

# Data Encryption Workshop

## User Guide

**Issue** 02  
**Date** 2023-01-30



**Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.**

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

## **Trademarks and Permissions**



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

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

## **Notice**

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

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

# Security Declaration

## Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

---

# Contents

---

<b>1 Key Management Service.....</b>	<b>1</b>
1.1 Key Types.....	1
1.2 Creating a Key.....	2
1.3 Creating CMKs Using Imported Key Materials.....	7
1.3.1 Overview.....	7
1.3.2 Importing Key Materials.....	8
1.3.3 Deleting Key Materials.....	16
1.4 Managing CMKs.....	17
1.4.1 Viewing a CMK.....	18
1.4.2 Enabling One or More CMKs.....	20
1.4.3 Disabling One or More CMKs.....	20
1.4.4 Deleting One or More CMKs.....	21
1.4.5 Canceling the Scheduled Deletion of One or More CMKs.....	23
1.4.6 Adding a Key to a Project.....	23
1.5 Using the Online Tool to Encrypt and Decrypt Small-Size Data.....	24
1.6 Managing Tags.....	26
1.6.1 Adding a Tag.....	26
1.6.2 Modifying Tag Values.....	28
1.6.3 Deleting Tags.....	29
1.7 Rotating CMKs.....	29
1.7.1 About Key Rotation.....	30
1.7.2 Enabling Key Rotation.....	32
1.7.3 Disabling Key Rotation.....	35
1.8 Managing a Grant.....	36
1.8.1 Creating a Grant.....	36
1.8.2 Querying a Grant.....	38
1.8.3 Revoking a Grant.....	39
<b>2 Cloud Secret Management Service.....</b>	<b>41</b>
2.1 Creating a Shared Secret.....	41
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 Saving and Viewing Secret Values.....	46
2.3.2 Managing Secret Version Statuses.....	47
2.4 Managing Tags.....	49
2.4.1 Adding a Tag.....	49
2.4.2 Modifying a Tag Value.....	50
2.4.3 Deleting a Tag.....	51
<b>3 Key Pair Service.....</b>	<b>52</b>
3.1 Creating a Key Pair.....	52
3.2 Importing a Key Pair.....	57
3.3 Upgrading a Key Pair.....	61
3.4 Deleting a Key Pair.....	62
3.5 Using Key Pairs.....	62
3.5.1 Binding a Key Pair.....	62
3.5.2 Binding Key Pairs in Batches.....	65
3.5.3 Viewing a Key Pair.....	67
3.5.4 Resetting a Key Pair.....	70
3.5.5 Replacing a Key Pair.....	71
3.5.6 Unbinding a Key Pair.....	73
3.6 Managing Private Keys.....	75
3.6.1 Importing a Private Key.....	75
3.6.2 Exporting a Private Key.....	77
3.6.3 Clearing a Private Key.....	78
3.7 Using a Private Key to Log In to the Linux ECS.....	79
3.8 Using a Private Key to Obtain the Login Password of Windows ECS .....	81
<b>4 Dedicated HSM.....</b>	<b>83</b>
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.....	92
4.4 Using Dedicated HSM Instances.....	95
4.5 Managing Tags.....	97
4.5.1 Adding a Tag.....	97
4.5.2 Searching for a Dedicated HSM Instance by Tag.....	99
4.5.3 Modifying a Tag Value.....	100
4.5.4 Deleting a Tag.....	101
<b>5 Auditing Logs.....</b>	<b>103</b>
5.1 Operations supported by CTS.....	103
5.2 Querying Real-Time Traces.....	106
<b>6 Permission Control.....</b>	<b>108</b>
6.1 Creating a User and Authorizing the User the Permission to Access DEW.....	108

---

6.2 Creating a Custom DEW Policy..... 113

# 1 Key Management Service

## 1.1 Key Types

CMKs include custom keys and default keys. This section describes how to create, view, enable, disable, schedule the deletion, and cancel the deletion of custom keys.

Custom keys can be categorized into symmetric keys and asymmetric keys.

Symmetric keys are most commonly used for data encryption protection. 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	<ul style="list-style-type: none"><li>AES_256</li></ul>	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.

Key Type	Algorithm Type	Key Specifications	Description	Usage
Digest key	SHA	<ul style="list-style-type: none"> <li>• HMAC_256</li> <li>• HMAC_384</li> <li>• HMAC_512</li> </ul>	SHA digest key	<ul style="list-style-type: none"> <li>• Data tampering prevention</li> <li>• Data integrity verification</li> </ul>
Asymmetric key	RSA	<ul style="list-style-type: none"> <li>• RSA_2048</li> <li>• RSA_3072</li> <li>• RSA_4096</li> </ul>	RSA asymmetric password	Encrypts and decrypts a small amount of data or creates digital signatures.
	ECC	<ul style="list-style-type: none"> <li>• EC_P256</li> <li>• EC_P384</li> </ul>	Elliptic curve recommended by NIST	Digital signature

## 1.2 Creating a Key

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

Custom keys can be categorized into symmetric keys and asymmetric keys.

### Prerequisites

The account has KMS CMKFullAccess or higher permissions.

### Constraints

- You can create up to 20 custom keys, excluding default keys.
- Symmetric keys are created using the AES key. The AES-256 key can be used to encrypt and decrypt a small amount of data or data keys. The HMAC key is used to verify data integrity.
- 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 keys end with **/default**. When choosing aliases for your custom keys, do not use aliases ending with **/default**.
- DEW keys can be called through APIs for 20,000 times free of charge per month.

### Scenarios


- [Encrypt data in OBS](#)
- [Encrypt data in EVS](#)



- [Encrypt data in IMS](#)
- [Encrypt an RDS DB instance](#)
- Use custom keys to directly encrypt and decrypt small volumes of data.
- DEK encryption and decryption for user applications
- Message authentication code generation and verification
- Asymmetric keys can be used for digital signatures and signature verification.

## Creating a Key

**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** > **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](#)

You can organize cloud resources and users by enterprise project for more convenient management.

Keystore  [Create Keystore](#)

Description (Optional)  0/255

Tag (Optional) 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 20 more tags.

Key Price

API Request Price

This price is an estimate and may differ from the final price. For sites that support cross-region replication of keys, the project name prefix is added to the resource ID of the bill

- **Alias** is the alias of the key 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	<ul style="list-style-type: none"> <li>- AES_256</li> </ul>	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Digest key	SHA	<ul style="list-style-type: none"> <li>- HMAC_256</li> <li>- HMAC_384</li> <li>- HMAC_512</li> </ul>	SHA digest key	<ul style="list-style-type: none"> <li>- Data tampering prevention</li> <li>- Data integrity verification</li> </ul>
Asymmetric key	RSA	<ul style="list-style-type: none"> <li>- RSA_2048</li> <li>- RSA_3072</li> <li>- RSA_4096</li> </ul>	RSA asymmetric password	Encrypts and decrypts a small amount of data or creates digital signatures.
	ECC	<ul style="list-style-type: none"> <li>- EC_P256</li> <li>- EC_P384</li> </ul>	Elliptic curve recommended by NIST	Digital signature

- **Usage:** Select **SIGN\_VERIFY** or **ENCRYPT\_DECRYPT**.
  - For an AES\_256 symmetric key, the default value is **ENCRYPT\_DECRYPT**.
  - For an HMAC symmetric key, the default value is **GENERATE\_VERIFY\_MAC**.
  - 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 custom key.

 **NOTE**

You can enter up to 255 characters.

- 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**

- 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 custom key as needed, and enter the tag key and tag value.

 **NOTE**

- After creating a CMK, you can click the alias of the CMK to go to the CMK details page and add a tag to the CMK.
- The same tag (including tag key and tag value) can be used for different custom keys. However, under the same custom key, one tag key can have only one tag value.
- A maximum of 20 tags can be added for one custom key.
- To delete a tag, click **Delete** next to it.

**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 key list, you can view the created keys. The default status of a key 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 *Object Storage Service User 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 *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 *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 *Data Encryption Workshop API Reference*.

## 1.3 Creating CMKs Using Imported Key Materials

### 1.3.1 Overview

A custom key 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 custom key, the KMS automatically generates a key material for the custom key.
- If you want to use your own key material, you can use the key import function on the KMS console to create a custom key whose key material is empty, and import the key material to the custom key.

### 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
Imported keys	<ul style="list-style-type: none"> <li>• You can delete the key material, but cannot delete the custom key and its metadata.</li> <li>• Such keys cannot be rotated.</li> <li>• 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 custom key 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.</li> </ul> <p><b>NOTE</b> 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>

Key Material Source	Difference
Keys created in KMS	<ul style="list-style-type: none"> <li>• The key material cannot be manually deleted.</li> <li>• Symmetric keys can be rotated.</li> <li>• You cannot set the expiration time for key material.</li> </ul>

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

#### Constraints

- The HMAC key algorithm does not support the import of key materials.

#### 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 > 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:   [View predefined tags.](#)

Key Price:

API Request Price:

I understand the security and durability of using an imported key.

- **Alias** is the alias of the key 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.

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

- **Usage:** Select **SIGN\_VERIFY** or **ENCRYPT\_DECRYPT**.
  - For an AES\_256 symmetric key, the default value is **ENCRYPT\_DECRYPT**.
  - For an HMAC symmetric key, the default value is **GENERATE\_VERIFY\_MAC**.
  - 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 custom key.

 **NOTE**

You can enter up to 255 characters.

- 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**

- 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 custom key as needed, and enter the tag key and tag value.



 **NOTE**

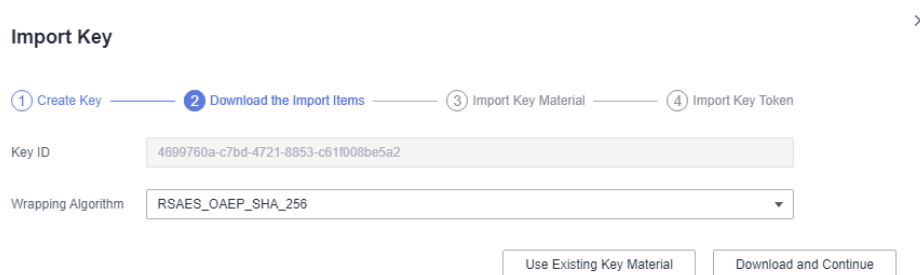
- If a custom key has been created without any tag, you can add a tag to the custom key later if needed. Click the alias of the custom key, choose the **Tags** tab, and click **Add Tag**.
- The same tag (including tag key and tag value) can be used for different custom keys. However, under the same custom key, one tag key can have only one tag value.
- A maximum of 20 tags can be added for one custom key.
- 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 custom key whose key material is empty.

**Step 9** Click **Next** to go to the **Download the Import Items** step. Select a key wrapping algorithm by referring to [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 algorithm that uses OAEP and has the <b>SHA-256</b> hash function	Select an algorithm based on your HSM functions. If the HSMs support the <b>RSAES_OAEP_SHA_256</b> algorithm, use <b>RSAES_OAEP_SHA_256</b> to encrypt key materials.

 **NOTE**


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

**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** to download the wrapping key file, as shown in **Figure 1-4**.

**Figure 1-4** Downloaded file

 wrappingKey\_ffe a7-a29927851940.bin

- **wrappingKey\_KeyID** is the wrapping key. It is encoded in binary format and used to encrypt the wrapping key of the key material.
- Import token: You do not need to download it. The import wizard automatically transfers the import token. If you close the wizard before completing the import, the token will automatically become invalid.

---

#### NOTICE

The wrapping key expires in 24 hours. If the wrapping key is invalid, download it again.

The import wizard automatically transfers the import token. If you close the wizard before completing the import, the token will automatically become invalid. To retry import, open the import wizard 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**; 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 pkeyutl** 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 RSA 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*.

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

Wrapping Key Algorithm	Key Material Encryption
RSAES_OAEP_SHA_256	<pre>openssl pkeyutl -in PlaintextKeyMaterial.bin -inkey PublicKey.bin -out EncryptedKeyMaterial.bin -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256</pre>

- 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 pkcs1_rsa_private_key.pem 4096
```

- 2) Convert the format to PKCS8.

```
openssl pkcs8 -topk8 -inform PEM -in
pkcs1_rsa_private_key.pem -outform pem -nocrypt -out
rsa_private_key.pem
```

- 3) Convert the PKCS8 format to the DER format.

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

- 4) 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 FAQs.

**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

Parameter	Description
Key material	Import a key material. For example, use the <b>EncryptedKeyMaterial.bin</b> file in <a href="#">Step 10.2.b</a> .

**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 <b>EncryptedKeyMaterial.bin</b> file in <a href="#">Step 10.2.b</a> .
Private key ciphertext	Select private key ciphertext. For example, select the <b>out_rsa_private_key.der</b> file in <a href="#">Step 10.2.c</a> .

**Figure 1-5** Importing key materials

**Import Key Material** ×

① Download the Import Items — ② **Import Key Material** — ③ Import Key Token

Key ID:

★ Temporary Key Material:

★ Private Key Ciphertext:

**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 import token obtained via API in <a href="#">12.b</a> .
Key material expiration mode	<ul style="list-style-type: none"> <li>• <b>Key material will never expire:</b> You use this option to specify that key materials will not expire after import.</li> <li>• <b>Key material will expire:</b> 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 <b>Pending import</b>.</li> </ul>

**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 the custom key 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.

 **NOTE**

- 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 custom key was deleted. To decrypt the data, re-import the key material.

## 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 custom key 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** > **Data Encryption Workshop**.

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

**Step 5** In the displayed dialog box, 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

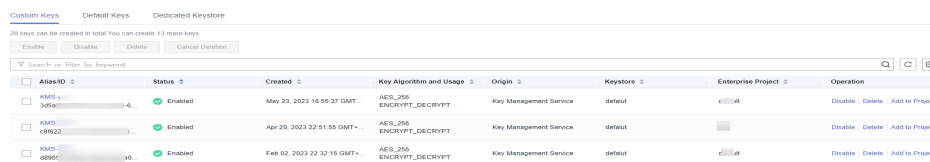
## 1.4.1 Viewing a CMK

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

### Procedure

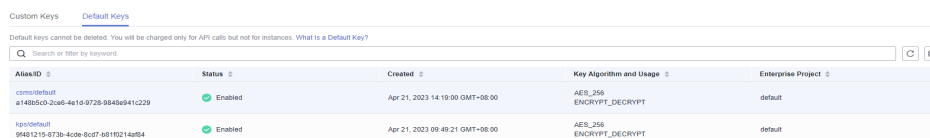
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security > Data Encryption Workshop**.
- Step 4** Check the key list. [Table 1-10](#) describes the parameters.

**Figure 1-7** Custom keys



AliasID	Status	Created	Key Algorithm and Usage	Origin	Keystore	Enterprise Project	Operation
KMS-3456	Enabled	May 23, 2023 16:55:37 GMT	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	at	Disable Delete Add to Project
KMS-0982	Enabled	Apr 20, 2023 22:51:55 GMT	AES_256 ENCRYPT_DECRYPT	Key Management Service	default		Disable Delete Add to Project
KMS-0986	Enabled	Feb 02, 2023 22:32:15 GMT	AES_256 ENCRYPT_DECRYPT	Key Management Service	default	at	Disable Delete Add to Project

**Figure 1-8** Default keys



AliasID	Status	Created	Key Algorithm and Usage	Enterprise Project
cmisdefault-41480600-2045-4615-9728-084069412229	Enabled	Apr 21, 2023 14:19:00 GMT+08:00	AES_256 ENCRYPT_DECRYPT	default
ipisdefault-9681215-873b-4c0e-8c07-08192114d54	Enabled	Apr 21, 2023 09:49:21 GMT+08:00	AES_256 ENCRYPT_DECRYPT	default

**Table 1-10** Key list parameters

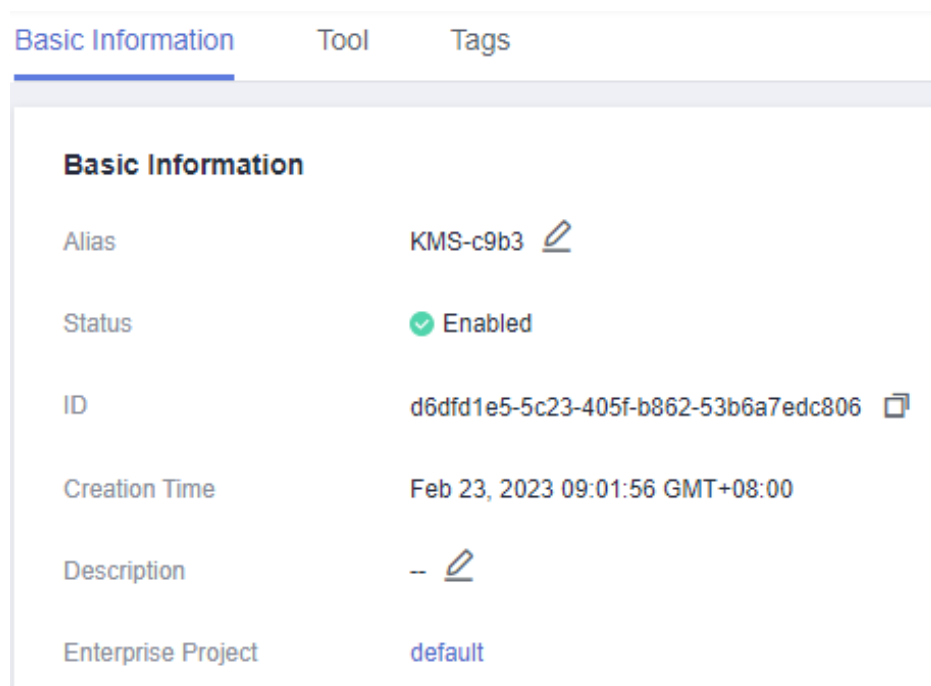
Parameter	Description
Alias/ID	<p>Alias of a key and the random ID of a key generated during its creation.</p> <p><b>NOTE</b> Use this ID as the value of <b>Path</b> if you are creating a custom policy in IAM and have selected <b>Specify resource path</b> for <b>KeyId</b>.</p>
Status	<p>Status of a CMK, which can be one of the following:</p> <ul style="list-style-type: none"> <li>● <b>Enabled</b> The CMK is enabled.</li> <li>● <b>Disabled</b> The CMK is disabled.</li> <li>● <b>Pending deletion</b> The CMK is scheduled for deletion.</li> <li>● <b>Pending import</b> If your CMK does not have materials, its status is <b>Pending import</b>.</li> </ul>



Parameter	Description
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"> <li>• <b>External</b> The key is imported to the KMS from an external system.</li> <li>• <b>Key Management Service</b> The key is a default key or created in KMS.</li> </ul>
Enterprise Project	Enterprise project the CMK is used for
Operation	Operations you can perform on the key, 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 key to view its details, as shown in [Figure 1-9](#).

**Figure 1-9** CMK details



 NOTE

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

- A default 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 custom keys. Only enabled custom keys can be used to encrypt or decrypt data. A new custom key is in the **Enabled** state by default.

### Prerequisites

The custom key 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 > Data Encryption Workshop**.

**Step 4** In the row containing the target custom key, click **Enable**.

**Step 5** In the displayed dialog box, click **OK** to enable the key.

 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 custom keys, thereby protecting data in urgent cases.

After being disabled, a custom key 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 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 > Data Encryption Workshop**.

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

**Step 5** In the displayed dialog box, 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 either of the following ways:

- Check the CMK permission to determine its possible usage scope. For details, see [Querying a Grant](#).
- Check audit logs to determine the actual usage. For details, see [Querying Real-Time Traces](#).

## Prerequisites


- The key to be deleted is in **Enabled**, **Disabled**, or **Pending import** 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 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 > Data Encryption Workshop.**

**Step 4** In the row containing the target CMK, click **Delete** in the **Operation** column.

**Figure 1-10** Scheduling the deletion of one CMK

AliasID	Status	Created	Key Algorithm and Usage	Origin	Keystore	Enterprise Project	Operation
KMS-adt6 27c473c7-ctfc-4b23-a9b3-2aa...	Enabled	Aug 08, 2023 19:37:46 GMT+	AES_256 ENCRYPT_DECRYPT	Key Management Service	dt		Disable <b>Delete</b> Add to Project

**Step 5** On the key deletion dialog box, enter the deletion delay time.

**Figure 1-11** Entering the period after which you want the deletion to take effect

Waiting Period (days)

---

**Delete Key**

The following 1 keys will be deleted.  
After the key is deleted, the data encrypted using the key cannot be decrypted. The key will be deleted seven or more days from now, and will not incur charges during the waiting period.

Alias	Status	ID
KMS-8299	Enabled	8b-812f

To confirm deletion, enter "DELETE" below:

**OK** Cancel

### 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** If a key is used to encrypt DDS, RDS, or NoSQL, after you click **OK**, a message "Key XXX is being used by XXX. Are you sure you want to delete it?" is displayed, as shown in [Figure 1-12](#). Click **Yes**.

**Figure 1-12** Confirming the deletion

Key is being used by dds. Are you sure you want to delete it?

----End

### NOTE

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

## 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 custom keys prior to deletion execution. After the cancellation, the key 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 > Data Encryption Workshop**.

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

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

- If a key is created on the KMS console, the status of the key changes to **Disabled** after its scheduled deletion is canceled. For details about how to enable the key, see [Enabling One or More CMKs](#).
- If the CMK is created using imported materials, its status becomes **Disabled** after the cancellation. To enable the CMK, see [Enabling One or More CMKs](#).
- If the CMK is created using imported materials and no key materials have been imported for it, its status becomes **Pending import** after the cancellation. To use the CMK, perform [Creating CMKs Using Imported Key Materials](#).

#### 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

Enterprise Project is a cloud governance platform that matches the organizational structure and service management model of your company. It helps you manage enterprise projects, resources, personnel, finance, and applications in the cloud based on the hierarchical organization structure (companies, departments, and projects) and project service structure.

If you have enabled enterprise project management, you can add specified custom keys to enterprise projects on the KMS console.

### Constraints


- The enterprise project management function has been enabled.

If you did not enable the enterprise project management function, the **Enterprise Project** option is not displayed on the console by default, and you cannot add keys to a project. For details about how to enable an enterprise project, see [Enabling Enterprise Center](#).

- The enterprise project of default keys cannot be changed.

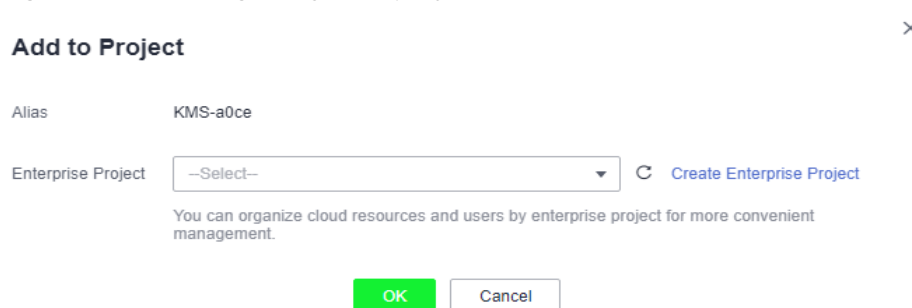
## Procedure

**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** Locate the target key, click **Add to Project**.

**Figure 1-13** Adding a key to a project



### NOTE

If you are a non-enterprise user, the **Add to Project** option is not displayed in the operation column.

For details about how to enable the enterprise project function, see [Enabling the Enterprise Center](#).

**Step 4** Select a project. 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.

### Prerequisites

The custom key is in **Enabled** status.


### Constraints

- Default keys cannot be used to encrypt or decrypt such data with the tool.

- Asymmetric keys cannot be used to encrypt or decrypt such data with the tool.
- You can call an API to use a default 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](#).

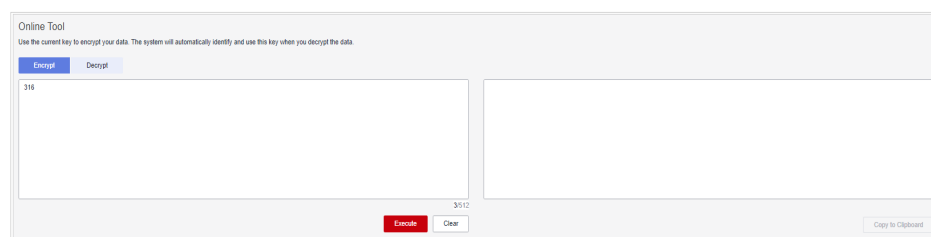
**Step 2** Click  in the upper left corner of the management console and select a region or project.

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

**Step 4** Click the alias of a custom key 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, as shown in [Figure 1-14](#).

**Figure 1-14** 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** > **Data Encryption Workshop**.

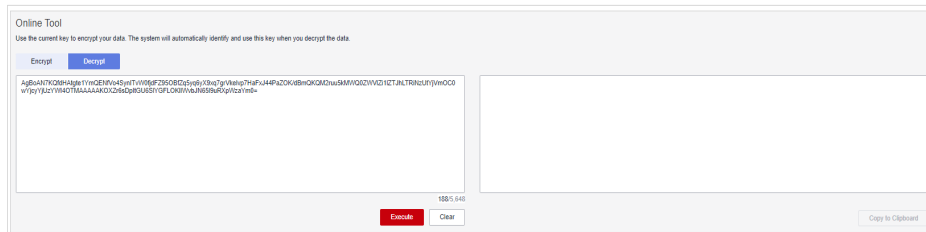
**Step 3** You can click any non-default key in **Enabled** status to go to the encryption and decryption page of the online tool.

**Step 4** Click **Decrypt**. In the text box on the left, enter the data to be decrypted. For details, see [Figure 1-15](#).

 **NOTE**

- The tool will identify the original encryption CMK and use it to decrypt the data.
- If the key has been deleted, the decryption will fail.

**Figure 1-15** 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.
- Enter the plaintext on the console, the text will be encoded to Base64 format before encryption.

The decryption result returned via API will be in Base64 format. Perform Base64 decoding to obtain the plaintext entered on the console.

----End

## 1.6 Managing Tags

### 1.6.1 Adding a Tag


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

#### Constraints

Tags cannot be added to default 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 > Data Encryption Workshop**.

**Step 4** Click the alias of the target custom key 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 1-16 Adding a tag

**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*.
- 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 custom keys. However, under the same custom key, one tag key can have only one tag value.</p> <p>A maximum of 20 tags can be added for one custom key.</p>	<ul style="list-style-type: none"> <li>• Mandatory.</li> <li>• The tag key must be unique for the same custom key.</li> <li>• 128 characters limit.</li> <li>• The value cannot start or end with a space.</li> <li>• Cannot start with <b>_sys_</b>.</li> <li>• The following character types are allowed: <ul style="list-style-type: none"> <li>- Chinese</li> <li>- English</li> <li>- Numbers</li> <li>- Space</li> <li>- Special characters: <code>._:/=+-@</code></li> </ul> </li> </ul>	cost

Parameter	Description	Value	Example Value
Tag value	Value of the tag	<ul style="list-style-type: none"> <li>• This parameter can be empty.</li> <li>• 255 characters limit.</li> <li>• The following character types are allowed:                             <ul style="list-style-type: none"> <li>- Chinese</li> <li>- English</li> <li>- Numbers</li> <li>- Space</li> <li>- Special characters: <code>._:/=+-@</code></li> </ul> </li> </ul>	100

**Step 7** Click **OK** to complete.


----End

## 1.6.2 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.

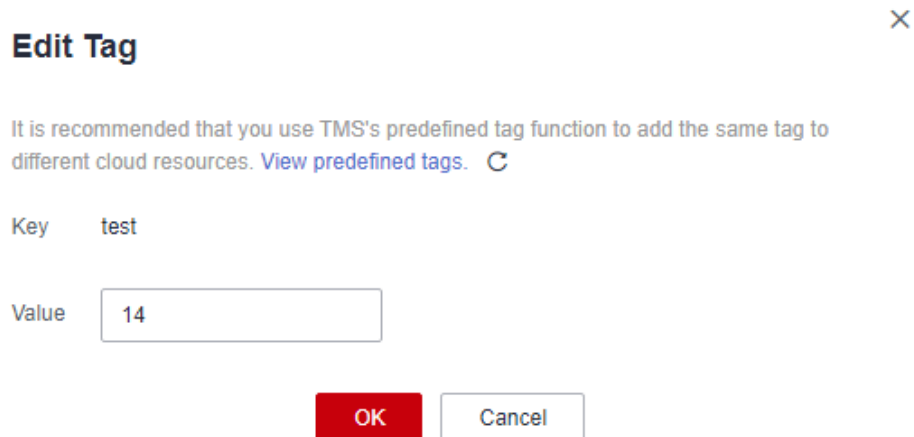
**Step 3** Click . Choose **Security > Data Encryption Workshop**.

**Step 4** Click the alias of the target custom key 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 1-17 Editing a tag



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


----End

### 1.6.3 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 > Data Encryption Workshop**.

**Step 4** Click the alias of the target custom key 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 **Confirm**.

----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.

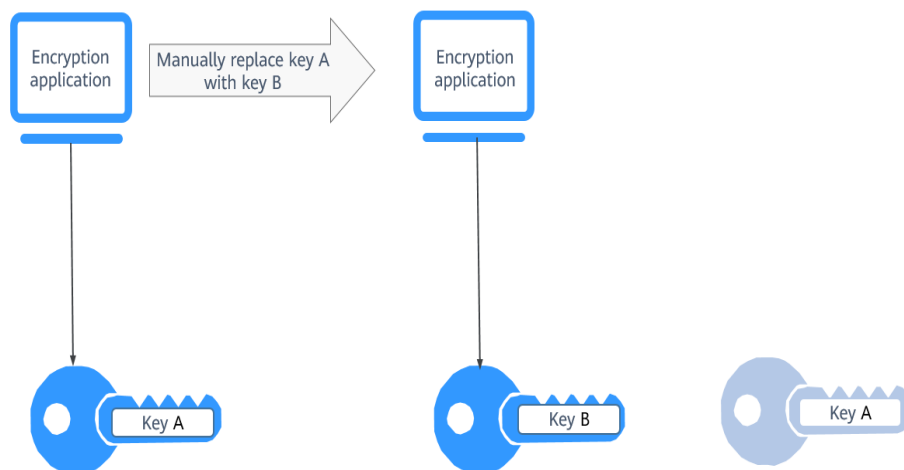
### Key Rotation Methods

You can use either of the following key rotation methods:

- Manual key rotation  
Method 1: Create a key B to replace the currently used key A.  
Method 2: Modify the key A and use it.

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

**Figure 1-18** Manual key rotation



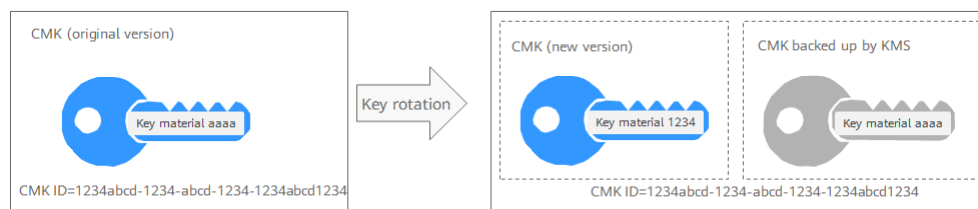
- Automatic key rotation
 

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 key will not change, including its key ID, alias, description, and permissions.

Automatic key rotation has the following characteristics:

  - a. Enable rotation for an existing custom key. KMS will automatically generate new key materials for the custom key.
  - b. 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 1-19** Key rotation



**NOTE**

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

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

## Rotation Modes

**Table 1-12** Key rotation modes

Key Type	Rotation Mode
Default key	Cannot be rotated.
Custom key	Keys can be rotated automatically or manually, depending on the key algorithm type. <ul style="list-style-type: none"> <li>• Symmetric key: Can be automatically or manually rotated.</li> <li>• Asymmetric key: Can only be manually rotated.</li> </ul>

Key Type	Rotation Mode
Disabled CMK	Disabled CMKs are not rotated. KMS keeps their rotation status unchanged. After a custom key is enabled, if it has been used for longer than the rotation period, KMS will immediately rotate keys. If the custom key has been used for shorter than the rotation period, KMS will implement the original rotation plan. For more information, see <a href="#">Disabling One or More CMKs</a> .
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 custom key 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 <a href="#">Scheduling the Deletion of One or More Keys</a> .

 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 key on the KMS console.

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

#### Prerequisites

- The key is enabled.
- The **Origin** of the key is **KMS**.
- Only symmetric keys can be rotated.


#### Constraints

- A disabled custom key is never rotated, even if rotation is enabled for it. KMS resumes rotation when this custom key is enabled. If you enable this custom key after one rotation period has passed, KMS will rotate it within 24 hours.

- Only CMKs can be rotated.

## Procedure

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

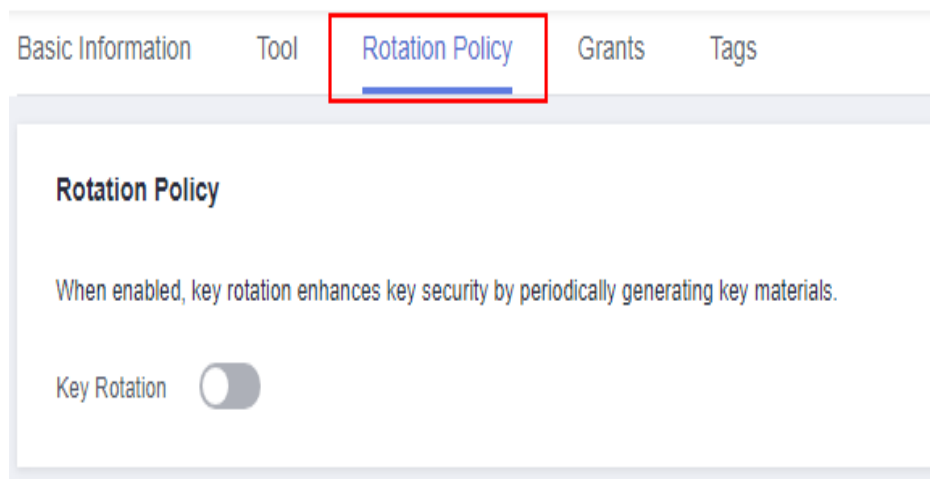
**Step 2** Click  in the upper left corner of the management console and select a region or project.


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

**Step 4** Click the alias of the target custom key to view its details.

**Step 5** Click the **Rotation Policy** tab. The rotation switch is displayed, as shown in [Figure 1-20](#).

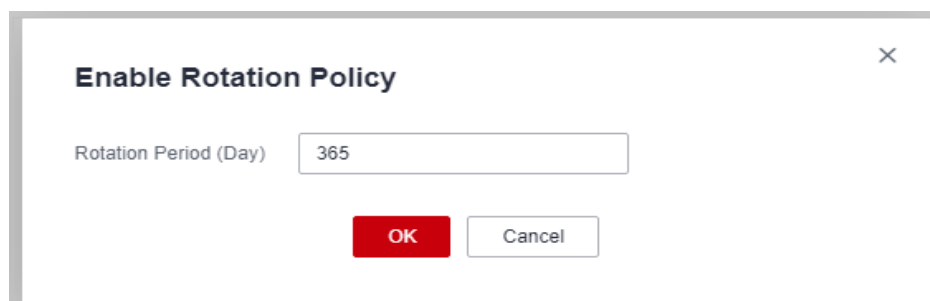
**Figure 1-20** Key rotation






**Step 6** Click  to enable key rotation.

**Step 7** Configure the rotation period and click **OK**, as shown in [Figure 1-21](#). For more information, see [Table 1-13](#).

**Figure 1-21** Enabling key rotation

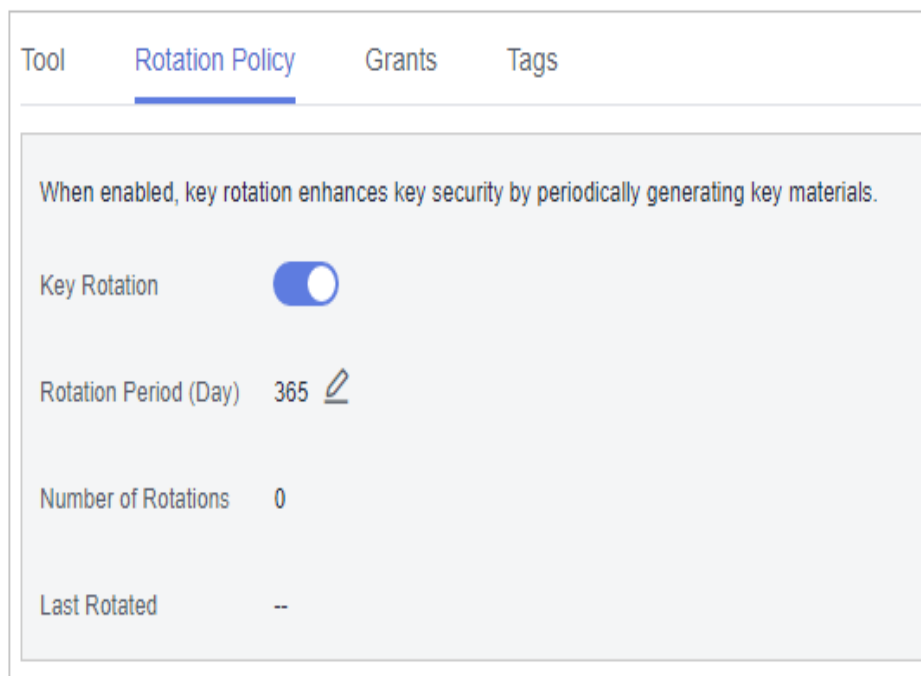


**Table 1-13** Key rotation parameters

Parameter	Description
Key rotation	<p>Rotation switch. The default status is .</p> <p> : disabled</p> <p> : enabled</p> <p>After rotation is enabled, the key will be rotated based on your set period.</p> <p><b>NOTE</b> A disabled custom key is never rotated, even if rotation is enabled for it.</p> <p>KMS resumes rotation when this custom key is enabled. If you enable this custom key after one rotation period has passed, KMS will rotate it within 24 hours.</p>
Rotation Period (day)	<p>Rotation period (day). The value is an integer ranging from 30 to 365. The default value is <b>365</b>.</p> <p>Configure the period based on how often a custom key is used. If it is frequently used, configure a short period. Otherwise, set a long one.</p>


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

**Figure 1-22** Key rotation details





 **NOTE**

You can click  to change the rotation period. After the period is changed, KMS rotates the key 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 key 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** > **Data Encryption Workshop**.

**Step 4** Click the alias of a symmetric key.

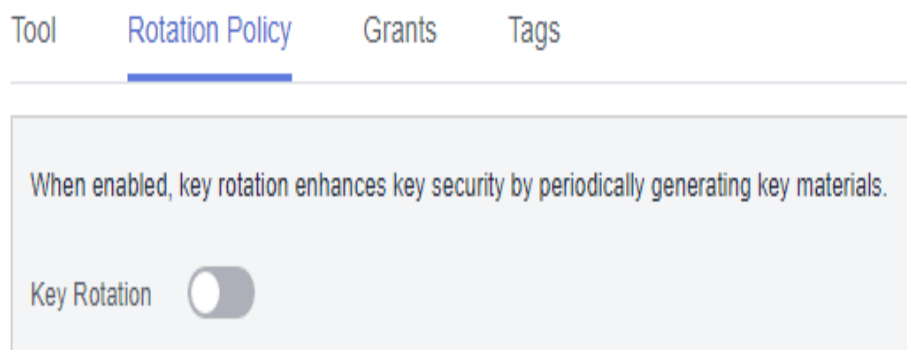
**Step 5** Click **Rotation Policy** and the dialog box is displayed.

**Step 6** Click  to disable key rotation.

**Step 7** In the displayed confirmation dialog box, click **OK**.

**Step 8** Check the rotation status, as shown in [Figure 1-23](#).

**Figure 1-23** 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 custom key. You can create a maximum of 100 grants on a custom key.

#### Prerequisites


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

#### Constraints

- The owner of a custom key can create a grant for the custom key 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 custom key can create grants for the custom key only by calling APIs.
- A maximum of 100 grants can be created for a custom 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 > Data Encryption Workshop**.

**Step 4** Click the alias of the target custom key to go to its details page and create a grant on it.

**Step 5** Click the **Grants** tab.

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

Figure 1-24 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 (?)

<input type="checkbox"/> Select all	<input type="checkbox"/> Describe Key
<input type="checkbox"/> Create Data Key Without Plaintext	<input type="checkbox"/> Create Grant
<input type="checkbox"/> Create Data Key	<input type="checkbox"/> Retire Grant
<input type="checkbox"/> Encrypt Data Key	<input type="checkbox"/> Encrypt Data
<input type="checkbox"/> Decrypt Data Key	
<input type="checkbox"/> Decrypt Data	

Figure 1-25 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 (?)

<input type="checkbox"/> Select all	<input type="checkbox"/> Describe Key
<input type="checkbox"/> Create Data Key Without Plaintext	<input type="checkbox"/> Create Grant
<input type="checkbox"/> Create Data Key	<input type="checkbox"/> Retire Grant
<input type="checkbox"/> Encrypt Data Key	<input type="checkbox"/> Encrypt Data
<input type="checkbox"/> Decrypt Data Key	
<input type="checkbox"/> 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 details, 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
User or Tenant	<p>Whether a user or an account is authorized.</p> <ul style="list-style-type: none"><li>• User User ID: Enter the IAM user ID. To obtain the ID, click the username in the upper right corner of the page, choose <b>My Credentials</b>. Choose <b>API Credentials</b> from the navigation pane, and copy the value of <b>IAM User ID</b>. After the authorization is complete, the IAM user can use the specified keys.</li><li>• Account Account ID: Enter the IAM user ID. To obtain the ID, click the username in the upper right corner of the page, choose <b>My Credentials</b>. Choose <b>API Credentials</b> from the navigation pane and copy the value of <b>Account ID</b>. After the authorization is complete, all IAM users under the account can use the specified keys.</li></ul>	d9a6b2bdaedd 4ba586cabe63 72d1b312
Grant Name	<p>You can name the grant.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>• You can enter digits, letters, underscores (_), hyphens (-), colons (:), and slashes (/).</li></ul>	test
Operations		-

**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 name, grant type, grantee ID, granted operation, and creation time of the grant.

----End



## 1.8.2 Querying a Grant

You can view the details about a custom key 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

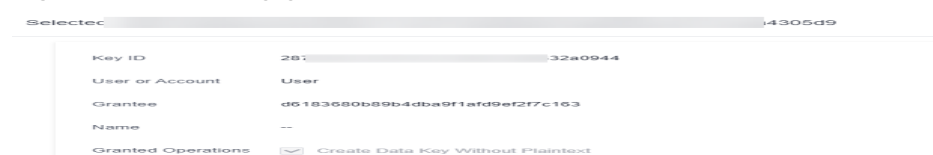
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security > Data Encryption Workshop**.
- Step 4** Click the alias of the target custom key to view its details.
- Step 5** Click **Grant** to view the created grant of the current custom key. [Table 1-15](#) describes the parameters.

**Table 1-15** Parameter description

Parameter	Description
Grant Name	Name of the grant when created
Granted To	Whether permissions are granted to a user or account.
Granted Operations	Authorized operations (such as <b>Create Data Key</b> ) on the custom key
Created	Time when the grant is created
Operation	You can revoke a grant in the Operation column.

- Step 6** Click the target grant, the grant details are displayed on the right, as shown in [Figure 1-26](#).

**Figure 1-26** Viewing 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 custom key 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 > Data Encryption Workshop**.
- Step 4** Click the alias of the target custom key to view its details.
- Step 5** In the row of a grantee, click **Revoke Grant**.
- Step 6** In the displayed dialog box, click **OK**. If **Grant *grant ID* revoked successfully** is displayed in the upper right corner, the grant has been revoked.

### NOTE

You can call the API to verify that the key grant has been revoked. For details about how to use APIs, see *Key Management Service API Reference*.

For example, if the grant to create a data key is revoked for a user, an error will be reported when the user calls the API to create a data key.

----End

# 2 Cloud Secret Management Service

---

## 2.1 Creating a Shared 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 secrets.
- By default, the default key **csms/default** created by CSMS is used as the encryption key of the current secret. You can also create a user-defined symmetric 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 > Data Encryption Workshop**.

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

**Step 5** Click **Create Secret**. Configure parameters in the **Create Secret** dialog box, as shown in [Figure 2-1](#). For details, see [Table 2-1](#).

**Figure 2-1** Creating a secret

**Table 2-1** Secret parameters

Parameter	Description
Type	Secret type. The default value is <b>Shared secret</b> .
Secret Name	Secret name <b>NOTE</b> Only letters, digits, hyphens (-), and underscores (_) are supported.



Parameter	Description
Enterprise Project	This parameter is provided 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 <b>default</b> . <b>NOTE</b> If you have not enabled enterprise management, this parameter will not be displayed.
Secret Value	Secret key/value pair and the plaintext secret to be encrypted
Description (optional)	Description of a secret
KMS Encryption Key	Select the default key <b>csms/default</b> or a custom key created on KMS. <b>NOTE</b> <ul style="list-style-type: none"><li>CSMS encrypts private keys using the encryption key provided by KMS. When you use the KMS encryption function of the key pair, KMS creates a default key <b>csms/default</b> for you to use.</li><li>For details about the custom keys created on KMS, see <a href="#">Creating a Key</a>.</li><li>After a grant is created, you can switch to the manual input mode, and enter the key ID to use the granted key for encryption. For details, see .</li></ul>
Associated Event	When creating a secret, you can associate it with a secret event. You can add, delete, modify, and query secret versions on the event notification page.

**Step 6** Click **Next** and set the rotation period.

**Step 7** Click **Next** and confirm the creation information.

**Step 8** Click **OK**.

In the secret list, you can view the 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 secret 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 > 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 2-2.](#)

**Figure 2-2** Secret list

Secret Name/ID	Status	Type	Associated Event	Created	Enterprise Project	Operation
ad0c777db... 12224...	Enabled	Shared secret	--	Dec 27, 2022 01:59:10 GMT+08:00	default	<a href="#">Download Backup</a>   <a href="#">Delete</a>
ad0c738b0f5... 1afa...	Enabled	Shared secret	--	Jun 20, 2023 14:40:31 GMT+08:00	default	<a href="#">Download Backup</a>   <a href="#">Delete</a>

**Table 2-2** Secret list parameters

Parameter	Description
Secret Name/ID	Secret name
Status	Status of a secret. The value can be <b>Enabled</b> or <b>Pending deletion.</b>
Type	Secret type. The value can be <b>Shared secret.</b>
Created	Time when the secret is created
Enterprise Project	Enterprise project that the secret is to be bound to
Operation	You can manage secrets by performing operations in the <b>Operation</b> column, for example, download secret backup and delete a secret.

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

**Figure 2-3** Secret details

Secret Details	
Basic Information	
Name	ad0c777db... 12224...
Type	Shared secret
Created	Oct 27, 2023 16:06:50 GMT+08:00
Updated	Nov 20, 2023 14:25:16 GMT+08:00
Enterprise Project	default
Secret ID	50bb760a-0458-4f9c-8a9a-1155b1f6770a
Status	Enabled
Encryption Key	6452d410-dbb7-4700-9c10-9ff1d470e132
Description	--
Associated Event	--

 **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 secret to be deleted, see [Are Credentials Scheduled to Be Deleted Billed?](#)
- If you delete a secret immediately, you can restore it using the secret backup that you have downloaded in advance. Exercise caution when performing this operation.

### Deleting 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.

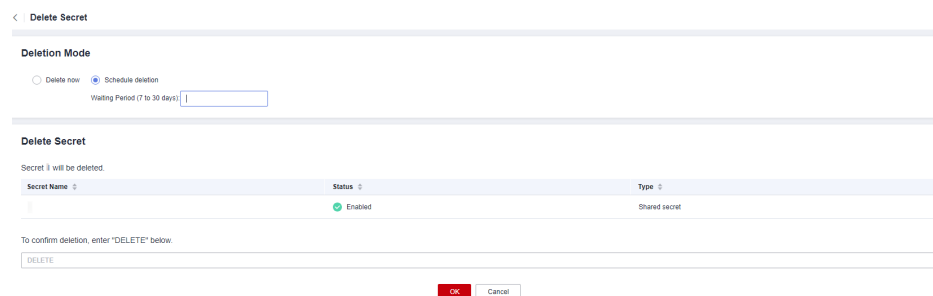
**Step 3** Click . Choose **Security > Data Encryption Workshop**.

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

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

**Step 6** On the displayed page, select a deletion mode. If you want to delete the secret in a specific time, set **Schedule deletion**.

**Figure 2-4** Setting schedule deletion



**Step 7** Enter **DELETE** in the confirmation dialog box and 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 secret to be deleted, see [Are Credentials Scheduled to Be Deleted Billed?](#)
- If you delete a secret immediately, you can restore it using the secret backup that you have downloaded in advance. Exercise caution when performing this operation.

----End

## 2.3 Managing Secret Versions

### 2.3.1 Saving and Viewing Secret Values

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 > 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 , click **Add Secret Version**, as shown in [Figure 2-5](#). Configure **Secret key/value** or **Plaintext**.

**Figure 2-5** Adding a secret value

- Step 7** You can select an expiration time for the stored secret value. The time can be specific to seconds. After the setting is complete, you can view the expiration time in the secret version list. For example, Jun 30, 2023 19:52:59.
- Step 8** Click **OK**. A message is displayed in the upper right corner of the page, indicating that the value is added successfully.
- Step 9** In the **Version List** area, locate the target secret version, click **View Secret** in the **Operation** column, as shown in [Figure 2-6](#).

**Figure 2-6** Secret version list

Version	KMS Encryption Key ID	Version Status	Created	csms_list_tr_expire_time	Operation
v1	81...	SYSCURRENT	Apr 24, 2023 16:32:18 GMT+08:00	-	Manage Status View Secret Configure Expiration

- 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.

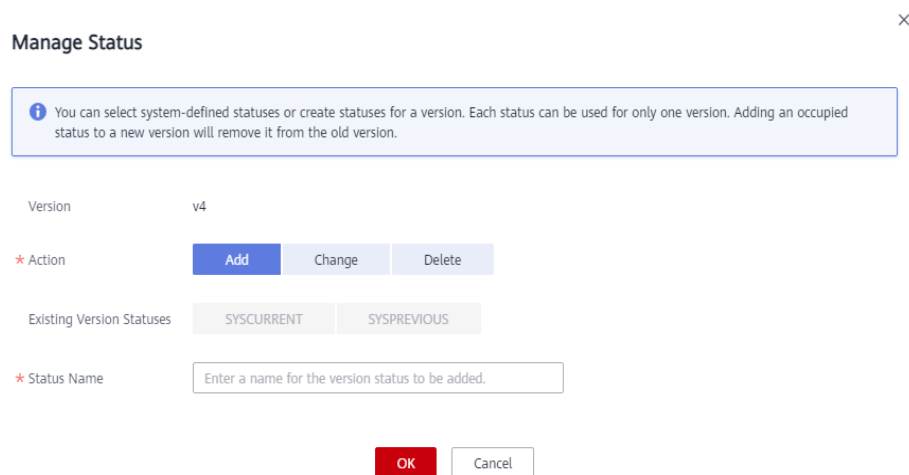
### Constraints

- The initial version is marked by the **SYSCURRENT** status tag.
- You can mark a version with a tag created in the service or a custom tag. 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** > **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.
- Step 7** In the **Manage Status** dialog box, add, change, or delete the status of a secret version.

**Figure 2-7** 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

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

- Deleting the version status

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

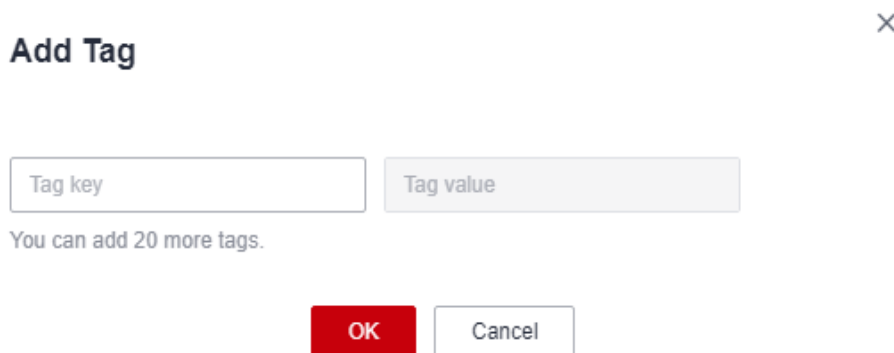
### 2.4.1 Adding a Tag

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 > 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**, as shown in [Figure 2-8](#). In the **Add Tag** dialog box, enter the tag key and tag value. [Table 2-3](#) describes the parameters.

**Figure 2-8** Adding a tag



**Add Tag** ×

Tag key  Tag value

You can add 20 more tags.

**OK** Cancel

#### 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 2-3** 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 20 tags.	<ul style="list-style-type: none"><li>• Mandatory.</li><li>• The tag key must be unique for the same custom key.</li><li>• 128 characters limit.</li><li>• The value cannot start or end with a space.</li><li>• Cannot start with <b>_sys_</b>.</li><li>• The following character types are allowed:<ul style="list-style-type: none"><li>- Chinese</li><li>- English</li><li>- Numbers</li><li>- Space</li><li>- Special characters: <code>_:/=+-@</code></li></ul></li></ul>
Tag value	Value of the tag	<ul style="list-style-type: none"><li>• Optional</li><li>• 255 characters limit.</li><li>• The following character types are allowed:<ul style="list-style-type: none"><li>- Chinese</li><li>- English</li><li>- Numbers</li><li>- Space</li><li>- Special characters: <code>_:/=+-@</code></li></ul></li></ul>

**Step 7** Click **OK**.


----End

## 2.4.2 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 > 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**.
- Step 7** In the **Edit Tag** dialog box, enter a tag value and click **OK**.
- End

### 2.4.3 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 > 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**.
- Step 7** In the **Delete Tag** dialog box, click **Confirm**.
- End

# 3 Key Pair Service

---

## 3.1 Creating a Key Pair

For system security reasons, you should 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/>.

## Prerequisites


When creating an account key pair for the first time, you need to obtain a user with the Tenant Administrator system role.

## Constraints

- IAM users cannot create account key pairs.

## Creating a Key Pair Using the Management Console

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

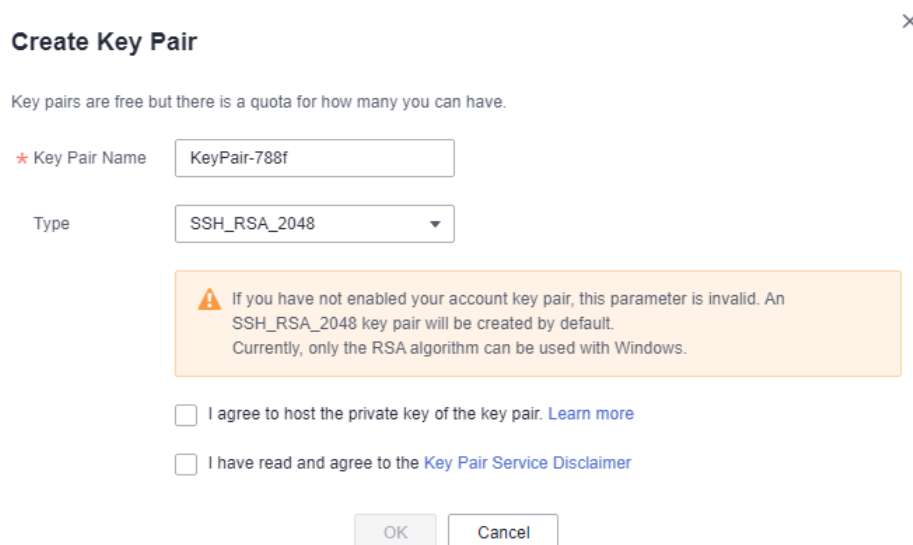
**Step 2** Click  in the upper left corner of the management console and select a region or project.

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

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

**Step 5** Click **Create Key Pair**. In the displayed dialog box, enter the key pair name, as shown in [Figure 3-1](#).

**Figure 3-1** Creating a key pair



**Step 6** (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

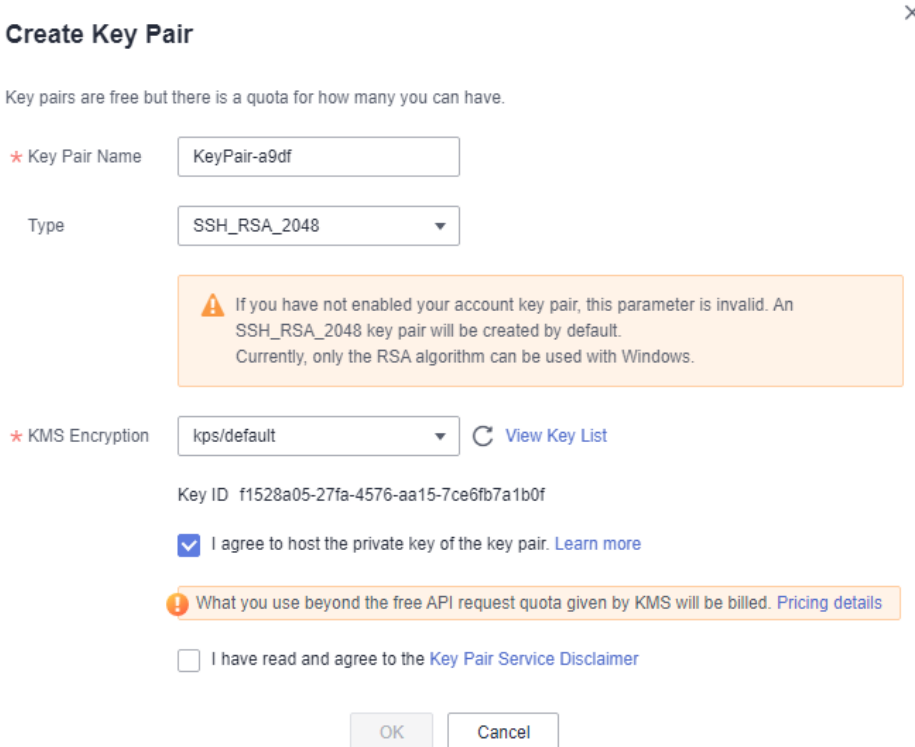
Currently, only the RSA algorithm can be used with Windows.

**Step 7** Read and select **I agree to host the private key of the key pair**, if needed. Select an encryption key from the **KMS encryption** drop-down list box. Skip this step if not needed.

 **NOTE**

- KPS encrypts private keys using the encryption key provided by KMS. When you use the KMS encryption function of the key pair, KMS creates a default key **kps/default** for you to use.
- For details about the custom keys created on KMS, see [Creating a Key](#).

**Figure 3-2** Managing private keys




**Create Key Pair** ×

Key pairs are free but there is a quota for how many you can have.

\* Key Pair Name


Type

 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  [View Key List](#)

Key ID f1528a05-27fa-4576-aa15-7ce6fb7a1b0f

I agree to host the private key of the key pair. [Learn more](#)

 What you use beyond the free API request quota given by KMS will be billed. [Pricing details](#)

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

**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**. The browser automatically downloads the private key. When the private key is downloaded, a dialog box is displayed.

**Step 10** 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 11** Click **OK**. After the key pair is created, you can view the information in the key pair list, including name, fingerprint, status, and private key.

**NOTE**

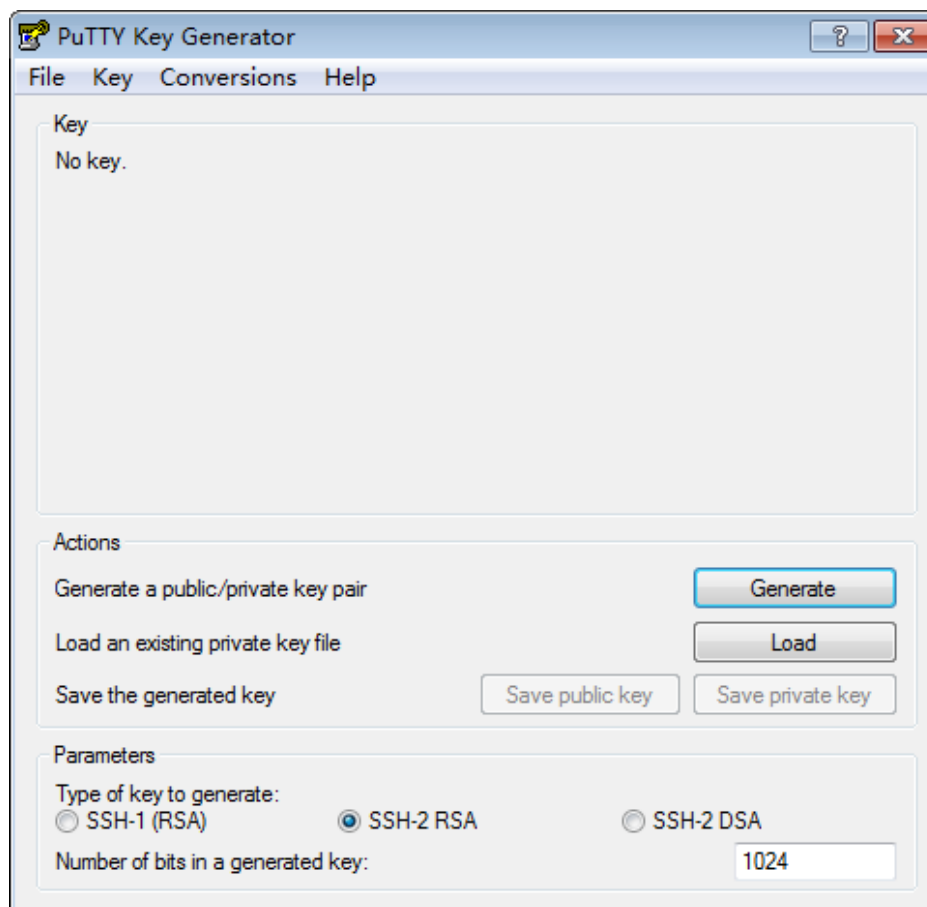
After the key pair is created, download the private key to your local host and keep it securely.

----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**.

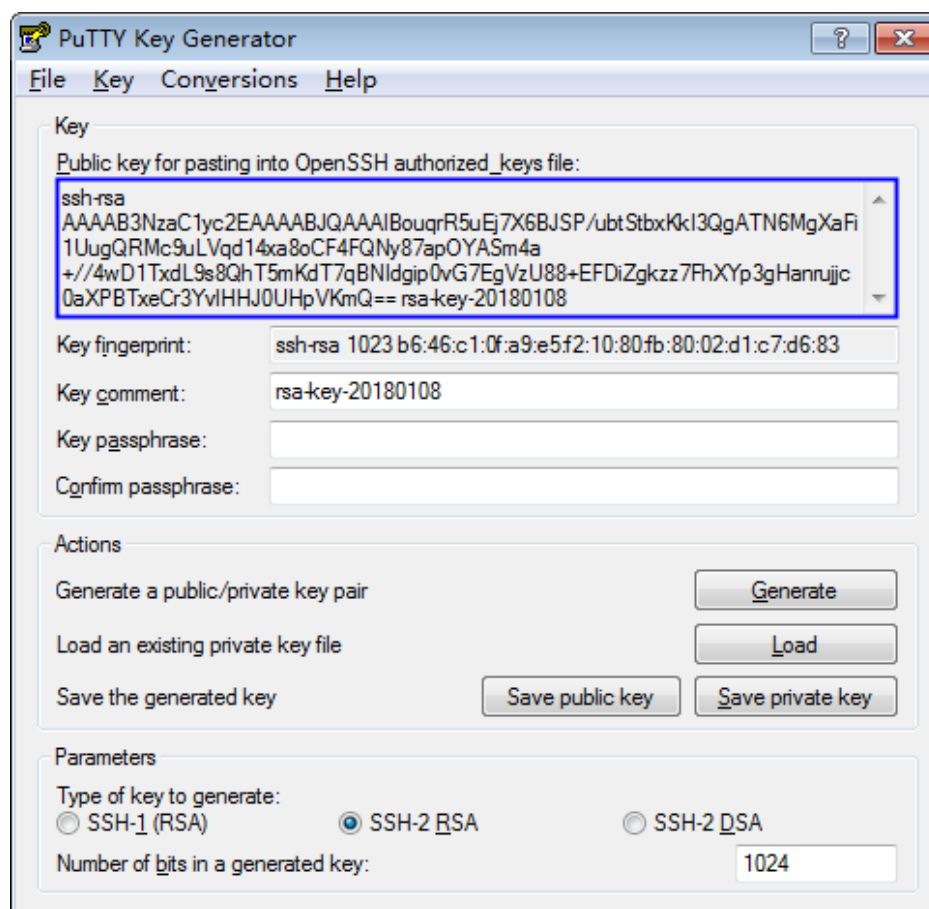
**Table 3-1** Parameter description

Parameter	Description
Type of key to generate	Encryption and decryption algorithm of key pairs to be imported to the management console. Currently, only <b>SSH-2 RSA</b> is supported.

Parameter	Description
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: <b>1024</b> , <b>2048</b> , and <b>4096</b> .

**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**. If you save a public key using **Save public key**, the public key format will be changed and cannot be imported to the management console directly.

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

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.
- The imported key pair is an account key pair. If a private key pair with the same name has been created, a message will be displayed, indicating that the name already exists.
- Each IAM user does not have a private key pair with the same name.
- PKCS8 is supported for imported private keys. Convert the format if PKCS1 is used.

## 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 length can be 2048, 3072, and 4096 bits.
- 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?](#)
- If the imported private key is encrypted, the upload will fail.

## 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 > Data Encryption Workshop**.

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

**Step 5** Click **Import Key Pair**. In the displayed dialog box, click **Select File** and import a public key file, or paste the public keys in the **Public Key Content** text box, as shown in [Figure 3-5](#).



**Figure 3-5** Importing a key pair

×

### Import Key Pair

Key pairs are free but there is a quota for how many you can have.

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

I agree to host the private key of the key pair. [Learn more](#)

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

 **NOTE**

- You can customize the name of an imported key pair.
- If a message is displayed, indicating that the name already exists, change the key pair name.

**Step 6** Read and select **I agree to host the private key of the key pair.** if needed, as shown in [Figure 3-6](#). Skip this step if not needed.

**Figure 3-6** Managing private keys

✕

### Import Key Pair

Key pairs are free but there is a quota for how many you can have.

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 614a94b5-c077-4551-8bd6-85c24b2645d8

I agree to host the private key of the key pair. [Learn more](#)

! What you use beyond the free API request quota given by KMS will be billed. [Pricing details](#)

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 encrypts private keys using the encryption key provided by KMS. When you use the KMS encryption function of the key pair, KMS creates a default key **kps/default** for you to use.
- For details about the custom keys created on KMS, see [Creating a Key](#).

**Step 7** Read the *Key Pair Service Disclaimer* and select **I have read and agree to the Key Pair Service Disclaimer**.

**Step 8** 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.
- Users with the Tenant Administrator system role must perform the upgrade at least once. The number of key pairs to be upgraded is not limited.
- The service ticket for key upgrade has been handled.

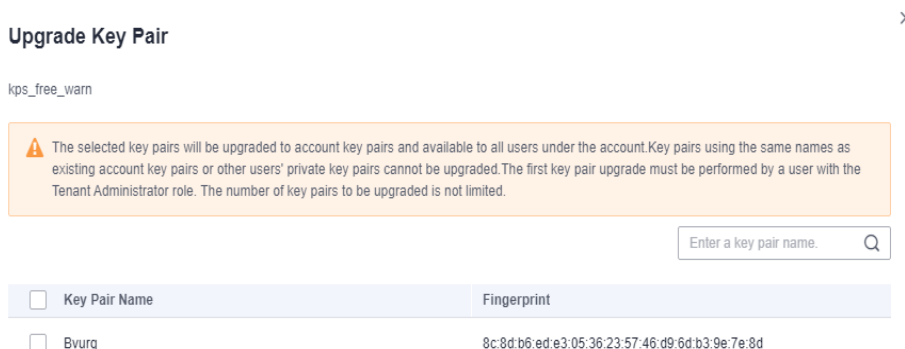
### Constraints

- Key pairs using the same names as existing account key pairs or other users' private key pairs cannot be upgraded.
- If a private key pair is upgraded to an account key pair, the account key pair quota is not occupied.
- Once a private key pair is upgraded to an account key pair, it cannot be changed back.

### 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** > **Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, click **Key Pair Service**.
- Step 5** Click the **Private Key Pairs** tab and then click **Upgrade Key Pair**.
- Step 6** In the displayed dialog box, 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 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 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 > Data Encryption Workshop**.

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

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

 NOTE

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

----End

## 3.5 Using Key Pairs

### 3.5.1 Binding a Key Pair

If you set the login mode to **Password** when purchasing an ECS running Linux, and you need to change the login mode to **Key Pair**, you can bind the key pair to the ECS on the KPS console, KPS will configure the 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.
- The SSH port (**22** by default) of the ECS security group must allow traffic from the **100.125.0.0/16** CIDR block in advance.

## 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 > Data Encryption Workshop**.

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

**Step 5** Click **ECS List** to view ECSs.

**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 3-8](#).

Figure 3-8 Binding a key pair (1)

×

### Bind Key Pair

**i** The key pair bound to the server can be used for login. For security purposes, you are advised to disable password login for this server. An ECS will be temporarily created and then deleted to complete this operation. In most cases this only costs cents.7

ECS Name

IP Address 17  6

Status Shut down

\* New Key Pair

Disable the password login mode. [Learn more](#)

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

- If the ECS is running, you need to provide the root password, as shown in [Figure 3-9](#).

Figure 3-9 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 c  2

IP Address 1  2

Status Running

\* New Key Pair

\* Root Password

\* Port  ?

Disable the password login mode. [Learn more](#)

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

 **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 **Shut down** state.

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

**Step 8** The default port number is 22 and can be modified.

 **NOTE**

**Step 9** 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 10** Read and select **I have read and agree to the Key Pair Service Disclaimer**.

**Step 11** 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

## 3.5.2 Binding Key Pairs in Batches

When ECS is in the **Running** state, you can bind key pairs in batches on the console.

This section describes how to bind key pairs in batches on the KMS console.

### Application Scenario

- If multiple ECSs to be bound have the same password, you can enter the password and select the key pair with just a few clicks.
- If the passwords of the ECSs to be bound are different, you can enter their passwords and select the same key pair for binding.

### Prerequisites

- The ECS must be in the **Running** state.
- The ECS has not been bound to a key pair.


### 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.
- You can bind key pairs to a maximum of 10 ECSs at a 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 > Data Encryption Workshop.**

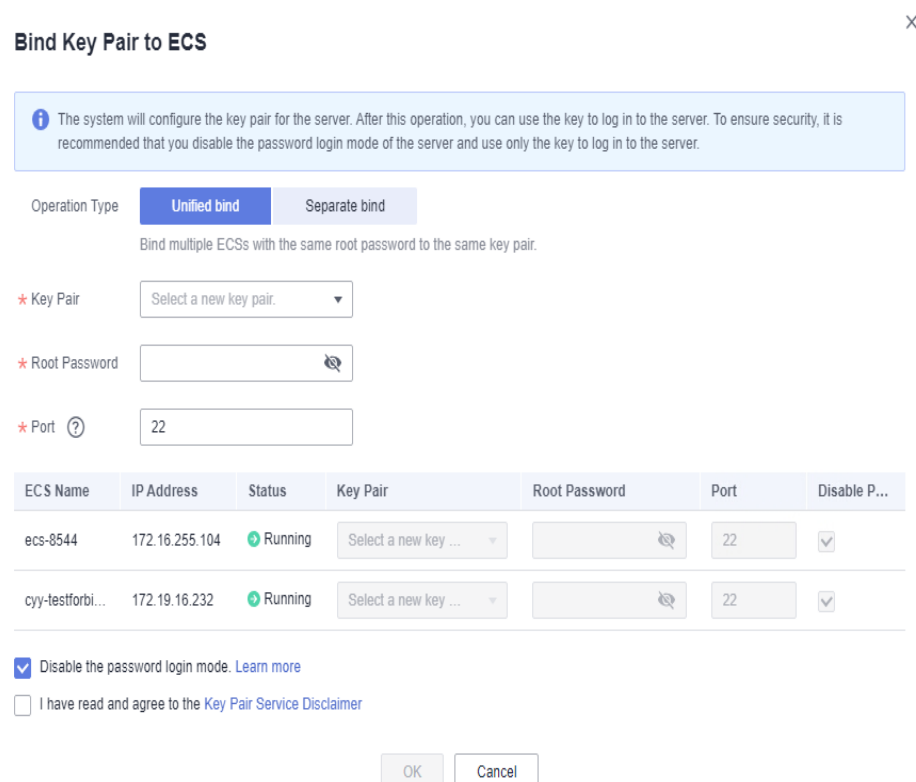
**Step 4** In the navigation pane on the left, click **Key Pair Service.**

**Step 5** Click **ECS List** to view ECSs.

**Step 6** Select the servers to be bound in batches and click **Bind** above the search box.

- If the passwords of the ECSs to be bound are the same, you can select a key pair by one click and enter the password to bind the key pair. For details, see [Figure 3-10.](#)

**Figure 3-10** Unified bind



**Bind Key Pair to ECS** ×

**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.

Operation Type: **Unified bind** | Separate bind

Bind multiple ECSs with the same root password to the same key pair.

\* Key Pair: Select a new key pair. ▾

\* Root Password:

\* Port <sup>?</sup>: 22

ECS Name	IP Address	Status	Key Pair	Root Password	Port	Disable P...
ecs-8544	172.16.255.104	Running	Select a new key ... ▾	<input type="password"/>	22	<input checked="" type="checkbox"/>
cyy-testforbi...	172.19.16.232	Running	Select a new key ... ▾	<input type="password"/>	22	<input checked="" type="checkbox"/>

Disable the password login mode. [Learn more](#)

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

OK Cancel

- If the passwords of the ECSs to be bound are different, you can bind them separately. For details, see [Figure 3-11.](#)



**Figure 3-11** Separate bind

**Bind Key Pair to ECS**

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.

Operation Type:  Unified bind  **Separate bind**

Bind ECSs with different root passwords to the same key pair.

\* Key Pair: KeyPair-4083

ECS Name	IP Address	Status	Key Pair	Root Password	Port	Disable P...
	192.168.1.26	Running	KeyPair-4083		22	<input checked="" type="checkbox"/>
	192.168.1.36	Running	KeyPair-4083		22	<input checked="" type="checkbox"/>

Disable the password login mode. [Learn more](#)

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

OK Cancel

**NOTE**

If you select **Unified bind**, only the same key pair can be used for binding.

**Step 7** The default port number is 22 and can be modified.

**NOTE**

**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**. The key pairs are bound in batches. The binding takes about 3 to 5 minutes.



----End

### 3.5.3 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](#).

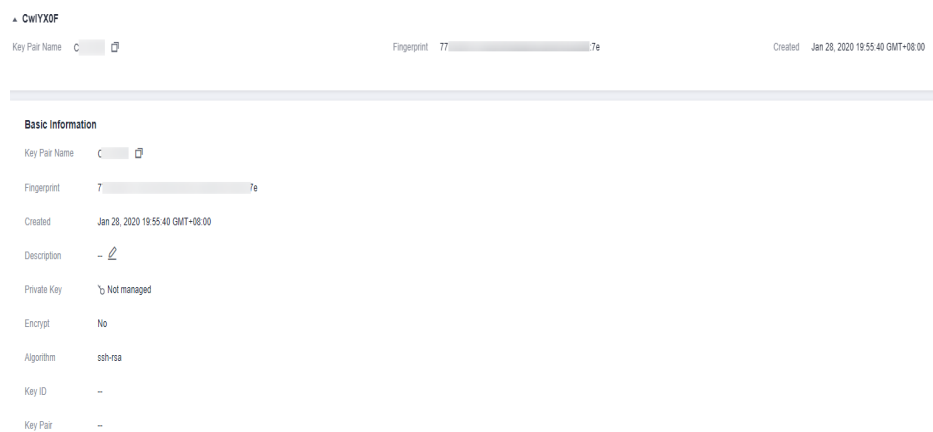
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click . Choose **Security > Data Encryption Workshop**.
- Step 4** In the navigation pane on the left, click **Key Pair Service**.
- Step 5** Click the **Private Key Pairs** tab and view information about the key pair in the key pair list.

 **NOTE**

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

- Step 6** 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, as shown in [Figure 3-12](#).

**Figure 3-12** Key pair details



 **NOTE**

When you purchase an ECS and set login mode to **Key Pair**, the selected key pair is bound to the ECS.

[Table 3-3](#) lists the parameters of the ECS to which the key pair is bound.

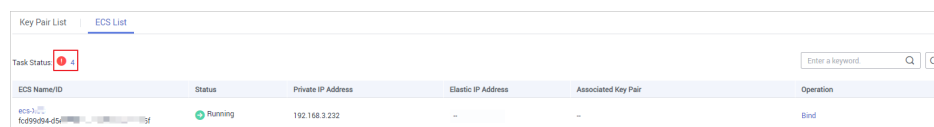
**Table 3-3** ECS parameters


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

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

**Step 7** Click **ECS List** to view ECSs.

**Figure 3-13** ECS list



**Step 8** Click the number next to the task status icon  to view failed tasks, as shown in [Figure 3-14](#).

 **NOTE**

Status of resetting or replacing the key pair:

 : Executing

 : Execution failed

**Figure 3-14** 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

### 3.5.4 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 > 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** Locate the target ECS and click **Reset**. The key pair reset dialog box is displayed, as shown in **Figure 3-15**.

**Figure 3-15** Resetting a key pair

**Are you sure you want to reset the key pair of the following server?**

The key pair bound to the ECS can be used for login. For security purposes, you are advised to disable password login for this ECS. An ECS will be temporarily created and then deleted to complete this operation. In most cases this generates less than ¥0.1 in incidental charges.

ECS Name: ir-...-219

IP Address: 192...:4

Status: Shut down

Key Pair: 2

\* New Key Pair:

\* Port :

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

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

**Step 8** The default port number is 22 and can be modified.

**NOTE**

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

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

----End

## 3.5.5 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** > **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** Locate the target ECS and click **Replace**, the key pair replacement dialog box is displayed, as shown in [Figure 3-16](#).

**Figure 3-16** Replacing a key pair

**Are you sure you want to replace the key pair of the following server?** ×

The system will use the new key pair for the server. After this operation is executed, the existing key pair cannot be used to log in to the server.

ECS Name	image- <span style="background-color: #ccc;">                    </span> 19
IP Address	1 <span style="background-color: #ccc;">          </span> 4
Status	<span style="color: green;">➔</span> Running
Key Pair	2
* New Key Pair	<input type="text" value="Select a new key pair."/> ▾
* Private Key in Use <span>?</span>	No file is selected. <input type="button" value="Select File"/>
	<input type="text" value="Paste the private key file content here."/>
* Port <span>?</span>	<input type="text" value="22"/>

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

**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** The default port number is 22 and can be modified.

 **NOTE**

**Step 10** Read and select **I have read and agree to the Key Pair Service Disclaimer**.

**Step 11** Click **OK**. The key pair will be replaced in about one minute.

----End

## 3.5.6 Unbinding a Key Pair

When you use a key pair to log in to an ECS, and you need to change the login mode to **Password**, unbind the key pair on the KPS management console. 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 whose key pair is to be unbound 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 a password for logging in to the ECS, or you have forgotten your password, reset the login password on the ECS management console. For details, see *Elastic Cloud Server User Guide*.
- If you set login mode to **Key Pair** when you create the ECS, after the key pair is unbound, shut down the ECS first to bind a key pair again.
- To log in to the ECS, after you unbind the key pair, reset the password in time on the ECS console. For details, see *Elastic Search 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** > **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** Locate the target ECS and click **Unbind**.

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


**Figure 3-17** Unbinding a key pair (1)

**Are you sure you want to unbind the key pair from the following ECS?** ×

The system will unbind the key pair from the ECS. After this operation, you can only use the original password to log in. If you forget the password or have not set a password, you can reset the password on the ECS page. An ECS will be temporarily created and then deleted to complete this operation. In most cases this generates less than ¥0.1 in incidental charges.

ECS Name

IP Address 1

Status  Shut down

Key Pair

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

- If the ECS is running, a dialog box will be displayed, as shown in [Figure 3-18](#).


**Figure 3-18** Unbinding a key pair (2)

**Are you sure you want to unbind the key pair from the following ECS?** ×

The system will unbind the key pair from the ECS. After this operation, you can only use the original password to log in. If you forget the password or have not set a password, you can reset the password on the ECS page.

ECS Name image  9

IP Address  4

Status  Running

Key Pair 2

\* Private Key in Use (?) No file is selected.

Paste the private key file content here.

\* Port (?)

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

**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** The default port number is 22 and can be modified.

 NOTE

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

**Step 10** Click **OK**. The key pair will be unbound from the ECS in about one minute.

 NOTE

To log in to the ECS, after you unbind the key pair, reset the password in time on the ECS console. For details, see *Elastic Search Server User Guide*.

----End

## 3.6 Managing Private Keys

### 3.6.1 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

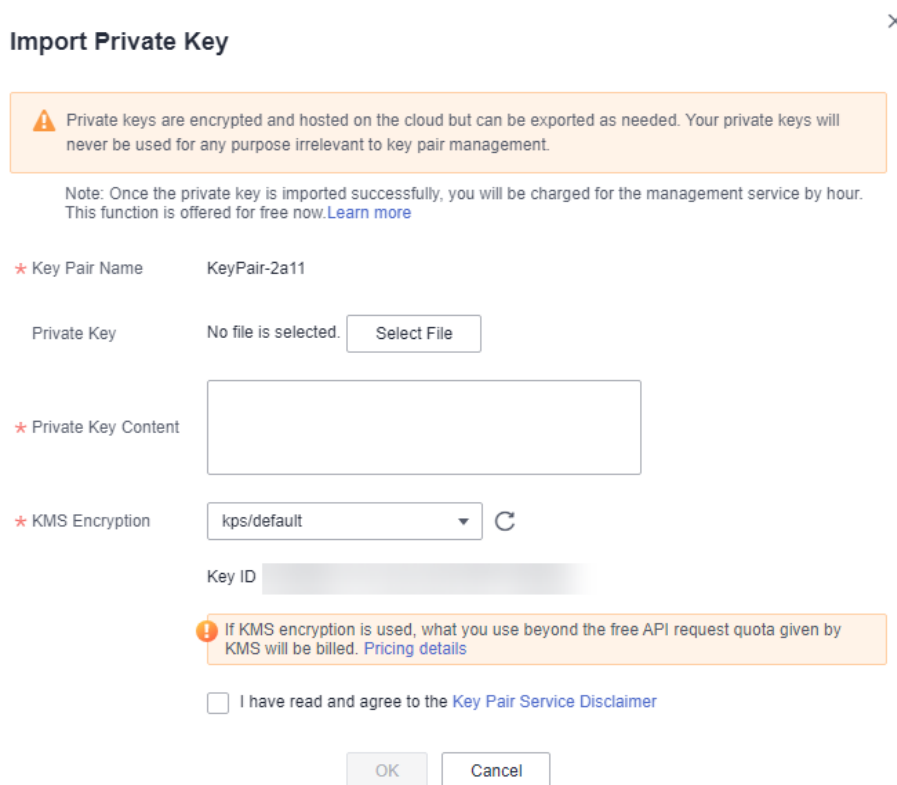
- Only the private key that matches a public key can be imported for the public key.
- The private key to be uploaded or copied to the text box must be in the .pem format. If it is in the .ppk format, convert it by referring to [How Do I Convert the Format of a Private Key File?](#).
- When you enable the encryption function for a key pair, KMS automatically creates a default 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 > 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, as shown in [Figure 3-19](#).

**Figure 3-19** Importing a private key



- 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 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 **.pk** format, convert it by referring to [How Do I Convert the Format of a Private Key File?](#)

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

 **NOTE**

- When you enable the encryption function for a key pair, KMS automatically creates a default 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** Read and select **I have read and agree to the Key Pair Service Disclaimer**.

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

----End

## 3.6.2 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](#).

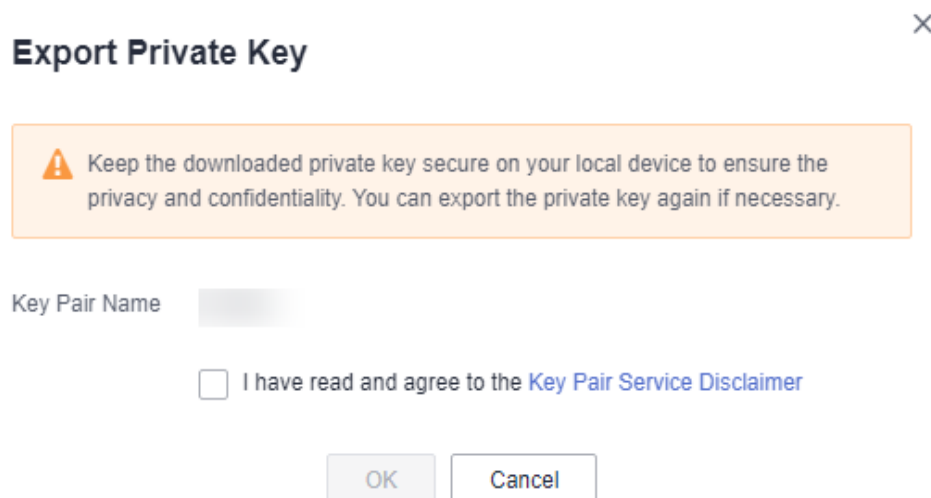
**Step 2** Click  in the upper left corner of the management console and select a region or project.

**Step 3** Click . Choose **Security > 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 3-20](#).

**Figure 3-20** Exporting a private key



**Step 6** Read and 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

### 3.6.3 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 > Data Encryption Workshop**.

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

**Step 5** Locate the target key pair, choose **More > Clear Private Key** in the **Operation** column.

 **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

## 3.7 Using a Private Key to Log In to the Linux ECS

After you create or import a key pair on the KMS console, set login mode to **Key Pair** 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 private key files of the ECS must meet the requirements list in the following table.

**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**.

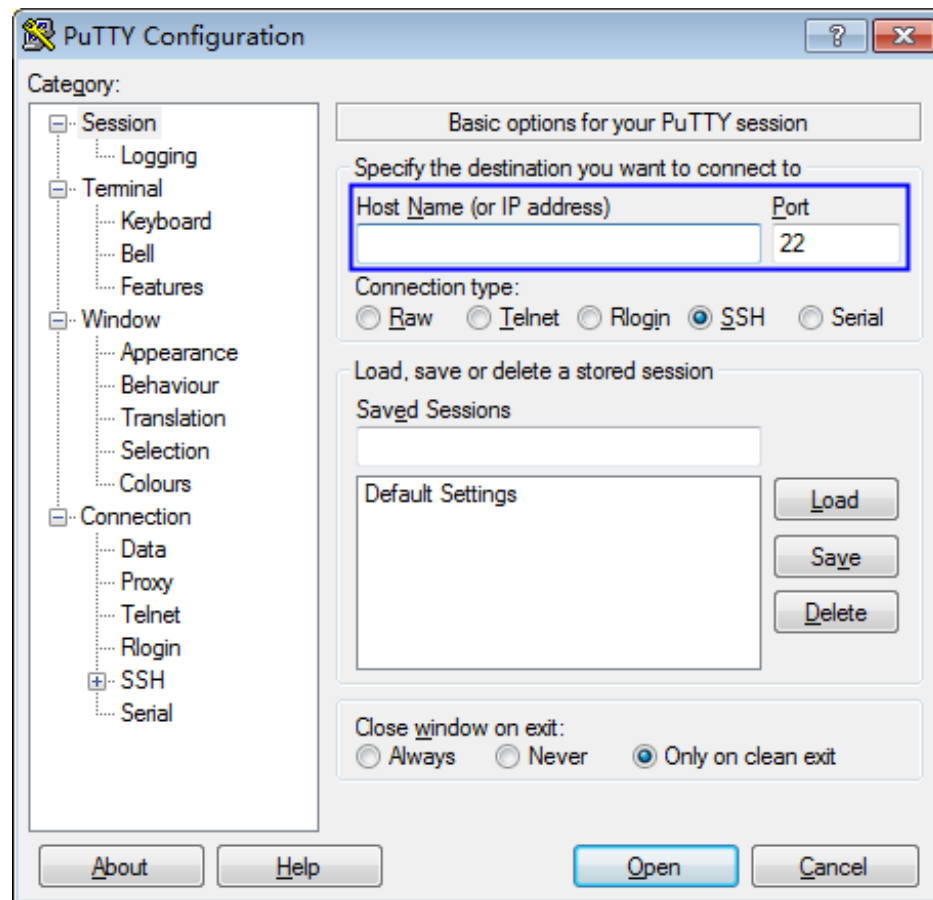
#### NOTE

- 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 3-21** 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 in this section. 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

## 3.8 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, obtain the administrator password generated during the initial installation of the ECS from the private key file downloaded when you create the ECS. The administrator password is the password of account **Administrator** or an account set in Cloudbase-init. 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, record the password information. For details, see the *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 . Under **Computing**, click **Elastic Cloud Server**.

**Step 4** In the ECS, click the ECS whose password is to be obtained.

**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

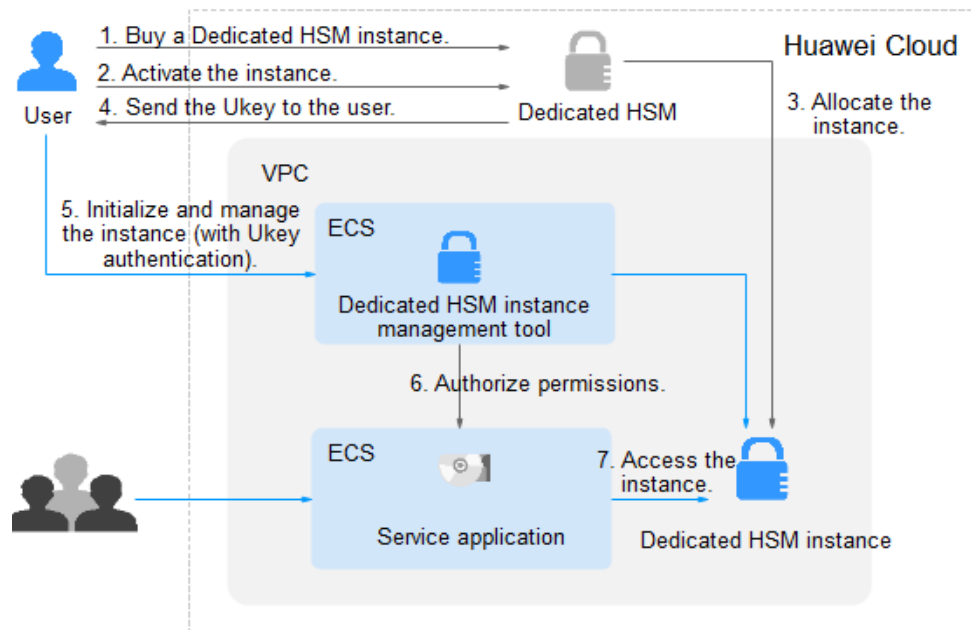
### Restrictions

- Dedicated HSM instances must be used together with VPC. After a Dedicated HSM instance is created, you need to configure its VPC, security group, and NIC on the management console before using it.
- To manage Dedicated HSM instances, you need to deploy the Dedicated HSM management tool in the same VPC as the instances.

### Operation Guide

To use Dedicated HSM on the cloud, you can create Dedicated HSM instances through the management console. After a Dedicated HSM instance is created, 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 <a href="#">Activating a Dedicated HSM Instance</a> .	User
3	Allocate a Dedicated HSM instance.	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	Obtain the UKey, initialization documents, and software.	<ul style="list-style-type: none"> <li>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.</li> <li>A security expert will provide you with the software and guide for initializing Dedicated HSM instances. If you have any questions, contact the expert.</li> </ul> <p><b>NOTE</b> You can submit a <a href="#">Service Ticket</a> to provide the UKey recipient address and contact security experts for guidance.</p>	Dedicated HSM security expert
5	Initialize and manage instances (involving UKey authentication).	<ol style="list-style-type: none"> <li>Install the tool for managing Dedicated HSM instances on the instance management node.</li> <li>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.</li> </ol> <p>For details, see <a href="#">Initializing a Dedicated HSM Instance</a>.</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 <a href="#">Installing the Security Agent and Granting Access Permissions</a>.</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 > Data Encryption Workshop**.

**Step 4** In the navigation pane on the left, choose **Dedicated HSM > Instances**.

**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

计费模式

包年/包月

**Step 7** Select a region and project.

Figure 4-3 Selecting a region

当前区域

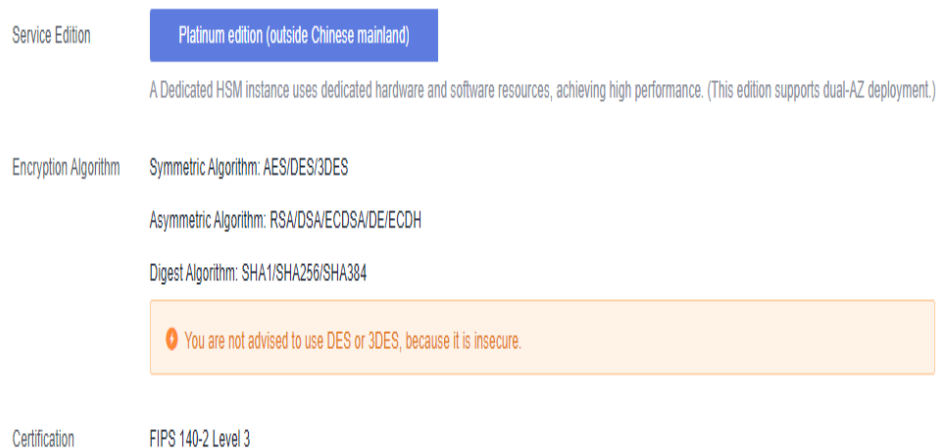
当前项目

 **NOTE**

- Select the current region and the default project.
- Only the default project is supported. User-defined projects cannot be created.


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

**Figure 4-4** Platinum edition (outside Chinese mainland)



Service Edition **Platinum edition (outside Chinese mainland)**  
A Dedicated HSM instance uses dedicated hardware and software resources, achieving high performance. (This edition supports dual-AZ deployment.)

Encryption Algorithm  
Symmetric Algorithm: AES/DES/3DES  
Asymmetric Algorithm: RSA/DSA/ECDSA/DE/ECDH  
Digest Algorithm: SHA1/SHA256/SHA384

 You are not advised to use DES or 3DES, because it is insecure.

Certification FIPS 140-2 Level 3

**Table 4-2** Edition parameters

Parameter	Description
Service Edition	Platinum edition (outside Chinese mainland)
Encryption Algorithm	Algorithm supported by the HSM instance. <ul style="list-style-type: none"> <li>• Symmetric algorithm: AES</li> <li>• Asymmetric algorithm: RSA, DSA, ECDSA, DE, and ECDH</li> <li>• Digest algorithm: SHA1, SHA256, SHA384</li> </ul>
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**.
- **Contact Information**: Enter the phone number and email address to receive the progress information of the service ticket.

**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 4-5** Creating a service ticket

**Create Service Ticket**

① Select Service/Product ——— ② Select Issue Category ——— ③ Submit Service Ticket

**My Issue: DEW - General Consulting**

\* Region

\* Case Severity

\* Problem Description

UKey Recipient Information

26/1,200

Upload Attachments

---

**Contact Options**

Contact Information

---

I have read and agree to the [Ticket Service Protocol](#) 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 cannot be changed to another type. 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.

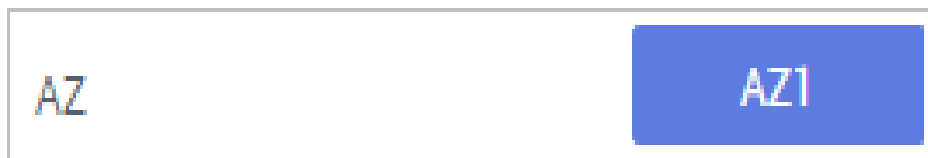
**Step 3** Click . Choose **Security > Data Encryption Workshop**.

**Step 4** In the navigation pane on the left, choose **Dedicated HSM > Instances**.

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

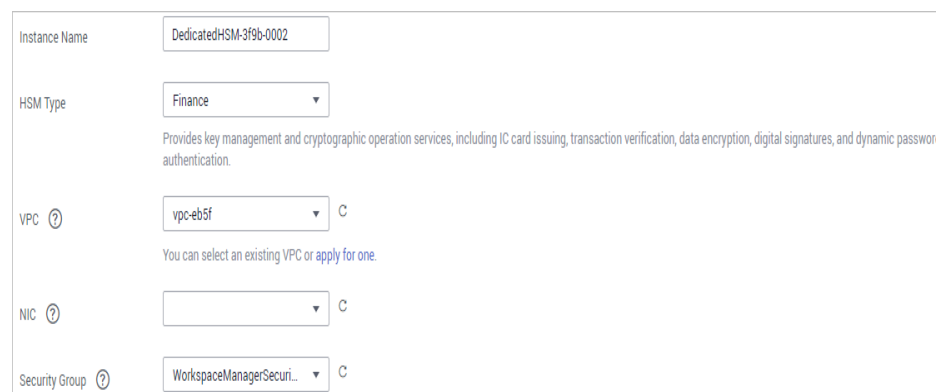
**Step 6** Select an AZ.

**Figure 4-6** Selecting an AZ



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

**Figure 4-7** Configuring a Dedicated HSM instance

A screenshot of a configuration form for a Dedicated HSM instance. The form contains the following fields:

- Instance Name: DedicatedHSM-3f9b-0002
- HSM Type: Finance (dropdown menu)
- VPC: vpc-eb5f (dropdown menu) with a 'C' icon and a note: "You can select an existing VPC or apply for one."
- NIC: (empty dropdown menu) with a 'C' icon
- Security Group: WorkspaceManagerSecuri... (dropdown menu) with a 'C' icon

**Table 4-3** Activation parameters

Parameter	Description	Example Value
Instance Name	Name of a Dedicated HSM instance <b>NOTE</b> The instance name can contain only letters, digits, underscores (_), and hyphens (-).	DedicatedHSM-3c98-0002
Enterprise Project	Enterprise project that the dedicated HSM is to be bound to	default
HSM Type	Available HSM types include <b>Finance</b> , <b>Server</b> , and <b>Signature server</b> . <ul style="list-style-type: none"><li>• <b>Finance</b>: Provides key management and encryption computing services, including IC card issuing, transaction verification, data encryption, digital signatures, and dynamic password authentication.</li><li>• <b>Server</b>: Provides secure, complete key management services and high-performance concurrent cryptographic operations, such as data signatures, signature verification, and data encryption/decryption.</li><li>• <b>Signature server</b>: Guarantees the integrity, confidentiality, anti-repudiation, and post-event traceability of user data by using digital signatures, digital envelopes, and digital digests.</li></ul>	<b>Finance</b>
VPC	You can select an existing Virtual Private Cloud (VPC), or click <b>Apply for VPC</b> to create one.  For more information about VPC, see the <i>Virtual Private Cloud User Guide</i> .	vpc-test-dhsm
Subnet	All available subnets are displayed on the page. The system automatically assigns three IP address to the instance. For more information about subnets, see the <i>Virtual Private Cloud User Guide</i> . <b>NOTE</b> 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.	<b>subnet-test-dhsm (192.168.0.0/24)</b>
EIP Binding	After this parameter is enabled, you can bind an EIP to the Dedicated HSM instance to enable public access to the instance.	-



Parameter	Description	Example Value
Security Group	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. For more information about security groups, see the <i>Virtual Private Cloud User Guide</i> .	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 locate the instance, and click **Delete**. 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 > Data Encryption Workshop**.

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

**Step 4** You can check the Dedicated HSM instance information in the list. The following table describes the parameters.

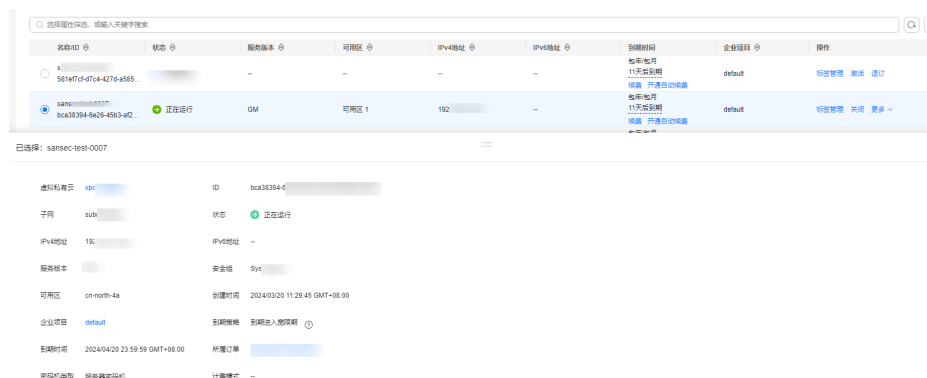
**Table 4-4** Dedicated HSM instance parameters

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"> <li>● <b>Installing</b> After you pay the initial installation fee, the purchased instance will be installed. The status of the Dedicated HSM instance will be <b>Installing</b>.</li> <li>● <b>To be activated</b> The status of an instance that has been installed but not activated is <b>To be activated</b>.</li> <li>● <b>Creating</b> 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 <b>Creating</b> during this process.</li> <li>● <b>Creation failed</b> 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 <b>Creation failed</b>.</li> <li>● <b>Running</b> After an instance is configured and allocated, it will be in the status of <b>Running</b>.</li> <li>● <b>Frozen</b> If an instance is not renewed upon its expiration, its status changes to <b>Frozen</b>.</li> </ul>
Service Edition	Platinum edition (outside Chinese mainland): You can exclusively use the HSM subrack, power supply, the network bandwidth, and API resources of the HSM.
AZ	AZ of a device
Expiration Time	Expiration time of the purchased HSM instance.

**Step 5** You can click the name of an instance to view details about the instance, as shown in [Figure 4-8](#).

**Figure 4-8** Details about Dedicated HSM instances



Parameter	Value
Name	DedicatedHSM-ee7c-000134b53k4gsl
ID	c492f912-1a5c-4e96-81...
Status	192.168.0.47
Service Edition	Basic edition
AZ	
Device Vendor	TASS
Device Model	SJ1528
HSM Type	Finance
VPC	vpc-HSM
Subnet	subnet-HSM
IP Address	192.168.0.47
Security Group	default
Creation Time	2020/02/20 21:14:53 GMT+08:00
Expiration Time	2020/09/04 23:59:59 GMT+08:00
Order	CS190904
Billing Mode	Yearly/Monthly

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"> <li>● <b>Installing</b> After you pay the initial installation fee, the purchased instance will be installed. The status of the Dedicated HSM instance will be <b>Installing</b>.</li> <li>● <b>To be activated</b> The status of an instance that has been installed but not activated is <b>To be activated</b>.</li> <li>● <b>Creating</b> 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 <b>Creating</b> during this process.</li> <li>● <b>Creation failed</b> 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 <b>Creation failed</b>.</li> <li>● <b>Running</b> After an instance is configured and allocated, it will be in the status of <b>Running</b>.</li> <li>● <b>Frozen</b> If an instance is not renewed upon its expiration, its status changes to <b>Frozen</b>.</li> </ul>
Service Edition	Platinum edition (outside Chinese mainland): You can exclusively use the HSM subrack, power supply, the network bandwidth, and API resources of the HSM.
HSM Type	HSM types of an instance, including <b>Finance</b> , <b>Server</b> , and <b>Signature verification server</b> .

Parameter	Description
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

----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.

Item	Description	How to Obtain
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 <a href="#">Purchasing an ECS</a> .
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.

 **NOTE**

EIP: Bind an EIP to use the HSM as an instance locally. For details about how to bind an EIP, see [How Do I Enable Public Access to a Dedicated HSM Instance?](#)

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

## 4.5 Managing Tags

### 4.5.1 Adding a Tag

You can use tags to identify Dedicated HSM instances. Tags can be added to Dedicated HSM instances to facilitate instance classification and query.

## Procedure



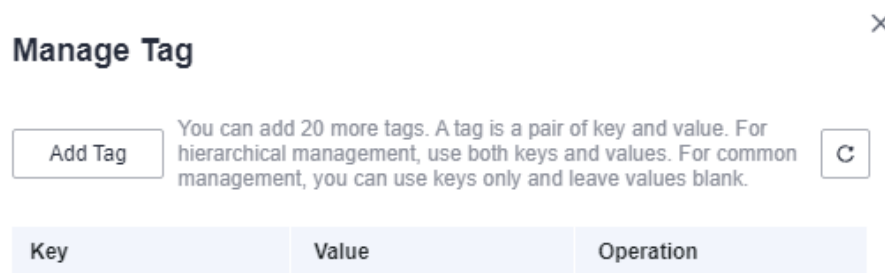
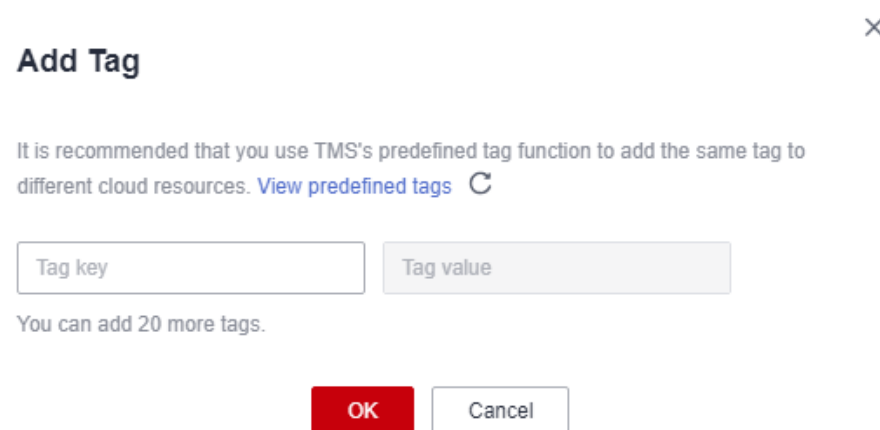
- Step 1** Click  in the upper left corner of the management console and select a region or project.
- Step 2** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Step 3** In the navigation pane, choose **Dedicated HSM**.
- Step 4** In the **Operation** column of an instance, click **Manage Tag**. The **Manage Tag** page is displayed, as shown in [Figure 4-9](#).

Figure 4-9 Manage Tag



- Step 5** Click **Add Tag**. In the dialog box that is displayed, enter the tag key and tag value. For details about the parameters, see [Table 4-7](#).

Figure 4-10 Adding a tag



### 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 4-7** Tag parameters

Parameter	Description	Remarks
Tag key	<p>Tag name.</p> <p>The tag keys of a secret cannot have duplicate values. A tag key can be used for multiple secrets.</p> <p>A secret can have up to 20 tags.</p>	<ul style="list-style-type: none"> <li>• Mandatory.</li> <li>• The tag key must be unique for the same custom key.</li> <li>• 128 characters limit.</li> <li>• The value cannot start or end with a space.</li> <li>• Cannot start with <b>_sys_</b>.</li> <li>• The following character types are allowed: <ul style="list-style-type: none"> <li>- Chinese</li> <li>- English</li> <li>- Numbers</li> <li>- Space</li> <li>- Special characters: <code>._:/=+-@</code></li> </ul> </li> </ul>
Tag value	Value of the tag	<ul style="list-style-type: none"> <li>• Optional</li> <li>• 255 characters limit.</li> <li>• The following character types are allowed: <ul style="list-style-type: none"> <li>- Chinese</li> <li>- English</li> <li>- Numbers</li> <li>- Space</li> <li>- Special characters: <code>._:/=+-@</code></li> </ul> </li> </ul>

**Step 6** Click **OK**.

----End



## 4.5.2 Searching for a Dedicated HSM Instance by Tag

This section describes how to search for HSM instances by tag in the current project on the **Instances (New)** page.

### Prerequisites

Tags have been added.

## Procedure

- Step 1** Click  in the upper left corner of the management console and select a region or project.
- Step 2** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Step 3** In the navigation pane, choose **Dedicated HSM**.
- Step 4** Click the search box and select a tag as the filter attribute to search for Dedicated HSM instances, as shown in [Figure 4-11](#).

**Figure 4-11** Searching for a Dedicated HSM instance



Name	ID	Status	Service Edition	AZ	IP Address	Expiration Time	Enterprise Project	Operation
1C	b4	Creating	--	AZ 3	--	9 hours 18 minutes until expi...	default	Manage Tag

----End

## 4.5.3 Modifying a Tag Value

This section describes how to modify tag values on the Dedicated HSM page.

### Procedure



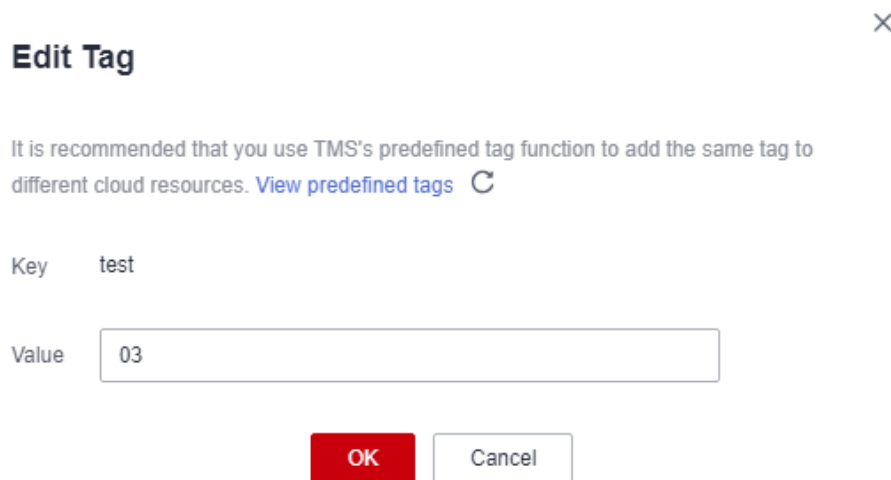
- Step 1** Click  in the upper left corner of the management console and select a region or project.
- Step 2** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Step 3** In the navigation pane, choose **Dedicated HSM**.
- Step 4** Click **Manage Tag** in the row where the target instance is located. The **Manage Tag** dialog box is displayed.
- Step 5** Click **Edit**. The **Edit Tag** dialog box is displayed. After changing the tag value, click **OK**.

Figure 4-12 Editing a tag



----End

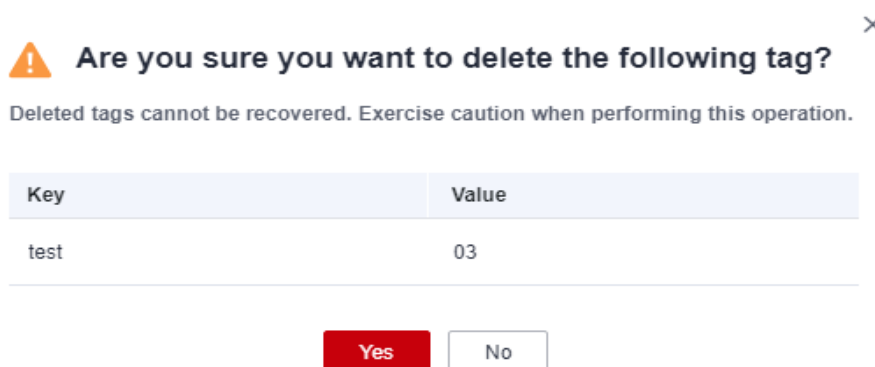
## 4.5.4 Deleting a Tag

This section describes how to delete tags on the Dedicated HSM page.

### Procedure

- Step 1** Click in the upper left corner of the management console and select a region or project.
- Step 2** Click . Choose **Security & Compliance > Data Encryption Workshop**.
- Step 3** In the navigation pane, choose **Dedicated HSM**.
- Step 4** Click **Manage Tag** in the row where the target instance is located. The **Manage Tag** dialog box is displayed.
- Step 5** In the **Operation** column of a tag, click **Delete**.

Figure 4-13 Deleting a tag



**Step 6** In the **Delete Tag** dialog box, click **Yes**.  
----End

# 5 Auditing Logs

## 5.1 Operations supported by CTS

The tables in this section describe the DEW operations supported by CTS.

**Table 5-1** KMS operations recorded by CTS

Operation	Resource Type	Trace Name
Create a key	cmk	createKey
Create a DEK	cmk	createDataKey
Create a plaintext-free DEK	cmk	createDataKeyWithout-Plaintext
Enable a key	cmk	enableKey
Disable a key	cmk	disableKey
Encrypt a DEK	cmk	encryptDatakey
Decrypt a DEK	cmk	decryptDatakey
Schedule key deletion	cmk	scheduleKeyDeletion
Cancel scheduled key deletion	cmk	cancelKeyDeletion
Generate random numbers	rng	genRandom
Modify a key alias	cmk	updateKeyAlias
Modify key description	cmk	updateKeyDescription
Prompt risks about CMK deletion	cmk	deleteKeyRiskTips
Import key materials	cmk	importKeyMaterial

Operation	Resource Type	Trace Name
Delete key materials	cmk	deleteImportedKeyMaterial
Create a grant	cmk	createGrant
Retire a grant	cmk	retireGrant
Revoke a grant	cmk	revokeGrant
Encrypt data	cmk	encryptData
Decrypt data	cmk	decryptData
Add a tag	cmk	dealUnifiedTags
Delete a tag	cmk	dealUnifiedTags
Add tags in batches	cmk	dealUnifiedTags
Delete tags in batches	cmk	dealUnifiedTags
Enable key rotation	cmk	enableKeyRotation
Modify key rotation interval	cmk	updateKeyRotationInterval

**Table 5-2** KMS operations recorded by CSMS

Operation	Resource Type	Trace Name
Create a secret	secret	createSecret
Update a secret	secret	updateSecret
Delete a secret	secret	forceDeleteSecret
Schedule the deletion of a secret	secret	scheduleDelSecret
Cancel the scheduled secret deletion	secret	restoreSecretFromDeletedStatus
Create a secret status	secret	createSecretStage
Update a secret status	secret	updateSecretStage
Delete a secret status	secret	deleteSecretStage
Create a secret version	secret	createSecretVersion
Download a secret backup	secret	backupSecret
Restore a secret backup	secret	restoreSecretFromBackupBlob

Operation	Resource Type	Trace Name
Update the secret version	secret	putSecretVersion
Start the secret rotation	secret	rotateSecret
Create a secret event	secret	createSecretEvent
Update a secret event	secret	updateSecretEvent
Delete a secret event	secret	deleteSecretEvent
Create a resource tag	secret	createResourceTag
Delete a resource tag	secret	deleteResourceTag

**Table 5-3** KMS operations recorded by KPS

Operation	Resource Type	Trace Name
Create or import an SSH key pair	keypair	createOrImportKeypair
Delete an SSH key pair	keypair	deleteKeypair
Import a private key	keypair	importPrivateKey
Export a private key	keypair	exportPrivateKey
Bind an SSH key pair	keypair	bindKeypair
Unbind an SSH key pair	keypair	unbindKeypair
Clear private keys	keypair	clearPrivateKey

**Table 5-4** KMS operations recorded by Dedicated HSM

Operation	Resource Type	Trace Name
Purchase an HSM instance	hsm	purchaseHsm
Configure an HSM instance	hsm	createHsm
Delete an HSM instance	hsm	deleteHsm

## 5.2 Querying Real-Time Traces


### Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

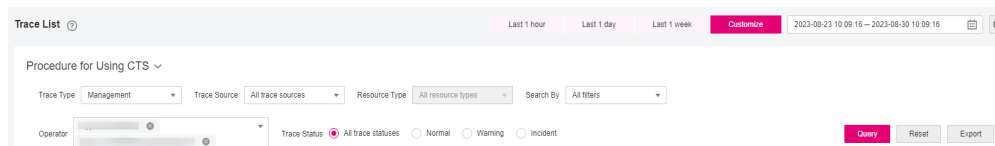
This section describes how to query and export operation records of the last seven days on the CTS console.

- [Viewing Real-Time Traces in the Trace List](#)

### Viewing Real-Time Traces in the Trace List



1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Set filters to search for your desired traces, as shown in [Figure 5-1](#). The following filters are available:

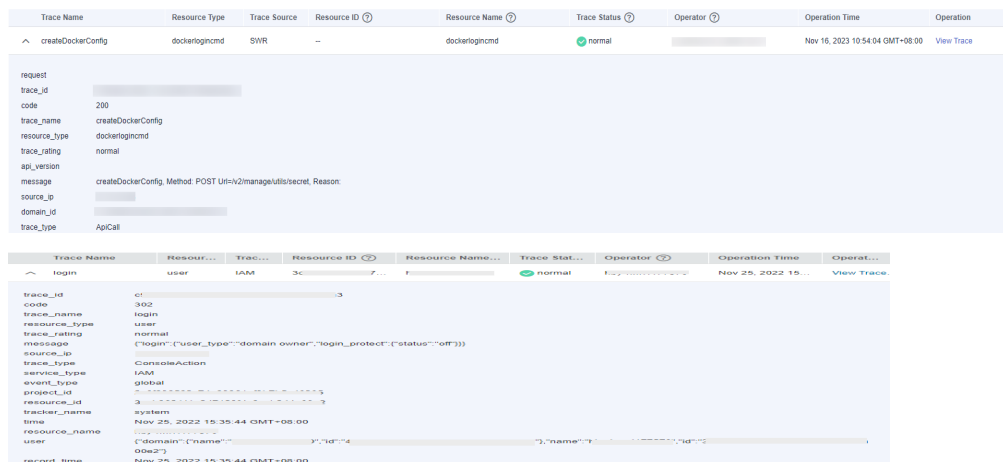
**Figure 5-1** Filters



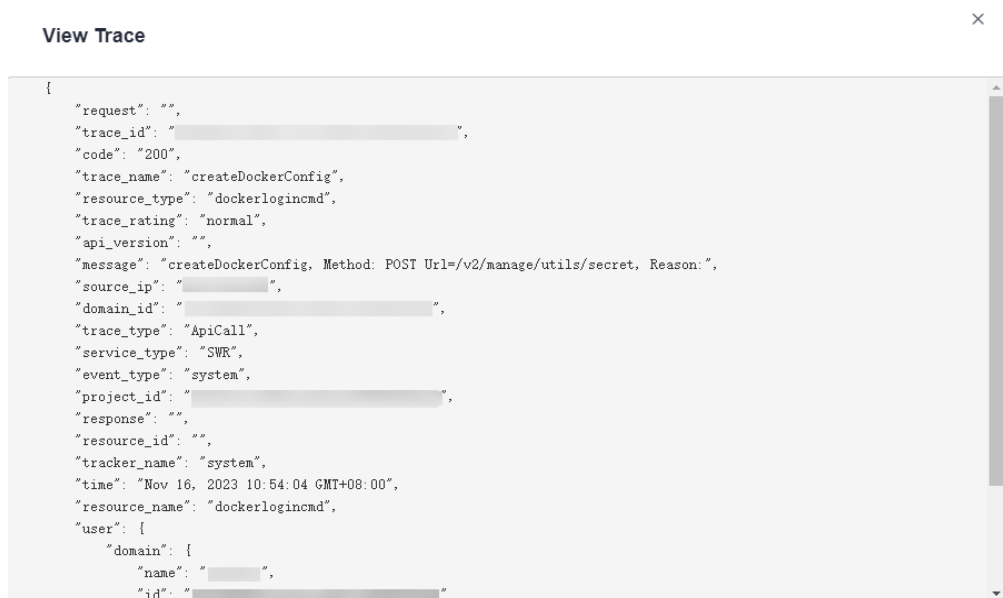
- **Trace Type, Trace Source, Resource Type, and Search By:** Select a filter from the drop-down list.
    - If you select **Resource ID** for **Search By**, specify a resource ID.
    - If you select **Trace name** for **Search By**, specify a trace name.
    - If you select **Resource name** for **Search By**, specify a resource name.
  - **Operator:** Select a user.
  - **Trace Status:** Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
  - **Time range:** You can query traces generated during any time range in the last seven days.
  - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
5. Click **Query**.
  6. On the **Trace List** page, you can also export and refresh the trace list.
    - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.



- Click  to view the latest information about traces.
7. Click  on the left of a trace to expand its details.



8. Click **View Trace** in the **Operation** column. The trace details are displayed.



9. For details about key fields in the trace structure, see section "Trace References" > "Trace Structure" and section "Trace References" > "Example Traces" in the *CTS User Guide*.

# 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.
- Entrust a Huawei account or cloud service to perform professional, efficient O&M on your DEW resources.

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

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

### Prerequisites

Before granting permissions to a user group, you need to understand the available DEW permissions, and grant permissions based on the real-life scenario. The following tables describe the permissions supported in DEW.

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

**Table 6-1** KMS system policies

Role/Policy	Description	Type	Dependency
KMS Administrator	All permissions of KMS	Role	None

Role/Policy	Description	Type	Dependency
KMS CMKFullAccess	All permissions for KMS keys. Users with these permissions can perform all the operations allowed by policies.	Policy	None
KMS CMKReadOnlyAccess	Read-only permissions for KMS keys. Users with these permissions can perform all the operations allowed by policies.	Policy	None

**Table 6-2** KPS system policies

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

**Table 6-3** CSMS system policies

Role/Policy	Description	Type	Dependency
CSMS FullAccess	All permissions for CSMS in DEW. Users with these permissions can perform all the operations allowed by policies.	Policy	None
CSMS ReadOnlyAccess	Read-only permissions for CSMS in DEW. Users with these permissions can perform all the operations allowed by policies.	Policy	None

**Table 6-4** describes the common operations supported by each system-defined permission of DEW. Select the permissions as needed.

**Table 6-4** Common operations supported by each system-defined policy or role

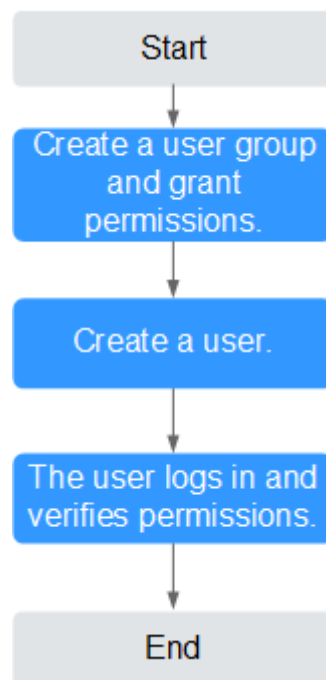
Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
Creating a key	√	√	x	x
Enable a key	√	√	x	x
Disable a key	√	√	x	x
Schedule key deletion	√	√	x	x
Cancel scheduled key deletion	√	√	x	x
Modify a key alias	√	√	x	x
Modify key description	√	√	x	x
Generate a random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

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
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
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

Operation	KMS Administrator	KMS CMKFullAccess	DEW KeypairFullAccess	DEW KeypairReadOnlyAccess
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
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. **Creating a User Group and Assigning Permissions**

Create a user group on the IAM console and grant the user group the **KMS CMKFullAccess** permission (indicating full permissions for keys).

### 2. **Creating an IAM User**

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 the assigned permissions.

- 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](#). This section describes typical DEW custom policies.

## Example Custom Policies of DEW

- 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"  
      ]  
    }  
  ]  
}
```