

Key Management Service

Console Guide

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

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

Key Management

Creating a Key

Viewing keys

Editing Key

Enabling/Disabling Key

Key Rotation

Encryption and Decryption

Deleting Key

Access Control

Overview

Managing Sub-account

Creating Access Control Policy

Audit

Operations Logged by CloudAudit

Viewing Audit Logs

Console Guide

Getting Started

Last updated : 2024-01-11 16:28:54

Key Management Service (KMS) provides the capabilities for secure and compliant full-lifecycle key management, data encryption, and data decryption.

The core key components involved in KMS include customer master key (CMK) and data encryption key (DEK). A CMK is a first-level key used to encrypt and decrypt sensitive data and generate DEKs. A DEK is a second-level key used in the envelope encryption process. It is protected by a CMK, and used to encrypt business data.

For scenarios where CMKs and DEKs are used for business data encryption and decryption, please see [Sensitive Data Encryption](#) and [Envelope Encryption Best Practice](#).

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 CMK is a logical representation of a master key, and it contains metadata such as key ID, creation date, description, and key status. Generally, you can use the automatic CMK generation feature in KMS or import your own key to generate a CMK.

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

A **Customer Managed CMK** is a CMK that you create in the console or through APIs. You can create, enable, disable, rotate keys and manage permissions of your user keys.

A **Tencent Cloud Managed CMK** is a CMK that is automatically created for you when a Tencent Cloud product/service (such as CBS, COS, or TDSQL) calls the KMS service. You can query and rotate Tencent Cloud managed CMKs, but cannot disable them or set the schedule deletion for them.

Data encryption key (DEK)

A DEK is a second-level key generated based on a CMK, used for encrypting and decrypting local data.

KMS allows you to use your CMKs to generate DEKs, but KMS will not store, manage, or track them or use them to perform encryption operations. You have to use and manage your DEKs outside of KMS.

Generally, DEKs are used in envelop encryption to encrypt local business data. They are protected by CMKs and customizable. DEKs can be created through the [GenerateDataKey](#) API.

Operation Overview

Operation	Description
Creating key	Creates a key quickly in the console.
Viewing key	Views the ID and details of a key in the console.
Editing key	Edits the name, description, and other information of a key in the console.
Enabling and disabling key	Enables and disables a key in the console.
Rotating key	Enables key rotation in the console.
Encryption and decryption	Uses keys to encrypt and decrypt data in the console.
Deleting key	Deletes a key quickly in the console.
Access control	Sets KMS permissions for a sub-account.

Key Management

Creating a Key

Last updated : 2024-01-11 16:28:54

Scenarios

A CMK can be created in the KMS console or by calling the CreateKey API. After creation, you can manage the CMK by enabling, disabling, rotation and granting permission. This document describes how to create a CMK in the console.

Directions

1. Log in to the [KMS Console](#).
2. Select the region for which you want to create a key and click **Create**.



3. Enter the following information in the pop-up box:

Key Name: This is required and must be unique within the region. It can contain letters, numbers, `_`, `-`, and cannot begin with "KMS-".

Description: This is optional and used to specify the type of data to be protected, or the application to be used in conjunction with the CMK.

Tag: This is optional. [Tag](#) is a Tencent Cloud resource management tool that allows you to categorize, search and aggregate keys.

Key Usage: This is required and supports symmetric encryption and decryption, asymmetric encryption and decryption, or asymmetric signature verification.

Key Material Source: This is required. You can choose to generate the key in KMS or import your own key.

Note:


External key material is supported only for symmetric encryption and decryption.

Create Key ✕

Key Name *

Description

Tag ✕

[+ Add](#)
If there is no desired tag or tag value, you can [create](#)  one in the console.

Key Usage

Key Material Source KMS External

Click **OK** to go back to the key list, and then you can see the new key at the top of the list.

Viewing keys

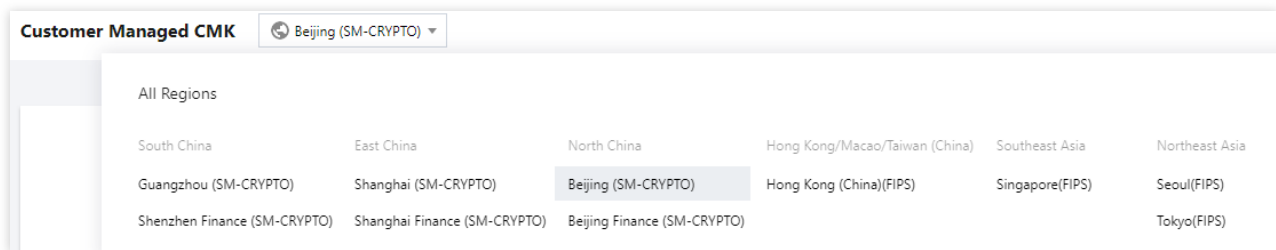
Last updated : 2024-01-11 16:28:54

Overview

You can log in to the KMS Console or call KMS TCCLI to view key details, such as the CMK ID list and CMK name, ID, status, and region. This document describes how to view the CMK ID list and details in the console.

Viewing Key ID List

1. Log in to the [KMS Console](#).
2. Switch regions to view the CMK list in other regions.



3. You can enter the CMK's full or partial name or ID in the filter box on the right of the page to search for the target key.

Search by name

Search by ID

Viewing Key ID Details

1. Log in to the [KMS Console](#).
2. Locate the target key. For more information, please see [Viewing Key ID List](#).
3. Click the key ID/name to view its details.

Editing Key

Last updated : 2024-01-11 16:28:54

Operation Scenarios

You can edit a CMK in the KMS Console or by calling KMS TCCLI, such as modifying the description and enabling/disabling key rotation. This document describes how to edit a CMK in the console.

Directions

1. Log in to the [KMS Console](#).
2. Click the ID/name of the target key to enter the details page, where you can modify the key name, status, rotation configuration, and description, among others.
3. Click "OK" for the changes to take effect.

Enabling/Disabling Key

Last updated : 2024-01-11 16:28:54

Operation Scenarios

You can log in to the KMS Console or call KMS TCCLI to enable and disable a CMK. This document describes how to do so in the console.

Directions

Single operation

1. Log in to the [KMS Console](#).
2. Locate the target key, and enable or disable it in the "Operation" column on the right.

Batch operation

1. Log in to the [KMS Console](#).
2. Select the keys for which you want to change the status in batches.
3. Click **Enable** or **Disable** at the top. In the pop-up window, click **View Details** to confirm the status of keys in this batch operation.
4. Confirm that everything is correct and click **OK**.

Key Rotation

Last updated : 2024-01-11 16:28:54

Operation Scenarios

To improve the security of ciphertext storage, Tencent Cloud KMS provides the capability of imperceptible key rotation to refresh the stored ciphertext.

Key rotation is imperceptible and has no impact on your business. After being rotated, the CMK is compatible with the ciphertext encrypted before rotation. The [ReEncrypt](#) API is offered to refresh the ciphertext. This document describes how to enable key rotation in the console.

Directions

1. Log in to the [KMS Console](#).
2. Locate the key to be rotated and click **Enable Rotation** in the "Key Rotation" column.

Note :

By default, key rotation is disabled. Once it is enabled, the CMK will be rotated annually.

Encryption and Decryption

Last updated : 2024-01-11 16:28:54

Scenarios

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 tools

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:

Prerequisites

You have [created a key](#) and enabled it.

Directions

1. Log in to the [KMS Console](#).
2. Find the target key. In the "Key ID/Name" section, click the key name to enter 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 **Convert**, and the resulting data processed by the system will be displayed in the gray box on the right.

Key Information

Key Name [Modify](#)

ID

Rotation Status

Status

Region **Beijing**

Creation Time 2021-03-31 08:23:28

Creator

Description [Modify](#)

Key Usage Symmetric Encryption/Decryption

Download Public Key [Download](#)

Online Tool ⓘ

Please enter plaintext

6. After encryption is completed, you can click **Download** to download the encrypted data to your local file system.
7. If you need to decrypt the data, click **Decryption** in the "Online Tools" module.
8. Paste the encrypted data into the input box below, click **Convert**, and the decrypted data will be displayed in the gray box on the right.

Key Information

Key Name	<input type="text"/> Modify
ID	<input type="text"/>
Rotation Status	<input type="checkbox"/>
Status	<input checked="" type="checkbox"/>
Region	Beijing
Creation Time	2021-03-31 08:23:28
Creator	<input type="text"/>
Description	<input type="text"/> Modify
Key Usage	Symmetric Encryption/Decryption
Download Public Key	Download

Online Tool ⓘ

Please enter ciphertext

Note:

The decryption operation automatically calls the CMK used in the encryption. After decryption, the plaintext will be Base64-encoded for display.

9. You can click **Download** to download the decrypted data to your local file system.

Deleting Key

Last updated : 2024-01-11 16:28:54

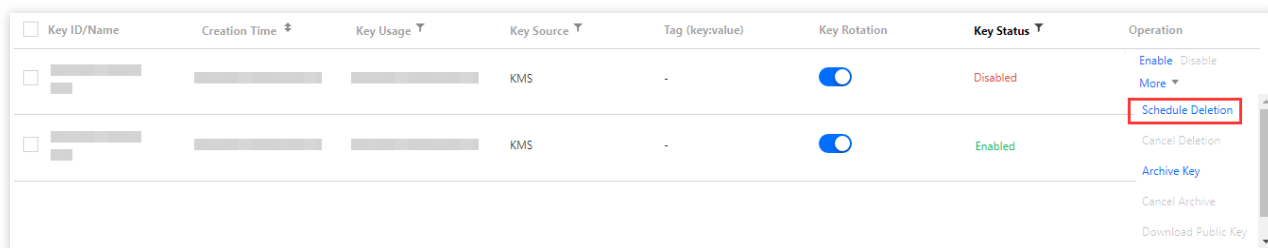
Overview

A key cannot be recovered after being deleted, and all data encrypted with it cannot be decrypted. To prevent accidental deletion, KMS adopts a scheduled deletion mechanism, i.e., a mandatory waiting period of 7-30 days is imposed on a deletion operation. Within the waiting period, you can cancel the deletion.

You can log in to the KMS console or call KMS TCCLI to create and cancel a scheduled deletion task. This guide describes how to delete a key in the console.

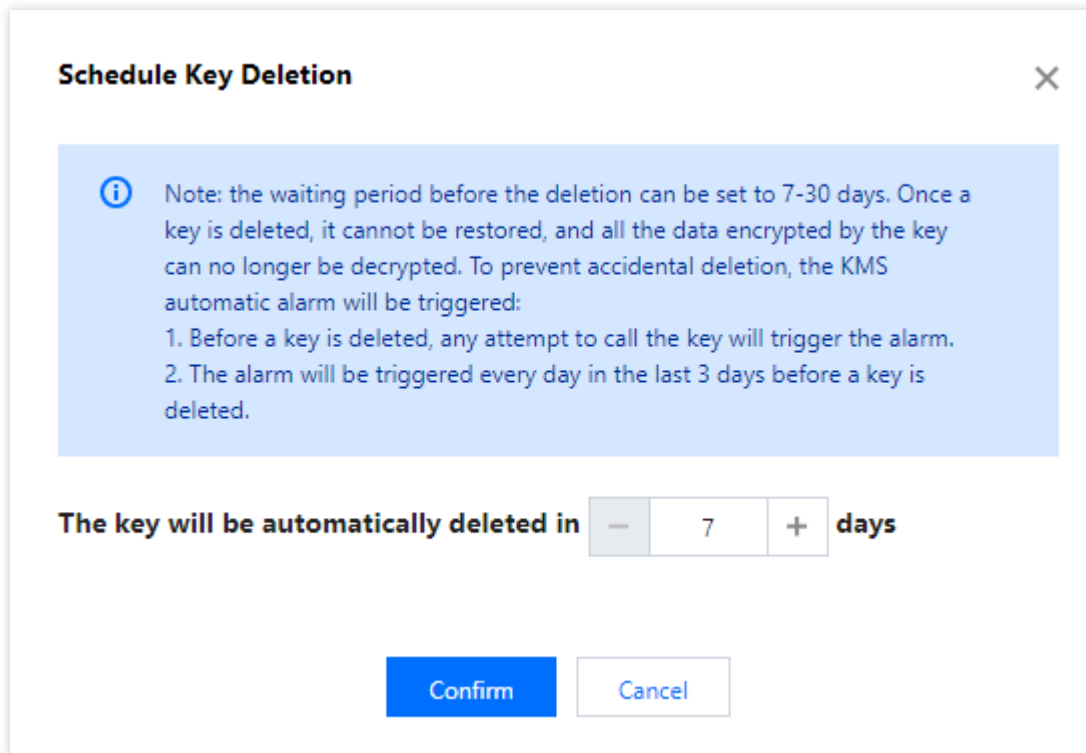
Directions

1. Log in to the [KMS Console](#).
2. Select the key to be deleted, and click **Schedule Deletion** on the right. If the key is enabled, please disable it first.



<input type="checkbox"/>	Key ID/Name	Creation Time	Key Usage	Key Source	Tag (key:value)	Key Rotation	Key Status	Operation
<input type="checkbox"/>	[Redacted]	[Redacted]	[Redacted]	KMS	-	<input checked="" type="checkbox"/>	Disabled	Enable Disable More Schedule Deletion
<input type="checkbox"/>	[Redacted]	[Redacted]	[Redacted]	KMS	-	<input checked="" type="checkbox"/>	Enabled	Cancel Deletion Archive Key Cancel Archive Download Public Key

3. Enter the days of waiting period, click **OK**. The key will be deleted as scheduled.

**Note:**

The waiting period can be set to 7-30 days. After being deleted, a key cannot be recovered, and all data encrypted with it cannot be decrypted.

To prevent accidental deletion, the KMS automatic alarm will be triggered:

Before a key is deleted, any attempt to call the key will trigger the alarm.

The alarm will be triggered every day in the last 3 days before a key is deleted.

4. If you need to cancel the scheduled deletion task, click **Cancel Deletion**. After the key is reset to "Disabled" status, you can enable/modify/delete it or perform other operations.

Access Control

Overview

Last updated : 2024-01-11 16:28:54

If you use multiple services such as KMS, VPC, CVM, and TencentDB, which are managed by different users sharing your Tencent Cloud account key, the following problems may exist:

Your key is shared by multiple users, leading to high risk of compromise.

You cannot control the access permissions of other users, which poses a security risk due to potential accidental operations.

[Cloud Access Management \(CAM\)](#) is used to manage the access permissions for the resources under Tencent Cloud accounts. With CAM, you can use the identity management and policy management features to control which Tencent Cloud resources can be accessed by which sub-accounts.

For example, if you have a CMK under your root account, and you want it to be used by sub-account A but not sub-account B, you can control the permissions of the sub-accounts by configuring a corresponding policy in CAM.

If you do not need to manage the access to KMS resources by sub-accounts, you can skip this chapter. This will not affect your understanding and usage of other parts in the documentation.

Basic CAM Concepts

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

Account

Root account: As the fundamental owner of Tencent Cloud resources, a root account acts as the basis for resource usage fee calculation and billing and can be used to log in to Tencent Cloud services.

Sub-account: An account created by the root account, which has a specific ID and identity credential that can be used to log in to the Tencent Cloud Console. A root account can create multiple sub-accounts (users). **A sub-account does not own any resources by default; instead, such resources should be authorized by its root account.**

Identity credential: This includes login credentials and access certificates. **Login credential** refers to user login name and password. **Access certificate** refers to the TencentCloud API keys (SecretId and SecretKey).

Resources and permissions

Resource: A resource is an object that is managed in Tencent Cloud services, such as a CMK in KMS, a CVM instance, a bucket in COS, or a VPC instance.

Permission: Permission is an authorization to allow or forbid certain users to perform certain operations. By default, **a root account has full access to all the resources under it**, while **a sub-account does not have access to any resources under its root account**.

Policy: Policy is the syntax rule used to define and describe one or multiple permissions. **A root account** performs authorization by **associating policies** with users/user groups.

For more information, please see the [CAM](#) product documentation.

Related Documents

Document Description	Link
Relationship between policy and user	Policy Management
Basic policy structure	Policy Syntax
More products that support CAM	List of Tencent Cloud Services that Support CAM

Managing Sub-account

Last updated : 2024-01-11 16:28:54

Overview

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

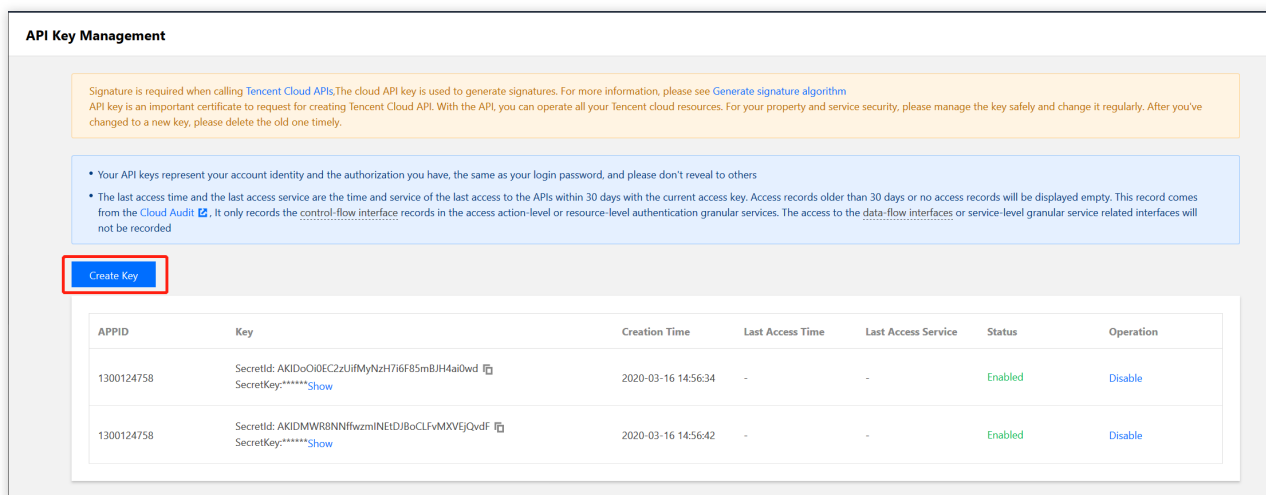
Directions

Step 1. Create a sub-account

1. Log in to the [CAM Console](#) with your root 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 details page.
2. Select **API Key** > **Create Key** to create `SecretId` and `SecretKey`. The API key is used to access KMS.



The screenshot shows the 'API Key Management' interface. At the top, there is a warning box about signatures and API keys. Below that, there are two informational bullet points. A blue 'Create Key' button is highlighted with a red box. Below the button is a table with the following data:

APPID	Key	Creation Time	Last Access Time	Last Access Service	Status	Operation
1300124758	SecretId: AKIDoOj0EC2zJifMyNzH7i6F85mBJH4ai0wd SecretKey:*****Show	2020-03-16 14:56:34	-	-	Enabled	Disable
1300124758	SecretId: AKIDMWR8NNfWzmiNETDjBoCLFvMXVEjQvdf SecretKey:*****Show	2020-03-16 14:56:42	-	-	Enabled	Disable

Step 3. Authorize the sub-account

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

1. Go to **Permissions** > **Associate Policies** > **Select Policies from the Policy List to Associate** and select the appropriate KMS policy.

Policies All Policies ▾

Bind users or user groups with the policy to assign them related permissions.

Create Custom Policy Delete Support search by policy name 🔍

<input type="checkbox"/>	Policy Name	Description	Service Type ▾	Operation
<input type="checkbox"/>	AdministratorAccess	This policy allows you to manage all users under your account and their permissions, financial information an...	-	Bind User/Group
<input type="checkbox"/>	ReadOnlyAccess	This policy authorizes you with the read-only access to all cloud assets that support authentication at API or ...	-	Bind User/Group
<input type="checkbox"/>	QCloudResourceFullAccess	This policy allows you to manage all cloud assets in your account.	-	Bind User/Group
<input type="checkbox"/>	QCloudFinanceFullAccess	This policy allows you to manage all financial items in your account, such as payment and billing.	-	Bind User/Group
<input type="checkbox"/>	QcloudNARMSFullAccess	QcloudNARMSFullAccess	Network Assets Risk Monitor System	Bind User/Group
<input type="checkbox"/>	QcloudNARMSReadOnlyAccess	QcloudNARMSReadOnlyAccess	Network Assets Risk Monitor System	Bind User/Group
<input type="checkbox"/>	QcloudAAFFullAccess	Full read-write access to ActivityAntiRush (AA)	ActivityAntiRush	Bind User/Group
<input type="checkbox"/>	QcloudAccessForAegisRole	Aegis\' access to cloud resources	-	Bind User/Group
<input type="checkbox"/>	QcloudAccessForASRole	AutoScaling permissions (including but not limited to): CVM(add/delete/query CVM instances); VPC(query V...	-	Bind User/Group

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

Creating Access Control Policy

Last updated : 2024-01-11 16:28:54

Overview

This document describes how to create a KMS policy in the CAM Console.

Directions

1. Log in to the [CAM Console](#).
2. On the left sidebar, click **Policies > Create Custom Policy > Create by Policy Syntax** to enter the policy creation page.
3. Select a policy template, such as a blank template or KMS policy template, and click **Next**.
4. Enter policy name and content as shown below.
5. Click **Create Policy**.

Audit

Operations Logged by CloudAudit

Last updated : 2024-06-21 21:25:31

Tencent Cloud [CloudAudit](#) logs KMS operation events. The operations that can be logged by CloudAudit are as follows:

Operation Name	Event Name
Creating a CMK	CreateKey
Getting the attributes of a CMK	DescribeKey
Getting the attributes of multiple CMKs	DescribeKeys
Getting the CMK list	ListKey
Getting the CMK list details	ListKeyDetail
Modifying the CMK description	UpdateKeyDescription
Modifying an alias	UpdateAlias
Enabling a CMK	EnableKey
Disabling a CMK	DisableKey
Batch enabling CMKs	EnableKeys
Batch disabling CMKs	DisableKeys
Setting schedule deletion for a CMK	ScheduleKeyDeletion
Canceling schedule deletion for a CMK	CancelKeyDeletion
Getting the parameters of the CMK materials to be imported	GetParametersForImport
Importing key materials	ImportKeyMaterial
Creating a white-box key	CreateWhiteBoxKey
Encrypting data with a white-box key	EncryptByWhiteBox
Enabling a white-box key	EnableWhiteBoxKey
Disabling a white-box key	DisableWhiteBoxKey

Batch enabling white-box keys	EnableWhiteBoxKeys
Batch disabling white-box keys	DisableWhiteBoxKeys
Deleting a white-box key	DeleteWhiteBoxKey
Getting the white-box key service status	DescribeWhiteBoxServiceStatus
Overwriting the device fingerprint of a specified key	OverwriteWhiteBoxDeviceFingerprints
Getting the device fingerprint list of a specified key	DescribeWhiteBoxDeviceFingerprints
Getting a white-box decryption key	DescribeWhiteBoxDecryptKey
Decrypting data	Decrypt
Encrypting data	Encrypt
Generating a signature	SignByAsymmetricKey
Verifying a signature	VerifyByAsymmetricKey
Archiving a key	ArchiveKey
Canceling archive	CancelKeyArchive
Getting the service AZs	GetRegions
Refreshing the ciphertext	ReEncrypt
Generating a random number	GenerateRandom
Generating a DEK	GenerateDataKey
Querying service status	GetServiceStatus
Listing the encryption methods supported in the current region	ListAlgorithms
Disabling key rotation	DisableKeyRotation
Enabling key rotation	EnableKeyRotation
Querying key rotation status	GetKeyRotationStatus
Binding a CMK with a Tencent Cloud service	BindCloudResource
Unbinding a CMK from a Tencent Cloud service	UnbindCloudResource
Getting the public key of a pair of asymmetric keys	GetPublicKey

Using SM2 to decrypt data with asymmetric keys	AsymmetricSm2Decrypt
Using RSA to decrypt data with asymmetric keys	AsymmetricRsaDecrypt

Viewing Audit Logs

Last updated : 2024-01-11 16:28:54

1. Log in to the [CloudAudit console](#).
2. Click **Event history** in the left sidebar to enter the event history page.
3. You can check event history with relevant username, resource type, resource name, event source, event ID, keyword, or event time. The list part displays the events.

i The list below presents the API events of the last 30 days. For having records of a longer time period, please create a tracking set, by which you can view records for a longer time.

Operation Type: Last 7 Days:

Event Time	Username	Event Name	Resource Type
▶ 2021-03-08 10:52:05	root	GetServiceStatus	kms
▶ 2021-03-08 10:52:04		GetRegions	kms
▶ 2021-03-08 10:51:45		ListAlgorithms	kms

4. Click the triangle on the left of an event to view the details, including event time, username, event name, access key, and event ID, etc. You can then click **View Event** to view more about the event.

Event Time	Username	Event Name	Resource Type
▼ 2021-03-08 10:52:05	root	GetServiceStatus	kms

Key ID: [REDACTED] CAM Error Code

Event ID: [REDACTED] Event Region

Event Name: GetServiceStatus Event Source

Event Time: 2021-03-08 10:52:05 Request ID

Source IP Address: 0.0.0.0 Username

Resource Region

[View Event](#)