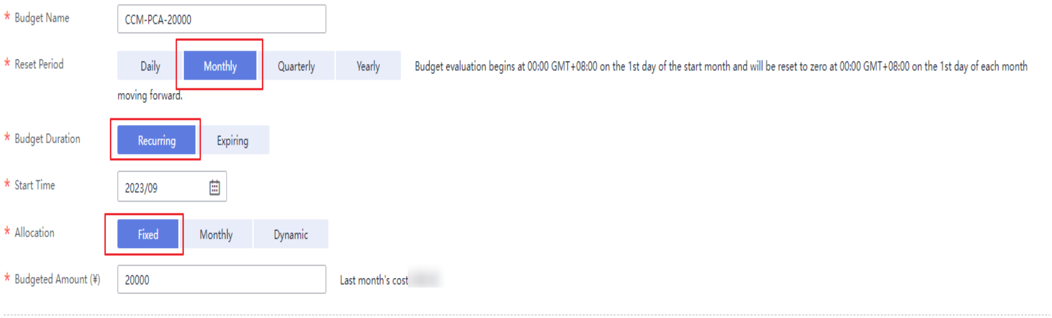
Cost Optimization

- **Cost control**

  You can create different types of budgets on the **Budgets** page of Cost Center to track your costs against the budgeted amount you specified and send alerts to the recipients you configured if the thresholds you defined are reached. You can also create budget reports and we will periodically generate and send to the recipients you configured on a schedule you set.

  For example, an enterprise needs to create a monthly cost budget for PCA in CCM. The monthly budget is ¥20,000. The system should send an alarm when the forecast amount is greater than 80% of the budget amount. Then, the created budget is as follows:

Figure 9-2 Basic budget information



* Budget Name: CCM-PCA-20000

* Reset Period: Daily [✓ Monthly] Quarterly Yearly

Budget evaluation begins at 00:00 GMT+08:00 on the 1st day of the start month and will be reset to zero at 00:00 GMT+08:00 on the 1st day of each month moving forward.

* Budget Duration: [✓ Recurring] Expiring

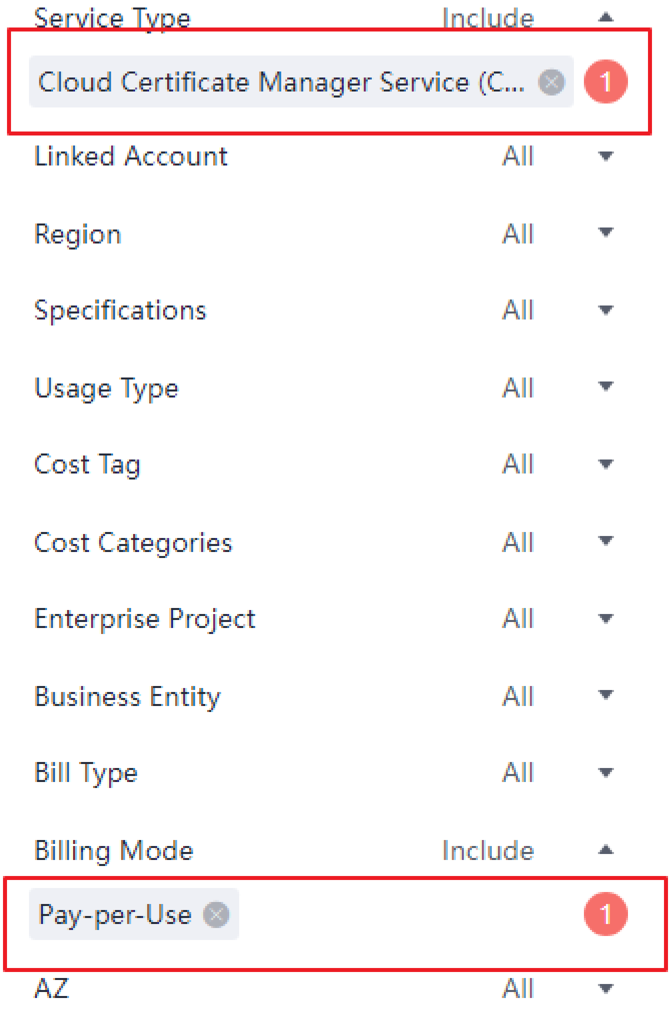
* Start Time: 2023/09

* Allocation: [✓ Fixed] Monthly Dynamic

* Budgeted Amount (¥): 20000

Last month's cost [redacted]

Figure 9-3 Budget Scope



Service Type Include

Cloud Certificate Manager Service (C...

Linked Account All

Region All

Specifications All

Usage Type All

Cost Tag All

Cost Categories All

Enterprise Project All

Business Entity All

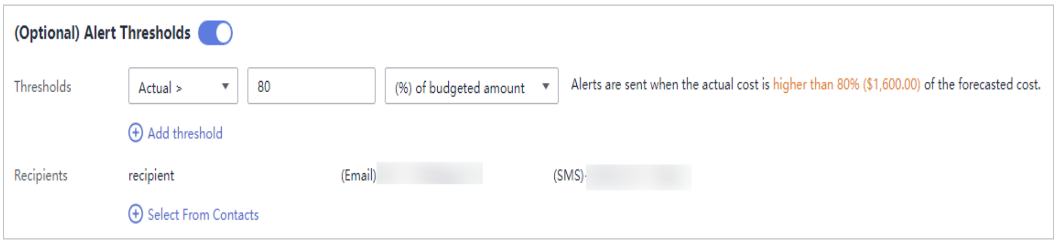
Bill Type All

Billing Mode Include

Pay-per-Use

AZ All

Figure 9-4 Alert Thresholds



(Optional) Alert Thresholds

Thresholds: Actual > | 80 | (%) of budgeted amount — Alerts are sent when the actual cost is higher than 80% ($1,600.00) of the forecasted cost.

Recipients: recipient (Email)[redacted] (SMS)[redacted]

For details, see **Enabling Forecasting and Creating Budgets to Track Cost and Usage**.

- **Resource optimization**

  You can identify resources with high costs based on the results of **Cost Center** and take optimization measures accordingly.

Beyond that, you can detect idle resources to avoid waste. For example, a certificate has been purchased but not applied for, or has been issued but not used.

10 Billing FAQs

10.1 Can I Renew an SSL Certificate?

Yes.

An SSL certificate issued by a CA is valid for one year. An expired SSL certificate cannot enable HTTPS-encrypted communication. Your SSL certificate has to be renewed before it expires.

For details, see **Renewing an SSL Certificate**.

Restrictions

- The manual renewal entry is available only for **30 calendar days** before an SSL certificate expires.
- Only paid SSL certificates that have been purchased in Huawei Cloud SCM and are about to expire can be renewed. Uploaded certificates, free certificates, and single-domain expansion packages cannot be renewed.
- Manually renewing an SSL certificate is to purchase a new certificate with the exact same configurations as the original one. The configurations include the certificate authority, certificate type, domain type, domain quantity, and primary domain name.
- 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

- 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.

10.2 Can I Unsubscribe from an SSL Certificate?

The 7-day unconditional refund policy applies to SCM.

Constraints

- You can request a refund for an SSL certificate order that meets all of the following conditions:
  - You have purchased an SSL certificate on the 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

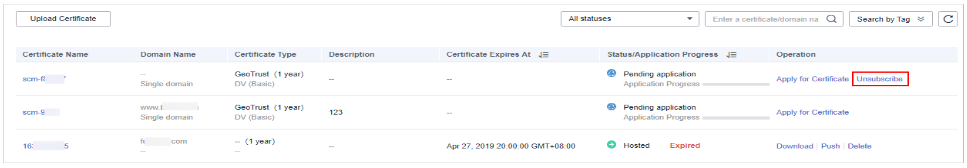
Step 1 Log in to the **management console**.

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 on the left, choose **SSL Certificate Manager**. The **SSL Certificate Manager** page is displayed.

Step 4 In the row containing the desired certificate, click **Unsubscribe** in the **Operation** column. **Figure 10-1** shows an example.

Figure 10-1 Unsubscribing



Certificate Name	Domain Name	Certificate Type	Description	Certificate Expires At	Status/Application Progress	Operation
scm-f[redacted]	-- Single domain	GeoTrust (1 year) DV (Basic)	--	--	Pending application Application Progress	Apply for Certificate Unsubscribe
scm-9[redacted]	www.[redacted] Single domain	GeoTrust (1 year) DV (Basic)	123	--	Pending application Application Progress	Apply for Certificate
16[redacted]5	f[redacted]com --	-- (1 year) --	--	Apr 27, 2019 20:00:00 GMT+08:00	Hosted Expired	Download | Push | Delete

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

10.3 How Is PCA in CCM Billed?

You will be billed based on how many private CAs and private certificates you use. The pricing details are displayed on the purchase page.

How Do I Stop the Billing for a Private CA or Certificate?

Private CAs and private certificates are billed on a pay-per-use basis. A root CA is billed from the moment it is created. Subordinate CAs are not billed until they are activated.

To stop billing for a private CA or certificate, delete it.

⚠ CAUTION

- Disabled private CAs will also be billed.
- If you delete a private CA, it takes a few days for the deletion to take effect. It takes at least 7 days for a scheduled deletion to take effect (depending on the delay time you configured). During the scheduled deletion period, you will be billed in accordance with the following rules:
  - If you have not canceled the scheduled deletion and the private CA is deleted, the private CA is not billed for this period.
  - If you cancel the scheduled deletion but the private CA is not deleted during this period, the private CA is still billed for this period.

  For example, if you delete a private CA at 00:00 on January 1, 2022 and the private CA is deleted seven days later as scheduled, you will not be billed for the seven days. If you cancel the scheduled deletion at 00:00 on January 4, 2022 and the private CA is not deleted, you will still be billed for the CA for the period from 00:00 on January 1, 2022 to 00:00 on January 4, 2022.

A Change History

Released On	Description
2023-08-25	This issue is the first official release.