

Data Encryption Workshop

User Guide

Issue 02
Date 2023-01-30



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



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

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

Notice

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

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

Contents

1 Key Management Service.....	1
1.1 Key Types.....	1
1.2 Creating a CMK.....	2
1.3 Creating CMKs Using Imported Key Materials.....	5
1.3.1 Overview.....	5
1.3.2 Importing Key Materials.....	7
1.3.3 Deleting Key Materials.....	15
1.4 Managing CMKs.....	16
1.4.1 Viewing a CMK.....	16
1.4.2 Enabling One or More CMKs.....	18
1.4.3 Disabling One or More CMKs.....	19
1.4.4 Deleting One or More CMKs.....	20
1.4.5 Canceling the Scheduled Deletion of One or More CMKs.....	21
1.4.6 Adding a Key to a Project.....	22
1.5 Using the Online Tool to Encrypt and Decrypt Small-Size Data.....	23
1.6 Managing Tags.....	25
1.6.1 Adding a Tag.....	25
1.6.2 Searching for a CMK by Tag.....	26
1.6.3 Modifying Tag Values.....	28
1.6.4 Deleting Tags.....	28
1.7 Rotating CMKs.....	29
1.7.1 About Key Rotation.....	29
1.7.2 Enabling Key Rotation.....	31
1.7.3 Disabling Key Rotation.....	34
1.8 Managing a Grant.....	36
1.8.1 Creating a Grant.....	36
1.8.2 Querying a Grant.....	39
1.8.3 Revoking a Grant.....	40
2 Cloud Secret Management Service.....	42
2.1 Creating a Secret.....	42
2.2 Managing Secrets.....	43
2.2.1 Viewing a Secret.....	43
2.2.2 Deleting a Secret.....	45

2.3 Managing Secret Versions.....	46
2.3.1 Viewing a Secret Value.....	46
2.3.2 Managing Secret Version Statuses.....	48
2.4 Managing Tags.....	49
2.4.1 Adding a Tag.....	49
2.4.2 Searching for a Secret by Tag.....	51
2.4.3 Modifying a Tag Value.....	52
2.4.4 Deleting a Tag.....	53
3 Key Pair Service.....	55
3.1 Creating a Key Pair.....	55
3.2 Importing a Key Pair.....	60
3.3 Upgrading a Key Pair.....	62
3.4 Managing Key Pairs.....	64
3.4.1 Binding a Key Pair.....	64
3.4.2 Viewing a Key Pair.....	66
3.4.3 Resetting a Key Pair.....	69
3.4.4 Replacing a Key Pair.....	70
3.4.5 Unbinding a Key Pair.....	72
3.4.6 Deleting a Key Pair.....	74
3.5 Managing Private Keys.....	74
3.5.1 Importing a Private Key.....	74
3.5.2 Exporting a Private Key.....	76
3.5.3 Clearing a Private Key.....	77
3.6 Using a Private Key to Log In to the Linux ECS.....	78
3.7 Using a Private Key to Obtain the Login Password of Windows ECS	81
4 Dedicated HSM.....	83
4.1 Operation Guide.....	83
4.2 Purchasing a Dedicated HSM Instance.....	85
4.2.1 Creating a Dedicated HSM Instance.....	85
4.2.2 Activating a Dedicated HSM Instance.....	88
4.3 Viewing Dedicated HSM Instances.....	91
4.4 Using Dedicated HSM Instances.....	95
5 Auditing Logs.....	98
5.1 Operations supported by CTS.....	98
5.2 Using CTS to Query DEW Operation Traces.....	99
6 Permission Control.....	102
6.1 Creating a User and Authorizing the User the Permission to Access DEW.....	102
6.2 Creating a Custom DEW Policy.....	107
A Change History.....	110

1 Key Management Service

1.1 Key Types

CMKs can be categorized into symmetric keys and asymmetric keys.

Symmetric keys are commonly used for data encryption. Asymmetric keys are used for digital signature verification or sensitive information encryption in systems where the trust relationship is not mutual. An asymmetric key consists of a public key and a private key. The public key can be sent to anyone. The private key must be securely stored and only accessible to trusted users.

An asymmetric key can be used to generate and verify a signature. To securely transfer data, a signer sends the public key to a receiver, uses the private key to sign data, and then sends the data and signature to the receiver. The receiver can use the public key to verify the signature.

Table 1-1 Key algorithms supported by KMS

Key Type	Algorithm Type	Key Specifications	Description	Usage
Symmetric key	AES	AES_256	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Asymmetric key	RSA	<ul style="list-style-type: none">• RSA_2048• RSA_3072• RSA_4096	RSA asymmetric password	Encrypts and decrypts a small amount of data or creates digital signatures.
	ECC	<ul style="list-style-type: none">• EC_P256• EC_P384	Elliptic curve recommended by NIST	Digital signature

1.2 Creating a CMK

This section describes how to create a CMK on the KMS console.

CMKs can be categorized into symmetric keys and asymmetric keys.

Prerequisites

The account has KMS CMKFullAccess or higher permissions.

Constraints


- You can create up to 50 CMKs, excluding default master keys.
- Symmetric keys are created using the AES-256 encryption and decryption algorithm. The key is 256 bit long and can be used to encrypt and decrypt a small amount of data or data keys.
- Asymmetric keys are created using RSA or ECC algorithms. RSA keys can be used for encryption, decryption, digital signature, and signature verification. ECC keys can be used only for digital signature and signature verification.
- Aliases of default master keys end with **/default**. Therefore, in choosing aliases for your CMKs, do not use aliases ending with **/default**.
- DEW does not limit the number of times that a CMK can be called.

Scenarios

- [Encrypt data in OBS](#)
- [Encrypt data in EVS](#)
- [Encrypt data in IMS](#)
- [Encrypt an RDS DB instance](#)
- Direct encryption and decryption of small volumes of data
- DEK encryption and decryption for user applications
- Asymmetric keys can be used for digital signatures and signature verification.

Creating a CMK

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 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 Click **Create Key** in the upper right corner.

Step 5 Configure parameters in the **Create Key** dialog box.

Figure 1-1 Creating a key

Create Key

★ Alias

Key Algorithm

Usage

★ Enterprise Project [Create Enterprise Project](#)

Description 0/255

Tag

You can add 20 more tags.

Key Price

API Request Price

OK Cancel

- **Alias** is the alias of the CMK to be created.

NOTE

- You can enter digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/).
- You can enter up to 255 characters.
- **Key Algorithm:** Select a key algorithm. For more information, see [Table 1-2](#).

Table 1-2 Key algorithms supported by KMS

Key Type	Algorithm Type	Key Specifications	Description	Usage
Symmetric key	AES	AES_256	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Asymmetric key	RSA	<ul style="list-style-type: none">- RSA_2048- RSA_3072- RSA_4096	RSA asymmetric password	Encrypts and decrypts a small amount of data or creates digital signatures.
	ECC	<ul style="list-style-type: none">- EC_P256- EC_P384	Elliptic curve recommended by NIST	Digital signature

- **Usage:** Select **SIGN_VERIFY** or **ENCRYPT_DECRYPT**.
 - For a symmetric key, the default value is **ENCRYPT_DECRYPT**.
 - For RSA asymmetric keys, select **ENCRYPT_DECRYPT** or **SIGN_VERIFY**. The default value is **SIGN_VERIFY**.
 - For an ECC asymmetric key, the default value is **SIGN_VERIFY**.

NOTE

The key usage can only be configured during key creation and cannot be modified afterwards.

- (Optional) **Description** is the description of the CMK.
- The **Enterprise Project** parameter needs to be set only for enterprise users. 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.

NOTE

https://support.huaweicloud.com/usermanual-em/em_eps_01_0000.html

- You can use enterprise projects to manage cloud resources and project members. For more information about enterprise projects, see [What Is Enterprise Project Management Service?](#)
- For details about how to enable the enterprise project function, see [Enabling the Enterprise Center](#).

Step 6 (Optional) Add tags to the CMK 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, click the **Tags** tab, and click **Add 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.
- If you want to delete a tag from the tag list 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 **OK**. A message is displayed in the upper right corner of the page, indicating that the key is created successfully.

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 Console Operation Guide*.
- For details about how to encrypt data on EVS disks, see section **Purchasing 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 disks for a database instance in RDS, see section "Purchasing an 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 *Data Encryption Workshop 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 *Data Encryption Workshop API Reference*.

1.3 Creating CMKs Using Imported Key Materials

1.3.1 Overview

A CMK contains key metadata (key ID, key alias, description, key status, and creation date) and key materials 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 the 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 materials. When using the import key function, you need to be responsible for the security of your key materials. 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 1-3](#).

Table 1-3 Differences between the imported key material and the key material generated by KMS

Key Material Source	Difference
CMKs using imported key materials	<ul style="list-style-type: none"> • You can delete the key material, but cannot delete the CMK and its metadata. • Such keys cannot be rotated. • 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 materials or key material mis-deletion. <p>NOTE Keys using RSA_2048, RSA_3072, RSA_4096, EC_P256, and EC_P384 algorithms are permanently valid. Their key materials cannot be manually deleted, and their expiration time cannot be configured.</p>
CMKs using KMS generated key materials	<ul style="list-style-type: none"> • The key material cannot be manually deleted. • Symmetric keys can be rotated. • 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 materials 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.

1.3.2 Importing Key Materials

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

This section describes how to import key materials on the KMS console.

Procedure



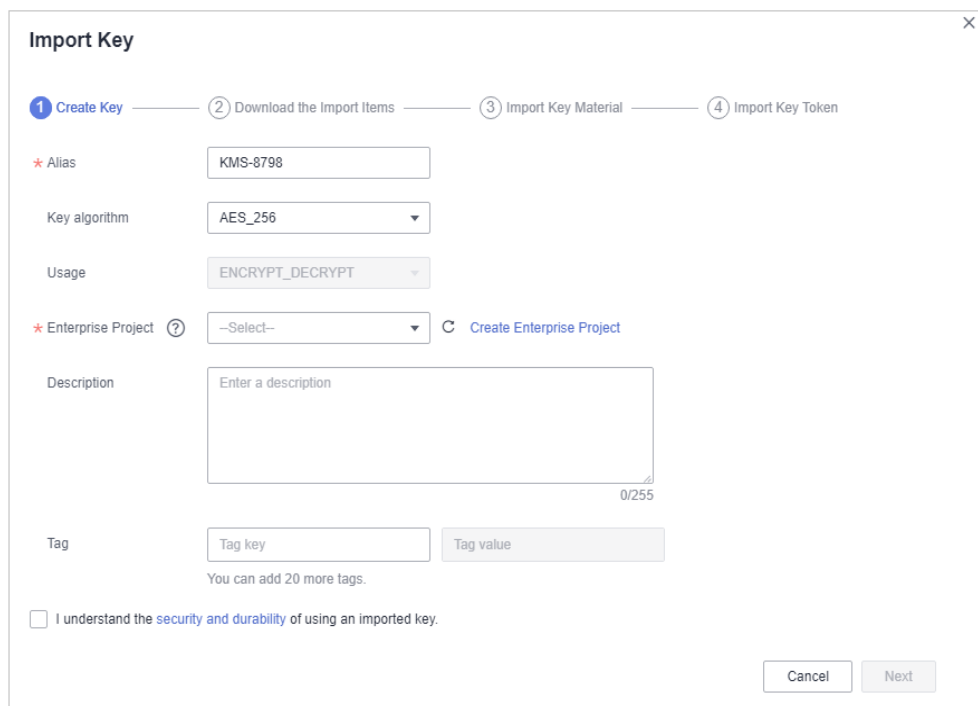
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** Click **Import Key**. The **Import Key** dialog box is displayed.
- Step 5** Configure key parameters.

Figure 1-2 Creating an empty key



Import Key

1 Create Key — 2 Download the Import Items — 3 Import Key Material — 4 Import Key Token

* Alias

Key algorithm

Usage

* Enterprise Project [Create Enterprise Project](#)

Description 0/255

Tag

You can add 20 more tags.

I understand the [security and durability](#) of using an imported key.

- **Alias** is the alias of the CMK to be created.

 **NOTE**

- You can enter digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/).
 - You can enter up to 255 characters.
- **Key Algorithm:** Select a key algorithm. For more information, see [Table 1-4](#).

Table 1-4 Key algorithms supported by KMS

Key Type	Algorithm Type	Key Specifications	Description	Usage
Symmetric key	AES	AES_256	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Asymmetric key	RSA	<ul style="list-style-type: none"> - RSA_2048 - RSA_3072 - RSA_4096 	RSA asymmetric password	Encrypts and decrypts a small amount of data or creates digital signatures.
	ECC	<ul style="list-style-type: none"> - EC_P256 - EC_P384 	Elliptic curve recommended by NIST	Digital signature

- **Usage:** Select **SIGN_VERIFY** or **ENCRYPT_DECRYPT**.
 - For a symmetric key, the default value is **ENCRYPT_DECRYPT**.
 - For RSA asymmetric keys, select **ENCRYPT_DECRYPT** or **SIGN_VERIFY**. The default value is **SIGN_VERIFY**.
 - For an ECC asymmetric key, the default value is **SIGN_VERIFY**.

 **NOTE**

The key usage can only be configured during key creation and cannot be modified afterwards.

- (Optional) **Description** is the description of the CMK.
- The **Enterprise Project** parameter needs to be set only for enterprise users. 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.

 **NOTE**

https://support.huaweicloud.com/usermanual-em/em_eps_01_0000.html

- You can use enterprise projects to manage cloud resources and project members. For more information about enterprise projects, see [What Is Enterprise Project Management Service?](#)
- For details about how to enable the enterprise project function, see [Enabling the Enterprise Center.](#)

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

 **NOTE**

- If a CMK was created without any tag, you can add a tag to the CMK later as necessary. Click the alias of the CMK, click the **Tags** tab, and click **Add 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 each CMK.
- If you want to delete a tag from the tag list 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 understand 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 based on [Table 1-5](#).

Figure 1-3 Obtaining the wrapping key and import token

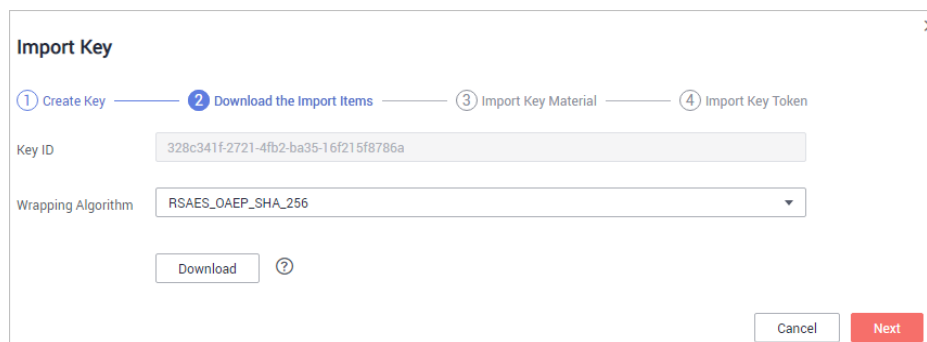


Table 1-5 Key wrapping algorithms

Algorithm	Description	Configuration
RSAES_OAEP_SHA_256	RSA encryption algorithm that uses OAEP and has the SHA-256 hash function	Select an encryption algorithm based on your HSM functions. 1. If the HSMs support the RSAES_OAEP_SHA_256 algorithm, use RSAES_OAEP_SHA_256 to encrypt key materials.

Algorithm	Description	Configuration
RSAES_OAEP_SHA_1	RSA encryption algorithm that uses Optimal Asymmetric Encryption Padding (OAEP) and has the SHA-1 hash function	<p>2. If the HSMs do not support OAEP, use RSAES_PKCS1_V1_5 to encrypt key materials.</p> <p>NOTICE The RSAES_OAEP_SHA_1 encryption algorithm is no longer secure. Exercise caution when performing this operation.</p>

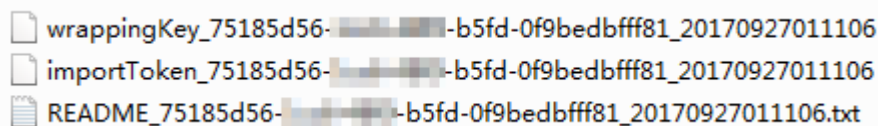
 **NOTE**

If you stop a key material import process and want to try again, click **Import Key Material** in the row of the required CMK, and import key material in the dialog box that is displayed.

Step 10 Obtain the wrapping key and import token. If you already have a key material, skip this step.

1. Obtain the wrapping key and import token.
 - Method 1: Click **Download and Continue**. The downloaded files include the wrapping key, import token, and description file, as shown below.

Figure 1-4 Downloading a file



- **wrappingKey_KeyID_DownloadTime** is the wrapping key. It is encoded in binary format and used to encrypt the wrapping key of the key material.
- **importToken_KeyID_DownloadTime** is a token used to import key materials to KMS.
- **README_KeyID_DownloadTime** 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 in 24 hours. If they have expired, download them again.

- Method 2: Obtain the wrapping key and import token by calling APIs.
 - i. Call the **get-parameters-for-import** API to obtain the wrapping key and import token.

- **public_key**: content of the wrapping key (Base-64 encoding) returned after the API call
- **import_token**: content of the import token (Base-64 encoding) returned after the API call

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_OAEP_SHA_256**).

- Example request

```
{
  "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
  "wrapping_algorithm": "RSAES_OAEP_SHA_256"
}
```

- Example response

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

- ii. Save the wrapping key and convert its format. Only the key material encrypted using the converted wrapping key can be imported to the management console.
 - 1) Copy the content of the wrapping key **public_key**, paste it to a .txt file, and save the file as **PublicKey.b64**.
 - 2) Use OpenSSL to run the following command to perform Base-64 coding on the content of the **PublicKey.b64** file to generate binary data, and save the converted file as **PublicKey.bin**:
openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin
 - iii. 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**.
2. Use the wrapping key to encrypt the key material.

NOTE

After performing this step, you will obtain either of the following files:

Symmetric key scenario: **EncryptedKeyMaterial.bin** (key material)

Asymmetric key scenario: **EncryptedKeyMaterial.bin** (temporary key material) and **out_rsa_private_key.der** (private key ciphertext)

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

Method 2: Use OpenSSL to generate a key material and use the downloaded wrapping key to encrypt the key material.

NOTE

If you need to run the **openssl pkeyutil** command, ensure your OpenSSL version is 1.0.2 or later.

- a. Generate a key material (256-bit symmetric key) and save it as **PlaintextKeyMaterial.bin**.

- If the AES256 symmetric key algorithm is used, run the following command on the client where the OpenSSL tool has been installed:
openssl rand -out PlaintextKeyMaterial.bin 32
- If the SA and ECC asymmetric key algorithms are used, run the following command on the client where the OpenSSL tool has been installed:
 - 1) Generate a hexadecimal AES256 key.
openssl rand -out 0xPlaintextKeyMaterial.bin -hex 32
 - 2) Convert the hexadecimal AES256 key to the binary format.
cat 0xPlaintextKeyMaterial.bin | xxd -r -ps > PlaintextKeyMaterial.bin
- b. Use the downloaded wrapping key to encrypt the key material and save the encrypted key material as **EncryptedKeyMaterial.bin**.
If the wrapping key was downloaded from the console, replace **PublicKey.bin** in the following command with the wrapping key name *wrappingKey_keyID_DownloadTime*.

Table 1-6 Encrypting the generated key material using the downloaded wrapping key

Wrapping Key Algorithm	Key Material 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_OAEP_SHA_1	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

- c. (Optional) To import an asymmetric key, generate an asymmetric private key, use the temporary key material (**EncryptedKeyMaterial.bin**) to encrypt the private key, and import the encrypted file as the private key ciphertext.

- Take the RSA4096 algorithm as an example. Perform the following operations:

- 1) Generate a private key.

```
openssl genrsa -out rsa_private_key.pem 4096
```

- 2) Convert the key to DER format.

```
openssl pkcs8 -topk8 -inform PEM -outform DER -in  
rsa_private_key.pem -out rsa_private_key.der -nocrypt
```

- 3) Use a temporary key material to encrypt the private key.

```
openssl enc -id-aes256-wrap-pad -K $(cat  
0xPlaintextKeyMaterial.bin) -iv A65959A6 -in  
rsa_private_key.der -out out_rsa_private_key.der
```

 NOTE

By default, the `-id-aes256-wrap-pad` algorithm is not enabled in OpenSSL. To wrap a key, upgrade OpenSSL to the latest version and patch it first. For details, see .

Step 11 If you already have the key material, click **Existing Key Material**. The **Import Key Material** page is displayed.

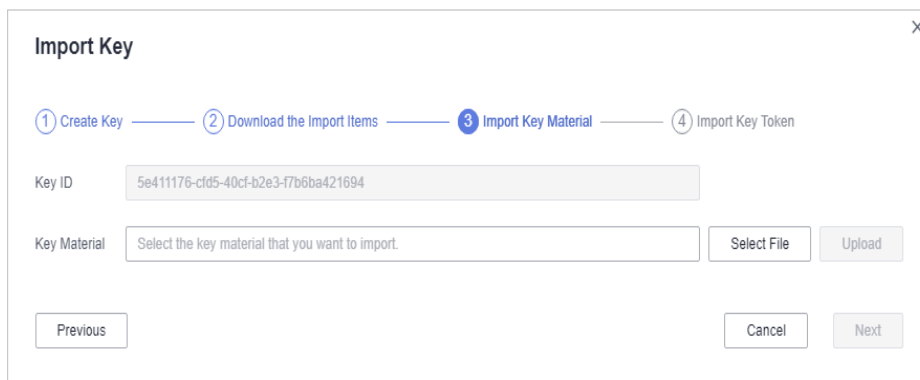
Table 1-7 Parameters for importing key materials (for symmetric keys)

Parameter	Description
Key ID	Random ID of a CMK generated during the CMK creation
Key material	This API allows you to import CMK material. For example, use the EncryptedKeyMaterial.bin file in Step 10.2.b .

Table 1-8 Parameters for importing key materials (for asymmetric keys)

Parameter	Description
Key ID	Random ID of a CMK generated during the CMK creation
Temporary key material	Import a temporary key material. For example, select the EncryptedKeyMaterial.bin file in Step 10.2.b .
Private key ciphertext	Select private key ciphertext. For example, select the out_rsa_private_key.der file in Step 10.2.c .

Figure 1-5 Importing key materials



Step 12 Click **Next** to go to the **Import Key Token** step. Configure the parameters as described in [Table 1-9](#).

Figure 1-6 Importing a key token

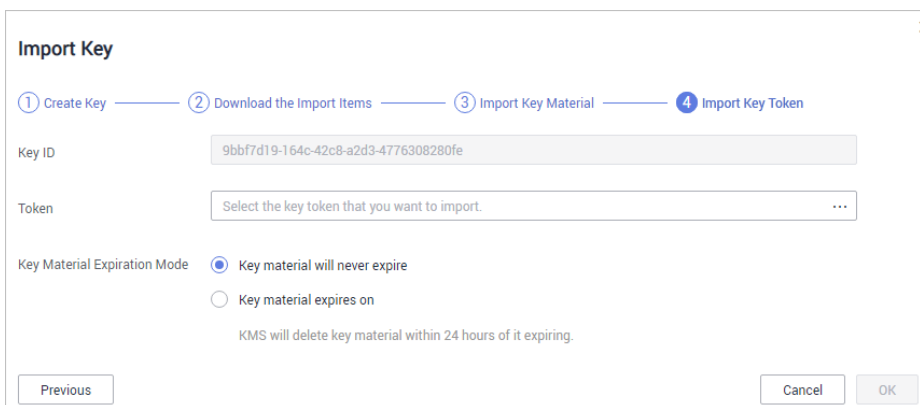


Table 1-9 Parameters for importing a key token

Parameter	Description
Key ID	Random ID of a CMK generated during the CMK creation
Key import token	Select the token downloaded in Step 10.1 .
Key material expiration mode	<ul style="list-style-type: none"> Key material will never expire: You use this option to specify that key materials will not expire after import. Key material will expire: You use this option to specify the expiration time of the key materials. By default, key materials expire in 24 hours after import. After the key material expires, the system automatically deletes the key material within 24 hours. Once the key material is deleted, the key cannot be used and its status changes to Pending import.

Step 13 Click **OK**. When the **Key imported successfully** message is displayed in the upper right corner, the materials are imported.

NOTICE

Key materials can be successfully imported when they match the corresponding CMK ID and token.

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

----End

1.3.3 Deleting Key Materials

When importing key materials, you can specify their expiration time. After the key material expires, KMS deletes it, and the status of CMK changes to **Pending import**. You can manually delete the key materials 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 materials on the KMS console.

Prerequisites


- You have imported key materials for a CMK.
- The material source of the CMK is **External**.
- The CMK status is **Enabled** or **Disabled**.

Constraints

- To re-import a deleted key material, ensure the imported material is the same as the deleted one.
- Data encrypted using a CMK cannot be decrypted if the key material of the CMK was deleted. To decrypt the data, re-import the key material.
- After the deletion, the CMK will become unavailable and its status will change to **Pending import**.
- The key materials of asymmetric keys cannot be directly deleted. To delete them, perform the instructions in [Deleting One or More CMKs](#).

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 Click . Choose **Security & Compliance** > **Data Encryption Workshop**.

Step 4 In the row containing the desired CMK, click **Delete Key Material**.

Step 5 In the dialog box that is displayed, click **OK**. When **Key material deleted successfully** is displayed in the upper right corner, the key materials are successfully deleted.

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

----End

1.4 Managing CMKs

1.4.1 Viewing a CMK

This section describes how to view the information about the master key on the KMS console, including the key alias, status, ID, and creation time. The status of a CMK can be **Enabled**, **Disabled**, or **Pending deletion**.

Procedure



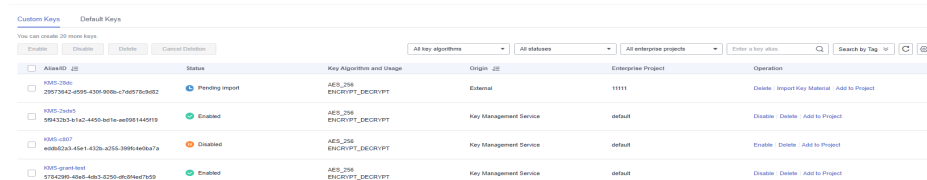
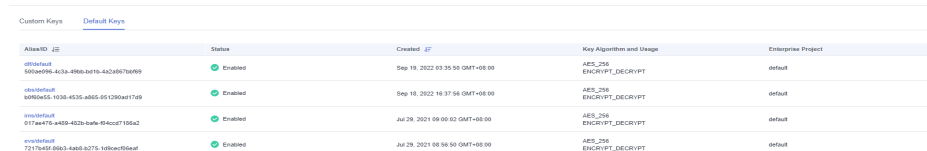
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** Check the key list. [Table 1-10](#) describes the parameters.

Figure 1-7 Custom keys



AliasID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
29575642-4995-4306-800b-c76d575b0822	Pending import	AES_256 ENCRVPT_DECRVPT	External	11111	Delete Import Key Material Add to Project
9943235-9142-4450-bd1e-ae0911449f19	Enabled	AES_256 ENCRVPT_DECRVPT	Key Management Service	default	Enable Delete Add to Project
4686223-45e1-432b-a256-3996-ae0ba7a	Disabled	AES_256 ENCRVPT_DECRVPT	Key Management Service	default	Enable Delete Add to Project
578c209-464d-46b3-825b-06394eaf705d	Enabled	AES_256 ENCRVPT_DECRVPT	Key Management Service	default	Enable Delete Add to Project

Figure 1-8 Default keys



AliasID	Status	Created	Key Algorithm and Usage	Enterprise Project
default 590a096-6c3a-496b-b01b-4a2d897a0f09	Enabled	Sep 19, 2022 03:35:50 GMT+08:00	AES_256 ENCRVPT_DECRVPT	default
default 8090665-103b-4535-a855-9512964d17d9	Enabled	Sep 18, 2022 16:37:58 GMT+08:00	AES_256 ENCRVPT_DECRVPT	default
default 017aa476-4439-482b-ba96-95Ac0d7155e2	Enabled	Jul 29, 2021 09:00:02 GMT+08:00	AES_256 ENCRVPT_DECRVPT	default
default 7217b65f-9863-4a6b-8217c5-169c0e05eaf	Enabled	Jul 29, 2021 08:56:59 GMT+08:00	AES_256 ENCRVPT_DECRVPT	default



Table 1-10 Key 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 materials, its status is Pending import.
ID	Random ID of a CMK generated during the CMK creation NOTE Use this ID as the value of Path if you are creating a custom policy in IAM and have selected Specify resource path for KeyId .
Creation Time	Creation time of the CMK
Key Algorithm and Usage	Key algorithm selected during key creation and its usage
Origin	Source of key material, which can be one of the following: <ul style="list-style-type: none">• External The key is imported to the KMS from an external system.• Key Management Service The key is a default master key or created in KMS.
Enterprise Project	Enterprise project the CMK is used for
Operation	Operations you can perform on the CMK, such as disable, delete, import key material, or cancel deletion. You can also assign keys to projects.

Step 5 You can click the alias of a CMK to view its details, as shown in [Figure 1-9](#).

Figure 1-9 CMK details

Keys / KMS-f0c1	
Alias	KMS-f0c1 
Status	Enabled
ID	ed3224a9..... a101-8e63ae478791
Creation Time	2019/12/11 18:03:40 GMT+08:00
Description	-- 

 NOTE

To change the alias or description of the CMK, click  next to the value of **Alias** or **Description**.

- 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.

----End

1.4.2 Enabling One or More CMKs


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

Prerequisites

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 Click . Choose **Security & Compliance > Data Encryption Workshop.**

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

Figure 1-10 Enabling one CMK

AliasID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
KMS-236c 29073942-4595-436f-903b-c16d573cd6d2	 Pending import	AES_256 ENCRYPT_DECRYPT	External	11111	Delete Import Key Material Add to Project
KMS-2ad5 568432b3-b1a2-446b-bd1e-aa0981445f19	 Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Disable Delete Add to Project
KMS-c807 e9b6b23-45e1-432b-a255-399e4e7ba7a	 Disabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Enable Delete Add to Project
KMS-grant-test 57842980-4648-4463-8259-d8304e4d7659	 Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Disable Delete Add to Project

Step 5 In the dialog box that is displayed, click **OK** 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

1.4.3 Disabling One or More CMKs

This section describes how to use the KMS console to disable one or more 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 More CMKs](#).

Prerequisites


The CMK you want to disable is in **Enabled** status.

Constraints

- Default master keys created by KMS cannot be disabled.
- A disabled CMK is still billable. It will stop incurring charges if it is deleted.

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 Click . Choose **Security & Compliance > Data Encryption Workshop.**

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

Figure 1-11 Disabling one CMK

AliasID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
KMS-238c 29573643-d595-4308-800b-c7a0578c0682	Pending Import	AES_256 ENCRYPT_DECRYPT	External	11111	Delete Import Key Material Add to Project
KMS-2a85 59432b3-b1a2-4450-bd7e-ae0911445919	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Disable Delete Add to Project
KMS-c307 a0802a3-45e1-432b-a255-3998-ae0ba7a	Disabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Enable Delete Add to Project
KMS-grant-test 5784298-4b6d-4ab3-8250-d0d8feaf7659	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Delete Delete Add to Project

Step 5 In the dialog box that is displayed, select **I understand the impact of disabling keys** and click **OK**.

NOTE

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

----End

1.4.4 Deleting One or More CMKs

Before deleting the CMK, confirm that it is not in use and will not be used. You can check the key usage in audit logs.

Prerequisites


- The CMK you want to schedule deletion for is in **Enabled** or **Disabled** status.

Constraints

- A key will not be deleted until its scheduled deletion period expires. You can set the period to a value within the range 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 the CMK. Exercise caution when performing this operation.
- For details about the billing information about a CMK scheduled to be deleted, see [Will a CMK Be Charged After It Is Scheduled to Delete?](#)
- Default Master Keys created by KMS cannot be scheduled for deletion.

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 Click . Choose **Security & Compliance > Data Encryption Workshop**.

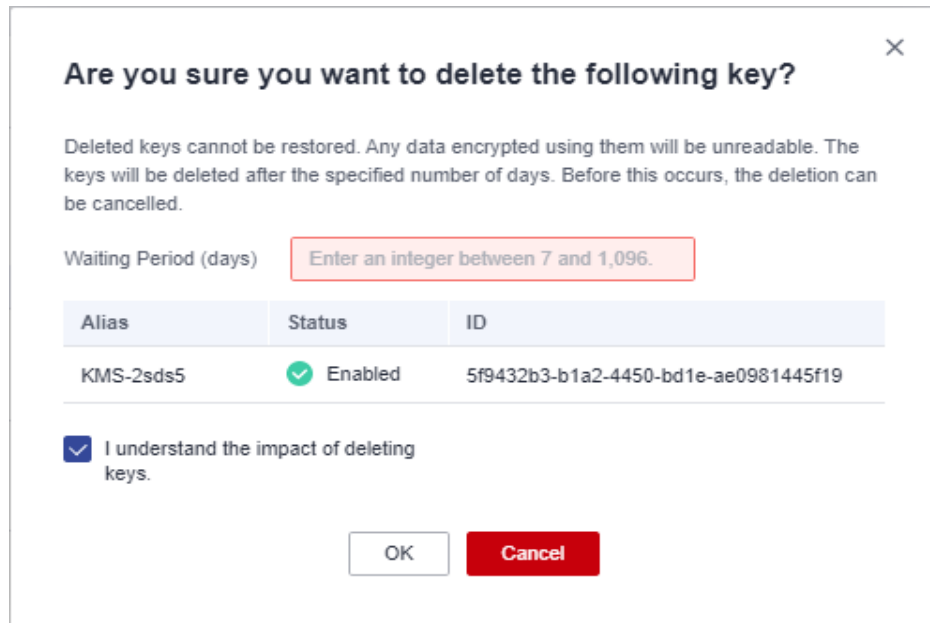
Step 4 In the row containing the desired CMK, click **Delete**.

Figure 1-12 Scheduling the deletion of one CMK

AliasID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
KMS-238c 29573643-d595-4308-800b-c7a0578c0682	Pending Import	AES_256 ENCRYPT_DECRYPT	External	11111	Delete Import Key Material Add to Project
KMS-2a85 59432b3-b1a2-4450-bd7e-ae0911445919	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Delete Delete Add to Project
KMS-c307 a0802a3-45e1-432b-a255-3998-ae0ba7a	Disabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Enable Delete Add to Project
KMS-grant-test 5784298-4b6d-4ab3-8250-d0d8feaf7659	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Delete Delete Add to Project

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

Figure 1-13 Entering the period after which you want the deletion to take effect



NOTE

- A key will not be deleted until its scheduled deletion period expires. You can set the period to a value within the range 7 to 1096 days. Before the specified deletion date, you can cancel the deletion if you want to use the CMK.
- For details about the billing information about a CMK scheduled to be deleted, see [Will a CMK Be Charged After It Is Scheduled to Delete?](#)

- Step 6** In the dialog box that is displayed, select **I understand the impact of deleting keys** and click **OK**.

NOTE

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

----End

1.4.5 Canceling the Scheduled Deletion of One or More CMKs


This section describes how to use the KMS console to cancel the scheduled deletion of one or more CMKs prior to deletion execution. After the cancellation, the CMK is in **Disabled** status.

Prerequisites

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 Click . Choose **Security & Compliance > Data Encryption Workshop.**

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

Figure 1-14 Canceling the scheduled deletion of one CMK

AliasID	Status	Key Algorithm and Usage	Origin	Enterprise Project	Operation
KMS-2696 29573442-6195-4308-900b-c76d570d8d52	Pending import	AES_256 ENCRYPT_DECRYPT	External	11111	Delete Import Key Material Add to Project
KMS-2695 5943203-01a2-4459-8d1e-3a0981448f19	Pending deletion	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Cancel Deletion Add to Project
KMS-c807 e68b2a3-61e1-432b-4255-3996-6a7ba7a	Disabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Enable Delete Add to Project
KMS-grant-test 5764280-48a0-48b3-325b-0b086eaf7b59	Enabled	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	Disable Delete Add to Project

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

After the cancellation, the CMK's status becomes **Disabled**. If you need to enable the CMK, see [Enabling One or More CMKs](#).

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

1.4.6 Adding a Key to a Project


You can allocate keys to enterprise projects on the KMS console.

NOTE

The enterprise project of default master keys cannot be changed.

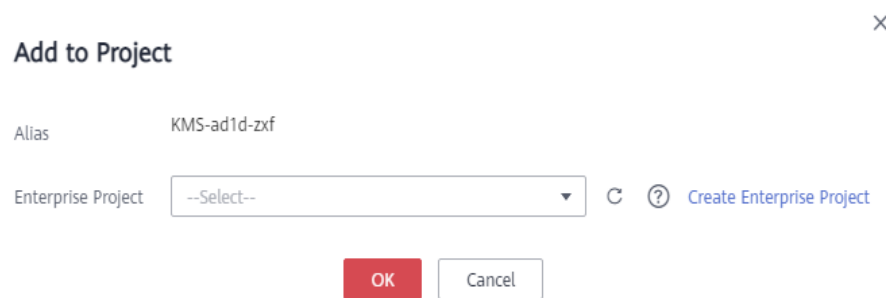
Procedure

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 Click . Choose **Security & Compliance > Data Encryption Workshop.**

Step 4 In the row containing the target key, click **Add to Project.**

Figure 1-15 Adding a key to a project

Step 5 Select a project.

Step 6 Click **OK**.

----End

1.5 Using the Online Tool to Encrypt and Decrypt Small-Size Data


This section describes how to use the online tool to encrypt or decrypt small-size data (4 KB or smaller) on the KMS console.

Constraints

- Default Master Keys cannot be used to encrypt or decrypt such data with the tool.
- You can call an API to use a default master key to encrypt or decrypt small volumes of data. For details, see the *Data Encryption Workshop API Reference*.
- Use the current CMK to encrypt the data.
- Exercise caution when you delete a CMK. The online tool cannot decrypt data if the CMK used for encryption has been deleted.

Encrypting Data

Step 1 [Log in to the management console](#).

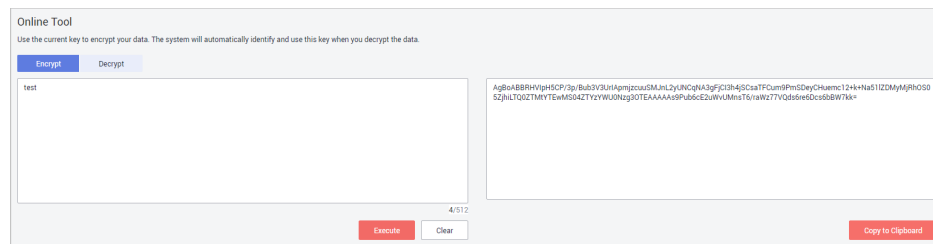
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 Click the alias of the desired CMK to view its details, and go to the online tool for data encryption and decryption.

Step 5 Click **Encrypt**. In the text box on the left, enter the data to be encrypted. For details, see [Figure 1-16](#).

Figure 1-16 Encrypting data



Step 6 Click **Execute**. Ciphertext of the data is displayed in the text box on the right.

NOTE

- Use the current CMK to encrypt the data.
- You can click **Clear** to clear the entered data.
- You can click **Copy to Clipboard** to copy the ciphertext and save it in a local file.

----End

Decrypting Data

Step 1 [Log in to the management console](#).

Step 2 Click . Choose **Security & Compliance > Data Encryption Workshop**.

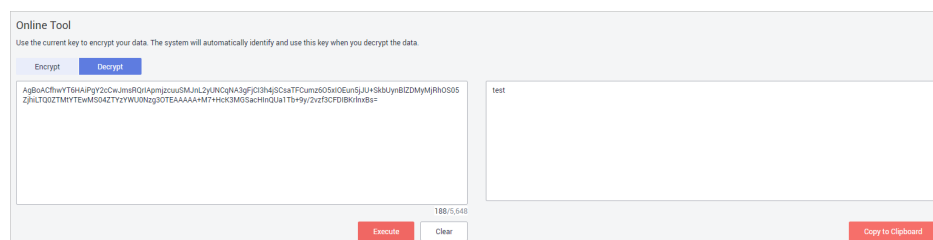
Step 3 You can click any CMK in **Enabled** status to go to the encryption and decryption page of the online tool.

Step 4 Click **Decrypt**. In the text box on the left, enter the data to be decrypted. For details, see [Figure 1-17](#).

NOTE

- The tool will identify the original encryption CMK and use it to decrypt the data.
- However, if the CMK has been deleted, the decryption fails.

Figure 1-17 Decrypting data



Step 5 Click **Execute**. Plaintext of the data is displayed in the text box on the right.

NOTE

You can click **Copy to Clipboard** to copy the plaintext and save it in a local file.

----End

1.6 Managing Tags

1.6.1 Adding a Tag

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.

Constraints

Tags cannot be added to default master keys.

Procedure



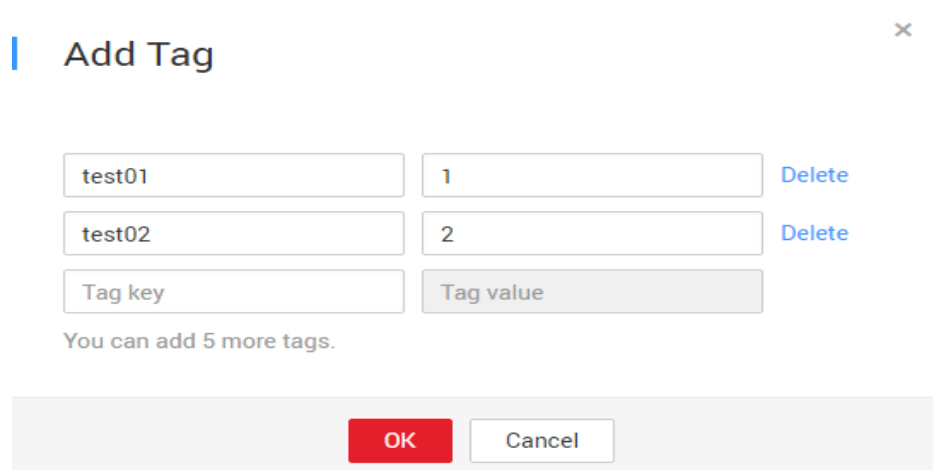
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop.**
- Step 4** Click the alias of the desired CMK to view its details.
- Step 5** Click **Tags** to go to the tag management page.
- Step 6** Click **Add Tag**. In the **Add Tag** dialog box, enter the tag key and tag value. [Table 1-11](#) describes the parameters.

Figure 1-18 Adding a tag



Tag key	Tag value	Action
test01	1	Delete
test02	2	Delete
Tag key	Tag value	

You can add 5 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 1-11 Tag parameters

Parameter	Description	Value	Example Value
Tag key	<p>Name of a tag.</p> <p>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.</p> <p>A maximum of 20 tags can be added for one CMK.</p>	<ul style="list-style-type: none"> • Mandatory. • Each tag key must be unique under the same CMK. • 36 characters limit. • The following character types are allowed: <ul style="list-style-type: none"> - Uppercase letters - Lowercase letters - Digits - Special characters, including hyphens (-) and underscores (_) 	cost
Tag value	Value of the tag	<ul style="list-style-type: none"> • This parameter can be empty. • 43 characters limit. • The following character types are allowed: <ul style="list-style-type: none"> - Uppercase letters - Lowercase letters - Digits - Special characters, including hyphens (-) and underscores (_) 	100

Step 7 Click **OK** to complete.

----End


1.6.2 Searching for a CMK by Tag

This section describes how to search for a CMK by tag in a project on the KMS console.

Prerequisites


Tags have been added.

Constraints

- Multiple tags can be added for at one search. A maximum of 20 tags can be added for one search. If multiple tags are searched for at one time, each CMK in the search result meets the combined search criteria.
- 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.

Procedure

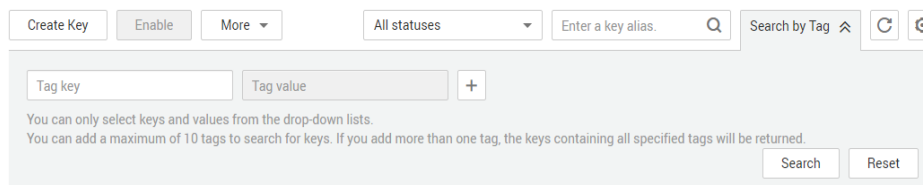
Step 1 [Log in to the management console.](#)

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

Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop.**

Step 4 Click **Search by Tag** to show the search box. For details, see [Figure 1-19](#).

Figure 1-19 Searching for tags



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


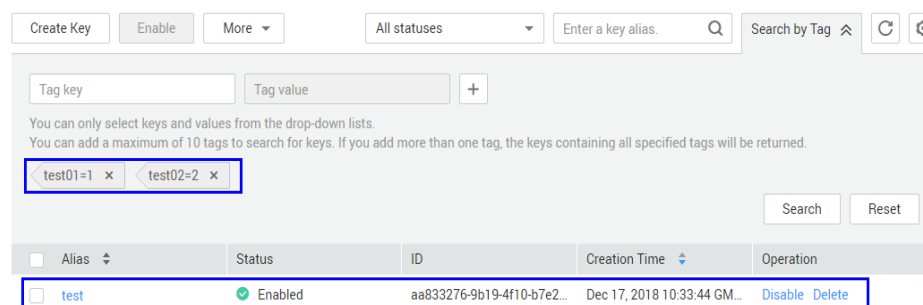

Step 6 Click  to add the input to the search criteria, and click **Search**. The list displays the CMKs that meet the search criteria. For details, see [Figure 1-20](#).

Figure 1-20 Search results



Alias	Status	ID	Creation Time	Operation
test	Enabled	aa833276-9b19-4f10-b7e2...	Dec 17, 2018 10:33:44 GM...	Disable Delete

 **NOTE**

- Multiple tags can be added for at one search. A maximum of 20 tags can be added for one search. If multiple tags are searched for at one time, each CMK in the search result meets the combined search criteria.
- 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

1.6.3 Modifying Tag Values

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

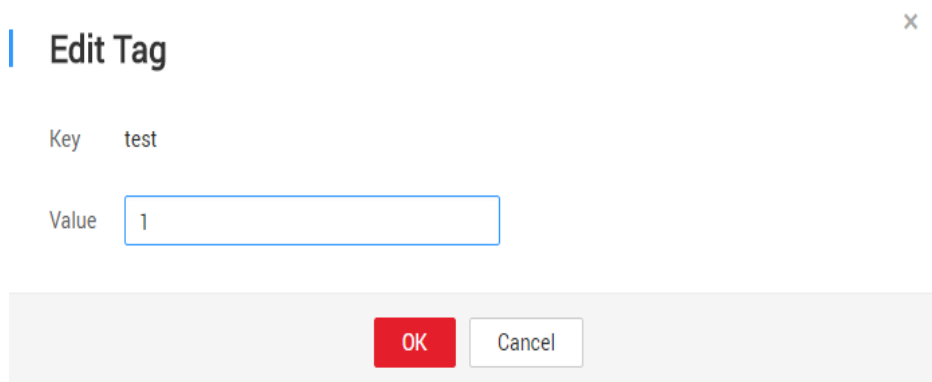
Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop.**

Step 4 Click the alias of the desired CMK to view its details.

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

Step 6 Click **Edit** of the target tag, and the **Edit Tag** dialog box is displayed.

Figure 1-21 Editing a tag



Step 7 In the **Edit Tag** dialog box, enter a tag value, and click **OK** to complete the editing.


----End

1.6.4 Deleting Tags

This section describes how to delete tags on the KMS 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 Click . Choose **Security & Compliance > Data Encryption Workshop.**

Step 4 Click the alias of the desired CMK to view its details.

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

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

1.7 Rotating CMKs

1.7.1 About Key Rotation

Purpose of Key Rotation

Keys that are widely or repeatedly used are insecure. To enhance the security of encryption keys, you are advised to periodically rotate keys and change their key materials.

The purposes of key rotation are:

- To reduce the amount of data encrypted by each key.
A key will be insecure if it is used to encrypt a huge number of data. The amount of data encrypted a key refers to the total number of bytes or messages encrypted using the key.
- To enhance the capability of responding to security events.
In your initial system security design, you shall design the key rotation function and use it for routine O&M, so that it will be at hand when an emergency occurs.
- To enhance the data isolation capability.
The ciphertext data generated before and after key rotation will be isolated. You can identify the impact scope of a security event based on the key involved and take actions accordingly.

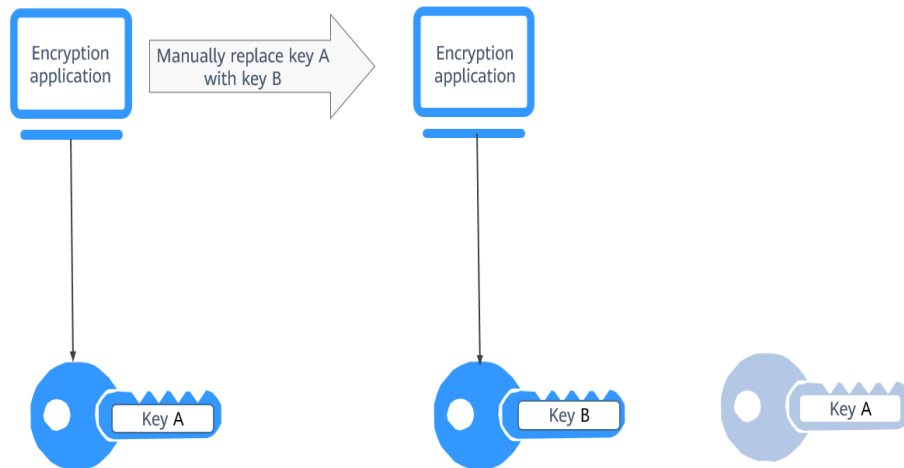
Key Rotation Methods

You can use either of the following key rotation methods:

- Manual key rotation
Replace the key in use with a new key. For example, if key A is in use, you can create key B using a new encryption material, and replace key A with key B. This achieves the same outcome as changing the key material of key A.

Take OBS as an example. To manually rotate a key, create a new CMK on the KMS console. Replace the old CMK with the new one on the OBS console.

Figure 1-22 Manual key rotation



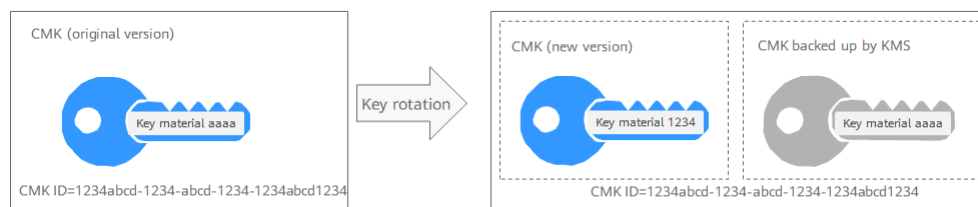
- Automatic key rotation

KMS automatically rotates keys based on the configured rotation period (365 days by default). The system automatically generates a new key to replace the key in use. Automatic key rotation only changes the key material of a CMK. The logical attributes of the CMK will not change, including its key ID, alias, description, and permissions.

Automatic key rotation has the following characteristics:

- Enable rotation for an existing CMK. KMS will automatically generate new key materials for the CMK.
- Data is not re-encrypted in an automatic key rotation. The DEK generated using the CMK is not automatically rotated, and data that has been encrypted using the CMK will not be encrypted again. If a DEK has been leaked, automatic rotation cannot contain the impact of the leakage.

Figure 1-23 Key rotation



NOTE

KMS retains all versions of a CMK, so that you can decrypt any ciphertext encrypted using the CMK.

- KMS uses the latest version of the CMK to encrypt data.
- When decrypting data, KMS uses the CMK version that was used to encrypt the data.

Rotation Modes

Table 1-12 Key rotation modes

Key Type	Rotation Mode
Default master key	Cannot be rotated.
User-defined key (imported CMK)	Can only be manually rotated. For more information about user-defined keys, see CMK Overview .
Symmetric key	Can be automatically or manually rotated.
Asymmetric key	Can only be manually rotated.
Disabled CMK	Disabled CMKs are not rotated. KMS keeps their rotation status unchanged. After a CMK is enabled, if it has been used for longer than the rotation period, KMS will immediately rotate keys. If the CMK has been used for shorter than the rotation period, KMS will implement the original rotation plan. For more information, see Disabling One or More CMKs .
CMKs in pending deletion state	KMS does not rotate CMKs in pending deletion status. After you cancel the deletion of a CMK, the previous key rotation status will be restored. If the CMK has been used for longer than the rotation period, KMS will immediately rotate keys. If the CMK has been used for shorter than the rotation period, KMS will implement the original rotation plan. For more information, see Scheduling the Deletion of One or More Keys .

 **NOTE**

You can check the rotation details on the **Rotation Policy** page, including the last rotation time and number of rotations.

Pricing for Key Rotation

Enabling key rotation may incur additional fees. For details, see [Billing Description](#).

1.7.2 Enabling Key Rotation

This section describes how to enable rotation for a CMK on the KMS console.

By default, automatic key rotation is disabled for a CMK. Every time you enable key rotation, KMS automatically rotates CMKs based on the rotation period you set.

Prerequisites

- The CMK is enabled.
- The **Origin** of the CMK is **KMS**.


Constraints

A disabled CMK is never rotated, even if rotation is enabled for it.

KMS resumes rotation when this CMK is enabled. If you enable this CMK after one rotation period has passed, KMS will rotate it within 24 hours.

Procedure

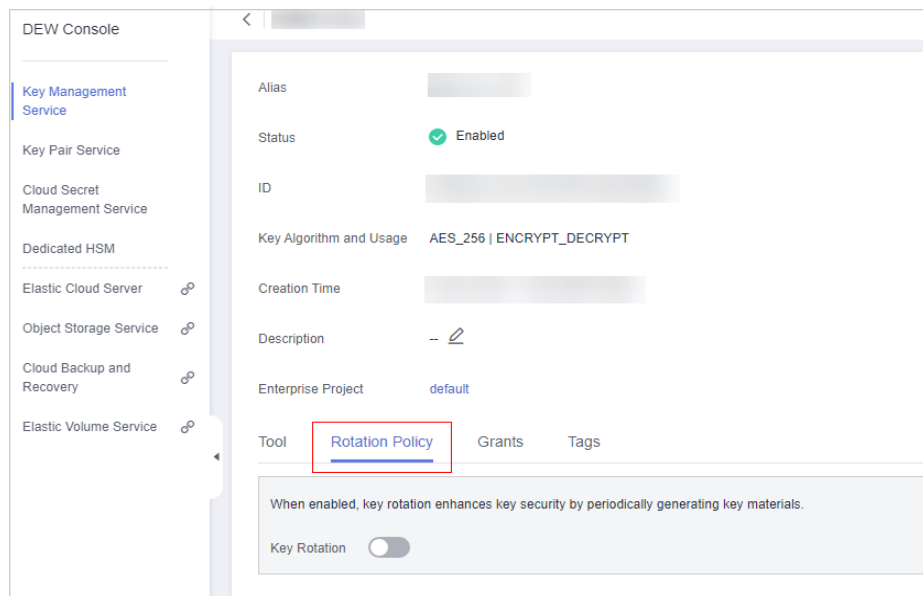
Step 1 [Log in to the management console](#).

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

Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

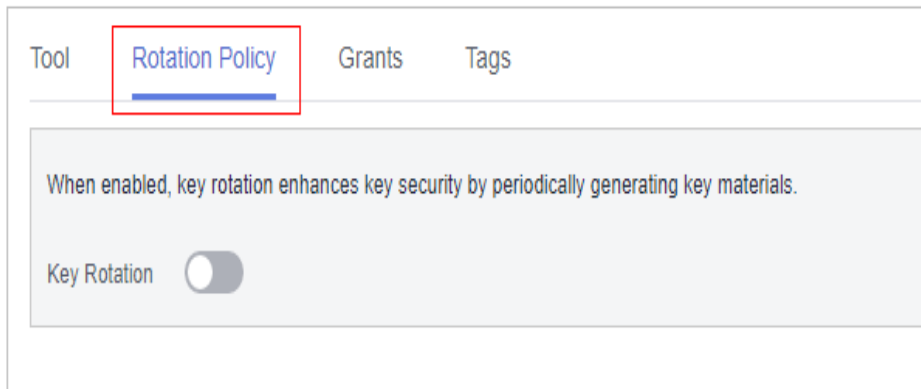
Step 4 Click the alias of the desired CMK to view its details.


Figure 1-24 CMK details



Step 5 Click the **Rotation Policy** tab. The rotation switch is displayed.

Figure 1-25 CMK rotation



Step 6 Click  to enable key rotation.

Step 7 Configure the rotation period and click **OK**, as shown in [Figure 1-26](#). For more information, see [Table 1-13](#).

Figure 1-26 Enabling key rotation

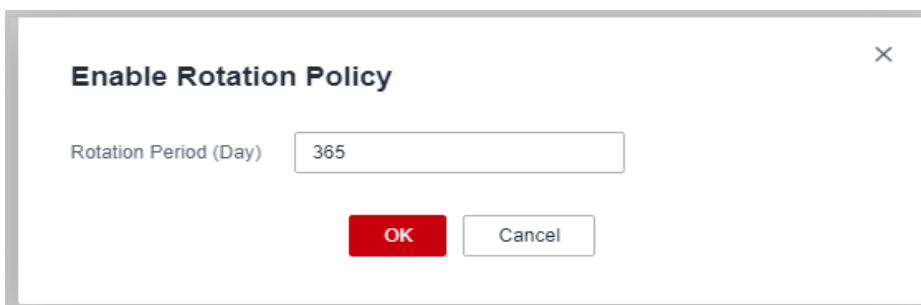





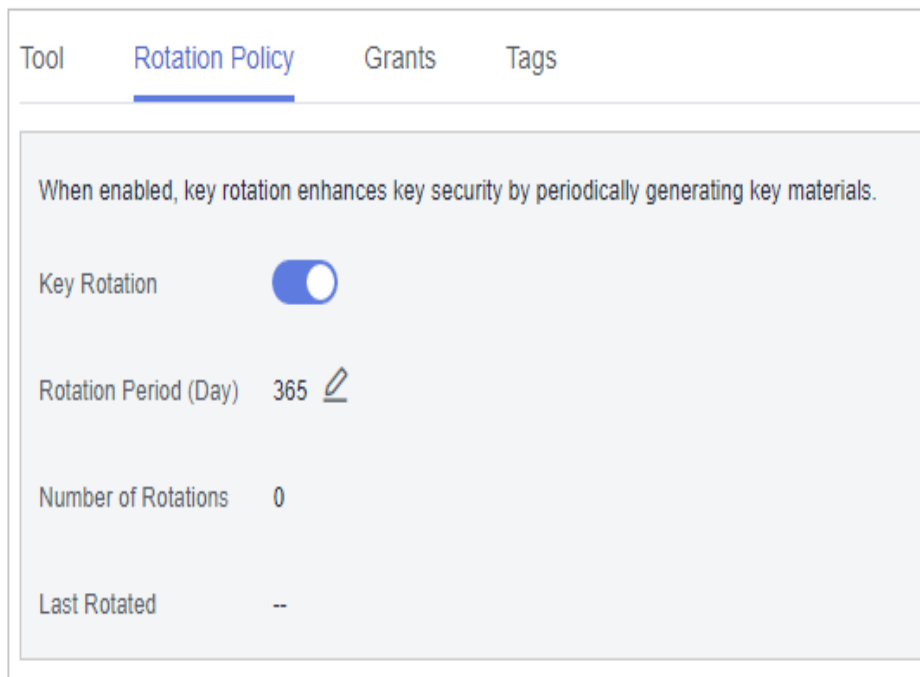
Table 1-13 Key rotation parameters

Parameter	Description
CMK rotation	<p>Rotation switch. The default status is .</p> <p> : disabled</p> <p> : enabled</p> <p>After rotation is enabled, the CMK will be rotated based on your set period.</p> <p>NOTE A disabled CMK is never rotated, even if rotation is enabled for it. KMS resumes rotation when this CMK is enabled. If you enable this CMK after one rotation period has passed, KMS will rotate it within 24 hours.</p>


Parameter	Description
Rotation Period (day)	Rotation period (day). The value is an integer ranging from 30 to 365. The default value is 365 . Configure the period based on how often a CMK is used. If it is frequently used, configure a short period; otherwise, set a long one.

Step 8 Check rotation details, as shown in the following figure.

Figure 1-27 CMK rotation details



NOTE

You can click  to change the rotation period. After the period is changed, KMS rotates the CMK by the new period.

----End

1.7.3 Disabling Key Rotation

This section describes how to disable rotation for a key on the KMS console.

Prerequisites

- The key is enabled.
- The **Origin** of the CMK is **KMS**.
- Key rotation has been enabled.

Procedure



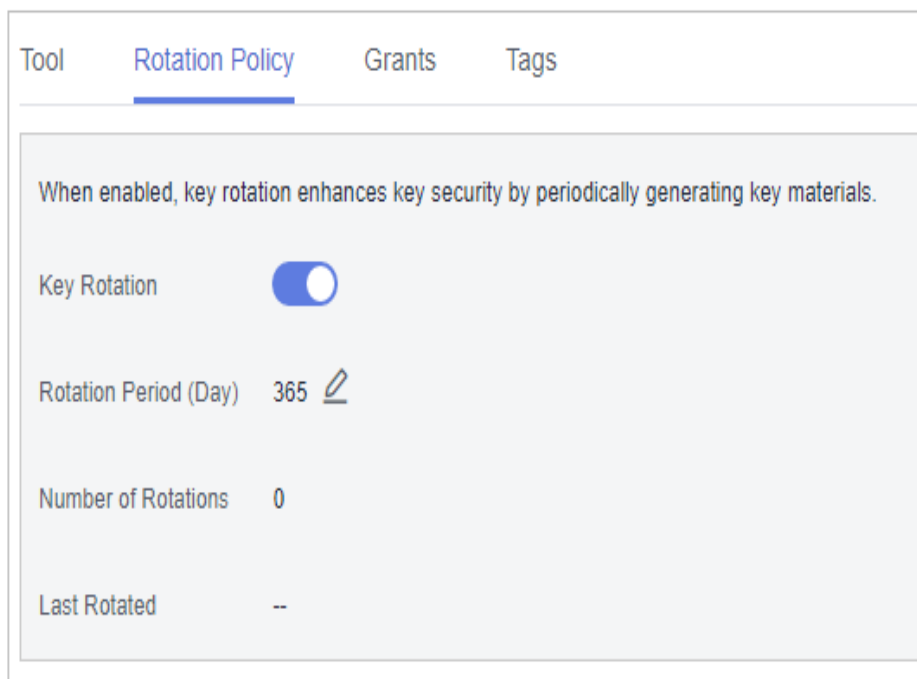
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop.**
- Step 4** Click the alias of a symmetric key.
- Step 5** Click the **Rotation Policy** tab. The rotation switch is displayed.

Figure 1-28 CMK rotation details




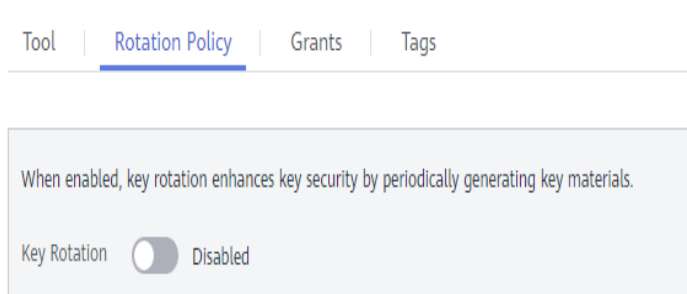
- Step 6** Click  to disable key rotation.
- Step 7** Check the rotation status, as shown in [Figure 1-29](#).

Figure 1-29 Disabling key rotation



----End

1.8 Managing a Grant

1.8.1 Creating a Grant

You can create grants for other IAM users or accounts to use the CMK. You can create a maximum of 100 grants on a CMK.

Prerequisites


- You have obtained the ID of the grantee (user to whom permissions are to be authorized).
- The desired CMK is in **Enabled** status.

Constraints

The owner of a CMK can create a grant for the CMK on the KMS console or by calling APIs. The IAM users or accounts who have the grant creation permission assigned by the owner of the CMK can create grants for the CMK only by calling APIs.

Procedure

Step 1 [Log in to the management console.](#)

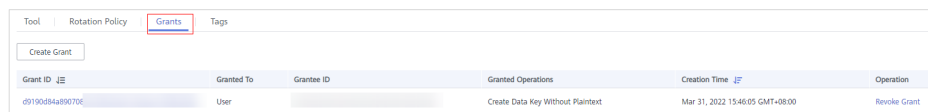
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 Click the alias of the desired CMK to go to the page displaying its details to create a grant on it.

Step 5 Click the **Grants** tab.

Figure 1-30 Grant tab page



Grant ID	Granted To	Grantee ID	Granted Operations	Creation Time	Operation
09190d84a89070c	User		Create Data Key Without Plaintext	Mar 31, 2022 15:46:05 GMT+08:00	Revoke Grant

Step 6 Click **Create Grant**. The **Create Grant** dialog box is displayed.

Figure 1-31 Creating a grant (for a user)

Create Grant ×

Key ID

* User or Account User Account

A grantee is a cloud service user to whom you want to grant operation permissions associated with the key. You can obtain the user ID of the grantee from the page of My Credential by logging in to the management console with the grantee's username and password.

Granted Operations ?

- Select all
- Create Data Key Without Plaintext
- Describe Key
- Create Data Key
- Create Grant
- Encrypt Data Key
- Retire Grant
- Decrypt Data Key
- Encrypt Data
- Decrypt Data

Figure 1-32 Creating a grant (for an account)

Create Grant ×

Key ID

* User or Account User Account

A account ID is displayed on the tenant's My Credentials page.

Granted Operations ?

- Select all
- Create Data Key Without Plaintext
- Describe Key
- Create Data Key
- Create Grant
- Encrypt Data Key
- Retire Grant
- Decrypt Data Key
- Encrypt Data
- Decrypt Data

Step 7 In the dialog box that is displayed, enter the ID of the user to be authorized and select permissions to be granted. For more information, see [Table 1-14](#).

NOTICE

A grantee can perform the authorized operations only by calling the necessary APIs. For details, see the .

Table 1-14 Parameter description

Parameter	Description	Example Value
Key ID	ID of a CMK (automatically read by the system)	-
User or Tenant	<p>Whether a user or an account is authorized.</p> <ul style="list-style-type: none">• User User ID: Enter the IAM user ID. To obtain the ID, click the username in the upper right corner of the page, choose My Credentials. Choose API Credentials from the navigation pane, and copy the value of IAM User ID. After the authorization is complete, the IAM user can use the specified keys.• Account Account ID: Enter the IAM user ID. To obtain the ID, click the username in the upper right corner of the page, choose My Credentials. Choose API Credentials from the navigation pane, and copy the value of Account ID. After the authorization is complete, all IAM users under the account can use specified keys.	d9a6b2bdaedd 4ba586cabe63 72d1b312

Parameter	Description	Example Value
Operations	<p>The following permissions can be authorized:</p> <p>NOTE</p> <ul style="list-style-type: none"> • You can create multiple grants on a CMK to provide different permissions to the same user. The user's permissions on the CMK are the combination of all the grants. • This parameter cannot be left blank. • Selecting only Create Grant is not allowed. • Create Data Key Without Plaintext • Create Data Key • Encrypt Data Key • Decrypt Data Key • Query Key Information • Create Grant • Retire Grant <ul style="list-style-type: none"> – A grantee can retire a grant if the grantee does not need that permission. – If, before retiring a grant, the grantee has granted the permission to another user, that user's permission will not be affected by the grant retirement. • Encrypt Data • Decrypt Data 	-

Step 8 Click **OK**. When message **Grant created successfully** is displayed in the upper right corner, the grant has been created.

In the list of grants, you can view the grant ID, grant type, grantee ID, granted operation, and creation time of the grant.

----End

1.8.2 Querying a Grant

This section describes how to view the details about a grant on the KMS console, such as the grant ID, grantee user ID, granted operation, and creation time.

Prerequisites

You have created a grant.

Procedure

Step 1 [Log in to the management console.](#)



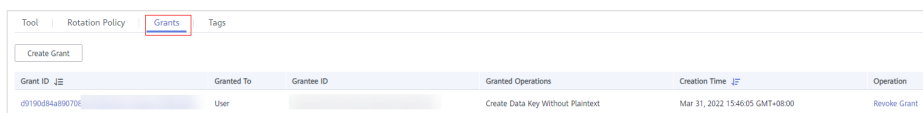
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** Click the alias of the desired CMK to view its details.
- Step 5** Click the **Grants** tab. Information about the CMK and grants created on it are displayed. See [Figure 1-33](#).

Figure 1-33 Grant tab page



Grant ID	Granted To	Grantee ID	Granted Operations	Creation Time	Operation
09190d84a8970c	User		Create Data Key Without Plaintext	Mar 31, 2022 15:46:05 GMT+08:00	Revoke Grant

[Table 1-15](#) describes the parameters.

Table 1-15 Parameter description

Parameter	Description
Grant ID	Randomly generated unique identification of a grant
Granted To	Whether permissions are granted to a user or account.
Grantee ID	ID of the authorized user or account.
Granted Operations	Authorized operations (such as Create Data Key) on the CMK
Creation Time	Creation time of the grant
Operation	Operations that can be performed on a grant. For example, you can revoke a grant.

- Step 6** Click a grant ID to view the grant details.

----End

1.8.3 Revoking a Grant

You can revoke a grant on the KMS console in either of the following scenarios:

- A grantee does not need the grant. (The grantee can either tell the user who has created the grant to revoke the grant or call the necessary API to revoke the grant directly.)
- You do not want the grantee to have the grant.

When a grant is revoked, the grantee does not have the corresponding permission anymore. However, if the grantee has created the same grant to another user, permission of that user will not be affected.


This section describes how to revoke a grant on the KMS console.

Prerequisites

You have created a grant.

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 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 Click the alias of the desired CMK to view its details.

Step 5 In the row of a grantee, click **Revoke Grant**.

Step 6 In the dialog box that is displayed, click **Yes**. When **Grant revoked successfully** is displayed in the upper right corner, the grant has been revoked.

----End

2 Cloud Secret Management Service

2.1 Creating a Secret

This section describes how to create a secret on the CSMS console.


You can create a secret and store its value in its initial version, which is marked as **SYSCURRENT**.

Constraints

- A user can create a maximum of 200 credentials.
- By default, the default master key **csms/default** created by CSMS is used as the encryption master key of the current secret. You can also create a key and use a user-defined encryption key on the KMS console.

Creating a Secret

Step 1 [Log in to the management console.](#)

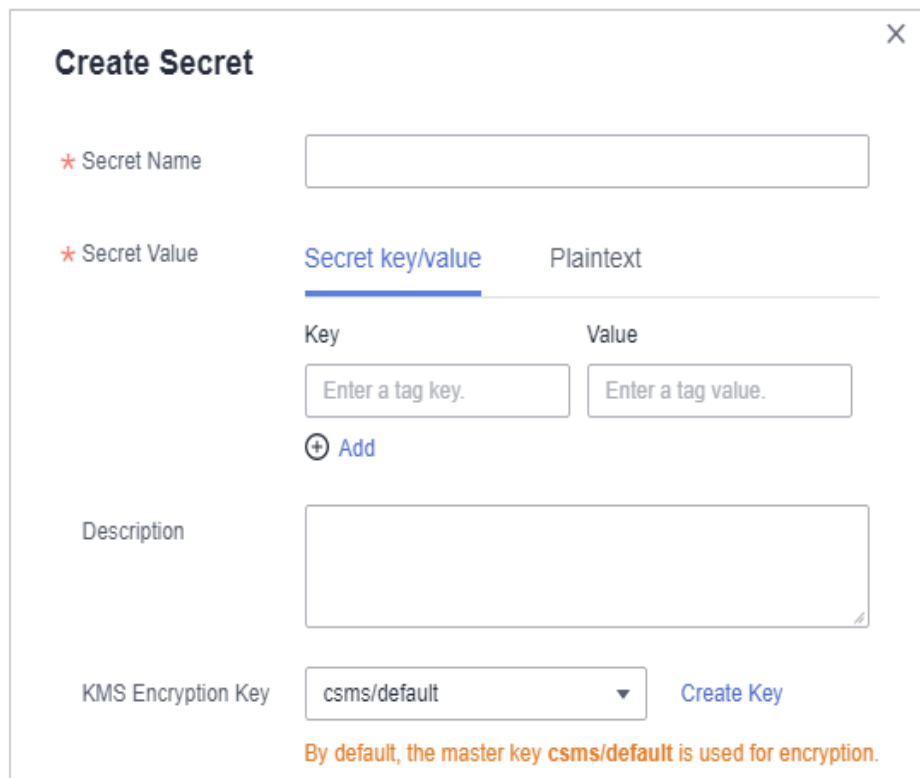
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane, choose **Cloud Secret Management Service**.

Step 5 Click **Create Secret**.

Figure 2-1 Creating a secret



Step 6 In the **Create Secret** dialog box, enter the secret name, value, description, and select a KMS encryption key.

- **Secret Name:** Enter a secret name.
- **Secret Value:** Enter the secret key/value or plaintext secret.
- **Description:** Enter the secret description.
- **KMS Encryption Key:** Select the default CMK **csms/default** or a user-defined key in KMS.

 **NOTE**

By default, the default master key **csms/default** created by CSMS is used as the encryption master key of the current secret. You can also create a key and use a user-defined encryption key on the KMS console. For details, see [Creating a CMK](#).

Step 7 Click **OK**.

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

----End

2.2 Managing Secrets

2.2.1 Viewing a Secret

This section describes how to check secret names, statuses, and creation time on the CSMS console. The credential status can be **Enabled** or **Pending deletion**.

Procedure



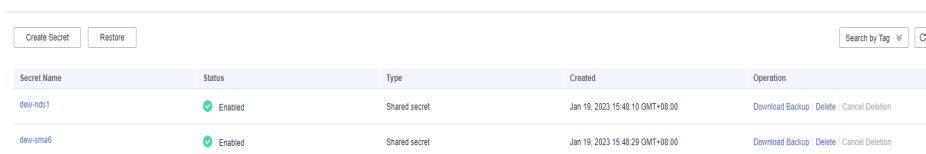
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop.**
- Step 4** In the navigation pane, choose **Cloud Secret Management Service.**
- Step 5** Check the secret list. For more information, see [Table 2-1.](#)

Figure 2-2 Secret list



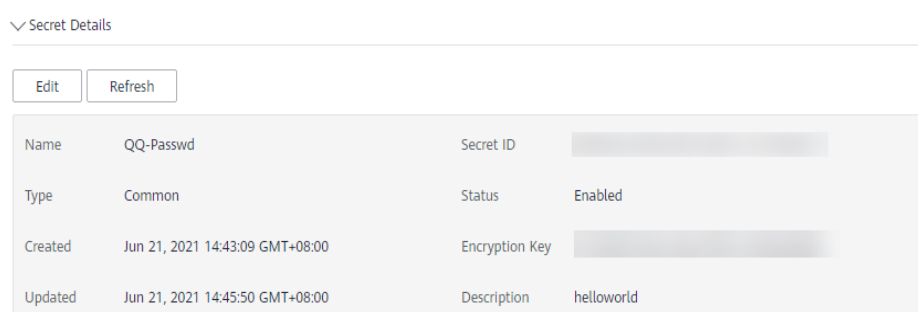
Secret Name	Status	Type	Created	Operation
dew-nds1	Enabled	Shared secret	Jan 19, 2023 15:48:10 GMT+08:00	Download Backup Delete Cancel Deletion
dew-sma6	Enabled	Shared secret	Jan 19, 2023 15:48:29 GMT+08:00	Download Backup Delete Cancel Deletion

Table 2-1 Secret list parameters

Parameter	Description
Secret Name	Secret name
Status	Status of a secret. The value can be Enabled or Pending deletion .
Type	Secret type, including shared secrets and RDS DB instance secrets.
Created	Time when a secret is created
Operation	You can schedule or cancel the deletion of a secret in the Operation column.

- Step 6** Click a secret to view its details. See [Figure 2-3.](#)

Figure 2-3 Secret details



Name	QQ-Passwd	Secret ID	
Type	Common	Status	Enabled
Created	Jun 21, 2021 14:43:09 GMT+08:00	Encryption Key	
Updated	Jun 21, 2021 14:45:50 GMT+08:00	Description	helloworld

NOTE

- You can click **Edit** to modify the encryption key and description of a secret.
- You can click **Refresh** to refresh secret information.

----End

2.2.2 Deleting a Secret

Before deleting a secret, confirm that it is not in use and will not be used.

Prerequisites


The secret to be deleted is in **Enabled** state.

Constraints

- A secret will not be deleted until its scheduled deletion period expires. You can set the period to a value within the range 7 to 30 days. Before the specified deletion date, you can cancel the deletion if you want to use the secret. If the scheduled deletion period of a secret expires, the secret will be deleted and cannot be restored.
- For details about the billing information about a credential to be deleted, see [Are Credentials Scheduled to Be Deleted Billed?](#)
- If you choose to delete a secret immediately, it cannot be restored. Exercise caution when performing this operation.

Procedure

Step 1 [Log in to the management console.](#)

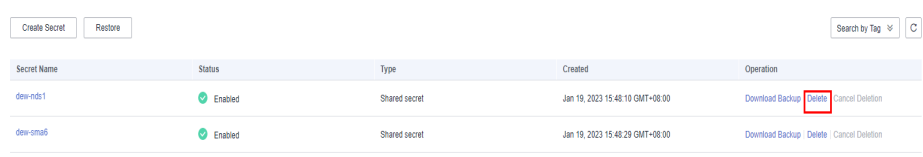
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane, choose **Cloud Secret Management Service**.

Step 5 In the row of a secret, click **Delete**.

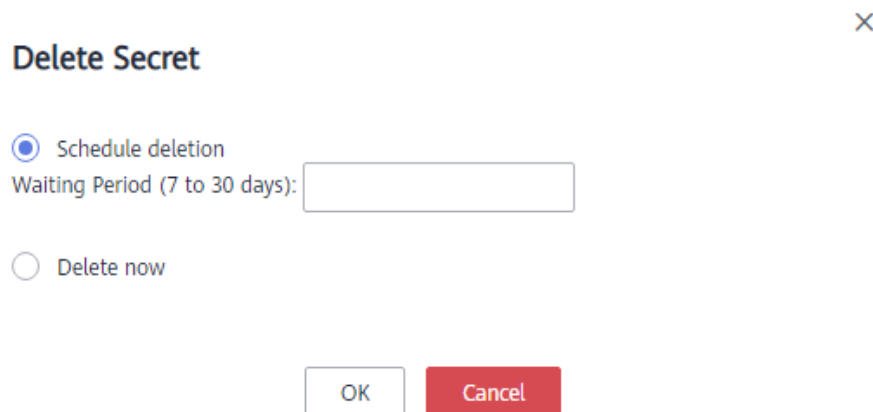
Figure 2-4 Deleting a secret



Secret Name	Status	Type	Created	Operation
dev-nds1	Enabled	Shared secret	Jan 19, 2023 15:48:10 GMT+08:00	Download Backup Delete Cancel Deletion
dev-sma8	Enabled	Shared secret	Jan 19, 2023 15:48:29 GMT+08:00	Download Backup Delete Cancel Deletion

Step 6 In the dialog box that is displayed, click **Schedule deletion** or **Delete now**.

Figure 2-5 Deleting a secret



Delete Secret

Schedule deletion
Waiting Period (7 to 30 days):

Delete now

OK Cancel

Step 7 Click **OK**.

 **NOTE**

- A secret will not be deleted until its scheduled deletion period expires. You can set the period to a value within the range 7 to 30 days. Before the specified deletion date, you can cancel the deletion if you want to use the secret. If the scheduled deletion period of a secret expires, the secret will be deleted and cannot be restored.
- For details about the billing information about a credential to be deleted, see [Are Credentials Scheduled to Be Deleted Billed?](#)
- If you choose to delete a secret immediately, it cannot be restored. Exercise caution when performing this operation.

----End

2.3 Managing Secret Versions

2.3.1 Viewing a Secret Value

This section describes how to save and view secret values on the CSMS console.


You can create a new version of a secret to encrypt and keep a new secret value. By default, The latest secret version in **SYSCURRENT** state. The previous version is in the **SYSPREVIOUS** state.

Constraints

- A secret can have up to 20 versions.
- Secret versions are numbered v1, v2, v3, and so on based on their creation time.

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.


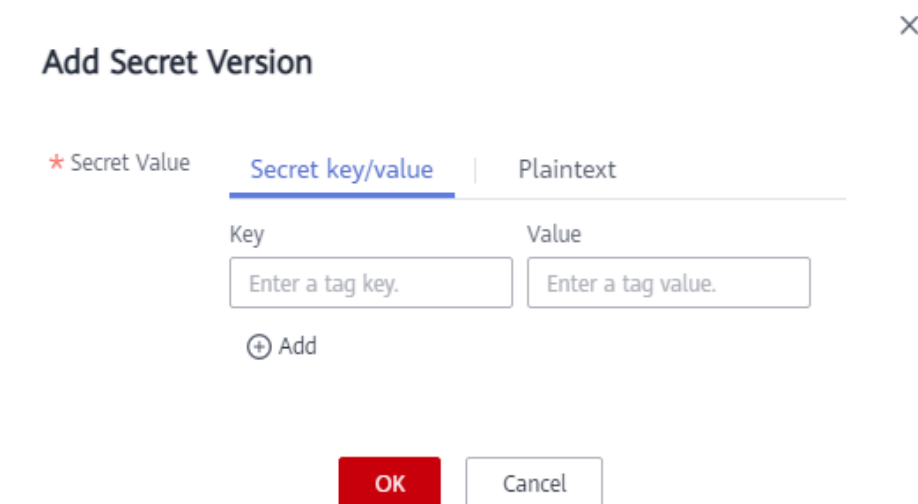
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** In the navigation pane, choose **Cloud Secret Management Service**.
- Step 5** Click a secret name to go to the details page.
- Step 6** In the **Version List** area, click **Add Secret Version**. Configure the secret key and value in the dialog box that is displayed.

Figure 2-6 Adding a secret value



- Step 7** Click **OK**. A message is displayed in the upper right corner of the page, indicating that the value is added successfully.

View the latest secret value in the secret version list.

- Step 8** In the **Version List** area, click **View Secret** in the **Operation** column of a secret.

Figure 2-7 Secret version list

Version List

[Add Secret Version](#) [Refresh](#)

Version	KMS Encryption Key ID	Version Status	Created	Operation
v4	1473d85f-9da3-4ba5-9ff9-e15b4baf548b	SYSCURRENT	Aug 03, 2021 15:07:46 GMT+08:00	Manage Status View Secret
v3	1473d85f-9da3-4ba5-9ff9-e15b4baf548b	SYSPREVIOUS	Jul 22, 2021 11:23:38 GMT+08:00	Manage Status View Secret
v2	1473d85f-9da3-4ba5-9ff9-e15b4baf548b		Jul 14, 2021 10:20:11 GMT+08:00	Manage Status View Secret
v1	1473d85f-9da3-4ba5-9ff9-e15b4baf548b		Jul 14, 2021 10:18:01 GMT+08:00	Manage Status View Secret

- Step 9** In the **View Secret** dialog box, click **Yes**.

 **NOTE**

Secret values are generally obtained via APIs. Checking the values on the console incurs security risks.

- Step 10** View the secret value and click **OK**.

----End

2.3.2 Managing Secret Version Statuses

This section describes how to add, change, and delete secret version statuses.


Secret values are encrypted and stored in secret versions. A version can have multiple statuses. Versions without any statuses are regarded as deprecated and can be automatically deleted by CSMS.

Constraints

- The initial version is marked by the **SYSCURRENT** status tag.
- You can mark a version with preconfigured or user-defined tags. A version can have multiple status tags, but a status tag can be used for only one version. For example, if you add the status tag used by version A to version B, the tag will be moved from version A to version B.
- A secret can have up to 12 version statuses. A status can be used for only one version.
- **SYSCURRENT** and **SYSPREVIOUS** are preconfigured statuses and cannot be deleted.

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.

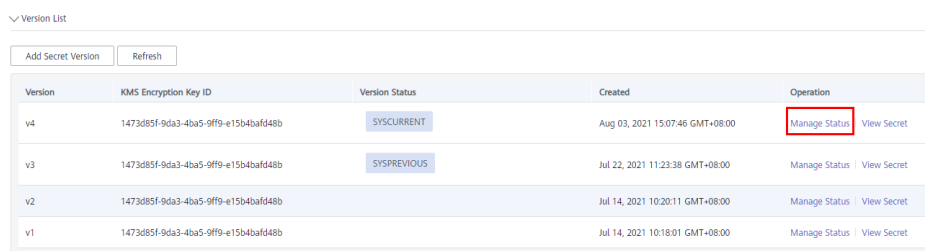
Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop.**

Step 4 In the navigation pane, choose **Cloud Secret Management Service.**

Step 5 Click a secret name to go to the details page.

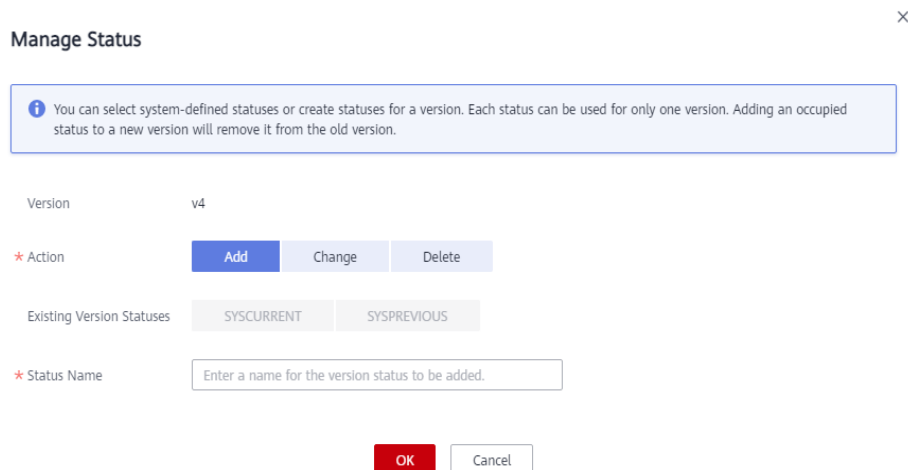
Step 6 In the **Version List** area, click **Manage Status** in the **Operation** column.

Figure 2-8 Secret version list



Version	KMS Encryption Key ID	Version Status	Created	Operation
v4	1473d85f-9da3-4ba5-9ff9-e15b4baf48b	SYSCURRENT	Aug 03, 2021 15:07:46 GMT+08:00	Manage Status View Secret
v3	1473d85f-9da3-4ba5-9ff9-e15b4baf48b	SYSPREVIOUS	Jul 22, 2021 11:23:38 GMT+08:00	Manage Status View Secret
v2	1473d85f-9da3-4ba5-9ff9-e15b4baf48b		Jul 14, 2021 10:20:11 GMT+08:00	Manage Status View Secret
v1	1473d85f-9da3-4ba5-9ff9-e15b4baf48b		Jul 14, 2021 10:18:01 GMT+08:00	Manage Status View Secret

Step 7 In the **Manage Status** dialog box, add, change, or delete the status of a secret version.

Figure 2-9 Managing statuses

- Adding a version status

In the **Manage Status** dialog box, click **Add** and enter a status name. Click **OK**.

NOTE

A secret can have up to 12 version statuses. A status can be used for only one version.

- Updating the version status of a secret

In the **Manage Status** dialog box, click **Change** and select an existing version status. Click **OK**.

- Deleting the version status of a secret

In the **Manage Status** dialog box, click **Delete** and select a version status. Click **OK**.

NOTE

SYSCURRENT and **SYSPREVIOUS** are preconfigured statuses and cannot be deleted.

----End

2.4 Managing Tags

2.4.1 Adding a Tag

Tags are used to identify secrets. You can easily classify and track secrets using tags.

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.


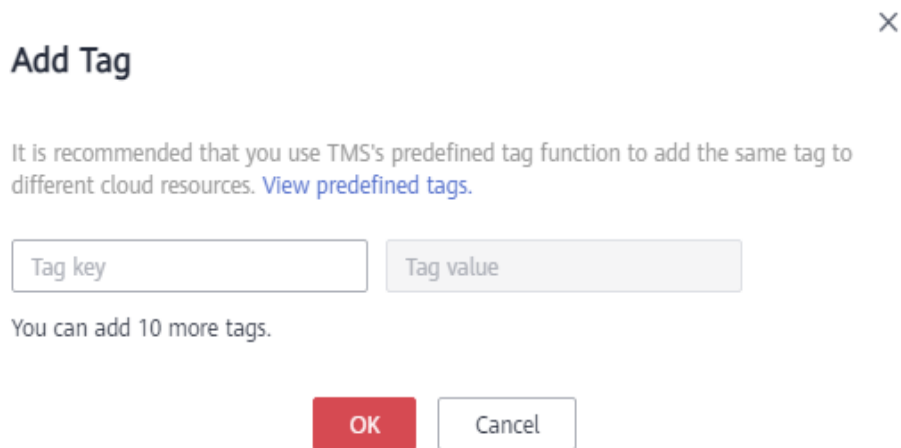
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Step 4** In the navigation pane, choose **Cloud Secret Management Service**.
- Step 5** Click a secret name to go to the details page.
- Step 6** In the **Tags** area, click **Add Tag**. In the **Add Tag** dialog box, enter the tag key and tag value. [Table 2-2](#) describes the parameters.

Figure 2-10 Add a tag



Add Tag ×

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

You can add 10 more tags.

 **NOTE**

- If you want to use the same tag to identify multiple cloud resources, you can create predefined tags in the TMS. In this way, the same tag can be selected for all services. For more information about predefined tags, see the *Tag Management Service User Guide*.
- To delete a tag, click **Delete** next to it.

Table 2-2 Tag parameters

Parameter	Description	Remarks
Tag key	Tag name. The tag keys of a secret cannot have duplicate values. A tag key can be used for multiple secrets. A secret can have up to 10 tags.	<ul style="list-style-type: none">• Mandatory.• The tag keys of a secret cannot have duplicate values.• 36 character limit.• The following character types are allowed:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Numbers- Special characters, including hyphens (-) and underscores (_)- Chinese characters
Tag value	Value of the tag	<ul style="list-style-type: none">• Optional• 43 character limit.• The following character types are allowed:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Numbers- Special characters, including hyphens (-) and underscores (_)- Chinese characters

Step 7 Click **OK**.

----End

2.4.2 Searching for a Secret by Tag


This section describes how to search for a secret by tag in a project on the CSMS console.

Prerequisites

Tags have been added.

Procedure

Step 1 [Log in to the management console](#).

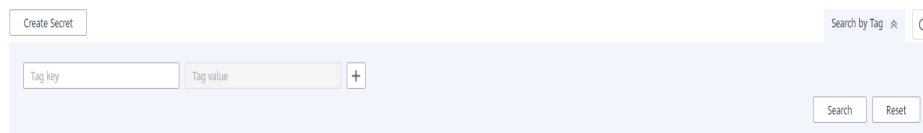
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane, choose **Cloud Secret Management Service**.

Step 5 Click **Search by Tag** to show the search box.

Figure 2-11 Search box



Step 6 In the search box, enter or select a tag key and a tag value.


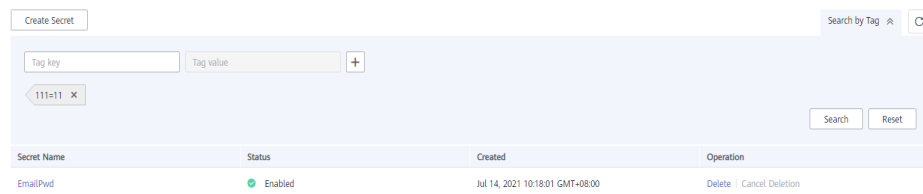

Step 7 Click  to add the input to the search criteria, and click **Search**.

Figure 2-12 Search result



NOTE

- Multiple tags can be added for one search. A maximum of 10 tags can be added for one search. Each search result meets all the search criteria.
- To delete a tag from the search criteria, click  next to the tag.
- You can click **Reset** to reset the search criteria.


----End

2.4.3 Modifying a Tag Value

This section describes how to modify tag values on the CSMS 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.

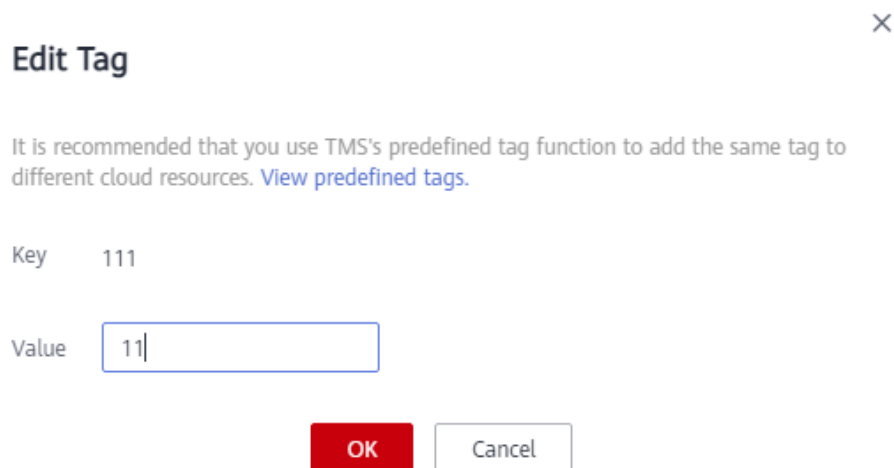
Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane, choose **Cloud Secret Management Service**.

Step 5 Click a secret name to go to the details page.

Step 6 In the **Tags** area, click **Edit**.

Figure 2-13 Editing a tag



Step 7 In the **Edit Tag** dialog box, enter a tag value and click **OK**.


----End

2.4.4 Deleting a Tag

This section describes how to delete tags on the CSMS 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.

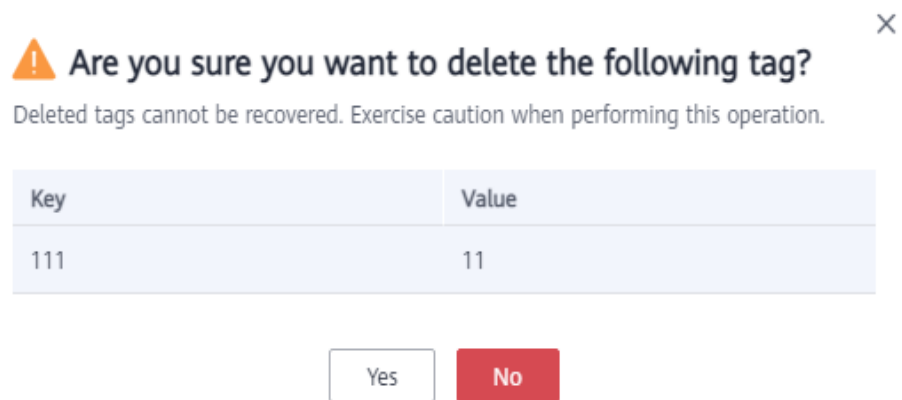
Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane, choose **Cloud Secret Management Service**.

Step 5 Click a secret name to go to the details page.

Step 6 In the **Tags** area, click **Delete**.

Figure 2-14 Deleting a tag



Step 7 In the **Delete Tag** dialog box, click **Yes**.

----End

3 Key Pair Service

3.1 Creating a Key Pair

For system security purposes, it is recommended that you use the key pair authentication mode to authenticate the user who attempts to log in to an ECS.

You can create a key pair and use it for authentication when logging in to your ECS.

NOTE

If you have already created a key pair, you do not need to create again.

You can create a key pair using either of the following methods:

- Creating a key pair on the management console

The public key is automatically saved in Huawei Cloud. The private key can be downloaded and saved on your local host. You can also save your private keys in Huawei Cloud and manage them with KPS based on your needs. Huawei Cloud uses encryption keys provided by KMS to encrypt your private keys to ensure secure storage and access. For details, see [Creating a Key Pair Using the Management Console](#).

NOTE


- The key pair created on the management console uses the **SSH-2 (RSA, 2048)** encryption and decryption algorithm.
- Key pairs created by an IAM user on the management console can be used only by the user. If multiple IAM users need to use the same key pair, you can create an account key pair.
- Creating a key pair using the PuTTYgen tool
Both the public key and private key can be stored on the local host. For details, see [Creating a Key Pair Using PuTTYgen](#).

NOTE

PuTTYgen is a tool for generating public and private keys. You can obtain the tool from <https://www.putty.org/>.

Creating a Key Pair Using the Management Console

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.

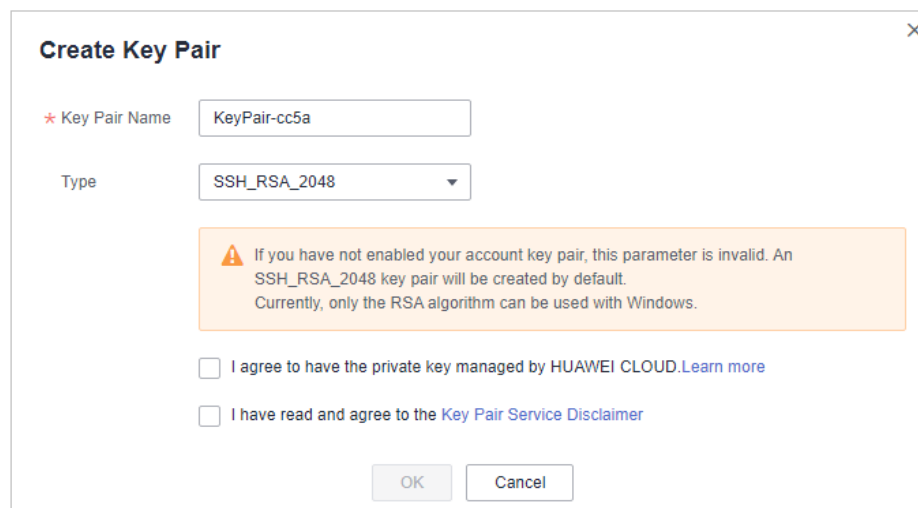
Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop.**

Step 4 In the navigation pane on the left, click **Key Pair Service.**

Step 5 Click **Create Key Pair.**

Step 6 In the **Create Key Pair** dialog box, enter a name for the key pair to be created.

Figure 3-1 Creating a key pair



Step 7 (Optional) Select a key pair type. If no key pair is enabled for your account, an SSH_RSA_2048 key pair will be created by default.

 **NOTE**

Currently, only the RSA algorithm can be used with Windows.

Step 8 If you want to have your private key managed, read and confirm **I agree to have the private key managed by HUAWEI CLOUD.** Select an encryption key from the **KMS encryption** drop-down list box. Skip this step if you do not need to have the private key managed.

 **NOTE**

- KPS uses the encryption key provided by KMS to encrypt private keys. When the user uses the KMS encryption function of the key pair, KMS automatically creates a default master key **kps/default** for encryption of the key pair.
- When selecting an encryption key, you can select an existing encryption key or click **View Key List** to create an encryption key.

Figure 3-2 Managing private keys

Create Key Pair

* Key Pair Name: KeyPair-ac98

Type: SSH_RSA_2048

Warning: If you have not enabled your account key pair, this parameter is invalid. An SSH_RSA_2048 key pair will be created by default. Currently, only the RSA algorithm can be used with Windows.

* KMS Encryption: kps/default [View Key List](#)

Key ID: f083197b-

I agree to have the private key managed by HUAWEI CLOUD. [Learn more](#)

I have read and agree to the [Key Pair Service Disclaimer](#)

OK Cancel

- Step 9** Read the *Key Pair Service Disclaimer* and select **I have read and agree to the Key Pair Service Disclaimer**.
- Step 10** Click **OK**. The browser automatically downloads the private key. When the private key is downloaded, a dialog box is displayed.
- Step 11** Save the private key as prompted by the dialog box.

NOTICE

- If the private key is not managed, it can be downloaded only once. Keep it properly. If the private key is lost, you can bind a key pair to the ECS again by resetting the password or key pair. For details, see [How Do I Handle the Failure in Logging In to ECS After Unbinding the Key Pair?](#)
- If you have authorized Huawei Cloud to manage the private key, you can export the private key anytime as required.

-
- Step 12** After the private key is saved, click **OK**. The key pair is created successfully.

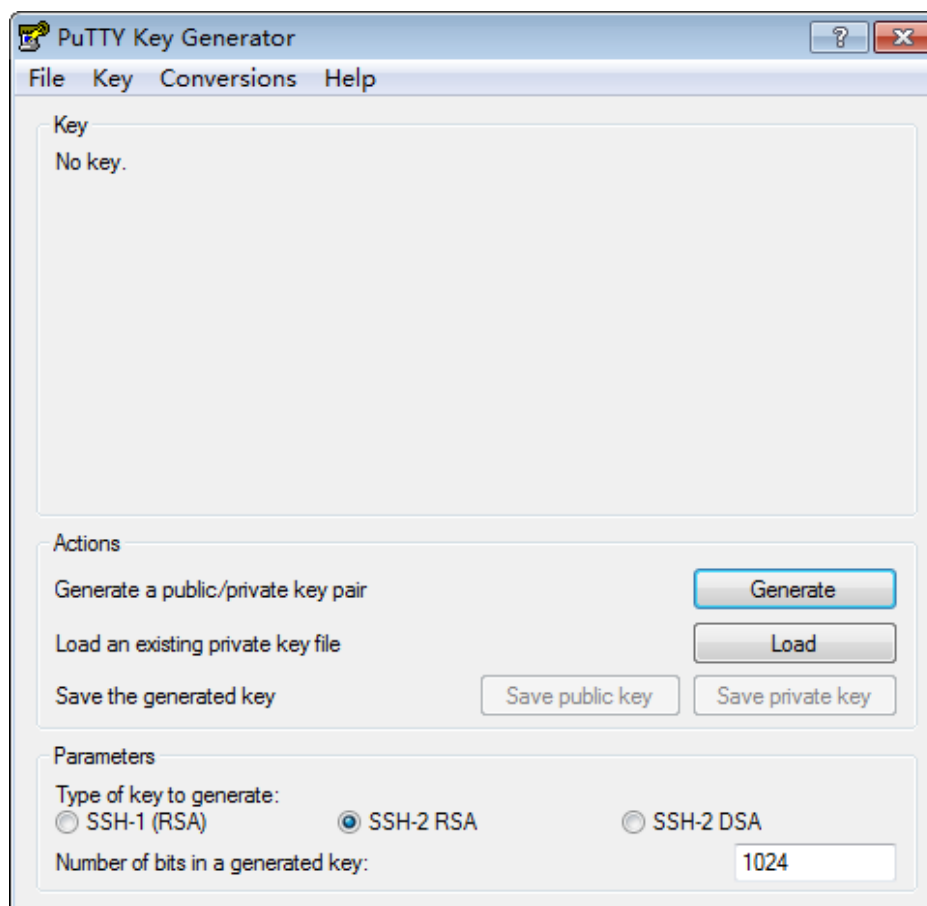
After the key pair is created, you can view it in the list of key pairs. The list displays information such as key pair name, fingerprint, private key, and quantity.

----End

Creating a Key Pair Using PuTTYgen

- Step 1** Generate the public and private keys. Double-click **PuTTYgen.exe**. The **PuTTY Key Generator** page is displayed, as shown in [Figure 3-3](#).

Figure 3-3 PuTTY Key Generator



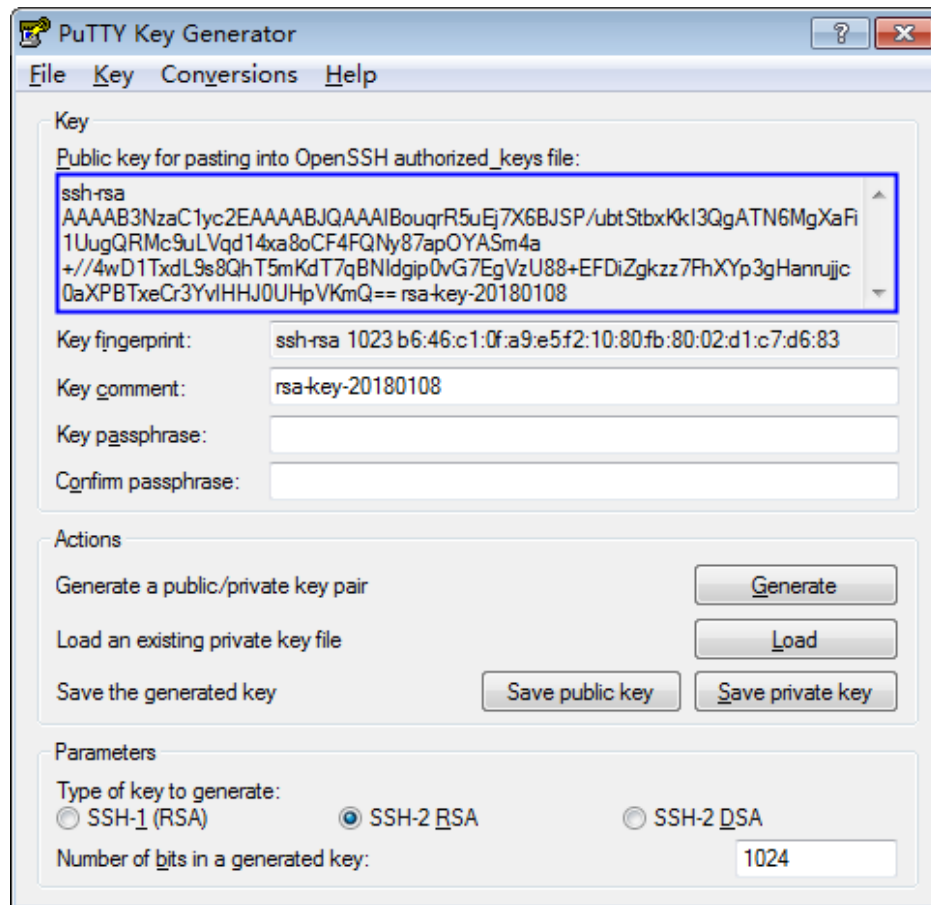
Step 2 Configure the parameters as described in [Table 3-1](#).

Table 3-1 Parameter description

Parameter	Description
Type of key to generate	Encryption and decryption algorithm of key pairs to be imported to the management console. Currently, only SSH-2 RSA is supported.
Number of bits in a generated key	Length of a key pair to be imported to the management console. Currently, the following length values are supported: 1024, 2048, and 4096 .

Step 3 Click **Generate** to generate a public key and a private key. See [Figure 3-4](#). Contents highlighted by the blue-line box show a generated public key.

Figure 3-4 Obtaining the public and private keys



Step 4 Copy the information in the blue square and save it in a local .txt file.

NOTICE

Do not save the public key by clicking **Save public key**. Saving a public key by clicking **Save public key** of PuTTYgen will change the format of the public key content. Such a key cannot be imported to the management console.

Step 5 Save the private key in PPK or PEM format.

NOTICE

For security purposes, the private key can only be downloaded once. Keep it secure.

Table 3-2 Format of a private key file

Private Key File Format	Private Key Usage Scenario	Saving Method
PEM	<ul style="list-style-type: none"> Use the Xshell tool to log in to the cloud server running the Linux operating system. Manage the private key on the management console. 	<ol style="list-style-type: none"> Choose Conversions > Export OpenSSH key. Save the private key, for example, kp-123.pem, to a local directory.
	Obtain the password of a cloud server running the Windows operating system.	<ol style="list-style-type: none"> Choose Conversions > Export OpenSSH key. NOTE Do not enter the Key passphrase information. Otherwise, the password fails to be obtained. Save the private key, for example, kp-123.pem, to a local directory.
PPK	Use the PuTTY tool to log in to the cloud server running the Linux operating system.	<ol style="list-style-type: none"> On the PuTTY Key Generator page, choose File > Save private key. Save the private key, for example, kp-123.ppk, to a local directory.

After the public key and private key are correctly saved, you can import the key pair to the management console.

----End

3.2 Importing a Key Pair

If you need to use your own key pair (for example, using the key pair created by the PuTTYgen tool), you can import the public key to the management console and use its private key to remotely log in to an ECS. You can also manage the private key on the management console of Huawei Cloud as necessary.

If multiple IAM users need to use the same key pair, use another tool (such as PuTTYgen) to create a key pair and import it for each of the IAM users separately.

Prerequisites

The public and private key files of the key pair to be imported are ready.


Constraints

- The SSH keys imported to the KPS console support the following cryptographic algorithms:

- ssh-dss
 - ssh-ed25519
 - ecdsa-sha2-nistp256
 - ecdsa-sha2-nistp384
 - ecdsa-sha2-nistp521
 - ssh-rsa. The maximum valid length is 2048,3072,4096.
- The format of the private key file that can be imported is PEM.
If the file is in the .ppk format, convert it to a .pem file. For details, see [How Do I Convert the Format of a Private Key File?](#)

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.

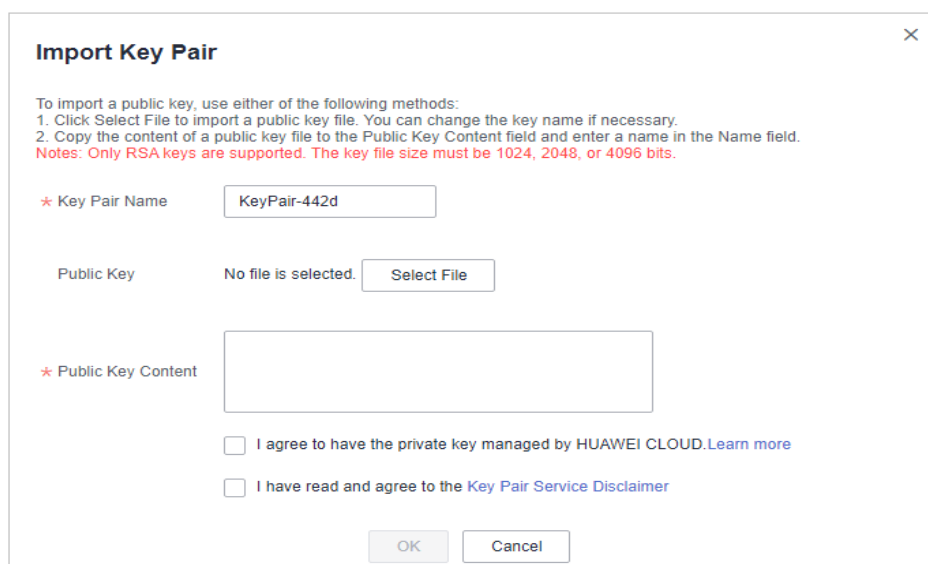
Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop.**

Step 4 In the navigation pane on the left, click **Key Pair Service.**

Step 5 Click **Import Key Pair.**

Step 6 In the **Import Key Pair** dialog box, click **Select File** and import a public key file, or copy and paste public keys in the **Public Key Content** text box.

Figure 3-5 Importing a key pair



NOTE

You can customize the name of an imported key pair.

- Step 7** If you want to have your private key managed, read and confirm **I agree to have the private key managed by HUAWEI CLOUD**. Skip this step if you do not need to have the private key managed.

Figure 3-6 Managing private keys

Import Key Pair

To import a public key, use either of the following methods:
1. Click Select File to import a public key file. You can change the key name if necessary.
2. Copy the content of a public key file to the Public Key Content field and enter a name in the Name field.
Notes: Only RSA keys are supported. The key file size must be 1024, 2048, or 4096 bits.

* Key Pair Name

Public Key No file is selected.

* Public Key Content

Private Key No file is selected.

* Private Key Content

* KMS Encryption

Key ID f083197b-

I agree to have the private key managed by HUAWEI CLOUD. [Learn more](#)

I have read and agree to the [Key Pair Service Disclaimer](#)

1. Click **Select File**, select the **.pem** private key file to be imported. Alternatively, you can copy and paste the private key content to the **Private Key Content** text box.
2. Select an encryption key from the **KMS Encryption** drop-down list box.

NOTE

- KPS uses the encryption key provided by KMS to encrypt private keys. When the user uses the KMS encryption function of the key pair, KMS automatically creates a default master key **kps/default** for encryption of the key pair.
- You can select an existing encryption key or click **View Key List** to create one.

- Step 8** Read the *Key Pair Service Disclaimer* and select **I have read and agree to the Key Pair Service Disclaimer**.

- Step 9** Click **OK** to import the key pair.

----End

3.3 Upgrading a Key Pair

To allow all the users under your account to use your key pairs, you can upgrade the key pairs to account key pairs.

Prerequisites


- A key pair has been created or imported.
- The service ticket for key upgrade has been handled.

Constraints

- Key pairs using the same names as existing account key pairs or other users' private key pairs cannot be upgraded.

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.

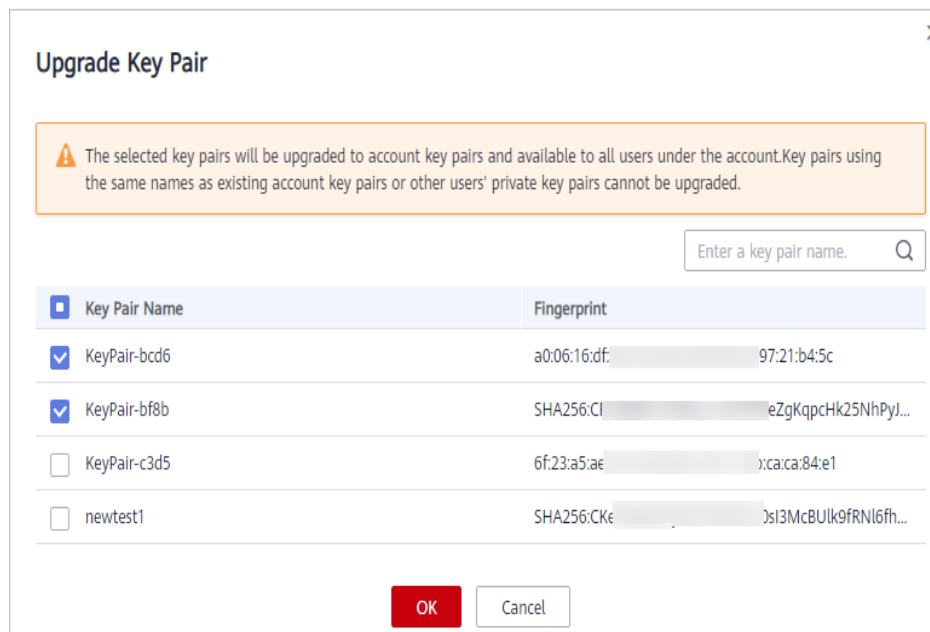
Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane on the left, click **Key Pair Service**.

Step 5 Click **Upgrade Key Pair**.

Step 6 In the dialog box that is displayed, select the key pair to be upgraded and click **OK**, as shown in [Figure 3-7](#).

Figure 3-7 Upgrading a key pair



NOTE

Upgraded key pairs are displayed in the account key pair list.

----End

3.4 Managing Key Pairs

3.4.1 Binding a Key Pair

If you set the login mode to **Password** when purchasing an ECS that runs Linux, you can bind a key pair to the ECS on the KPS console. KPS will configure the key pair, and then the ECS login mode will be changed to **Key Pair**. After the key pair is bound, you can use the private key to log in to the ECS.

This section describes how to bind a key pair to an ECS on the KPS console.

Prerequisites


- The ECS must be in the **Running** or **Shut down** state.
- The ECS has not been bound to a key pair.
- The ECS whose key pair is to be reset uses the public image provided by Huawei Cloud.
- To bind to a key pair, you can write the public key of the user to the `/root/.ssh/authorized_keys` file on the server. Ensure that the file is not modified before binding to the key pair. Otherwise, the binding will fail.

Constraints

- On the management console, key pairs cannot be bound to ECSs that run Windows.
- Key pairs cannot be bound to public images running CoreOS, OpenEuler, FreeBSD (Other), Kylin V10 64-bit, or UnionTech OS Server 20 Euler 64-bit.

Binding a Key Pair

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 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane on the left, click **Key Pair Service**.

Step 5 Click the **ECS List** tab.

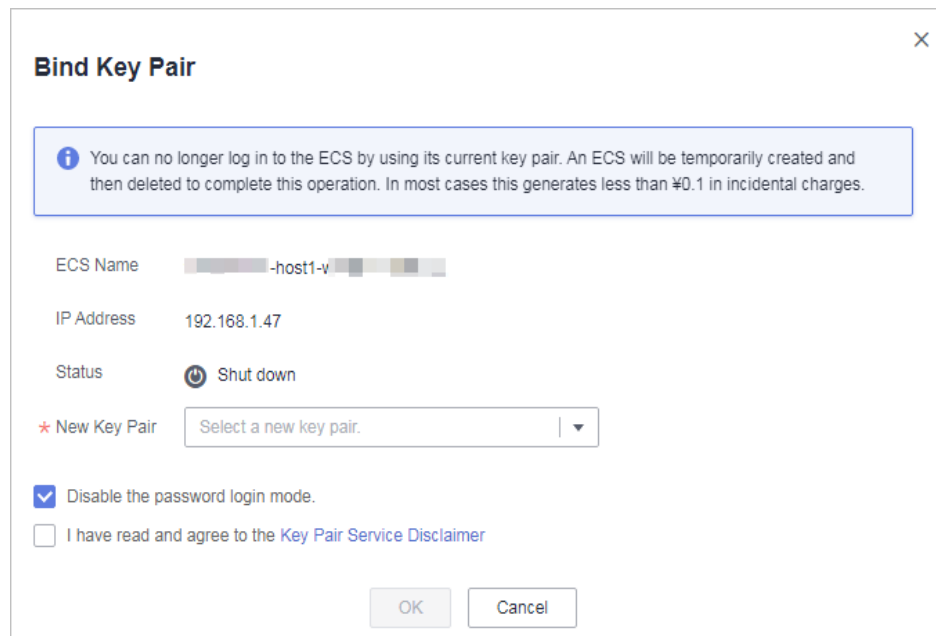
Figure 3-8 Binding

ECS Name/ID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
ecs-6501 0ea1e6df-cc80-49ce-a9...	Running	192.168.0.32		-	Bind
BT_smq 0e9a1102-5226-4c53-a2...	Running	192.168.0.95		-	Bind

Step 6 Click **Bind** in the row of an ECS to open the **Bind Key Pair** dialog box.

- If the ECS is shut down, a dialog box will be displayed, as shown in [Figure 3-9](#).

Figure 3-9 Binding a key pair (1)



- If the ECS is running, you need to provide the root password. See [Figure 3-10](#).

Figure 3-10 Binding a key pair (2)

Bind Key Pair

i The system will configure the key pair for the server. After this operation, you can use the key to log in to the server. To ensure security, it is recommended that you disable the password login mode of the server and use only the key to log in to the server.

ECS Name ecs-ee06-cmv-...
IP Address 192.168.1.40
Status ➔ Running

* New Key Pair Select a new key pair. | ▾
* Root Password

Disable the password login mode.
 I have read and agree to the [Key Pair Service Disclaimer](#)

OK Cancel

NOTE

- If you have the root password of the ECS, you can directly enter the password to bind the key pair to the ECS.
- If you do not have the root password of the ECS, you can shut down the ECS and bind the key pair when the ECS is in the shut-down state.

Step 7 Select a new key pair from the drop-down list box of **New Key Pair**.

Step 8 You can choose whether to disable the password login mode as necessary. By default, the password login mode is disabled.

NOTE

- If you do not disable the password login mode, you can use the password or the key pair to log in to the ECS.
- If the password login mode is disabled, you can use only the key pair to log in to the ECS. If you need to use the password login mode later, you can enable the password login mode again. For details, see [How Do I Enable the Password Login Mode for an ECS?](#)

Step 9 Select **I have read and agree to the Key Pair Service Disclaimer**.

Step 10 Click **OK** to complete the operation.

- If the ECS is not shut down, use the root password to bind the key pair. It takes about 30 seconds to complete.
- If the ECS is shut down, the binding operation may take about five minutes.


----End

3.4.2 Viewing a Key Pair

This section describes how to view the key pair information, including the names, fingerprints, private keys, and used keys on the KPS page of the DEW 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 Click . Choose **Security & Compliance > Data Encryption Workshop.**

Step 4 Check key pair information in the list.

NOTE

The list describes the names, fingerprints, private keys, and statuses of key pairs.

Step 5 Click the name of the target key pair. The detailed information about the key pair and the list of ECSs using the key pair are displayed.

Figure 3-11 Key pair details



Key Pair Name	01UEVNI				
Fingerprint	53:aa:b8:0b:58:1...:98:f8:3d:b3				
Private Keys	--				
Quantity	1				
Created	Mar 24, 2020 19:42:58 GMT+08:00				
Description	-- 				
ECS List					
ECS Name/ID	Status	Private IP Address	Elastic IP Address	Associated Key Pair	Operation
ecs-XSS fcd99d94-d5e9-4b8d-b80...	 Running	192.168.3.232		01UEVNI	Replace Reset Unbind

NOTE

When you purchase an ECS, choose the login method of using a key pair. Then the key pair will be bound to the ECS after the ECS is purchased.

Bind a key pair to ECSs. For details about parameters, see [Table 3-3](#).

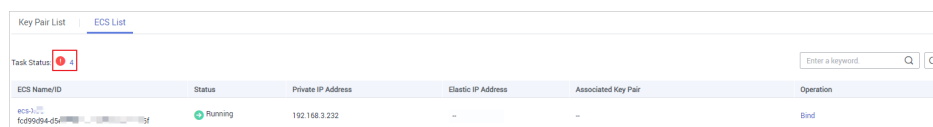
Table 3-3 Parameter description


Parameter	Description
ECS Name/ID	Name and ID of an ECS

Parameter	Description
Status	Statuses of an ECS are as follows: <ul style="list-style-type: none"> • Running • Creating • Faulty • Shut down • DELETE • HARD_REBOOT • MIGRATING • REBOOT • RESIZE • REVERT_RESIZE • SHELVED • SHELVED_OFF • LOADED • UNKNOWN • VERIFY_RESIZE
Private IP address	Private IP Address
EIP	Elastic IP address
Bound key pair	Key pair that is bound to the ECS

Step 6 Click **ECS List** to view ECSs.

Figure 3-12 ECS list



Step 7 Click the number next to the task status icon  to view failed tasks, as shown in [Figure 3-13](#).

 **NOTE**

Status of resetting or replacing the key pair:

 : Executing

 : Execution failed

Figure 3-13 Failed key pair tasks

Failed Key Pair Tasks

 You can view the key pair execution failure records in the following list. For ECSs on which key pairs are successfully configured, view them in the key pair list. You can delete failure records if they are no longer needed. [Learn more](#)

Delete All

ECS Name/ID	Key Pair Name	Operati...	Executed On	Failure Cause	Opeartion
xiaosong_hsm_test	3a-lc	Bind	Aug 09, 2021 16:...	Server login credential in...	Delete
xiaosong_hsm_test	3a-lc	Bind	Aug 09, 2021 16:...	Server login credential in...	Delete
scc-dbss-bj4-81617	3a-lc	Bind	Aug 09, 2021 16:...	Server login credential in...	Delete

NOTE

- You can click **Delete** in the row where the target key pair is displayed to delete the failed key pair task. You can also click **Delete All** on top of the list to delete all failed tasks.
- Click **Learn more** to view related documents.

----End

3.4.3 Resetting a Key Pair

If your private key is lost, you can use a new key pair to reconfigure the ECS through the management console. After resetting the key pair, you need to use the private key of the new key pair to log in to the ECS, and the original private key cannot be used to log in to the ECS.


This section describes how to reset a key pair on the KPS console.

Prerequisites

- The ECS whose key pair is to be reset uses the public image provided by Huawei Cloud.
- To reset the key pair, you can replace the public key of the user by modifying the `/root/.ssh/authorized_keys` file on the server. Ensure that the file is not modified before resetting the key pair. Otherwise, the reset will fail.
- The ECS must be in the **Shut down** state.

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.

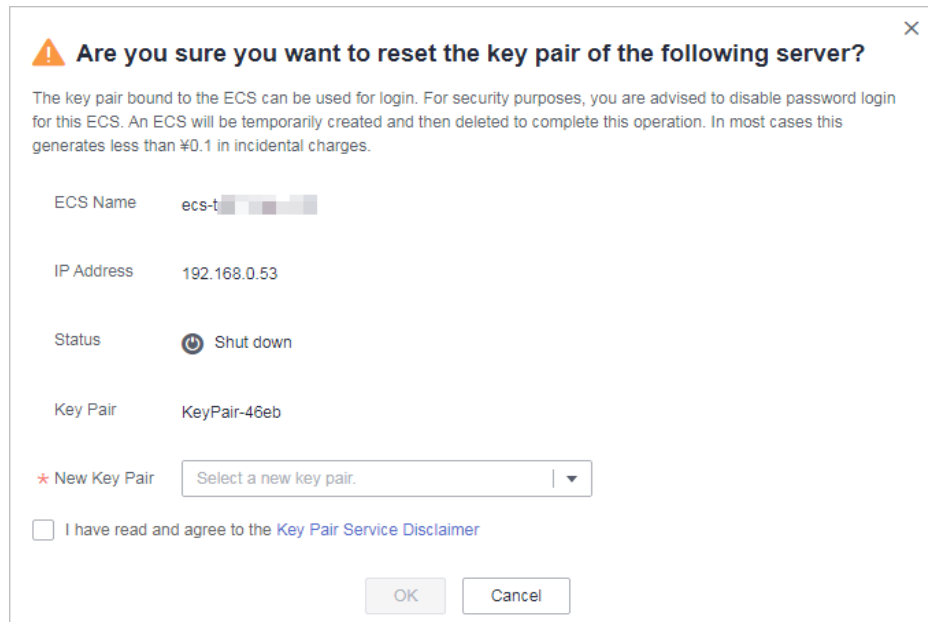
Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane on the left, click **Key Pair Service**.

Step 5 Click the **ECS List** tab.

Step 6 Click **Reset** in the row of an ECS.

Figure 3-14 Resetting a key pair



Step 7 Select a new key pair from the drop-down list box of **New Key Pair**.

Step 8 Select **I have read and agree to the Key Pair Service Disclaimer**.

Step 9 Click **OK**. The ECS key pair will be reset in about 10 minutes.

-----End

3.4.4 Replacing a Key Pair

If your private key is leaked, you can use a new key pair to replace the public key of the ECS through the management console. After replacing the key pair, you need to use the private key of the new key pair to log in to the ECS, and the original private key cannot be used to log in to the ECS.

This section describes how to replace a key pair on the KPS console.

Prerequisites

- The ECS whose key pair is to be replaced uses the public image provided by Huawei Cloud.
- To replace the key pair, you can replace the public key of the user by modifying the `/root/.ssh/authorized_keys` file on the server. Ensure that the file is not modified before replacing the key pair. Otherwise, replacing the public key will fail.
- The ECS must be in the **Running** state.

Procedure



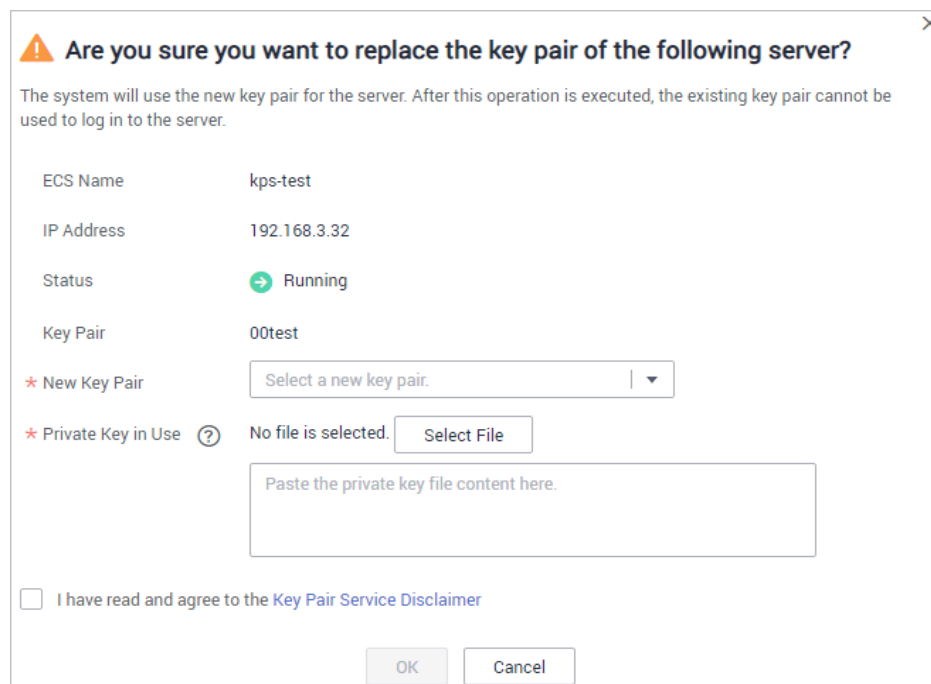
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop.**
- Step 4** In the navigation pane on the left, click **Key Pair Service.**
- Step 5** Click the **ECS List** tab.
- Step 6** Click **Replace** in the row of an ECS. Set parameters in the dialog box that is displayed.

Figure 3-15 Replacing a key pair



- Step 7** Select a new key pair from the drop-down list box of **New Key Pair.**
- Step 8** Click **Select File** to upload the private key (in .pem format) of the original key pair or copy the private key content to the text box.

NOTE

The private key to be uploaded or copied to the text box must be in the .pem format. If it is in the .ppk format, convert it by referring to [How Do I Convert the Format of a Private Key File?](#)

- Step 9** Select **I have read and agree to the Key Pair Service Disclaimer.**
- Step 10** Click **OK.** The key pair will be replaced from the ECS in about one minute.

----End

3.4.5 Unbinding a Key Pair

When you use a key pair to log in to an ECS, if you want to change the key pair mode to password, you can unbind the key pair on the management console. The KPS will unbind the key pair from the ECS. After the key pair is unbound, you can use the password to log in to the ECS.

Prerequisites


- The ECS must be in the **Running** or **Shut down** state.
- The ECS has been bound to a key pair.
- The ECS to be unbound from its key pair uses the public image provided by Huawei Cloud.
- To unbind from a key pair, you can delete the public key of the user from the `/root/.ssh/authorized_keys` file on the server. Ensure that the file is not modified before unbinding from the key pair. Otherwise, the unbinding will fail.

Constraints

- If you have not set the password for logging in to the ECS or forget the login password, you can reset the login password of the ECS on the ECS console. For more information, see *Elastic Cloud Server User Guide*.
- If you enabled key pair login for an ECS during its creation but unbound the key pair used for login, to bind the key pair again, shut down the ECS first.
- After you unbound an ECS from its key pair, reset the password on the ECS console in a timely manner. For more information, see *Elastic Cloud Server User Guide*.

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 Click . Choose **Security & Compliance** > **Data Encryption Workshop**.

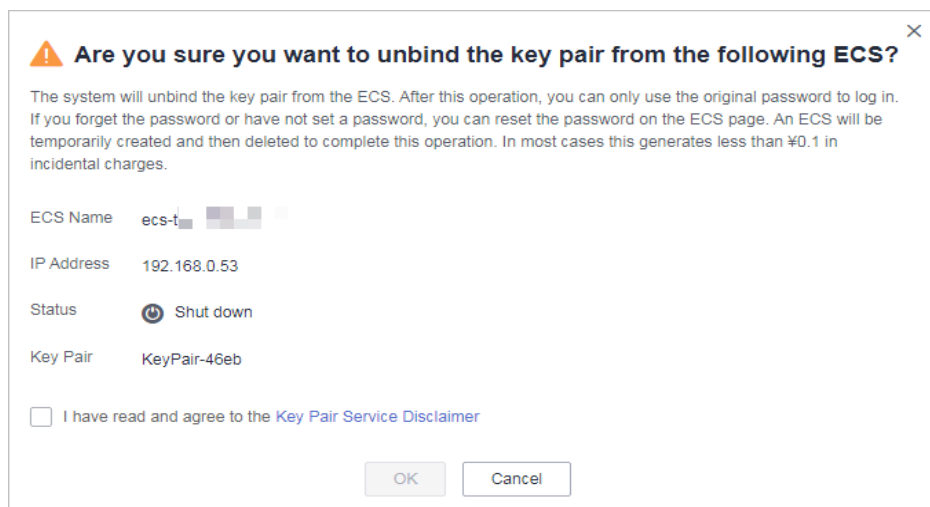
Step 4 In the navigation pane on the left, click **Key Pair Service**.

Step 5 Click the **ECS List** tab.

Step 6 Click **Unbind** in the row of an ECS.

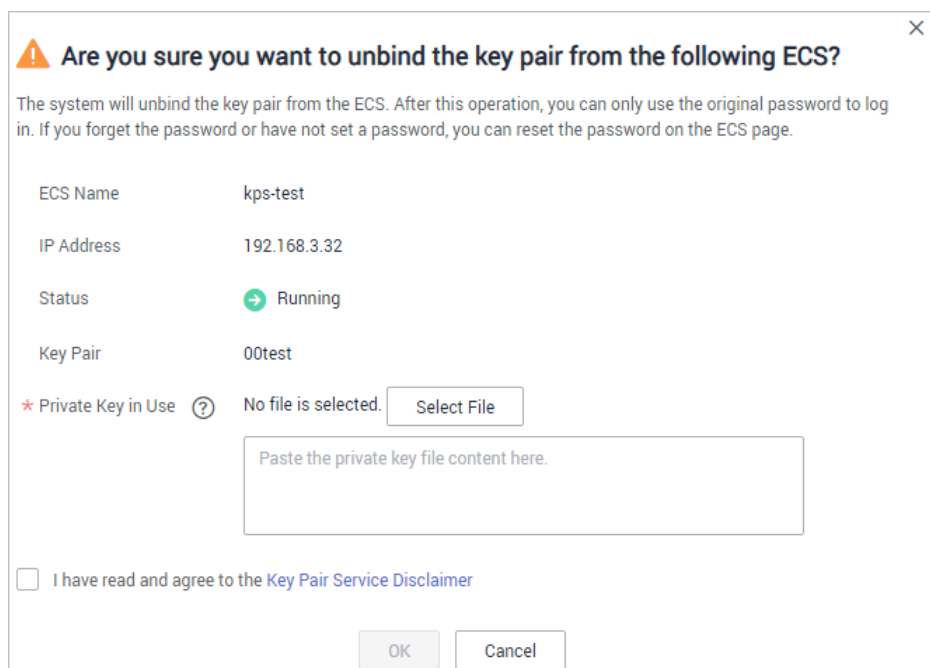
- If the ECS is shut down, a dialog box will be displayed, as shown in [Figure 3-16](#).

Figure 3-16 Unbinding a key pair (1)



- If the ECS is running, a dialog box will be displayed, as shown in [Figure 3-17](#).

Figure 3-17 Unbinding a key pair (2)



Step 7 If you unbind the key pair when the ECS is in the running state, you need to upload the private key. Click **Select file** to upload the private key (in the **.pem** format) of the existing key pair or copy the private key to the text box. If the ECS is shut down, skip this step.

NOTE

The private key to be uploaded or copied to the text box must be in the **.pem** format. If it is in the **.ppk** format, convert it by referring to [How Do I Convert the Format of a Private Key File?](#)

Step 8 Select **I have read and agree to the Key Pair Service Disclaimer**.

Step 9 Click **OK**. The key pair will be unbound from the ECS in about one minute.

 **NOTE**

After you unbound an ECS from its key pair, reset the password on the ECS console in a timely manner. For more information, see *Elastic Cloud Server User Guide*.

----End

3.4.6 Deleting a Key Pair

You can delete a key pair if it is no longer used.


This section describes how to delete a key pair on the KPS console

Constraints

- A deleted key cannot be recovered. Therefore, exercise caution when performing this operation.
- The private key imported for a key pair will be deleted with it.
- If you delete the public key that has been bound to an ECS on the KMS console and the private key has been saved locally, you can use the private key to log in to the ECS. The deletion operation does not affect the ECS login.

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 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane on the left, click **Key Pair Service**.

Step 5 In the row containing the desired key pair, click **Delete**.

 **NOTE**

If you have upgraded the key pair to an account key pair, perform the next step in the account key pair list.

Step 6 In the **Delete Key Pair** dialog box that is displayed, click **OK**. When **Key pair deleted successfully** is displayed in the upper right corner, the key pair is deleted.

----End

3.5 Managing Private Keys

3.5.1 Importing a Private Key

To facilitate local private key management, you can import the private key to the KPS console for centralized management of your private keys. The managed private keys are encrypted by the keys provided by KMS, ensuring security for

storage, import, and export of the private keys. You can download the private keys from the management console whenever you need. To ensure the security of the private keys, keep the downloaded private keys properly.

This section describes how to import a key pair on the KPS console.

Prerequisites


The private key file matching the public key has been obtained.

Constraints

- Only the private key that matches a public key can be imported for the public key.
- The private key to be uploaded or copied to the text box must be in the .pem format. If it is in the .ppk format, convert it by referring to [How Do I Convert the Format of a Private Key File?](#)
- When you enable the KMS encryption function for a key pair, KMS automatically creates a default master key **kps/default** for the key pair.
- When selecting an encryption key, you can select an existing encryption key or click **View Key List** to create an encryption key.

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 Click . Choose **Security & Compliance > Data Encryption Workshop.**

Step 4 In the navigation pane on the left, click **Key Pair Service.**

Step 5 Click **Import Private Key** in the row where the target public key is located. Set parameters in the **Import Private Key** dialog box.

Figure 3-18 Importing a private key

Import Private Key

! The private key is encrypted and managed by HUAWEI CLOUD. You can export the private key any time as necessary. HUAWEI CLOUD ensures that your private key is not used for any other purposes irrelevant to key pair management.

Note: The private key management service is currently free of charge. After the trial, the management service is charged by hour. [Learn more](#)

* Key Pair Name KeyPair-40a4

Private Key No file is selected.

* Private Key Content

* KMS Encryption

Key ID 864e64c8-4dbe-44b6-b8b1-1f9cb9d51b13

I have read and agree to the [Key Pair Service Disclaimer](#)

Step 6 Click **Select File**, select a local **.pem** private key file. Alternatively, you can copy and paste the private key content to the **Private Key Content** text box.

NOTE

- Only the private key that matches a public key can be imported to the public key.

Step 7 Select an encryption key from the **KMS encryption** drop-down list box.

NOTE

- When you enable the KMS encryption function for a key pair, KMS automatically creates a default master key **kps/default** for the key pair.
- When selecting an encryption key, you can select an existing encryption key or click **View Key List** to create an encryption key.

Step 8 Select **I have read and agree to the Key Pair Service Disclaimer**.

Step 9 Click **OK** to complete the import.

----End

3.5.2 Exporting a Private Key

If you have the private keys managed by the management console, you can download the private keys whenever you need. To ensure the security of the private key, keep the downloaded private key properly.

Prerequisites

The private key has been managed on the management console.

Constraints

A private key is encrypted and decrypted using the same encryption key. If the encryption key is deleted, the private key will fail to be exported.

Procedure



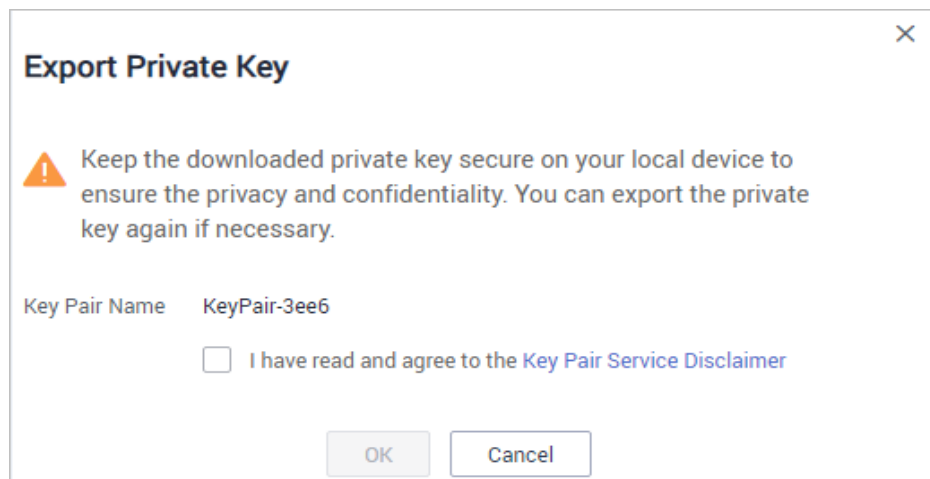
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security & Compliance > Data Encryption Workshop.**
- Step 4** In the navigation pane on the left, click **Key Pair Service.**
- Step 5** Click **Export Private Key** in the row where the target key pair resides. The **Export Private Key** dialog box is displayed, as shown in [Figure 3-19](#).

Figure 3-19 Exporting a private key



- Step 6** Select **I have read and agree to the Key Pair Service Disclaimer.**
- Step 7** Click **OK.** The browser automatically downloads the private key.

NOTICE

When exporting a private key, you need to use the encryption key that encrypts the private key to decrypt the private key. If the encryption key has been completely deleted, exporting the private key will fail.

----End

3.5.3 Clearing a Private Key

If the private keys managed by KPS are no longer needed, you can clear the managed private keys on the KPS console.

Prerequisites


The private key has been managed on the management console.

Constraints

After the private key is cleared, you cannot obtain the private key from Huawei Cloud. Exercise caution when performing this operation. If you need to have the private key managed again, you can import the private key 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 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane on the left, click **Key Pair Service**.

Step 5 Click **Clear Private Key** in the row where the target public key is located to clear the private key.

NOTE

If you have upgraded the key pair to an account key pair, perform the following steps in the account key pair list.

Step 6 In the displayed **Clear Private Key** dialog box, click **OK**.

NOTE

After the private key is cleared, you cannot obtain the private key from Huawei Cloud. Exercise caution when performing this operation. If you need to have the private key managed again, you can import the private key to the management console.

----End

3.6 Using a Private Key to Log In to the Linux ECS

After you create or import a key pair on the KMS console, select the key pair as the login mode when purchasing an ECS, and select the created or imported key pair.

After purchasing an ECS, you can use the private key of the key pair to log in to the ECS.

Prerequisites

- The network connection between the login tool (such as PuTTY and XShell) and the target ECS is normal.
- You have bound an EIP to the ECS.
- You have obtained the private key file of the ECS.

Constraints

The formats of ECS private key files must meet the following requirements.

Table 3-4 Private key file formats

Local OS	Linux ECS Login Tool	Private Key File Format
Windows OS	Xshell	.pem
	PuTTY	.ppk
Linux OS	-	.pem or .ppk

If your private key file is not in the required format, convert it by referring to [How Do I Convert the Format of a Private Key File?](#)

Logging In from a Windows Computer

To log in to the Linux ECS from a Windows computer, perform the operations described in this section.

Method 1: Use PuTTY to log in to the ECS.

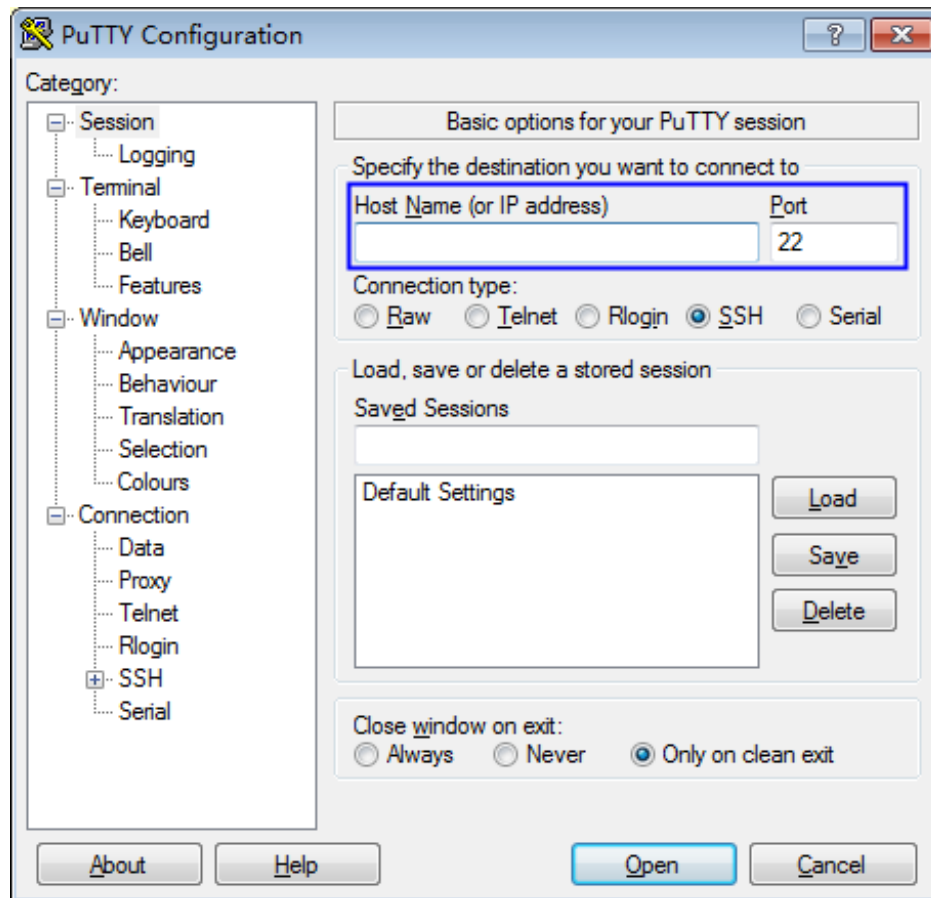
- Step 1** Double-click **PuTTY.EXE**. The **PuTTY Configuration** page is displayed.
- Step 2** Choose **Connection > Data**. Enter the image username in **Auto-login username**.

 **NOTE**

- If the public image of the **CoreOS** is used, the username of the image is **core**.
- For a **non-CoreOS** public image, the username of the image is **root**.

- Step 3** Choose **Connection > SSH > Auth**. In **Private key file for authentication**, click **Browse** and select a private key file (in the **.ppk** format).
- Step 4** Click **Session** and enter the EIP of the ECS under **Host Name (or IP address)**.

Figure 3-20 Configuring the EIP



Step 5 Click **Open** to log in to the ECS.

----End

Method 2: Use Xshell to log in to the ECS.

Step 1 Start the Xshell tool.

Step 2 Run the following command to remotely log in to the ECS through SSH:

```
ssh Username@EIP
```

An example command is provided as follows:

```
ssh root@192.168.1.1
```

Step 3 (Optional) If the system displays the **SSH Security Warning** dialog box, click **Accept & Save**.

Step 4 Select **Public Key** and click **Browse** next to the CMK text box.

Step 5 In the displayed dialog box, click **Import**.

Step 6 Select the locally stored key file (in the **.pem** format) and click **Open**.

Step 7 Click **OK** to log in to the ECS.

----End

Logging In from a Linux Computer

To log in to the Linux ECS from a Linux computer, perform the operations described as follows: The following procedure uses private key file **kp-123.ppk** as an example to log in to the ECS. The name of your private key file may differ.

Step 1 On the Linux CLI, run the following command to change operation permissions:

```
chmod 600 /path/kp-123.ppk
```

 NOTE

In the preceding command, **path** is the path where the key file is saved.

Step 2 Run the following command to log in to the ECS:

```
ssh -i /path/kp-123 root@EIP
```

 NOTE

- In the preceding command, **path** is the path where the key file is saved.
- *EIP* is the EIP bound to the ECS.

----End

3.7 Using a Private Key to Obtain the Login Password of Windows ECS

A password is required when you log in to a Windows ECS. First of all, you must obtain the administrator password (password of account **Administrator** or another account set in Cloudbase-Init) generated during the initial installation of the ECS from the private key file downloaded when you create the ECS. This password is randomly generated, with high security.

You can obtain the password for logging in to a Windows ECS through the management console

Prerequisites


You have obtained the private key file (in the **.pem** format) for logging in to the ECS.

Constraints

- After obtaining the initial password, you are advised to clear the password information recorded in the system to increase system security.
Clearing the initial password information does not affect ECS operation or login. Once cleared, the password cannot be restored. Before deleting a password, you are advised to record it. For details, see *Elastic Cloud Server User Guide*.
- You can also call the API to obtain the initial password of the Windows ECS. For details, see *Elastic Cloud Server API Reference*.
- The ECS private key file must be in .pem format.
If the file is in the .ppk format, convert it to a .pem file. For details, see [How Do I Convert the Format of a Private Key File?](#)

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 Click  and choose **Compute > Elastic Cloud Server**.

Step 4 In the ECS list, select the ECS whose password you want to get.

Step 5 In the **Operation** column, click **More** and choose **Get Password**.

Step 6 Use either of the following methods to obtain the password:

- Click **Select File** and upload the key file from a local directory.
- Copy the key file content to the text field.

Step 7 Click **Get Password** to obtain a new random password.

----End

4 Dedicated HSM

4.1 Operation Guide

Restrictions

- Dedicated HSM instances must be used together with VPC. After a Dedicated HSM instance is purchased, you need to configure its VPC, security group, and NIC on the management console before using it.
- For security purposes, Dedicated HSM instances do not provide services for the public network. To manage the instances, deploy their management tool in their VPC.

Operation Guide

To use Dedicated HSM on the cloud, you can purchase Dedicated HSM instances through the management console. After a Dedicated HSM instance is purchased, you will receive the UKey sent by Dedicated HSM. You need to use the UKey to initialize and control the instance. You can use the management tool to authorize service applications the permission to access Dedicated HSM instances. [Figure 4-1](#) illustrates the operation flow.

Figure 4-1 Operation Guide

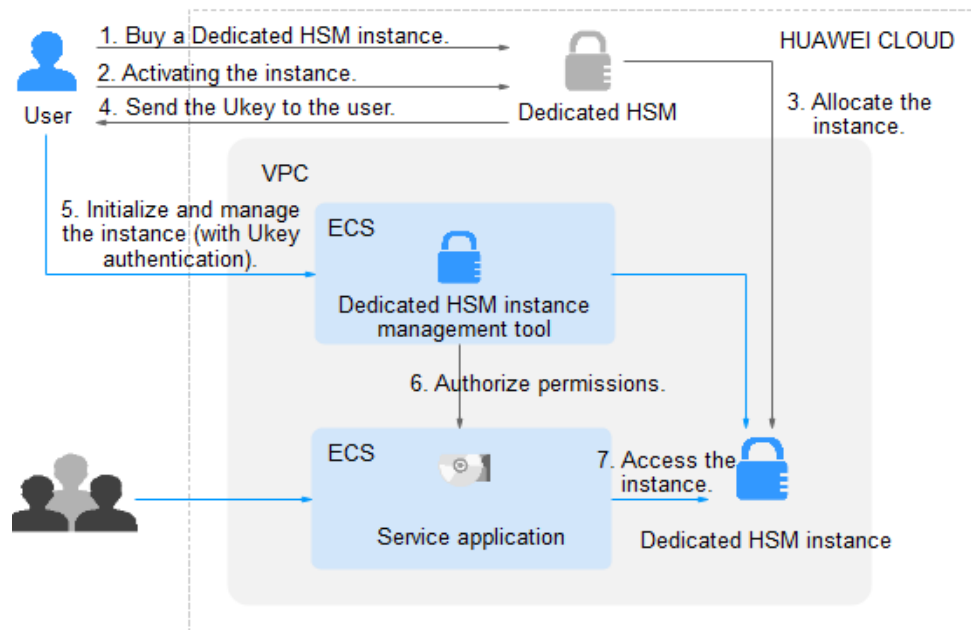


Table 4-1 describes the operation guide.

Table 4-1 Operation guide descriptions

No.	Procedure	Description	Operated By
1	Create a Dedicated HSM instance.	Create an instance on the Dedicated HSM management console. Huawei Cloud security team will evaluate your use scenarios to ensure that the instance meets your service requirements. Then you can pay for the ordered instance.	User
2	Activate a Dedicated HSM instance.	After an instance is purchased, you need to configure the instance on the management console. You need to select the VPC where the instance belongs and the function type of the instance. For details, see Activating a Dedicated HSM Instance .	User
3	Allocate a Dedicated HSM instance.	A purchased instance will be allocated to the user. A security expert will contact you through the contact information you provided and determine whether the instance ordered meets your service requirements. The instance will be allocated after the expert reviews and confirms your order.	Dedicated HSM security expert

No.	Procedure	Description	Operated By
4	Provide the UKey, initialization guide, and software.	<ul style="list-style-type: none"> A security expert sends the Ukey to the email address you provided. A UKey is the only identifier of a Dedicated HSM user. Keep it properly. A security expert will provide you with the software and guide for initializing Dedicated HSM instances. If you have any questions, contact the expert. 	Dedicated HSM security expert
5	Initialize and manage instances (involving UKey authentication).	<ol style="list-style-type: none"> Install the tool for managing Dedicated HSM instances on the instance management node. Use the UKey and the management tool to initialize the Dedicated HSM instance, and register an administrator to manage the Dedicated HSM instance and the key. <p>For details, see Initializing a Dedicated HSM Instance.</p>	User
6	Install the security agent and granting access permissions.	<p>Install and initialize the security agent on service application nodes.</p> <p>For details, see Installing the Security Agent and Granting Access Permissions.</p>	User
7	Access the instance.	Service applications access the Dedicated HSM instances through APIs or SDK.	User

4.2 Purchasing a Dedicated HSM Instance

4.2.1 Creating a Dedicated HSM Instance

When creating a Dedicated HSM instance, you need to specify the region and fill in your contact information.

The fee for a Dedicated HSM instance in platinum edition consists of the following two parts:

- Initial installation fee, charged when you create a Dedicated HSM instance.
- Yearly/Monthly fee, charged when [Activating a Dedicated HSM Instance](#).

Prerequisites

You have obtained the login account (with the **Ticket Administrator** and **KMS Administrator** permissions) and password for logging in to the management console.


Constraints

- When purchasing a Dedicated HSM instance, you need to submit a service ticket to set the UKey recipient information. Only the accounts with the **Ticket Administrator** permission can submit service tickets.
- After you created an instance, a UKey will be sent to the address in your contact information. Then you can use the UKey to initialize and authorize your service applications to access the instance.

You need to activate the instance before using it.

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 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane, choose **Dedicated HSM**.

Step 5 Click **Create Dedicated HSM** in the upper right corner of the page.

Step 6 **Billing Mode** can only be set to **Yearly/Monthly**.

Figure 4-2 Billing Mode



Step 7 Select the current region.

Figure 4-3 Selecting a region



Step 8 Select the service edition for the instance. [Table 4-2](#) lists related parameters.

Table 4-2 Edition parameters

Parameter	Description
Service Edition	Platinum edition
Encryption Algorithm	Encryption algorithm supported by the HSM instance. <ul style="list-style-type: none"> • Symmetric algorithm: AES • Asymmetric algorithm: RSA, DSA, ECDSA, DE, and ECDH • Digest algorithm: SHA1, SHA256, SHA384
Certification	FIPS 140-2 Level 3 certified

Step 9 Choose **Service Tickets > Create Service Ticket**. Our Huawei Cloud experts will contact you and provide a customized purchase plan and its quote.

- In the **Case Severity** drop-down list, select **General guidance**.
- In the **Problem Description** text box, enter **Dedicated HSM Contact Information**.

NOTICE

Ensure that the contact information provided in the **Confidential Information** text box is valid so that our security experts can contact you in a timely manner.

Figure 4-4 Creating a service ticket

The screenshot shows the 'Create Service Ticket' form with the following details:

- Case Severity:** A dropdown menu set to 'General guidance'.
- Region:** A dropdown menu.
- Problem Description:** A text area with a red border, containing the text 'Drag and drop images here. Markdown is supported.' and a character count '0/1,200'.
- Upload Attachments:** A field for selecting files to upload, with an 'Upload' button.
- Contact Method:** Radio buttons for 'Service Ticket Message', 'Mobile' (selected), and 'Email'.
- Mobile Number:** A field with a dropdown for '+86 (China)' and a text input containing '135****8834', with a green checkmark icon.
- Call Me at:** Radio buttons for 'Any Time' (selected) and 'Set Time'.
- Agreement:** A checked checkbox for 'I have read and agree to the Tenant Authorization Letter and Privacy Statement'.

Step 10 Click **Submit**. The service ticket is displayed on the **My Service Tickets** page.

 **NOTE**

After the service ticket is created successfully, you can click **View Details** in the **Operation** column to view details. You can remind the support team of a service ticket, leave your messages, cancel a service ticket, or closed a service ticket based on service ticket statuses.

----End

4.2.2 Activating a Dedicated HSM Instance

You need to activate a Dedicated HSM instance before using it. The yearly or monthly package will be charged during activation.

This section describes how to activate a Dedicated HSM instance through the management console.

Prerequisites


The status of the Dedicated HSM instance is **To be activated**.

Constraints

- The instance name can contain only letters, digits, underscores (_), and hyphens (-).
- Two nodes are created as the background resource pool for a Dedicated HSM instance. To ensure high availability of the nodes, a floating IP address is assigned to the instance.
- If the instance fails to be created, you can click **Delete** in the row where the instance is located to delete it. Then apply for a refund by submitting a service ticket.
- After a Dedicated HSM instance is successfully created, it can neither be changed to another type nor be refunded. To use a Dedicated HSM instance of another type, you need to buy another one.

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.

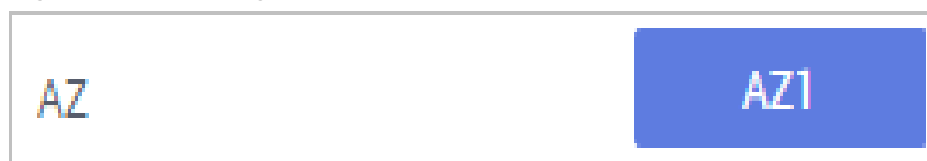
Step 3 Click . Choose **Security & Compliance > Data Encryption Workshop**.

Step 4 In the navigation pane, choose **Dedicated HSM**.

Step 5 Click **Activate** in the row where the target instance is located.

Step 6 Select an AZ.

Figure 4-5 Selecting an AZ



Step 7 Enter activation information, as shown in **Figure 4-6**. **Table 4-3** describes the parameters.

Figure 4-6 Configuring a Dedicated HSM instance

The screenshot shows a configuration form for a Dedicated HSM instance. The fields are as follows:

- Instance Name:** DedicatedHSM-3f9b-0002
- HSM Type:** Finance (dropdown menu). Below it, a description reads: "Provides key management and cryptographic operation services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication."
- VPC:** vpc-eb5f (dropdown menu). Below it, a note says: "You can select an existing VPC or apply for one."
- NIC:** (empty dropdown menu)
- Security Group:** WorkspaceManagerSecuri... (dropdown menu)

Table 4-3 Activation parameters

Parameter	Description	Example Value
Instance Name	Name of a Dedicated HSM instance NOTE The instance name can contain only letters, digits, underscores (_), and hyphens (-).	DedicatedHSM-3c98-0002
HSM Type	Available HSM types include Finance , Server , and Signature server . <ul style="list-style-type: none"> • Finance: Provides key management and encryption computing services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication. • Server: Provides secure, complete key management services and high-performance concurrent cryptographic operations, such as data signatures, signature verification, and data encryption/decryption. • Signature server: Guarantees the integrity, confidentiality, anti-repudiation, and post-event traceability of user data by using digital signatures, digital envelopes, and digital digests. 	Finance
VPC	You can select an existing Virtual Private Cloud (VPC), or click Apply for VPC to create one. For more information about VPC, see the <i>Virtual Private Cloud User Guide</i> .	vpc-test-dhsm

Parameter	Description	Example Value
NIC	<p>All available subnets are displayed on the page. The system automatically assigns three IP address to the instance.</p> <p>NOTE Two nodes are created as the background resource pool for a Dedicated HSM instance. To ensure high availability of the nodes, a floating IP address is assigned to the instance.</p> <p>For more information about subnets, see the <i>Virtual Private Cloud User Guide</i>.</p>	subnet-test-dhsm (192.168.0.0 /24)
Security Group	<p>The security group configured for the instance is displayed on the page. Once a security group is selected for an instance, the instance is protected by the security group access rules.</p> <p>For more information about security groups, see the <i>Virtual Private Cloud User Guide</i>.</p>	WorkspaceUserSecurityGroup

Step 8 If you have purchased a Dedicated HSM instance in standard edition:

Click **Create Now** to return to the Dedicated HSM instance list. You can view information about the activated instance.

If the status of the Dedicated HSM instance is **Creating**, the instance is successfully activated.

Step 9 If you have purchased a Dedicated HSM instance in platinum edition:

1. Set the required duration.

The required duration ranges from one month to one year.

 **NOTE**

The **Auto-renew** option enables the system to renew your service by the purchased period when the service is about to expire.

2. Confirm the configuration and click **Next**.

For any doubt about the pricing, click **Pricing details**.

3. On the **Order Details** page, confirm the order details, read and select **I have read and agree to the Privacy Policy Statement**.

4. Click **Pay Now** to pay for the yearly or monthly package.

5. On the **Pay** page, select a payment method to pay for your order.

After successful payment, you can view the information about the HSM instance on the HSM instance list page.

If the **Status** of the instance is **Creating**, the instance has been activated and is being allocated to you. It will be available in 5 to 10 minutes.

Creating: The system is allocating an instance to you. This process usually lasts for 5 to 10 minutes.

After the assignment, the instance status may change to either of the following:

- **Creation failed:** An instance fails to be created due to insufficient resources or network faults.

 **NOTE**

If the instance fails to be created, you can click **Delete** in the row where the instance is located to delete it. Then apply for a refund by submitting a service ticket.

- **Running:** An instance has been successfully assigned to you and is running properly.

 **NOTE**

After a Dedicated HSM instance is successfully created, it can neither be changed to another type nor be refunded. To use a Dedicated HSM instance of another type, you need to buy another one.


----End

4.3 Viewing Dedicated HSM Instances

This section describes how to view the Dedicated HSM instance information, including the name/ID, status, service version, device vendor, device model, IP address, and creation time.

Procedure

Step 1 [Log in to the management console.](#)

Step 2 Click . Choose **Security & Compliance > Data Encryption Workshop**. The **Key Management Service** page will be displayed.

Step 3 In the navigation pane, choose **Dedicated HSM**.

Step 4 In the list, you can view the information about the HSM instances.

[Table 4-4](#) describes the parameters in the HSM instance list.

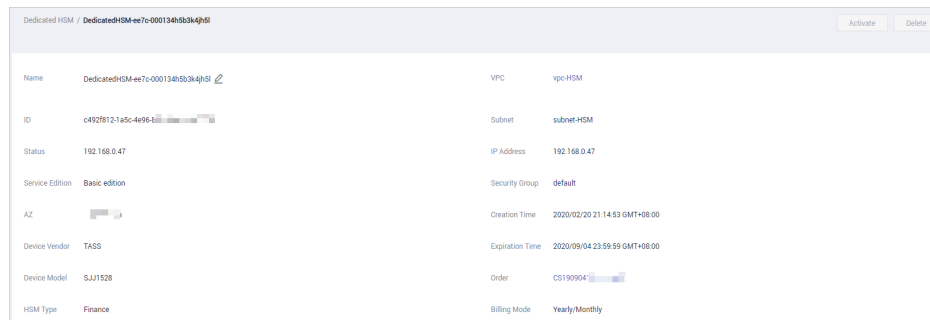
Table 4-4 Dedicated HSM instance parameters

Parameter	Description
Name/ID	Name and ID of a Dedicated HSM instance

Parameter	Description
Status	<p>Status of a Dedicated HSM instance:</p> <ul style="list-style-type: none"> • Installing After you pay the initial installation fee, the purchased instance will be installed. The status of the Dedicated HSM instance will be Installing. • To be activated The status of an instance that has been installed but not activated is To be activated. • Creating After you have activated an instance, the system will allocate the instance to you according to your configuration. The instance is in the status of Creating during this process. • Creation failed Due to insufficient resources or network faults, an instance may fail to be created. In this case, the instance will be in the status of Creation failed. • Running After an instance is configured and allocated, it will be in the status of Running. • Frozen If an instance is not renewed upon its expiration, its status changes to Frozen.
Service Edition	Platinum edition: You can exclusively use the HSM subrack, power supply, the network bandwidth, and API resources of the HSM.
AZ	AZ of a device
Device Vendor	Name of a device vendor.
Device Model	Model of the device
IP Address	Floating IP address of the Dedicated HSM instance
Expiration Time	Expiration time of the purchased HSM instance.

Step 5 You can click the name of a Dedicated HSM instance to view details about the instance, as shown in [Figure 4-7](#).

Figure 4-7 Details about Dedicated HSM instances



For more information, see [Table 4-5](#).

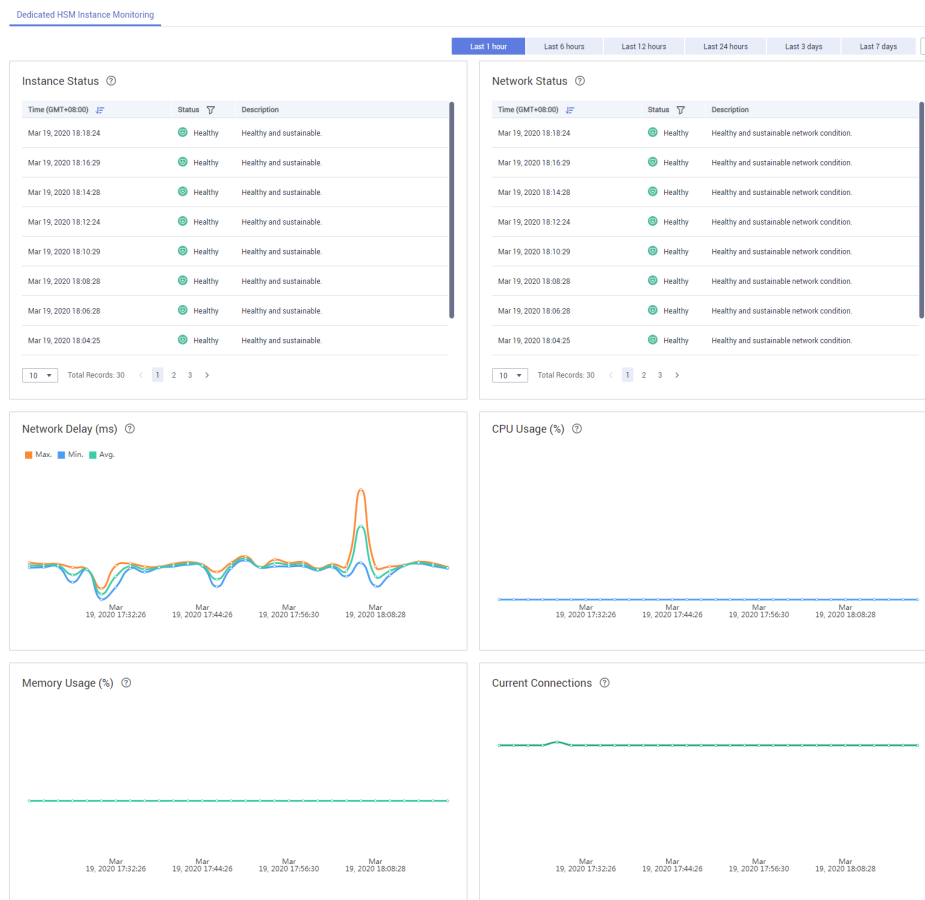
Table 4-5 Parameter description

Parameter	Description
Name	Name of a Dedicated HSM instance
ID	ID of an instance
Status	<p>Status of a Dedicated HSM instance:</p> <ul style="list-style-type: none"> ● Installing After you pay the initial installation fee, the purchased instance will be installed. The status of the Dedicated HSM instance will be Installing. ● To be activated The status of an instance that has been installed but not activated is To be activated. ● Creating After you have activated an instance, the system will allocate the instance to you according to your configuration. The instance is in the status of Creating during this process. ● Creation failed Due to insufficient resources or network faults, an instance may fail to be created. In this case, the instance will be in the status of Creation failed. ● Running After an instance is configured and allocated, it will be in the status of Running. ● Frozen If an instance is not renewed upon its expiration, its status changes to Frozen.
Service Edition	Platinum edition: You can exclusively use the HSM subrack, power supply, the network bandwidth, and API resources of the HSM.
Device Vendor	Name of a device vendor.

Parameter	Description
Device Model	Model of the device
HSM Type	Function types of an instance, including Finance , Server , and Signature Server .
VPC	VPC to which the instance belongs For more information about VPC, see <i>Virtual Private Cloud User Guide</i> .
Subnet	Subnet where the instance is located. For more information about subnets, see <i>Virtual Private Cloud User Guide</i> .
IP Address	Floating IP address of the Dedicated HSM instance
Security Group (SG)	Security group to which the instance belongs For more information about security groups, see <i>Virtual Private Cloud User Guide</i> .
Creation Time	Time when the instance is purchased
Expiration Time	Time when the instance expires
Order	Order ID of the instance. You can click the order number to query the order details.
Billing Mode	Yearly/Monthly prepaid package

Step 6 View the monitoring information about the Dedicated HSM instance, including the instance health, network health, network latency, CPU usage, memory usage, and number of current connections.

Figure 4-8 Dedicated HSM instance monitoring



----End

4.4 Using Dedicated HSM Instances

After your payment is complete, please wait for us to send the Ukey used for initializing the Dedicated HSM instance to your email address. A Dedicated HSM service expert will also contact you and send related documents and software, including the tool used for managing Dedicated HSM instances, and the security agent and SDK used for service calls.

Prerequisites

After configuring a Dedicated HSM instance, you need to initialize the instance, install the security agent, and grant access permissions. The following information is required.

Table 4-6 Required information

Item	Description	How to Obtain
Ukey	Stores the permission management information about the instance.	After the order is paid and the Dedicated HSM instance is configured, the Ukey will be sent to the recipient email address your provided.
Dedicated HSM instance management tool	Works with the UKey to remotely manage instances.	A service expert will also contact you and send related documents and software.
Dedicated HSM instance documents	<i>Dedicated HSM Instance User Manual</i> and <i>Dedicated HSM Instance Installation Guide</i>	
Security agent software	Establishes a secure connection with the instance.	
SDK	Provides APIs for Dedicated HSM. You can use the SDK to establish secure connections with instances.	
Dedicated HSM instance management node (for example, an ECS)	Run the Dedicated HSM instance management tool, which is in the same VPC where the Dedicated HSM instance resides, and allocate elastic IP addresses for remote connections.	Purchase ECSs as needed. For details, see Purchasing an ECS .
Service application nodes (for example, ECSs)	Run the security agent software and users' service applications, which must be in the VPC where the Dedicated HSM instance is deployed.	


Initializing a Dedicated HSM Instance

NOTE

Currently, you cannot log in to Dedicated HSM instances via SSH. You need to use the Dedicated HSM instance management tool to manage the instances.

Assume you want to use a Windows ECS as the Dedicated HSM instance management node. Perform the following steps to initialize the Dedicated HSM instance:

Step 1 Purchase a Windows ECS as the Dedicated HSM instance management node.

1. Log in to the management console.
2. Click . Choose **Computing** > **Elastic Cloud Server**.
3. Click **Buy ECS**.
 - Set **Region** and **AZ** to the same as those of the Dedicated HSM instance you purchased.
 - Set **Image** to a Windows public image.
 - Set **VPC** to the VPC where the Dedicated HSM instance belongs.
 - Configure **EIP**. It enables you to locally configure HSM instances conveniently.

 **NOTE**

After the Dedicated HSM instance is initialized, you can unbind from the elastic IP address. The binding and unbinding operations can be performed whenever needed.

- Set other parameters based on the site requirements.

Step 2 Initialize the Dedicated HSM instance by using the received management tool and related documents.

Step 3 After the initialization is complete, you can use the management tool to generate, destroy, back up, and restore keys.

 **NOTE**

If you have any questions during initialization and management, consult the Dedicated HSM service expert.

For more information, see the documents about Dedicated HSM instance: *Dedicated HSM Instance User Manual* and *Dedicated HSM Instance Installation Guide*.

----End

Installing the Security Agent and Granting Access Permissions

You need to install the security agent on a service application node to establish a secure channel to the Dedicated HSM instance.

Step 1 Download the certificate for accessing the Dedicated HSM instance from the management tool.

Step 2 Install the security agent on the service application node.

Step 3 Import the certificate to the security agent. Grant the service application the permission to access the Dedicated HSM instance.

Step 4 The service application can access the Dedicated HSM instance through SDK or APIs.

 **NOTE**

You can configure multiple Dedicated HSM instances in the security agent to balance loads.

----End

5 Auditing Logs

5.1 Operations supported by CTS

Table 5-1 lists DEW operations that are recorded by CTS.

Table 5-1 DEW operations supported by CTS

Operation	Resource Type	Trace Name
Key creation	cmk	createKey
Data key creation	cmk	createDatakey
Plaintext-free data key creation	cmk	createDatakeyWithoutPlaintext
Key enabling	cmk	enableKey
Key disabling	cmk	disableKey
Data key encryption	cmk	encryptDatakey
Data key decryption	cmk	decryptDatakey
Scheduled key deletion	cmk	scheduleKeyDeletion
Cancel of scheduled key deletion	cmk	cancelKeyDeletion
Random number generation	rng	genRandom
Key alias update	cmk	updateKeyAlias
Key description update	cmk	updateKeyDescription
Risk prompt of key deletion	cmk	deleteKeyRiskTips
Importing key material	cmk	importKeyMaterial

Operation	Resource Type	Trace Name
Deleting key material	cmk	deleteImportedKeyMaterial
Authentication creation	cmk	createGrant
Grant retiring	cmk	retireGrant
Grant revoking	cmk	revokeGrant
Data encryption	cmk	encryptData
Data decryption	cmk	decryptData
Tag adding	cmk	dealUnifiedTags
Tag deletion	cmk	dealUnifiedTags
Batch tag adding	cmk	dealUnifiedTags
Batch tag deletion	cmk	batchDeleteKeyTags
SSH key pair creation and import	keypair	createOrImportKeypair
SSH key pair deletion	keypair	deleteKeypair
Private key import	keypair	importPrivateKey
Private key export	keypair	exportPrivateKey
Purchasing an HSM instance	hsm	purchaseHsm
Configuring an HSM instance	hsm	createHsm
Deleting an HSM instance	hsm	deleteHsm

5.2 Using CTS to Query DEW Operation Traces

Once CTS is enabled, the system starts recording operations on KMS. Operation records for the last 7 days are stored on the CTS console.

Viewing Audit Logs of DEW

Step 1 Log in to the management console.

Step 2 Click . Under **Management & Governance**, click **Cloud Trace Service**.

Step 3 On the displayed page, you can query traces by setting the filtering criteria. The following four filters are available:

- **Trace Type, Trace Source, Resource Type, and Search By**
Select the filter from the drop-down list.

- Set **Trace Type** to **Management**.
- Set **Trace Source** to **KMS**.
- When you select **Trace name** for **Search By**, you also need to select a specific trace name. When you select **Resource ID** for **Search By**, you also need to select or enter a specific resource ID. When you select **Resource name** for **Search By**, you also need to select or enter a specific resource name.
- **Operator**: Select a specific operator (a user rather than tenant).
- **Trace Rating**: Available options include **all trace status**, **normal**, **warning**, and **incident**. You can only select one of them.
- **Time Range**: In the upper right corner of the page, you can query traces in the last one hour, last one day, last one week, or within a customized period.

Step 4 Click **Search** to view the corresponding operation event.

Step 5 Click  on the left of a trace to see its details. See [Figure 5-1](#).

Figure 5-1 Expanding trace details

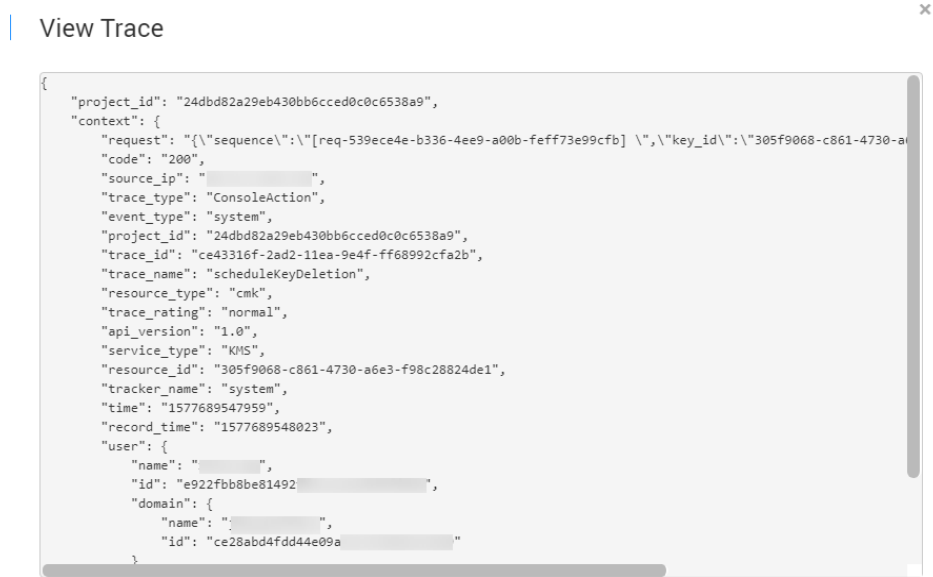
Trace Name	Resource Type	Trace Source	Resource ID	Resource Name	Trace Status	Operator	Operation Time	Operation
scheduleKeyDe...	cmk	KMS	305f9068-c861-4...	-	normal		Dec 30, 2019 15:05:47 GMT+08:00	View Trace


```

request [{"sequence":"req-539e4e-b336-4ee9-a00b-fef73e99cfd","key_id":"305f9068-c861-4730-a6e3-f98c28824de1","pending_days":7}]
code 200
source_ip
trace_type ConsoleAction
event_type system
project_id 244dbd82a29eb430bb6cced0c0c6538a9
trace_id ce43316f2ad2-11ea-9e4f-ff68992cfa2b
trace_name scheduleKeyDeletion
resource_type cmk
trace_rating normal
apiVersion 1.0
service_type KMS
resource_id 305f9068-c861-4730-a6e3-f98c28824de1
tracker_name system
time Dec 30, 2019 15:05:47 GMT+08:00
record_time Dec 30, 2019 15:05:48 GMT+08:00
user {"name":"","id":"e222fb8bc":"","domain":"","name":"","id":"ce28abd4fd44e09a"}
    
```

Step 6 Click **View Trace** in the **Operation** column. On the displayed **View Trace** dialog box shown in [Figure 5-2](#), the trace structure details are displayed.

Figure 5-2 Viewing traces



----End

6 Permission Control

6.1 Creating a User and Authorizing the User the Permission to Access DEW

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 Huawei Cloud account or cloud service to perform professional, efficient O&M on your DEW resources.

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

This section describes the procedure for granting permissions (see [Figure 6-1](#)).

Prerequisites

Before authorizing permissions to a user group, you need to know which DEW permissions can be added to the user group. [Table 6-1](#) lists the DEW system policies.

For the system policies of other services, see [System Permissions](#).

Table 6-1 System-defined roles and policies supported by DEW

Role/Policy Name	Description	Type	Dependency
KMS Administrator	Administrator permissions for KMS	System role	None

Role/Policy Name	Description	Type	Dependency
KMS CMKFullAccess	Full permissions for KMS. Users with these permissions can perform all the operations allowed by policies.	System policy	None
DEW KeypairFullAccess	Full permissions for KPS. Users with these permissions can perform all the operations allowed by policies.	System policy	None
DEW KeypairReadOnlyAccess	Read-only permissions for KPS. Users with this permission can only view KPS data.	System policy	None

Table 6-2 describes the common operations supported by each system-defined permission of DEW. Select the permissions as needed.

Table 6-2 Common operations supported by each system-defined policy or role

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Creating a key	√	√	x	x
Enable a key	√	√	x	x
Disable a key	√	√	x	x
Schedule key deletion	√	√	x	x
Cancel scheduled key deletion	√	√	x	x
Modify a key alias	√	√	x	x
Modify key description	√	√	x	x
Generate a random number	√	√	x	x
Create a DEK	√	√	x	x

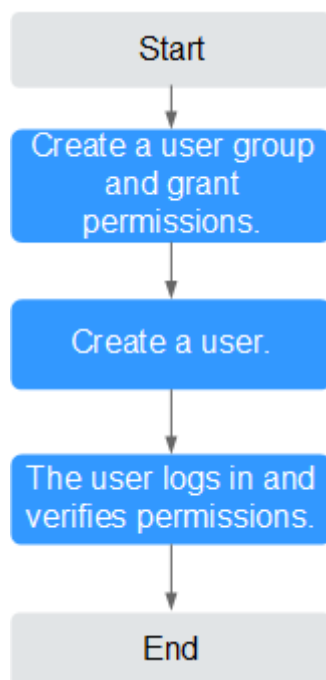
Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Create a plaintext-free DEK	√	√	x	x
Encrypt a DEK	√	√	x	x
Decrypt a DEK	√	√	x	x
Obtain parameters for importing a key	√	√	x	x
Import key materials	√	√	x	x
Delete key materials	√	√	x	x
Create a grant	√	√	x	x
Revoke a grant	√	√	x	x
Retire a grant	√	√	x	x
Query the grant list	√	√	x	x
Query retirable grants	√	√	x	x
Encrypt data	√	√	x	x
Decrypt data	√	√	x	x
Send signature messages	√	√	x	x
Authenticate signature	√	√	x	x
Enabling key rotation	√	√	x	x
Modify key rotation interval	√	√	x	x

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Disabling key rotation	√	√	x	x
Query key rotation status	√	√	x	x
Query CMK instances	√	√	x	x
Query key tags	√	√	x	x
Query project tags	√	√	x	x
Batch add or delete key tags	√	√	x	x
Add tags to a key	√	√	x	x
Delete key tags	√	√	x	x
Query the key list	√	√	x	x
Query key details	√	√	x	x
Query public key	√	√	x	x
Query instance quantity	√	√	x	x
Query quotas	√	√	x	x
Query the key pair list	x	x	√	√
Create or import a key pair	x	x	√	x
Query key pairs	x	x	√	√
Delete a key pair	x	x	√	x

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Update key pair description	x	x	√	x
Bind a key pair	x	x	√	x
Unbind a key pair	x	x	√	x
Query a binding task	x	x	√	√
Query failed tasks	x	x	√	√
Delete all failed tasks	x	x	√	x
Delete a failed task	x	x	√	x
Query running tasks	x	x	√	√

Authorization Process

Figure 6-1 Authorizing the DEW 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).

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 console as newly created user, and verify that the user only has read permissions for DEW.

- Choose **Service List > Data Encryption Workshop**. 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.

6.2 Creating a Custom DEW Policy

Custom policies can be created as a supplement to the system policies of DEW. For details about the actions supported by custom policies, see [Permissions Policies and Supported Actions](#).

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

- Visual editor: You can select policy configurations 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 about how to create custom policies, see [Creating a Custom Policy](#).

Example Custom Policies

- Example: authorizing users to create and import keys

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:cmk:create",
        "kms:cmk:getMaterial",
        "kms:cmkTag:create",
        "kms:cmkTag:batch",
        "kms:cmk:importMaterial"
      ]
    }
  ]
}
```

```
]
}
```

- Example: denying deletion of key tags

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 tags (**kms:cmkTag:delete**). Create a custom policy with the action to delete key tags, 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 except deleting key tags. The following is a policy for denying key pair tags.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "kms:cmkTag:delete"
      ]
    }
  ]
}
```

- Example: authorizing users to use keys

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:dek:crypto",
        "kms:cmk:get",
        "kms:cmk:crypto",
        "kms:cmk:generate",
        "kms:cmk:list"
      ]
    }
  ]
}
```

- Example: 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": [
        "rds:task:list"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:dek:crypto",
        "kms:cmk:get",
        "kms:cmk:crypto",
        "kms:cmk:generate",
        "kms:cmk:list"
      ]
    }
  ]
}
```



```
}  
  }  
  ]  
}
```

A Change History

Released On	Description
2023-01-30	This is the third official release. Added: Cloud Secret Management Service Key Pair Service Dedicated HSM
2023-01-10	This is the second official release. Optimized the description about encrypting key materials in Importing Key Materials .
2022-09-30	This is the first official release.