Cloud Certificate Manager

Private Certificate Authority (PCA) User Guide

Issue 13

Date 2024-05-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Overview of Private Certificate Application

Private Certificate Authority (PCA) is a private CA and certificate management platform. It allows you to set up a complete CA hierarchy and use it to issue and manage private certificates within an organization through simple and visualized operations. It is used to authenticate application identities and encrypt and decrypt data within an organization.

Certificates issued by private CAs are trusted only within your organization but not trusted on the Internet. To use a certificate that is trusted on the Internet, purchase an SSL certificate. For details, see **Purchasing an SSL Certificate**.

For details, see **Figure 1-1** and **Table 1-1**.

Figure 1-1 Private certificate application procedure

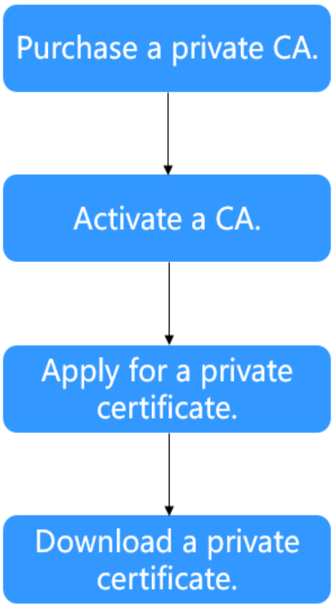

Purchase a private CA.
Activate a CA.
Apply for a private certificate.
Download a private certificate.

Table 1-1 Application procedure

Step	Operation	Description
1	**Purchasing a Private CA**	Purchase a private CA as required.
2	**Activating a Private CA**	A private CA instance must be activated before it is used to issue certificates. You can activate the purchased private CA instance as the **root CA** or **subordinate CA**. A subordinate private CA takes effect and can be used to issue private certificates only after it is activated.
3	**Applying for a Private Certificate**	Apply for a private certificate with the activated private CA.
4	**Downloading a Private Certificate**	After the application is approved, you can download the private certificate and install it on the server.

2 Private CA Management

2.1 Purchasing a Private CA

Huawei Cloud CCM provides you with the PCA service, which helps you set up an internal CA for your organization with low costs and use it to issue certificates with ease.

This topic describes how to purchase a private CA on the CCM console.

Background

- A maximum of 1,000 CAs can be created for each user.
- Private CAs in the pending deletion state are also counted in the private CA quota until the private CAs are deleted.

Prerequisites

The account for creating a private CA has the **PCA FullAccess** permission.

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 In the upper right corner of the private CA list, click **Buy Private CA**. The page is displayed.

Step 4 On the page, set the quota specifications. The following table **Table 2-1** describes the parameters.

Table 2-1 Parameters

Parameter	Description
Billing	Currently, the private CA supports only the **Yearly/Monthly** billing mode.
Service Type	Set the **Type** to **Private CAs**.
Region	PCA is available in all regions. You do not need to select an AZ.
Key Algorithm	The international algorithm RSA and ECC are supported.
Required Duration	Select a duration based on your service requirements. You are advised to select **Auto-renewal** to prevent your services from being affected by service expiration.
Quantity	Enter the number of private CAs to be purchased based on your requirements.
Tags (Optional)	Add a tag to the private CA that you have purchased. For details, see **Creating a Tag**.

Step 5 After setting the parameters, click **Next** in the lower right 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 (CCM) Statement**.

Step 7 Click **Pay** and complete the payment.

NOTICE

The service duration will be calculated after the payment. Please go to the console to activate the CA as soon as possible after the payment.

----End

Follow-up Operations

After purchasing a private CA, you need to activate the CA before using it. For details about how to activate a private CA, see **Activating a Private CA**.

2.2 Activating a Private CA

To use private CAs, you need to activate it first. Only activated private CAs can issue private certificates.

This topic describes how to activate a CA. You can activate a private CA instance and use it as root CA or a subordinate CA. If you activate a CA instance for the first time, you need to activate it as the root CA.

Prerequisites

- You have purchased a private CA instance. For details, see **Buying a Private CA**.
- The private CA is in the **Pending activation** state.

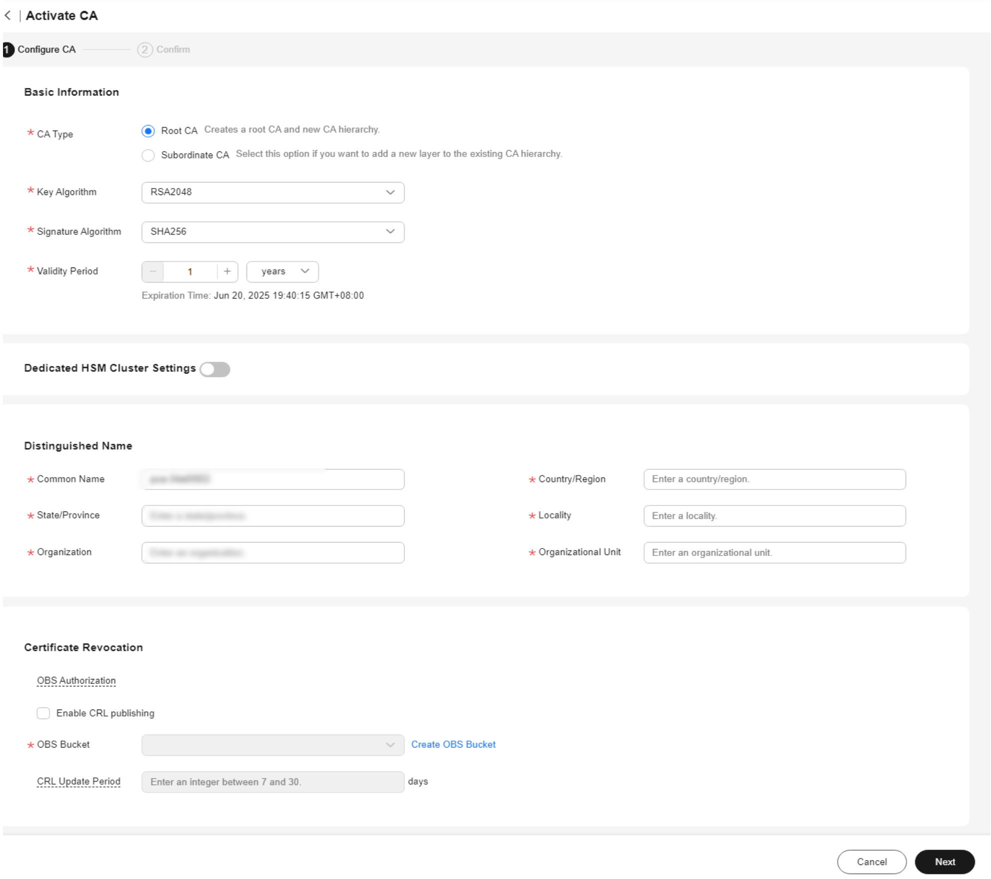
Activating a Root CA.

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificates**.

Step 3 Locate the row of the target CA and click **Activate** in the **Operation** column. On the **Activate CA** page, configure the required parameters.

Figure 2-1 CA settings



< | Activate CA

1 Configure CA — 2 Confirm

Basic Information

* CA Type: ● Root CA Creates a root CA and new CA hierarchy.
○ Subordinate CA Select this option if you want to add a new layer to the existing CA hierarchy.

* Key Algorithm: RSA2048

* Signature Algorithm: SHA256

* Validity Period: 1 years

Expiration Time: Jun 20, 2025 19:40:15 GMT+08:00

Dedicated HSM Cluster Settings

Distinguished Name

* Common Name: [redacted]

* Country/Region: Enter a country/region.

* State/Province: [redacted]

* Locality: Enter a locality.

* Organization: [redacted]

* Organizational Unit: Enter an organizational unit.

Certificate Revocation

OBS Authorization

□ Enable CRL publishing

* OBS Bucket:

CRL Update Period: Enter an integer between 7 and 30. days

1. **CA Type**: Select **Root CA**.

   Root CA: Select this option if you want to create a CA hierarchy.

2. Configure the following parameters.

Table 2-2 Parameters for activating a root CA

Parameter		Description
Basic Information	Key Algorithm	Select a key algorithm from the drop-down list. – RSA2048 – RSA3072 – RSA4096 – EC256 – EC384
	Signature Algorithm	You can select any of the following hash algorithms: – SHA256 – SHA384 – SHA512 – SHA256_PSS – SHA384_PSS – SHA512_PSS
	Validity Period	The validity period of the private CA. Maximum validity period: 30 years.
Distinguished Name (DN)	Common Name	CA name you specify. -
	Country/Region	The country or region where your organization belongs. Enter the two-letter code of the country or region. For example, enter **CN** for China. CN
	State/Province	The name of the province or state where your organization is located. ShenZhen
	Locality	The name of the city where your organization is located. GuangZhou
	Organization	The legal name of your company. -
	Organizational Unit	The department of your company that the applicant belongs to. Cloud Dept.

Parameter		Description
(Optional) Certificate Revocation	OBS Authorization	Whether to authorize PCA to access your OBS bucket and upload the CRL file. If you want to authorize, click **Authorize Now** and complete the authorization as prompted. If you want to cancel the authorization, go to the IAM console to delete the PCAAccessPrivateOBS agency from the agency list. Once you complete the authorization, it will not be required again in the subsequent operations.
	Enable CRL publishing	Whether to enable CRL publishing.
	OBS Bucket	Select an OBS bucket you already have or click **Create OBS Bucket** to create one.
	CRL Update Period	How often the CRL is updated. PCA will generate a new CRL at the specified time. You can set the period to an integer between 7 and 30. If you do not specify a value, it is set to 7 days by default.

Step 4 Check the information and click **Next**.

Step 5 On the confirmation page, check the parameter settings again. Make sure all parameters are set correctly and click **Confirm & Activate**.

----End

Activating a Subordinate CA through an Existing CA

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificates**.

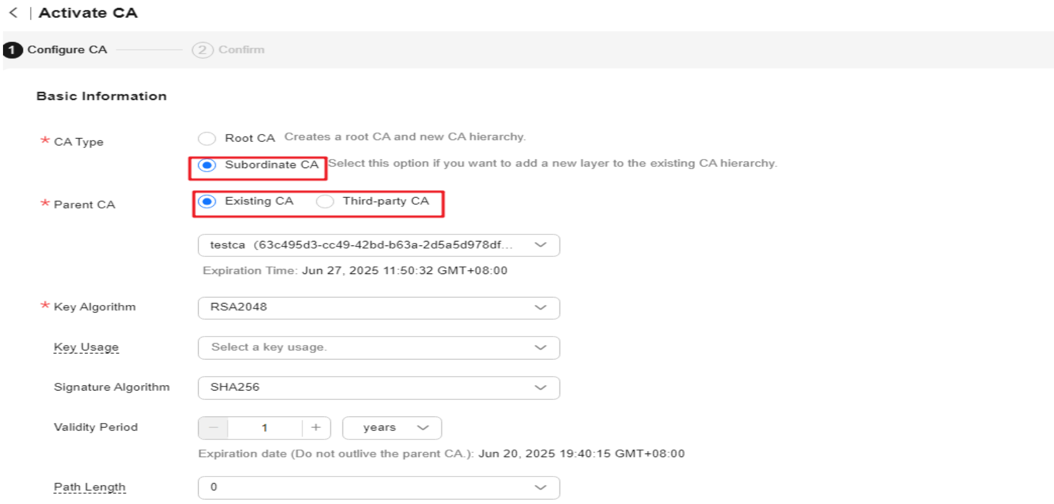
Step 3 Locate the row of the subordinate CA and click **Activate** in the **Operation** column. On the **Install CA Certificate and Activate CA** page, configure the required parameters.

1. To activate a subordinate CA, set the **CA Type** to **Subordinate CA**.

   Subordinate CA: Select this option if you want to add a layer to the existing CA hierarchy.

2. To activate a subordinate CA, you need to specify its parent CA.

Figure 2-2 Parent CA



< | Activate CA

1 Configure CA — 2 Confirm

Basic Information

* CA Type ○ Root CA Creates a root CA and new CA hierarchy.
● Subordinate CA Select this option if you want to add a new layer to the existing CA hierarchy.

* Parent CA ● Existing CA ○ Third-party CA

testca (63c495d3-cc49-42bd-b63a-2d5a5d978df...
Expiration Time: Jun 27, 2025 11:50:32 GMT+08:00

* Key Algorithm RSA2048

Key Usage Select a key usage.

Signature Algorithm SHA256

Validity Period 1 years
Expiration date (Do not outlive the parent CA.): Jun 20, 2025 19:40:15 GMT+08:00

Path Length 0

– Select **Existing CA**, select a CA you have created from the drop-down list box, and set the following parameters.

Parameter		Description
Basic Information	Key Algorithm	Select a key algorithm from the drop-down list. ■ RSA2048 ■ RSA3072 ■ RSA4096 ■ EC256 ■ EC384
	(Optional) Key Usage	Select a key usage. ■ digitalSignature ■ nonRepudiation ■ keyEncipherment ■ dataEncipherment ■ keyAgreement ■ keyCertSign ■ cRLSign ■ encipherOnly ■ decipherOnly

Parameter		Description
	Signature Algorithm	You can select any of the following hash algorithms: ▪ SHA256 ▪ SHA384 ▪ SHA512 ▪ SHA256_PSS ▪ SHA384_PSS ▪ SHA512_PSS
	Validity Period	The validity period of the private CA. Maximum validity period: 20 years.
	Path Length	The path length of the subordinate CA. The path length controls how many layers of subordinate CAs the current subordinate CA can issue. (The last layer of the certificate chain is a private certificate). **NOTE** A certificate chain is made up of root CAs, subordinate CAs, and private certificates in a fixed sequence to validate the trust of a certificate at a lower layer.
Distinguished Name (DN)	Common Name	CA name you specify. -
	Country/Region	The country or region where your organization belongs. Enter the two-letter code of the country or region. For example, enter **CN** for China. CN
	State/Province	The name of the province or state where your organization is located. ShenZhen
	Locality	The name of the city where your organization is located. GuangZhou
	Organization	The legal name of your company. -
	Organizational Unit	The department of your company that the applicant belongs to. Cloud Dept.

Parameter		Description
(Optional) Certificate Revocation	OBS Authorization	Whether to authorize PCA to access your OBS bucket and upload the CRL file. If you want to authorize, click **Authorize Now** and complete the authorization as prompted. If you want to cancel the authorization, go to the IAM console to delete the PCAAccessPrivateOBS agency from the agency list. Once you complete the authorization, it will not be required again in the subsequent operations.
	Enable CRL publishing	Whether to enable CRL publishing.
	OBS Bucket	Select an OBS bucket you already have or click **Create OBS Bucket** to create an OBS bucket.
	CRL Update Period	How often the CRL is updated. PCA will generate a new CRL at the specified time. You can set the period to an integer between 7 and 30. If you do not specify a value, it is set to 7 days by default.

Step 4 Check the information and click **Next**.

Step 5 On the confirmation page, check the parameter settings again. Make sure all parameters are set correctly and click **Confirm & Activate**.

----End

Activating a Subordinate CA from a Third-Party CA

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificates**.

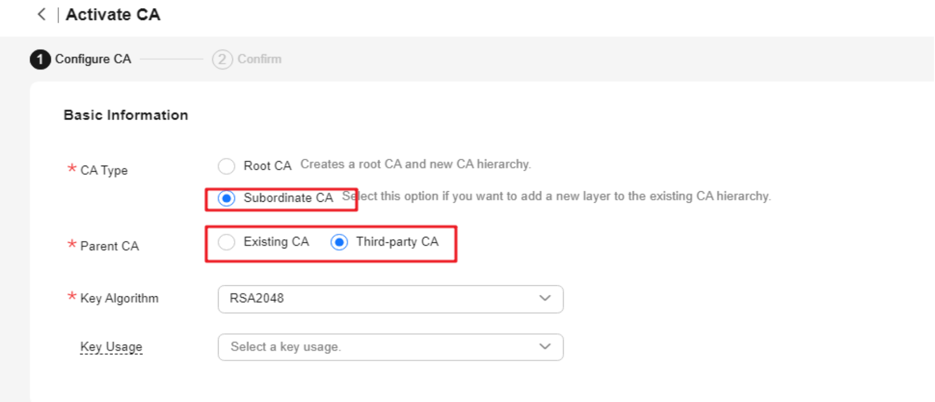
Step 3 Locate the row of the subordinate CA and click **Activate** in the **Operation** column. On the **Activate CA** page, configure the required parameters.

1. To activate a subordinate CA, set the **CA Type** to **Subordinate CA**.

   Subordinate CA: Select this option if you want to add a layer to the existing CA hierarchy.

2. To activate a subordinate CA, you need to specify its parent CA.

Figure 2-3 Parent CA



< | Activate CA

1 Configure CA — 2 Confirm

Basic Information

* CA Type ○ Root CA Creates a root CA and new CA hierarchy.

● Subordinate CA Select this option if you want to add a new layer to the existing CA hierarchy.

* Parent CA ○ Existing CA ● Third-party CA

* Key Algorithm RSA2048

Key Usage Select a key usage.

– Select **Third-party CA** and set the following parameters.

Parameter		Description
Basic Information	Key Algorithm	Select a key algorithm from the drop-down list. ■ RSA2048 ■ RSA3072 ■ RSA4096 ■ EC256 ■ EC384
	(Optional) Key Usage	Select a key usage. ■ digitalSignature ■ nonRepudiation ■ keyEncipherment ■ dataEncipherment ■ keyAgreement ■ keyCertSign ■ cRLSign ■ encipherOnly ■ decipherOnly

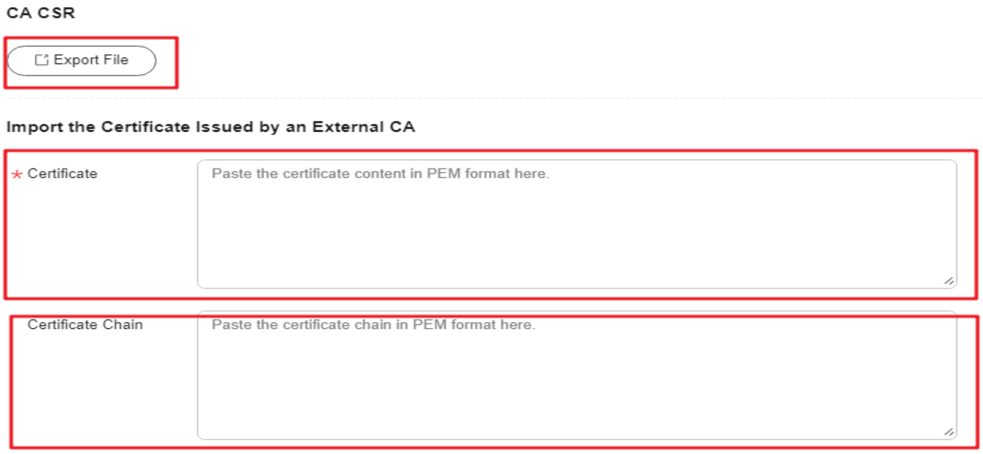
Parameter		Description
	Signature Algorithm	You can select any of the following hash algorithms: ▪ SHA256 ▪ SHA384 ▪ SHA512 ▪ SHA256_PSS ▪ SHA384_PSS ▪ SHA512_PSS
	Validity Period	The validity period of the private CA. Maximum validity period: 20 years.
	Path Length	The path length of the subordinate CA. The path length controls how many layers of subordinate CAs the current subordinate CA can issue. (The last layer of the certificate chain is a private certificate). **NOTE** A certificate chain is made up of root CAs, subordinate CAs, and private certificates in a fixed sequence to validate the trust of a certificate at a lower layer.
Distinguished Name (DN)	Common Name	CA name you specify. -
	Country/Region	The country or region where your organization belongs. Enter the two-letter code of the country or region. For example, enter **CN** for China. CN
	State/Province	The name of the province or state where your organization is located. ShenZhen
	Locality	The name of the city where your organization is located. GuangZhou
	Organization	The legal name of your company. -
	Organizational Unit	The department of your company that the applicant belongs to. Cloud Dept.

Parameter		Description
(Optional) Certificate Revocation	OBS Authorization	Whether to authorize PCA to access your OBS bucket and upload the CRL file. If you want to authorize, click **Authorize Now** and complete the authorization as prompted. If you want to cancel the authorization, go to the IAM console to delete the agency from the agency list. Once you complete the authorization, it will not be required again in the subsequent operations.
	Enable CRL publishing	Whether to enable CRL publishing.
	OBS Bucket	Select an OBS bucket you already have or click **Create OBS Bucket** to create an OBS bucket.
	CRL Update Period	How often the CRL is updated. PCA will generate a new CRL at the specified time. You can set the period to an integer between 7 and 30. If you do not specify a value, it is set to 7 days by default.

Step 4 Check the information and click **Save and Next**.

Step 5 Check the information again and complete required parameters.

Figure 2-4 Third-Party CA



CA CSR

Export File

Import the Certificate Issued by an External CA

* Certificate: Paste the certificate content in PEM format here.

Certificate Chain: Paste the certificate chain in PEM format here.

1. Export the CSR.

   On the **CA CSR** pane, click **Export File**.

   The PEM CSR is exported to a file and is signed by a parent CA.

2. Use an external CA to issue a certificate.

   Use your private CA to issue a certificate for the subordinate private CA you want to activate.

3. Import the certificate.

   Import the certificate and certificate chain in the **Import the Certificate Issued by an External CA** pane.

Table 2-3 Parameter descriptions

Parameter	Description
Certificate	Open the PEM file in the certificate to be uploaded as a text file with the extension **.pem** and copy the certificate content to this text box.
Certificate Chain	Open the PEM file in the certificate to be uploaded as a text file with the extension **.pem** and copy the certificate chain to this text box.

Step 6 Check the settings and click **Confirm & Activate**. The subordinate CA is activated.

----End

Follow-up Operations

You can use an activated subordinate CA to issue private certificates. For details, see **Applying for a Private Certificate**.

2.3 Viewing Private CA Details

This topic describes how to view the private CA information, including **Common Name**, **Organizational Unit**, **Type**, and **Status**.

Prerequisites

A private CA has been purchased. For details, see **Buying a Private CA**.

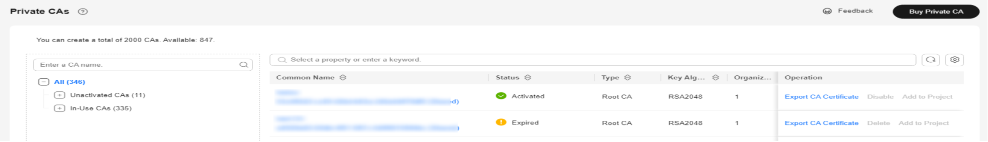
Procedure

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificates**.

Step 3 View private CA information in the private CA list. **Table 2-4** describes the parameters.

Figure 2-5 Private CA list



You can create a total of 2000 CAs. Available: 847.

Common Name	Status	Type	Key Alg...	Organiz...	Operation
[illegible]	Activated	Root CA	RSA2048	1	Export CA Certificate Disable Add to Project
[illegible]	Expired	Root CA	RSA2048	1	Export CA Certificate Delete Add to Project

NOTE

- Select a CA type or status from the type or status search box. CAs of the selected type or status will be displayed in the list.
- Enter a name of a CA in the search box in the upper right corner and click 🔍 or press **Enter** to search for a specified CA.

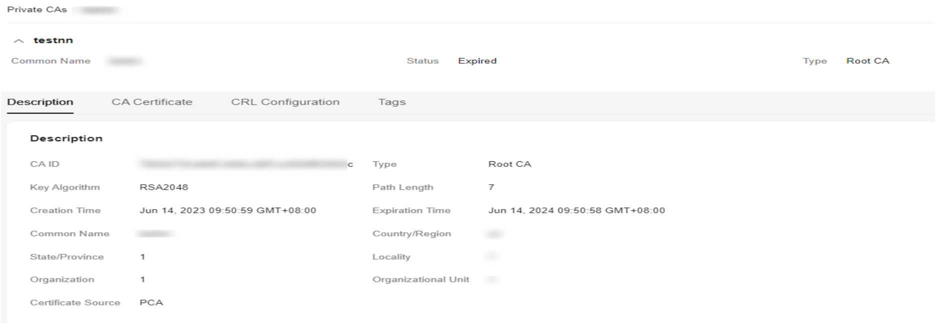
Table 2-4 CA parameter description

Parameter	Description
Common Name	Indicates the user-defined CA name.
Type	Indicates the private CA type. The value can be: ● **Root CA**: The private CA is a root CA and can be used to issue subordinate CAs. ● **Subordinate CA**: The private CA is a subordinate CA.
Organizational Unit	Indicates the name of the organizational unit to which the private CA belongs.
Issued By	Indicates the name of the CA that issues the private CA.
Creation Time	Indicates the time when a private CA is created.
Expiration Time	Indicates the time when a private CA expires.
Status	Indicates the private CA status. The value can be: ● **Pending activation**: The private CA is to be activated. ● **Activated**: The private CA is activated. ● **Disabled**: The private CA is disabled. ● **Pending deletion**: The private CA is to be deleted. ● **Expired**: The private CA is expired.
Operation	You can activate, enable, or disable a CA.

Step 4 Click the common name of a private CA to view its details.

You can click **Add Tag** on the CA details page to identify the CA. TMS's predefined tag function is recommended for adding the same tag to different cloud resources.

Figure 2-6 Private CA details



Common Name [redacted] Status Expired Type Root CA

Description

CA ID	[redacted]c	Type	Root CA
Key Algorithm	RSA2048	Path Length	7
Creation Time	Jun 14, 2023 09:50:59 GMT+08:00	Expiration Time	Jun 14, 2024 09:50:58 GMT+08:00
Common Name	[redacted]	Country/Region	[redacted]
State/Province	1	Locality	[redacted]
Organization	1	Organizational Unit	[redacted]
Certificate Source	PCA		

----End

2.4 Configuring a CRL

If you want to use PCA to publish the certificate revocation list (CRL) for a private CA, you can enable CRL configuration.

This topic walks you through how to enable or disable CRL configuration.

Prerequisites

The private CA for which you want to configure a CRL is in the **Activated** or **Disabled** state.

Enabling CRL Configuration

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 Click the name of a private CA to go to its details page.

Step 4 On the private CA details page, click the **CRL Configuration** tab and configure certificate revocation by referring to **Table 2-5**.

Figure 2-7 CRL Configuration

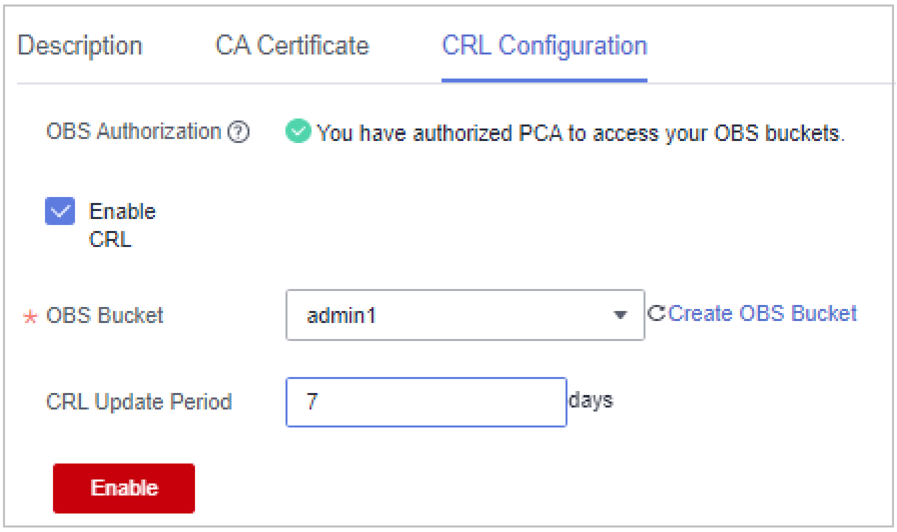


Table 2-5 Certificate revocation parameters

Parameter	Description
OBS Authorization	Whether to authorize PCA to access your OBS bucket and upload the CRL file. If you want to authorize, click **Authorize Now** and complete the authorization as prompted. If you want to cancel the authorization, go to the IAM console to delete the PCAAccessPrivateOBS agency from the agency list. After the permission has been granted, follow-up operations do not require the permission to be granted again.
Enable CRL publishing	Indicates whether to enable CRL publishing.
OBS Bucket	Select an existing OBS bucket or click **Create OBS Bucket** to create an OBS bucket.
CRL Update Period	Indicates the CRL update period. PCA will generate a new CRL at the specified time. You can set the period to an integer between 7 and 30. If you do not specify a value, it is set to 7 days by default.

Step 5 Click **Enable** to enable the CRL. If the system displays a message indicating that the CRL configuration is enabled, the CRL configuration has been enabled.

----End

Disabling CRL Configuration

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 Click the name of a private CA to go to its details page.

Step 4 On the private CA details page, click the **CRL Configuration** tab and click **Disable**. If the system displays a message indicating that the CRL configuration is disabled, the CRL configuration has been disabled.

----End

2.5 Exporting a Private CA Certificate

After a private CA is created and activated, you can export the private CA certificate.

If your web services are accessible through browsers, add the root certificate to your browser trust list and install the private certificate issued by the root CA on your web server to implement HTTPS communications between the client and the server.

If your web services are accessible through a client like Java, manually install the root certificate on the client to ensure that the client can validate the encrypted information on the server.

This topic walks you through how to export a private CA certificate.

Prerequisites

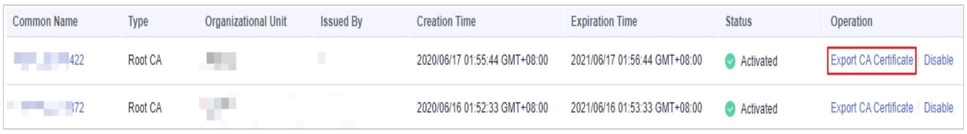
The private CA for which the certificate is to be exported is in the **Activated** state.

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 Locate the row of the desired private CA and click **Export CA Certificate** in the **Operation** column.



Common Name	Type	Organizational Unit	Issued By	Creation Time	Expiration Time	Status	Operation
[redacted]422	Root CA	[redacted]	[redacted]	2020/06/17 01:55:44 GMT+08:00	2021/06/17 01:56:44 GMT+08:00	✓ Activated	Export CA Certificate | Disable
[redacted]72	Root CA	[redacted]		2020/06/16 01:52:33 GMT+08:00	2021/06/16 01:53:33 GMT+08:00	✓ Activated	Export CA Certificate | Disable

Step 4 In the displayed dialog box, click **OK**.

When you click **OK**, PCA will use the download tool provided by the browser to download the private CA certificate to the specified local directory.

Now, you will obtain a private CA certificate file named ***root CA name_certificate*.pem**.

----End

2.6 Disabling a Private CA

If you no longer need a private CA to issue certificates, you can disable the private CA.

If a private CA is disabled, it cannot be used to issue any private certificates. If you want to use this private CA to issue certificates again, it must be enabled first. For details, see .

This topic describes how to disable a private CA.

⚠ CAUTION

Private CAs will also remain billed while they are disabled.

Prerequisites

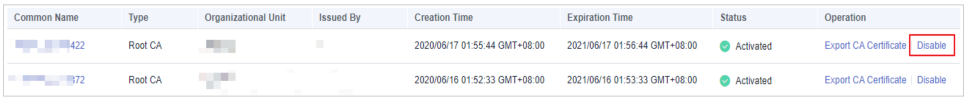
The private CA to be disabled is in the **Activated** or **Expired** state.

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

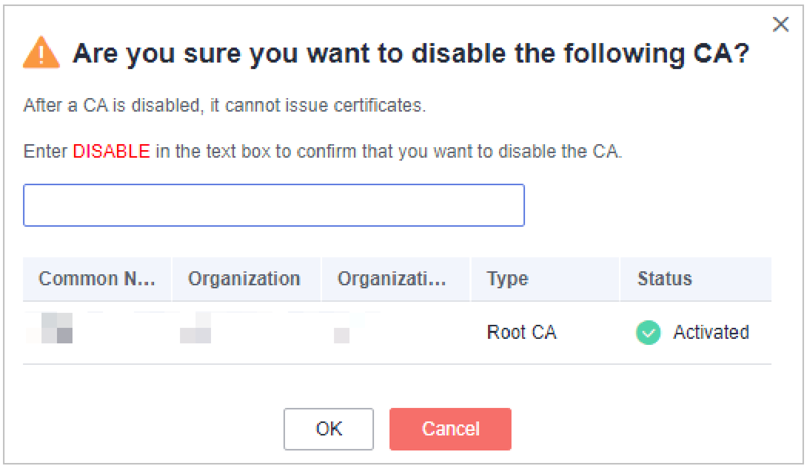
Step 3 Locate the row of the desired private CA and click **Disable** in the **Operation** column.



Common Name	Type	Organizational Unit	Issued By	Creation Time	Expiration Time	Status	Operation
[redacted]422	Root CA	[redacted]	[redacted]	2020/06/17 01:55:44 GMT+08:00	2021/06/17 01:56:44 GMT+08:00	● Activated	Export CA Certificate | Disable
[redacted]72	Root CA	[redacted]		2020/06/16 01:52:33 GMT+08:00	2021/06/16 01:53:33 GMT+08:00	● Activated	Export CA Certificate | Disable

Step 4 In the displayed dialog box, enter **DISABLE** and click **OK**.

Figure 2-8 Disable CA



Are you sure you want to disable the following CA?

After a CA is disabled, it cannot issue certificates.

Enter DISABLE in the text box to confirm that you want to disable the CA.

Common N...	Organization	Organizati...	Type	Status
[redacted]	[redacted]	[redacted]	Root CA	✓ Activated

When "CA xxx disabled successfully." is displayed in the upper right corner of the page, and the private CA status changes to **Disabled**, the private CA is disabled successfully.

----End

2.7 Enabling a Private CA

If you need to use a disabled private CA to issue certificates, you can restore the certificate to the activated state.

The following walks you through how to enable a private CA so that you can quickly restore a disabled private CA to the activated or expired state.

Prerequisites

The private CA to be enabled is in the **Disabled** state. For details about how to disable a private CA, see **Disabling a Private CA**.

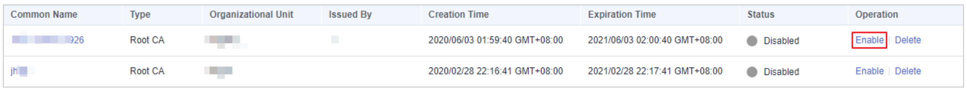
Procedure

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 Locate the row of the desired private CA and click **Enable** in the **Operation** column.

Figure 2-9 Enabling a private CA



Common Name	Type	Organizational Unit	Issued By	Creation Time	Expiration Time	Status	Operation
[redacted]26	Root CA	[redacted]	[redacted]	2020/06/03 01:59:40 GMT+08:00	2021/06/03 02:00:40 GMT+08:00	● Disabled	Enable | Delete
jh[redacted]	Root CA	[redacted]		2020/02/28 22:16:41 GMT+08:00	2021/02/28 22:17:41 GMT+08:00	● Disabled	Enable | Delete

When "CA xxx enabled successfully." is displayed in the upper right corner of the page, and the private CA status changes to **Activated**, the private CA is enabled successfully.

----End

2.8 Deleting a Private CA

Before deleting a private CA, ensure that it is not in use and will not be used.

If deletion is scheduled for a private CA in the **Disabled** or **Expired** state, the deletion will take effect after a waiting period of 7 to 30 days. If deletion is scheduled for a private CA in the **Pending activation** state, the deletion will take effect immediately. Before the specified deletion date, you can cancel the deletion if you want to use the private CA again. If the specified deletion period expires, the private CA will be permanently deleted. Exercise caution when performing this operation.

⚠ CAUTION

- Private CAs will also remain billed while they are disabled.
- 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.

Prerequisites

The private CA to be deleted is in the **Disabled** or **Pending activation** state.

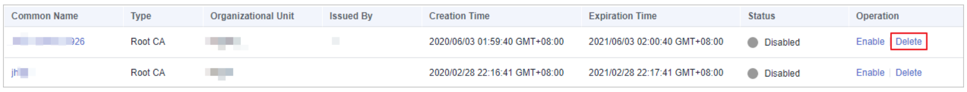
Procedure

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 Locate the row of the private CA to be deleted and click **Delete** in the **Operation** column.

Figure 2-10 Deleting a private CA



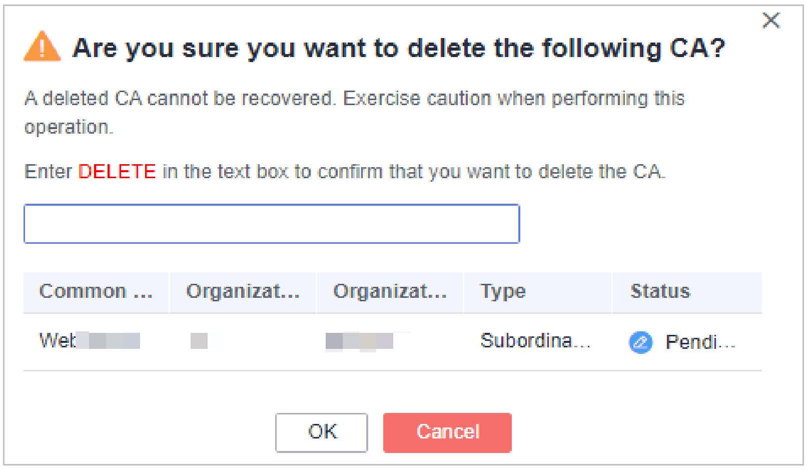
Common Name	Type	Organizational Unit	Issued By	Creation Time	Expiration Time	Status	Operation
[redacted]	Root CA	[redacted]	[redacted]	2020/06/03 01:59:40 GMT+08:00	2021/06/03 02:00:40 GMT+08:00	● Disabled	Enable Delete
[redacted]	Root CA	[redacted]		2020/02/28 22:16:41 GMT+08:00	2021/02/28 22:17:41 GMT+08:00	● Disabled	Enable | Delete

Step 4 The operations vary according to the private CA status.

- Private CA in the **Pending activation** state

  In the displayed dialog box, enter **DELETE** in the text box.

  Figure 2-11 Deleting a private CA in the **Pending activation** state

  Are you sure you want to delete the following CA?

  A deleted CA cannot be recovered. Exercise caution when performing this operation.

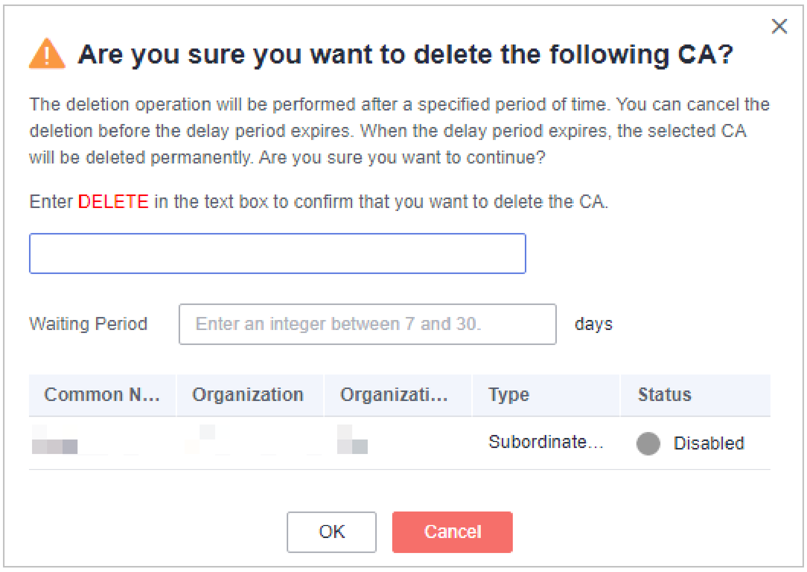
  Enter DELETE in the text box to confirm that you want to delete the CA.

Common ...	Organizat...	Organizat...	Type	Status
[redacted]	[redacted]	[redacted]	Subordina...	Pendi...

- Private CA in the **Disabled** or **Expired** state

  In the dialog box that is displayed, enter **DELETE** in the text box and configure the waiting period.

  Figure 2-12 Configuring the waiting period

  Are you sure you want to delete the following CA?

  The deletion operation will be performed after a specified period of time. You can cancel the deletion before the delay period expires. When the delay period expires, the selected CA will be deleted permanently. Are you sure you want to continue?

  Enter DELETE in the text box to confirm that you want to delete the CA.

  Waiting Period: Enter an integer between 7 and 30. days

Common N...	Organization	Organizati...	Type	Status
[redacted]	[redacted]	[redacted]	Subordinate...	● Disabled

Step 5 Click **OK**.

- Private CA in the **Pending activation** state: If message "CA xxx deleted successfully." is displayed in the upper right corner of the page, the private CA is deleted successfully.

- Private CA in the **Disabled** or **Expired** state: If the private CA status changes to **Pending deletion**, the private CA will be deleted after the waiting period expires.

----End

2.9 Canceling the Deletion of a Private CA

This topic describes how to cancel the scheduled deletion of one or more private CAs prior to the real deletion. After the cancellation, the private CA is in the **Disabled** state.

Prerequisites

The private CA for which you want to cancel the scheduled deletion is in **Pending deletion** status.

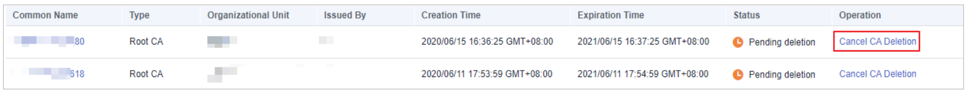
Procedure

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 Locate the row of the desired private CA and click **Cancel CA Deletion** in the **Operation** column.

Figure 2-13 Canceling the deletion of a private CA



Common Name	Type	Organizational Unit	Issued By	Creation Time	Expiration Time	Status	Operation
[redacted]80	Root CA	[redacted]	[redacted]	2020/06/15 16:36:25 GMT+08:00	2021/06/15 16:37:25 GMT+08:00	● Pending deletion	Cancel CA Deletion
[redacted]618	Root CA	[redacted]		2020/06/11 17:53:59 GMT+08:00	2021/06/11 17:54:59 GMT+08:00	● Pending deletion	Cancel CA Deletion

Step 4 In the displayed dialog box, click **OK**.

If message "Deletion of CA xxx cancelled successfully." is displayed in the upper right corner of the page and the private CA status changes to **Disabled**, the deletion of the private CA is cancelled successfully.

After the deletion is canceled, if you want to use the private CA to issue certificates, you need to enable the private CA. For details, see **Enabling a Private CA**.

----End

3 Private Certificate Management

3.1 Applying for a Private Certificate

After you create and activate a private CA, you can apply for private certificates from the private CA and use them for identity authentication, data encryption, and data decryption of internal applications.

This topic walks you through how to apply for a private certificate. You can apply for a maximum of 100,000 certificates.

Prerequisites

You have created and activated a private CA. For details, see Creating a Private CA and Activating a Private CA.

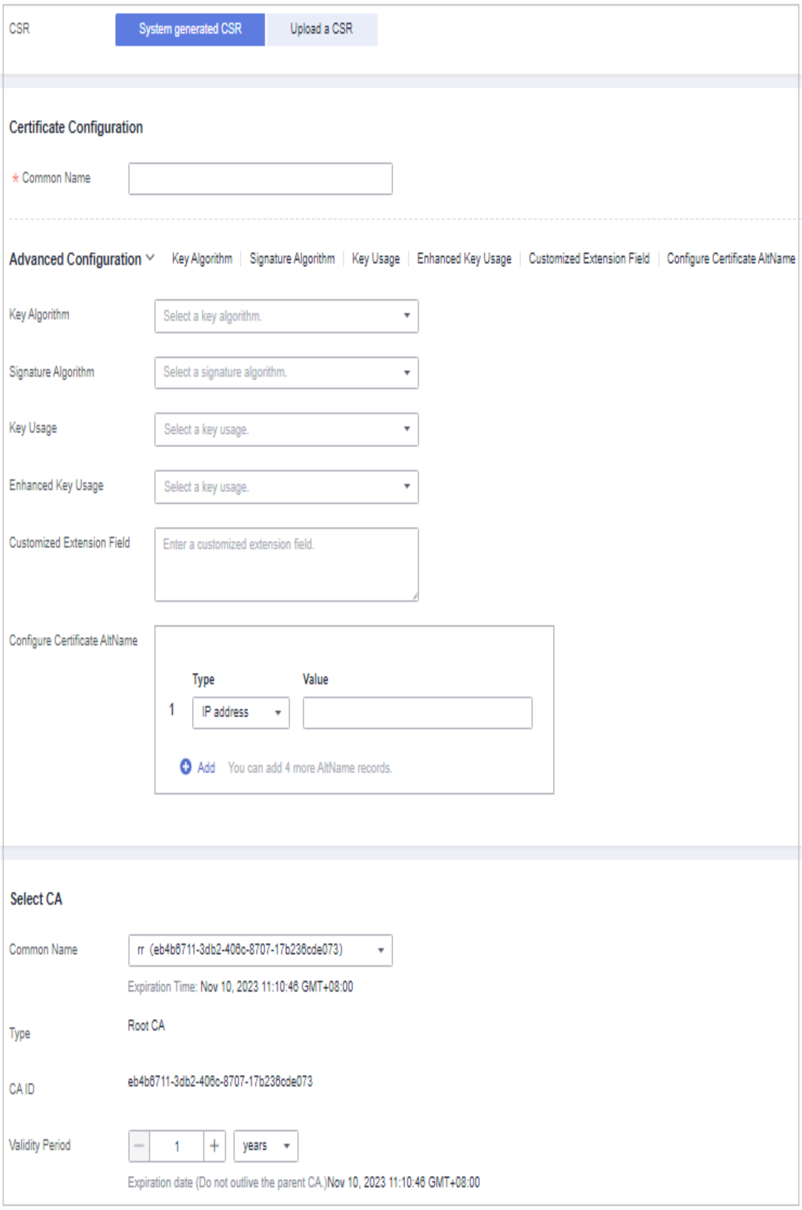
Procedure

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 In the upper right corner of the private certificate list, click **Apply for Certificate**.

Figure 3-1 System generated CSR


CSR
System generated CSR
Upload a CSR
Certificate Configuration
* Common Name
Advanced Configuration
Key Algorithm | Signature Algorithm | Key Usage | Enhanced Key Usage | Customized Extension Field | Configure Certificate AltName
Key Algorithm
Select a key algorithm.
Signature Algorithm
Select a signature algorithm.
Key Usage
Select a key usage.
Enhanced Key Usage
Select a key usage.
Customized Extension Field
Enter a customized extension field.
Configure Certificate AltName
Type
Value
Add
You can add 4 more AltName records.
Select CA
Validity Period

Type: 1 IP address

Common Name: rr (eb4b6711-3db2-406c-8707-17b236cde073)

Expiration Time: Nov 10, 2023 11:10:46 GMT+08:00

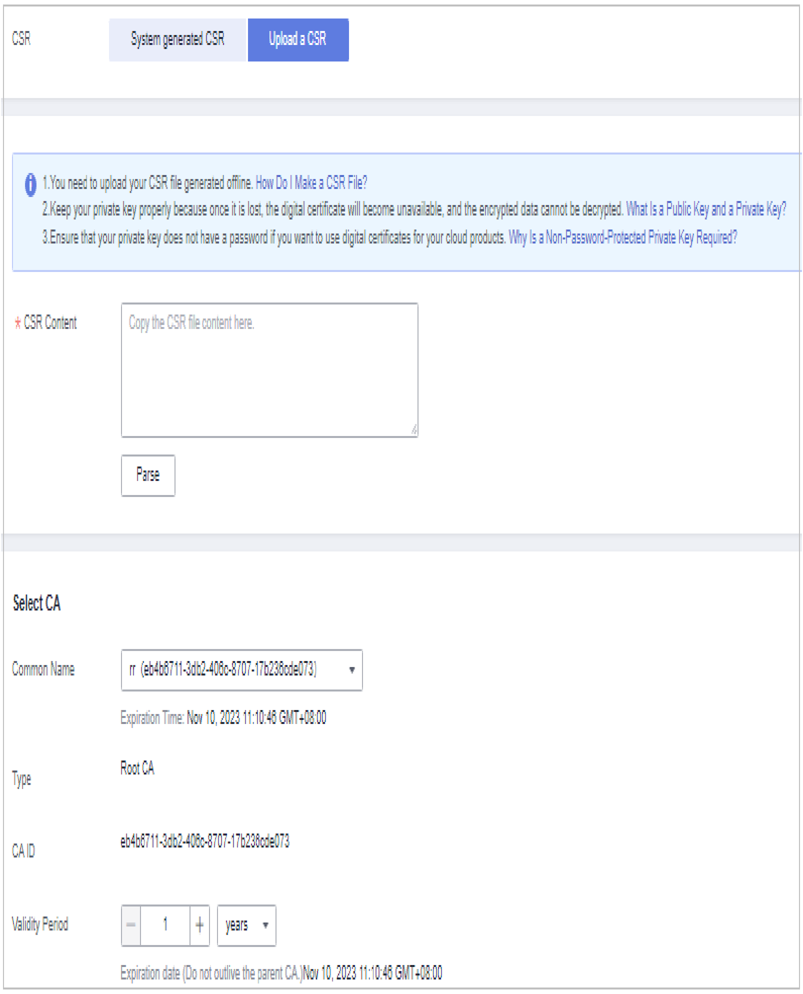
Type: Root CA

CA ID: eb4b6711-3db2-406c-8707-17b236cde073

Validity Period: 1 years

Expiration date (Do not outlive the parent CA.)Nov 10, 2023 11:10:46 GMT+08:00

Figure 3-2 Upload a CSR



1.You need to upload your CSR file generated offline. How Do I Make a CSR File?
2.Keep your private key properly because once it is lost, the digital certificate will become unavailable, and the encrypted data cannot be decrypted. What Is a Public Key and a Private Key?
3.Ensure that your private key does not have a password if you want to use digital certificates for your cloud products. Why Is a Non-Password-Protected Private Key Required?

* CSR Content: Copy the CSR file content here.

Select CA

Common Name: rr (eb4b6711-3db2-406c-8707-17b236cde073)
Expiration Time: Nov 10, 2023 11:10:46 GMT+08:00

Type: Root CA

CA ID: eb4b6711-3db2-406c-8707-17b236cde073

Validity Period: 1 years
Expiration date (Do not outlive the parent CA.)Nov 10, 2023 11:10:46 GMT+08:00

1. Select the CSR file generation method.

Table 3-1 Certificate signing request (CSR)

Parameter	Description
System generated CSR	The system automatically generates a certificate private key. Once the certificate is issued, you can download your certificate and private key on the certificate management page.
Upload a CSR	You can use an existing CSR. The procedure is as follows: 1. You need to manually generate a CSR file and paste the content of the CSR file into the text box. 2. Click **Parse**.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td colspan="2"><b>NOTE</b>
– To obtain a certificate, a CSR file needs to be submitted to the CA for review. A CSR file contains a public key and a distinguished name (DN). Typically, a CSR file is generated by a web server, and a pair of public and private keys are created along with the CSR file.
– You are advised to select <b>System generated CSR</b> to avoid approval failure caused by incorrect content.
– A private key file will be generated when the CSR file is generated manually. Keep and back up your private key properly. A private key maps to a certificate. If a private key is lost, the corresponding certificate becomes invalid. Huawei Cloud is not responsible for keeping your private key. You need to purchase a new certificate if the private key is lost.
– CCM has strict requirements on the key length of a CSR file. The key length must be 2,048 bits and the key type must be RSA.</td></tr>
</table>

2. Configure certificate details.

   Perform this step only when you select **System generated CSR** for **CSR**.

   Common Name: You can customize the name of the private certificate.

3. Click ^ on the right of **Advanced Configuration**.

   Perform this step only when you select **System generated CSR** for **CSR**.

Table 3-2 Advanced settings

Parameter	Description	Example Value
Key Algorithm	**Key Algorithm**: Select the key algorithm and key size for the private certificate. The value can be **RSA2048**, **RSA4096**, **EC256**, or **EC384**.	RSA2048
Signature Algorithm	Select the signature hash algorithm for the private certificate. The value can be **SHA256**, **SHA384**, or **SHA512**.	SHA256

Parameter	Description	Example Value
Key Usage	Select the key usage of the certificate. You can select more than one option. – **digitalSignature**: The key is used as a digital signature. – **nonRepudiation**: The key can be used for non-repudiation. – **keyEncipherment**: The key can be used for key encryption. – **dataEncipherment**: The key can be used for data encryption. – **keyAgreement**: The key can be used as a key-agreement protocol. – **keyCertSign**: The key can be used to issue certificates. – **cRLSign**: The key can be used for signing blacklists. – **encipherOnly**: The key can be used for encryption only. – **decipherOnly**: The key can be used for decryption only.	digitalSignature
Enhanced Key Usage	Select the enhanced key usage for the certificate. You can select more than one option. – **Server identity authentication** – **Client identity authentication** – **Code signature** – **Secure email** – **Timestamp**	Server identity authentication
Customized Extension Field	Enter customized information.	None

Parameter	Description	Example Value
Configure Certificate AltName	This field is optional. If you want to use the private certificate to multiple subjects, you can add more AltName records. You can configure **IP address**, **DNS**, **Email**, or **URI** for **AltName**. When you configure **AltName**, enter the value according to the value type you select. – **IP address**: Enter an IP address. – **DNS**: Enter the domain name. – **Email**: Enter an email address. – **URI**: Enter the network address. A maximum of five AltName records can be configured.	None

4. Select a CA.

Table 3-3 Parameters for selecting a CA

Parameter	Description
Common Name	Select a common name of the private CA you want.
Type	The CA type is autofilled after you specify **Common Name**.
CA ID	The CA ID is autofilled after you specify **Common Name**.
Validity Period	Configure the validity period of the private certificate. **NOTE** – You can customize the validity period of a private certificate. The validity period cannot outlive the validity period of the activated private CA. – A private CA can be valid for up to 30 years.

Step 4 Confirm the information and click **OK**.

After you submit your application, the system will return to the private certificate list page. Message "Certificate xxx applied for successfully." is displayed in the upper right corner of the page, indicating that the private certificate application is successful.

----End

Follow-up Operations

When a private certificate is issued, you can download it and distribute it to the certificate subject for installation. For details, see **Downloading a Private Certificate**.

3.2 Downloading a Private Certificate

Before using a private certificate, you need to download it. Only downloaded certificate can be assigned to the corresponding certificate subject so that they can install and use the certificate.

This topic describes how to download a private certificate. Only certificates in the **Issued** state can be downloaded.

Prerequisites

Your private certificate is in the **Issued** state. For details, see **Applying for a Private Certificate**.

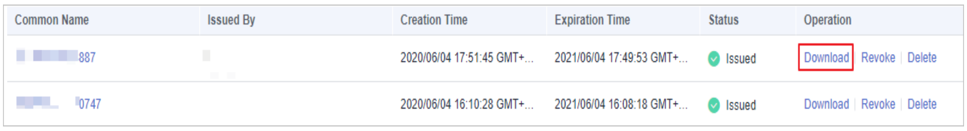
Procedure

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 Locate the row of the desired private certificate and click **Download** in the **Operation** column.

Figure 3-3 Downloading a private certificate



Common Name	Issued By	Creation Time	Expiration Time	Status	Operation
[redacted]887	[redacted]	2020/06/04 17:51:45 GMT+...	2021/06/04 17:49:53 GMT+...	✓ Issued	Download | Revoke | Delete
[redacted]0747		2020/06/04 16:10:28 GMT+...	2021/06/04 16:08:18 GMT+...	✓ Issued	Download | Revoke | Delete

Step 4 Click the target tab based on your server type and click **Download Certificate**.

PCA will use the download tool provided by the browser to download the private certificate to the specified local directory.

----End

Installing a Private Certificate

A private certificate must be installed on the corresponding server. The installation procedure for private certificates is the same as that for SSL certificates. You can refer to **Table 3-4**.

Table 3-4 Example for installing an SSL certificate

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

Description of Downloaded Certificate Files

The downloaded certificate files vary depending on the CSR file type (**System generated CSR** or **Upload a CSR**) configured when you apply for a private certificate.

- **System generated CSR**

  Table 3-5 describes the downloaded files.

Table 3-5 Description of downloaded files (1)

Server Type	Files in the Package
Tomcat	**keystorePass.txt**: certificate password **server.jks**: certificate file
Nginx	**server.crt**: certificate files, containing the server certificate and certificate chain **server.key**: certificate private key file
Apache	**chain.crt**: certificate chain file **server.crt**: certificate file **server.key**: certificate private key file
IIS	**keystorePass.txt**: certificate password **server.pfx**: certificate file
Others	**chain.pem**: certificate chain file **server.key**: certificate private key file **server.pem**: certificate file

- **Upload a CSR**

  Table 3-6 describes the downloaded files.

Table 3-6 Description of downloaded files (2)

Server Type	Files in the Package
Tomcat	**server.crt**: certificate file **chain.crt**: certificate chain file
Nginx	**server.crt**: certificate file
Apache	**server.crt**: certificate file **chain.crt**: certificate chain file
IIS	**server.crt**: certificate file **chain.crt**: certificate chain file
Others	**cert.pem**: certificate file **chain.pem**: certificate chain file

3.3 Revoking a Private Certificate

If a private certificate is no longer needed or its private key is lost before it expires, you can revoke it on the console. If a private certificate is revoked, it is no longer trusted within the organization.

If a private certificate is revoked, the billing stops.

The following describes how to revoke a private certificate.

Prerequisites

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

Constraints

- After you apply for revoking a private certificate, your application cannot be withdrawn. Exercise caution when performing this operation.
- All its records will be cleared and cannot be recovered, including private CA records. Therefore, exercise caution when performing this operation.

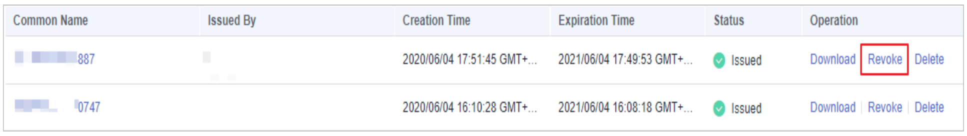
Procedure

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 Locate the row of the desired private certificate and click **Revoke** in the **Operation** column.

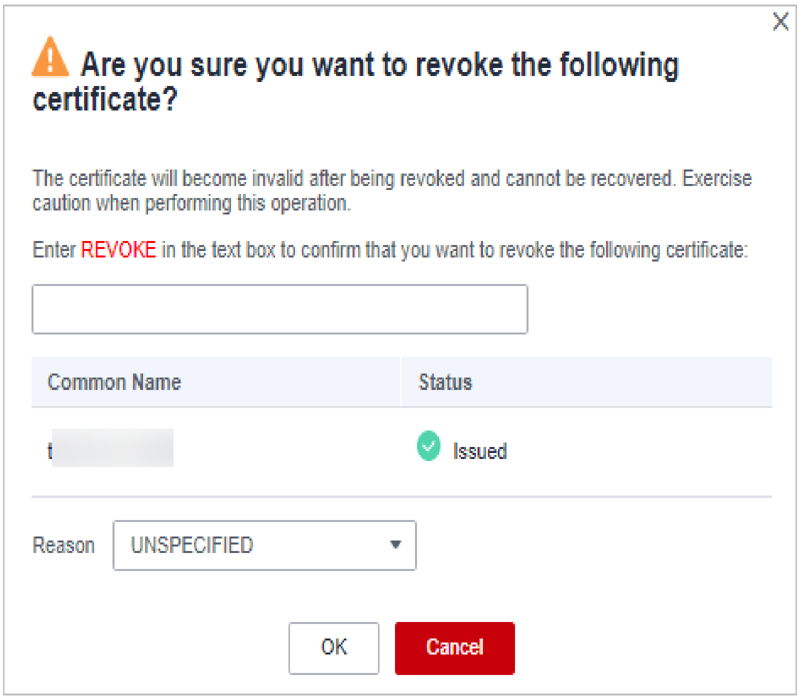
Figure 3-4 Revoking a private certificate



Common Name	Issued By	Creation Time	Expiration Time	Status	Operation
[redacted]887	[redacted]	2020/06/04 17:51:45 GMT+...	2021/06/04 17:49:53 GMT+...	✓ Issued	Download Revoke Delete
[redacted]0747		2020/06/04 16:10:28 GMT+...	2021/06/04 16:08:18 GMT+...	✓ Issued	Download | Revoke | Delete

Step 4 In the displayed dialog box, enter **REVOKE** and select the revocation reason to confirm the revocation. The default revocation reason is in the **UNSPECIFIED** field. Table 3-7 describes the revocation reasons you can select.

Figure 3-5 Revoke Certificate



Are you sure you want to revoke the following certificate?

The certificate will become invalid after being revoked and cannot be recovered. Exercise caution when performing this operation.

Enter REVOKE in the text box to confirm that you want to revoke the following certificate:

Common Name	Status
t[redacted]	✓ Issued

Reason UNSPECIFIED

Table 3-7 Revocation reasons and meaning

Reason for Revocation	Reason Code in RFC 5280	Description
UNSPECIFIED	0	Default value. No reason is specified for revocation.
KEY_COMPROMISE	1	The certificate key material has been leaked.
CERTIFICATE_AUTHORITY_COMPROMISE	2	Key materials of the CA have been leaked in the certificate chain.

Reason for Revocation	Reason Code in RFC 5280	Description
AFFILIATION_CHANGED	3	The subject or other information in the certificate has been changed.
SUPERSEDED	4	The certificate has been replaced.
CESSATION_OF_OPERATION	5	The entity in the certificate or certificate chain has ceased to operate.
CERTIFICATE_HOLD	6	The certificate should not be considered valid currently and may take effect in the future.
PRIVILEGE_WITHDRAWN	9	The certificate no longer has the right to declare its listed attributes.
ATTRIBUTE_AUTHORITY_COMPROMISE	10	The authority that warrants the attributes of the certificate may have been compromised.

Step 5 Click **OK**.

When "Certificate xxx revoked successfully" is displayed in the upper right corner of the page, and the private certificate status changes to **Revoked**, the private certificate is revoked successfully.

----End

3.4 Viewing Details of a Private Certificate

This topic describes how to view details of a private certificate, including the common name, expiration time, and status.

Prerequisites

You have applied for a private certificate. For details, see **Applying for a Private Certificate**.

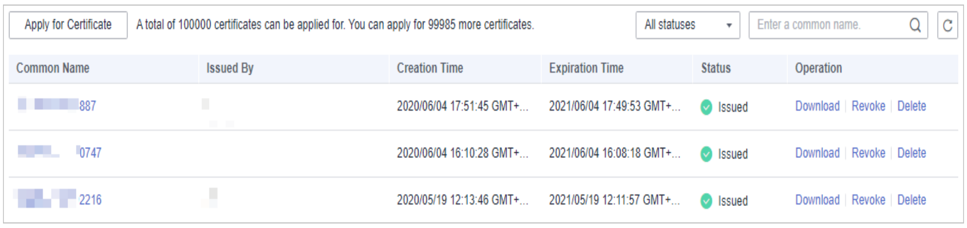
Procedure

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 View the private certificate information. **Table 3-8** describes the private certificate parameters.

Figure 3-6 Private certificate list



Apply for Certificate A total of 100000 certificates can be applied for. You can apply for 99985 more certificates. All statuses Enter a common name.

Common Name	Issued By	Creation Time	Expiration Time	Status	Operation
[redacted]887	[redacted]	2020/06/04 17:51:45 GMT+...	2021/06/04 17:49:53 GMT+...	Issued	Download | Revoke | Delete
[redacted]0747		2020/06/04 16:10:28 GMT+...	2021/06/04 16:08:18 GMT+...	Issued	Download | Revoke | Delete
[redacted]2216	[redacted]	2020/05/19 12:13:46 GMT+...	2021/05/19 12:11:57 GMT+...	Issued	Download | Revoke | Delete

NOTE

- Select a certificate state from the drop-down list of **All statuses**. Then the certificate list displays only the private certificates in the corresponding state.
- Enter a name of a private certificate in the search box in the upper right corner and click 🔍 or press **Enter** to search for a specified private certificate.

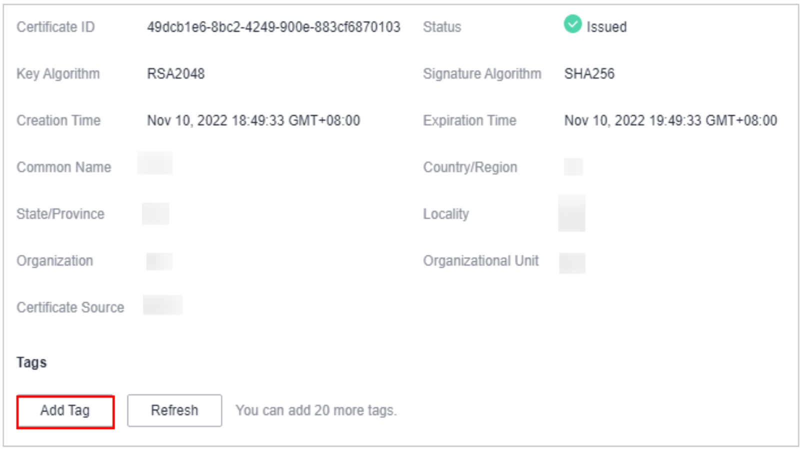
Table 3-8 Private certificate parameters

Parameter	Description
Common Name	Indicates the name of the private certificate configured during certificate application.
Issued By	Indicates the name of the private CA that issues the private certificate.
Creation Time	Indicates the time when a private certificate is created.
Expiration Time	Indicates the time when a certificate expires.
Status	Indicates the certificate status. The value can be: ● **Issued** The private certificate is issued. ● **Expired** The private certificate is expired. ● **Revoked** The private certificate is revoked.
Operation	You can download, revoke, or delete the certificate.

Step 4 Click the common name of a private certificate to view its details.

You can click **Add Tag** on the private certificate details page to identify the private certificate. TMS's predefined tag function is recommended for adding the same tag to different cloud resources.

Figure 3-7 Private certificate details



Certificate ID	49dcb1e6-8bc2-4249-900e-883cf6870103	Status	✓ Issued
Key Algorithm	RSA2048	Signature Algorithm	SHA256
Creation Time	Nov 10, 2022 18:49:33 GMT+08:00	Expiration Time	Nov 10, 2022 19:49:33 GMT+08:00
Common Name	[redacted]	Country/Region	[redacted]
State/Province	[redacted]	Locality	[redacted]
Organization	[redacted]	Organizational Unit	[redacted]
Certificate Source	[redacted]		

Tags

----End

3.5 Deleting a Private Certificate

This topic describes how to delete a private certificate from Huawei Cloud. A deleted private certificate remains valid and trusted.

You can delete a certificate that is no longer needed.

Prerequisites

The private certificate is in the **Issued**, **Expired**, or **Revoked** state.

Constraints

- A deleted certificate cannot be restored. Exercise caution with the deletion.
- After you submit a certificate deletion application, you cannot cancel it. Exercise caution when performing this operation.

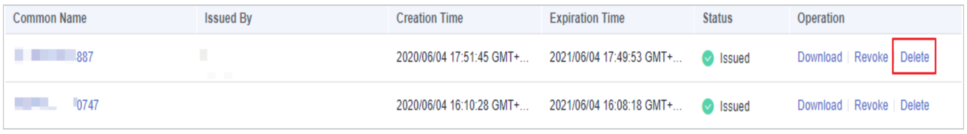
Procedure

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**. In the navigation pane on the left, choose **Private Certificate Management** > **Private Certificate**. The **Private Certificate** page is displayed.

Step 3 Locate the row of the private certificate to be deleted and click **Delete** in the **Operation** column.

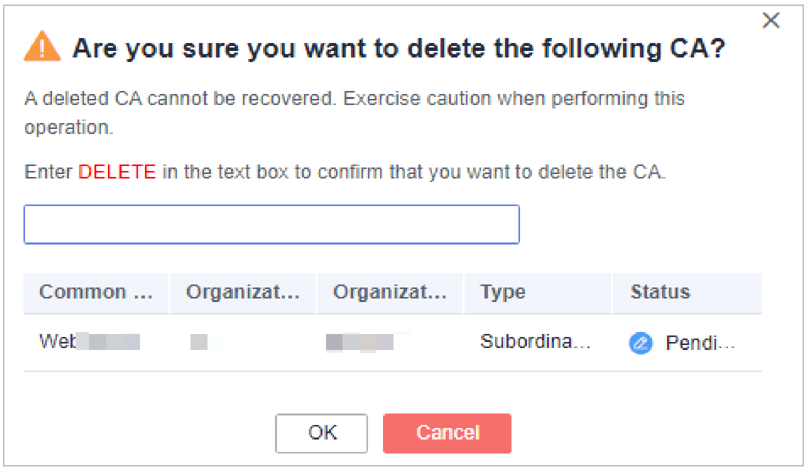
Figure 3-8 Deleting a private certificate



Common Name	Issued By	Creation Time	Expiration Time	Status	Operation
[redacted]887	[redacted]	2020/06/04 17:51:45 GMT+...	2021/06/04 17:49:53 GMT+...	✓ Issued	Download | Revoke | Delete
[redacted]0747		2020/06/04 16:10:28 GMT+...	2021/06/04 16:08:18 GMT+...	✓ Issued	Download | Revoke | Delete

Step 4 In the displayed dialog box, enter **DELETE** to confirm the deletion.

Figure 3-9 Delete Certificate



Are you sure you want to delete the following CA?

A deleted CA cannot be recovered. Exercise caution when performing this operation.

Enter DELETE in the text box to confirm that you want to delete the CA.

Common ...	Organizat...	Organizat...	Type	Status
Wet[redacted]	[redacted]	[redacted]	Subordina...	Pendi...

Step 5 Click **OK**. If message "Certificate xxx deleted successfully." is displayed in the upper right corner of the page, the private certificate is deleted successfully.

----End

4 Sharing

4.1 Overview

Introduction

The Private Certificate Management service in CCM allows you to share private CAs of account A with all member accounts in the same organization unit. These member accounts, such as accounts B and C, can use the shared CA to issue certificates.

- Account A is the private CA owner (owner for short).
- Accounts B and C are private CA recipients.

Private CA Owner and Recipient Permissions

Owners can perform all operations on private CAs, while recipients can only perform certain operations. For details, see **Table 4-1**.

Table 4-1 Operations supported for private CA recipients

Role	Operation Supported	Description
Recipient	pca:ca:export	Access through the console or API
	pca:ca:get	Access through the console or API
	pca:ca:listTags	Access through the console or API
	pca:ca:issueCert	Access through the console or API
	pca:ca:issueCertByCsr	Access through the console or API
	pca:ca:revokeCert	Access through the console or API

Supported Resource Types and Regions

Table 4-2 lists the resource types and regions can be shared in PCA.

Table 4-2 Resources and regions supported by PCA

Cloud Service	Resource Type	Supported Region
PCA	ca: private CA	ALL

Billing Description

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

The owner of a shared private CA pays for the CA. So, only the resource owner will be charged for shared resources.

4.2 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 **pca:ca**, choose the corresponding region, and select private CAs 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 4-3 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

4.3 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 **pca:ca**. 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

4.4 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 private CAs and resource principals. For details, see **Viewing Your Shared Resources** and **Viewing Principals You Share With**.

----End

4.5 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

4.6 Leaving a Resource Share

If you no longer need to access shared private CAs, you can leave a share at any time. After you leave the share, you will lose access to the shared private CA.

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

5 Managing Tags

5.1 Overview

Scenario

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

You can add tags when purchasing a CA or private certificate, or add tags on the details page of the CA or private certificate after the purchase.

Tag Naming Rules

- Each tag consists of a key-value pair.
- A maximum of 20 tags can be added to each private CA or private certificate.
- For each resource, 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 5-1**.

  NOTE

  If your organization has configured a tag policy for the CCM service, you need to add tags to private CA or private CAs based on the tag policy. Otherwise, the tagging operation might fail. For more information about the tag policy, contact your organization administrator.

Table 5-1 Tag parameters

Parameter	Rule	Example
Tag key	● This parameter is mandatory. ● For a private CA or private certificate, the tag key must be unique. ● 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 field cannot be left blank. ● The value can contain a maximum of 255 characters. ● The following character types are allowed: – Chinese – English – Digit – Space – Special characters: _.:/=+-@	100

5.2 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**.

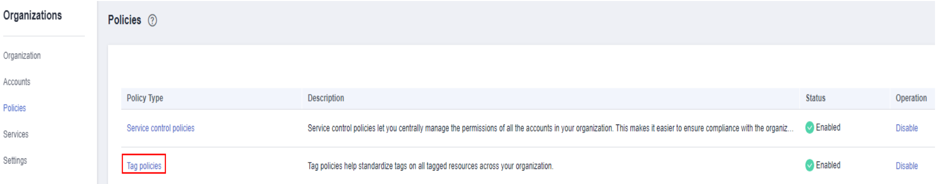
Procedure

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**.

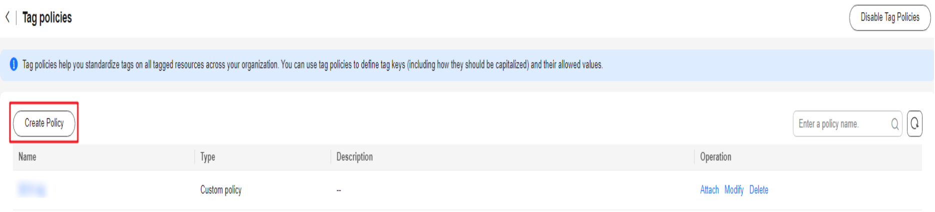
Figure 5-1 Accessing the **Tag policies** page



Policy Type	Description	Status	Operation
Service control policies	Service control policies let you centrally manage the permissions of all the accounts in your organization. This makes it easier to ensure compliance with the organiz...	✓ Enabled	Disable
Tag policies	Tag policies help standardize tags on all tagged resources across your organization.	✓ Enabled	Disable

Step 4 Click **Create Policy**.

Figure 5-2 Creating a policy



Tag policies

Disable Tag Policies

Tag policies help you standardize tags on all tagged resources across your organization. You can use tag policies to define tag keys (including how they should be capitalized) and their allowed values.

Create Policy

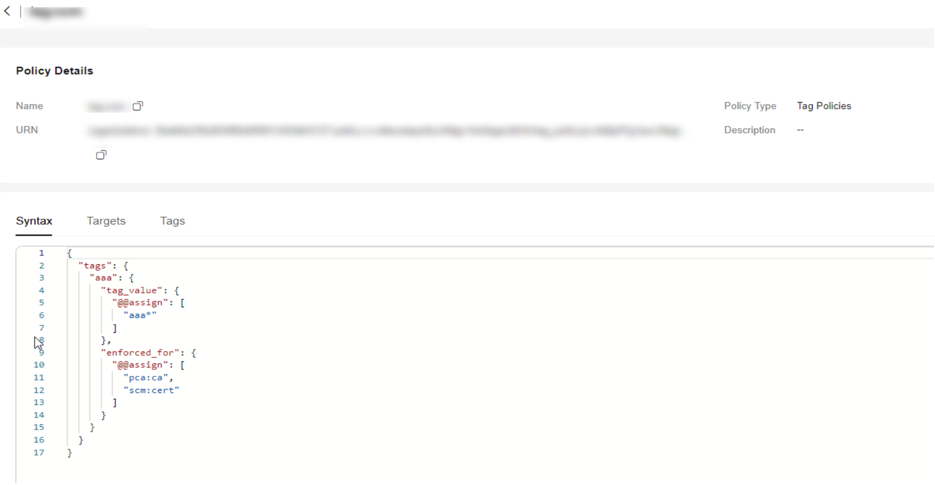
Enter a policy name.

Name	Type	Description	Operation
	Custom policy	--	Attach Modify Delete

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

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

Figure 5-3 Setting a policy tag



Policy Details

Name		Policy Type	Tag Policies
URN		Description	--

Syntax Targets Tags

```
{
  "tags": {
    "aaa": {
      "tag_value": {
        "@@assign": [
          "aaa*"
        ]
      },
      "enforced_for": {
        "@@assign": [
          "pca:ca",
          "scm:cert"
        ]
      }
    }
  }
}
```

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

5.3 Creating a Tag

This topic describes how to add tags to private CAs and private certificates.

Creating a Tag for a Private CA

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.

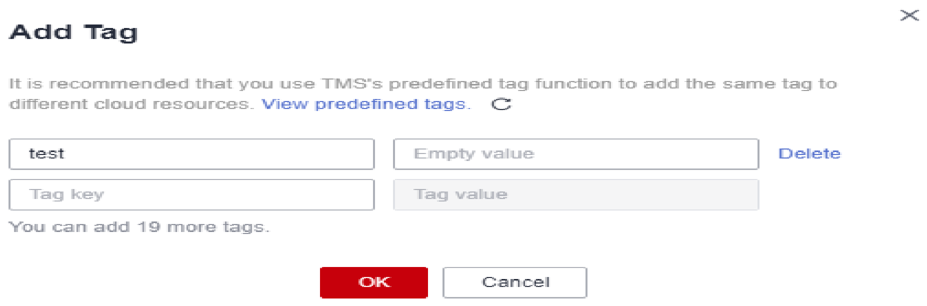
Step 3 In the navigation pane on the left, choose **Private Certificate Management > Private CAs**.

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

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

Step 6 Click **Edit Tag**. In the displayed **Edit Tag** dialog box, click **Add Tag**. In the text box, specify **Tag key** and **Tag value**.

Figure 5-4 Add Tag



Add Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags.

test | Empty value

Tag key | Tag value

You can add 19 more tags.

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

Creating a Tag for a Private Certificate

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

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

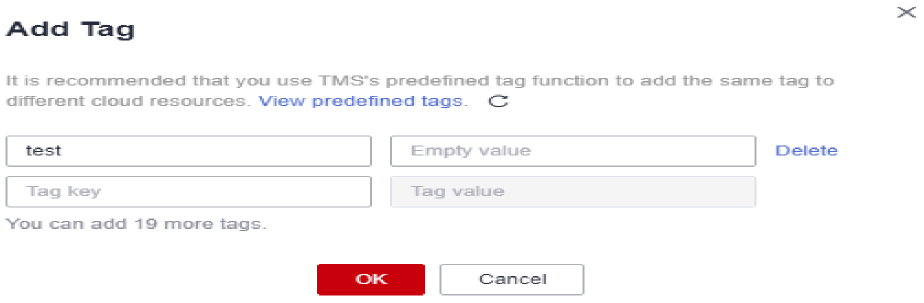
Step 3 In the navigation pane on the left, choose **Private Certificate Management > Private Certificates**.

Step 4 Click the name of the target private 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 **Edit Tag** dialog box, click **Add Tag**. In the text box, specify **Tag key** and **Tag value**.

Figure 5-5 Add Tag



Add Tag

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags.

test | Empty value | Delete

Tag key | Tag value

You can add 19 more tags.

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

5.4 Searching for Private CAs or Certificates by Tag

This topic describes how to search for private CAs or certificates that meet the search criteria by tag in the current project.

Prerequisites

A tag has been added.

Constraints

- At most 20 tags can be added for one search. If multiple tags are added, private CAs or 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.

Searching for Private CAs by Tag

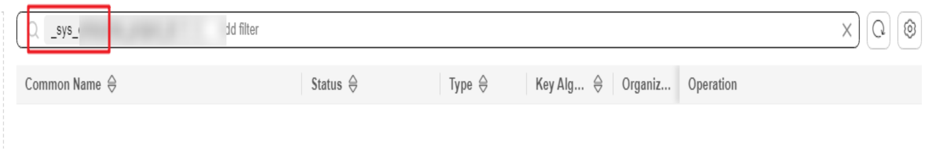
Step 1 Log in to the **management console**.

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 **Private Certificate Management > Private CAs**.

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

Figure 5-6 Search result



sys [redacted] dd filter

Common Name	Status	Type	Key Alg...	Organiz...	Operation

NOTE

- At most 20 tags can be added for one search. If multiple tags are added, private CAs 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

Searching for Private Certificates by Tag

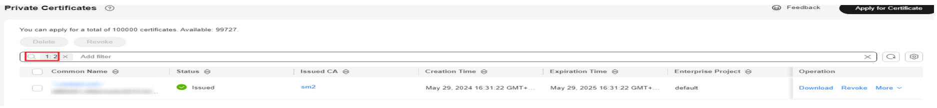
Step 1 Log in to the **management console**.

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 **Private Certificate Management** > **Private Certificates**.

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

Figure 5-7 Search result



You can apply for a total of 100000 certificates. Available: 99727.

1: 2 × Add filter

Common Name	Status	Issued CA	Creation Time	Expiration Time	Enterprise Project	Operation
[redacted]	Issued	sm2	May 29, 2024 16:31:22 GMT+...	May 29, 2025 16:31:22 GMT+...	default	Download Revoke More

NOTE

- At most 20 tags can be added for one search. If multiple tags are added, private 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

5.5 Modifying a Tag Value

This section describes how to modify a private CA or private certificate tag.

Modifying the Private CA Tag Value

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 **Private Certificate Management > Private CAs**.

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

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

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

----End

Changing the Tag Value of a Private Certificate

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

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

Step 3 In the navigation pane on the left, choose **Private Certificate Management > Private Certificates**.

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

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

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

----End

5.6 Deleting a Tag

This section describes how to delete a private CA tag or private certificate tag.

Deleting a Private CA Tag

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 **Private Certificate Management > Private CAs**.

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

Step 5 Click **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

Deleting a Private Certificate Tag

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 **Private Certificate Management > Private Certificates**.

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

Step 5 Click **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

6 PCA Permissions Management

6.1 Creating a User and Granting PCA Permissions to the User

This topic describes how to use **IAM** to implement fine-grained permissions control for your PCA 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 PCA resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M to your PCACCM resources.

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

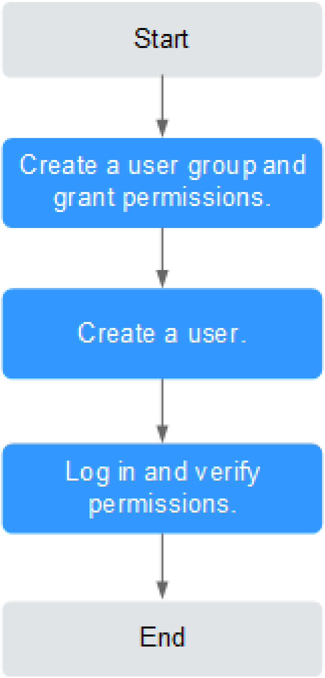
This section provides some methods for you to assign permissions to a user. **Figure 6-1** shows the process.

Prerequisites

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

Process Flow

Figure 6-1 Process for granting PCA permissions


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

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

   Create a user group on the IAM console and grant the user group the **PCA FullAccess**.

2. **Create a user and add it to a user group**.

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

3. **Log in and verify the 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 no permissions to access the service, the policy **PCA FullAccess** has already taken effect.

6.2 PCA Custom Policies

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

You can create custom policies in either of the following two 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 PCA custom policies.

Example PCA Custom Policies

- Example 1: authorizing users to create a CA

  ```
  {
          "Version": "1.1",
          "Statement": [
                  {
                          "Action": [
                                  "pca:ca:create
                          ],
                          "Effect": "Allow"
                  }
          ]
  }
  ```

- Example 2: denying certificate deletion

  A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. 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 **PCA FullAccess** 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 deny policy:

  ```
  {
          "Version": "1.1",
          "Statement": [
                  {
                          "Action": [
                                  "pca:ca:delete"
                          ],
                          "Effect": "Deny"
                  }
          ]
  }
  ```

A Change History

2024-05-30	This issue is the thirteenth official release. Added **Managing Tags**, which describes the interconnection with Tag Management Service (TMS).
2023-1-11	This issue is the fifth official release. Added **Configuring a CRL**.
2022-11-16	This issue is the fourth official release. Added **PCA Custom Policies**. Optimized the following topics: ● **Purchasing a Private CA** ● **Applying for a Private Certificate**
2022-10-31	This issue is the third official release. ● Optimized the document structure. Split the CCM user guide into two manuals: *SSL Certificate Manager User Guide* and *Private Certificate Manager User Guide*. ● Optimized **PCA Permissions Management**.
2022-09-29	This issue is the second official release. Optimized **Deleting a Private Certificate**.
2022-03-24	This issue is the first official release.