

Key Management Service

User Guide (ME-AbuDhabi)

Issue 02
Date 2021-06-03



Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Contents

1 Introduction.....	1
1.1 Concepts.....	1
1.1.1 KMS.....	1
1.1.2 CMK.....	1
1.1.3 Default Master Key.....	1
1.1.4 DEK.....	2
1.1.5 HSM.....	2
1.1.6 Envelope Encryption.....	2
1.1.7 TRNG.....	2
1.2 Application Scenarios.....	2
1.3 Functions.....	4
1.4 Accessing and Using KMS.....	4
1.4.1 How to Access KMS.....	4
1.4.2 How to Use KMS.....	4
1.4.3 Related Services.....	6
1.4.4 KMS Permissions Management.....	7
2 Management.....	11
2.1 Creating a Key.....	11
2.2 Creating CMKs Using Imported Key Material.....	13
2.2.1 Overview.....	13
2.2.2 Importing Key Material.....	14
2.2.3 Deleting Key Material.....	20
2.3 Scheduling the Deletion of One or Multiple CMKs.....	21
2.4 Encrypting and Decrypting Small Data Online.....	23
2.5 Managing Tags.....	24
2.5.1 Adding a Tag.....	24
2.5.2 Searching for Tags.....	26
2.5.3 Modifying Tag Values.....	27
2.5.4 Deleting Tags.....	28
2.6 Managing CMKs.....	28
2.6.1 Querying a CMK.....	29
2.6.2 Changing the Alias and Description of a CMK.....	31
2.6.3 Enabling One or Multiple CMKs.....	32

2.6.4 Disabling One or Multiple CMKs.....	33
2.6.5 Canceling the Scheduled Deletion of One or Multiple CMKs.....	34
2.7 Permissions Management.....	34
2.7.1 Creating a User and Authorizing the User the Permission to Access KMS.....	34
2.7.2 Creating a Custom Policy.....	36
3 FAQs.....	39
3.1 What Is Key Management Service?.....	39
3.2 What Is a Customer Master Key?.....	39
3.3 What Is a Data Encryption Key?.....	39
3.4 Why Cannot I Delete a CMK Immediately?.....	39
3.5 Which Cloud Services Can Use KMS for Encryption?.....	40
A Change History.....	41

1 Introduction

1.1 Concepts

1.1.1 KMS

Key Management Service (KMS) is a secure, reliable, and easy-to-use service that helps users centrally manage and safeguard their Customer Master Keys (CMKs).

This service uses hardware security modules (HSMs) to protect CMKs. HSMs help you create and control CMKs with ease. All CMKs are protected by root keys in HSMs to avoid leakage caused by human error. KMS implements access control and log-based tracking on all operations involving CMKs. Additionally, it provides use records of all CMKs, meeting your audit and regulatory compliance requirements.

1.1.2 CMK

A Customer Master Key (CMK) is a Key Encryption Key (KEK) created by a user using KMS. It is used to encrypt and protect Data Encryption Keys (DEKs). One CMK can be used to encrypt one or multiple DEKs.

1.1.3 Default Master Key

A Default Master Key is automatically created by another cloud service using KMS, such as Object Storage Service (OBS). The alias of a Default Master Key ends with **/default**.

You can use the management console to query the status of Default Master Keys, but cannot disable or schedule the deletion of Default Master Keys.

Table 1-1 Default Master Keys

Alias	Cloud Service
obs/default	OBS

Alias	Cloud Service
evs/default	Elastic Volume Service (EVS)
ims/default	Image Management Service (IMS)
sfs/default	Scalable File Service (SFS)
rds/default	Relational Database Service (RDS)

 **NOTE**

A Default Master Key is automatically created when a user employs the KMS encryption function for the first time in another cloud service.

1.1.4 DEK

Data Encryption Keys (DEKs) are used by users to encrypt data.

1.1.5 HSM

A hardware security module (HSM) is a hardware device that securely produces, stores, manages, and uses CMKs. In addition, it provides encryption processing services.

1.1.6 Envelope Encryption

Envelope encryption is an encryption method that enables DEKs to be stored, transmitted, and used in "envelopes." As a result, CMKs are not used to directly encrypt and decrypt data.

1.1.7 TRNG

A true random number generator (TRNG) is a device that generates unpredictable random numbers by physical procedures instead of computer programs.

1.2 Application Scenarios

KMS provides central management and control capabilities of CMKs for Object Storage Service (OBS), Elastic Volume Service (EVS), Image Management Service (IMS), Relational Database Service (RDS), and user applications. It is perfectly suited for data encryption and decryption scenarios.

- For OBS, KMS applies to object encryption on OBS.

 **NOTE**

OBS is an object-based storage service that provides customers with massive, secure, reliable, and cost-effective data storage capabilities, including but not limited to bucket creation, modification, deletion, and management, as well as object upload, download, deletion, and general management. OBS can store all file types, and is suitable for individual subscribers, websites, enterprises, and developers. For more information about OBS, see *Object Storage Service User Guide*.

- For EVS, KMS applies to data encryption in EVS disks.

NOTE

Based on a distributed architecture, an EVS disk is a virtual block storage device that can be elastically scaled up and down. EVS disks can be operated online. Using them is the same as using common server hard disks. Compared with traditional hard disks, EVS disks have higher data reliability and I/O throughput and are easier to use. EVS disks can be used in file systems, databases, and system software applications that require block storage devices. For more information about EVS, see the *Elastic Volume Service User Guide*.

- For IMS, KMS applies to the creation of encrypted private images.

NOTE

IMS provides easy-to-use self-service image management functions. You can apply for an Elastic Cloud Server (ECS) using either a private image or a public image. You can also create a private image using an existing ECS or an external image file. For more information about IMS, see the *Image Management Service User Guide*.

- For RDS, KMS applies to disk encryption in RDS database instances.

NOTE

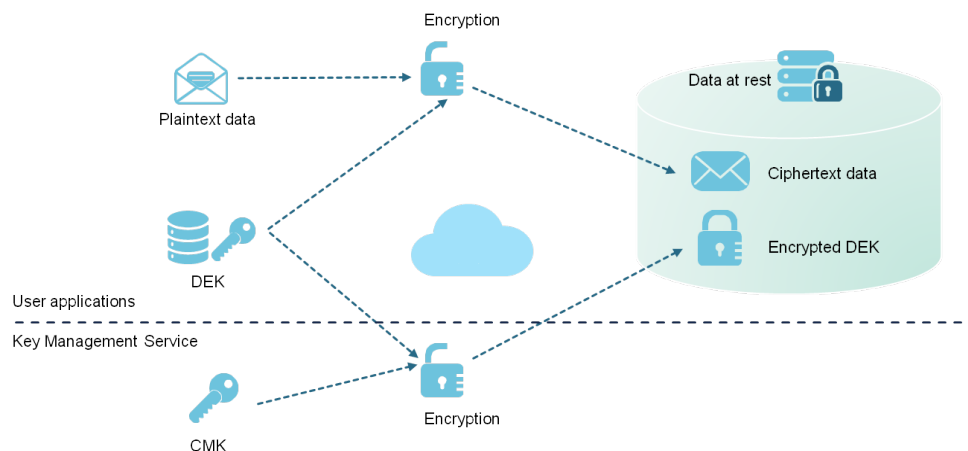
RDS is an online relational database service based on the cloud computing platform. RDS is out-of-box, reliable, scalable, and easy to manage. For more information about RDS, see the *Relational Database Service User Guide*.

- For user applications

To encrypt plaintext data, a user application can call the necessary KMS API to generate a DEK, which can then be used to encrypt the plaintext data. Then the application can store the encrypted data. In addition, the user application can call the necessary KMS APIs to create CMKs. DEKs can be stored in ciphertext after being encrypted with the CMKs. **Figure 1-1** shows envelope encryption working principles.

To ensure the security of the user's encrypted data, KMS does not save DEKs in plaintext or ciphertext. Instead, it manages the CMKs of users to enable users to obtain and use DEKs securely.

Figure 1-1 Envelope encryption working principles



1.3 Functions


KMS provides the following functions:

- Manages CMKs.
Using the KMS console or APIs, you can perform the following operations on CMKs:
 - Creating, querying, enabling, disabling, scheduling the deletion of, and canceling the deletion of CMKs
 - Importing CMKs and deleting CMK material
 - Modifying the aliases and description of CMKs
- Creates, encrypts, and decrypts DEKs.
You can create, encrypt, and decrypt a DEK by calling KMS APIs. For details, see the *Key Management Service API Reference*.
- Generates hardware true random numbers.
You can generate 512-bit hardware true random numbers using a KMS API. The 512-bit hardware true random numbers can be used as or serve as basis for keys and encryption parameters. For details, see the *Key Management Service API Reference*.

1.4 Accessing and Using KMS

1.4.1 How to Access KMS

The public cloud provides a web-based service management platform. You can access KMS using HTTPS-compliant APIs or the management console.

- Management console
If you have registered with the public cloud, you can log in to the management console directly. In the upper left corner of the console, click . Select a region or project. Choose **Security > Key Management Service**.
- API
You can access KMS using APIs. For details, see the *Key Management Service API Reference*.

1.4.2 How to Use KMS

Working with OBS

Users can upload objects to and download them from Object Storage Service (OBS) in common mode or server-side encryption mode. When users upload objects in encryption mode, data is encrypted at the server side and then securely stored on OBS in ciphertext. When users download encrypted objects, the data in ciphertext is decrypted at the server side and then provided to users in plaintext. OBS supports the server-side encryption with KMS-managed keys (SSE-KMS)

mode. In SSE-KMS mode, OBS uses the keys provided by KMS for server-side encryption.

For details about how to upload objects to OBS in SSE-KMS mode, see the *Object Storage Service User Guide*.

Working with EVS

If you enable the encryption function when creating an EVS disk and select a CMK provided by KMS to encrypt the EVS disk, data stored to the EVS disk is automatically encrypted.

For details about how to use the encryption function of EVS, see the *Elastic Volume Service User Guide*.

Working with IMS

When creating a private image using an external image file, you can enable the private image encryption function and select a CMK provided by KMS to encrypt the image.

For details about how to use the private image encryption function of Image Management Service (IMS), see the *Image Management Service User Guide*.

Working with SFS

When creating a file system on SFS, the CMK provided by KMS can be selected to encrypt the file system, so that files stored in the file system are automatically encrypted.

For details about how to use the encryption function of SFS, see the *Scalable File Service User Guide*.

Working with RDS

When creating a database instance, you can enable the disk encryption function of the database instance and select a CMK created on KMS to encrypt the disk of the database instance. The enablement of disk encryption will enhance data security.

For details about how to use the disk encryption function of RDS, see the *Relational Database Service User Guide*.

Working with User Applications

To encrypt plaintext data, a user application can call the necessary KMS APIs to generate a DEK. The DEK can then be used to encrypt the plaintext data. Then the application can store the encrypted data. In addition, the user application can call the necessary KMS APIs to create CMKs. DEKs can be stored in ciphertext after being encrypted with the CMKs. For details, see the *Key Management Service API Reference*.

1.4.3 Related Services

OBS

KMS provides central management and control capabilities of CMKs for Object Storage Service (OBS). It is used for server-side encryption with KMS-managed keys (SSE-KMS) function of OBS.

EVS

KMS provides central management and control capabilities of CMKs for Elastic Volume Service (EVS). It is applied to the encryption function of EVS.

IMS

KMS provides central management and control capabilities of CMKs for Image Management Service (IMS). It is applied to the private image encryption function of IMS.

SFS

KMS provides central management and control capabilities of CMKs for Scalable File Service (SFS). It is applied to the file system encryption function of SFS.

RDS

KMS provides central management and control capabilities of CMKs for Relational Database Service (RDS). It is applied to the disk encryption of database instances in RDS.

CTS

Cloud Trace Service (CTS) provides you with a history of KMS operations. After enabling CTS, you can view all generated traces to review and audit performed KMS operations. For details, see the *Cloud Trace Service User Guide*.

Table 1-2 KMS operations supported by CTS

Operation	Resource Type	Trace Name
Creating a CMK	cmk	createKey
Creating a DEK	cmk	createDataKey
Creating a plaintext-free DEK	cmk	createDataKeyWithoutPlaintext
Enabling a CMK	cmk	enableKey
Disabling a CMK	cmk	disableKey
Encrypting a DEK	cmk	encryptDataKey
Decrypting a DEK	cmk	decryptDataKey

Operation	Resource Type	Trace Name
Scheduling the deletion of a CMK	cmk	scheduleKeyDeletion
Canceling the scheduled deletion of a CMK	cmk	cancelKeyDeletion
Generating random numbers	rng	genRandom
Changing the alias of a CMK	cmk	updateKeyAlias
Changing the description of a CMK	cmk	updateKeyDescription
Prompting risks about CMK deletion	cmk	deleteKeyRiskTips
Importing key material	cmk	importKeyMaterial
Deleting key material	cmk	deleteImportedKeyMaterial
Adding a tag	cmk	createKeyTag
Deleting a tag	cmk	deleteKeyTag
Batch creating tags	cmk	batchCreateKeyTags
Batch deleting tags	cmk	batchDeleteKeyTags

IAM

Identity and Access Management (IAM) provides the permission management function for KMS. Only users who have KMS Administrator permissions can use KMS. To apply for KMS Administrator permissions, contact a user with Security Administrator permissions. For details, see the *Identity and Access Management User Guide*.

1.4.4 KMS Permissions Management

If you want to assign different access permissions to employees in an enterprise for the KMS resources purchased on the cloud platform, you can use Identity and Access Management (IAM) to perform refined permission management. IAM provides identity authentication, permissions management, and access control, helping you secure the access to your HUAWEI CLOUD resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific cloud resource types. For example, if you have software developers and you want to assign them the permission to access KMS but not to delete KMS or its resources, then you can create an IAM policy to assign the developers the permission to access KMS but prevent them from deleting KMS related data.

If the system account has met your requirements and you do not need to create an independent IAM user for permission control, then you can skip this section. This will not affect other functions of KMS.

IAM is offered for free, and you pay only for the billable resources in your account. For more information about IAM, see [What Is IAM?](#)

KMS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from their groups and can perform specified operations on cloud services based on the permissions.

KMS is a project-level service deployed and accessed in specific physical regions. To assign permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. Users need to switch to the authorized region when accessing KMS.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you also need to assign other roles that the permissions depend on to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- **Policies:** A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant KMS users only the permissions for managing a certain type of cloud servers. Most policies contain permissions for specific APIs, and permissions are defined using API actions. .

[Table 1-3](#) lists all the system policies of KMS.

Table 1-3 System-defined roles and policies supported by KMS

Role/Policy Name	Description	Type	Dependency
KMS Administrator	Users with this set of permissions can perform administrator operations on DEW.	System role	None
KMS CMKFullAccess	Users with this set of permissions have full permissions for encryption keys in DEW.	System policy	None

[Table 1-4](#) lists the common operations supported by each system-defined permission of KMS. Select the permissions as needed.

Table 1-4 Common operations supported by each system-defined policy or role

Operation	KMS Administrator	KMS CMKFullAccess
Create a key	√	√
Enable a key	√	√
Disable a key	√	√
Schedule key deletion	√	√
Cancel scheduled key deletion	√	√
Modify a key alias	√	√
Modify key description	√	√
Generate a random number	√	√
Create a DEK	√	√
Create a plaintext-free DEK	√	√
Encrypt a DEK	√	√
Decrypt a DEK	√	√
Obtain parameters for importing a key	√	√
Import key materials	√	√
Delete key materials	√	√
Create a grant	√	√
Revoking a grant	√	√
Retire a grant	√	√
Query the grant list	√	√
Query retirable grants	√	√
Encrypt data	√	√
Decrypt data	√	√
Enable key rotation	√	√
Modify key rotation interval	√	√
Disable key rotation	√	√
Query key rotation status	√	√

Operation	KMS Administrator	KMS CMKFullAccess
Query CMK instances	√	√
Query key tags	√	√
Query project tags	√	√
Batch add or delete key tags	√	√
Add tags to a key	√	√
Delete key tags	√	√
Query the key list	√	√
Query key details	√	√
Query instance quantity	√	√
Query quotas	√	√

Helpful Links

- [What Is IAM?](#)
- "Creating a User and Authorizing the User the Permission to Access KMS"
- "Permissions Policies and Supported Actions"
- Two types of permission policies are provided by default: default policies and custom policies. Default policies are pre-defined by IAM and cannot be modified. If default policies do not meet your requirements, you can create custom policies for fine-grained permission control.
- Configure permission policies for a user group and add users to the group so that these users can obtain operation permissions defined in the policies.

2 Management

2.1 Creating a Key

Scenario

This section describes how to create a CMK on the KMS management console. You can create up to 100 CMKs, excluding Default Master Keys.

The CMK is perfectly suited for but not limited to the following scenarios:

- Server-side encryption on OBS
- Encryption of data on EVS disks
- Encryption of private images on IMS
- File system encryption on SFS
- Disk encryption for database instances in RDS
- DEK encryption and decryption for user applications


NOTE

Aliases of Default Master Keys end with **/default**. It is not allowed to use aliases ending with **/default** for your CMKs.

Prerequisites

You have obtained an account and its password for logging in to the management console.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 4 Click **Create Key** in the upper right corner of the page. In the dialog box that is displayed, enter the alias, enterprise project, and description of the key.

Figure 2-1 Create Key dialog box

The screenshot shows a 'Create Key' dialog box with the following fields and controls:

- Alias:** A text input field containing 'KMS-c9c2'.
- Enterprise Project:** A dropdown menu with 'default' selected and a help icon (?).
- Description:** A large text area with the placeholder 'Enter a description' and a character count '0/255'.
- Tag:** Two input fields labeled 'Tag key' and 'Tag value'.
- Footer:** 'OK' and 'Cancel' buttons, and the text 'You can add 20 more tags.'

- **Alias** is the alias of the CMK to be created.
- (Optional) **Description** is the description of the CMK.
- **Enterprise Project:**
If you are an enterprise user and have created an enterprise project, select the required enterprise project from the drop-down list. The default project is **default**.
If there are no **Enterprise Management** options displayed, you do not need to configure it.

Step 5 (Optional) Add tags as needed, and enter the tag key and tag value.

NOTE

- When a CMK has been created without any tag, you can add a tag to the CMK later as necessary. Click the alias of the CMK. The page with key details is displayed. Then you can add tags to the CMK.
- The same tag (including tag key and tag value) can be used for different CMKs. However, under the same CMK, one tag key can have only one tag value.
- A maximum of 20 tags can be added for one CMK.
- If you want to delete a tag to be added when adding multiple tags, you can click **Delete** in the row where the tag to be added is located to delete the tag.

Step 6 Click **OK**.

In the CMK list, you can view created CMKs. The default status of a CMK is **Enabled**.

----End

Related Operations

- For details about how to upload objects with server-side encryption, see section **Uploading a File with Server-Side Encryption** in the *Object Storage Service User Guide*.
- For details about how to encrypt data on EVS disks, see section **Creating an EVS Disk** in the *Elastic Volume Service User Guide*.
- For details about how to encrypt private images, see section **Encrypting an Image** in the *Image Management Service User Guide*.
- For details about how to encrypt the file system on SFS, see section **Creating a File System** in the *Scalable File Service User Guide*.
- For details about how to encrypt disks for a database instance in RDS, see section **Creating an RDS MySQL DB Instance** in the *Relational Database Service User Guide*.
- For details about how to create a DEK and a plaintext-free DEK, see sections **Creating a DEK** and **Creating a Plaintext-Free DEK** in the *Key Management Service API Reference*.
- For details about how to encrypt and decrypt a DEK for a user application, see sections **Encrypting a DEK** and **Decrypting a DEK** in the *Key Management Service API Reference*.

2.2 Creating CMKs Using Imported Key Material

2.2.1 Overview

A CMK contains key metadata (key ID, key alias, description, key status, and creation date) and the key material used for encrypting and decrypting data.

- When a user uses the KMS Console to create a CMK, the KMS automatically generates a key material for the CMK.
- If you want to use your own key material, you can use the key import function on KMS Console to create a CMK whose key material is empty, and import the key material to the CMK.

Important Notes

- **Security**
You need to ensure that random sources meet your security requirements when using them to generate key material. When using the import key function, you need to be responsible for the security of your key material. Save the original backup of the key material so that the backup key material can be imported to the KMS in time when the key material is deleted accidentally.
- **Availability and Durability**
Before importing the key material into KMS, you need to ensure the availability and durability of the key material.
Differences between the imported key material and the key material generated by KMS are shown in [Table 2-1](#).

Table 2-1 Differences between the imported key material and the key material generated by KMS

Key Material Source	Difference
CMKs using the imported key material	<ul style="list-style-type: none"> • You can delete the key material, but cannot delete the CMK and its metadata. • When importing the key material, you can set the expiration time of the key material. After the key material expires, the KMS automatically deletes the key material within 24 hours, but does not delete the CMK and its metadata. It is recommended that you save a copy of the material on your local device because it may be used for re-import in cases of invalid key material or unintended deletion of key material.
CMKs using KMS generated key material	<ul style="list-style-type: none"> • The key material cannot be manually deleted. • You cannot set the expiration time for key material.

- Association
When a key material is imported to a CMK, the CMK is permanently associated with the key material. Other key material cannot be imported into the CMK.
- Uniqueness
If you use the CMK created using the imported key material to encrypt data, the encrypted data can be decrypted only by the CMK that has been used to encrypt the data, because the metadata and key material of the CMK must be consistent.

2.2.2 Importing Key Material

Scenario

If you want to use your own key material instead of the KMS-generated material, you can use the console to import your key material to KMS. CMKs created using imported material and KMS-generated material are managed together by KMS.

This section describes how to import key material through KMS Console.

NOTE

- A CMK with imported material works in the same way as one using KMS-generated material, that is, you enable and disable them as well as schedule their deletion and cancel their scheduled deletion in the same way.
- You can only import 256-bit symmetric keys.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- You have prepared the key material to be imported.

Procedure


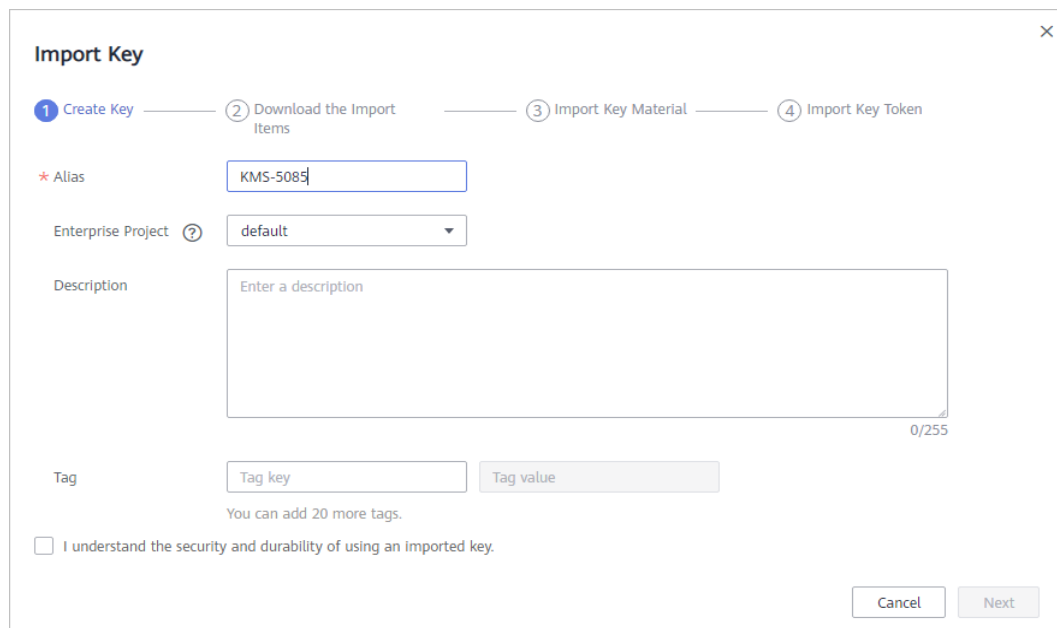
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 4** In the upper right corner, click **Import Key**.
- Step 5** In the **Import Key** dialog box, set the alias, enterprise project, and description of the key.

Figure 2-2 Creating a CMK



- Step 6** (Optional) Add tags as needed, and enter the tag key and tag value.

NOTE

- When a CMK has been created without any tag, you can add a tag to the CMK later as necessary. Click the alias of the CMK. The page with key details is displayed. Then you can add tags to the CMK.
- The same tag (including tag key and tag value) can be used for different CMKs. However, under the same CMK, one tag key can have only one tag value.
- A maximum of 20 tags can be added for one CMK.
- If you want to delete a tag to be added when adding multiple tags, you can click **Delete** in the row where the tag to be added is located to delete the tag.

- Step 7** Click **security and durability** to read and confirm information regarding the security and durability of the imported key.
- Step 8** Select **I understand the security and durability of using an imported key**, and create a CMK whose key material is empty.
- Step 9** Click **Next** to go to the **Download the Import Items** step. Select a key-wrapping algorithm according to [Table 2-2](#).

Figure 2-3 Obtaining the wrapping key and import token

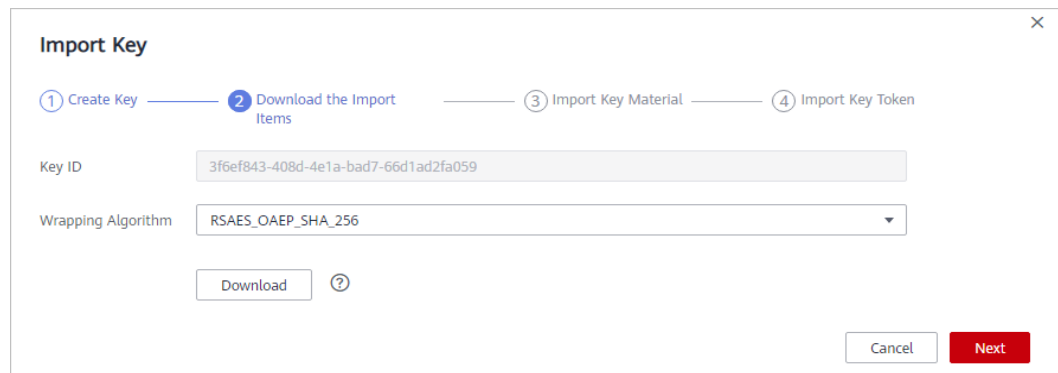
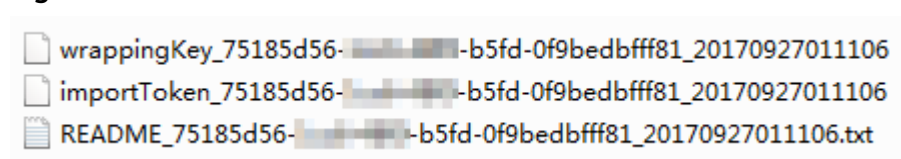


Table 2-2 Key wrapping algorithms

Algorithm	Description	Configuration
RSAES_OAEP_SHA_256	RSA encryption algorithm that uses OAEP and has the SHA-256 hash function	Choose an algorithm from the drop-down list box. <ol style="list-style-type: none"> If the HSMs support the RSAES_OAEP_SHA_256 algorithm, use RSAES_OAEP_SHA_256 to encrypt the key material. If the HSMs do not support OAEP, use RSAES_PKCS1_V1_5 to encrypt the key material. <p>NOTICE The RSAES_OAEP_SHA_1 encryption algorithm is no longer secure. Exercise caution when performing this operation.</p>
RSAES_PKCS1_V1_5	RSA encryption algorithm (v1.5) of Public-Key Cryptography Standards number 1 (PKCS #1)	
RSAES_OAEP_SHA_1	RSA encryption algorithm that uses Optimal Asymmetric Encryption Padding (OAEP) and has the SHA-1 hash function	

- Step 10** Click **Download**. The following files are downloaded: **wrappingKey**, **importToken**, and **README**. These are displayed in [Figure 2-4](#).

Figure 2-4 Downloaded files



- **wrappingKey_CMK ID_download time** is a wrapping key used to encrypt the key material.
- **importToken_CMK ID_download time** is an import token used to import key material to KMS.
- **README_CMK ID_download time** is a description file recording information such as a CMK's serial number, wrapping algorithm, wrapping key name, token file name, and the expiration time of the token file and wrapping key.

NOTICE

The wrapping key and import token expire within 24 hours of creation. If they have expired, download them again.

Alternatively, you can obtain the wrapping key and import token by calling the API.

1. Call the **get-parameters-for-import** API to obtain the wrapping key and import token.

The following example describes how to obtain the wrapping key and import token of a CMK (ID: **43f1ffd7-18fb-4568-9575-602e009b7ee8**; encryption algorithm: **RSAES_PKCS1_V1_5**).

public_key: The content of the wrapping key (Base-64 encoding) returned after calling the API

import_token: Content of the import token (Base-64 encoding) returned after calling the API

- Request example

```
{
  "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
  "wrapping_algorithm": "RSAES_PKCS1_V1_5"
}
```

- Response example:

```
{
  "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
  "public_key": "public key base64 encoded data",
  "import_token": "import token base64 encoded data",
  "expiration_time": 1501578672
}
```

2. Save the wrapping key, and convert its format according to the following procedure. Only the key material that is encrypted using the converted wrapping key can be imported to the management console.
 - a. Copy the content of the wrapping key **public_key**, save it to the **.txt** file as **PublicKey.b64**.
 - b. Run the following command to convert the Base-64 coding of the **PublicKey.b64** file to binary data, and save the converted file as **PublicKey.bin**:
openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin
3. Save the import token, copy the content of the **import_token** token, paste it to a **.txt** file, and save the file as **ImportToken.b64**.

Step 11 You use the downloaded **wrappingKey** file to encrypt the key material to be imported.

- Method 1: Use the downloaded wrapping key to encrypt the key material on your HSM. For details, see the operation guide of your HSM.
- Method 2: Use OpenSSL to encrypt the key material.

 **NOTE**

If you need to run the **openssl pkeyutl** command, the OpenSSL version must be 1.0.2 or later.

The following example describes how to use the downloaded wrapping key to encrypt the generated key material (256-bit symmetric key). The procedure is as follows:

- Run the following command to generate the key material (256-bit symmetric key) and save the generated key material as **PlaintextKeyMaterial.bin**:

openssl rand -out PlaintextKeyMaterial.bin 32

- Use the downloaded wrapping key to encrypt the key material and save the encrypted key material as **EncryptedKeyMaterial.bin**.

Replace **PublicKey.bin** in the command with the name of the wrapping key *wrappingKey_key ID_download time* downloaded in [Step 10](#).

Table 2-3 Encrypting the generated key material using the downloaded wrapping key

Wrapping Key Algorithm	Key Materials Encryption
RSAES_OAEP_SHA_256	openssl pkeyutl -in PlaintextKeyMaterial.bin -inkey PublicKey.bin -out EncryptedKeyMaterial.bin -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256
RSAES_PKCS1_V1_5	openssl rsautl -encrypt -in PlaintextKeyMaterial.bin -pkcs -inkey PublicKey.bin -keyform der -pubin -out EncryptedKeyMaterial.bin

Wrapping Key Algorithm	Key Materials Encryption
RSAES_OAEP_SHA_1	<pre>openssl pkeyutl -in PlaintextKeyMaterial.bin -inkey PublicKey.bin -out EncryptedKeyMaterial.bin -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha1</pre>

Step 12 Click **Next** to go to the **Import Key Material** step. Configure the parameters as described in [Table 2-4](#).

Figure 2-5 Importing key material

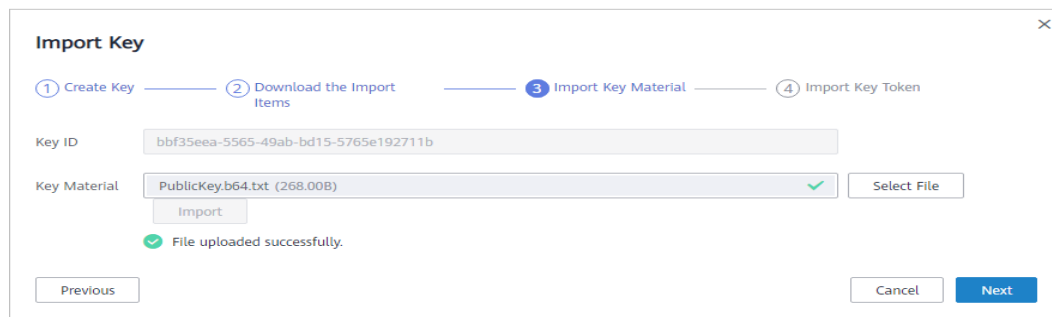


Table 2-4 Parameters for importing key material

Parameter	Description
Key ID	Random ID of a CMK generated during the CMK creation
Key material	<ol style="list-style-type: none"> Use the key material encrypted by the wrappingKey file downloaded in Step 10. Click Import to import the key material.

Step 13 Click **Next** to go to the **Import Key Token** step. Configure the parameters as described in [Table 2-5](#).

Figure 2-6 Importing a key token

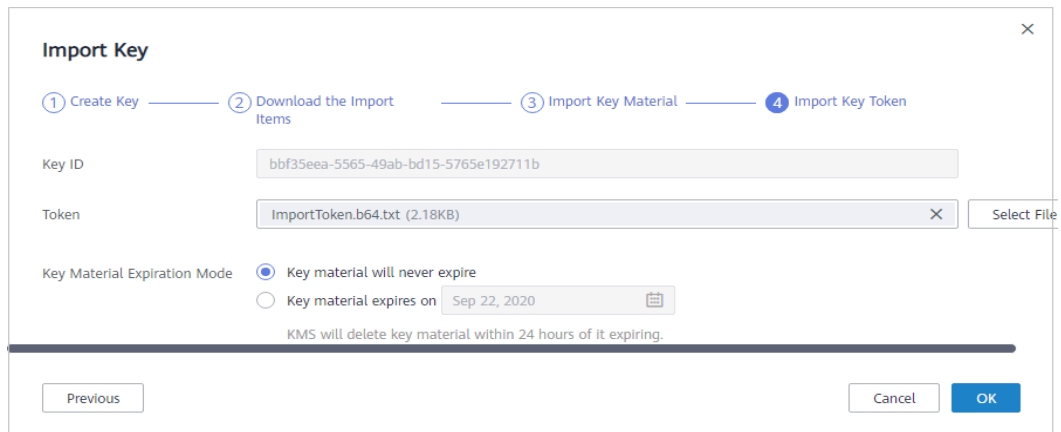


Table 2-5 Parameters for importing a key token

Parameter	Description
Key ID	Random ID of a CMK generated during the CMK creation
Token	Select the importToken downloaded in Step 10 .
Key material expiration mode	<ul style="list-style-type: none"> • Key material will never expire: This option specifies that key material will not expire after import. • Key material expires on: This option specifies the expiration time of the key material. By default, the key material expires in 24 hours after import. When the key material expires, KMS will delete them in 24 hours, making the CMK unusable and the CMK status Pending import.

Step 14 Click **OK**.

NOTICE

Key material can be successfully imported when it matches the corresponding CMK ID and token.

Your imported material is displayed in the list of CMKs. The default status of an imported CMK is **Enabled**.

----End

2.2.3 Deleting Key Material

Scenario

When importing key material, you can specify the expiration time. After the key material expires, KMS deletes it, and the status of the CMK changes to **Pending import**. You can manually delete the key material as needed. The effect of

expiration of the key material is the same as that of manual deletion of the key material.

This section describes how to delete imported key material on the management console.

 **NOTE**

- After the key material is deleted, if you need to re-import the key material, the key material to be imported must be the same as that has been deleted.
- After the same key material is re-imported, you can use the CMK to decrypt all data encrypted using this key before deletion.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- You have imported the key material for a CMK.
- The material source of the CMK is **External**.
- The CMK status is **Enabled** or **Disabled**.

Procedure

Step 1 Log in to the management console.

Step 2 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 3 In the row containing the desired CMK, click **Delete Key Material**.

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

After the deletion, the CMK will become unavailable and its status changes to **Pending import**.

----End

2.3 Scheduling the Deletion of One or Multiple CMKs

Scenario

This section describes how to use the management console to schedule the deletion of one or multiple unwanted CMKs.

If deletion is scheduled for a CMK, the deletion will not take effect immediately. Instead, it will take effect after a waiting period of 7 to 1096 days. Before the specified deletion date, you can cancel the deletion if you want to use the CMK. Once the scheduled deletion has taken effect, the CMK will be deleted permanently and you will not be able to decrypt data encrypted by it. Therefore, you are advised to exercise caution when performing this operation.

Before deleting the CMK, confirm that it is not in use and will not be used.

 **NOTE**

Default Master Keys created by KMS cannot be scheduled for deletion.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK to be deleted is in **Enabled**, **Disabled**, or **Pending Import** status.

Procedure



- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 4** In the row containing the desired CMK, click **Delete**.

Figure 2-7 Scheduling the deletion for one CMK

Alias	Status	ID	Creation Time	Operation
KMS-B6C	Pending import	b5f35ee4-5565-49ab-bd15-5765a192711b	Sep 21, 2020 17:49:18 GMT+08:00	Delete
KMS-R515	Pending deletion	a048370f-a013-421f-944c-b59faa0903af	Sep 21, 2020 16:19:03 GMT+08:00	Cancel Deletion
KMS-a975	Enabled	6aa54ba5-f750-47f1-91d7-f6a3f5a4f226	Sep 21, 2020 16:19:22 GMT+08:00	Disable Delete

- Step 5** In the dialog box that is displayed, enter the number of days after which you want the deletion to take effect.

Figure 2-8 Scheduling a deletion time

 **Are you sure you want to delete the following key?**

Deleted keys cannot be restored. Any data encrypted using them will be unreadable. The keys will be deleted after the specified number of days. Before this occurs, the deletion can be cancelled.

Waiting Period (days)

Alias	Status	ID
KMS-e603	Enabled	df620ba4-a347-4063-a52a-e1e982252e24

I understand the impact of deleting keys.

- Step 6** Click **Yes** to schedule the deletion.

 **NOTE**

To delete multiple CMKs at a time, select them and click **Delete** in the upper left corner of the list.

----End

2.4 Encrypting and Decrypting Small Data Online

This section describes how to use an online tool to encrypt and decrypt data less than or equal to 4 KB on the KMS console.

 **NOTE**


- The online tool cannot encrypt or decrypt small data by using Default Master Keys.
- You can call APIs to use a Default Master Key to encrypt or decrypt small data. For details, see the *Key Management Service API Reference*.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The desired CMK is in **Enabled** status.

Encrypting Data

Step 1 Log in to the management console.

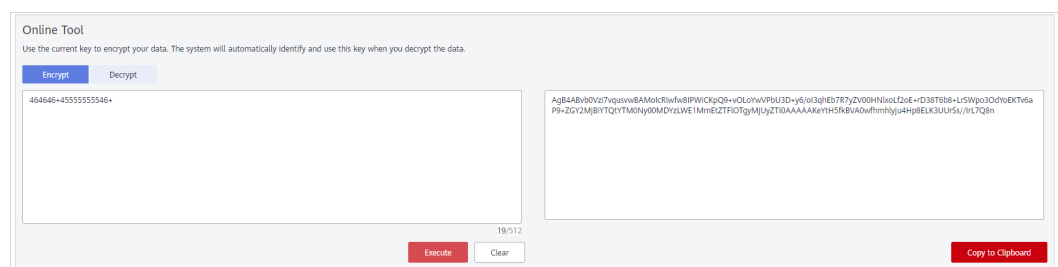
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 4 Click the alias of the desired CMK to view its details on the online data encryption page.

Step 5 Click **Encrypt**. In the text box on the left, enter the data to be encrypted.

Figure 2-9 Encrypting data



Step 6 Click **Execute**. The data encryption result is displayed in the text box on the right.

 **NOTE**

- The key you clicked is used for encryption.
- To clear your input, click **Clear**.
- To copy the encrypted data, click **Copy to Clipboard**. You can then paste and save it to a local file.

----End

Decrypting Data

Step 1 Log in to the management console.

Step 2 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 3 Click the alias of an enabled key (excepting Default Master Keys) to open the online tool page.

Step 4 Click **Decrypt**. In the text box on the left, enter the data to be decrypted.

 **NOTE**

- The online tool automatically identifies the key used for data encryption, and uses it to decrypt data.
- If the key has been deleted, the decryption will fail.

Step 5 Click **Execute**. The data decryption result is displayed in plaintext in the text box on the right.

 **NOTE**

To copy the decrypted data, click **Copy to Clipboard**. You can then paste and save it to a local file.

----End

2.5 Managing Tags

2.5.1 Adding a Tag

Scenario

Tags are used to identify CMKs. You can add tags to CMKs so that you can classify CMKs, trace them, and collect their usage status according to the tags.

NOTICE

KMS does not support adding tags to Default Master Keys.

Prerequisites

You have obtained an account and its password for logging in to the management console.

Procedure


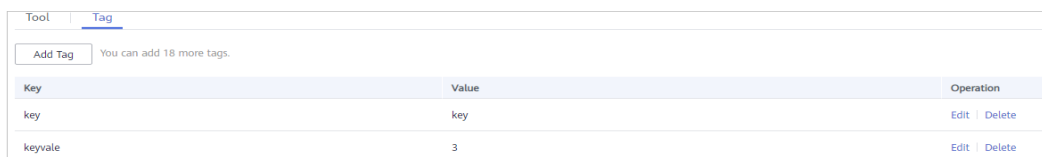
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 4** Click the alias of the desired CMK to view its details.
- Step 5** Click **Tags** to go to the tag management page.

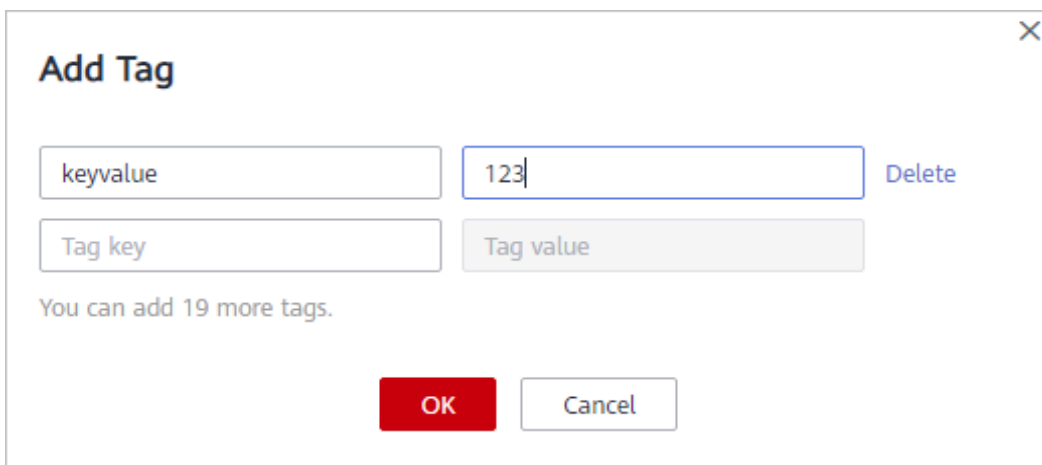
Figure 2-10 Managing tags



Key	Value	Operation
key	key	Edit Delete
keyvale	3	Edit Delete

- Step 6** Click **Add Tag**. In the **Add Tag** dialog box, enter the tag key and tag value. [Table 2-6](#) describes the parameters.

Figure 2-11 Adding a tag



Add Tag

keyvalue 123 Delete

Tag key Tag value

You can add 19 more tags.

OK Cancel

NOTE

If you want to delete a tag to be added when adding multiple tags, you can click **Delete** in the row where the tag to be added is located to delete the tag.

Table 2-6 Tag parameters

Parameter	Description	Value	Example Value
Tag key	Name of a tag. The same tag (including tag key and tag value) can be used for different CMKs. However, under the same CMK, one tag key can have only one tag value. A maximum of 20 tags can be added for one CMK.	<ul style="list-style-type: none"> • Mandatory. • Each tag key must be unique under the same CMK. • Contains a maximum of 36 characters. • Only digits, letters, underscores (_), and hyphens (-) are allowed. 	cost
Tag value	Value of the tag	<ul style="list-style-type: none"> • This parameter can be empty. • Can contain a maximum of 43 characters. • Only digits, letters, underscores (_), and hyphens (-) are allowed. 	100

Step 7 Click **OK** to complete.

----End

2.5.2 Searching for Tags

Scenario


This section describes how to search for tags through KMS. You can search for tags of all CMKs that meet the search criteria in the current project.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- Tags have been added.

Procedure

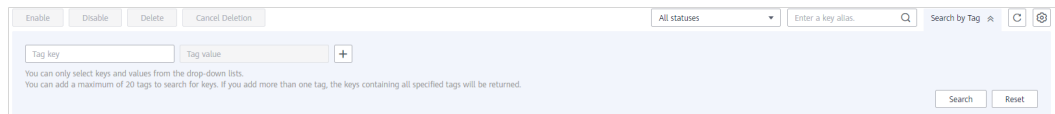
Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the management console and select a region or project.


Step 3 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 4 Click **Search by Tag** to show the search box.


Figure 2-12 Searching for tags



Step 5 In the search box, enter the tag key and tag value.

Step 6 Click  to add the input to the search criteria, and click **Search**. The list displays the CMKs that meet the search criteria.

NOTE

- Multiple tags can be added at one search. A maximum of 20 tags can be added for one search. If multiple tags are searched for at one time, only CMKs meet the combined search criteria will be displayed in the search result.
- If you want to delete an added tag from the search criteria, click  next to the tag.
- You can click **Reset** to reset the search criteria.

----End

2.5.3 Modifying Tag Values

Scenario

This section describes how to modify tag values on the KMS management console.

Prerequisites

You have obtained an account and its password for logging in to the management console.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 4** Click the alias of the desired CMK to view its details.
- Step 5** Click **Tags** to go to the tag management page.

Figure 2-13 Managing tags

Key	Value	Operation
key	key	Edit Delete
keyvale	3	Edit Delete

- Step 6** Click **Edit** of the target tag, and the **Edit Tag** dialog box is displayed.
- Step 7** In the **Edit Tag** dialog box, enter a tag value, and click **OK** to complete the editing.
- End

2.5.4 Deleting Tags

Scenario

This section describes how to delete tags on the KMS management console.

Prerequisites

You have obtained an account and its password for logging in to the management console.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 4** Click the alias of the desired CMK to view its details.
- Step 5** Click **Tags** to go to the tag management page.

Figure 2-14 Managing tags



Key	Value	Operation
key	key	Edit Delete
keyvale	3	Edit Delete

- Step 6** Click **Delete** of the target tag, and the **Delete Tag** dialog box is displayed.
- Step 7** In the **Delete Tag** dialog box, click **Yes** to complete the deletion.
- End

2.6 Managing CMKs

2.6.1 Querying a CMK

Scenario

This section describes how to use the management console to view the information about a CMK, such as its alias, status, ID, and creation time. The status of a CMK can be **Enabled**, **Disabled**, **Pending deletion**, or **Pending import**.

Prerequisites

You have obtained an account and its password for logging in to the management console.

Procedure


- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 4** In the CMK list you can view details about the CMKs.

Figure 2-15 CMK list



Alias	Status	ID	Creation Time	Operation
KMS-8c5	Pending import	bbf356ea-5505-49ab-bd15-5705e192711b	Sep 21, 2020 17:49:18 GMT+08:00	Delete
KMS-8515	Pending deletion	a048370f-a013-4211-944c-559faa0003af	Sep 21, 2020 16:19:03 GMT+08:00	Cancel Deletion
KMS-a975	Enabled	6aa54ba5-f790-47f1-91d7-fbe35ef4f28	Sep 21, 2020 16:15:22 GMT+08:00	Disable Delete

NOTE



- Select the CMK status from the drop-down list of **All statuses**. Then the CMK list displays only the CMKs in the corresponding state.
- Enter the alias of a CMK in the search box on top of the CMK list. Click  or press Enter to search for the specified CMK.
- You can click **Search Tag** to search for the CMK that meets the search criteria.
- You can click  at the upper right corner on top of the CMK list to show or hide columns of the CMK list.

Table 2-7 describes the parameters of a CMK list.



Table 2-7 CMK list parameters

Parameter	Description
Alias	Alias of a CMK

Parameter	Description
Status	Status of a CMK, which can be one of the following: <ul style="list-style-type: none"> • Enabled The CMK is enabled. • Disabled The CMK is disabled. • Pending deletion The CMK is scheduled for deletion. • Pending import If your CMK does not have the key material, its status is Pending import.
ID	Random ID of a CMK generated during the CMK creation
Creation Time	Creation time of the CMK
Expiration Time	Expiration time of the key material. When the material expires, the CMK becomes an empty CMK.
Origin	Source of key material, which can be one of the following: <ul style="list-style-type: none"> • External You import the key material for the CMK. • Key Management Service The CMK uses KMS-generated material.

Step 5 You can click the alias of a CMK to view its details.

Figure 2-16 Viewing CMK details

Alias	KMS-8cfc 
Status	Pending import
ID	bbf35eea-5565-49ab-bd15-5765e192711b
Creation Time	Sep 21, 2020 17:49:18 GMT+08:00
Description	-- 

----End

2.6.2 Changing the Alias and Description of a CMK

Scenario

The alias of a CMK is a user-friendly name designed to help you locate the CMK easier.

This section describes how to change the alias and description of a CMK on the KMS management console.

NOTICE

- A Default Master Key (the alias suffix of which is **/default**) does not allow alias and description changes.
 - The alias and description of a CMK cannot be changed if the CMK is in **Pending deletion** status.
-

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK is in **Enabled**, **Disabled**, or **Pending import** status.

Procedure






- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.
- Step 4** Click the alias of the desired CMK. Details about the CMK are displayed.
- Step 5** To change the alias or description of the CMK, click  next to the value of **Alias** or **Description**.

Figure 2-17 CMK details

Alias	KMS-8cfc 
Status	Pending import
ID	bbf35eea-5565-49ab-bd15-5765e192711b
Creation Time	Sep 21, 2020 17:49:18 GMT+08:00
Description	-- 

 NOTE

- The alias must be 1 to 255 characters in length. Only digits, letters, underscores (_), hyphens (-), colons (:), and forward slashes (/) are allowed.
- Length of the description cannot exceed 255 characters.

Step 6 Click  to save the changes.

----End

2.6.3 Enabling One or Multiple CMKs

Scenario


This section describes how to use the management console to enable one or multiple CMKs. Only enabled CMKs can be used to encrypt/decrypt data. A new CMK is in the **Enabled** state by default.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK you want to enable is in **Disabled** status.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 4 In the row containing the desired CMK, click **Enable**.

Figure 2-18 Enabling one CMK

Alias	Status	ID	Creation Time	Operation
<input type="checkbox"/> KMS-8cfc	Pending import	bbf35eea-5565-49ab-bd15-5765e192711b	Sep 21, 2020 17:49:18 GMT+08:00	Delete
<input type="checkbox"/> KMS-8515	Pending deletion	a048370f-a013-421f-944c-b59faa093ef	Sep 21, 2020 16:19:03 GMT+08:00	Cancel Deletion
<input type="checkbox"/> KMS-a975	Disabled	6aa54ba5-f790-47f1-91d7-f9e3f5e4f28	Sep 21, 2020 16:15:22 GMT+08:00	Enable Delete

Step 5 In the dialog box that is displayed, click **Yes** to enable the CMK.

NOTE

To enable multiple CMKs at a time, select them and click **Enable** in the upper left corner of the list.

----End

2.6.4 Disabling One or Multiple CMKs

Scenario

This section describes how to use the management console to disable one or multiple CMKs, thereby protecting data in urgent cases.

After being disabled, a CMK cannot be used to encrypt or decrypt any data. Before using a disabled CMK to encrypt or decrypt data, you must enable it by following instructions in [Enabling One or Multiple CMKs](#).

NOTE

Default Master Keys created by KMS cannot be disabled.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK you want to disable is in **Enabled** status.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 4 In the row containing the desired CMK, click **Disable**.

Figure 2-19 Disabling one CMK

Alias	Status	ID	Creation Time	Operation
<input type="checkbox"/> KMS-8cfc	Pending import	bbf35eea-5565-49ab-bd15-5765e192711b	Sep 21, 2020 17:49:18 GMT+08:00	Delete
<input type="checkbox"/> KMS-8515	Pending deletion	a048370f-a013-421f-944c-b59faa093ef	Sep 21, 2020 16:19:03 GMT+08:00	Cancel Deletion
<input type="checkbox"/> KMS-a975	Enabled	6aa54ba5-f790-47f1-91d7-f9e3f5e4f28	Sep 21, 2020 16:15:22 GMT+08:00	Disable Delete

----End

2.6.5 Canceling the Scheduled Deletion of One or Multiple CMKs

Scenario


This section describes how to use the management console to cancel the scheduled deletion of one or multiple CMKs prior to deletion execution.

Prerequisites

- You have obtained an account and its password for logging in to the management console.
- The CMK 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 management console and select a region or project.

Step 3 Choose **Security > Key Management Service**. The **Key Management Service** page is displayed.

Step 4 In the row containing the desired CMK, click **Cancel Deletion**.

Figure 2-20 Canceling the scheduled deletion of one CMK

Alias	Status	ID	Creation Time	Operation
<input type="checkbox"/> KMS-8cfc	Pending import	bbf35eea-5565-49ab-bd15-5765e192711b	Sep 21, 2020 17:49:18 GMT+08:00	Delete
<input type="checkbox"/> KMS-8515	Pending deletion	a048370f-a013-421f-944c-b59faa9093ef	Sep 21, 2020 16:19:03 GMT+08:00	Cancel Deletion
<input type="checkbox"/> KMS-a975	Enabled	6aa54ba5-f790-47f1-91d7-f8c35ef4f28	Sep 21, 2020 16:15:22 GMT+08:00	Disable Delete

Step 5 In the displayed dialog box, click **OK** to cancel the scheduled deletion for the CMK.

NOTE

To cancel the deletion of multiple CMKs at a time, select them and click **Cancel Deletion** in the upper left corner of the list.

----End

2.7 Permissions Management

2.7.1 Creating a User and Authorizing the User the Permission to Access KMS

This section describes how to use **IAM** to implement fine-grained permissions control for your DEW resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has its own security credentials to access DEW resources.
- Grant users only the permissions required to perform a task.
- Delegate a trusted account or cloud service to perform professional, efficient O&M on your KMS resources.

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

This section describes the procedure for granting permissions (see [Figure 2-21](#)).

Prerequisites

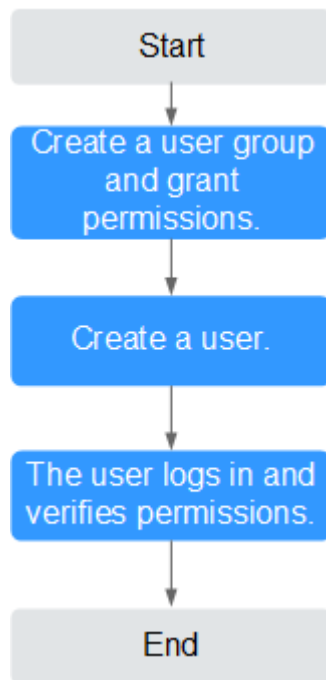
Before authorizing permissions to a user group, you need to know which KMS permissions can be added to the user group. [Table 2-8](#) lists the KMS system policies. For the permissions of other services, see [Permission Description](#).

Table 2-8 System-defined roles and policies supported by KMS

Role/Policy Name	Description	Type	Dependency
KMS Administrator	Users with this set of permissions can perform administrator operations on DEW.	System role	None
KMS CMKFullAccess	Users with this set of permissions have full permissions for encryption keys in DEW.	System policy	None

Authorization Process

Figure 2-21 Authorizing the KMS access permission to a user



1. **Create a user group and assign permissions.**
Create a user group on the IAM console and grant the user group the **KMS CMKFullAccess** permission (indicating full permissions for keys) for DEW.
2. **Create a user and add it to a user group.**
Create a user on the IAM console and add the user to the user group created in **1**.
3. **Log in** and verify permissions.
Log in to the CGS console by using the newly created user, and verify that the user only has read permissions for CGS.
 - Choose **Service List > Key Management Service**. In the navigation pane, choose **Key Pair Service**. If a message appears indicating lack of permissions, the **KMS CMKFullAccess** policy has taken effect.
 - Click **Service List** and select a service other than DEW. If a message is displayed indicating that you do not have permission to access the service, the **KMS CMKFullAccess** policy has taken effect.

2.7.2 Creating a Custom Policy

Custom policies can be created as a supplement to the system policies of KMS. For the actions that can be added to custom policies, see "Permissions Policies and Supported Actions".

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.

Custom KMS policy parameters:

- **Select service:** Select **Key Management Service**.
 - **Select action:** Set it as required.
 - **(Optional) Select resource:** Set **Resources** to **Specific** and **KeyId** to **Specify resource path**. In the dialog box that is displayed, set **Path** to the ID generated when the key was created. For details about how to obtain the ID, see "Viewing a CMK".
- 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 DEW custom policies.

Example Custom Policies

- Example 1: authorizing users to create and import keys

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:serverKMS:create"
      ]
    }
  ]
}
```

- Example 2: forbidding users from deleting account key pairs

A deny policy must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used if you need to assign permissions of the **KMS Administrator** policy to a user but also forbid the user from deleting key pairs (**ecs:serverKeypairs:delete**). Create a custom policy with the action to delete key pairs, set its **Effect** to **Deny**, and assign both this and the **KMS Administrator** policies to the group the user belongs to. Then the user can perform all operations on key pairs except deleting them. The following is a policy for denying key pair deletion.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ecs:serverKeypairs:delete"
      ]
    },
  ]
}
```

- Multi-action policy

A custom policy can contain actions of multiple services that are all of the global or project-level type. The following is a policy with multiple statements:

```
{
  "Version": "1.1",
  "Statement": [
    {
```

```
    "Effect": "Allow",
    "Action": [
      "ecs:serverKeypairs:create"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:cmk:*",
      "kms:dek:*",
      "kms:grant:*",
      "kms:tag:*"
    ]
  }
]
```

3 FAQs

3.1 What Is Key Management Service?

Key Management Service (KMS) is a secure, reliable, and easy-to-use service that helps users centrally manage and safeguard their Customer Master Keys (CMKs).

This service uses hardware security modules (HSMs) to protect CMKs. HSMs help you create and control CMKs with ease. All CMKs are protected by root keys in HSMs to avoid leakage caused by human error. KMS implements access control and log-based tracking on all operations involving CMKs. Additionally, it provides CMK operation records, meeting your audit and regulatory compliance requirements.

3.2 What Is a Customer Master Key?

A Customer Master Key (CMK) is a Key Encryption Key (KEK) created by a user using KMS. It is used to encrypt and protect Data Encryption Keys (DEKs). One CMK can be used to encrypt one or multiple DEKs.

3.3 What Is a Data Encryption Key?

A data encryption key (DEK) is used to encrypt data.

3.4 Why Cannot I Delete a CMK Immediately?

The decision to delete a CMK should be taken with caution. Before deletion, confirm that the CMK's encrypted data has all been migrated. Once the CMK is deleted, you will not be able to decrypt data with it. Therefore, KMS offers a waiting period of 7 to 1096 days for the deletion to finally take effect. On the scheduled day of deletion, the CMK will be permanently deleted. However, prior to the scheduled day, you can still cancel the deletion.

3.5 Which Cloud Services Can Use KMS for Encryption?

Object Storage Service (OBS), Elastic Volume Service (EVS), Image Management Service (IMS), and Relational Database Service (RDS) can use KMS for encryption.

A Change History

Date	Description
2021-06-03	This issue is the second official release. Added section "KMS Permissions Management". Added section "Permissions Management".
2020-12-16	This issue is the first official release.