Key Management Service Console Guide

Copyright Notice

Trademark Notice

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Console Guide
Getting Started

Last updated：2023-08-24 11:32:37

Key Management System (KMS) offers secure and compliant full lifecycle management and encryption/decryption capabilities for keys.

For users, the core key components involved in the KMS service include Customer Master Keys (CMKs) and Data Encryption Keys (DEKs). CMKs are first-level keys belonging to users, used for encrypting and decrypting sensitive data as well as deriving DEKs. DEKs are second-level keys in the envelope encryption process, used for encrypting business data and protected by the user's CMK.

For scenarios where CMKs and DEKs are used for business data encryption and decryption, please see Sensitive Data Encryption and Envelope Encryption Best Practices.

Key Overview

Customer Master Key (CMK)

A CMK, as a core resource in KMS, is protected by a third-party certified hardware security module (HSM) and used as a first-level key for encryption and decryption. KMS is mainly a management service for CMKs.

A Customer Master Key (CMK) is the logical representation of a primary key. CMKs include metadata such as key ID, creation date, description, and key status. Typically, you can use KMS's auto-generated customer master key feature to create CMKs, and it also supports importing your own keys to form CMKs.

There are two types of CMKs: Customer Managed CMK and Tencent Cloud Managed CMK.

- **User Keys** are Customer Master Keys created by users through the console or API. You can perform operations such as creating, enabling, disabling, rotating, and controlling permissions for user keys.
- **Cloud Product Keys** are CMKs automatically created for users by Tencent Cloud products/services (such as CBS, COS, TDSQL, etc.) when invoking the Key Management System. You can query and enable key rotation for cloud product keys, but disabling and scheduled deletion operations are not supported.

Data Encryption Key (DEK)

Data Encryption Keys (DEKs) are secondary keys generated based on CMKs and can be used for local data encryption and decryption. You can generate DEKs using KMS Customer Master Keys (CMKs); however, KMS does not store, manage, or track your DEKs, nor does it perform encryption operations with DEKs. You must use and manage DEKs outside of KMS.

Typically, DEKs are used in the envelope encryption process for encrypting local business data. DEKs are protected by the Customer Master Key (CMK) and can be customized or created through the GenerateDataKey interface.

Operation Overview

Action	Note
Create a Key	Create a key quickly in the console.
View a Key	Viewing Key ID and Details Information via Console
Edit a Key	Edit key name, description, and other information via the console.
Enable/Disable a Key	Enable/Disable a key through the console
Key Rotation	Enable key rotation in the console.
Encryption and Decryption	Encrypting Data with Keys in the Console
Delete a Key	Quickly delete a key through the console.
Key Archiving	Enable or disable key archiving in the console.
Access Control	Set sub-account permissions for managing the Key Management System

Key Management
Creating Key

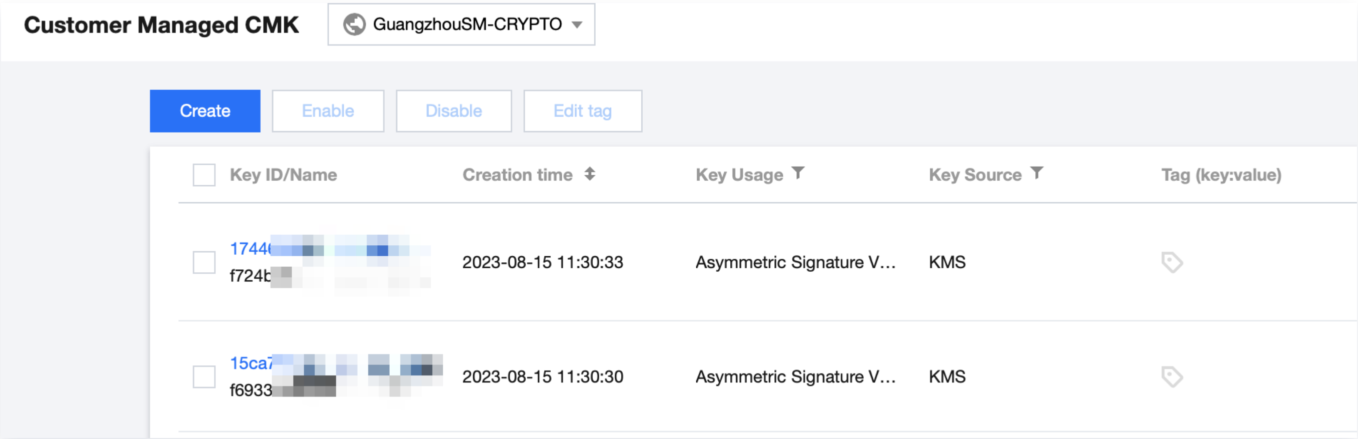
Last updated：2023-08-24 17:25:06

Scenario

You can create a CMK in the Tencent Cloud KMS Console or by using the CreateKey API. Once created, you can enable, disable, rotate, and manage permissions for the CMK. This document describes how to create a CMK through the console.

Instructions

1. Log in to the Key Management System (Compliance) console.
2. Select the region where you want to create the key, and click **Create**.

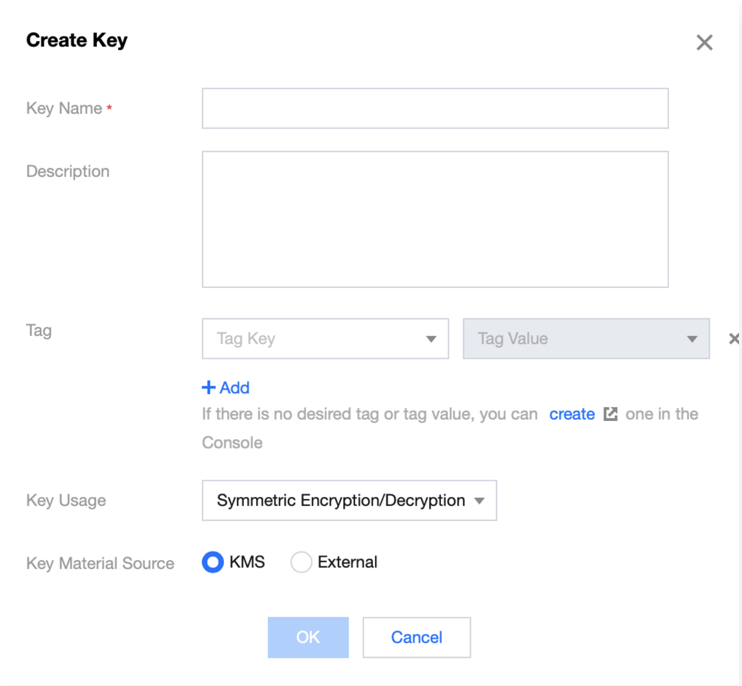


□ Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)
□ 1744[redacted] f724[redacted]	2023-08-15 11:30:33	Asymmetric Signature V...	KMS	
□ 15ca7[redacted] f6933[redacted]	2023-08-15 11:30:30	Asymmetric Signature V...	KMS	

3. In the pop-up configuration box, enter the following information:
   - Key Name: This is required and must be unique within the region. It can contain letters, numbers, `_`, `-`, and cannot begin with "KMS-".
   - Description: Optional, used to describe the type of data you plan to protect or the application intended to be used in conjunction with the CMK.
   - Tags: Optional, Tags are resource management tools provided by Tencent Cloud, allowing users to categorize, search, and aggregate keys by adding tags.
   - Key Usage: This is required and supports symmetric encryption and decryption, asymmetric encryption and decryption, or asymmetric signature verification.
   - Key Material Source: Required, choose the key generation method, either KMS-generated or user-imported key material.

> **Note**

> When the key material is sourced externally, only symmetric encryption and decryption purposes are supported.



Create Key

Key Name *

Description

Tag: Tag Key / Tag Value

+ Add

If there is no desired tag or tag value, you can create one in the Console

Key Usage: Symmetric Encryption/Decryption

Key Material Source: ● KMS ○ External

4. After clicking **Confirm**, you will return to the Key List, and the newly created key will appear at the top of the list.

Viewing keys

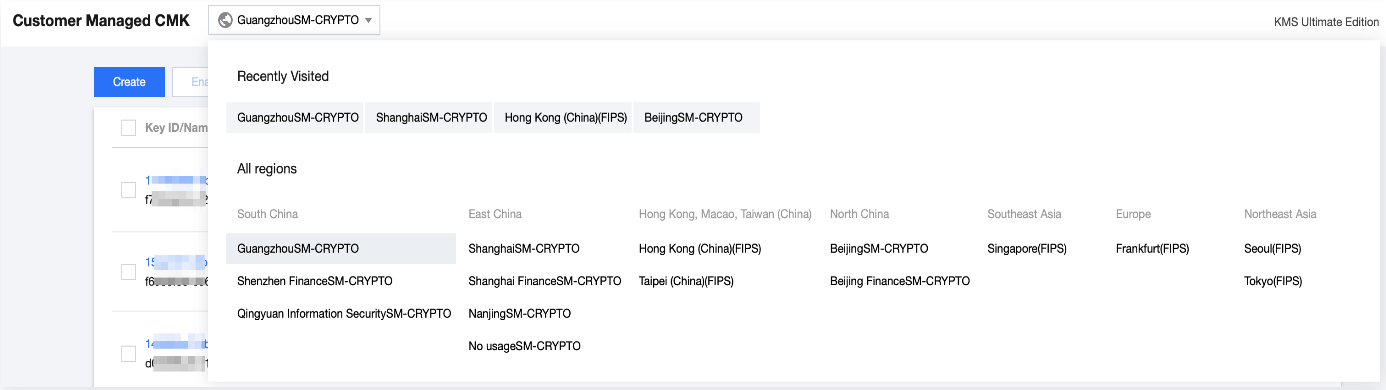
Last updated：2023-08-24 17:30:56

Scenario

You can log in to the Tencent Cloud Key Management System (Compliant) Console or call KMS TCCLI to view the CMK ID information list, name, ID, status, region, and other key details. This document introduces how to view the CMK ID information list and details through the console.

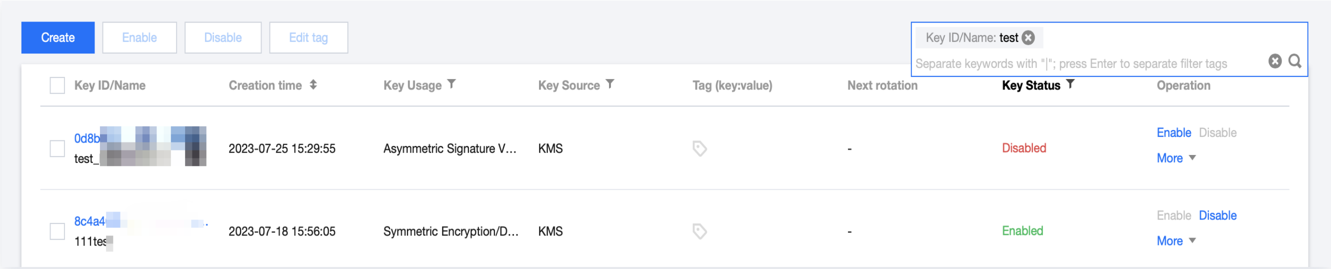
Viewing Key ID List

1. Log in to the Key Management System (Compliance) console.
2. Switch the region at the top to view the master key list for other regions.



In the filter box on the right side of the page, enter the full or partial name of the CMK or the key ID to filter and find your key.

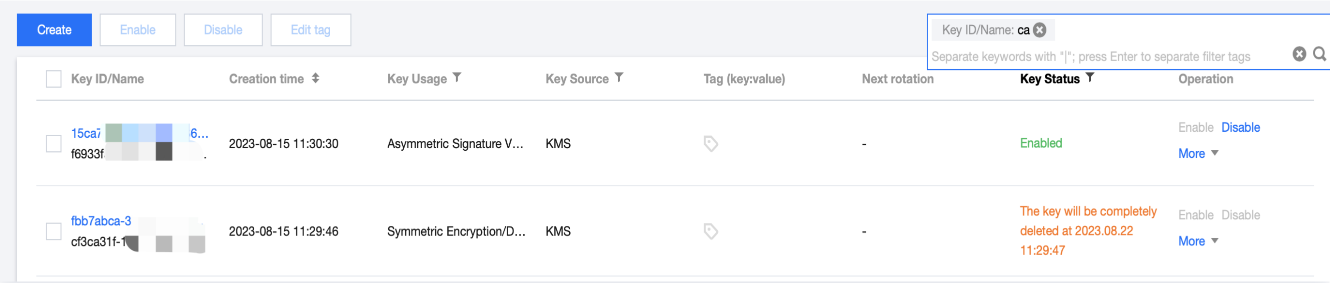
- Search by name


Create
Enable
Disable
Edit tag
Separate keywords with "|"; press Enter to separate filter tags

Key ID/Name: test

□ Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Next rotation	Key Status	Operation
□ 0d8b[redacted] test_[redacted]	2023-07-25 15:29:55	Asymmetric Signature V...	KMS		-	Disabled	Enable Disable More
□ 8c4a4[redacted] 111tes[redacted]	2023-07-18 15:56:05	Symmetric Encryption/D...	KMS		-	Enabled	Enable Disable More

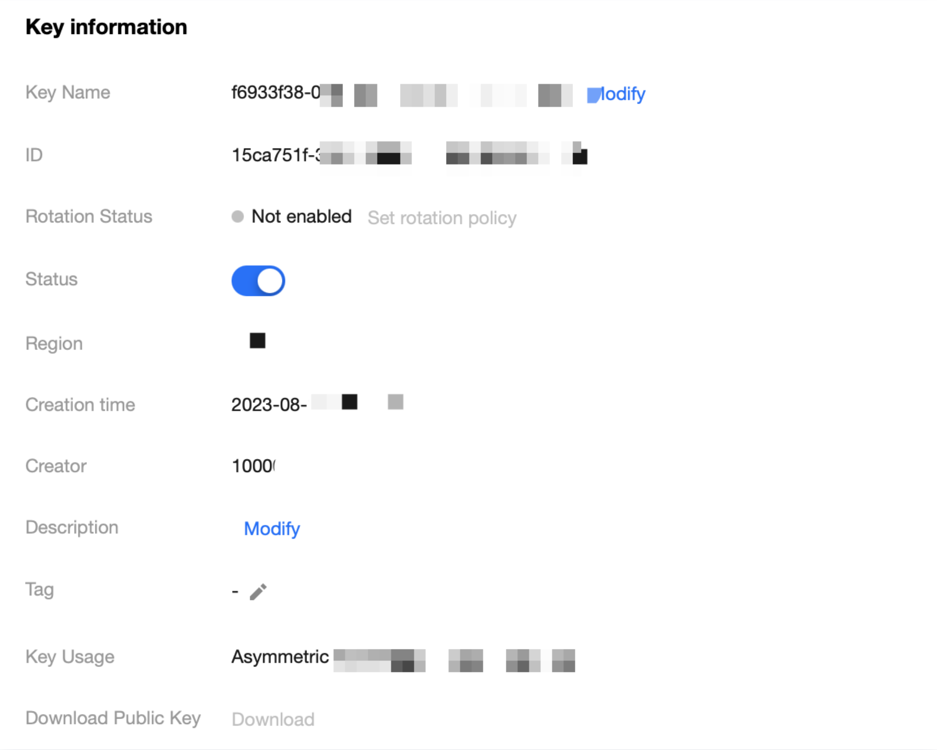
- Search by ID


Create
Enable
Disable
Edit tag
Key ID/Name: ca
Separate keywords with "|"; press Enter to separate filter tags

Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Next rotation	Key Status	Operation
15ca7[redacted]6... f6933f[redacted].	2023-08-15 11:30:30	Asymmetric Signature V...	KMS		-	Enabled	Enable Disable More
fbb7abca-3[redacted] cf3ca31f-1[redacted]	2023-08-15 11:29:46	Symmetric Encryption/D...	KMS		-	The key will be completely deleted at 2023.08.22 11:29:47	Enable Disable More

Viewing Key ID Details

1. Log in to the Key Management System (Compliance) console.
2. Locate the key for which you need to view details. For detailed methods on finding keys, please refer to Viewing Key ID List.
3. Click the key's ID/name to view detailed information about the key.



Key information

Key Name	f6933f38-0[redacted] Modify
ID	15ca751f-[redacted]
Rotation Status	● Not enabled Set rotation policy
Status	●
Region	[redacted]
Creation time	2023-08-[redacted]
Creator	1000[redacted]
Description	Modify
Tag	-
Key Usage	Asymmetric [redacted]
Download Public Key	Download

Editing Key

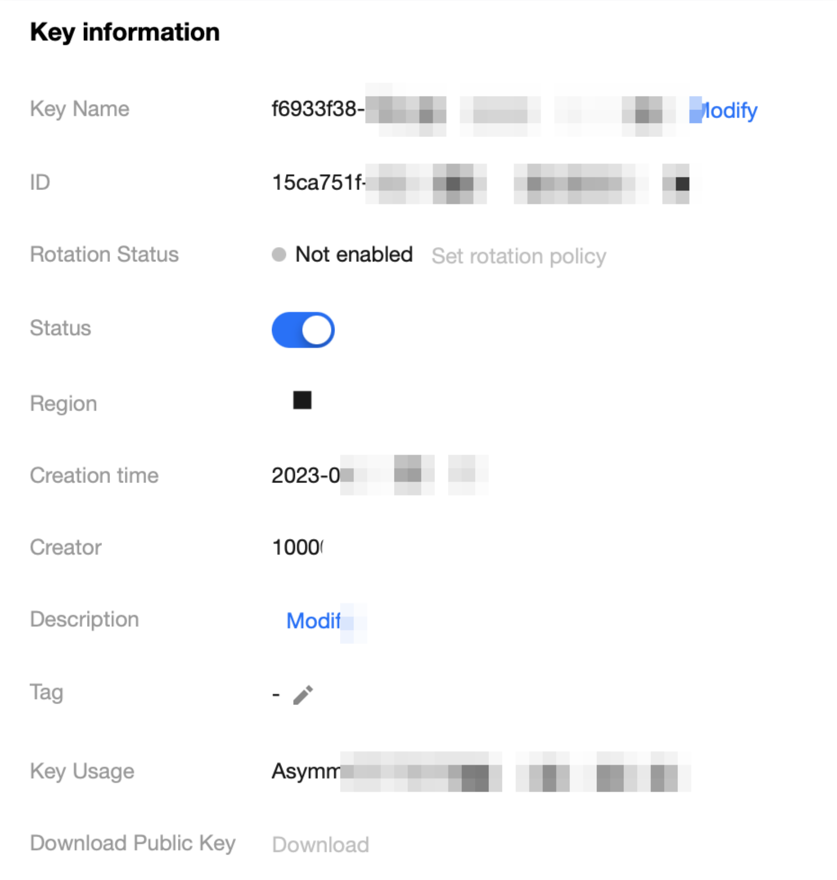
Last updated：2023-08-24 16:57:31

Scenario

You can edit the Customer Master Key (CMK) in the Tencent Cloud Key Management System (KMS) Console or by calling KMS TCCLI. You can modify the description and enable or disable key rotation. This document provides a detailed guide on how to edit the CMK through the console.

Instructions

1. Log in to the Key Management System (Compliance) console.
2. Click the ID/name of the key you want to edit to enter its details page. You can modify the key's name, status, rotation settings, and description information.



Key information

Key Name	f6933f38-[redacted] Modify
ID	15ca751f-[redacted]
Rotation Status	● Not enabled Set rotation policy
Status	
Region	[redacted]
Creation time	2023-0[redacted]
Creator	1000[redacted]
Description	Modif[redacted]
Tag	-
Key Usage	Asymm[redacted]
Download Public Key	Download

3. Click **OK** for the changes to take effect.

Enabling/Disabling Key

Last updated：2023-08-24 16:58:10

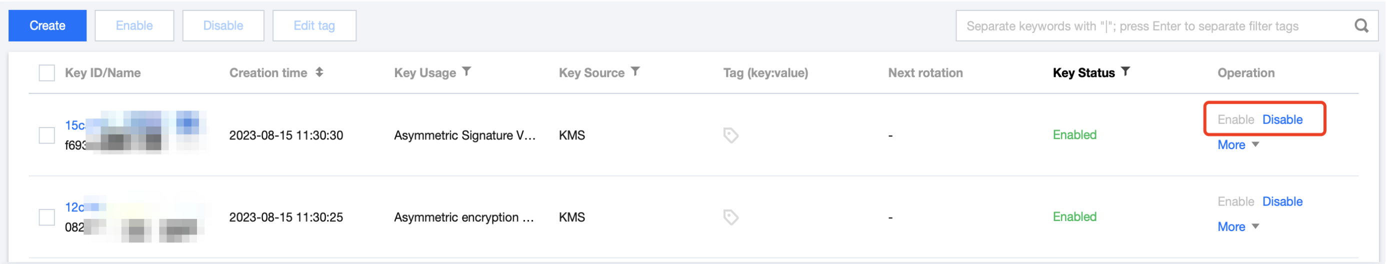
Scenario

You can log in to the Tencent Cloud Key Management System (Compliant) Console or call KMS TCCLI to enable/disable the status of created Customer Master Keys (CMKs). This document introduces how to enable/disable keys through the console.

Instructions

Single operation

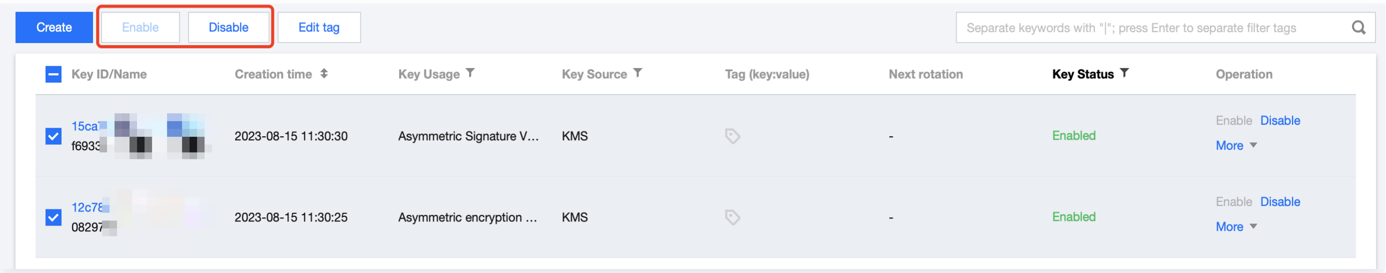
1. Log in to the Key Management System (Compliance) console.
2. Locate the key for which you need to change the status. In the operation area on the right side of the key information, you can enable or disable the key.


Create
Enable
Disable
Edit tag
Separate keywords with "|"; press Enter to separate filter tags

□ Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Next rotation	Key Status	Operation
□ [redacted]	2023-08-15 11:30:30	Asymmetric Signature V...	KMS		-	Enabled	Enable Disable More
□ [redacted]	2023-08-15 11:30:25	Asymmetric encryption ...	KMS		-	Enabled	Enable Disable More

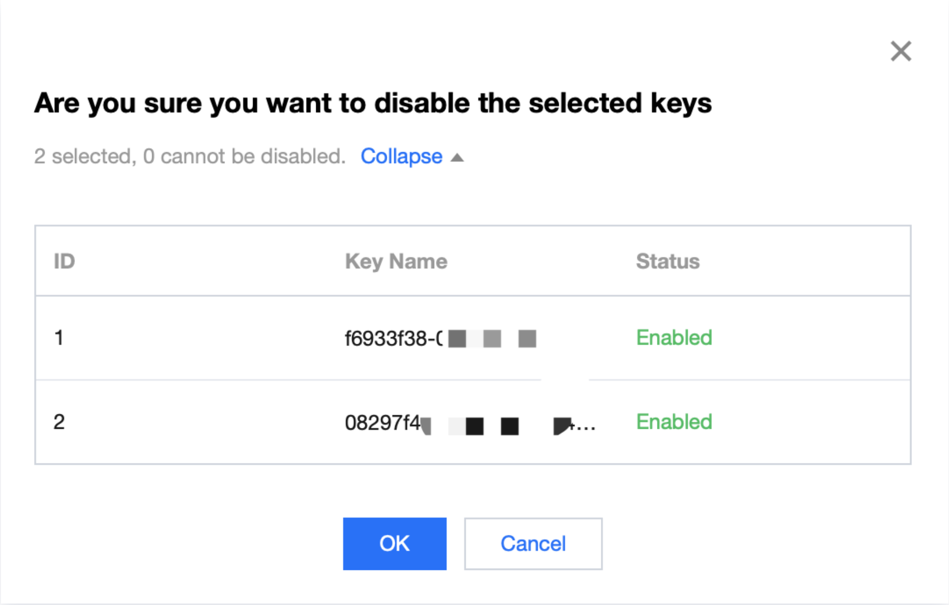
Batch Operation

1. Log in to the Key Management System (Compliance) console.
2. Select multiple keys for which you need to change the status.


Create
Enable
Disable
Edit tag
Separate keywords with "|"; press Enter to separate filter tags

Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Next rotation	Key Status	Operation
☑ [redacted]	2023-08-15 11:30:30	Asymmetric Signature V...	KMS		-	Enabled	Enable Disable More
☑ [redacted]	2023-08-15 11:30:25	Asymmetric encryption ...	KMS		-	Enabled	Enable Disable More

3. At the top of the list, click **Enable Key** or **Disable Key**. The system will display a confirmation dialog box as shown below. Click **View Details** to confirm the status of the keys in this batch operation.



Are you sure you want to disable the selected keys

2 selected, 0 cannot be disabled.

ID	Key Name	Status
1	f6933f38-[redacted]	Enabled
2	08297f4[redacted]...	Enabled

4. After confirming that everything is correct, click **OK** to enable or disable keys in bulk.

Key Rotation

Last updated：2023-08-24 16:58:46

Scenario

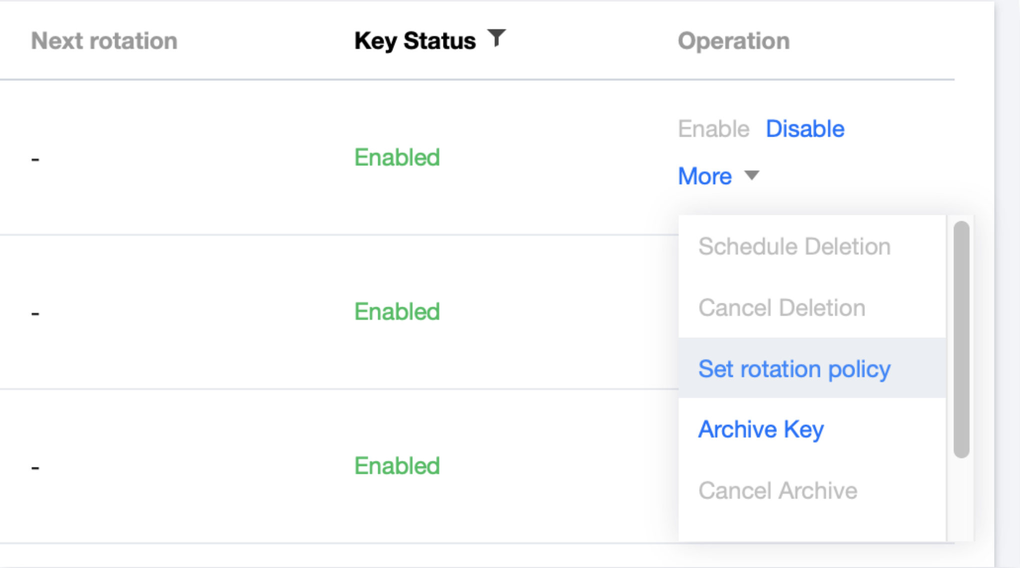
To further enhance the security of encrypted data storage, Tencent Cloud Key Management System (KMS) provides users with transparent key rotation capabilities to refresh stored ciphertext.

CMK key rotation offers transparent key rotation capabilities without affecting user operations and is compatible with ciphertext encrypted before rotation. Additionally, the ReEncrypt interface is available for refreshing ciphertext. This document describes how to enable key rotation through the console.

Instructions

1. Log in to the Key Management System (Compliance) console.
2. Locate the key for which you want to enable rotation, and in the "Key Rotation" column on the right, click **Enable Rotation** to enable rotation for that key.

> **Note**
> By default, key rotation is disabled. You can choose whether to enable it. Once enabled, the CMK will rotate once a year.



Next rotation	Key Status	Operation
-	Enabled	Enable Disable More
-	Enabled	
-	Enabled	

Encryption and Decryption

Last updated：2023-08-24 16:59:02

Scenario

Tencent Cloud KMS provides APIs, SDKs, and online tools for you to encrypt and decrypt small pieces of data. You can choose any of them based on your needs for different scenarios.

Online Tool

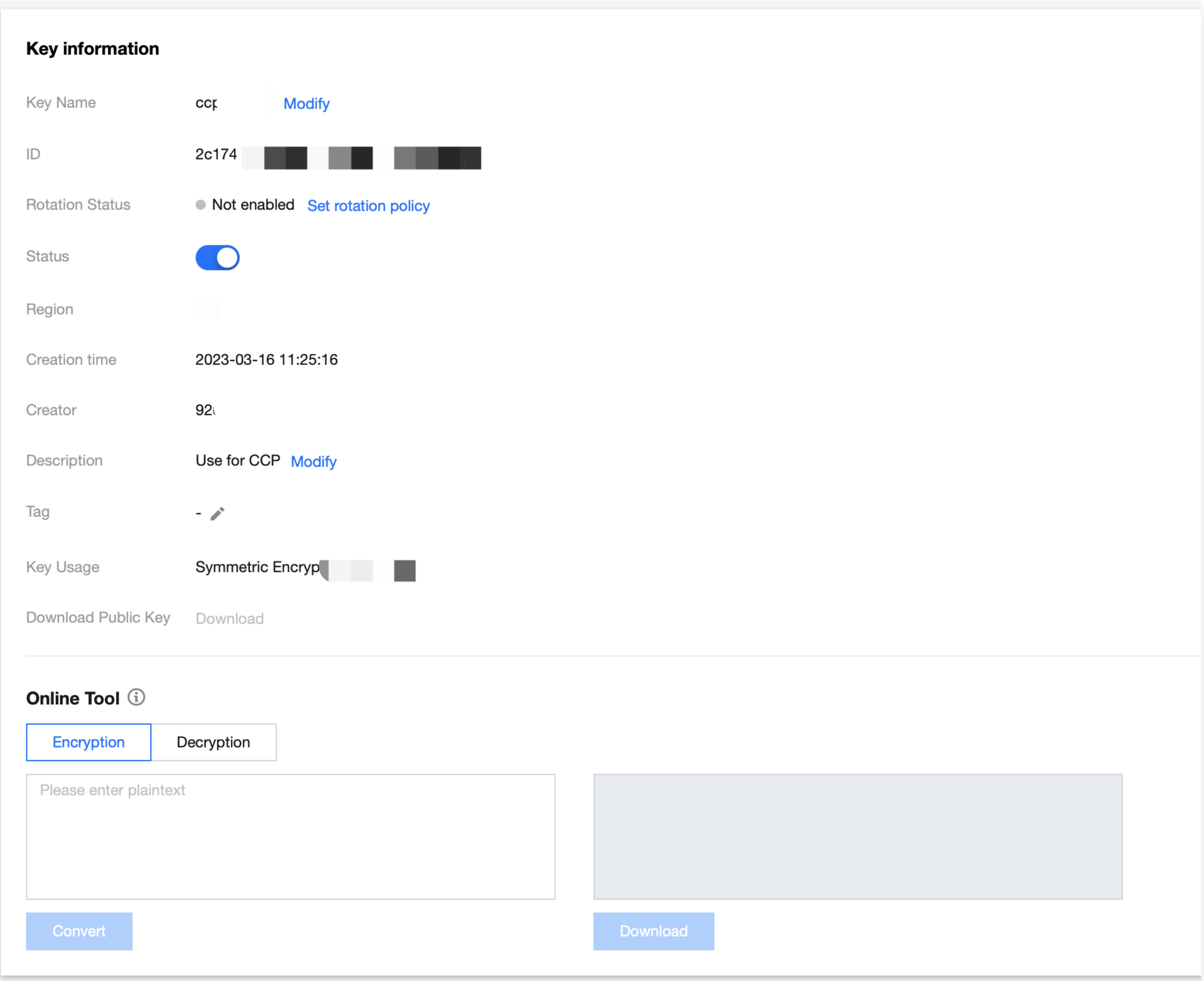
The online tools are suitable for one-time or non-batch encryption and decryption operations, such as the initial generation of key ciphertext. With the online tools, you can focus on your core business without developing tools for non-batch encryption and decryption. They can be used in the following steps:

Preparations

Ensure that you have created a key beforehand and that the key is in an enabled state.

Instructions

1. Log in to the Key Management System (Compliance) console.
2. Locate the key you need to encrypt or decrypt, and click **Key Name** under the "Key ID/Key Name" operation column to access the key details page.
3. In the "Online Tools" module, click **Encryption**.
4. Enter the data to be processed in the input box below.
5. Click **Execute**, and the processed data will be displayed in the gray box on the right.



Key information

Key Name	ccp Modify
ID	2c174 [redacted]
Rotation Status	● Not enabled Set rotation policy
Status	
Region	
Creation time	2023-03-16 11:25:16
Creator	92
Description	Use for CCP Modify
Tag	-
Key Usage	Symmetric Encryp [redacted]
Download Public Key	Download

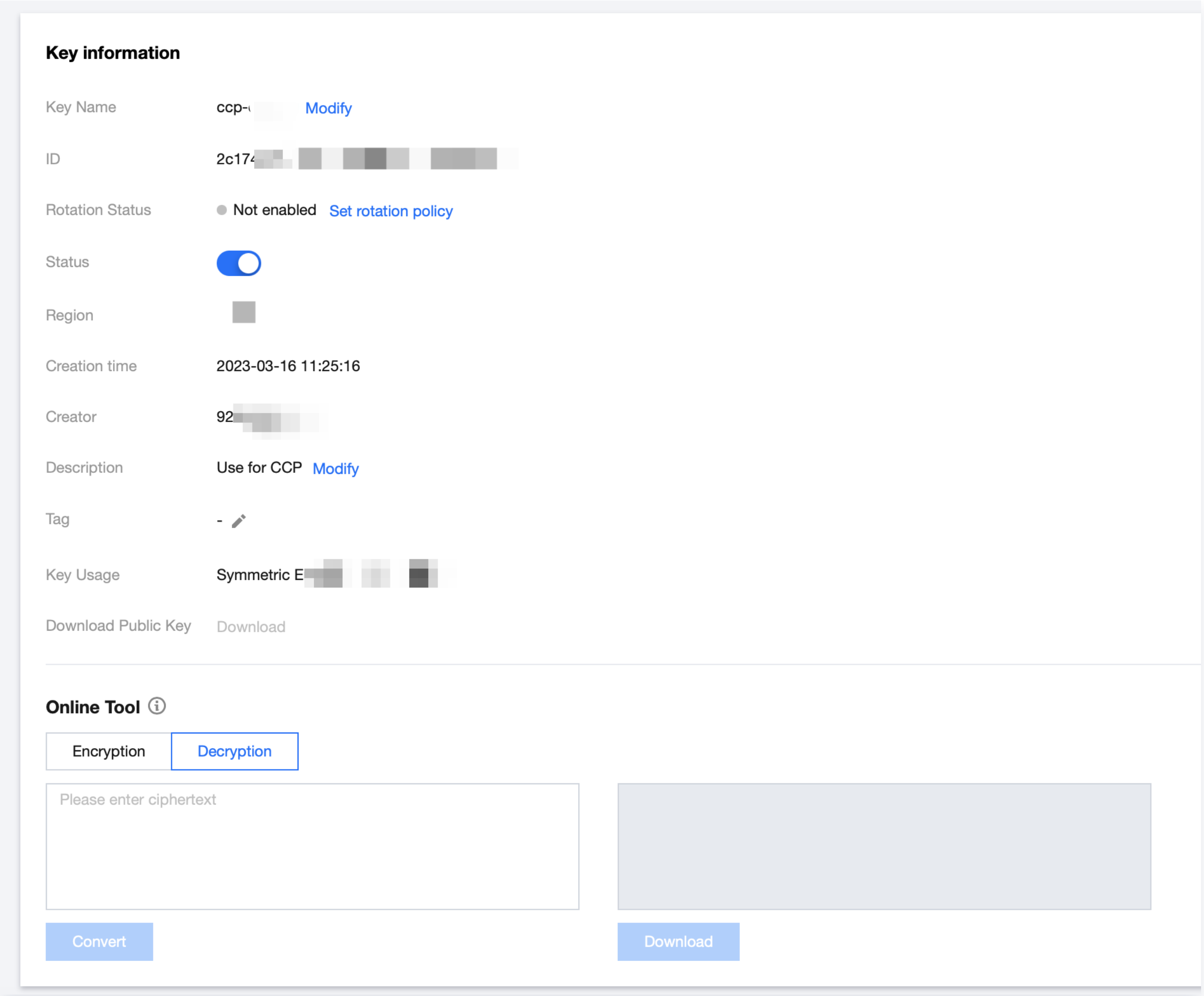
Online Tool

Encryption | Decryption

Please enter plaintext

Convert | Download

6. After encrypting the data, you can click **Download** to save the encrypted data to your local computer, completing the encryption process.
7. If decryption is needed, in the "Online Tools" module, click **Decryption**.
8. Paste the encrypted data into the input box below, click **Execute**, and the decrypted data will be displayed in the gray box on the right.



Key information

Key Name ccp-[redacted] Modify

ID 2c174[redacted]

Rotation Status ● Not enabled Set rotation policy

Status

Region [redacted]

Creation time 2023-03-16 11:25:16

Creator 92[redacted]

Description Use for CCP Modify

Tag -

Key Usage Symmetric E[redacted]

Download Public Key Download

Online Tool

> **Note**
>
> The decryption operation automatically calls the master key used by the ciphertext to perform the decryption. The decrypted plaintext is displayed in Base64 format.

9. You can click **Download** to save the decrypted data to your local computer.

Deleting Key

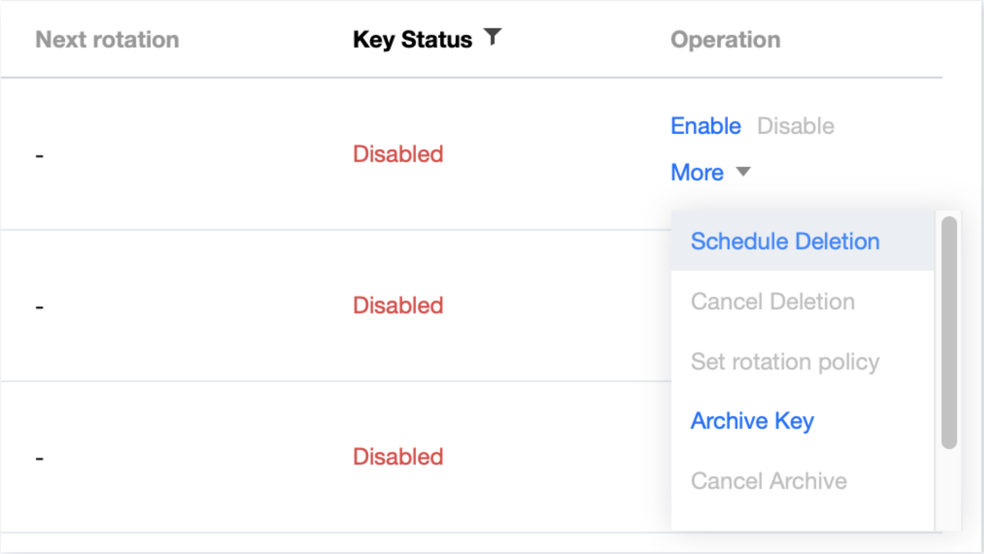
Last updated：2023-08-24 17:00:16

Scenario

Once a key is deleted, it cannot be recovered, and all encrypted data under this key will become irretrievable. To prevent accidental deletion, KMS employs a scheduled deletion mechanism, enforcing a mandatory waiting period of 7 to 30 days for deletion operations. During this waiting period, you can cancel the scheduled deletion of the key.
You can log in to the Tencent Cloud Key Management System (Compliance) Console or call KMS TCCLI to perform scheduled key deletion and cancel scheduled deletion operations. This document provides a detailed guide on how to delete a key through the console.

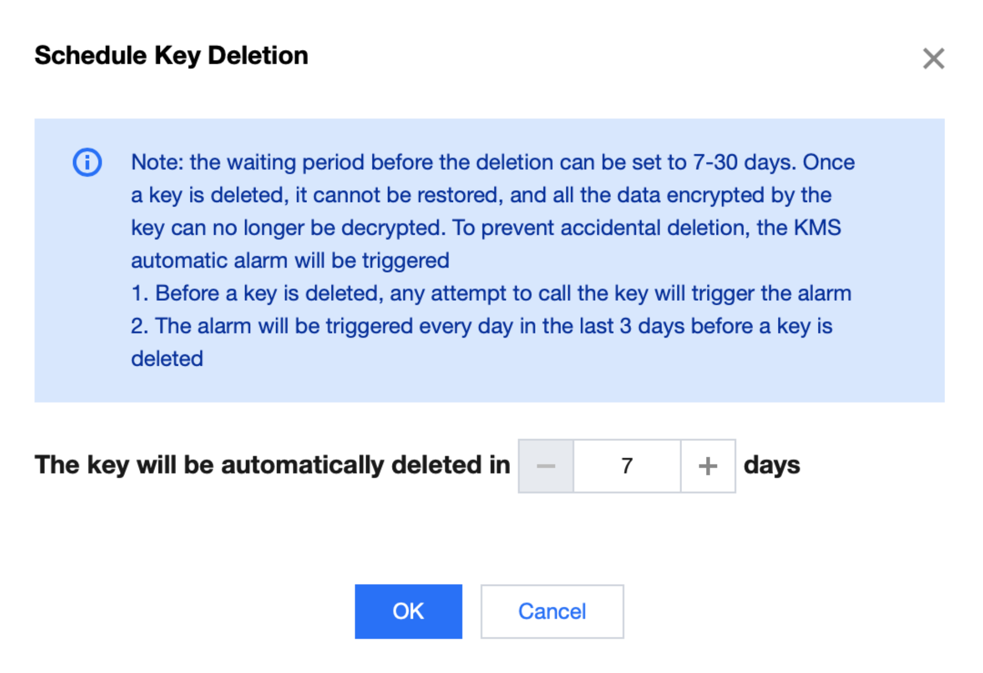
Instructions

1. Log in to the Key Management System (Compliance) console.
2. Select the key you want to schedule for deletion, and click **Schedule Deletion** on its right side. If the key is currently enabled, please disable it first.



Next rotation	Key Status	Operation
-	Disabled	Enable Disable More
-	Disabled	
-	Disabled	

3. Enter the number of days for the scheduled deletion and click **OK**. After confirming the scheduled deletion and the specified number of days, the key will be deleted as planned.



Schedule Key Deletion

Note: the waiting period before the deletion can be set to 7-30 days. Once a key is deleted, it cannot be restored, and all the data encrypted by the key can no longer be decrypted. To prevent accidental deletion, the KMS automatic alarm will be triggered
1. Before a key is deleted, any attempt to call the key will trigger the alarm
2. The alarm will be triggered every day in the last 3 days before a key is deleted

The key will be automatically deleted in 7 days

> **Note**
> The scheduled deletion period can be set between 7 and 30 days. Once a key is deleted, it cannot be recovered, and all encrypted data under this key will become irretrievable. To prevent accidental deletion, KMS service will automatically trigger alarms for the following operations:
> - An alarm will be triggered for any attempts to use the key before it is permanently deleted.
> - The alarm will be triggered daily for the last 3 days before a key is permanently deleted.

4. To cancel the key deletion, click **Cancel Deletion**. This will cancel the deletion of the key. Once the cancellation is confirmed, the key status will be reset to "Disabled," allowing you to enable, modify, or delete the key as needed.

Archive Key

Last updated：2023-08-24 16:59:50

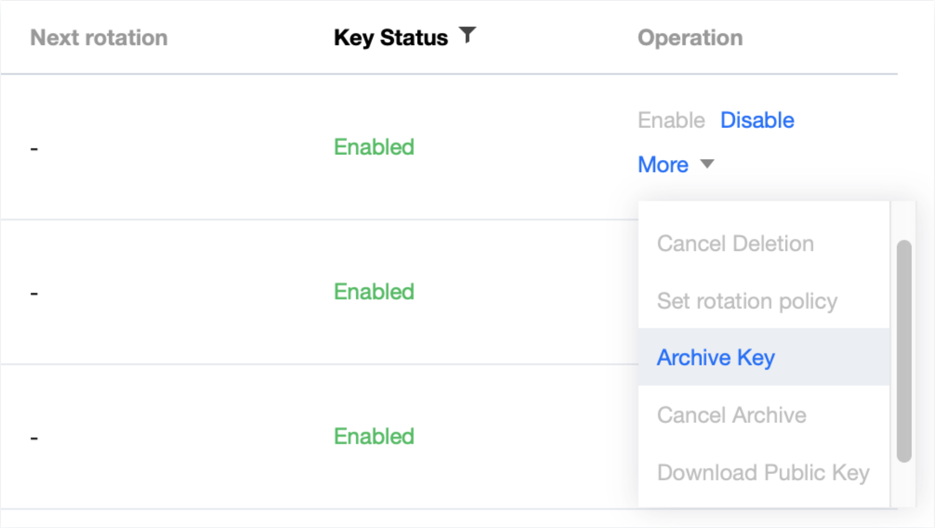
Scenario

Key archiving is a process where keys can only be decrypted but not encrypted. Tencent Cloud Key Management System (Compliant) KMS provides users with the ability to archive keys, enabling more comprehensive key management.

You can log in to the Tencent Cloud Key Management System (Compliant) or call KMS TCCLI to enable or disable key archiving for the created customer master keys. This document describes how to enable or disable key archiving through the console.

Instructions

1. Log in to the Key Management System (Compliance) console.
2. Locate the key for which you want to change the status. In the operation area on the right side of the key information, you can enable or disable key archiving.



Next rotation	Key Status	Operation
-	Enabled	Enable Disable More
-	Enabled	
-	Enabled	

> **Note**
>
> - Currently, the key archiving feature only supports **customer master keys not occupied by cloud products**; other keys are not supported.
> - The key archiving feature can only be used when the customer master key is in the **Enabled** or **Disabled** state; other states are not supported.
> - When the key archiving feature is enabled, the key is in the **Archived** state:
> - This key can only be used for **decryption** and not for **encryption.**
> - For this key, you can perform **scheduled deletion**, **cancel archiving**, and **edit labels** operations, but you cannot enable the **rotation** feature.

- When the customer master key is in the **archived** state, charges apply for its storage and invocation services.

Tag Management

Last updated：2023-08-24 17:00:49

Scenario

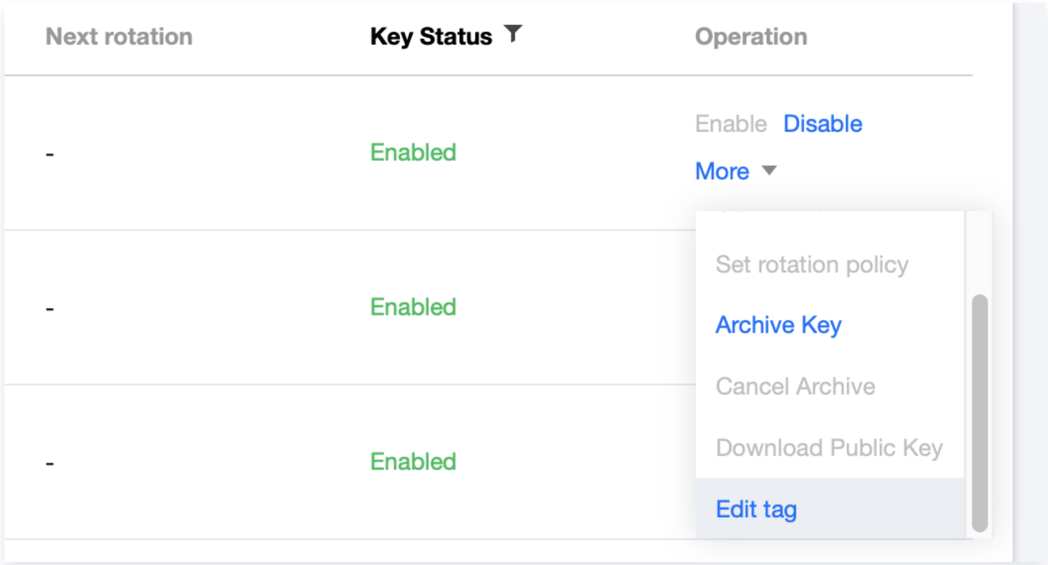
- Tag is used for resource categorization and permission management from different dimensions.
- In Key Management System (KMS), tags are primarily used to identify Customer Master Keys (CMKs).
- Adding tags to CMKs is intended to facilitate user classification and tracking management of CMKs, while also allowing for usage summaries of corresponding keys based on tags.

Usage Limits

There are corresponding restrictions on the usage of tag content (tag keys and tag values). For more information, please refer to Tag Usage Limits.

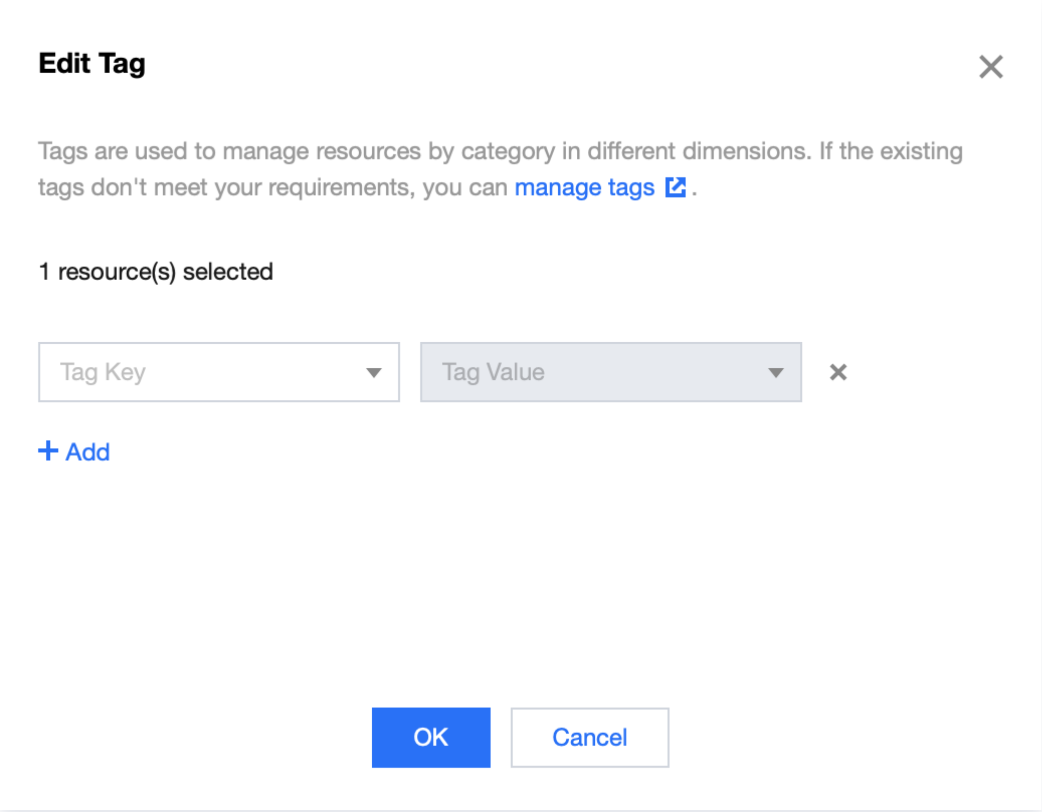
Add tag

1. Log in to the Key Management System console. In the left navigation pane, click **User Keys**.
2. Select the key to which you want to add a tag, click **More** on the right side of the key, and then click **Edit Tag** in the expanded operation options.



Next rotation	Key Status	Operation
-	Enabled	Enable Disable More ▾
-	Enabled	
-	Enabled	

3. In the **Edit Tags** pop-up window, you can see that one resource has been selected. Add or delete tags based on your actual needs. For example, add two sets of tags.



Edit Tag

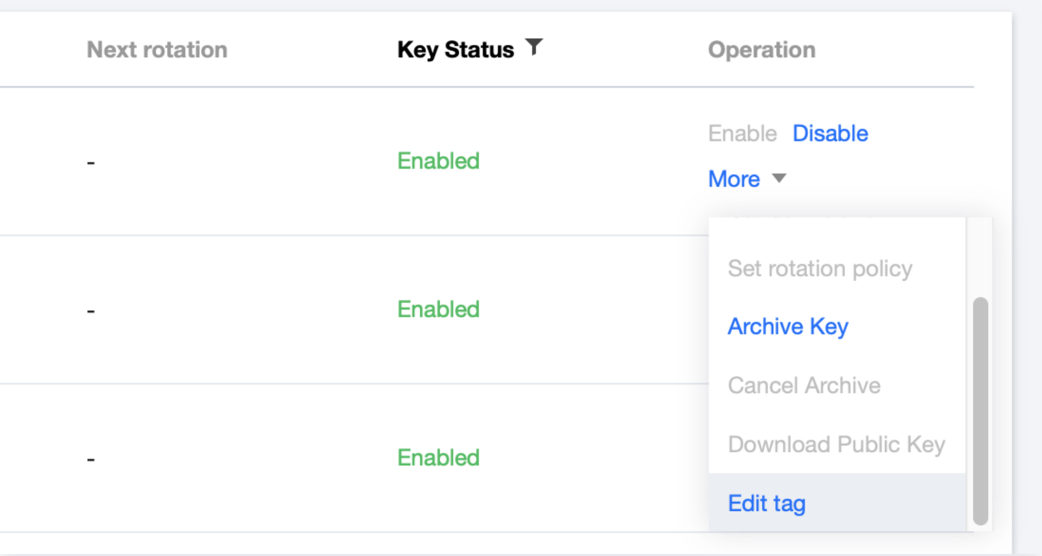
Tags are used to manage resources by category in different dimensions. If the existing tags don't meet your requirements, you can manage tags.

1 resource(s) selected

4. Click **OK**, and if the system displays a successful modification prompt, it indicates that the tag has been modified successfully.

Editing Tag

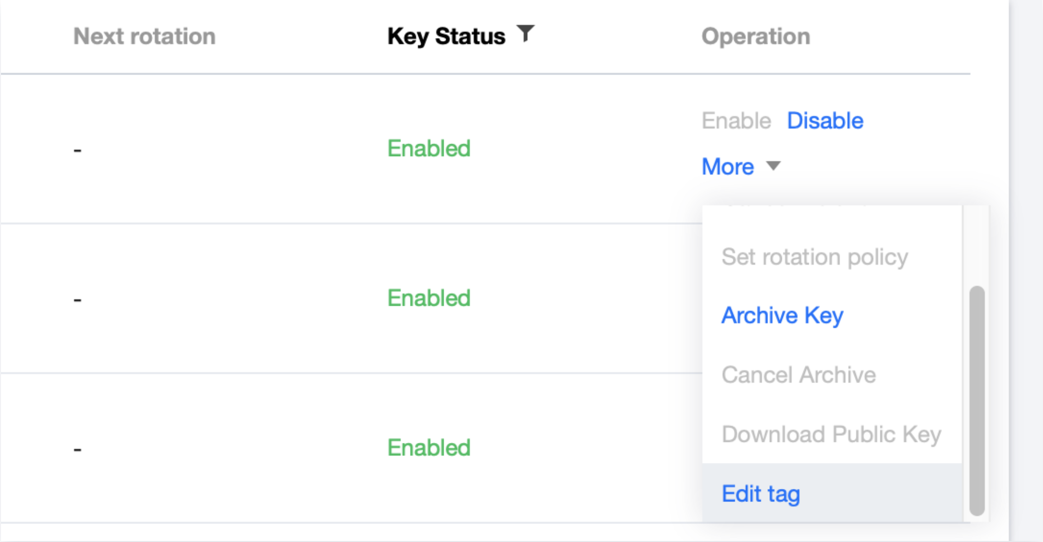
1. Log in to the Key Management System console. In the left navigation pane, click **User Keys**.
2. Select the key to which you want to add a tag, click **More** on the right side of the key, and then click **Edit Tag** in the expanded operation options.



Next rotation	Key Status	Operation
-	Enabled	Enable Disable More
-	Enabled	
-	Enabled	

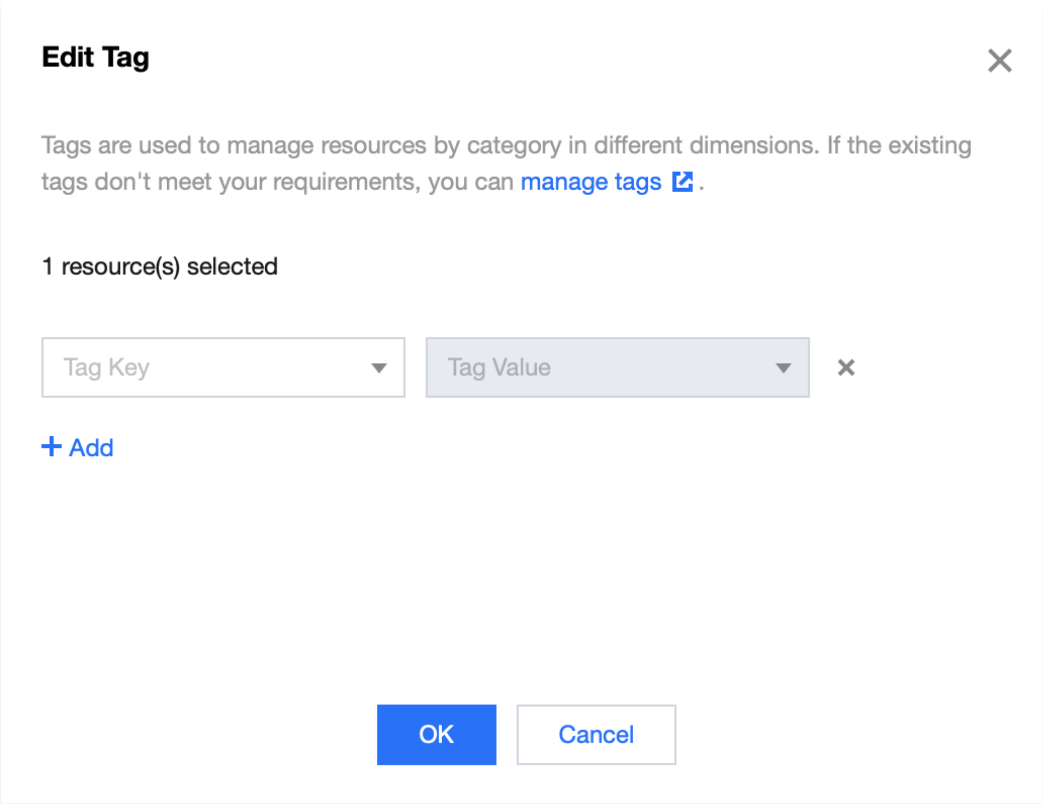
Editing a Single Tag

1. Select the key to which you want to add a tag, click **More** on the right side of the key, and then click **Edit Tag** in the expanded operation options.



Next rotation	Key Status	Operation
-	Enabled	Enable Disable More
-	Enabled	
-	Enabled	

2. In the **Edit Tags** pop-up window, you can see that 1 resource has been selected. Based on your actual needs, you can **add** or **delete** tags.



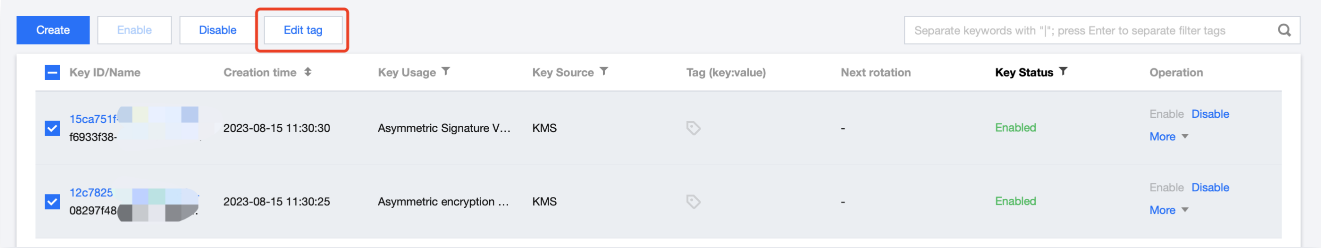
Edit Tag

Tags are used to manage resources by category in different dimensions. If the existing tags don't meet your requirements, you can manage tags.

1 resource(s) selected

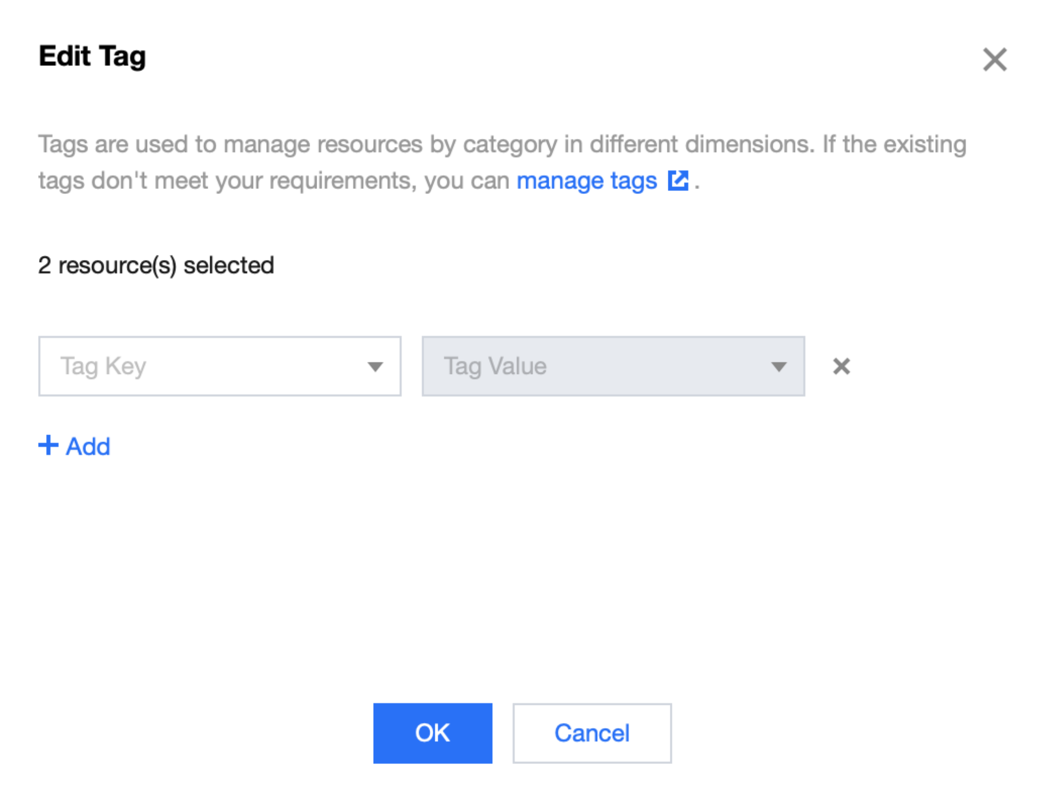
Editing the tags of multiple secrets

1. Select the key for which you want to edit the tag, and click **Edit Tag** at the top of the key.


Create
Enable
Disable
Edit tag
Separate keywords with "|"; press Enter to separate filter tags

☐	Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Next rotation	Key Status	Operation
☑	15ca751f [redacted] f6933f38-	2023-08-15 11:30:30	Asymmetric Signature V...	KMS		-	Enabled	Enable Disable More
☑	12c7825 [redacted] 08297f48	2023-08-15 11:30:25	Asymmetric encryption ...	KMS		-	Enabled	Enable Disable More

2. In the **Edit Tags** pop-up window, you can view the selected multiple resources and, based on actual needs, **add** or **delete** tags.



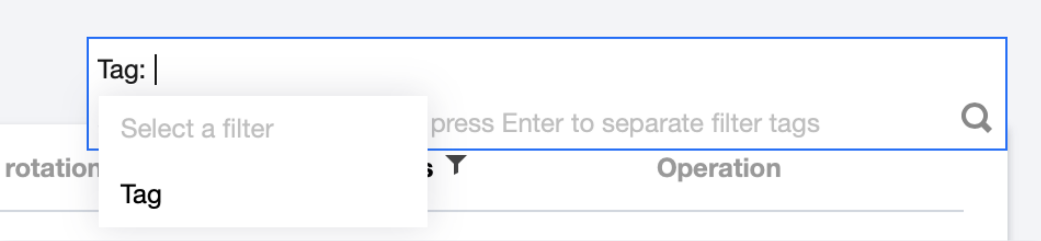
Edit Tag

Tags are used to manage resources by category in different dimensions. If the existing tags don't meet your requirements, you can manage tags .

2 resource(s) selected

Filtering keys with tags

1. Log in to the Key Management System console. In the left navigation pane, click **User Keys**.
2. Select **Tag** as the filter condition in the search box on the right, choose the tag key and tag value, then click **Confirm**.



Access Control
Overview

Last updated：2023-08-24 11:37:56

If you utilize services such as Key Management System (KMS), Virtual Private Cloud (VPC), Cloud Virtual Machine, and databases, which are managed by different individuals but all share your cloud account key, you may encounter the following issues:

- Your key will be easily compromised because it is shared by several users.
- Your users might introduce security risks from maloperations due to the lack of user access control.

Access Control (CAM) is used to manage access permissions for resources under Tencent Cloud accounts. With CAM, you can control which sub-accounts have access to specific resources through identity management and policy management.

For instance, if you have a master key under your root account and you only want sub-account A to use this master key while preventing sub-account B from using it, you can configure policies in CAM to control the permissions of the sub-accounts.

If you do not require access control for KMS-related resources for sub-accounts, you can skip this section. Skipping this part will not affect your understanding and usage of the remaining portions of the documentation.

Basic CAM Concepts

The root account authorizes sub-accounts by associating policies. The policy setting can be specific to the level of **(API, Resource, User/User Group, Allow/Deny, and Condition)**.

1. **Account**
    - **Root account:** The primary entity responsible for Tencent Cloud resource ownership, usage measurement, and billing, which can log in to Tencent Cloud services.
    - **Sub-account**: Created by the root account, a sub-account has a specific identity ID and credentials, and can log in to the Tencent Cloud console. The root account can create multiple sub-accounts (users).**By default, sub-accounts do not possess resources and must be authorized by their associated root account.**
    - **Identity Credentials**: These include login credentials and access certificates. **Login credentials** refer to the user's login name and password, while **Access certificates** pertain to the cloud API keys (SecretId and SecretKey).
2. **Resources and Permissions**
    - **Resource:** An object that is operated in Tencent Cloud services, such as a KMS master key, a CVM instance, a COS bucket, or a VPC instance.

- **Permission:** It is an authorization that allows or forbids users to perform certain operations. By default, the **root account** has full access to all resources under the account, while a **sub-account** does not have access to any resources under its root account.
- **Policy:** It is a syntax rule that defines and describes one or more permissions. The **root account** performs authorization by **associating policies** with users/user groups.

For more information, please refer to the CAM product documentation.

Documentation

Content	Document
Understand the relationship between policies and users	Policy Management
Understand the basic structure of policies	Policy Syntax
Check CAM-enabled products	CAM-Enabled Products

Managing Sub-Accounts

Last updated：2023-08-24 17:01:09

Overview

This document describes how to create a sub-account and grant it permission to manage KMS.

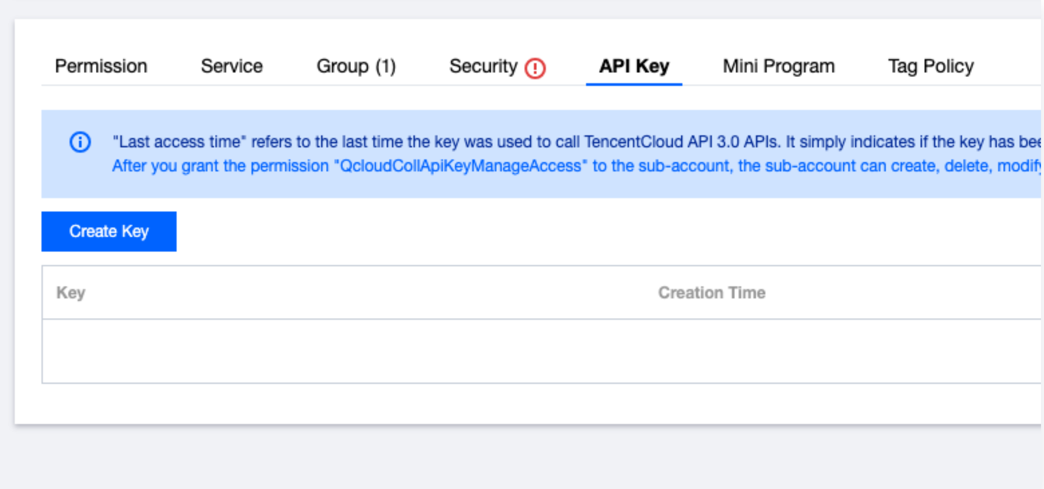
Instructions

Step 1: Create a Sub-account

1. Log in to the Tencent Cloud Access Management (CAM) console with the primary account.
2. On the user list page, click **Create User** to create a sub-account.

Step 2: Create an API Key

1. Click the sub-account name to enter the sub-account details page.
2. Select **API Key** > **Create Key** to generate a SecretId and SecretKey. This API key will be used to access KMS.

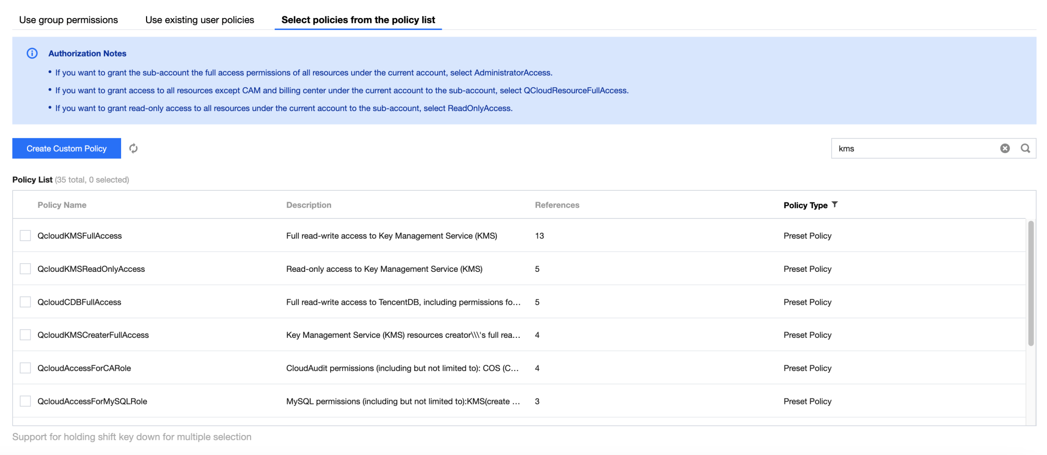


"Last access time" refers to the last time the key was used to call TencentCloud API 3.0 APIs. It simply indicates if the key has bee
After you grant the permission "QcloudCollApiKeyManageAccess" to the sub-account, the sub-account can create, delete, modif

Step 3: Grant permissions to the sub-account

The newly created sub-account can be granted with the access to KMS by associating a KMS policy.

1. Select **Permissions** > **Assign Policy** > **Choose a policy from the list**, and select the appropriate KMS policy.



Use group permissions
Use existing user policies
Select policies from the policy list

Authorization Notes

- If you want to grant the sub-account the full access permissions of all resources under the current account, select AdministratorAccess.
- If you want to grant access to all resources except CAM and billing center under the current account to the sub-account, select QCloudResourceFullAccess.
- If you want to grant read-only access to all resources under the current account to the sub-account, select ReadOnlyAccess.

Policy List (35 total, 0 selected)

	Policy Name	Description	References	Policy Type
□	QcloudKMSFullAccess	Full read-write access to Key Management Service (KMS)	13	Preset Policy
□	QcloudKMSReadOnlyAccess	Read-only access to Key Management Service (KMS)	5	Preset Policy
□	QcloudCDBFullAccess	Full read-write access to TencentDB, including permissions fo...	5	Preset Policy
□	QcloudKMSCreaterFullAccess	Key Management Service (KMS) resources creator\\\'s full rea...	4	Preset Policy
□	QcloudAccessForCARole	CloudAudit permissions (including but not limited to): COS (C...	4	Preset Policy
□	QcloudAccessForMySQLRole	MySQL permissions (including but not limited to):KMS(create ...	3	Preset Policy

Support for holding shift key down for multiple selection

2. Click **Next** > **OK** to grant KMS permissions to the sub-account.

Creating an Access Control Policy

Last updated: 2023-08-24 17:01:20

Types of Manageable Resources

Resource-level permission allows specifying which resources a user has the ability to perform operations on. Some Key Management System (KMS) interfaces support using resource-level permissions for key operations, controlling when users are allowed to perform actions or whether they can use specific resources. The current resource types that can be authorized in KMS are as follows:

ResourceType	Resource Description Method in Authorization Policy
All Key Resources	`qcs::kms:$region:uin/$uin:key/*`
All Key Resources Created by Account $creatorUin	`qcs::kms:$region:uin/$uin:key/creatorUin/$creatorUin/*`
Key resource with ID $keyId created by account $creatorUin	`qcs::kms:$region:uin/$uin:key/creatorUin/$creatorUin/$keyId`

Words with a $ prefix are used as aliases:
- $uin refers to the root account ID.
- $region represents the region.
- `$creatorUin` refers to the account ID that created the resource.
- $keyId refers to the Key ID.

List of APIs supporting resource-level authorization

KMS supports resource-level authorization for some interfaces. You can grant a specified sub-account the API permission of a specific resource.

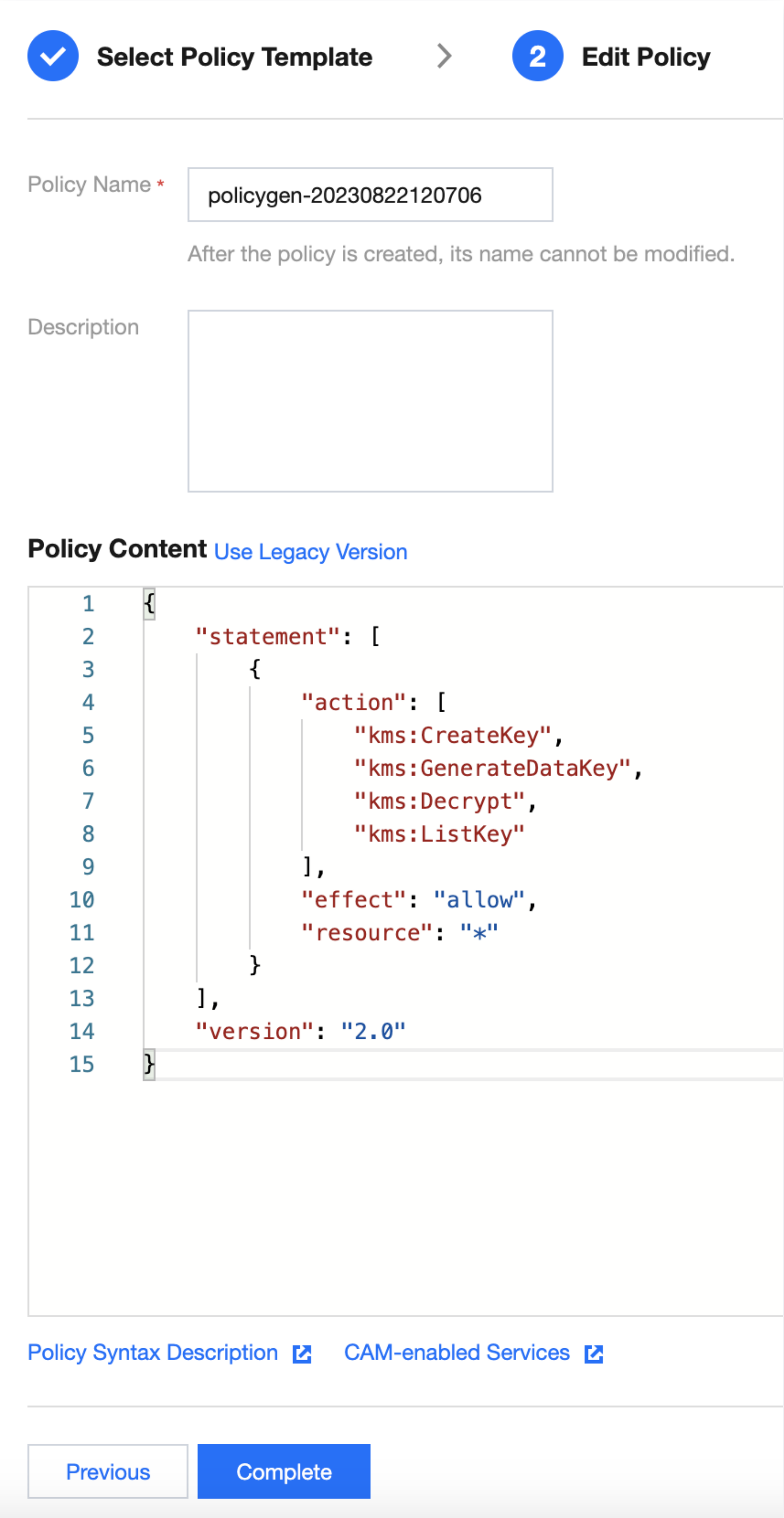
Related APIs	Description
DescribeWhiteBoxKeyDetails	Gets the white-box key list
EnableWhiteBoxKeys	Batch enabling white-box keys
DeleteWhiteBoxKe	Deleting a white-box key

y	
DescribeWhiteBoxKey	This API is used to display white-box key information.
EnableWhiteBoxKey	This API is used to enable a white-box key.
EncryptByWhiteBox	This API is used to encrypt data with a white-box key.
DescribeWhiteBoxDecryptKey	This API is used to get a white-box decryption key.
DisableWhiteBoxKey	This API is used to disable a white-box key.
AsymmetricSm2Decrypt	Using SM2 to decrypt data with asymmetric keys
AsymmetricRsaDecrypt	Using RSA to decrypt data with asymmetric keys
GetPublicKey	Gets the information of the public key that is encrypted with the asymmetric cryptographic algorithm
EnableKey	Activate the Customer Master Key (CMK)
DisableKey	Disable Master Key
GetKeyRotationStatus	Querying key rotation status
ReEncrypt	VerifyByAsymmetricKey
DisableWhiteBoxKeys	Displaying White-box Key Information in Bulk
UpdateKeyDescription	Modifying CMK Description
UpdateAlias	Modify Alias
Disable Key Rotation	Disable Key Rotation
Enable Key Rotation	Enable Key Rotation

EnableKeys	Batch Enable CMKs
DisableKeys	Batch Disabling CMKs
DescribeKey	Retrieving CMK Attributes
DescribeKeys	Getting attributes of multiple CMKs
CancelKeyDeletion	Cancel CMK Scheduled Deletion Operation
ScheduleKeyDeletion	CMK Scheduled Deletion API
DeleteImportedKeyMaterial	Deletes imported key material
ImportKeyMaterial	Imports key material
GetParametersForImport	Getting the parameters of the key material imported to a CMK
GenerateDataKey	Generating a DEK
Decrypt	Decrypt
Encrypt	Encryption

Create policy

1. Log in to the Access Management Console.
2. In the left sidebar, select **Policies** > **Create Custom Policy** > **Create by Policy Syntax** to access the policy creation page.
3. Select a policy template, such as a Blank Template or KMS Policy Template, and click **Next**.
4. Enter the policy name and policy content, referring to the example provided below for the policy content.



Policy Name * policygen-20230822120706

After the policy is created, its name cannot be modified.

Description

Policy Content Use Legacy Version

```
{
    "statement": [
        {
            "action": [
                "kms:CreateKey",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:ListKey"
            ],
            "effect": "allow",
            "resource": "*"
        }
    ],
    "version": "2.0"
}
```

5. Click **Create Policy** to create.

Audit

Operations Logged by CloudAudit

Last updated：2023-08-24 11:38:53

In Tencent Cloud's CloudAudit service, related operation events of the Key Management System service are recorded. The operations supported by CloudAudit are as follows:

Operation Name	Event name
Creating a CMK	CreateKey
Retrieving CMK Attributes	DescribeKey
Getting attributes of multiple CMKs	DescribeKeys
This example shows you how to get the list of CMKs.	ListKey
Getting CMK list details	ListKeyDetail
Modifying CMK Description	UpdateKeyDescription
Modify Alias	UpdateAlias
Enable the Customer Master Key (CMK)	EnableKey
Disable Master Key	DisableKey
Batch Enable CMKs	EnableKeys
Batch Disabling CMKs	DisableKeys
Scheduling CMK Deletion	ScheduleKeyDeletion
Disable Key Deletion Schedule	CancelKeyDeletion
Getting the parameters of the key material imported to a CMK	GetParametersForImport
Imports key material	ImportKeyMaterial
Creating a white-box key	CreateWhiteBoxKey
This API is used to encrypt data with a white-box key.	EncryptByWhiteBox
This API is used to enable a white-box key.	EnableWhiteBoxKey

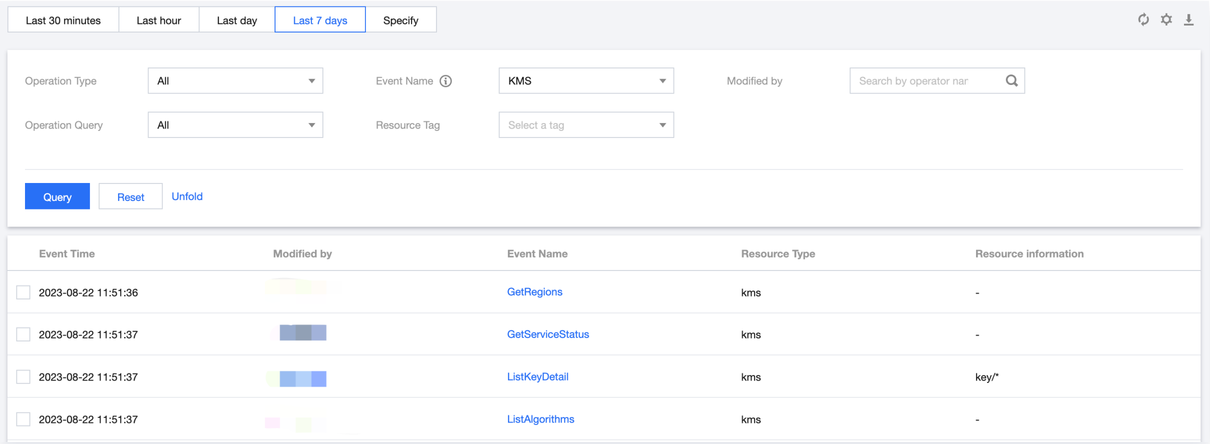
This API is used to disable a white-box key.	DisableWhiteBoxKey
Batch enabling white-box keys	EnableWhiteBoxKeys
Batching disabling white-box keys	DisableWhiteBoxKeys
Deleting a white-box key	DeleteWhiteBoxKey
Querying the white-box key service status	DescribeWhiteBoxServiceStatus
Overwriting the device fingerprint information of a specified key	OverwriteWhiteBoxDeviceFingerprints
This API is used to get the device fingerprint list of a specified key.	DescribeWhiteBoxDeviceFingerprints
This API is used to get a white-box decryption key.	DescribeWhiteBoxDecryptKey
Decrypt	Decrypt
Encryption	Encrypt
Signature	SignByAsymmetricKey
Verify Signature	VerifyByAsymmetricKey
Key Archiving	ArchiveKey
Canceling Key Archival	CancelKeyArchive
Obtaining Available Service Regions	GetRegions
VerifyByAsymmetricKey	ReEncrypt
Generates a random number	GenerateRandom
Generating a DEK	GenerateDataKey
This example shows you how to query service status.	GetServiceStatus
Listing Supported Encryption Methods in the Current Region	ListAlgorithms
DisableKeyRotation	DisableKeyRotation
EnableKeyRotation	EnableKeyRotation
Querying key rotation status	GetKeyRotationStatus

Binds a key with a Tencent Cloud resource	BindCloudResource
Unbinding the association between CMK and cloud resources	UnbindCloudResource
Gets the information of the public key that is encrypted with the asymmetric cryptographic algorithm	GetPublicKey
Using SM2 to decrypt data with asymmetric keys	AsymmetricSm2Decrypt
Using RSA to decrypt data with asymmetric keys	AsymmetricRsaDecrypt

Viewing Audit Logs

Last updated：2023-08-24 17:01:40

1. Log in to the CloudAudit Console.
2. Click **Event history** in the left sidebar to enter the event history page.
3. On the event history page, you can retrieve relevant operation records based on the username, resource type, resource name, event source, event ID, keyword, or corresponding event time. By default, only a portion of the data is displayed.

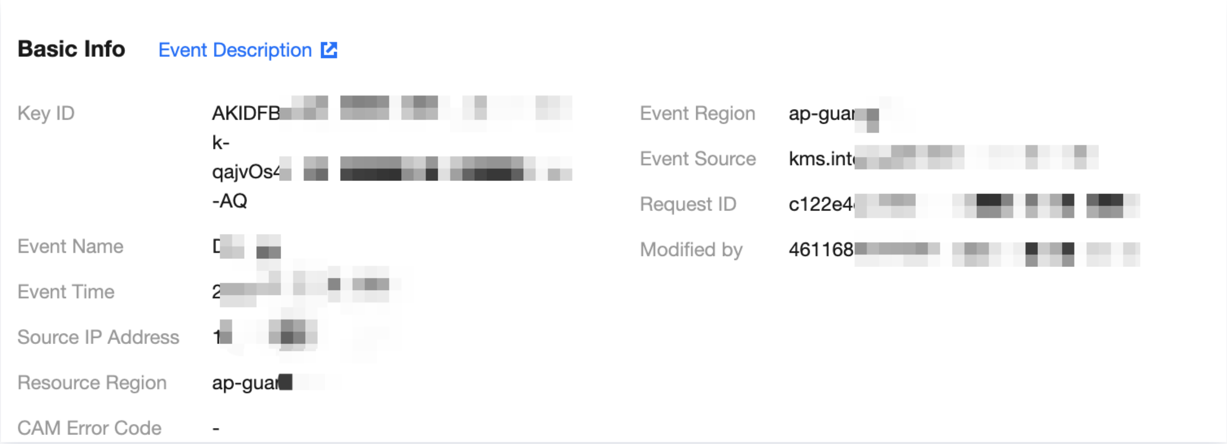


Last 30 minutes | Last hour | Last day | Last 7 days | Specify

Operation Type: All
Event Name: KMS
Modified by: Search by operator nar
Operation Query: All
Resource Tag: Select a tag

	Event Time	Modified by	Event Name	Resource Type	Resource information
□	2023-08-22 11:51:36	[redacted]	GetRegions	kms	-
□	2023-08-22 11:51:37	[redacted]	GetServiceStatus	kms	-
□	2023-08-22 11:51:37	[redacted]	ListKeyDetail	kms	key/*
□	2023-08-22 11:51:37	[redacted]	ListAlgorithms	kms	-

4. After obtaining the relevant operation record list, click the expand button on the left side of the record to view its details, including event time, username, event name, access key, event ID, etc. Click **View Event** to learn more about the event.



Basic Info Event Description

Key ID	AKIDFB[redacted] k- qajvOs[redacted] -AQ	Event Region	ap-guar[redacted]
Event Name	D[redacted]	Event Source	kms.int[redacted]
Event Time	2[redacted]	Request ID	c122e4[redacted]
Source IP Address	1[redacted]	Modified by	461168[redacted]
Resource Region	ap-guar[redacted]		
CAM Error Code	-		

Dedicated HSM Key Management Overview

Last updated：2023-08-24 17:01:51

The Dedicated Key Management System (KMS) is an exclusive cloud-based key management service with a dedicated physical Hardware Security Module (HSM). Encryption operations are performed within the exclusive physical HSM, which also possesses a dedicated cryptographic resource pool.

> **Note**
> For purchase information on the Dedicated version, see Billing Overview.

Advantages

- **Security:** When invoking KMS encryption, all cryptographic operations are performed within your dedicated physical HSM, ensuring physical isolation of your resources and encryption operations from other tenants.
- **High Performance:** KMS Dedicated version offers exclusive, high-performance encryption instances with dedicated HSM resources.
- **Reliability:** The dedicated encryption device is isolated from shared encryption device instances, ensuring that failures in the shared resource pool do not affect the exclusive encryption resource pool.
- **Flexibility:** Users can customize the size of the HSM resource pool according to their performance and reliability requirements.

Instruction

- **Key Management**
- **Create Key**
- **Edit Key**
- **View Key**
- **Key Archiving**
- **Key Rotation**
- **Enable/Disable Key**
- **Delete Key**
- **Encryption and Decryption**
- **Tag Management**

Key Management
Creating Key

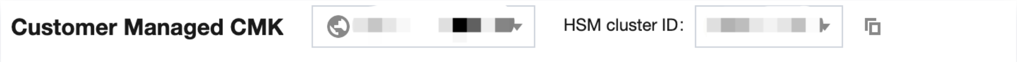
Last updated：2023-08-24 17:23:51

Scenario

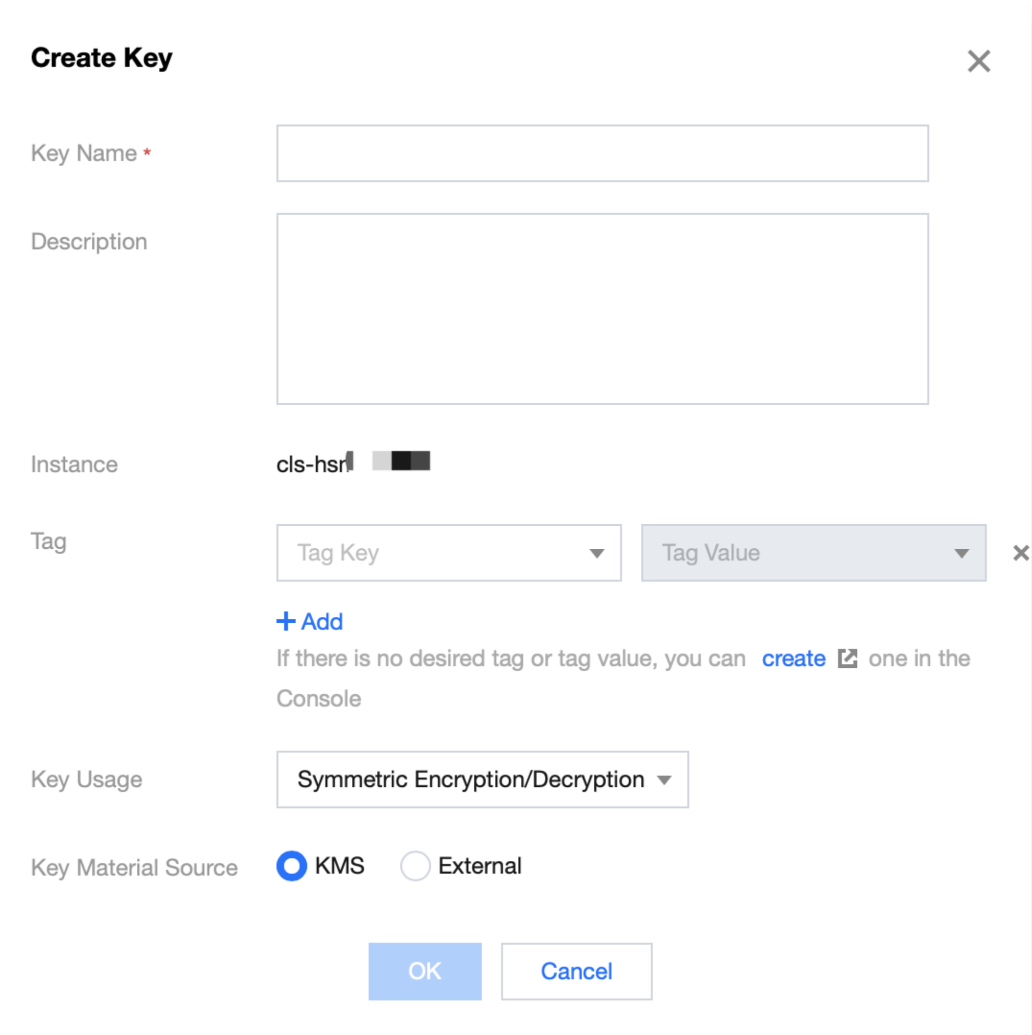
You can create a CMK in the Tencent Cloud KMS Console or by using the CreateKey API. Once created, you can enable, disable, rotate, and manage permissions for the CMK. This document describes how to create a CMK through the console.

Instructions

1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu, select the region and HSM cluster ID where you want to create the key, and click **Create**.



3. In the pop-up configuration window, configure the relevant parameters.



Create Key

Key Name *

Description

Instance cls-hsr[redacted]

Tag

If there is no desired tag or tag value, you can create one in the Console

Key Usage: Symmetric Encryption/Decryption

Key Material Source: ● KMS ○ External

Parameter description:

- Key Name: This is required and must be unique within the region. It can contain letters, numbers, `_`, `-`, and cannot begin with "KMS-".
- Description: Optional, used to describe the type of data you plan to protect or the application intended to be used in conjunction with the CMK.
- Encryption Instance ID: Required, select the HSM cluster ID needed to create the key.
- Tags: Optional, Tags are resource management tools provided by Tencent Cloud, allowing users to categorize, search, and aggregate keys by adding tags.
- Key Usage: This is required and supports symmetric encryption and decryption, asymmetric encryption and decryption, or asymmetric signature verification.
- Key Material Source: Required, choose the key generation method, either KMS-generated or user-imported key material.

> **Note**
> When the key material is sourced externally, only symmetric encryption and decryption purposes are supported.

4. After clicking **Confirm**, you will return to the Key List, and the newly created key will appear at the top of the list.

Editing Key

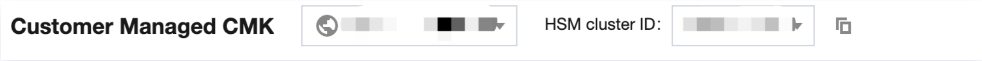
Last updated：2023-08-24 17:02:49

Scenario

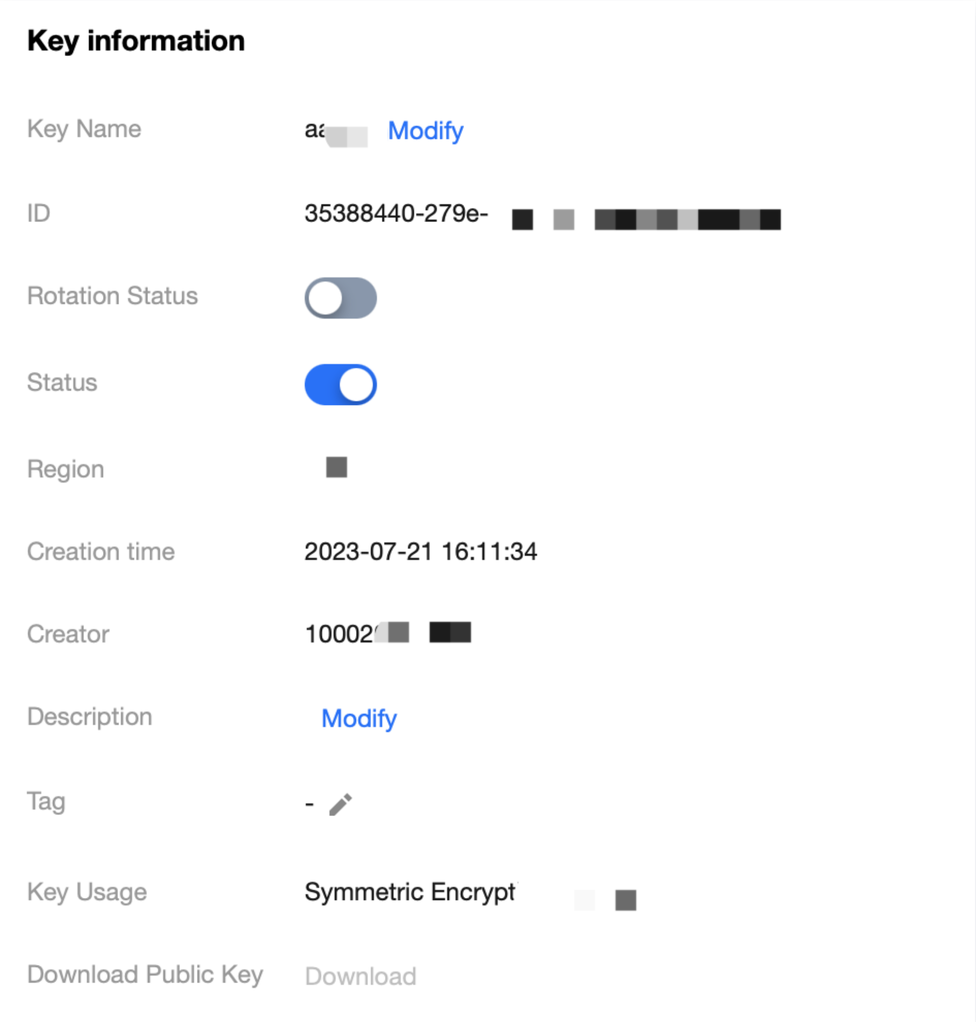
You can edit the Customer Master Key (CMK) in the Tencent Cloud Key Management System (KMS) Console or by calling KMS TCCLI. You can modify the description and enable or disable key rotation. This document provides a detailed guide on how to edit the CMK through the console.

Instructions

1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu, and select the region and HSM cluster ID for the key you want to edit.



3. Click the **ID/Name** of the key you want to edit to enter its details page, where you can modify the key's name, status, rotation settings, and description, among other things.



Key information

Key Name a[redacted] Modify

ID 35388440-279e-[redacted]

Rotation Status

Status

Region [redacted]

Creation time 2023-07-21 16:11:34

Creator 10002[redacted]

Description Modify

Tag -

Key Usage Symmetric Encrypt [redacted]

Download Public Key Download

4. Click **OK** for the changes to take effect.

Viewing keys

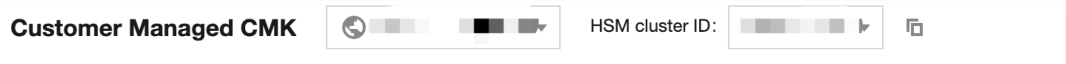
Last updated：2023-08-24 17:32:34

Scenario

You can log in to the Tencent Cloud Key Management System (Compliant) Console or call KMS TCCLI to view the CMK ID information list, name, ID, status, region, and other key details. This document introduces how to view the CMK ID information list and details through the console.

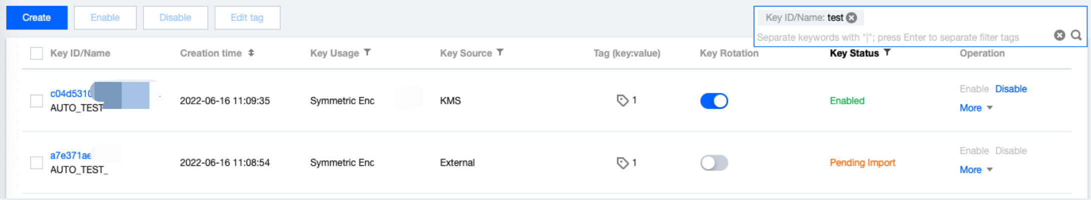
Viewing Key ID List

1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu, and select the region and HSM cluster ID for the key you want to view.



Customer Managed CMK [redacted] HSM cluster ID: [redacted]

3. In the filter box on the right side of the page, enter the full or partial name of the CMK or the key ID to filter and find your key.



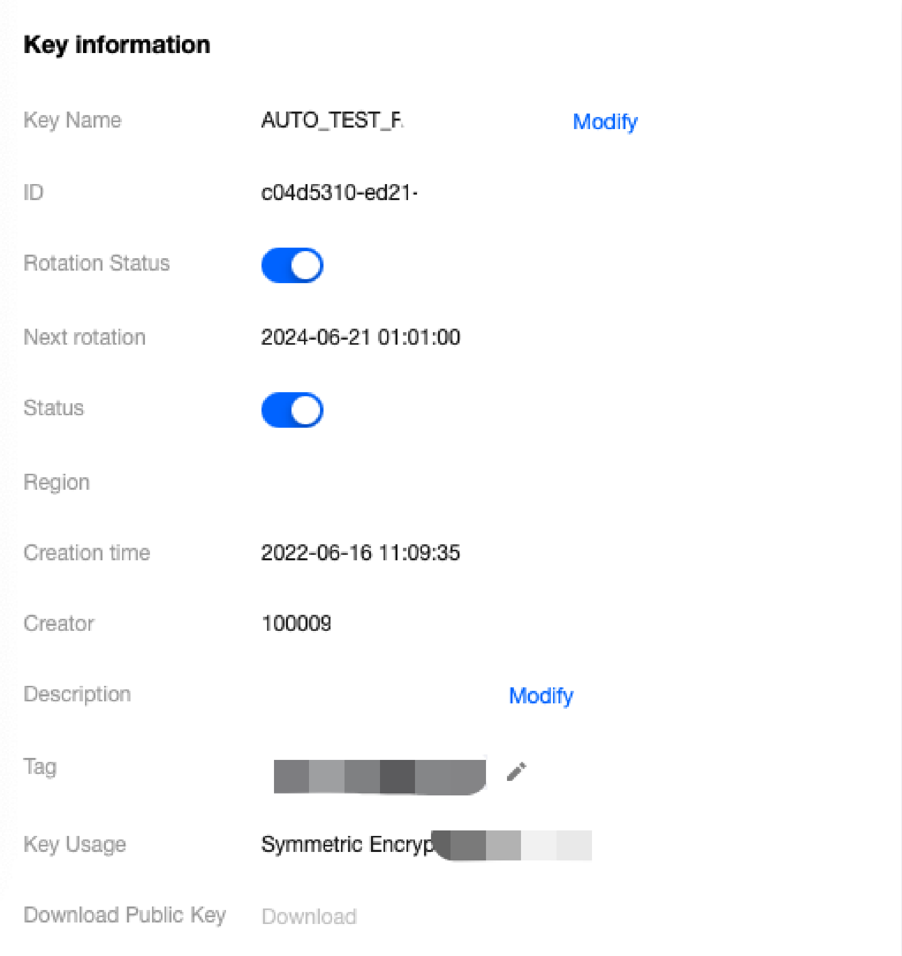
Key ID/Name: test

Separate keywords with "|"; press Enter to separate filter tags

□	Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Key Rotation	Key Status	Operation
□	c04d531[redacted] AUTO_TEST	2022-06-16 11:09:35	Symmetric Enc	KMS	1	●	Enabled	Enable Disable More
□	a7e371ae AUTO_TEST_	2022-06-16 11:08:54	Symmetric Enc	External	1	○	Pending Import	Enable Disable More

Viewing Key ID Details

1. Log in to the Key Management System (Compliance) console.
2. Locate the key for which you need to view details. For detailed methods on finding keys, please refer to Viewing Key ID List.
3. Click the key's **ID/Key Name** to view the detailed information of the key.



Key information

Key Name	AUTO_TEST_F.	Modify
ID	c04d5310-ed21-	
Rotation Status	●	
Next rotation	2024-06-21 01:01:00	
Status	●	
Region		
Creation time	2022-06-16 11:09:35	
Creator	100009	
Description		Modify
Tag	[redacted]	
Key Usage	Symmetric Encryp [redacted]	
Download Public Key	Download	

Archive Key

Last updated：2023-08-24 17:13:26

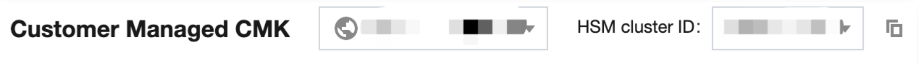
Scenario

Key archiving is a process where keys can only be decrypted but not encrypted. Tencent Cloud Key Management System (Compliant) KMS provides users with the ability to archive keys, enabling more comprehensive key management.

You can log in to the Tencent Cloud Key Management System (Compliant) or call KMS TCCLI to enable or disable key archiving for the created customer master keys. This document describes how to enable or disable key archiving through the console.

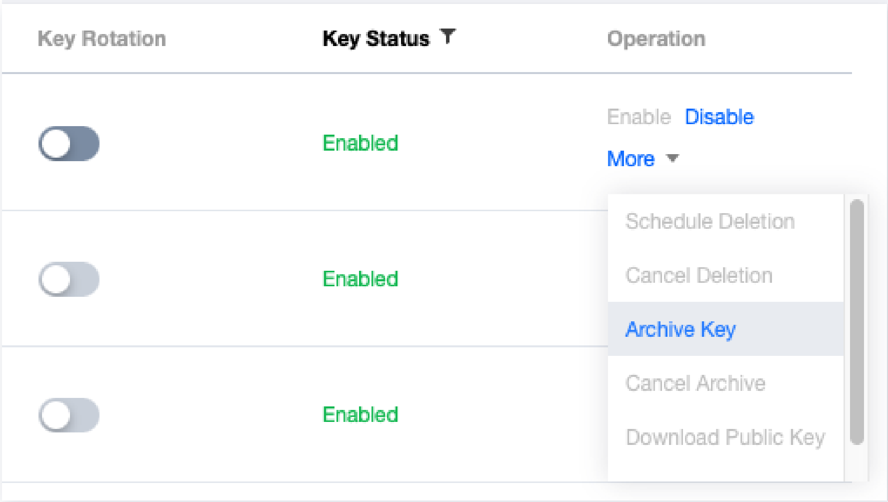
Instructions

1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu, and select the key region and HSM cluster ID.



Customer Managed CMK [redacted] HSM cluster ID: [redacted]

3. Locate the key for which you want to change the status. In the operation area on the right side of the key information, you can enable or disable key archiving.



Key Rotation	Key Status	Operation
●	Enabled	Enable Disable More ▾
○	Enabled	
○	Enabled	

> **Note**
> - Currently, the key archiving feature only supports customer master keys that are not occupied by cloud products; other keys are not supported.
> - The key archiving feature can only be used when the customer master key is in the enabled or disabled state; other states are not supported.

- When the key archiving feature is enabled and the key is in the archived state:
  - This key can only be used for decryption and not for encryption.
  - The key can be scheduled for deletion, unarchived, and have its labels edited, but the rotation feature cannot be enabled.
  - When a customer master key is in the archived state, its storage and invocation services are subject to billing.

Key Rotation

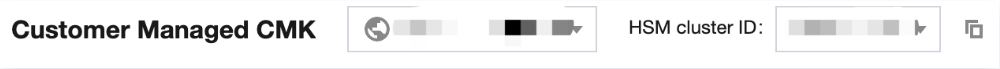
Last updated：2023-08-24 17:04:11

Scenario

To further enhance the security of encrypted data storage, Tencent Cloud Key Management System (KMS) provides users with transparent key rotation capabilities to refresh stored ciphertext. CMK key rotation offers transparent key rotation without affecting user operations and is compatible with ciphertext encrypted before rotation. Additionally, the ReEncrypt interface is available for ciphertext refreshing. This document describes how to enable key rotation through the console.

Instructions

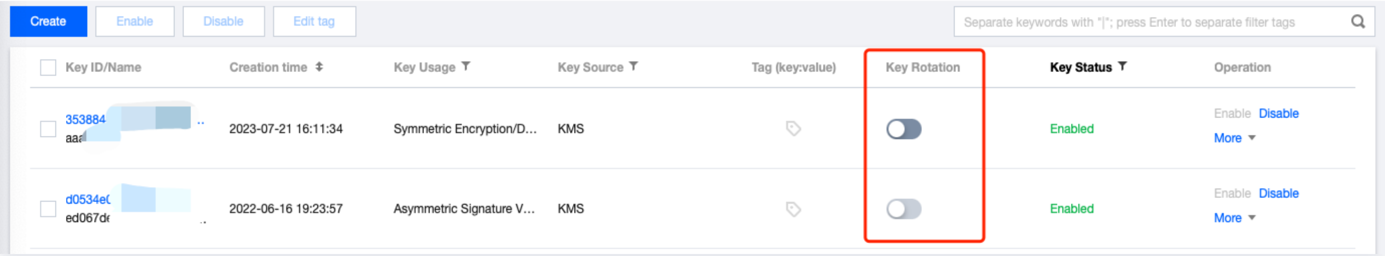
1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu, and select the key region and HSM cluster ID.



Customer Managed CMK [redacted] HSM cluster ID: [redacted]

3. Locate the key for which you want to enable rotation, and in the "Key Rotation" column on the right, click **Enable Rotation** to enable rotation for that key.

> **Note**
> By default, key rotation is disabled. You can choose whether to enable it. Once enabled, the CMK will rotate once a year.



Create
Enable
Disable
Edit tag
Separate keywords with "|"; press Enter to separate filter tags

Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Key Rotation	Key Status	Operation
353884 [redacted] aa [redacted]	2023-07-21 16:11:34	Symmetric Encryption/D...	KMS			Enabled	Enable Disable More
d0534e [redacted] ed067d [redacted]	2022-06-16 19:23:57	Asymmetric Signature V...	KMS			Enabled	Enable Disable More

Enabling/Disabling Key

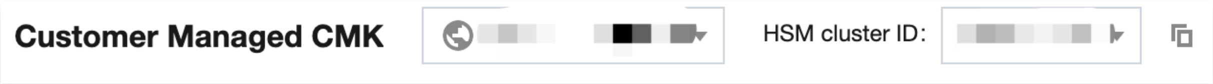
Last updated：2023-08-24 17:04:25

Scenario

You can log in to the Tencent Cloud Key Management System (Compliant) Console or call KMS TCCLI to enable/disable the status of created Customer Master Keys (CMKs). This document introduces how to enable/disable keys through the console.

Instructions

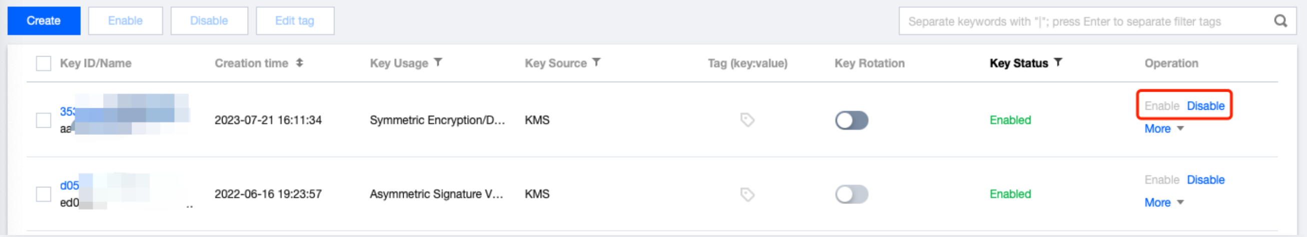
1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu. Select the key's region and HSM cluster ID. You can view the master key list of other regions by switching the region and cluster ID at the top.



Customer Managed CMK [redacted] HSM cluster ID: [redacted]

Single operation

Locate the key for which you need to change the status. In the operation area on the right side of the key information, you can enable or disable the key.



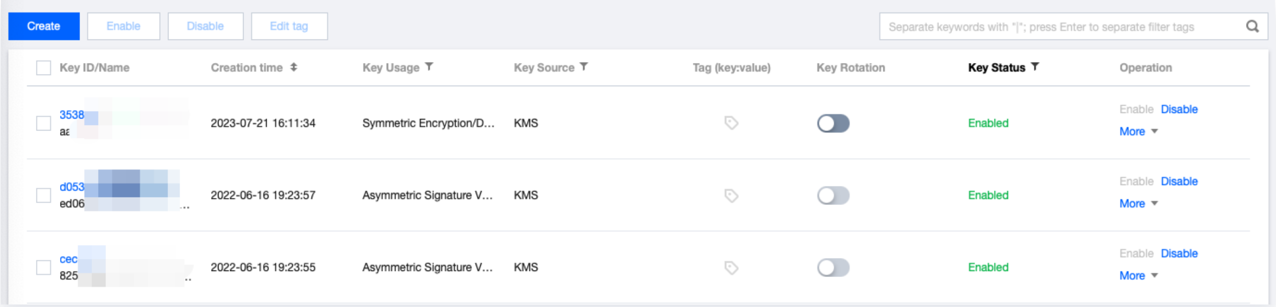
Create | Enable | Disable | Edit tag

Separate keywords with "|"; press Enter to separate filter tags

□ Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Key Rotation	Key Status	Operation
□ [redacted]	2023-07-21 16:11:34	Symmetric Encryption/D...	KMS			Enabled	Enable Disable More
□ [redacted]	2022-06-16 19:23:57	Asymmetric Signature V...	KMS			Enabled	Enable Disable More

Batch Operation

1. Select multiple keys for which you need to change the status.



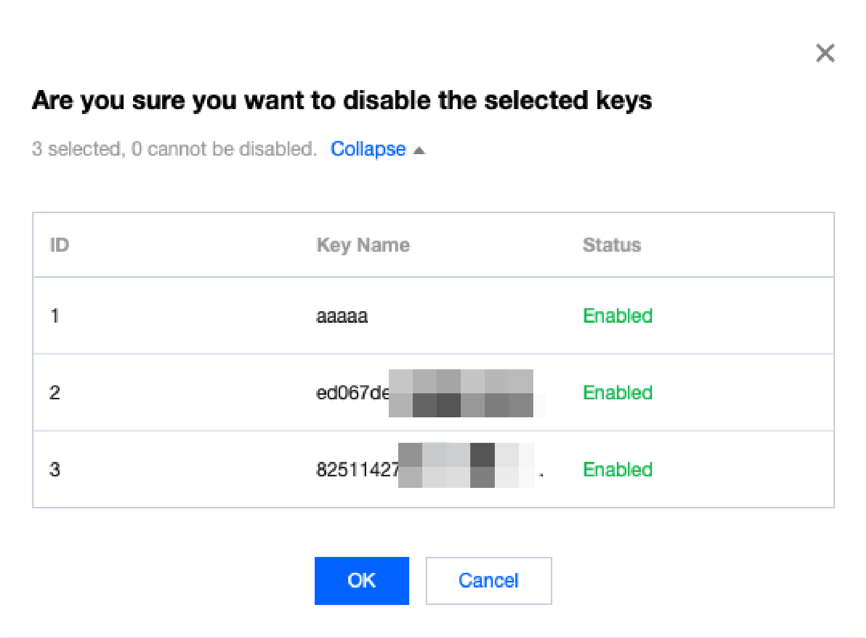
Create | Enable | Disable | Edit tag

Separate keywords with "|"; press Enter to separate filter tags

□ Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Key Rotation	Key Status	Operation
□ [redacted]	2023-07-21 16:11:34	Symmetric Encryption/D...	KMS			Enabled	Enable Disable More
□ [redacted]	2022-06-16 19:23:57	Asymmetric Signature V...	KMS			Enabled	Enable Disable More
□ [redacted]	2022-06-16 19:23:55	Asymmetric Signature V...	KMS			Enabled	Enable Disable More

2. At the top of the list, click **Enable Key** or **Disable Key**. The system will display a confirmation box as shown below. Click **View Details** to confirm the status of the keys in

this batch operation.



Are you sure you want to disable the selected keys

3 selected, 0 cannot be disabled. Collapse ▲

ID	Key Name	Status
1	aaaaa	Enabled
2	ed067de[redacted]	Enabled
3	82511427[redacted]	Enabled

3. After confirming that everything is correct, click **OK** to enable or disable keys in bulk.

Deleting Key

Last updated：2023-08-24 17:04:43

Scenario

You can log in to the Tencent Cloud Key Management System (Compliant) Console or call KMS TCCLI to enable/disable the status of created Customer Master Keys (CMKs). This document introduces how to enable/disable keys through the console.

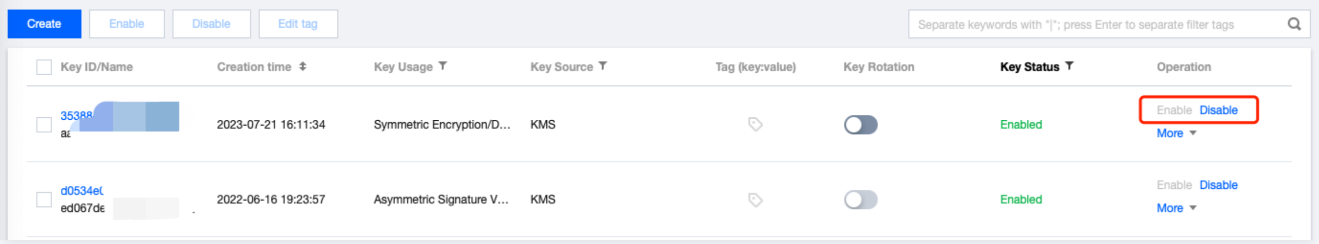
Instructions

1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu. Select the key's region and HSM cluster ID. You can view the master key list of other regions by switching the region and cluster ID at the top.

Customer Managed CMK [redacted] HSM cluster ID: [redacted]

Single operation

Locate the key for which you need to change the status. In the operation area on the right side of the key information, you can enable or disable the key.

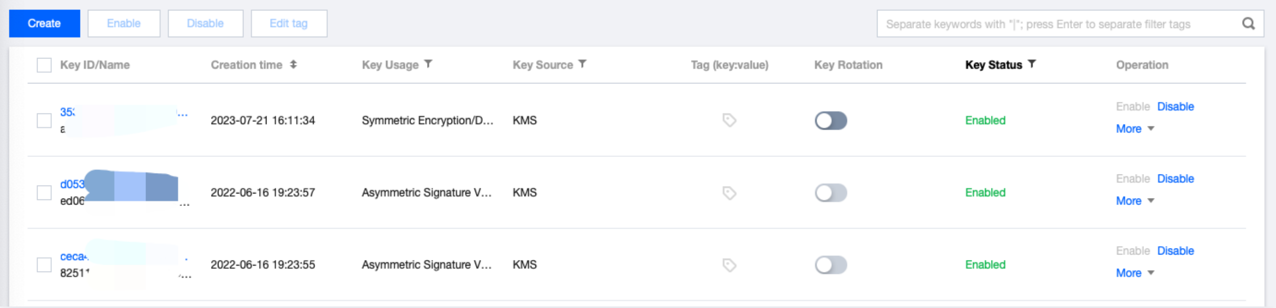


Create
Enable
Disable
Edit tag
Separate keywords with "|"; press Enter to separate filter tags

□ Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Key Rotation	Key Status	Operation
□ [redacted]	2023-07-21 16:11:34	Symmetric Encryption/D...	KMS			Enabled	Enable Disable More
□ [redacted]	2022-06-16 19:23:57	Asymmetric Signature V...	KMS			Enabled	Enable Disable More

Batch Operation

1. Select multiple keys for which you need to change the status.

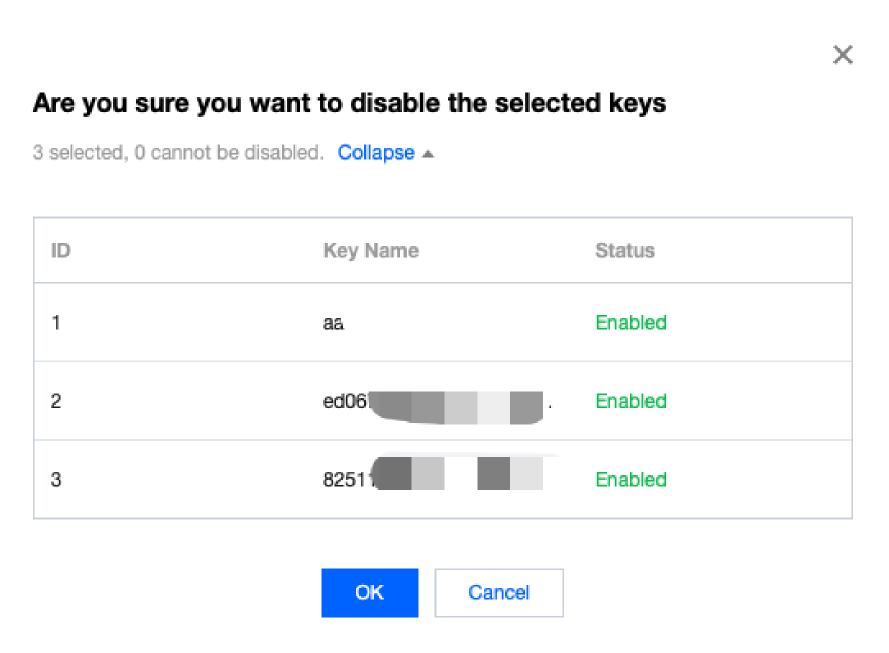


Create
Enable
Disable
Edit tag
Separate keywords with "|"; press Enter to separate filter tags

□ Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)	Key Rotation	Key Status	Operation
□ [redacted]	2023-07-21 16:11:34	Symmetric Encryption/D...	KMS			Enabled	Enable Disable More
□ [redacted]	2022-06-16 19:23:57	Asymmetric Signature V...	KMS			Enabled	Enable Disable More
□ [redacted]	2022-06-16 19:23:55	Asymmetric Signature V...	KMS			Enabled	Enable Disable More

2. At the top of the list, click **Enable Key** or **Disable Key**. The system will display a confirmation box as shown below. Click **View Details** to confirm the status of the keys in

this batch operation.



Are you sure you want to disable the selected keys

3 selected, 0 cannot be disabled.

ID	Key Name	Status
1	aa	Enabled
2	ed06[redacted]	Enabled
3	8251[redacted]	Enabled

3. After confirming that everything is correct, click **OK** to enable or disable keys in bulk.

Encryption and Decryption

Last updated：2023-08-24 17:05:06

Scenario

Tencent Cloud KMS provides APIs, SDKs, and online tools for you to encrypt and decrypt small pieces of data. You can choose any of them based on your needs for different scenarios.

Online Tool

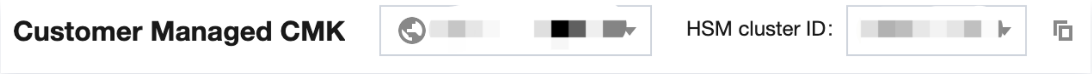
The online tools are suitable for one-time or non-batch encryption and decryption operations, such as the initial generation of key ciphertext. With the online tools, you can focus on your core business without developing tools for non-batch encryption and decryption. They can be used in the following steps:

Preparations

Ensure that you have created a key and that the key is in an enabled state.

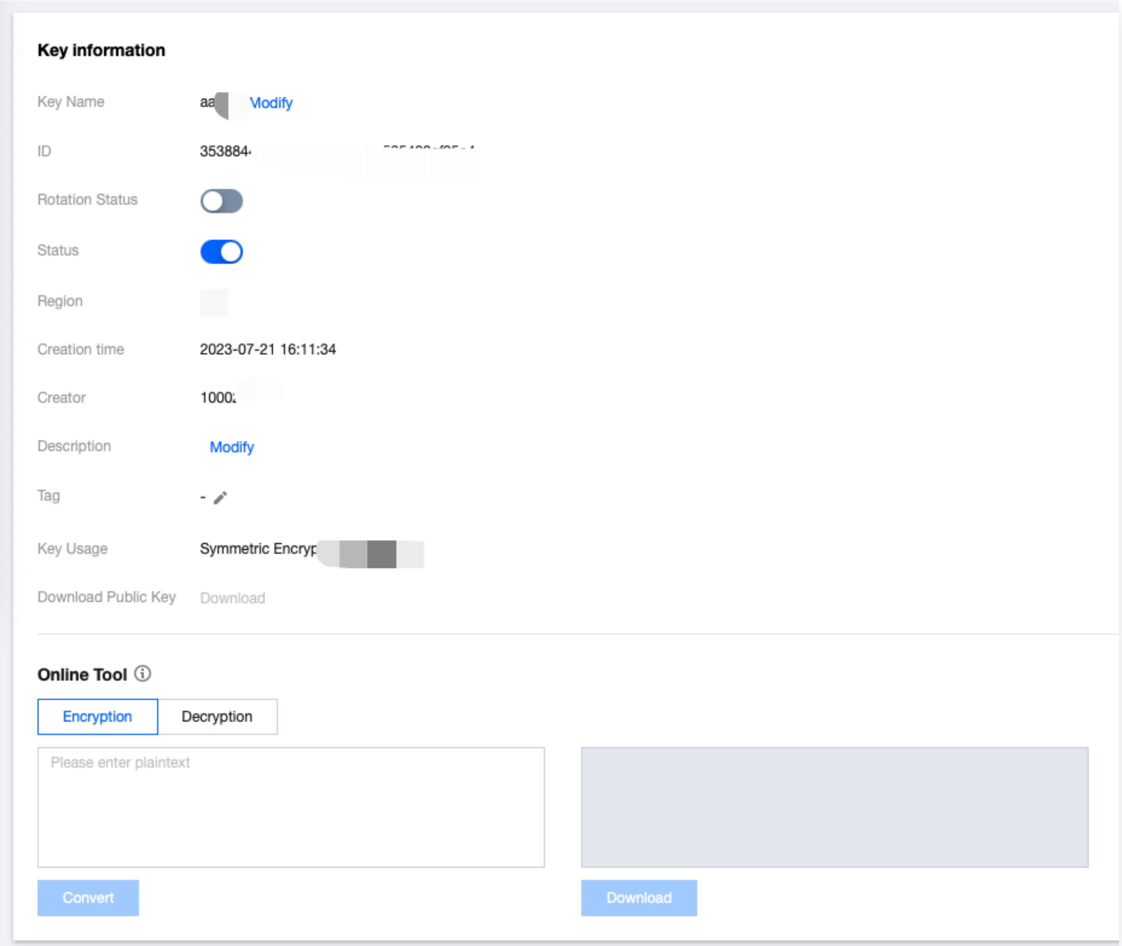
Instructions

1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu, and select the key region and HSM cluster ID.



Data encryption

1. Locate the key you need to encrypt or decrypt, and click **Key Name** under the "Key ID/Key Name" operation column to access the key details page.
2. Under the "Online Tools" module, click **Encryption** and enter the data to be processed.
3. Click **Execute**, and the processed data will be displayed in the gray box on the right.



Key information

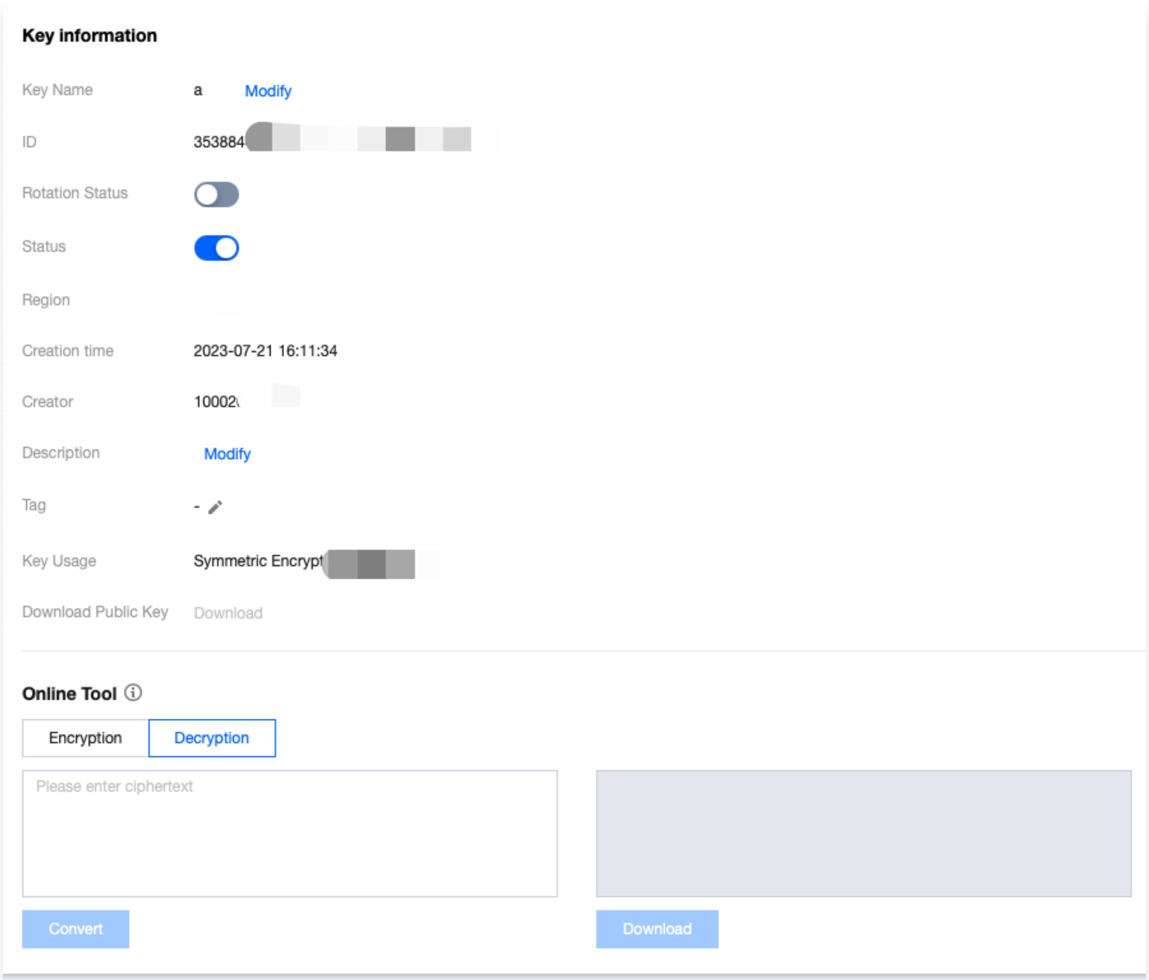
Key Name	aa[redacted] Modify
ID	353884[redacted]
Rotation Status	○
Status	●
Region	[redacted]
Creation time	2023-07-21 16:11:34
Creator	1000[redacted]
Description	Modify
Tag	-
Key Usage	Symmetric Encryp[redacted]
Download Public Key	Download

Online Tool

4. After encrypting the data, you can click **Download** to save the encrypted data to your local computer, completing the encryption process.

Data Decryption

1. If decryption is needed, in the "Online Tools" module, click **Decryption**.
2. Paste the encrypted data into the input box below, click **Execute**, and the decrypted data will be displayed in the gray box on the right.



Key information

Key Name	a Modify
ID	353884[redacted]
Rotation Status	○
Status	●
Region	
Creation time	2023-07-21 16:11:34
Creator	10002[redacted]
Description	Modify
Tag	-
Key Usage	Symmetric Encrypt[redacted]
Download Public Key	Download

Online Tool

> **Note**
> The decryption operation automatically calls the master key used by the ciphertext to perform the decryption. The decrypted plaintext is displayed in Base64 format.

3. You can click **Download** to save the decrypted data to your local computer.

Tag Management
Editing Tag

Last updated: 2023-08-24 17:14:54

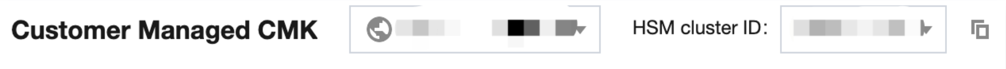
This document introduces the process of editing tags for resources.

Usage Limits

There are corresponding restrictions on the usage of tag content (tag keys and tag values). For more information, please refer to Tag Usage Limits.

Instructions

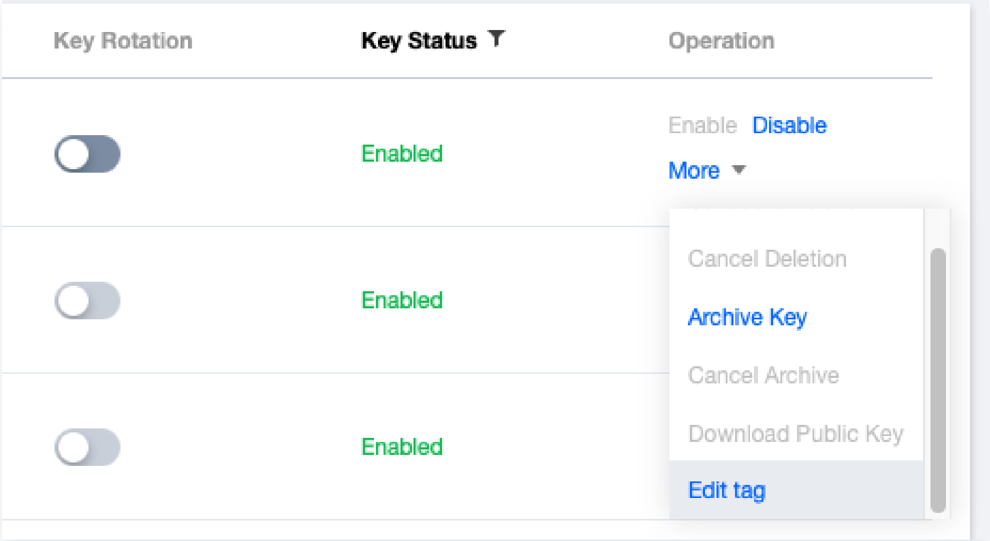
1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu, and select the key region and HSM cluster ID.



Customer Managed CMK [redacted] HSM cluster ID: [redacted]

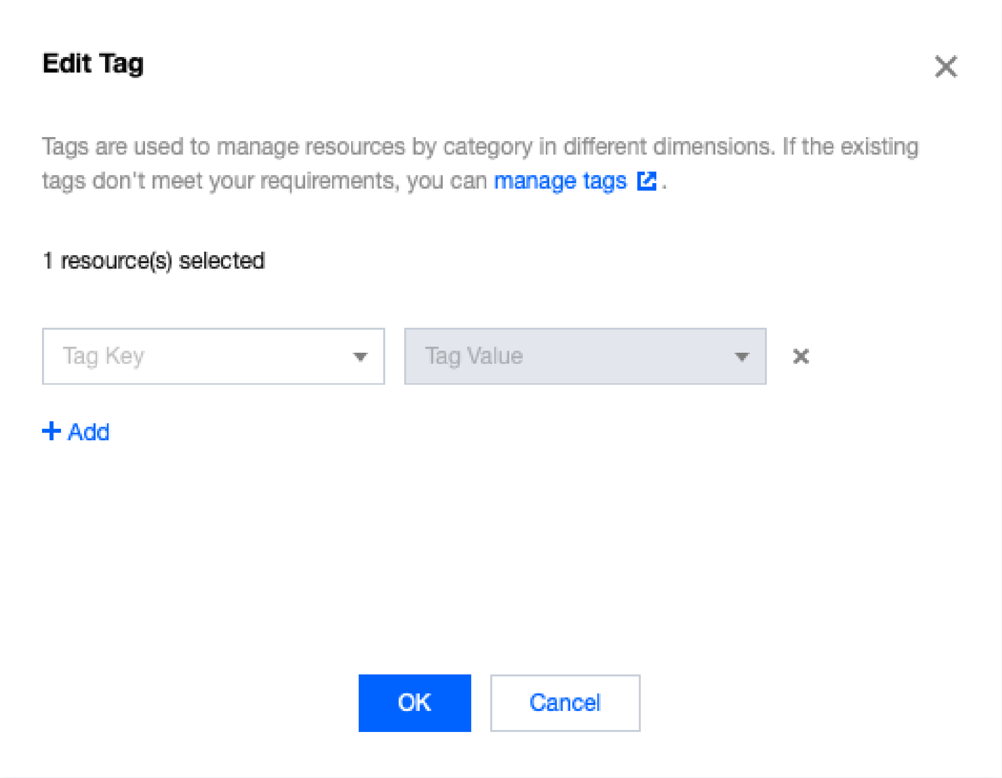
Edit Tag for an Individual Key

1. Select the key to which you want to add a tag, click **More** on the right side of the key, and then click **Edit Tag** in the expanded operation options.



Key Rotation	Key Status	Operation
	Enabled	Enable Disable More
	Enabled	
	Enabled	

2. In the **Edit Tags** pop-up window, you can see that 1 resource has been selected. Based on your actual needs, you can **add** or **delete** tags.



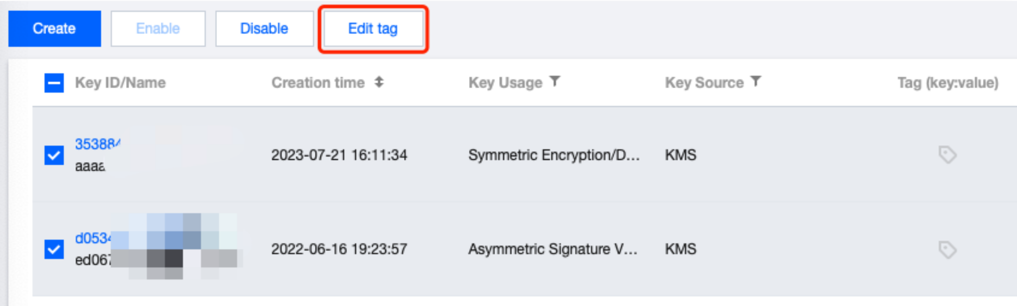
Edit Tag

Tags are used to manage resources by category in different dimensions. If the existing tags don't meet your requirements, you can manage tags.

1 resource(s) selected

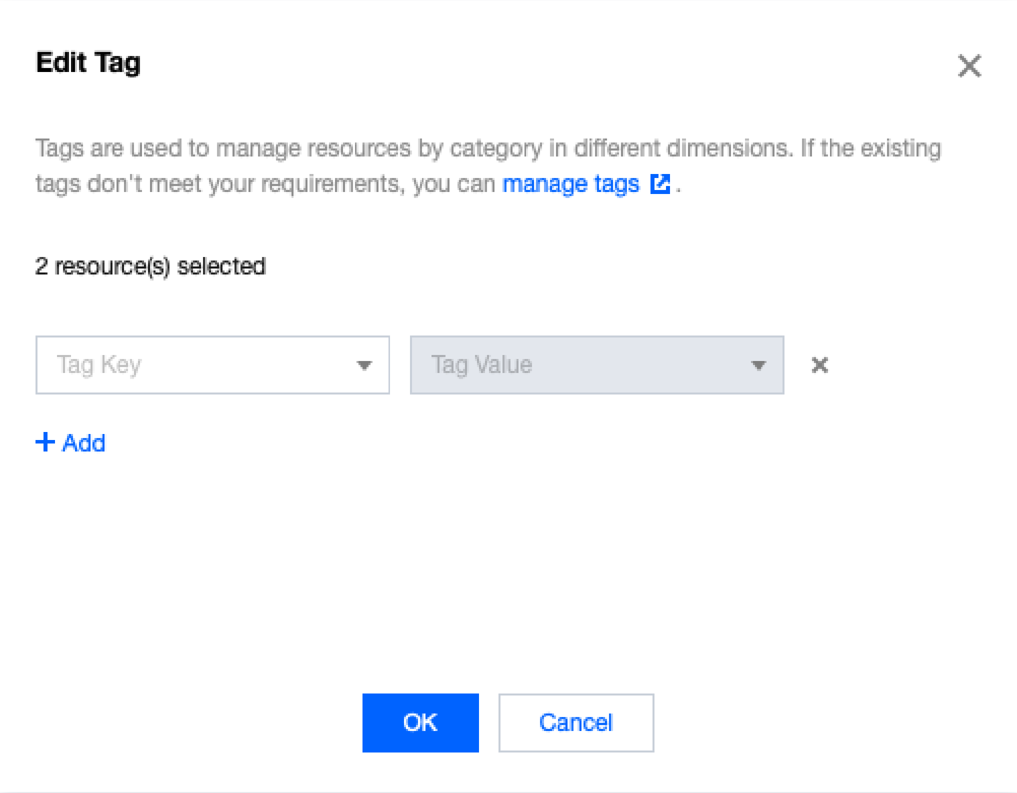
Editing the tags of multiple secrets

1. Select the key for which you want to edit the tag, and click **Edit Tag** at the top of the key.



▬	Key ID/Name	Creation time	Key Usage	Key Source	Tag (key:value)
☑	35388[redacted] aaaa	2023-07-21 16:11:34	Symmetric Encryption/D...	KMS	
☑	d053[redacted] ed06[redacted]	2022-06-16 19:23:57	Asymmetric Signature V...	KMS	

2. In the **Edit Tags** pop-up window, you can view the selected multiple resources and, based on actual needs, **add** or **delete** tags.



Edit Tag

Tags are used to manage resources by category in different dimensions. If the existing tags don't meet your requirements, you can manage tags .

2 resource(s) selected

Note

For information on how to use tags, please refer to Using Tags to Manage Instances.

Examples of Management via Tags

Last updated：2023-08-24 17:07:00

Scenario

- Tag is used for resource categorization and permission management from different dimensions.
- In Key Management System (KMS), tags are primarily used to identify Customer Master Keys (CMKs).
- Adding tags to CMKs is intended to facilitate user classification and tracking management of CMKs, while also allowing for usage summaries of corresponding keys based on tags.

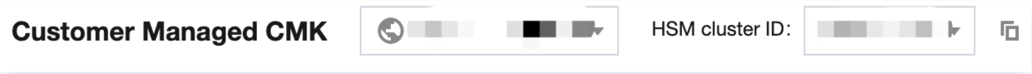
Usage Limits

There are corresponding restrictions on the usage of tag content (tag keys and tag values). For more information, please refer to Tag Usage Limits.

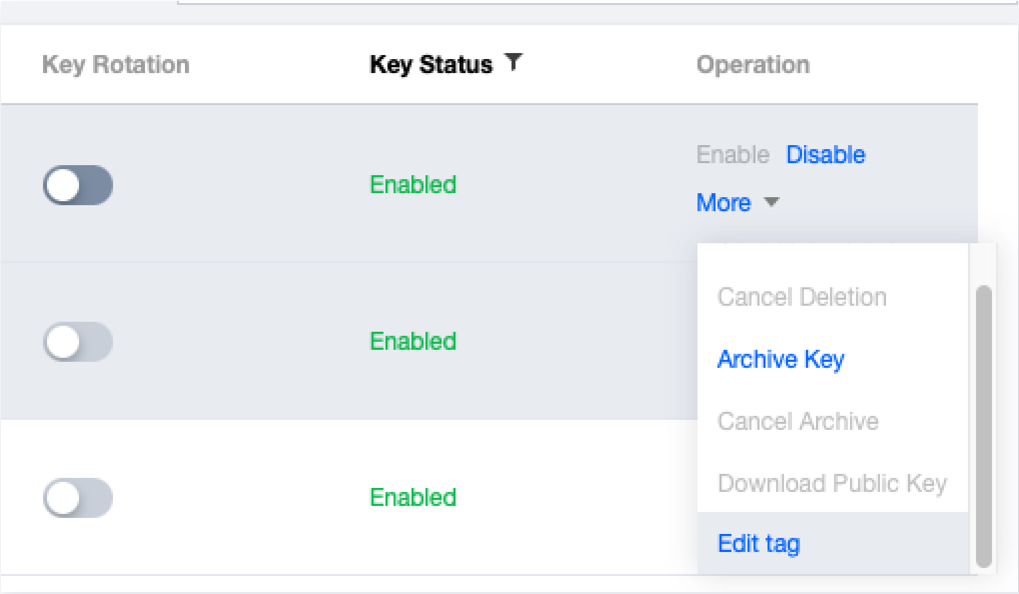
Instructions

Configuring Tags

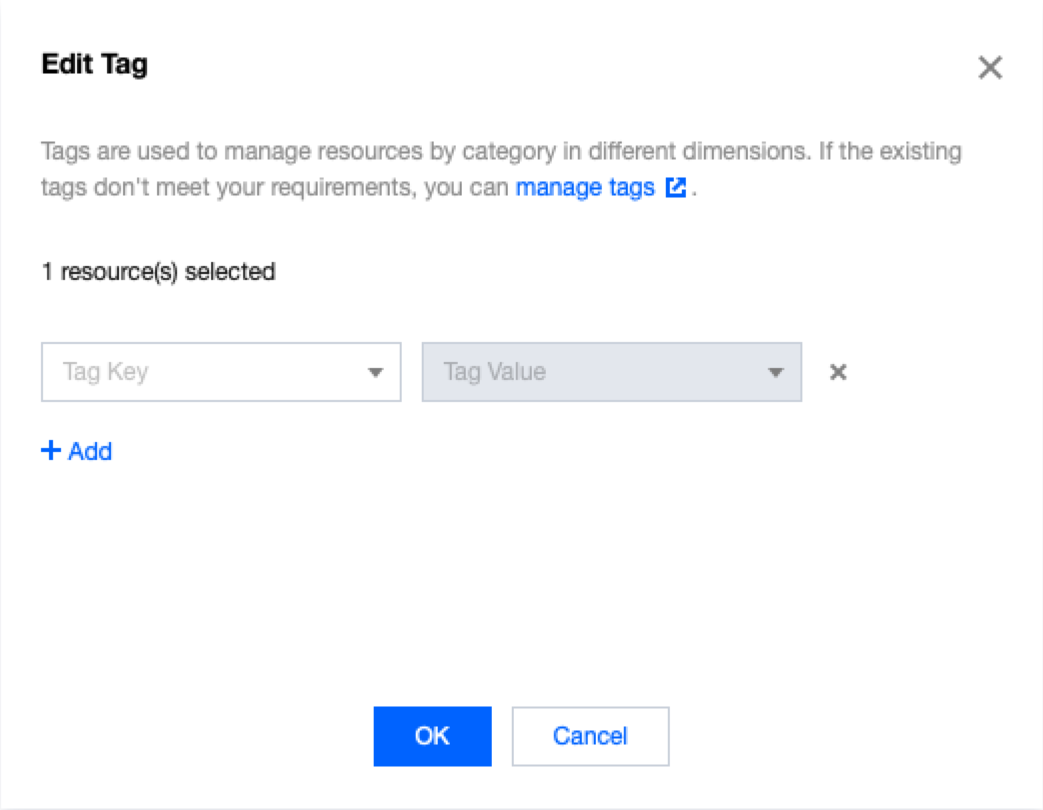
1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key Management menu, and select the key region and HSM cluster ID.



3. Select the key to which you want to add a tag, click **More** on the right side of the key, and then click **Edit Tag** in the expanded operation options.



4. In the **Edit Tags** pop-up window, you can see that one resource has been selected. Add or delete tags according to your actual needs. For example, add two sets of tags.


Edit Tag

Tags are used to manage resources by category in different dimensions. If the existing tags don't meet your requirements, you can manage tags .

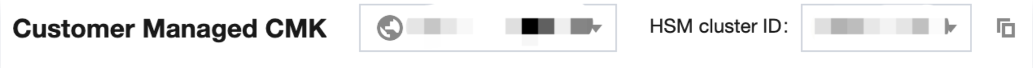
1 resource(s) selected

5. Click **OK**, and if the system displays a successful modification prompt, it indicates that the tag has been modified successfully.

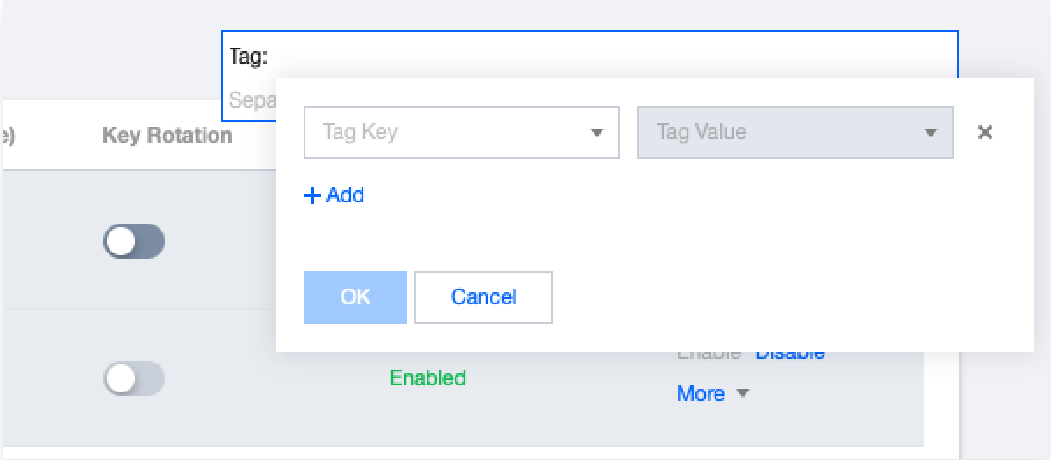
Filtering keys with tags

1. Log in to the Key Management System (Compliance) console.
2. In the left navigation menu, click **User Key Management** under the HSM Exclusive Key

Management menu, and select the key region and HSM cluster ID.



3. In the search box on the right, select **Tag** as the filter condition, choose the tag key and tag value, then click **Confirm**.



Tag:
Sepa
Key Rotation
Tag Key
Tag Value
×
+ Add
OK
Cancel
Enabled
Enable Disable
More ▾